BULLETIN DE LA S. M. F.

JACQUES TILOUINE

Un sous-groupe p-divisible de la jacobienne de $X_1(Np_r)$ comme module sur l'algèbre de Hecke

Bulletin de la S. M. F., tome 115 (1987), p. 329-360

<http://www.numdam.org/item?id=BSMF_1987__115__329_0>

Bull. Soc. math. France,
115, 1987, p. 329-360.

UN SOUS-GROUPE p-DIVISIBLE DE LA JACOBIENNE DE $X_1(Np^r)$ COMME MODULE SUR L'ALGÈBRE DE HECKE

PAR

JACQUES TILOUINE (*)

RÉSUMÉ. — Dans cet article, nous déterminons la structure d'un groupe p-divisible de la jacobienne de $X_1(Np^r)$ sur l'algèbre de Hecke, sous des hypothèses pour restrictives permettant ainsi de généraliser des résultats d'interpolation p-adique obtenus par Hida dans [7].

ABSTRACT. — In this paper, we determine the structure of a certain p-divisible group of the jacobian of $X_1(Np^r)$ as a module over the Hecke algebra, under rather weak hypotheses. This will allows us to generalize in a forthcoming paper some results of Hida [7] on p-adic interpolation of special values of L series.

Soit $\mathfrak{h}$ le demi-plan de Poincaré muni de l'action habituelle de $SL_2(\mathbf{Z})$ et soit $\mathfrak{h}^* = \mathfrak{h} \cup \mathbf{P}^1(\mathbf{Q})$, le demi-plan complété. L'élément de $\mathbf{P}^1\mathbf{Q} \backslash \mathbf{Q}$ est noté ∞. Pour chaque entier $M \geqslant 1$, on note $\Gamma_1(M)$ le sous-groupe de $SL_2(\mathbf{Z})$ constitué des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a \equiv d \equiv 1$ modulo M et $c \equiv 0$ modulo M. On peut munir l'espace quotient $\Gamma_1(M) \backslash \mathfrak{h}^*$ d'une structure de surface de Riemann compacte connexe. Son corps des fonctions admet un modèle défini sur $\mathbf{Q}$ composé des fonctions invariantes par $\Gamma_1(M)$ dont le q-développement au point ∞ est à coefficients rationnels. On note $X_1(M)$ la courbe algébrique définie sur $\mathbf{Q}$ projective lisse géométriquement connexe associée à ce corps de fonctions. On note φ la projection de $\mathfrak{h}^*$ sur $X_1(M)(\mathbf{C})$. Par construction $\varphi(\infty)$ est rationnel sur $\mathbf{Q}$.

On fixe désormais un entier $N \geqslant 1$ et p un nombre premier $\geqslant 5$ ne divisant pas N. Pour chaque $r \geqslant 1$, on note en abrégé $X_r = X_1(Np^r)$.

(*) Texte reçu le 10 février 1986, révisé le 16 février 1987

J. TILOUINE, Mathématiques, Bât. n 425, Université Paris-Sud, 91405 Orsay Cedex.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE — 0037-9484/1987/03 329 32/$5.20

Le groupe $G_r=(\mathbf{Z}/Np^r\mathbf{Z})^\times/\{\pm 1\}$ opère fidèlement par automorphismes $\mathbf{Q}$-rationnels sur X_r.

On note $a\mapsto\langle a\rangle$ (diamant de a) cette action. Elle est caractérisée par la formule suivante : pour $a\in G_r$, soit γ_a dans $SL_2(\mathbf{Z})$ tel que $\gamma_a\equiv\begin{pmatrix}a^{-1} & 0\\ 0 & a\end{pmatrix}$ mod. Np^r, pour tout z de $\mathfrak{h}$, $\langle a\rangle\varphi(z)=\varphi(\gamma_a(z))$.

Rappelons de plus qu'on peut définir pour chaque nombre premier l une correspondance de Hecke $T(l)$ sur X_r, rationnelle sur $\mathbf{Q}$ et caractérisée par les formules :

$$T(l)\varphi(z)=\begin{cases}\sum_{i=0}^{l-1}\varphi\left(\dfrac{z+i}{l}\right)+\langle l\rangle(\varphi(lz)) & \text{si } l\nmid Np\\ \sum_{i=0}^{l-1}\varphi\left(\dfrac{z+i}{l}\right) & \text{si } l\mid Np.\end{cases}$$

Pour $M\geqslant 1$, on note $J_1(M)$ la jacobienne de $X_1(M)/\mathbf{Q}$ et on note en abrégé J_r la jacobienne de X_r. On note $h_r(\mathbf{Z})$ l'algèbre engendrée sur $\mathbf{Z}$ par les correspondances de Hecke et les diamants dans l'anneau des endomorphismes $\mathbf{Q}$-rationnels de J_r vue comme variété de Picard de X_r. Pour tout anneau A, on pose $h_r(A)=h_r(\mathbf{Z})\otimes A$. On abrège $h_r=h_r(\mathbf{Z}_p)$.

Le but de cet article est d'améliorer un résultat récent de Hida sur la structure d'une partie du groupe p-divisible

$$J_{r,p}=J_r[p^\infty]$$

comme module sur l'algèbre de Hecke h_r. Nous aurons besoin pour préciser l'énoncé de notations supplémentaires.

Soit

$$J_{\infty,p}=\varinjlim_r J_{r,p}$$

où les applications de transition sont déduites des revêtements naturels $X_r\to X_s$ pour $r\geqslant s\geqslant 1$.

Posons de plus

$$h_\infty=\varprojlim_r h_r.$$

C'est une $\mathbf{Z}_p$-algèbre compacte opérant fidèlement sur J_{∞,p^r}. De plus h_∞ est une algèbre sur l'algèbre d'Iwasawa $\Lambda = \mathbf{Z}_p[[\Gamma]]$ où Γ est la pro-p-partie de $G_\infty = \varprojlim_r G_r = G_1 \times \Gamma$ vu comme sous-groupe de h_∞ via la représentation « diamant ».

Soit e (resp. e_r) l'idempotent de h_∞ (resp. de h_r) associé à $T(p)$ (*voir* [4], p. 236). On pose :

$$h_\infty^0 = eh_\infty, \qquad h_r^0 = e_r h_r.$$

HIDA [6] a montré que h_∞^0 est un Λ-module libre de type fini. En particulier, on peut la décomposer en un produit fini d'algèbres locales grâce au lemme de Hensel.

On choisit $\gamma = \langle 1 + Np \rangle \in \Lambda$ comme générateur topologique de Γ, et on note $\omega_r = \gamma^{p^{r-1}} - 1$. Le second résultat de théorie d'Iwasawa de l'algèbre h_∞^0 que nous invoquons alors ([7], théorème 1.2) affirme que la projection naturelle $h_\infty^0 \to h_r^0$ se factorise en un isomorphisme

$$h_\infty^0/\omega_r h_\infty^0 \simeq h_r^0.$$

Si donc R est un facteur local de h^0, $R_r = R/\omega_r R$ est facteur local de h_r^0 pour chaque $r \geqslant 1$.

D'autre part, le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ contenu dans G_∞ permet une décomposition $h_\infty^0 = \oplus_{a \bmod p-1} h_\infty^0(a)$ où

$$h_\infty^0(a) = \{ t \in h_\infty^0 ; \forall x \in (\mathbf{Z}/p\mathbf{Z})^\times ; \langle x \rangle . t = \omega^a(x) . t \},$$

où ω désigne le caractère de Teichmüller : $(\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times$.

On fixe désormais une composante locale R de h_∞^0 d'idempotent $1_R \in h_\infty^0$ et on suppose que l'entier a modulo $p-1$ pour lequel $R \subset h_\infty^0(a)$ vérifie l'hypothèse :

$$(\bigstar) \qquad a \neq -1, 0.$$

Soit $J_{\infty,p}(R) = 1_R J_{\infty,p}(\bar{\mathbf{Q}})$. C'est la limite inductive des groupes p-divisibles $1_{R_r} J_{r,p}(\bar{\mathbf{Q}})$. Soit $\mathbf{\Pi}_p = \mathbf{Q}_p/\mathbf{Z}_p$ le tore p-adique. Le théorème démontré dans cet article s'énonce alors :

THÉORÈME. — *Sous l'hypothèse* ($\bigstar$), *on a pour chaque r des isomorphismes compatibles de R_r-modules* :

$$J_{r,p}(R) \simeq (R_r \otimes \mathbf{\Pi}_p) \oplus \mathrm{Hom}(R_r, \mathbf{\Pi}_p)$$

d'où à la limite :

$$J_{\infty,p}(R) \simeq R \otimes_{\Lambda} \mathrm{Hom}(\Lambda, \Pi_p) \oplus \mathrm{Hom}(R, \Pi_p).$$

Le résultat analogue de Hida nécessitait l'hypothèse $(a, p-1) > 1$ donc excluait beaucoup de classes modulo $p-1$. La conséquence de l'affaiblissement d'hypothèses est de permettre au théorème III d'interpolation de [7] de rester valide pour toutes les branches de la fonction L autres que 1 et 2 modulo $p-1$ (*cf.* [7], § 1, pour le décalage de deux unités entre notre énoncé et celui du théorème III).

Pour démontrer cela, on loge, pour chaque $r \geqslant 1$, $J_{r,p}(R)$ dans une sous-variété abélienne A_r de J_r, ayant bonne réduction potentielle en p, puis on identifie cette variété à isogénie près au bon quotient de Mazur-Wiles B_r. On détermine alors la structure de la partie ordinaire du groupe p-divisible de B_r en suivant les idées de [15].

Je tiens à remercier J. Coates pour les exhortations incessantes au travail « concret » qu'il ne se lasse pas de me prodiguer, et H. Hida pour m'avoir suggéré la possibilité de ce travail, avoir répondu sans s'énerver aux questions tous azimuts dont je l'ai agoni et pour m'avoir communiqué le manuscrit de Mazur-Wiles utilisé ici.

1. Une sous-variété abélienne de J_r avec bonne réduction potentielle en p

Pour $C \geqslant 1$, on note $S_2(\Gamma_1(C))$ l'espace des formes $\Gamma_1(C)$-modulaires paraboliques de poids 2. Si $f \in S_2(\Gamma_1(C))$, on note

$$f = \sum_{n \geqslant 1} a(n, f) q^n \qquad \text{où} \quad q = e^{2i\pi z}$$

le q-développement de f. L'algèbre de Hecke $h_r(\mathbf{C})$ opère fidèlement sur $S_2(\Gamma_1(C))$.

Soit f une forme propre pour $h_r(\mathbf{C})$, normalisée :

$$\text{i.e. } \forall n \geqslant 1, \quad f \mid T(n) = a(n, f).f.$$

On la suppose en outre primitive au sens d'Atkin-Lehner [2]. On abrège propre normalisée primitive en p. n. p.

On note A_f la sous-variété abélienne de $J_1(C)$ définie par Shimura [19], (théorème 7.14) attachée à f.

Pour chaque diviseur $C \geqslant 1$ de $M = Np^r$ et $t \geqslant 1$, diviseur de M/C, on a un morphisme naturel $\mathbf{Q}$-rationnel $X_1(M) \to X_1(C)$ déduit de l'inclusion $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(M) \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}^{-1} \subset \Gamma_1(C)$.

En passant aux variétés de Picard, on obtient un morphisme $\mathbf{Q}$-rationnel

$$[t] : \quad J_1(C) \to J_r$$

dont l'application tangente s'identifie à

$$S_2(\Gamma_1(C)) \to S_2(\Gamma_1(M))$$
$$g \mapsto g(tz) = g \,|\, [t](z).$$

Or, la théorie d'Atkin-Lehner nous fournit une décomposition :

$$S_2(\Gamma_1(M)) = \oplus_{C \,|\, M,\, t \,|\, M/C} S_2^{\text{new}}(\Gamma_1(C)) \,|\, [t]$$

où $S_2^{\text{new}}(\Gamma_1(C))$ désigne le sous-espace de $S_2(\Gamma_1(C))$ composé des formes nouvelles au sens d'Atkin-Lehner.

On peut interpréter cette égalité par une isogénie : on fixe pour chaque $C \,|\, M$ une base $\mathscr{B}_C$ de $S_2^{\text{new}}(\Gamma_1(C))$ diagonalisant l'action de l'algèbre de Hecke, et on note pour $C \,|\, M$, n_C le nombre de diviseurs de M/C. Les applications produits des $[t] : A_f \to J_r$, t parcourant l'ensemble des diviseurs de M/C et f parcourant $\mathscr{B}_C$, donnent une isogénie :

$$\prod_{C \,|\, M} \prod_{f \in \mathscr{B}_C} A_f^{n_C} \to J_r$$

Grâce à l'hypothèse (★) on a $a \neq 0$, on voit donc aisément en comparant les modules de Tate que le groupe p-divisible $J_{r,p}(R)$ est contenu dans la somme des groupes p-divisibles des images $A_f \,|\, [t]$ pour des f dont le Nebentypus χ restreint à $(\mathbf{Z}/p\mathbf{Z})^\times$ n'est pas trivial, donc on peut supposer que $p \,|\, C$. Fixons alors un plongement τ de $\bar{\mathbf{Q}}$ dans une clôture algébrique de $\mathbf{Q}_p$ munie de sa valeur absolue normalisée par $|p|_p = p^{-1}$. Suivant Hida [4], on dit que la forme p. n. p. f, de niveau divisible par p, est ordinaire en p (pour τ) si $|\tau(a(p, f))|_p = 1$.

On voit comme précédemment qu'on peut supposer que les formes f intervenant sont ordinaires en p. On invoque alors un résultat de Ogg-Li-Asai ([17], [10], [1]) :

PROPOSITION 1.1. — *Si $f \in S_2(\Gamma_1(C))$ est propre normalisée primitive, $C = C_1 p^\alpha$, $p \nmid C_1$, $\alpha \neq 0$. Soit χ son Nebentypus, $C(\chi) = C_2 p^\beta$, $p \nmid C_2$*

Si $\beta \neq 0$, *on a*

$$\begin{cases} |a(p,f)|^2 = p & si \quad \alpha = \beta \\ = 0 & si \quad \alpha > \beta. \end{cases}$$

On applique cette proposition comme suit. Soit f une forme p. n. p. dont le Nebentypus χ restreint à $(\mathbf{Z}/p\mathbf{Z})^\times$ n'est pas trivial. Soit χ_p la p-partie de χ. Comme $\beta \neq 0$, on conclut que si f est ordinaire en p, χ_p est primitif.

Finalement, toujours en comparant les modules de Tate, on voit qu'on peut se limiter à des diviseurs t de M/C, premiers à p.

On peut donc poser la :

DÉFINITION 1.2. — *Soit* $A_r = \sum_{C \mid M,\ f \in \mathscr{P}_C} A_f[t]$ *où la somme est étendue aux diviseurs C de M divisibles par p, aux formes dans un système maximal* $\mathscr{P}_C$ *de formes* p. n. p. *de niveau C dont la p-partie du Nebentypus est primitive et deux à deux non conjuguées, et t parcourant l'ensemble des diviseurs premiers à p de M/C.*

Soit alors ζ une racine primitive p^r-ième de l'unité. Soit $\mathscr{O}_r = \mathbf{Z}_p[\zeta]$ l'anneau des entiers du corps cyclotomique $k_r = \mathbf{Q}_p(\zeta)$. $\mathscr{O}_r$ est un anneau de valuation discrète complet. On choisit $1-\zeta$ pour uniformisante de $\mathscr{O}_r$. On a le théorème de bonne réduction de Langlands :

THÉORÈME 1.3. — (1) *La variété* A_f *pour* $f \in \mathscr{P}_C$ (resp. A_r) *se prolonge en un schéma abélien sur* $\mathscr{O}_r$.

(2) *La variété* A_r *est stable sous l'action de* $h_r(\mathbf{Z})$.

Preuve :

(1) On applique les théorèmes 7.1 et 7.5 de [9] comme dans [7], §9.

(2) Pour voir la stabilité de A_r sous l'action des opérateurs de Hecke, on considère son espace tangent sur C à l'origine $T_0 A_{r/\mathbf{C}}$: Par définition, on trouve le sous-espace de $S_2(\Gamma_1(M))$

$$T_0 A_{r/\mathbf{C}} = \oplus_{\alpha=1}^{r} \oplus_{\varepsilon} S_2(\Phi_\alpha, \varepsilon)$$

où ε parcourt l'ensemble des caractères de Dirichlet primitifs de conducteur p^α, où $\Phi_\alpha = \Gamma_1(N) \cap \Gamma_0(p^\alpha)$, et l'espace $S_2(\Phi_\alpha, \varepsilon)$ est composé des formes $\Gamma_1(Np^\alpha)$-invariantes telles que si

$$a \in (\mathbf{Z}/Np^\alpha\mathbf{Z})^\times, \qquad a \equiv 1 \bmod N,$$

et $\gamma_a \in \mathrm{SL}_2(\mathbf{Z})$ vérifie $\gamma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$ modulo Np^α, on ait $f|\gamma_a = \varepsilon(a).f$.

Chaque espace $S_2(\Phi_\alpha, \varepsilon)$ est stable par $h_r(\mathbf{Z})$ car $\alpha \neq 0$, donc $T_0 A_{r/\mathbf{C}}$ est stable dans $h_r(\mathbf{Z})$.

Ainsi A_r est une sous-variété abélienne de J_r, définie sur $\mathbf{Q}$, stable par $h_r(\mathbf{Z})$ et ayant bonne réduction sur k_r.

DÉFINITION 1.4. — *On note $J_{r,p}(R)/\mathcal{C}_r$ l'adhérence schématique de $J_{r,p}(R)/k_r$ dans le schéma abélien $A_r/\mathcal{C}_r$. C'est un schéma en groupes p-divisibles au sens de Tate* [21].

On va maintenant comparer A_r et le bon quotient de Mazur-Wiles.

2. Le bon quotient B_r

Soit $r \geqslant 1$ et i un entier compris entre 0 et r.

Soit $\Phi_r^i = \Gamma_0(p^r) \cap \Gamma_1(Np^i)$. En particulier avec les notations précédentes, on a $\Phi_r^0 = \Phi_r$ et $\Phi_r^r = \Gamma_1(Np^r)$.

On note Z_r le modèle canonique sur $\mathbf{Q}$ de la surface de Riemann $\Phi_r^{r-1} \backslash \mathfrak{h}^*$ (i. e. le corps des fonctions est composé des fonctions invariantes sous Φ_r^{r-1}, de q-développement rationnel à l'∞). Des inclusions $\Gamma_1(Np^r) \subset \Phi_r^{r-1} \subset \Gamma_1(Np^{r-1})$ on déduit les $\mathbf{Q}$-morphismes :

$$X_r \xrightarrow{\pi} Z_r \xrightarrow{\rho} X_{r-1}$$

d'où en passant aux jacobiennes vues comme variétés de Picard :

$$JZ_r \xrightarrow{\pi^*} JX_r = J_r$$

et en passant aux jacobiennes vues comme variétés d'Albanese :

$$JZ_r \xrightarrow{\rho_*} J_{r-1}.$$

On construit les « bons quotients » par récurrence comme suit :

(i) $B_1 = J_1/\pi^* JZ_1$.

(ii) Si on s'est donné $J_{r-1} \xrightarrow{\alpha_{r-1}} B_{r-1}$ avec B_{r-1} et α_{r-1} définis sur $\mathbf{Q}$, on définit

$$K_r = \mathrm{Ker}\,(JZ_r \xrightarrow{\alpha_{r-1} \circ \rho_*} B_{r-1}) \qquad \text{et} \qquad J_r \xrightarrow{\alpha_r} B_r = J_r/\pi^* K_r$$

Il est clair que α_r et B_r sont définis sur $\mathbf{Q}$. Soit w_M l'involution de Weil, c'est un automorphisme de X_r défini sur $\mathbf{Q}(\zeta_M)$ déduit de l'action de $\begin{pmatrix} 0 & -1 \\ M & 0 \end{pmatrix}$ (*cf.* [2]). Notons $h_r(\mathbf{Z})^*$ l'image de l'algèbre $h_r(\mathbf{Z})$ par l'automorphisme de $\mathrm{End}(J_r)$ de conjugaison par w_M. C'est aussi l'image de $h_r(\mathbf{Z})$ par l'involution de Rosati de J_r associé à l'autodualité canonique de la jacobienne. Donc tous les éléments de $h_r(\mathbf{Z})^*$ sont définis sur $\mathbf{Q}$.

Notons encore, pour chaque $r \geqslant 1$, β_r le morphisme $\alpha_r \circ w_M$. On note encore α_r (resp. β_r) les restrictions de α_r (resp. β_r) à A_r. Remarquons que β_r est définie sur $\mathbf{Q}(\zeta_M)$.

PROPOSITION 2.1 :

(1) *α_r et β_r : $A_r \to B_r$ sont des isogénies (définies resp. sur $\mathbf{Q}$ et $\mathbf{Q}(\zeta_M)$).*

(2) *L'algèbre $h_r(\mathbf{Z})^*$ laisse stable K_r pour chaque $r \geqslant 1$ d'où une représentation $h_r(\mathbf{Z})^* \to \mathrm{End}(B_r)$ et on a :*

$$\forall\, T \in h_r(\mathbf{Z}); \qquad \beta_r \circ T = T^* \circ \beta_r$$

où

$$T^* = w_M \circ T \circ w_M.$$

Remarque. — Pour $r=1$, K_1 est stable par w_{Np} donc par $h_1(\mathbf{Z})$ et $h_1(\mathbf{Z})^*$, on a donc deux représentations

$$\begin{cases} h_1(\mathbf{Z}) \to \mathrm{End}(B_1) \\ h_1(\mathbf{Z})^* \to \mathrm{End}(B_1) \end{cases}$$

et pour tout T de $h_1(\mathbf{Z})$, on a :

$$\alpha_1 \circ T = T \circ \alpha_1$$

$$\alpha_1 \circ T^* = T^* \circ \alpha_1.$$

Cependant, pour $r > 1$, l'algèbre $h_r(\mathbf{Z})$ ne laisse pas stable K_r (en fait, $T(p) K_r \neq K_r$).

Preuve. — Pour montrer que α_r est une isogénie, on va montrer par récurrence sur r que les espaces tangents à l'origine de $A_{r,\mathbf{C}}$ et $K_{r,\mathbf{C}}$ sont en somme directe orthogonale.

On note $M_i = Np^i$, $i = 1, \ldots, r$.

D'abord, on sait que pour chaque $r \geqslant 1$ l'application tangente de l'inclusion

$$A_r \to J_r$$

n'est autre que l'inclusion

$$\oplus_{\alpha=1}^{r} \oplus_{\varepsilon \text{ prim., mod. } p^r} S_2(\Phi_\alpha, \varepsilon) \subset S_2(\Gamma_1(M_r)).$$

(i) $r=1$: On sait que l'application tangente du morphisme à noyau fini $K_1 \xrightarrow{\pi^*} J_1$ est l'inclusion $S_2(\Phi_1) \subset S_2(\Gamma_1(M_r))$ donc on a bien la décomposition orthogonale pour le produit scalaire de Petersson :

$$\begin{array}{ccccc} T_0 J_{1/\mathbf{C}} & = T_0 K_{1/\mathbf{C}} \oplus & & T_0 A_{1/\mathbf{C}} \\ \| & \| & & \| \\ S_2(\Gamma_1(M_1)) = S_2(\Phi_1) \oplus \oplus_{j \neq 0} S_2(\Phi_1 . \omega^j). \end{array}$$

On voit de plus que Φ_1 est normalisé par w_{M_1} et est de niveau M_1 donc K_1 est stable par l'algèbre $h_1(\mathbf{Z})$ et aussi sous w_{M_1} et $h_1(\mathbf{Z})^*$.

D'où les formules de commutation de la remarque.

(ii) Supposons qu'on ait montré pour $r-1$ la décomposition orthogonale :

$$T_0 J_{r-1/\mathbf{C}} = TK_{r-1/\mathbf{C}} \oplus TA_{r-1/\mathbf{C}},$$

on a

$$(2.1.1) \qquad S_2(\Gamma_1(M_r)) = \oplus_{\varepsilon \text{ prim., mod. } p^r} S_2(\Phi_r, \varepsilon) \oplus S_2(\Phi_r^{r-1}),$$

or par définition de $T_0 A_{r/\mathbf{C}}$, on a la décomposition orthogonale :

$$(2.1.2) \qquad T_0 A_{r/\mathbf{C}} = \oplus_{\varepsilon \text{ prim., mod. } p^r} S_2(\Phi_r, \varepsilon) \oplus T_0 A_{r-1/\mathbf{C}}$$

il s'agit donc de montrer :

$$(2.1.3) \qquad S_2(\Phi_r^{r-1}) = T_0 K_{r/\mathbf{C}} \oplus T_0 A_{r-1/\mathbf{C}}.$$

Mais par construction, l'application tangente de $\rho_* : JZ_r \to J_{r-1}$ n'est autre que la trace Tr de $S_2(\Phi_r^{r-1})$ à $S_2(\Gamma_1(M_{r-1}))$, et cette trace coïncide avec la multiplication par p sur le sous-espace $T_0 A_{r-1/\mathbf{C}}$ de $S_2(\Phi_r^{r-1})$. En outre, par définition, $T_0 K_{r/\mathbf{C}}$ est l'ensemble des formes de $S_2(\Phi_r^{r-1})$ dont la trace est dans $T_0 K_{r-1/\mathbf{C}}$.

Soit donc $f \in S_2(\Phi_r^{r-1})$, par hypothèse de récurrence $\mathrm{Tr}(f)=g+h$ où

$$g \in T_0 K_{r-1/\mathbf{C}} \qquad \text{et} \qquad h \in T_0 A_{r-1/\mathbf{C}}$$

donc

$$\mathrm{Tr}(f)=g+\frac{1}{p}\mathrm{Tr}(h) \qquad \text{et} \qquad f-\frac{1}{p}h \in T_0 K_{r/\mathbf{C}},$$

ceci montre l'existence de la décomposition (2.1.3).

Notons alors $\langle p, p \rangle_r$ le produit de Petersson sur $S_2(\Gamma_1(M_r))$; pour

$$f \in T_0 K_{r/\mathbf{C}} \qquad \text{et} \qquad g \in T_0 A_{r-1/\mathbf{C}},$$

on a :

$$\langle f, g \rangle_r = \langle \mathrm{Tr}(f), g \rangle_{r-1} = 0$$

par hypothèse de récurrence. Ce qui achève la démonstration. De ce qui précède, il découle que K_r est stable par $h_r(\mathbf{Z})^*$ car son espace tangent est orthogonal à $T_0 A_{r/\mathbf{C}}$ qui est stable par $h_r(\mathbf{Z})$, donc est stable par les adjoints pour le produit de Petersson des éléments de $h_r(\mathbf{Z})$ (*cf.* [Sh 1], chapitre 3, formule 3.4.5 et proposition 3.5.4).

Pour montrer que β_r est une isogénie on montre par récurrence que

$$(T_0 K_{r/\mathbf{C}}) \,|\, w_{M_r} \cap T_0 A_{r/\mathbf{C}} = \{0\}.$$

Pour $r=1$, c'est évident car $T_0 K_{1/\mathbf{C}}$ est stable par w_{M_1}.

Supposons le résultat acquis pour $r-1$.

D'après (2.1.1) et la stabilité évidente des deux facteurs du membre de droite de cette formule, il suffit de montrer que dans $S_2(\Phi_r^{r-1})$, on a :

$$T_0 A_{r-1} \,|\, w_{M_r} \cap T_0 K_r = \{0\}.$$

Soit donc $f \in T_0 A_{r-1}$ telle que $f|w_{M_r} \in T_0 K_r$ comme

$$\begin{pmatrix} 0 & -1 \\ M_r & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ M_{r-1} & 0 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix},$$

on a :

$$f|w_{M_r} = f|w_{M_{r-1}} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

On voit que l'on peut prendre pour représentants de $\Gamma_1(M_{r-1})\backslash\Phi_r^{r-1}$ les éléments $\begin{pmatrix} 1 & 0 \\ x M_{r-1} & 1 \end{pmatrix}$ $x=0, \ldots, p-1$. Ainsi pour tout $g \in S_2(\Phi_r^{r-1})$ on a

$$\mathrm{Tr}(g)=\sum_{x=0}^{p-1} g\left|\begin{pmatrix} 1 & 0 \\ x M_{r-1} & 1 \end{pmatrix}\right..$$

En outre l'opérateur $T(p)^* \in h_{r-1}(\mathbf{Z})^*$ agit par

$$T(p)^*=\sum_{x=0}^{p-1} h\left|\begin{pmatrix} p & 0 \\ x M_{r-1} & 1 \end{pmatrix}\right.$$

pour tout $h \in S_2(\Gamma_1(M_{r-1}))$.

On voit alors la formule :

$$\mathrm{Tr}(f|w_{M_r})=f|w_{M_{r-1}}T(p)^*=f|T(p)w_{M_{r-1}}$$

et comme $T_0 A_{r-1}$ est stable par $T(p)$ et que par hypothèse de récurrence $T_0 A_{r-1}|w_{M_{r-1}} \cap T_0 K_{r-1}$ est nul, on conclut $f|T(p)=0$, ce qui d'après la proposition (1.1) et la définition de $T_0 A_{r-1}$ est impossible car on voit que $f \neq 0 \Rightarrow f|T(p) \neq 0$.

[En effet, il y a une base de $T_0 A_{r-1}$ constituée de $g|[t]$ où g est p. n. p. de niveau Cp^α, $C|N$, $t|N/C$ le Nebentypus de g ayant sa p-partie primitive modulo p^α, donc par la proposition (1.1) on voit que $a(p, g) \neq 0$. Comme $T(p)$ commute aux opérateurs $[t]$, si on prend f quelconque non nulle dans $T_0 A_{r-1}$, on a :

$$f=\sum_{g,t} \lambda_{g,t} g|[t],$$

$\lambda_{g,t}$ non tous nuls et

$$f|T(p)=\sum_{g,t} a(g, p) g|[t] \neq 0.]$$

Ce qui achève la démonstration du fait que β_r est une isogénie.

Enfin, si $T \in h_r(\mathbf{Z})$, et $f \in T_0 A_{r/\mathbf{C}}$ on a

$$f \mid T \mid w_{M_r} = f \mid w_{M_r} \mid T^* \qquad \text{donc} \quad \beta_r \circ T = T^* \circ \beta_r.$$

3. Rappels sur la réduction mod. p de X_r et du morphisme $J_r \to B_r$

Soit $M \geqslant 1$. Pour $(a, b) \in (1/M\,\mathbf{Z}/\mathbf{Z})^2 \setminus \{(0, 0)\}$, on note $f_{(a, b)}$ la fonction de Fricke :

si $z \in \mathfrak{h}$,

$$f_{(a, b)}(z) = \frac{g_2(z)\, g_3(z)}{\Delta(z)}\, \mathfrak{p}(az + b; z) \quad (cf.\ [19], \text{chapitre 6}).$$

C'est une fonction $\Gamma(M)$-modulaire. On fixe désormais un plongement de $\overline{\mathbf{Q}}$ dans $\mathbf{C}$.

On sait que le corps des fonctions $\Gamma_1(M)$-modulaires est engendré sur $\mathbf{C}$ par l'invariant modulaire j et par $f_{(0,\ 1/M)}$. Ce corps est défini sur $\mathbf{Q}(\zeta_M)$ où $\zeta_M = e^{2i\pi/M}$. C'est-à-dire qu'en posant

$$K_M = \mathbf{Q}\left(\zeta_M, j, f_{(0,\ 1/M)}\right),$$

on a :

$$\mathbf{C}\left(j, f_{(0,\ 1/M)}\right) = K_M \otimes_{\mathbf{Q}(\zeta_M)} \mathbf{C}.$$

Soit $M \geqslant 4$; soit

$$A_M = \mathbf{Q}\left[\zeta_M, j, f_{(0,\ 1/M)}\right].$$

C'est une $\mathbf{Q}$-algèbre intégralement close dans K_M et on voit aisément qu'elle est solution du problème de modules grossiers au sens de [16], chapitre 5, §2 et [13], chapitre 4, n 2 :

$$[\Gamma_1(M)] : \quad \mathbf{Q}(\zeta_M) - \text{Alg} \to \text{Ens}$$

$$R \mapsto \left(\begin{array}{l} \text{ensemble des classes d'isomorphismes sur } R \text{ de } (E, P_M) \\ E : \text{courbe elliptique sur } R, \\ P_M : \text{point d'ordre exactement } M, \text{ rationnel sur } R. \end{array} \right)$$

Soit $G_M = \mathrm{Gal}(\mathbf{Q}(\zeta_M)/\mathbf{Q})$. Ce groupe opère sur le corps K_M par action sur les coefficients du q-développement en la pointe ∞.

L'algèbre $A_M^{G_M}$ est solution du problème

$$\mathbf{Q} - \mathrm{Alg} \to \mathrm{Ens}$$

$$R \mapsto \left(\begin{array}{l} \text{classes d'isomorphisme sur } R \text{ de } (E, \mu_M \overset{i}{\subsetneq} E)/R, \\ E : \text{courbe elliptique définie sur } R, \\ i : \text{immersion fermée définie sur } R \text{ du schéma en groupes } \mu_{M/R} \\ \text{dans } E/R. \end{array} \right)$$

En effet, si $a \in (\mathbf{Z}/M\mathbf{Z})^\times$, et $\sigma_a \in G_M$ est l'automorphisme tel que ${}^{\sigma_a}\zeta_M = {}^{r_a}\zeta_M$, on a :

$$f_{(0,\ 1/M)}^{\sigma_a} = f_{(0,\ a/M)} = \text{fonction de Weber de } a.P,$$

si

$$f_{(0,\ 1/M)} = \text{fonction de Weber de } P.$$

Alors qu'une immersion $i : \mu_M \subsetneq E$ est donnée par $P \in E[M](R \otimes \mathbf{Q}(\zeta_M))$ tel que $P^{\sigma_a} = a.P$ pour tout $a \in (\mathbf{Z}/M\mathbf{Z})^\times$.

En outre, IGUSA [8] a démontré que le problème sur $\mathbf{Z}$:

$$R \mapsto \left(\begin{array}{c} \mathbf{Z}\text{-Alg} \to \mathrm{Ens} \\ \text{classes d'isomorphisme sur } R \text{ de } (E, \mu_M \overset{i}{\subsetneq} E)/R \end{array} \right)$$

admet un schéma de modules grossiers, $\mathscr{N}/\mathbf{Z}$ lisse sur $\mathbf{Z}$, quasi-fini sur $\mathbf{P}^1_{\mathbf{Z}}$ la droite des j. On note $X_1(M)_{\mathbf{Z}}$ la normalisation de $\mathbf{P}^1_{\mathbf{Z}}$ dans $K_M^{G_M}$.

Pour tout schéma $T/\mathbf{Z}$ et tout anneau A, on note T/A ou $T \otimes A$ le changement de base de T de $\mathbf{Z}$ à A.

On voit facilement que sur les fibres génériques on a $\mathscr{N}/\mathbf{Q} \subsetneq X_1(M)_{\mathbf{Z}} \otimes \mathbf{Q}$ car cette dernière courbe n'est autre que le modèle noté $X_1(M)$ dans l'introduction du corps $K_M^{G_M}$. Il en résulte une immersion ouverte $\mathscr{N}/\mathbf{Z} \subsetneq X_1(M)_{\mathbf{Z}}$.

On pose désormais $M = Np^r$, $r \geqslant 1$, $p \nmid N$, et on rappelle que ζ désigne une racine p^r-ième de l'unité fixée disons $\zeta = e^{2i\pi/p^r}$. Soit $I \subset G_M$ le sous-groupe d'inertie en p. On a canoniquement $G_M = G_N \times I$. On introduit $X_1(M)_{\mathbf{Z}[\zeta]}$ la normalisation dans $K_M^{G_N}$ de $\mathbf{P}^1_{\mathbf{Z}}$. On voit aisément que $\mathscr{Y}/\mathbf{Z}[\zeta]$ est solution du problème d'Igusa sur $\mathbf{Z}[\zeta]$ et comme précédemment on obtient une immersion ouverte $\mathscr{Y}/\mathbf{Z}[\zeta] \subset X_1(M)_{\mathbf{Z}}$. Le groupe I opère par automorphismes sur $X_1(M)_{\mathbf{Z}[\zeta]}$ et le morphisme naturel déduit de l'identification $K_M^{G_N} \xrightarrow{\sim} K_M^{G_M} \otimes \mathbf{Q}(\zeta)$:

$$X_1(M)_{\mathbf{Z}[\zeta]} \to X_1(M)_{\mathbf{Z}} \otimes \mathbf{Z}[\zeta]$$

est I-équivariant. On récupère donc encore un morphisme I-équivariant sur les fibres spéciales. Soit alors $\mathrm{Ig}(M)$ le modèle projectif lisse de la courbe (affine) lisse $\mathscr{Y}/\mathbf{F}_p$. Comme $\mathbf{F}_p$ est aussi bien le corps résiduel en p de $\mathbf{Z}$ qu'en $(1-\zeta)$ de $\mathbf{Z}[\zeta]$, on obtient, en utilisant les immersions fermées de la fibre spéciale de $\mathscr{Y}/\mathbf{Z}$ (resp. $\mathscr{Y}/\mathbf{Z}[\zeta]$ c'est la même!) prolongées à la courbe lisse $\mathrm{Ig}(M)$ par propreté des images, un triangle commutatif :

$$\begin{array}{ccc} & & X_1(M)_{\mathbf{Z}[\zeta]} \otimes \mathbf{F}_p \\ & \nearrow & \downarrow \\ \mathrm{Ig}(M) & & \\ & \searrow & \\ & & X_1(M)_{\mathbf{Z}} \otimes \mathbf{F}_p \end{array}$$

Soit $X_1(M)_{\mathbf{Z}[\zeta]}$ le modèle régulier minimal de $X_1(M)_{\mathbf{Z}[\zeta]}$. Le groupe I opère dessus, par la propriété de minimalité, de façon compatible avec la projection $X_1(M)_{\mathbf{Z}[\zeta]} \to X_1(M)_{\mathbf{Z}[\zeta]}$.

Soit $\mathscr{N}$ la courbe somme disjointe des normalisées des composantes irréductibles réduites de $X_1(M)_{\mathbf{Z}[\zeta]} \otimes \mathbf{F}_p$, on obtient encore une immersion fermée naturelle i_∞ faisant commuter le triangle :

$$\begin{array}{ccc} & \overset{i_\infty}{\nearrow} & \mathscr{N} \\ & & \downarrow \\ \mathrm{Ig}(M) & & \\ & \searrow & \\ & & X_1(M)_{\mathbf{Z}} \otimes \mathbf{F}_p \end{array}$$

et par normalisation, I opère encore sur $\mathscr{N}$ par des $\mathbf{F}_p$-automorphismes. Chaque flèche du triangle étant bien sûr I-linéaire.

Soit $C_\alpha = i_\alpha(\mathrm{Ig}(M))$ la composante connexe de $\mathcal{M}$ définie par i_α.

On voit alors, et c'était le but de ces rappels, que l'action de I sur $\mathcal{M}$ est triviale sur C_α.

Soit finalement x, y deux entiers tels que $p^r x + Ny = 1$. On sait que la matrice $\begin{pmatrix} p^r & -1 \\ My & p^r x \end{pmatrix}$ fournit un automorphisme w_{p^r} de $X_1(M)_{\mathbf{Z}[\zeta]}$ indépendant en fait de x et y ([20], page 156). On a pour $\sigma \in I$ et $a \equiv 1 \bmod \mathcal{N}$, tel que $\zeta^\sigma = \zeta^a$,

$$w_{p^r}^\sigma = \langle a^{-1} \rangle \circ w_{p^r}$$

Ainsi, en posant $i_0 = w_{p^r} \circ i_\alpha$, on récupère une autre composante privilégiée de $\mathcal{M}$:

$$C_0 = i_0(\mathrm{Ig}(M)) = w_{p^r}(C_\alpha),$$

sur laquelle $I \simeq (\mathbf{Z}/p^r\mathbf{Z})^\times$ opère par $\langle\ \rangle^{-1}$.

Remarquons que les composantes de $\mathcal{M}$ autres que C_0 et C_α sont permutées sous l'action de I.

On peut maintenant étudier la réduction mod. $1-\zeta$ du morphisme $\alpha_r : J_r \to \mathrm{B}_r$ vu sur k_r.

A partir de α_r, vu sur k_r, on obtient par passage aux modèles de Néron un morphisme de $\mathcal{O}_r$-schémas $J_{r/\mathcal{O}_r} \xrightarrow{\tilde{\alpha}_r} B_{r/\mathcal{O}_r}$, et en le restreignant à la « composante neutre » $J^0_{r/\mathcal{O}_r}$ on trouve un morphisme, encore surjectif. En passant alors aux fibres spéciales, et en notant $\mathrm{Ab}(J_r^0 \otimes \mathbf{F}_p)$ la plus grande variété abélienne quotient de $J_r^0 \otimes \mathbf{F}_p$, on trouve un triangle commutatif :

$$\begin{array}{ccc} J_r^0 \otimes \mathbf{F}_p & \xrightarrow{\tilde{\alpha}_r} & B_r \otimes \mathbf{F}_p \\ \downarrow & \nearrow_{\tilde{\alpha}_r^{\mathrm{Ab}}} & \\ \mathrm{Ab}(J_r^0 \otimes \mathbf{F}_p) & & \\ \downarrow & & \\ 0 & & \end{array}$$

où $\tilde{\alpha}_r^{\mathrm{Ab}}$ est l'unique morphisme de variétés abéliennes au travers duquel $\tilde{\alpha}_r$ se factorise par la propriété universelle de $\mathrm{Ab}(J_r^0 \otimes \mathbf{F}_p)$. Ce morphisme est encore surjectif, défini sur $\mathbf{F}_p$.

Comme le schéma $X_1(M)_{\mathbf{Z}[\zeta]}$ est régulier, d'après un théorème de RAYNAUD [18], on a un isomorphisme canonique

$$J^0_{r/\mathcal{C}_r} \to \mathrm{Pic}^0(X_1(M)_{\mathbf{Z}[\zeta]} \otimes \mathcal{C}_r)$$

qui permet de décrire $\mathrm{Ab}(J^0_r \otimes \mathbf{F}_p)$ par le diagramme commutatif :

$$\begin{array}{ccc} J^0_r \otimes \mathbf{F}_p & \xrightarrow{\sim} & \mathrm{Pic}^0(X_1(M)^s{}_{\mathbf{Z}[\zeta]} \otimes \mathbf{F}_p) \\ \downarrow & & \downarrow \\ \mathrm{Ab}(J^0_r \otimes \mathbf{F}_p) & \xrightarrow{\sim} & \mathrm{Pic}^0(\mathcal{N}) \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

La flèche verticale à droite étant l'image de la flèche de normalisation par le foncteur Pic^0.

Or on peut décomposer $\mathrm{Pic}^0(\mathcal{N})$ comme suit :

soient

$$j^\infty_r = \mathrm{Pic}^0(C_\infty); \quad j^0_r = \mathrm{Pic}^0(C^0)$$

et $\mathscr{B}$ la variété abélienne produit cartésien des jacobiennes des composantes de $\mathcal{N}$ autres que C_∞ et C_0. On a alors

$$\mathrm{Pic}^0(\mathcal{N}) = j^\infty_r \times \mathscr{B} \times j^0_r.$$

Ceci permet de définir un morphisme $\sigma_r : j^\infty_r \times j^0_r \to B_r \otimes \mathbf{F}_p$, obtenu en composant l'inclusion naturelle dans $\mathrm{Ab}(J^0_r \otimes \mathbf{F}_p)$ avec $\tilde{\alpha}^{\mathrm{Ab}}_r$.

Soit d'autre par $\mathscr{A} = B_r$ ou J_r. On rappelle que pour une variété abélienne $\mathscr{A}$ définie sur $\mathbf{Q}$ (donc sur $\mathbf{Q}_p$), il y a une action naturelle du groupe I sur la fibre spéciale du modèle de Néron de $\mathscr{A}$ sur $\mathcal{C}_r$ (action géométrique de l'inertie). Soit en effet $\sigma \in I$ et u_σ l'automorphisme de $\mathscr{A}/k_r$ au-dessus de l'automorphisme de Spec k_r déduit de σ (on utilise ici que $\mathscr{A}$ est en fait définie sur $\mathbf{Q}_p$). En passant aux modèles de Néron, on prolonge u_σ à $\mathscr{A}/\mathcal{C}_r$. Comme le corps résiduel de $\mathcal{C}_r$ n'est autre que $\mathbf{F}_p$, on obtient un $\mathbf{F}_p$-automorphisme $\tilde{u}_\sigma$ de $\mathscr{A} \otimes \mathbf{F}_p$. On applique cela à $\mathscr{A} = J_r$ puis $\mathscr{A} = B_r$. En outre l'action de I sur $J_r \otimes \mathbf{F}_p$ définie ci-dessus coïncide avec l'action déduite de celle de I sur $X_1(M)/k_r$. Ce qui entraîne que $\tilde{\alpha}_r$,

donc σ_r, est I-équivariante lorsque l'on munit $j_r^\infty \times j_r^0$ de l'action de I déduite de celle sur $\mathrm{Ig}(\mathrm{M})$.

Pour $\sigma \in I$, on note à l'unique élément de $(\mathbf{Z}/\mathrm{M}\,\mathbf{Z})^\times$ tel que $a \equiv 1 \bmod. N$ et $\zeta^a = \zeta^a$, et on écrit $u = u_a$.

Pour ne pas risquer de confusion, nous noterons, pour chaque correspondance T sur X_r, $T = T_{\mathrm{Pic}}$ l'endomorphisme de $J_r = \mathrm{Pic}^0(X_r)$ qui s'en déduit, et T_{Alb} l'endomorphisme de J_r vue comme variété d'Albanase (*cf.* [14], *chapitre* 2, § 5).

On rappelle le théorème dont nous aurons à faire usage :

THÉORÈME (Mazur-Wiles) 3.1. — (1) σ_r *est une isogénie,*

(2) $\sigma_r \circ (\mathrm{Id} \times \langle a \rangle_{\mathrm{Alb}}) = u_a \circ \sigma_r$ *pour tout* $a \in G_r$, $a \equiv 1 \bmod. \mathcal{N}$,

(3) $T(p)_{\mathrm{Alb}} \circ \sigma_r = \sigma_r \circ U$, $T(p)_{\mathrm{Pic}} \circ \sigma_r = \sigma_r \circ U'$,

où U et U' sont les endomorphismes de $j_r^\infty \times j_r^0$ définis, en notation matricielle par :

$$\begin{pmatrix} x \\ y \end{pmatrix} \in j_r^\infty \times j_r^0; \qquad U\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \tilde{V} & c_1 \\ 0 & F \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

si

$$U'\begin{pmatrix} x \\ y \end{pmatrix} = \langle n_p \rangle_{\mathrm{Pic}} \circ \begin{pmatrix} F & 0 \\ c_2 & \tilde{V} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

où

E, désigne le Frobenius absolu;

V, le Verschiebung;

$n_p \in G_r$ avec $n_p \equiv 1 \pmod{p^r}$ et $n_p \equiv p \pmod{N}$,

et $\tilde{V} = \langle n_p \rangle_{\mathrm{Alb}} \circ V$.

De plus si

$$\pi_\infty : \; C_\infty \to X_1(N)/\mathbf{F}_p \qquad \text{et} \qquad \pi_0 : \; C_0 \to X_1(N)/\mathbf{F}_p$$

désignent les projections naturelles déduites de $X_1(M)/\mathbf{Z}[\zeta] \to X_1(N)/\mathbf{Z}[\zeta]$, on définit c_1 et c_2 par :

$$c_1 = \pi_\infty^* \; \pi_0 . \qquad \text{et} \qquad c_2 = \pi_0^* \; \pi_\infty .$$

Preuve. — Les assertions (1) et (3) sont prouvées dans [14], chapitre 3, proposition 2 et 3.

L'assertion (2) a été démontrée dans la discussion précédant l'énoncé du théorème.

Rappelons alors qu'à l'élément $T(p)=T(p)_{\mathrm{Pic}}$ de $h_r=h_r(\mathbf{Z}_p)$ est attaché un idempotent e_r de h_r de sorte que si $h_r^0=e_r h_r$ et $h_r^{s\cdot s\cdot}=(1-e_r)h_r$, dans la décomposition : $h_r=h_r^0\times h_r^{s\cdot s\cdot}$ on ait $T(p)=(T(p)^0, T(p)^{ss})$ où $(T(p)^0$ est inversible et $T(p)^{s\cdot s\cdot}$ est topologiquement nilpotent.

De même, pour $T(p)_{\mathrm{Alb}}\in h_r^*$, on définit un idempotent $e_{r,\,\mathrm{Alb}}$.

Soit $\tilde{B}_r$ la fibre spéciale de B_r sur $\mathbf{F}_p$, et $\tilde{B}_{r,\,p}$ son groupe p-divisible. On va étudier à l'aide de la proposition précédente le groupe p-divisible $e_{r,\,\mathrm{Alb}}\cdot\tilde{B}_{r,\,p}$.

Notons Γ^∞ (resp. Γ^0 (resp. Γ) le groupe p-divisible de j_r^∞ (resp. j_r^0, resp. $j_r^\infty\times j_r^0$).

Soit U l'endomorphisme de Γ défini dans la proposition. Il s'insère à l'évidence dans le diagramme commutatif de schémas en groupes p-divisibles sur $\mathbf{F}_p$ et de $h_r(\mathbf{Z}_p)_{\mathrm{Alb}}$-modules :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma^\infty & \longrightarrow & \Gamma & \longrightarrow & \Gamma^0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle U} & & \downarrow{\scriptstyle \tilde{V}} & & \\ 0 & \longrightarrow & \Gamma^\infty & \longrightarrow & \Gamma & \longrightarrow & \Gamma^0 & \longrightarrow & 0. \end{array}$$

On va définir des idempotents e_F, e_U, $e_{\tilde{V}}$ attachés à F, U, $\tilde{V}$ et montrer la :

PROPOSITION 3.2. — *Le schéma en groupes p-divisibles $e_U\cdot\Gamma$ se dévisse canoniquement en :*

$$0\to e_F\Gamma^\infty\to e_U\Gamma\to e_{\tilde{V}}\Gamma^0\to 0$$

où $e_F\Gamma^\infty$ est étale et $e_{\tilde{V}}\Gamma^0$ est de type multiplicatif. En particulier, $e_U\cdot\Gamma$ est un schéma ordinaire.

Preuve. — Soit Δ un groupe p-divisible sur un corps parfait k de caractéristique p. Soit $u\in\mathrm{End}(\Delta/k)$. Dans cette $\mathbf{Z}_p$-algèbre libre de type fini, u engendre sur $\mathbf{Z}_p$ une sous-algèbre commutative qui se décompose en produit d'algèbres locales. On note e_u la somme des idempotents orthogonaux associés à des composantes où u est inversible.

On applique cela à $u=F, U, \tilde{V}$ et $\Delta=\Gamma^\infty, \Gamma, \Gamma^0$ $(k=\mathbf{F}_p)$.

Une autre construction plus explicite de e_u utilise la notion de polynôme caractéristique :

Soit n le rang du schéma en groupes p-divisible Δ.

Soit $\mathbf{Z}_p[X]/k$ le k-schéma constant donné par le groupe $\mathbf{Z}_p[X]$ et soit $\Delta\otimes_{\mathbf{Z}_p}\mathbf{Z}_p[X]/k$ le k-schéma représentant le foncteur $R_{(R:k-\mathrm{alg})}\to\Delta(R)\otimes_{\mathbf{Z}_p}\mathbf{Z}_p[X]$, puis le k-schéma en $\mathbf{Z}_p[X]$-modules $\Lambda^n_{\mathbf{Z}_p[X]}(\Delta\otimes\mathbf{Z}_p[X])$.

L'endomorphisme $\Lambda^n(u-\mathrm{Id}\otimes X)$ s'identifie à un élément de $\mathbf{Z}_p[X]$ baptisé polynôme caractéristique de u, et on vérifie facilement sur les points de Δ le théorème d'Hamilton-Cayley : $P_u(u)=0\in\mathrm{End}(\Delta/k)$.

Soit alors $\bar{P}_u(X)\in\mathbf{F}_p[X]$ la réduction de P_u modulo p. Supposons $\bar{P}_u(X)=X^r\bar{S}(X)$ où $d^0\bar{S}=s$, $r+s=n$; $X\nmid\bar{S}$. D'après le lemme de Hensel, il existe $R(X)$ $R(X)$, $S(X)$ dans $\mathbf{Z}_p[X]$ tels que $P_u(X)=R(X)S(X)$ avec R distingué unitaire de degré r ($R(X)\equiv X^r$ (mod. p)) et $S(0)\not\equiv 0$ (mod. p). De plus, il existe A, B dans $\mathbf{Z}_p[X]$ tels que

$$A(X)R(X)+B(X)S(X)=1$$

et en posant

$$e_u=A(u)R(u)\in\mathbf{Z}_p[u]\subset\mathrm{End}(\Delta/k),$$

on retrouve explicitement l'idempotent e_u précédent. Cette construction à l'avantage de rendre évidentes les égalités :

$e_u\Delta=$sous-schéma en groupes p-divisible maximal sur lequel u est un automorphisme;

$(1-e_u)\Delta=$sous-schéma en groupes p-divisible maximal sur lequel u est localement nilpotent (i.e. pour tout $m\geqslant 1$ u est nilpotent sur $1-e_u).\Delta[p^m]/k)$, et $\Delta\simeq e_u\Delta\times(1-e_u)\Delta$.

Une fois ces définitions clarifiées, la suite exacte courte résulte des comparaisons des polynômes caractéristiques :

$$P_U(X)=P_F(X)P_{\tilde{V}}(X)$$
$$P_F(X)=X^{rF}.S_F(X)$$

et

$$P_{\tilde{V}}(X)=X^{r\tilde{V}}S_{\tilde{V}}(X)$$

donc

$$P_U(X)=X^{rF+r\tilde{V}}.S_F(X)S_{\tilde{V}}(X),$$

ce qui donne $S_U = S_F . S_{\tilde{V}}$, d'où résulte l'additivité des rangs :

$$\operatorname{rang}(e_U \Gamma) = \operatorname{rang}(e_F \Gamma^\infty) + \operatorname{rang}(e_{\tilde{V}} \Gamma^0).$$

On voit alors que $e_F \Gamma^\infty$ coïncide avec la partie étale de Γ^∞ (car le noyau de F est contenu dans la p-torsion de la partie connexe de Γ^∞). Puis on va voir par la dualité de Cartier que $e_{\tilde{V}} \Gamma^0 = e_V \Gamma^0$ est de type multiplicatif. Soit $is : \Gamma^0 \to (\Gamma^0)'$ l'isomorphisme du groupe p-divisible Γ^0 à son dual de Cartier résultant de l'autodualité des jacobiennes. On a la formule pour le Verschiebung : $is \circ V = F' \circ is$ où F' est le dual de Cartier de F. D'où un accouplement parfait de k-schémas :

$$(\ , \ ) : \quad \Gamma^0 \times \Gamma^0 \to \mathbf{G}_m$$

défini par : $(x, y) = \langle x, is(y) \rangle$, l'accouplement $\langle \ , \ \rangle$ étant donné par la dualité de Cartier.

On voit que $(Fx, y) = (x, Vy)$ donc grâce aux décompositions :

$$\begin{cases} \Gamma^0 = e_F \Gamma^0 \times (1 - e_F) \Gamma^0 \\ \Gamma^0 = e_V \Gamma^0 \times (1 - e_V) \Gamma^0 \end{cases}$$

on voit que $(\ , \ )$ induit la dualité

$$e_F \Gamma^0 \times e_V \Gamma^0 \to \mathbf{G}_m.$$

Or $e_F \Gamma^0$ est étale donc $e_V \Gamma^0$ est de type multiplicatif comme $\mathbf{F}_p$-schéma :

$$e_V \Gamma^0 \simeq (e_F \Gamma^0)'.$$

De tout ceci, il résulte que $e_U \Gamma$ est ordinaire car sa composante connexe est isomorphe à $e_V \Gamma^0$ qui est de type multiplicatif. Et on obtient le corollaire que l'on visait :

COROLLAIRE 3.3. — *Le schéma en groupes p-divisible $e_{r,\,\mathrm{Alb}} . B_{r/\mathcal{C}_r}$ est ordinaire et σ_r induit une isogénie de $(j_{r,\,p}^{\times})^{\mathrm{et}}$ à $(e_{r,\,\mathrm{Alb}} . \tilde{B}_{r,\,p})^{\mathrm{et}}$; l'action géométrique de l'inertie sur ce dernier groupe est donc triviale.*

Preuve. — C'est clair par ce qui précède. C'est le contenu de la proposition 2, paragraphe 4 de [15].

4. Preuve du théorème

Soit $R \subset h^0(a)$ la composante locale que l'on s'est donné, a satisfaisant l'hypothèse (★). Comme $A_r \subset J_r$ est $h_r(\mathbf{Z})$-stable, on définit $R(A_r)$ comme la projection de R_r dans les endomorphismes de A_r. Il lui correspond un idempotent $1_{R(A_r)}$ dans $\mathbf{Z}_p \otimes \mathrm{End}\, A_r$, et on vérifie tout de suite que

$$J_{r,\,p}(R) = 1_{R(A_r)} \cdot e_r A_r[p^\infty](\bar{\mathbf{Q}}).$$

Considérons alors l'isogénie $\beta_r : A_r \to B_r$ définie au paragraphe 2, rationnelle sur $\mathbf{Q}(\zeta_{M_r})$. Soit $\mathcal{O}_{M_r} = \mathcal{O}_r[\zeta_N]$. C'est un anneau de valuation discrète complet, non ramifié sur $\mathcal{O}_r$. En passant aux modèles de Néron sur $\mathcal{O}_{M_r}$ on obtient un morphisme

$$\beta_r : \quad A_{r/\mathcal{O}_{M_r}} \to B_{r/\mathcal{O}_{M_r}}$$

qui induit une isogénie sur les fibres génériques et spéciales (en fait, son noyau est fini et plat). Grâce à la proposition 2.1, on obtient une isogénie de groupes p-divisibles, définie sur le corps résiduel $\mathbf{F}$ de $\mathcal{O}_{M_r}$:

$$\tilde{\beta}_r : \quad e_r \tilde{A}_{r,\,p} \to e_{r,\,\mathrm{Alb}}\, \tilde{B}_{r,\,p}.$$

En particulier, le schéma en groupes p-divisible $e_r A_{r,\,p/\mathcal{O}_r}$ est ordinaire. Grâce à la formule de commutation : $w_{M_r} \circ u_a = \langle a \rangle_{\mathrm{Pic}} \circ u_a \circ w_{M_r}$ (*cf.* [14], chapitre 2, § 5) on voit que :

I agit sur la partie étale de $e_r \tilde{A}_{r,\,p}$ *par* $\langle\ \rangle_{\mathrm{Alb}}$: *si* $x \in e_r \tilde{A}_r(\bar{\mathbf{F}}_p)$: $u_a(x) = \langle a \rangle_{\mathrm{Alb}}\, x$.

Considérons maintenant les groupes p-divisibles, définis sur $\mathcal{O}_r$:

$C_r/\mathcal{O}_r$ = partie connexe de $e_r A_{r,\,p}/\mathcal{O}_r$ et

$E_r/\mathcal{O}_r$ = partie étale de $e_r A_{r,\,p}/\mathcal{O}_r$.

On renvoie à [24] pour leur définition et l'existence de la suite exacte courte de $\mathcal{O}_r$-schémas en groupes p-divisibles :

$$0 \to C_r/\mathcal{O}_r \to e_r A_{r,\,p}/\mathcal{O}_r \to E_r/\mathcal{O}_r \to 0.$$

On peut appliquer l'idempotent $1_{R(A_r)}$ à cette suite, grâce à la fonctorialité du dévissage connexe-étale, et on obtient la suite exacte de schémas en groupes p-divisibles :

$$0 \to C_r(R)/\mathcal{O}_r \to J_{r,\,p}(R)/\mathcal{O}_r \to E_r(R)/\mathcal{O}_r \to 0. \tag{4.1}$$

avec les notations évidentes.

PROPOSITION 4.1. — *La suite exacte de R_r-modules obtenue en prenant les points sur $\bar{\mathbf{Q}}_p$ dans* (4.1) *est scindée, pour chaque $r \geqslant 1$. Les scindages sont compatibles aux revêtements $X_r \to X_s$ d'où un scindage de R-modules :*

$$J_{\infty,\,p}(R) = C_\infty(R) \oplus E_\infty(R)$$

où

$$C_\infty(R) = \varinjlim_r C_r(R)$$

$$E_\infty(R) = \varinjlim_r E_r(R)$$

où l'on note

$$C_r(R) = C_r(R)/\mathcal{C}_r(\bar{\mathbf{Q}}_p) \qquad \text{et} \qquad E_r(R) = E_r(R)/\mathcal{C}_r(\bar{\mathbf{Q}}_p).$$

Preuve. — Soit $r \geqslant 1$ fixé. Le groupe $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ opère sur $J_{r,\,p}(R)$. Pour $k_r = \mathbf{Q}(\zeta_{p^r})$, le groupe de décomposition en p associé au plongement fixé de $\bar{\mathbf{Q}}$ dans $\mathbf{C}_p$ noté $D_p(\bar{\mathbf{Q}}/k_r)$ opère sur $E_r(R)$, $J_{r,\,p}(R)$ et $C_r(R)$. Mais en fait, comme J_r est défini sur $\mathbf{Q}$ (donc sur $\mathbf{Q}_p$), le groupe $D_p(\bar{\mathbf{Q}}/\mathbf{Q})$ opère sur $C_r(R)$, $J_r(R)$, $E_r(R)$.

Soit $I_p(\bar{\mathbf{Q}}/\mathbf{Q})$ le sous-groupe d'inertie de $D_p(\bar{\mathbf{Q}}/\mathbf{Q})$. Introduisons alors le caractère cyclotomique : $\kappa : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^*$ donnant l'action de Galois sur les racines p-primaires de l'unité.

LEMME 4.1. — *Soient r et m deux entiers $\geqslant 1$. L'accouplement*

$$(\ ,\ )_{r,\,m} : \quad J_r(R)[p^m] \times J_r(R)[p^m] \to \mu_{p^m}$$

donné par

$$(x, y)_{r,\,m} = \langle x, y \mid w_{M_r} \rangle_r$$

(où $\langle\ ,\ \rangle_r$ désigne l'accouplement de Weil de $J_{r/\mathbf{Q}}$) est parfait et satisfait les formules :

(i) *Si $T \in R_r$ et $x, y \in J_r(R)[p^m]$:*

$$(Tx, y)_{r,\,m} = (x, Ty)_{r,\,m}$$

(ii) *Si $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, $x, y \in J_r(R)[p^m]$*

$$(x^\sigma, y^\sigma) = (\langle \kappa(\sigma) \rangle_{r,\,\mathrm{Alb}} \cdot x, y)^\sigma_{r,\,m}.$$

En outre, il fournit un isomorphisme de R_r-modules

$$\Phi_{r,m}: \quad C_r(R)[p^m] \xrightarrow{\sim} \mathrm{Hom}(E_r(R)[p^m], \mu_{p^m})$$
$$x \mapsto (-, x)_{r,m}.$$

COROLLAIRE 4.2. — *Les actions de $I_p(\bar{\mathbf{Q}}/\mathbf{Q})$ sur $E_r(R)$ et $C_r(R)$ sont données respectivement par les caractères*

$$\langle \kappa \rangle_{r,\mathrm{Alb}} = \omega^{-a} \times \ll \quad \gg_{r,\mathrm{Alb}} \qquad \text{où} \quad x = \omega(x) \times \langle x \rangle$$

dans $\mathbf{Z}_p^x = \mu^{p-1} \times (1 + p\mathbf{Z}_p)$ et κ.

Preuve du lemme 4.1. :

(i) se démontre comme dans 2.1 grâce à $T_{\mathrm{Alb}} = w_{M_r} \circ T_{\mathrm{Pic}} \circ w_{M_r}$.

(ii) provient de l'équivariance sous Galois de l'accouplement de Weil non tordu :

$$\langle x, y \rangle_r^\sigma = \langle x^\sigma, y^\sigma \rangle_r$$

et de la formule $w_{M_r}^\sigma = \langle \kappa(\sigma) \rangle_{r,\mathrm{Alb}} \cdot w_{M_r}$ déjà notée.

On observe alors que si l'on passe aux duaux de Cartier dans le dévissage connexe-étale :

$$0 \to C_r(R)/\mathcal{C}_r \to J_r(R)/\mathcal{C}_r \to E_r(R)/\mathcal{C}_r \to 0$$

i. e.

$$0 \to E_r(R)'/\mathcal{C}_r \to J_r(R)'/\mathcal{C}_r \to C_r(R)'/\mathcal{C}_r \to 0$$

on obtient le dévissage connexe-étale de $J_r(R)'/\mathcal{C}_r$ parce qu'on a vu que $J_r(R)'/\mathcal{C}_r$ est ordinaire. En outre, l'autodualité naturelle

$$J_{r/\mathbf{Q}} \xrightarrow{\sim} \mathrm{Pic}^0(J_r)/\mathbf{Q}$$

induit une isogénie sur $\mathbf{Q}(\zeta_{M_r})$, composée des flèches :

$$A_r \xrightarrow{u_{M_r}} w_{M_r}(A_r) \to J_r \xrightarrow{\sim} \mathrm{Pic}^0(J_r) \to \mathrm{Pic}^0 A_r$$

où la dernière flèche est l'image par Pic^0 de l'inclusion $A_r \to J_r$. Ceci résulte de la proposition 2.1 car $\mathrm{Pic}^0(A_r)$ est isogène à B_r (égalité des espaces tangents). Or si on prend les groupes p-divisibles sur $\mathcal{C}_{M_r}$ correspondant,

on obtient un morphisme surjectif, plat et fini :

$$A_r[p^\infty]/\mathcal{C}_{M_r} \xrightarrow{i_r} \mathrm{Pic}^0(A_r)[p^\infty]/\mathcal{C}_{M_r}$$

tel que si $T \in h_r$,

$$i_r \circ T = T^* \circ i_r$$

et on peut identifier le dual de Cartier $A_r[p^\infty]'/\mathcal{C}_{M_r}$ avec $\mathrm{Pic}^0(A_r)[p^\infty]/\mathcal{C}_{M_r}$ de sorte que si $T \in h_r$, T' devienne T^* on applique alors l'idempotent $1_{R(A_r)}$ pour obtenir

$$i_r : \quad J_{r,\,p}(R)/\mathcal{C}_{M_r} \to J_{r,\,p}(R)'/\mathcal{C}_{M_r} = 1_R \cdot$$

et $i_r \cdot T = T' \cdot i_r$.

Ce morphisme de groupes p-divisibles a son noyau fini et plat qui est nul sur la fibre générique par autodualité de J_r. On conclut donc que i_r est un isomorphisme de schémas en groupes p-divisibles et il induit l'isomorphisme annoncé

$$C_r(R)/\mathcal{C}_r \underset{i_r}{\simeq} E_r(R)'/\mathcal{C}_r.$$

Sur les $\bar{\mathbf{Q}}_p$-points c'est le contenu de l'énoncé.

Preuve du corollaire 4.2. — L'action du groupe d'inertie $I_p = I_p(\bar{\mathbf{Q}}/\mathbf{Q})$ a déjà été calculée sur $E_r(R)$ car $E_r(R)/\mathcal{C}_r$ étant étale, l'action de I_p se factorise à travers I qui agit par $\langle \kappa \rangle_{r,\,\mathrm{Alb}}$ d'après (4.1). Pour x dans $C_r(R)[p^m]$, on calcule $\Phi_{r,\,m}(x^\sigma)$:

Pour tout y de $E_r(R)[p^m]$, on a :

$$\begin{aligned}(y, x^\sigma)_{r,\,m} &= ((y^{\sigma^{-1}})^\sigma, x^\sigma)_{r,\,m} \\ &= (\langle \kappa(\sigma) \rangle_{r,\,\mathrm{Alb}} y^{\sigma^{-1}}, x)^\sigma_{r,\,m} \\ &= (\kappa(\sigma) \times \langle \kappa(\sigma) \rangle_{r,\,\mathrm{Alb}} y^{\sigma^{-1}}, x)_{r,\,m}\end{aligned}$$

or $y^{\sigma^{-1}} = \langle \kappa(\sigma^{-1}) \rangle_{r,\,\mathrm{Alb}} \cdot y$ puisque $y \in E_r(R)[p^m]$.

On conclut donc :

$$(y, x^\sigma)_{r,\,m} = (y, \kappa(\sigma)\, x)_{r,\,m}$$

$$\text{i.e. } \Phi_{r,\,m}(x^\sigma) = \Phi_{r,\,m}(\kappa(\sigma)\, x).$$

Ainsi $x^\sigma = \kappa(\sigma)\, x$.

Soit alors σ un générateur de $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty N})/\mathbf{Q}_\infty(\zeta_N))$ où $\mathbf{Q}_\infty$ est la $\mathbf{Z}_p$-extension de $\mathbf{Q}$. Dans l'isomorphisme naturel:

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty N})/\mathbf{Q}) \xrightarrow{\sim} G_\infty = (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/N\mathbf{Z})^\times \times \Gamma$$

on demande donc que l'image de σ soit $(u, 1, 1)$ où u engendre $(\mathbf{Z}/p\mathbf{Z})^\times$. On note encore σ un relèvement de σ à I_p. L'action de σ sur $E_r(R)$ est via $\omega^{-a}(u)$ et sur $C_r(R)$, via $\omega(u)$. Soit $\zeta = \omega(u) \in \mu_{p-1}^{\mathrm{prim}}$. C'est alors que l'hypothèse $a \neq -1$ est utilisée:

LEMME 4.3. — (i) *On a le scindage de R_r-modules*:

$$J_{r,p}(R) = \mathrm{Ker}(\sigma - \zeta)^{p^\infty} \oplus \mathrm{Ker}(\sigma - \zeta^{-a})^{p^\infty}$$

où $\mathrm{Ker}(\sigma-\zeta)^{p^\infty} = C_r(R)$

et $\mathrm{Ker}(\sigma-\zeta^{-a})^{p^\infty}$ *est isomorphe à* $E_r(R)$ *par la projection naturelle* $J_r(R) \xrightarrow{j} E_r(R)$.

(ii) *Ceci reste valide pour* $J_\infty(R)$:

$$J_\infty(R) \simeq C_\infty(R) \oplus E_\infty(R)$$

comme R-modules.

Preuve. — Pour r, m fixés $\geqslant 1$, il existe $t_{r,m} \geqslant 1$ tel que si $t \geqslant t_{r,m}$ on ait

$$(\sigma-\zeta)^{p^t}(\sigma-\zeta^{-a})^{p^t} J_r(R)[p^m] = 0.$$

En effet, par le théorème de Hamilton Cayley, et parce que $\zeta \neq \zeta^{-a}$, on a: $(\sigma-\zeta)(\sigma-\zeta^{-a}) = 0$ comme endomorphisme de $J_r(R)[p^m] \otimes_{R_r} (R_{r/\mathrm{rad}(R_r)})$ et le module $J_r(R)[p^m]$ est artinien sur R_r.

Mais, d'autre part, il existe évidemment des polynômes $u_t(X)$ et $v_t(X)$ dans $\mathbf{Z}_p[X]$ tels que

$$u_t(\sigma)(\sigma-\zeta)^{p^t} + v_t(\sigma)(\sigma-\zeta^{-a})^{p^t} = 1$$

donc

$$J_r(R)[p^m] = \mathrm{Ker}(\sigma-\zeta)^{p^t m} \oplus \mathrm{Ker}(\sigma-\zeta^{-a})^{p^t m}$$

donc

$$C_r(R)[p^m] = \mathrm{Ker}(\sigma-\zeta)^{p^t m}$$

et

$$E_r(R)[p^m] \xrightarrow{j} \mathrm{Ker}(\sigma - \zeta^{-a})^{p^r m}.$$

(ii) Comme σ ne dépend ni de m, ni de r, on peut passer à la limite en r et m pour obtenir l'énoncé.

THÉORÈME 4.4. — *Pour chaque $r \geqslant 1$, on a des isomorphismes de R_r-modules*:

$$C_r(R) \xrightarrow{\sim} R_r \otimes \Pi_p \qquad (\Pi_p = \mathbf{Q}_p/\mathbf{Z}_p)$$

$$E_r(R) \xrightarrow{\sim} \mathrm{Hom}(R_r, \Pi_p)$$

$$J_{r,p}(R) \xrightarrow{\sim} (R_r \otimes \Pi_p) \oplus \mathrm{Hom}(R_r, \Pi_p).$$

Ces isomorphismes sont compatibles avec les revêtements $X_r \to X_s$ et on a à la limite

$$J_{\infty,p}(R) \xrightarrow{\sim} R \otimes_\Lambda \mathrm{Hom}(\Lambda, \Pi_p) \oplus \mathrm{Hom}(R, \Pi_p)$$

Preuve. — Soit $\Gamma_r = 1 + Np^r \mathbf{Z}_p \subset G_\infty \subset h^0$. On utilise le théorème 3.1 de [7] qui affirme que $J_\infty(R)^{\Gamma_r} = J_r(R)$ (les applications de transition $J_s(R) \to J_r(R)$ si $r > s$, étant toutes injectives). Comme on a démontré au lemme 4.2 que l'on a les scindages compatibles de R-modules:

$$J_r(R) = C_r(R) \oplus E_r(R)$$
$$J_\infty(R) = C_\infty(R) \oplus E_\infty(R)$$

on voit que

$$\begin{cases} C_r(R) = C_\infty(R)^{\Gamma_r} \\ E_r(R) = E_\infty(R)^{\Gamma_r}. \end{cases}$$

On passe alors aux duaux de Pontryagin (où M^* est le dual de Pontryagin du groupe p-profini ou p-divisible M) comme dans la preuve du théorème 9.3 de [7]:

Si

$$\omega_r = \gamma^{p^r} - 1, \qquad \gamma = \langle 1 + Np \rangle,$$

on a

$$C_\infty(R)^*/\omega_r C_\infty(R)^* \simeq C_r(R)^*$$
$$E_\infty(R)^*/\omega_r E_\infty(R)^* \simeq E_r(R)^*.$$

On applique alors la proposition 3.1 de [5] qui donne la structure de $C_1(R)$ et $E_1(R)$ sur R_1 :

$$\begin{cases} C_1(R) \simeq R_1 \otimes \Pi_p \\ E_1(R) \simeq \mathrm{Hom}(R_1, \Pi_p). \end{cases}$$

$$\text{i.e.} \quad \begin{cases} C_1(R)^* \simeq \mathrm{Hom}(R_1, \mathbf{Z}_p) \\ E_1(R)^* \simeq R_1. \end{cases}$$

Par le lemme de Nakayama, on tire de cela des morphismes surjectifs de R-modules :

$$(4.4.1) \qquad \begin{cases} R \to E_\infty(R)^* \\ R \to \mathrm{Hom}(C_\infty(R)^*, \Lambda) \end{cases}$$

mais on connaît le rang des Λ-modules qui interviennent ici : D'abord, d'après le théorème 3.1 de [7], on sait que R et $J_\infty(R)^*$ sont libres du type fini sur Λ et que

$$\mathrm{rang}_\Lambda J_\infty(R)^* = 2.\mathrm{rang}_\Lambda R.$$

D'autre part, un corollaire évident de la dernière assertion du lemme 4.1 est que

$$\mathrm{rang}_\Lambda E_\infty(R)^* = \mathrm{rang}_\Lambda C_\infty(R)^*.$$

Donc $\mathrm{rang}_\Lambda R = \mathrm{rang}_\Lambda E_\infty(R)^* = \mathrm{rang}_\Lambda C_\infty(R)^*$.

Les morphismes de 4.4.1 sont donc des isomorphismes. En reprenant les duaux de Pontryagin, on obtient la structure de $J_\infty(R)$ et $E_\infty(R)$. D'où clairement :

$$E_r(R) \simeq \mathrm{Hom}(R_r, \Pi_p).$$

Pour $C_r(R)$ on utilise la remarque.

Remarque. — Soit $\Lambda_r = \mathbf{Z}_p[[\Gamma]]\,(\omega_r) \simeq \mathbf{Z}_p[T]/((T+1)^{p^r} - 1)$.

L'application de trace $\mathrm{Tr}: \Lambda_r \to \mathbf{Z}_p$ permet de définir un isomorphisme de R_r-modules:

$$\mathrm{Hom}_r(R_r, \Lambda_r) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(R_r, \mathbf{Z}_p)$$

$$f \mapsto \frac{1}{p^r} \times \mathrm{Tr} \circ f.$$

De ceci, il résulte bien que

$$C_r(R)^* \simeq \mathrm{Hom}_{\mathbf{Z}_p}(R_r, \mathbf{Z}_p).$$

Remarque. — La détermination de la structure de $C_1(R)$ et $E_1(R)$ utilise l'application de Cartier $\mathrm{Pic}^0(C_1^\infty) \xrightarrow{\delta} \bar{\mathbf{F}}_p[[q]]$ (où C_1^∞ est la composante privilégiée de $\mathrm{Pic}^0(N)$ comme au paragraphe 3) mais cet ingrédient est beaucoup plus difficile à utiliser pour $r>1$, car l'isogénie $A_r \to B_r$ n'est plus un isomorphisme sur la fibre spéciale. Il y a donc un noyau inconnu pour la flèche $\tilde{A}_r[p](\bar{\mathbf{F}}_p) \to \mathbf{F}_p[[q]]$.

5. Un critère pour que R soit de Gorenstein

Rappelons d'abord la:

DÉFINITION 5.1. — *Soit R un anneau local nœtherien de dimension de Krull n.*

Soit $\mathfrak{m}$ (resp. k) son idéal maximal (resp. son corps résiduel). On dit que R est de Gorenstein si

(i) *R est de Cohen-Macaulay i.e.* $\mathrm{Ext}^i_R(k, R)=0$ *pour* $i=0, \ldots, n-1$ *et* $\mathrm{Ext}^n_R(k, R)\neq 0$,

(ii) $\dim_k \mathrm{Ext}^n_R(k, R)=1$.

On a les propriétés:

PROPOSITION 5.2. — (i) *Soit R local nœtherien et $\rho \in R$ ne divisant pas 0, alors R est de Gorenstein de dimension n si et seulement si $R/\rho R$ est de Gorenstein de dimension $n-1$.*

(ii) *Si R est artinien à corps résiduel fini, R est de Gorenstein de dimension 0 si et seulement si son dual de Pontryagin est un R-module libre (de rang 1).*

(iii) *Si R est une $\mathbf{Z}_p$-algèbre finie et plate R est de Gorenstein (de dimension 1) si et seulement si* $\mathrm{Hom}(\mathbf{R}, \mathbf{Z}_p)$ *est un R-module libre.*

Preuve. — Pour (i), *voir* [11], page 104.

Pour (ii), *voir* [14], proposition 4, page 328.

(iii) résulte facilement de (ii): si R est $\mathbf{Z}_p$-finie et plate, alors p ne divise pas 0 et R/pR est de dimension 0. De plus, son dual de Pontryagin coïncide avec son dual $\mathbf{F}_p$-linéaire, c'est-à-dire la réduction modulo p de $\mathrm{Hom}(R, \mathbf{Z}_p)$.

Considérons maintenant une composante locale R de $h^0(a)$, $a \neq 0, -1$. C'est un anneau local nœtherien de dimension 2. Soient $\omega_r = (1+X)^{p^{r-1}} - 1$, pour chaque $r \geqslant 1$, les polynômes d'Iwasawa. Comme R est finie et plate sur Λ, chacune des suites (ω_r, p) est m-régulière dans R. Soit $R_r = R/\omega_r R$ d'idéal maximal $\mathfrak{m}_r$ et $\bar{R}_r = R_r/pR_r$ d'idéal maximal $\bar{\mathfrak{m}}_r$. Grâce aux propriétés énoncées dans 5.2, on obtient aisément le:

LEMME 5.3. — *Il y a équivalence entre les assertions*:

(i) *R est de Gorenstein de dimension 2.*

(ii) *R_r est de Gorenstein de dimension 1 pour chaque $r \geqslant 1$.*

(iii) *R_1 est de Gorenstein (de dimension 1).*

On rappelle alors un critère dû à MAZUR [12] (lemme 15.1).

PROPOSITION 5.4. — *Si $J_1(R)[\mathfrak{m}_1]$ est de dimension 2 sur le corps résiduel de R_1, alors R_1 est de Gorenstein.*

Ainsi à l'aide de ce critère, pour savoir si une composante R est de Gorenstein, il faut étudier l'espace vectoriel sur $k = R/\mathfrak{m}$

$$W = J_1(R)[\mathfrak{m}_1].$$

L'outil pour cela est la notion de représentation résiduelle de [15], § 10, particularisée ici en la:

DÉFINITION 5.5. — *Une représentation*

$$\bar{\rho}: \quad \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL(V)$$

est dite $\mathfrak{m}$-résiduelle si elle est de degré 2 sur k, est non ramifiée hors de Np, et si le polynôme caractéristique d'un Frobenius en $l \nmid Np$ est $X^2 - T(l)X + l\langle l \rangle$ modulo $\mathfrak{m}$.

Le critère s'énonce alors:

PROPOSITION 5.6. — *Pour que R soit de Gorenstein, il suffit qu'il existe une représentation* m*-résiduelle irréductible.*

Preuve. — On utilise l'hypothèse qu'il existe une représentation m-résiduelle irréductible:

SOUS-LEMME 5.7 ([22], *proposition* 4.1). — *Soit G un groupe. Soient V un kG-module irréductible et W un kG-module tel que pour tout σ de G, on ait $P_{\sigma_V}(\sigma_W)=0$ (où $P_{\sigma_V}(X)$ est le polynôme caractéristique de l'élément $\sigma_V \in GL(V)$ déduit de σ, et $\sigma_W \in GL(W)$ est déduit de même de σ) alors tous les quotients d'une suite de Jordan-Hölder de W sont isomorphes à V.*

Preuve: Soit $\hat{W}$ la représentation contragrédiente de W et $\hat{W}(\det \rho_V)$ sa tordue par le caractère de degré 1 déterminant de $\rho_V : G \to GL(V)$. Soit $M = W \oplus \hat{W}(\det \rho_V)$ on voit facilement que le polynôme caractéristique de σ_M vaut $P_{\sigma_V}^{\dim W}$. Par conséquent, d'après le théorème de Brauer-Nesbitt, la semi-simplifiée $M^{s.s.}$ de M est isomorphe à $V^{\dim W}$ d'où l'on conclut que $W^{s.s.}$ est isomorphe à une puissance de V.

Revenons alors à la démonstration de la proposition (5.6) on a:

$$J_1(R) = R_1 \otimes \Pi_p \oplus \mathrm{Hom}(R_1, \Pi_p) \quad (cf. \text{ théorème } (4.4)),$$

donc

$$J_1(R)[p] = \bar{R}_1 \oplus \mathrm{Hom}(\bar{R}_1, \mathbf{F}_p)$$

où $\bar{R}_1$ et $\mathrm{Hom}(\bar{R}_1, \mathbf{F}_p)$ sont des modules indécomposables au sens de [3], paragraphe 14, sur l'anneau artinien $\bar{R}_1$.

D'autre part, l'action de la conjugaison complexe se diagonalise en:

$$J_1(R)[p] = J_1(R)[p]^+ \oplus J_1(R)[p]^-$$

où

$$J_1(R)[p]^{\pm} = \{ x \in J_1(R)[p] ; c(x) = \pm x \}.$$

D'après le théorème de Krull-Schmidt (*cf.* [3], § 14) on voit que

$$J_1(R)[p]^{\pm} \simeq \bar{R}_1 \qquad \text{et} \qquad J_1(R)^{\mp} \simeq \mathrm{Hom}(\bar{R}_1, \mathbf{F}_p)$$

comme R_1-modules. On prend alors les parties de $\mathfrak{m}_1$-torsion:

$$J_1(R)[\mathfrak{m}_1]^{\pm} \simeq \bar{R}_1[\bar{\mathfrak{m}}_1]$$
$$J_1(R)[\mathfrak{m}_1]^{\mp} \simeq \mathrm{Hom}(k, \mathbf{F}_p) \simeq k.$$

Notons que la propriété de Gorenstein équivaut à ce que $\bar{R}_1[\bar{\mathfrak{m}}_1] \simeq k$ mais que sans hypothèses, on a :

$$\mathrm{Hom}(\bar{R}_1, \mathbf{F}_p)[\mathfrak{m}_1] \simeq k.$$

Or, en approximant la conjugaison complexe c par un Frobenius F_l où $l \equiv -1 \bmod. Np$, on voit que son polynôme caractéristique sur V est du type $X^2 - aX - 1$ (i.e. $l\langle l \rangle \equiv -1 \bmod. \mathfrak{m}$) et $-1 \not\equiv 1 \bmod. p$, donc la conjugaison complexe n'agit pas par homothétie sur V :

$$V = V^+ \oplus V^- \qquad \text{avec} \quad \dim. V^{\mp} = 1.$$

On voit donc grâce au sous-lemme précédent que

$$\dim_k J^+(R)[\mathfrak{m}] = \dim J(\bar{R})[\mathfrak{m}]$$

et donc, que $\bar{R}_1[\bar{\mathfrak{m}}_1]$ est de dimension 1 sur k, donc que W est de dimension 2 sur k.

On peut par exemple appliquer ce critère à une composante locale R « de type C.M. » au sens de [7], proposition 2.3. On obtient une représentation $\mathfrak{m}$-résiduelle irréductible en considérant un Grössencharakter de type (1.0) au corps quadratique imaginaire K associé, de conducteur $\mathfrak{cp}$ (où $N = |\mathrm{disc}(K)| . N\mathfrak{c}$) et en induisant de K à $\mathbf{Q}$. Ce qui redémontre le fait (*cf.* HIDA, Séminaire de Théorie des Nombres de Paris, Exposé, 1985) qu'une composante locale « de type C.M. » est de Gorenstein.

Nous reviendrons dans un prochain article sur ces composantes et leur lien avec l'arithmétique de la $\mathbf{Z}_p$-extension anticyclotomique de K.

BIBLIOGRAPHIE

[1] ASAI (T.). – On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution. *J. Math. Soc. Japan*, t. 28, 1976, p. 48-61.

[2] ATKIN (A. O. L.) and LEHNER (J.). – Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, t. 185, 1970, p. 134-160.

[3] CURTIS (C.) and REINER (I.). – *Representation Theory of finite groups and associative algebras*, Interscience Publishers John Wiley & Sons, 1966.

[4] HIDA (H.). – On congruence divisors of cusp forms as factors of the special values of their zeta functions. *Inv. Math.*, t. 64, 1981, p. 221-262.

[5] HIDA (H.). – Kummer's criterion for the special values of Hecke L-functions of imaginary quadratic fields and congruences among cusp forms. *Inv. Math.*, t. 66, 1982, p. 415-459.

[6] HIDA (H.). – Iwasawa modules attached to congruences among cusp forms, *Ann. Scient. de l'E.N.S.* (à paraître).

[7] HIDA (H.). – Gclois Representations into $GL_2(Z_p[[X]])$ attached to ordinary cusp forms, *Inv. Math.* (à paraître).

[8] IGUSA (J.). – Kroneckerian model of fields of elliptic modular functions, *Amer. J. Math.*, t. 81, 1968, p. 561-577.

[9] LANGLANDS (R.-P.). – Modular forms and l-adic representations (International Summer School on Modular Functions, Antwerp, 1972). Modular Functions in one one variable II, *Lmcture Notes in Mathematics*, vol. 349, p. 361-500, Berlin-Heidelberg-New York: Springer, 1973.

[10] LI (W.). – Newforms and functional equations, *Math. Ann.*, t. 212, 1975, p. 285-315.

[11] MATSUMURA (H.). – *Commutative Algebra*, W. A. Benjamin, Inc. 1970.

[12] MAZUR (B.). – Modular Curves and the Eisenstein Ideal. *Publ. Math. I.H.E.S.* 47, 1978.

[13] MAZUR (B.) and KATZ (N.). – Arithmetic moduli of elliptic curves, *Annals of Math. Studies*, Nwmber 108. Princeton University Press., 1985.

[14] MAZUR (B) and WILES (A.). – Class fields of abelian extensions of Q, *Inv. Math.*, t. 76, 1984, p. 179-330.

[15] MAZUR (B.) and WILES (A.). – On p-adic analytic families of Galois Representations (To appear).

[16] MUMFORD (D.). – Geometric invariant theory, *Ergebnisse der Mathematik und Ihrer Grenzgebiete*, 36, Springer-Verlag, 1965.

[17] OGG (A.). – On the eigenvalues of Hecke operators, *Meth. Ann.*, t. 79, 1969, p. 101-108.

[18] RAYNAUD (M.). – Specialisation du Foncteur de Picard, *Publ. Math. I.H.E.S.*, 38, 1970, p. 27-76.

[19] SHIMURA (G.). – *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten Publishers and Princeton University Press., 1971.

[20] SHIMURA (G.). – Class fields over real quadratic fields and Hecke operators. *Ann. of Math.*, t. 295, 1970, p. 130-190.

[21] TATE (J.). – p-divisible Groups, *Proceedings of a Conference on Local Fields*, Driebergen, 1966, Springer-Verlag, 1967.

[22] WILES (A.). – *Modular Curves and the Class Group of* $Q(\zeta_p)$, *Inv. Math.*, 58, 1980, p. 1-35.