COMPOSITIO MATHEMATICA

JACQUES TILOUINE

Théorie d'Iwasawa classique et de l'algèbre de Hecke ordinaire

Compositio Mathematica, tome 65, nº 3 (1988), p. 265-320
<http://www.numdam.org/item?id=CM_1988__65_3_265_0>

Compositio Mathematica 65: 265–320 (1988)

Théorie d'Iwasawa classique et de l'algèbre de Hecke ordinaire

JACQUES TILOUINE
Université de Paris-Sud, Mathématique, Bât. 425, 91405 Orsay, France

Received 19 January 1987; accepted in revised form 20 October 1987

Plan

Introduction

Dans cet article, nous donnons une illustration de la philosophie de la Main Conjecture de Coates-Iwasawa (voir [2]). Notre point de départ a été l'article [8] de H. Hida et les méthodes que nous utilisons sont directement issues des idées qu'il a développées dans la série d'articles [6]–[11]. Pour parodier l'introduction de [8], on peut dire que nous nous intéressons à trois modules de type fini et de torsion sur l'algèbre d'Iwasawa $\Lambda = \mathbb{Z}_p[[T]]$ qu'on peut aussi considérer comme l'algèbre complétée du groupe de Galois d'une certaine $\mathbb{Z}_p$-extension de corps de nombres. Soit $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et ι un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}_p$, où p est un nombre premier et $\mathbb{C}_p$ est la complétion d'une clôture algébrique de $\mathbb{Q}_p$.

Soit M un corps quadratique imaginaire et λ un Grössencharakter de M de type $(v, 0)$ où v est un entier $\geqslant 1$ (c'est-à-dire que $\lambda(\alpha) = \alpha^v$ pour tout α de M congru à 1 modulo le conducteur $\mathfrak{f}$ de λ). On suppose maintenant que le nombre premier p est décomposé dans M, disons $(p) = \mathfrak{p}\mathfrak{p}^\varrho$, où ϱ désigne désormais la conjugaison complexe et $\mathfrak{p}$ est la place de M induite par ι. D'après une remarque de Weil, on peut associer à (λ, ι) un caractère:

$$\lambda\colon \mathrm{Gal}(\bar{\mathbb{Q}}/M) \to \mathbb{C}_p^\times .$$

Définissons alors:

$$\lambda^{\varrho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/M) \to \mathbb{C}_p^{\times}$$

par la formule $\lambda^{\varrho}(\sigma) = \lambda(\varrho\sigma\varrho^{-1})$.

Soit κ la partie d'ordre premier à p du caractère galoisien $\lambda/\lambda^{\varrho}$. On voit facilement que κ se factorise à travers le groupe de Galois de F sur M, où F désigne le corps de rayons de conducteur $p.\mathbf{N}\mathfrak{f}$. Soit M_∞ l'unique $\mathbb{Z}_p$-extension de M qui est galoisienne sur $\mathbb{Q}$ et non abélienne sur $\mathbb{Q}$ (on l'appelle la $\mathbb{Z}_p$-extension anticyclotomique de M). Posons:

$$F_\infty^- = M_\infty^- \cdot F \quad \text{et} \quad \Gamma^{-1} = \mathrm{Gal}(F_\infty^-/F)$$

La théorie d'Iwasawa classique (cf. [2]) associe à F_∞^- deux modules de type fini et de torsion sur $\mathbb{Z}_p[[\Gamma^-]]$; un de ces modules est le groupe de Galois X sur F_∞^- de la p-extension abélienne maximale non ramifiée hors de $\mathfrak{p}$ de F_∞^-; l'autre est la limite projective des unités locales en $\mathfrak{p}$ divisées par l'adhérence des unités elliptiques, dans la tour des sous-extensions de F_∞^-/F. Ceci dit, la Main Conjecture prédit l'égalité des séries caractéristiques de ces deux modules. L'ingrédient nouveau dans notre travail est un troisième module, le module de congruences, attaché à (λ, ι) par Hida (voir [10] pour la définition exacte, et aussi le paragraphe 1 de cet article). En fait, ce module de congruences n'est lié qu'à la κ-partie des deux modules classiques pour Γ^-. Le but de cet article est de montrer sous des conditions techniques malheureusement restrictives, que la série caractéristique du module de congruences divise la série caractéristique d'une version tordue de la κ-partie du module X. C'est le thorème 3.3 du texte. Sa démonstration occupe les paragraphes 4 à 6. Nous avons besoin pour celle-ci d'hypothèses techniques sur λ, M et p que nous rassemblons ici:

Hypothèses. On suppose que le conducteur $\mathfrak{f}$ de λ est étranger à son conjugué complexe $\mathfrak{f}^{\varrho}$, que l'entier v est différent de 1, donc $v \geqslant 2$. De plus, le nombre premier p décomposé dans M sera supposé strictement supérieur à $v + 1$ et premier à $6N\varphi(N)h$, où $N = D \cdot \mathbf{N}\mathfrak{f}$, $-D$ désignant le discriminant de M, h le nombre de classes de M, et φ la fonction d'Euler usuelle.

Notons l'hypothèse déplaisante $v \geqslant 2$. Nous l'utilisons malheureusement de façon essentielle pour appliquer les résultats de [24].

Il faut noter d'autre part que le théorème est une généralisation du théorème 0.1 de [8]. En effet, Hida définit un nombre rationnel $H(\lambda)$ de la forme:

$$H(\lambda) = * \cdot \prod_{\sigma} L(\lambda^{[\sigma]}\lambda^{[\sigma\varrho]}, v + 1)$$

où $*$ désigne un facteur de périodes défini au paragraphe 7 de [8], et où, pour tout automorphisme σ de $\mathbb{C}$ et tout idéal $\mathfrak{a}$ de M:

$$\lambda^{[\sigma]}(\mathfrak{a}) = \lambda(\sigma^{-1}\mathfrak{a})^{\sigma}$$

$$L(\lambda^{[\sigma]}\lambda^{[\sigma\varrho]}, s) = \sum \lambda^{[\sigma]}\lambda^{[\sigma\varrho]}(\mathfrak{a}) \cdot \mathrm{N}\mathfrak{a}^{-s}$$

son théorème 0.1 peut alors être réénoncé sous la forme:

THÉORÉME. *Si $p | H(\lambda)$, il existe une place $\mathfrak{P}$ de $\bar{\mathbb{Q}}$ au-dessus de $\mathfrak{p}$ et une représentation*:

$$\pi\colon \mathrm{Gal}(\bar{M}/M) \to GL_2(\bar{\mathbb{F}}_p)$$

telle que:

(i) *Pour tout σ de* $\mathrm{Gal}(\bar{M}/M)$, *on a*:

$$\pi(\sigma) = \begin{bmatrix} \tilde{\lambda}(\sigma) & a(\sigma) \\ 0 & \tilde{\lambda}^{\varrho}(\sigma) \end{bmatrix}$$

où $\tilde{\lambda}$ est la réduction de λ modulo $\mathfrak{P}$.

(ii) *La fonction a restreinte à* $\mathrm{Gal}(\bar{F}/F)$ *devient un homomorphisme de groupes a_F à valeurs dans $\mathbb{F}_p^+$, trivial sur les groupes d'inertie aux places de F ne divisant pas.*

(iii) *L'image de a_F n'est pas nulle.*

De même le théorème 3.3 est en fait corollaire du théorème suivant. Notons $\mathbb{H}$ la série caractéristique du module de congruences C et $\Lambda = \mathbb{Z}_p[[T]]$.

THÉORÈME. *Il existe une Λ-algèbre locale finie et plate R_2 un idéal $\mathfrak{c}_2$ de R_2 au-dessus de* $(\mathbb{H}) \subset \Lambda$, *et une fonction continue*:

$$a\colon \mathrm{Gal}(\bar{M}/M) \to \mathfrak{c}_2/\mathfrak{c}_2^2$$

telle que:

(i) $a(\sigma\sigma') = \Phi(\sigma) \cdot a(\sigma') + \Phi^{\varrho}(\sigma) \cdot a(\sigma)$

Φ *et* Φ^{ϱ} *désignant des généralisations de λ et λ^{ϱ}.*

(ii) *La restriction de a au groupe de Galois absolu de $\tilde{F}_\infty$, réunion des corps de rayons de M de conducteur $p^r \cdot \mathrm{N}\mathfrak{f}$, $r = 1, 2, \ldots$ est un homorphisme de groupes a_∞ trivial sur les groupes d'inertie aux places de $\tilde{F}_\infty$ ne divisant pas.*

(iii) *L'homorphisme a_∞ est surjectif.*

Dans cet énoncé, on a supposé pour simplifier que λ est à valeurs dans M. L'énoncé général se trouve dans la proposition 4.12. Le module de différentielles $C' = \mathfrak{c}_2/\mathfrak{c}_2^2$ a été introduit par Hida dans [28].

Pour déduire de ce théorème le résultat de divisibilité énoncé en 3.3, nous appliquons au module des différentielles un résultat d'algèbre commutative qui nous a été communiqué par Michel Raynaud et qui apporte la solution à une conjecture de H. Hida formulée dans [28]. Ce point est développé au paragraphe 6.

D'après le théorème 3.1 du présent article, pour que le théorème 3.3 soit non-vide, il suffit que $H(\lambda)$ soit divisible par p. Donnons quelques exemples (les calculs ont été effectués par J.-F. Mestre, et, pour le cas $M = \mathbb{Q}(\sqrt{-3})$, par Y. Maeda dans la table 8.11 de [6]):

M	v	p
$\mathbb{Q}(i)$	8	13
	12	149
$\mathbb{Q}(\sqrt{-3})$	30	30842593
$\mathbb{Q}(\sqrt{-7})$	8	191
	10	23
	12	79
	12	331

La méthode de démonstration, elle aussi, suit le plan de [8], et consiste à trouver un module galoisien dont la structure sur Λ soit proche de celle du module de congruences. C'est l'objet du paragraphe 4. On obtient ainsi les points (i) et (ii) de l'énoncé. Pour le point (iii) on raisonne par l'absurde en utilisant la définition même du module de congruences. C'est l'objet du paragraphe 5.

§1. "Théorie d'Iwasawa" de l'algèbra de Hecke ordinaire

Cette théorie est dûe à H. Hida. L'objet du présent paragraphe est de fixer les notations et de rappeler les résultats de la théorie qui nous seront utiles. Les références pour les démonstrations omises sont [10] et [11].

Soit N un entier $\geqslant 1$ et p un nombre premier impair ne divisant pas N. On s'intéressera principalement aux groupes de congruences:

$$\Gamma_1(Np^r) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ a \equiv d \equiv 1 \text{ mod. } Np^r \text{ et } c \equiv 0 \text{ mod. } Np^r \right\}$$

pour r entier positif ou nul.

Soit $k \geqslant 2$; comme d'habitude, on notera $S_k(\Gamma_1(Np^r))$ le $\mathbb{C}$-espace des formes modulaires pour $\Gamma_1(Np^r)$ paraboliques et de poids k. Le développement de Taylor de ces formes à l'infini fournit le morphisme de q-développement, identifiant $S_k(\Gamma_1(Np^r))$ à son image:

$$S_k(\Gamma_1(Np^r)) \to \mathbb{C}[[q]]$$

$$f = \sum_{n\geqslant 1} a(n,f) \exp(2\pi\sqrt{-1}nz) \mapsto \sum_{n\geqslant 1} a(n,f)q^n.$$

Pour tout sous-anneau A de $\mathbb{C}$, on note:

$$S_{k,r}(A) = S_k(\Gamma_1(Np^r)) \cap A[[q]].$$

Fixons pour l'instant $k \geqslant 2$ et $r \geqslant 0$. Pour chaque entier $n \geqslant 1$, on note $T(n)$ le $n^{\text{ième}}$ opérateur de Hecke vu comme endomorphisme de $S_{k,r}(\mathbb{C})$. On note $h_{k,r}(A)$ la A-algèbre engendrée par tous les opérateurs $T(n)$, $n \geqslant 1$. Il est facile de voir (cf. [22], théorème 3.45) que l'application:

$$\begin{aligned} h_{k,r}(\mathbb{C}) \times S_{k,r}(\mathbb{C}) &\to \mathbb{C} \\ (T,f) &\mapsto a(1,f|T) \end{aligned} \tag{1.1}$$

établit une dualité parfaite entre les deux espaces. Grâce à ce résultat, on peut montrer facilement le.

LEMME 1.1. *Les modules $S_{k,r}(\mathbb{Z})$ et $h_{k,r}(\mathbb{Z})$ sont libres de type fini de même rang sur $\mathbb{Z}$ egal à* $\dim_{\mathbb{C}} S_{k,r}(\mathbb{C})$. *De plus pour tout sous-anneau A de $\mathbb{C}$, on a canoniquement*

$$S_{k,r}(\mathbb{Z}) \otimes A \xrightarrow{\sim} S_{k,r}(A)$$

$$h_{k,r}(\mathbb{Z}) \otimes A \xrightarrow{\sim} h_{k,r}(A).$$

Nous pouvons alors poser la définition cohérente pour tout anneau A

$$S_{k,r}(A) = S_{k,r}(\mathbb{Z}) \otimes A$$

$$h_{k,r}(A) = h_{k,r}(\mathbb{Z}) \otimes A.$$

Cependant, notons qu'il n'est pas évident pour ces définitions que $h_{k,r}(A)$ opère sur $S_{k,r}(A)$. En fait, si A est un sous-corps de $\mathbb{C}$, il faut pour montrer cela utiliser l'interprétation modulaire sur $\mathbb{Q}$ de l'espace $S_{k,r}(\mathbb{Q})$, et pour $A = \mathbb{Z}$, on doit utiliser l'interprétation modulaire de Katz (cf. [10] §2 et [13]). On va se cantonner au cas suivant. Soit K une extension finie de $\mathbb{Q}_p$, $\mathcal{O}_K$ son anneau des entiers.

LEMME 1.2. *Le module $S_{k,r}(\mathcal{O}_K)$ est stable sous l'action des opérateurs de Hecke.*

Glose. On vient de mentionner que $h_{k,r}(\mathbb{Q})$ laissait stable $S_{k,r}(\mathbb{Q})$. On a donc une action naturelle de $h_{k,r}(K)$ sur $S_{k,r}(K)$ et le problème est celui de l'intégralité: voir [10] §2.

Formons maintenant les objets que régit la théorie de Hida. L'inclusion $S_{k,r}(\mathbb{Z}) \to \mathbb{Z}[[q]]$ fournit par tensorisation par $\mathcal{O}_K$ un morphisme $S_{k,r}(\mathcal{O}_K) \to \mathcal{O}_K[[q]]$ par lequel nous identifions l'espace source à son image. Si r croît, les inclusions ci-dessus sont compatibles.

Notations 1.3. Pour $k \geqslant 2$ fixé, on note $S_k = S_k(Np^\infty, \mathcal{O}_K)$ le sous-module de $\mathcal{O}_K[[q]]$ réunion des $\mathcal{O}_K$-modules $S_{k,r}(\mathcal{O}_K)$, $r = 0, 1, 2 \ldots$. De même on note $h_k = h_k(Np^\infty, \mathcal{O}_K)$ la limite projective des algèbres de Hecke $h_{k,r} = h_{k,r}(\mathcal{O}_K)$ $(r = 1, 2 \ldots)$ pour les applications de restriction.

Munissons $\mathcal{O}_K[[q]]$ de la topologie de la valeur absolue: $|\Sigma_{n\geqslant 0}\, a_n q^n| = \mathrm{Sup}_{n\geqslant 0}|a_n|_p$. Soit $\bar{S}_k$ le complété de S_k pour cette topologie. Par uniforme continuité, l'algèbre h_k opère encore sur $\bar{S}_k$. Par passage à la limite projective, on voit facilement que l'accouplement

$$\begin{aligned} h_k \times \bar{S}_k &\to \mathcal{O}_K \\ (T, f) &\mapsto a_1(f|T) \end{aligned} \tag{1.2}$$

établit encore une dualité parfaite entre les deux modules compacts $\bar{S}_k$ et h_k. C'est-à-dire qu'elle induit un isomorphisme de chaque espace sur le dual $\mathcal{O}_K$-linéaire de l'autre.

Définissons maintenant, suivant Katz et Hida ([10] et [13]), une structure de module sur l'algèbre d'Iwasawa pour h_k. Pour $k \geqslant 2, r \geqslant 0$ et a un entier premier à Np, on choisit $\sigma_a \in SL_2(\mathbb{Z})$ tel que $\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right)$ mod. Np^r et on pose:

$$f|\langle a\rangle_k = f|_k\sigma_a.$$

On voit facilement que si ℓ est premier et congru à a modulo Np^r, on a:

$$\langle a\rangle_k = \frac{T(\ell)^2 - T(\ell^2)}{\ell^{k-1}},$$

donc $\langle a\rangle_k \in h_{k,r}(\mathbb{Q})$, et même $\langle a\rangle_k \in h_{k,r}$. Notons que $\langle a\rangle_k$ ne dépend que de a mod. Np^r. On définit la représentation "diamant de poids k":

$$\langle\,.\,\rangle_k\colon (\mathbb{Z}/Np^r\mathbb{Z})^\times \to h_{k,r}.$$

Son noyau est contenu dans $\{\pm 1\}$. Soit $Z_{r-1} = (\mathbb{Z}/Np^r\mathbb{Z})^\times$ pour chaque $r \geqslant 1$. Si r croît, les applications ainsi définies sont compatibles et par passage à la limite projective, on obtient un morphisme de noyau contenu dans $\{\pm 1\}$:

$$\langle\,.\,\rangle_k\colon Z = \varprojlim Z_r \to h_k.$$

Notons $\Gamma = 1 + p\mathbb{Z}_p$. On a des décompositions canoniques:

$$\begin{aligned} Z_0 &= (\mathbb{Z}/N\mathbb{Z})^\times \times \mu_{p-1}; & \mathbb{Z}_p^\times &= \mu_{p-1} \times \Gamma \\ z_0 &= (z_N, \zeta) & z_p &= (\zeta, z_1) \\ Z &= (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times; & Z &= Z_0 \times \Gamma \\ z &= (z_N, z_p) & z &= (z_0, z_1). \end{aligned}$$

On définit alors l'action de poids 0 sur h_k:

DÉFINITION 1.4. On appelle action de poids 0 de Z sur $\bar{S}_k$ le morphisme suivant:

$$\langle\,.\,\rangle_0\colon Z \to h_k$$

si

$$z = (z_N, z_p), \quad \langle z\rangle_0 = z_p^k\langle z\rangle_k.$$

On peut munir le $\mathcal{O}_K$-module compact h_k d'une structure de module sur $\mathcal{O}_K[[Z]] = \mathcal{O}_K[[\Gamma]][Z_0]$ grâce aux diamants de poids 0. On choisit $u = 1 + Np \in \Gamma$ comme générateur topologique de Γ.

On identifiera désormais $\mathcal{O}_K[[\Gamma]]$ avec $\Lambda_K = \mathcal{O}_K[[T]]$ par $\langle u\rangle_0 \mapsto 1 + T$. D'autre part, pour $k \geqslant 2$, $r \geqslant 1$ la $\mathcal{O}_K$-algèbre finie et plate $h_{k,r}$ est semi-locale donc est produit direct de ses composantes locales. On forme le produit $h^0_{k,r}$ des composantes locales de $h_{k,r}$ dans lesquelles $T(p)$ est inversible. Cette opération est compatible avec le changement de niveau donc définit un système cohérent d'idempotents $e_{k,r}$ de $h_{k,r}$ et donne à la limite projective un idempotent e_k et une composante h^0_k de h_k (cf. [10] §3).

DÉFINITION 1.5. On appelle h^0_k la partie ordinaire de h_k et e_k l'idempotent ordinaire.

THÉORÈME 1.6 ([10], théorème 3.1). *h^0_k est une Λ_K-algèbre finie et plate.*

Soient k, k' deux entiers tels que $2 \leqslant k < k'$, on définit une application de changement de poids à l'aide des séries d'Eisenstein $E_{1,n}$ de poids 1, $\Gamma_0(p^n)$-modulaires et $\equiv 1$ mod. $p^n\mathbb{Z}_p$, de la façon suivante.

Si $n \geqslant r$, soit:

$$S_{k,r}(\mathcal{O}_K/p^n\mathcal{O}_K) \to S_{k',r}(\mathcal{O}_K/p^n\mathcal{O}_K)$$

$$f \to fE_{1,n}^{k'-k}.$$

Par passage au dual linéaire (grâce à (1.2)) puis à la limite projective sur n et enfin sur r, on obtient un morphisme surjectif d'algèbres $h_{k'} \to h_k$, qui applique $e_{k'}$ sur e_k. D'où un morphisme $h^0_{k'} \to h^0_k$.

THÉORÈME 1.7 ([11], théorème 1.1). *Le morphisme $h^0_{k'} \to h^0_k$ est un ismorphisme. On peut donc parler de h^0 sans spécifier le poids et de e comme de l'idempotent ordinaire.*

On munit désormais h, donc aussi h^0, de l'action de poids 0 de Z i.e., $\langle z\rangle_0 = z_p^\ell\langle z\rangle_\ell$ pour $z \in Z$; ℓ désignant un entier quelconque > 2 (cf. lemme 1.5). Soit $k \geqslant 2$, $r \geqslant 1$ et ε un caractère de Γ/Γ_r, qu'on peut supposer à valeurs dans K, quitte à faire une extension des scalaires. On pose:

$$P_{k,\varepsilon} = 1 + T - \varepsilon(u)u^k \tag{1.3}$$

$$\omega_{k,r} = (1 + T)^{p^{r-1}} - u^{kp^{r-1}}. \tag{1.4}$$

On remarque la formule $\omega_{k,r} = \Pi_{\substack{\varepsilon \text{ tel que} \\ \Gamma_r \subset \operatorname{Ker}\varepsilon}} P_{k,\varepsilon}$.

Soit $S^0_{k,r}(\varepsilon)$ la plus grande sous-$\mathcal{O}_K$-module de $S^0_{k,r}(\mathcal{O}_K)$ sur lequel Γ agit, en poids k, via le caractère ε. Il est stable sous $h^0_{k,r}$. On note $h^0_{k,\varepsilon}$ la $\mathcal{O}_K$-algèbre d'endomorphismes de $S^0_{k,r}(\varepsilon)$ image de l'algèbre $h^0_{k,r}$ par l'application de restriction. Les polynômes (1.3) et (1.4) permettent de contrôler l'algèbre h^0 au sens du

THÉORÈME 1.8. *Si* $k \geqslant 2$,
1) *Le morphisme d'algèbres* $h^0/P_{k,\varepsilon}h_0 \to h^0_{k,\varepsilon}$ *est un isomorphisme.*
2) *Le morphisme d'algèbres* $h^0/\omega_{k,r}h^0 \to h^0_{k,r}$ *est un isomorphisme.*

Démonstration. Voir le théorème 1.2 de [11].

D'autre part, on a un théorème de "contrôle de la primitivité". Soit $\mathscr{L}_K$ le corps des fractions de l'algèbre d'Iwasawa Λ_K et notons $\mathscr{Q}_K = h^0 \otimes_{\Lambda_K} \mathscr{L}_K$. C'est une algèbre artinienne, elle se décompose donc en produit de ses composantes locales. Isolons une composante locale $\mathscr{K}$:

$\mathscr{Q}_K = \mathscr{K} \oplus \mathscr{A}$. Soit $h(\mathscr{K})$ (resp. $h(\mathscr{A})$) l'image de h^0 par la projection sur $\mathscr{K}$ (resp. sur $\mathscr{A}$). On voit aisément à l'aide du théorème 1.8, que $F_{k,\varepsilon} = h(\mathscr{K})/P_{k,\varepsilon}h(\mathscr{K}) \otimes_{\mathscr{O}_K} K$ est facteur directe de $h^0_{k,\varepsilon} \otimes_{\mathscr{O}_K} K$. On énonce alors le:

THÉORÈME 1.9
1) *Les deux assertions suivantes sont équivalentes*:
   (i) *Il existe un couple* (k, ε), $(k \geqslant 2, r \geqslant 1$ *et* ε mod. $\Gamma_r)$ *pour lequel les formes modulaires de* $S_{k,r}$ (*propres pour tous les opérateurs de Hecke*) *correspondant par la dualité* (1.1) (ii) *aux caractères de* $F_{k,\varepsilon}$ *sont de niveau divisible par* N.
   (ii) *Pour tout couple* (k, ε) *comme ci-dessus, les formes modulaires de* $S_{k,r}$ *attachées aux caractères de* $F_{k,\varepsilon}$ *sont de niveau divisible par* N.
2) *Les conditions* (i) *ou* (ii) *étant remplies, la composante* $\mathscr{K}$ *est un corps et les* $F_{k,\varepsilon}$ *sont des* K*-algèbres semi-simples.*

Commentaire 1.10. Pour la définition du niveau, voir [10] corollaire 3.7 et [11] corollaire 1.3. Le démonstration est dans [10] corollaire 3.7. Une composante $\mathscr{K}$ satisfaisant les conditions (i) et (ii) de 1.9 est dite primitive. On appliquera le théorème 1.9 pour $\mathscr{K} = \mathscr{L}_K$ auquel cas $F_{k,\varepsilon} = K$ lorsque ε est à valeurs dans K. Définissons dans ce contexte le module de congruences et le théorème de contrôle qui le régit.

DÉFINITION 1.11. On appelle module de congruence C attaché à la composante primitive $\mathscr{K} = \mathscr{L}_K$ le conoyau du morphisme Λ_K-linéaire

$$h^0 \to h(\mathscr{K}) \oplus h(\mathscr{A}).$$

Commentaire. Cette définition est légérement différente de celle donnée par Hida dans [10] définition (3.9b). Cependant celles-ci coïncident dans le cas que voici. On sait que l'algèbre h^0 est produit direct de ses localisées. Il y a donc une unique composante locale R de h^0 telle que $\mathscr{K} \subset R \otimes \mathscr{L}_K$. Remarquons que R étant facteur direct de h^0 est un Λ_K-module libre de type fini. La coïncidence des définitions est alors assurée par la condition:

$$R \text{ est de Gorenstein.} \tag{1.5}$$

On expliquera cette hypothèse au paragraphe suivant et on montrera qu'elle est satisfaite dans notre cas. On la suppose vérifiée pour les énoncés ci-dessous.

Considérons la décomposition:

$$R \otimes \mathscr{L}_K = \mathscr{K} \oplus \mathscr{B} \tag{1.6}$$

on voit facilement que pour $R(\mathscr{K})$ et $R(\mathscr{B})$ les projections de R dans $\mathscr{K}$ et $\mathscr{B}$, on a un isomorphisme du conoyau de $R \to R(\mathscr{K}) \oplus R(\mathscr{B})$ avec C. Hida montre dans sa démonstration de la proposition (3.9) de [10] que (pour $\mathscr{K} = \mathscr{L}_K$ et sous (1.5)) $R(\mathscr{B})$ est un Λ_K-module libre et ceci entraîne que les définitions coïncident. Soient alors $k \geqslant 2$, $r \geqslant 1$, ε un caractère de Γ modulo Γ_r, à valeurs dans K. On pose:

$$R_{k,r} = R/\omega_{k,r}R \tag{1.7}$$

$$R_{k,\varepsilon} = R/P_{k,\varepsilon}R \tag{1.8}$$

On voit que d'après le théorème 1.8, $R_{k,r}$ est une $\mathcal{O}_K$-algèbre (locale, finie et plate) facteur direct de $h^0_{k,r}$, tandis que $R_{k,\varepsilon}$ est facteur direct de $h^0_{k,\varepsilon}$. On définit $R(\mathscr{B})_{k,\varepsilon}$ (resp. $(R(\mathscr{B})_{k,r})$ comme le quotient de $R(\mathscr{B})$ par $P_{k,\varepsilon}$ (resp. par $\omega_{k,r}$). Soit enfin $\Lambda_{K,r} = \Lambda_K/(\omega_{k,r})$. Désormais, on suppose que l'inclusion $\Lambda_K \to R(\mathscr{K})$ induit un isomorphisme. Donc on a, *a fortiori*, $\mathscr{L}_K \cong \mathscr{K}$. Sous cette hypothèse et sous l'hypothèse (1.5) on a la:

PROPOSITION 1.12. *Les suites naturelles de $\mathcal{O}_K$-modules, obtenues par réduction de* $0 \to R \to \Lambda_K \oplus R(\mathscr{B}) \to C \to 0$:

(i) $0 \to R_{k,\varepsilon} \to \mathcal{O}_K \otimes R(\mathscr{B})_{k,\varepsilon} \to C/P_{k,\varepsilon}C \to 0$

(ii) $0 \to R_{k,r} \to \Lambda_{k,r} \otimes R(\mathscr{B})_{k,r} \to C/\omega_{k,r}C \to 0$

sont exactes.

Démonstration. Il suffit de vérifier que $R_{k,\varepsilon}$ (resp. $R_{k,r}$) est bien le noyau de (i) (resp. (ii)). Comme tous les modules considérés sont $\mathcal{O}_K$-libres, il suffit de le voir après tensorisation par K. Pour cela, on considère l'idéal $\mathfrak{c}_1$ défini par $\mathfrak{c}_1 = R \cap R(\mathscr{K})$. C'est un idéal principal car R étant réflexif, sa trace sur $\mathscr{K}$ dans la décomposition (1.6) est aussi un module réflexif, sa trace sur l'anneau Λ_K (local régulier de dimension 2). De plus, si $P = P_{k,\varepsilon}$ la localisation en P de la suite exacte:

$$0 \to \mathfrak{c}_1 \to R \to R/\mathfrak{c}_1 \to 0 \tag{1.9}$$

montre que $\mathfrak{c}_{1,P}$ est facteur direct de R_P car le quotient $R/\mathfrak{c}_1$ est sans torsion donc localement libre. Il en résulte que le K-espace de dimension 1 $\bar{\mathfrak{c}}_1 = \mathfrak{c}_{1,P}/p\mathfrak{c}_{1,P}$ s'identifie à un idéal minimal de $R_{k,\varepsilon} \otimes K$. D'après le théorème de contrôle de la primitivité (1.9), il est contenu dans la partie nouvelle de $h^0_{k,\varepsilon}$(il résulte en effet de [9] lemme (3.3) que les parties nouvelles et anciennes de $S^0_{k,r}(\varepsilon) \otimes K$ sont stables par $h^0_{k,\varepsilon}$ et qu'on a une décomposition de cette algèbre de Hecke en produit des composantes nouvelle et ancienne qu'elle définit par restriction). Comme cette partie nouvelle est semi-simple grâce au théorème de multiplicité 1 (cf. [9] prop. 4.4) l'idéal $\bar{\mathfrak{c}}_1$ est une sous-algèbre facteur direct de $R_{k,\varepsilon} \otimes K$. Grâce au lemme de Hensel, on en déduit que $\mathfrak{c}_{1,P}$ est une sous-algèbre facteur direct de R_P. C'est donc que $\mathfrak{c}_{1,P} = \Lambda_P$ et en particulier $C_P = 0$ pour tout $P = P_{k,\varepsilon}$; $k \geqslant 2$, ε mod. Γ_r. On en déduit, par le lemme du serpent la suite exacte courte:

$$0 \longrightarrow R_{k,\varepsilon} \longrightarrow \mathcal{O}_K \oplus R(\mathscr{B})_{k,\varepsilon} \longrightarrow C/P_{k,\varepsilon}C \longrightarrow 0.$$

Comme ceci est vrai pour tout ε, on en déduit que pour $k \geqslant 2$ on a une suite exacte courte:

$$0 \longrightarrow R_{k,r} \xrightarrow{\alpha} \Lambda_r \oplus R(\mathscr{B})_{k,r} \longrightarrow C/\omega_{k,r}C \longrightarrow 0.$$

L'injectivité de α se voit en décomposant en les ε-parties après extensions des scalaires au corps K' des racines $(p^{r-1})^{\text{ièmes}}$.

Notons qu'au cours de la démonstration de 1.12, le phénomène important suivant est apparu. Soit $\mathfrak{c}_1 = R(\mathscr{B}) \cap R = \mathbb{H}\Lambda_K$. Il y a un isomorphisme naturel (induit par l'inclusion $\Lambda_K \to \Lambda_K \oplus R(\mathscr{B})$)

$$\Lambda_K/\mathbb{H}\Lambda_K \xrightarrow{\sim} C.$$

Et plus précisément, on a la

PROPOSITION 1.13. *Le module de congruences C attaché à une composante primitive de degré 1 est isomorphe à un module $\Lambda_K/\mathbb{H}\Lambda_K$ pour un $\mathbb{H} \in \mathcal{O}_K[[T]]$. En particulier, C n'a pas de sous-module pseudo-nul non nul.*

Notation 1.14. On note $\mathbb{H}$ une série caractéristique du module de congruence. Elle n'est définie qu'à multiplication par une unité de Λ_K près.

L'intérêt du module de congruences tient dans le théorème:

THÉORÈME 1.15. *Pour un couple (k, ε) donné, il y a équivalence entre:*
(i) *Le p-groupe fini $C_{k,\varepsilon}$ n'est pas trivial.*
(ii) *Pour toute forme $f_{k,\varepsilon}$ propre pour tous les opérateurs de Hecke attachée à la composante $F_{k,\varepsilon}$, il existe une autre forme $g \in S_{k,r}(\varepsilon)$ propre pour tous les opérateurs de Hecke, attachée à une autre composante (i.e., n'étant pas conjuguée à une forme de $F_{k,\varepsilon}$) et qui est congrue à $f_{k,\varepsilon}$ modulo l'idéal maximal de $\mathbb{C}_p$.*

Démonstration. C'est facile: cf. Doi–Ohta [4]. Il est également important, bien qu'évident, de noter que la non-nullité d'un $C_{k,\varepsilon}$ équivaut par Nakayama à celle de C, donc des $C_{k,\varepsilon}$ pour tous les couples (k, ε).

§2. Composante à multiplication complexe de l'algèbre de Hecke

Soit M un corps quadratique imaginaire d'anneau des entiers $\mathcal{O}$, de discriminant $-D$, et de nombre de classes h. Soit $v \geqslant 2$ un entier et λ un Grössencharacter de M de type $(v, 0)$. Son conducteur est un idéal de $\mathcal{O}$ noté $\mathfrak{f}$. On conserve toutes les hypothèses de l'introduction.

Notons $\mathbf{N}$ la norme des idéaux de $\mathcal{O}$ et posons

$$N = D \cdot \mathbf{N}\mathfrak{f}.$$

Soit p un nombre premier ne divisant pas $6h \cdot N \cdot \varphi(N)$, où φ est la fonction d'Euler habituelle. On rappelle l'hypothèse fondamentale que p est décomposé dans M disons en $\mathfrak{p}$ et $\mathfrak{p}^\varrho$: $p \cdot \mathcal{O} = \mathfrak{p}\mathfrak{p}^\varrho$. Pour chaque entier $r \geqslant 1$, on note $C\ell_{\mathfrak{f}\mathfrak{p}^r}$ le groupe des classes de rayons de M modulo $\mathfrak{f}\mathfrak{p}^r$, puis $C\ell_{\mathfrak{f}\mathfrak{p}^\infty} = \varprojlim C\ell_{\mathfrak{f}\mathfrak{p}^r}$. Soit I le monoïde des idéaux de $\mathcal{O}$ premiers à $\mathfrak{f}\mathfrak{p}$. Il s'injecte naturellement dans $C\ell_{\mathfrak{f}\mathfrak{p}^\infty}$. En effet, si $\mathfrak{a} \in I$ est d'image triviale dans tous les groupes $C\ell_{\mathfrak{f}\mathfrak{p}^r}$, c'est que $\mathfrak{a} = (\alpha)$ pour $\alpha \in \mathcal{O}, \alpha \equiv 1$ mod. $\mathfrak{f}\mathfrak{p}^r$, et pour chaque $r \geqslant 1$, il existe ε_r une unité de $\mathcal{O}$ telle que $\varepsilon_r\alpha = 1$ mod. $\mathfrak{f}\mathfrak{p}^r$. On prend la norme de cette congruence et on constate que $\mathbf{N}\alpha = 1$, donc α est une unité et $\mathfrak{a} = (1)$. L'injectivité provient alors de ce que I s'injecte dans son groupe symétrisé.

On note cette inclusion $\mathfrak{a} \to [\mathfrak{a}]$.

Fixons désormais un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}_p$ induisant le plongement p-adique de M. On note $\mathfrak{P}$ la place de $\bar{\mathbb{Q}}$ ainsi définie. Soit K le sous-corps de $\mathbb{C}_p$ adhérence de M_λ, corps engendré sur M par les valeurs de λ sur I. C'est une extension finie non ramifiée de $\mathbb{Q}_p$. On désigne par $\mathcal{O}_K$ son anneau des entiers. Considérons alors le morphisme:

$$\lambda\colon I \to \mathcal{O}_K^\times$$

il est continu pour la topologie de I induite par celle de $C\ell_{\mathfrak{f}p^\infty}$. Il admet donc un unique prolongement continu:

$$\hat{\lambda}\colon C\ell_{\mathfrak{f}p^\infty} \to \mathcal{O}_K^\times.$$

On considère alors l'application $\mathcal{O}_K$-linéaire de changement de base de GL_1/M à $GL_2/\mathbb{Q}$ (cf. [28] §4):

$$\begin{aligned} \theta\colon \mathscr{C}(C\ell_{\mathfrak{f}p^\infty}, \mathcal{O}_K) &\to \bar{S} = \bar{S}(Np^\infty, \mathcal{O}_K) \\ f &\mapsto \sum_{\mathfrak{a}\in I} f(\mathfrak{a}) q^{N\mathfrak{a}} \end{aligned} \tag{2.1}$$

définie sur l'espace des fonctions continues sur $C\ell_{\mathfrak{f}p^\infty}$. Les valeurs de θ sont dans le module des formes modulaires p-adiques grâce au théorème de Hecke et Shimura [23] ou Weil [25].

Grâce à la dualité (1.2) du paragraphe 1 et la théorie de la mesure p-adique (théorème de Mahler) donnant la dualité:

$$\begin{aligned} \mathcal{O}_K[[C\ell_{\mathfrak{f}p^\infty}]] \times \mathscr{C}(C\ell_{\mathfrak{f}p^\infty}, \mathcal{O}_K) &\to \mathcal{O}_K \\ (\xi, f) &\mapsto \int_{C\ell_{\mathfrak{f}p^\infty}} f(x)\, d\xi(x) \end{aligned}$$

(voir [14], chapitre 4, paragraphe 2), on obtient, en dualisant (2.1), un morphisme d'anneaux explicitement déterminé (voir [10] formule (7.9)) par:

$$\theta^*\colon h \to \mathcal{O}_K[[C\ell_{\mathfrak{f}p^\infty}]]$$

$$T(\ell) \mapsto \begin{cases} [\mathscr{L}] + [\mathscr{L}^\rho] & \text{si } \ell\mathcal{O} = \mathscr{L}\mathscr{L}^\rho,\ \mathscr{L} \neq \mathscr{L}^\rho, \quad \text{et} \quad (\ell, \mathfrak{f}p) = 1. \\ 0 & \text{si } \ell \text{ est inerte.} \\ [\mathscr{L}] & \text{si } \mathscr{L} \text{ est ramifié ou décomposé mais } \mathscr{L}^\rho | \mathfrak{f}p. \end{cases}$$

On munit alors h de sa structure de $\mathcal{O}_K[[Z]]$-algebre pour l'action de Z de poids 0. Or d'après l'hypothèse $p \nmid 6h\varphi(N)N$, on voit facilement qu'il y a un isomorphisme canonique

$$C\ell_{\mathfrak{f}\mathfrak{p}^\infty} \simeq C\ell_{\mathfrak{f}\mathfrak{p}} \times (1 + \mathfrak{f}\hat{\mathfrak{p}}),$$

$$x \mapsto (x_0, x_1)$$

où

$$1 + \mathfrak{f}\hat{\mathfrak{p}} = \varprojlim 1 + \mathfrak{f}\mathfrak{p}/1 + \mathfrak{f}\mathfrak{p}^r.$$

Ceci résulte de ce que $\# C\ell_{\mathfrak{f}\mathfrak{p}} | hN\varphi(N)$ et $1 + \mathfrak{f}\hat{\mathfrak{p}}$ est isomorphe à $1 + p\mathbb{Z}_p$ donc est un pro-p-groupe. Plus précisément, si $N_0 = \mathbb{N}\mathfrak{f}$, $\mathbb{Z} \to \mathcal{O}$ induit:

$$\forall r \geqslant 0, \quad (\mathbb{Z}/N_0 p^r \mathbb{Z})^\times \xrightarrow{\sim} (\mathcal{O}/\mathfrak{f}\mathfrak{p}^r)^\times$$

(on utilise ici l'hypothèse $(\mathfrak{f}, \mathfrak{f}^\varrho) = 1$) donc $1 + N_0 p\mathbb{Z}/1 + N_0 p^r \mathbb{Z} \xrightarrow{\sim} 1 + \mathfrak{f}\mathfrak{p}/(1 + \mathfrak{f}\mathfrak{p}^r)$.

C'est donc encore vrai pour $N = D \cdot N_0$ au lieu de N_0. En passant à la limite projective sur r, on trouve:

$$\Gamma \xrightarrow{\sim} 1 + \mathfrak{f}\hat{\mathfrak{p}}.$$

Grâce à cet isomorphisme, on peut identifier

$$\Lambda_K = \mathcal{O}_K[[\Gamma]] \quad \text{et} \quad \mathcal{O}_K[[1 + \mathfrak{f}\hat{\mathfrak{p}}]].$$

D'autre part, on peut décomposer le caractère en ses restrictions à $C\ell$ et à $1 + \mathfrak{f}\hat{\mathfrak{p}}$. Notons $\hat{\lambda}_0$ la restriction à $C\ell_{\mathfrak{f}\mathfrak{p}}$. Notons que le conducteur de ce caractère de Dirichlet est $\mathfrak{f}\mathfrak{p}$ car si $=(\alpha)$, avec $(\alpha, \mathfrak{p}) = 1$ et $\alpha = 1$ mod. $\mathfrak{f}$, on a $\hat{\lambda}((\alpha)) = \alpha^v \equiv 1$ mod. $\mathfrak{P}$ car $0 < v < p - 1$.

On forme alors le caractère η, composé de

$$\mathcal{O}_K[[C\ell_{\mathfrak{f}\mathfrak{p}^\infty}]] \to \mathcal{O}_K[[1 + \mathfrak{f}\hat{\mathfrak{p}}]] \xrightarrow{\sim} \Lambda_K$$

$$x = (x_0, x_1) \mapsto \hat{\lambda}_0(x_0) \cdot x_1^{-1} \cdot [x_1] \to \hat{\lambda}_0(x_0) x_1^{-1} \langle x_1 \rangle_0$$

où l'on note $x_1 \mapsto [x_1]$ l'inclusion du groupe $1 + \mathfrak{f}\hat{\mathfrak{p}}$ dans son algèbre complétée $\mathcal{O}_K[[1 + \mathfrak{f}\hat{\mathfrak{p}}]]$ et où $\langle x_1 \rangle_0$ est l'élément de Γ correspondant à $[x_1]$ vu dans $1 + \mathfrak{f}\hat{\mathfrak{p}}$. On note enfin $\mathrm{X} = \eta \circ \theta^*$.

PROPOSITION 2.1. *Le caractère* X: $h \to \Lambda_K$ *est un morphisme surjectif de* Λ_K*-algèbres, qui se factorise à travers une composante primitive* $\mathcal{K}$ *de degré* 1 *de* h^0.

Démonstration. Comme les nombres premiers ℓ congrus à 1 modulo Np sont denses dans Γ, il suffit pour vérifier la Λ_K-linéarité de s'assurer que pour chaque tel nombre ℓ, on a:

$$\mathrm{X}(\langle \ell \rangle_0) = \langle \ell \rangle_0.$$

Rappelons pour cela que
1) l'ensemble des caractères $\hat{\lambda}$ provenant des Grössencharakters de M de conducteur multiple de $\mathfrak{f}$, divisant $\mathfrak{f}\mathfrak{p}^\infty$ et de type variable $(v, 0)$ $v \geqslant 1$ engendre un sous-espace dense de $C(C\ell_{\mathfrak{f}\mathfrak{p}^\infty}, \mathcal{O}_K)$
2) si λ est de type $(v, 0)$, conducteur $\mathfrak{f}\mathfrak{p}^r$, le théorème de Hecke–Shimura montre que $\theta(\hat{\lambda})$ est une forme modulaire de poids $k = v + 1$, primitive de niveau Np^r, admettant pour Nebentypus le caractère de Dirichlet mod. Np^r:

$$\psi(\ell) = \left(\frac{-D}{\ell}\right)\frac{\lambda((\ell))}{\ell^v}. \tag{2.2}$$

Cette forme est de plus ordinaire car $\lambda(\mathfrak{p}^\varrho)$ est une unité en $\mathfrak{p}$.

Grâce à ces deux remarques, on voit que:

$$\theta^*(\langle \ell \rangle_k) = \left(\frac{-D}{\ell}\right)\cdot \ell^{-v}\cdot [\ell]$$

donc

$$\theta^*(\langle \ell \rangle_0) = \left(\frac{-D}{\ell}\right)\ell[\ell]. \tag{2.3}$$

Si on ajoute la condition $\ell \equiv 1$ mod. Np, on trouve $\theta^*(\langle \ell \rangle_0) = \ell[\ell]$ et $\eta([\ell]) = \ell^{-1}\langle \ell \rangle_0$ donc

$$\mathrm{X}(\langle \ell \rangle_0) = \langle \ell \rangle_0.$$

Pour voir, de plus, que la composante $\mathscr{K}$ de $\mathscr{Q}_K$ définie par X est primitive (de degré 1), il suffit grâce au théorème 1.9 de réduire modulo $P = P_k = 1 + T - u^k$ (où $k = v + 1$) et $u = 1 + Np$). On trouve le caractère:

$$h_k^0(\Gamma_1(Np), \mathcal{O}_K) \to \mathcal{O}_K$$

$$T(\ell) \to \begin{cases} \lambda(\mathscr{L}) + \lambda(\mathscr{L}^\varrho) \\ 0 \\ \lambda(\mathscr{L}) \end{cases}$$

C'est le caractère attaché à $\theta(\hat{\lambda})$. On voit que $\theta(\hat{\lambda}) = f_0(z) - \lambda(\mathfrak{p})f_0(pz)$, où $f_0 = \Sigma_{(\mathfrak{a},\mathfrak{f})=1} \lambda(\mathfrak{a})q^{N\mathfrak{a}}$. Cette dernière forme est primitive de niveau N grâce au théorème de Hecke–Shimura [23] déjà mentionné. La forme $\theta(\hat{\lambda})$ est donc ordinaire-primitive au sens de Hida, [10] corollaire 3.7. Le résultat s'ensuit par le théorème 1.9. On considère alors la composante locale R de h^0 telle que $R \otimes \mathscr{L}_K \supset \mathscr{K}$. L'action de Z sur h^0 induit une action de $\mu_{p-1} \to Z$ qui fournit une décomposition de h^0 en produit de composantes $h^0(a)$ (a modulo $p - 1$) telles que sur $h^0(a)$: $\langle\zeta\rangle_0 = \zeta^a$ pour tout ζ de μ_{p-1}. On voit grâce à la formule (2.3) que la composante R est contenue dans $h^0(v + 1)$. En effet, si $\ell \equiv 1$ mod. N, $\ell \equiv \zeta$ mod. p^r, on a par (2.3)

$$\theta^*(\langle\ell\rangle_0) = \ell \cdot [\ell]$$

et si on écrit $\ell = (\zeta, \ell_1)$ dans Z, on a:

$$\eta([(\ell)]) = \zeta^v \cdot \ell_1^{-1}\langle\ell_1\rangle_0$$

donc si ℓ tend vers ζ dans Z, on obtient à la limite:

$$\mathrm{X}(\langle\zeta\rangle_0) = \zeta^{v+1}.$$

On note désormais $a = v + 1$ mod. $p - 1$, et grâce à l'hypothèse $1 < v < p - 1$, on a:

$$a \neq 1, 2. \tag{2.4}$$

Comme $R \subset h^0(a)$, on va appliquer les résultats de [16] et [24] pour prouver le

THÉORÈME 2.2. *La composante locale R associée à la composante primitive $\mathscr{K}$ est de Gorenstein.*

Commentaires

1) Comme R est local noetherien de dimension 2 et est une Λ_K-algèbre finie et plate, cet énoncé équivaut à:

$$\mathrm{Hom}_{\Lambda_K}(R, \Lambda_K) \quad \text{est un } R\text{-module libre (de rang 1).}$$

2) Grâce au théorème 2.2 et à la proposition 3.9 de [10] (cf. aussi le lemme 4.1 ci-après) on voit que la définition 1.11 du module de congruences coïncide avec celle de [10] (3.9.b).

Démonstration. Sous l'hypothèse (2.4), on peut appliquer le critère 5.6 de [24]: Soit $\mathbb{F}$ le corps résiduel de $\mathcal{O}_K$, pour que R soit de Gorenstein, il suffit qu'il existe une représentation $\mathfrak{M}$-résiduelle irréductible. On prend ici la représentation W contragrédiente de $\mathrm{Ind}_{\mathbb{Q}}^{M}\mathbb{F}(\tilde{\lambda})$, où $\mathbb{F}(\tilde{\lambda})$ désigne le $\mathbb{F}$-espace vectoriel de dimension 1 sur lequel $G_M = \mathrm{Gal}(\bar{M}/M)$ opère par le caractère $\tilde{\lambda}$. Par le critère d'irréductibilité de Mackey (cf. [20] paragraphe 7.4) et le fait que $\tilde{\lambda} \neq \tilde{\lambda}^{\varrho}$, on conclut que W est irréductible sur $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Elle est $\mathfrak{M}$-résiduelle par définition. La composante R est donc de Gorenstein.

Q.E.D.

On a vérifié les hypothèses requises pour la validité des propositions 1.12 et 1.13. On connaît donc la structure sur Λ_K du module de congruences attaché à notre situation. On a en fait des renseignements supplémentaires sur la composante R.

PROPOSITION 2.3. *Toutes les composantes de $R \otimes_{\Lambda_K} \mathcal{L}_K$ sont primitives. Cette algèbre est donc semi-simple et on peut écrire*:

$$R \otimes \mathcal{L}_K = \mathcal{K} \times \mathcal{B} \tag{2.5}$$

où $\mathcal{B}$ est un produit de corps.

Démonstration. On voit facilement que le Nebentypus de $\theta(\hat{\lambda})$ est un caractère de Dirichlet de conducteur Np égal au niveau de la forme primitive $\theta(\hat{\lambda})$. En outre, la réduction $R_{k,1}$ de R modulo $P_{k,1}$ peut être caractérisée comme suit. Soit $\chi_{\hat{\lambda}}$ le caractère de $h^0_{k,1} = h^0_k(\Gamma_1(Np), \mathcal{O}_K)$ associé à $\theta(\hat{\lambda})$. On constate alors que $R_{k,1}$ est l'unique composante locale à travers laquelle tous les caractères χ de $h^0_{k,1}$ congrus à $\chi_{\hat{\lambda}}$ mod. $\mathfrak{P}$ se factorisent et eux seulement. Si donc χ est un caractère de la Λ_K-algèbre R, sa réduction modulo P_k définit une forme congrue à $\chi_{\hat{\lambda}}$ modulo $\mathfrak{P}$. En particulier, les Nebentypus sont congrus à cause de la formule:

$$\psi(\ell) = \frac{a_\ell^2 - a_{\ell^2}}{\ell}.$$

Comme $p \nmid 6N\varphi(N)$, on a en particulier $p \nmid \varphi(Np)$, donc les Nebentypus sont égaux. Il en résulte donc que le niveau des formes de poids 2 attachées à une composante de $R \otimes \mathscr{L}_K$ est divisible par N. D'après le théorème 1.9, on conclut que ces composantes sont primitives. Le théorème de multiplicité 1 nous dit que $R_{k,1} \otimes_{\mathcal{O}_K} K$ est produit de corps et le lemme de Hensel appliqué à l'anneau de valuation discrète complet Λ_{K,P_k} nous permet de conclure à la semi-simplicité de $R \otimes \mathscr{L}_K$: c'est un produit de corps qui sont composantes primitives.

On peut même affirmer:

PROPOSITION 2.4. *Les composantes de $\mathscr{R}$ ne sont pas à multiplication complexe par M.*

Explication. Soit $\mathfrak{f}'$ un idéal entier de M tel que $N = D \cdot \mathrm{N}\mathfrak{f}'$. Soit θ' l'application analogue à α, construite pour $C\ell_{\mathfrak{f}'\mathfrak{p}^\infty}$. On dira qu'un caractère de h^0 est à multiplication complexe par M s'il se factorise à travers θ' pour un idéal $\mathfrak{f}'$ convenable.

Démonstration. Supposons qu'on ait une composante $\mathscr{K}'$ de $\mathscr{R}$ à multiplication par M. En réduisant modulo $P_{2,1}$, on aura deux Grössencharakters μ et μ' de conducteurs $\mathfrak{f}\mathfrak{p}$ et $\mathfrak{f}'\mathfrak{p}$, de type (1, 0), tels que $\mu = \mu' \bmod. \mathfrak{P}$. On définit donc un caractère de Dirichlet α par $\mu' = \alpha\mu$, de conducteur divisant $\mathfrak{f}\mathfrak{f}'\mathfrak{p}$ et congru à 1 modulo $\mathfrak{P}$. Ceci entraîne que $p \mid \# C\ell_{\mathfrak{f}\mathfrak{f}'\mathfrak{p}}$ ce qui est exclu par l'hypothèse $p \nmid N\varphi(N)$.

§3. Lien entre le module de congruences et un module d'Iwasawa anticyclotomique

Considérons pour tout caractère de Dirichlet ε de M d'exposant p-primaire et conducteur $\mathfrak{p}^r$, $r \geqslant 0$, la forme parabolique $\theta(\lambda\varepsilon)$. On sait que si $\varepsilon \neq 1$, $\theta(\lambda\varepsilon)$ est propre normalisée primitive dans $S_k(\Gamma_1(Np^r))$, et si $\varepsilon = 1$, $\theta(\lambda) = f_0$ est propre normalisée primitive dans $S_k(\Gamma_1(N))$. Dans le paragraphe 10 de [11], Hida attache à de telles formes des périodes $U_{\lambda\varepsilon}$ et $U^{\lambda\varepsilon}$ différant du carré de Petersson de $\theta(\lambda\varepsilon)$ par un nombre algébrique.

On continue de prendre $u = 1 + Np$ comme générateur de Γ (pro-p-Sylow de Z) et aussi de $1 + \mathfrak{f}\hat{\mathfrak{p}}$. Un caractère ε comme ci-dessus peut également être considéré sur le groupe des classes de rayons modulo $\mathfrak{p}^r$. On peut donc parler de $\varepsilon(u)$. En notant enfin $L(\psi, s)$ la fonction L de Hecke primitive associée à un Grössencharakter ψ de M, on peut énoncer un théorème qui résulte immédiatement du théorème 10.5 de [11].

THÉORÈME 3.1. *La série caractéristique* $\mathbb{H}$ *du module de congruences associé à* (λ, ι) *satisfait les formules d'interpolation faible suivantes*:
(i) *Si* ε *est non-trivial comme ci-dessus, de conducteur* $\mathfrak{p}^r$, *on a*:

$$\mathbb{H}(\varepsilon(u)u^k - 1) \sim p^{2r-1} \cdot \frac{L(\lambda\lambda^{[\varrho]}\varepsilon\, \varepsilon^{[\varrho]}, k)}{\pi^k (U_{\lambda\varepsilon} U^{\lambda\varepsilon})^{1/2}}$$

(ii) *Si* ε *est trivial*,

$$\mathbb{H}(u^k - 1) \sim \frac{L(\lambda\lambda^{[\varrho]}, k)}{\pi^k (U_\lambda U^\lambda)^{1/2}}$$

où le tilde signifie "diffère par une unité $\mathfrak{P}$*-adique dans* $\mathbb{C}_p$".

Commentaire. On voit donc que la série $\mathbb{H}$ est une fonction L p-adique "faible" (au sens que les formules ci-dessus n'égalent que les valuations p-adiques des deux membres). J'espère dans un prochain article préciser le lien de $\mathbb{H}$ avec la spécialisation à la variable anticyclotomique de la fonction L p-adique à deux variables de Katz–Yager lorsque le Grössencharakter λ est puissance $\nu^{\text{ième}}$ du Grössencharakter d'une courbe elliptique à multiplication complexe par M et définie sur M.

On va maintenant introduire le module d'Iwasawa galoisien dont la série caractéristique est reliée à $\mathbb{H}$.

Pour tout idéal entier $\mathfrak{a}$ de M, on note $M_\mathfrak{a}$ le corps de classes de rayons de conducteur $\mathfrak{a}$. On abrège $F = M_{N\mathfrak{f}\cdot p}$. Soit F_∞^-, resp. F_∞^+, la $\mathbb{Z}_p$-extension anticyclotomique (resp. cyclotomique) de F. Soit $\tilde{F}_\infty = F_\infty^+ \cdot F_\infty^-$. Pour tout entier $r \geqslant 1$, on note F_r^+, F_r^-, $\tilde{F}_r$ le sous-corps de degré p^r sur F de F_∞^+, resp. p^r de F_∞^-, resp. p^{2r} de $\tilde{F}_\infty$. Soit F_∞ la $\mathbb{Z}_p$-extension de F non-ramifiée hors de $\mathfrak{p}$ et contenue dans $\tilde{F}_\infty$. On note F_r le sous-corps de degré p^r sur F de F_∞. Soit enfin $\mathcal{N}$ la pro-p-extension abélienne maximale non-ramifiée hors de $\mathfrak{p}$ de F_∞^-. Notons

$$\Gamma^- = \mathrm{Gal}(F_\infty^-/F), \quad \Gamma^+ = \mathrm{Gal}(F_\infty^+/F), \quad \tilde{\Gamma} = \mathrm{Gal}(\tilde{F}_\infty/F).$$

On a $\tilde{\Gamma} = \Gamma^+ \times \Gamma^-$. Soit $X = \mathrm{Gal}(\mathcal{N}/F_\infty^-)$.

Remarquons que grâce à l'hypothèse $p \nmid N\varphi(N)h$, la loi de réciprocité d'Artin fournit un isomorphisme:

$$C\ell_{\mathfrak{f}\mathfrak{p}^\infty} \xrightarrow{\sim} \mathrm{Gal}(F_\infty/M)$$

et que l'ordre du groupe $\Delta = \mathrm{Gal}(F/M)$ est premier à p. Si l'on pose $\mathscr{G} = \mathrm{Gal}(F_\infty/F)$ on peut compléter l'isomorphisme ci-dessus en le diagramme commutatif:

$$\begin{array}{ccc} C\ell_{\mathfrak{f}\mathfrak{p}^\infty} & \xrightarrow{\sim} & \mathrm{Gal}(F_\infty/M) \\ \| & & \| \\ C\ell_{\mathfrak{f}\mathfrak{p}} \times (1 + \mathfrak{f}\hat{\mathfrak{p}}) & \xrightarrow{\sim} & \Delta \times \mathscr{G} \end{array} \tag{3.1}$$

Ceci permet de considérer $\hat{\lambda}$ comme un caractère de Δ. Posons $\hat{\lambda}^\varrho(\sigma) = \hat{\lambda}(\varrho\sigma\varrho)$ et $\kappa = \hat{\lambda}/\hat{\lambda}^\varrho \colon \Delta \to \mathcal{O}_K^\times$. On note $X^{(\kappa)}$ le sous-groupe de $X \otimes_{\mathbb{Z}_p} \mathcal{O}_K$ constitué des éléments sur lesquels Δ opère par κ.

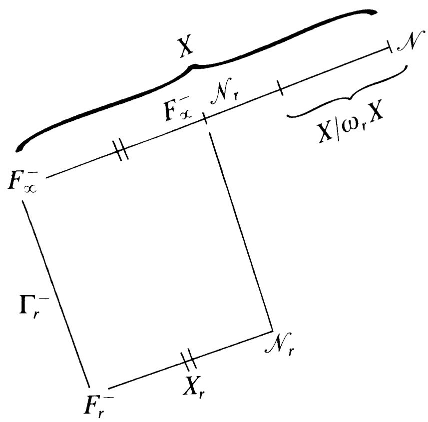
Proposition 3.2 (B. Perrin-Riou [17]). *Le $\mathcal{O}_K[[\Gamma^-]]$-module $X^{(\kappa)}$ et de type fini et de torsion.*

Démonstration. Soient $\mathscr{N}_r$, resp. X_r les analogues de $\mathscr{N}$ et X pour les corps F_r^-, et Y_r le groupe de Galois de la p-extension abélienne maximale non ramifiée de F_r^-, $r = 1, 2, \ldots$. Soit $U_r = U_r$, le groupe des unités semi-locales en $\mathfrak{p}$ de F_r^- (on peut voir en fait que $\mathfrak{p}$ est totalement ramifié dans F_r^-/F, donc le nombre de places au-dessus de $\mathfrak{p}$ est constant pour tout $r \geqslant 1$). Soit E_r le groupe des unités globales de F_r^-. La théorie du corps de classes global nous procure une suite exacte Δ-équivariante:

$$0 \to (U_r/\bar{E}_r)_p \to X_r \to Y_r \to 0$$

l'indice p signifiant qu'on prend le pro-p-Sylow du groupe qu'il affecte. La théorème du Brumer nous apprend que le rang sur $\mathbb{Z}_p$ de $\bar{E}_r$ vaut $[F_r^- \colon M] + 1$. En outre, on sait que le module galoisien $U_r \otimes \mathbb{Q}_p$ est isomorphe à $\mathbb{Q}_p[\mathrm{Gal}(F_r^-/M)]$ et on tire aisément du théorème de Dirichlet sur les unités que $E_r \otimes \mathbb{Q}_p$ est isomorphe à la représentation d'augmentation de $\mathrm{Gal}(F_r^-/M)$. On en tire que $(U_r/\bar{E}_r)_p \otimes \mathbb{Q}_p$ est le module galoisien $\mathbb{Q}_p$ avec action triviale. Soit κ le caractère de Δ défini précédemment; comme $\kappa \neq 1$, on tire des considérations précédentes que $X_r^{(\kappa)}$ est fini pour chaque $r \geqslant 1$.

Montrons alors que pour $\omega_r(T) = (1 + T)^{p^{r-1}} - 1$ on a: $X/\omega_r X \simeq X_r$ (par un isomorphisme Δ-équivariant) ce qui achèvera de montrer que $X^{(\kappa)}$ est de type fini et de torsion (cf. [14]). Soit $G_r = \mathrm{Gal}(\mathscr{N}/F_r^-)$, et soit I_r le sous-groupe d'inertie dans G_r en une place v de $\mathscr{N}$ au-dessus de $\mathfrak{p}^\varrho$. La



restriction $G_r \to \Gamma_r^-$ induit un isomorphisme $I_r \xrightarrow{\sim} \Gamma_r^-$ car la ramification en p^ϱ est totale. On en déduit que G_r est produit semi-direct de X et I_r; il en résulte que $I_r \cdot X/\omega_r X$ s'identifie au plus grand quotient abélien de G_r. Or, la partie abélienne sur F_r^- de $\mathcal{N}/F_r^-$ est égale à $F_\infty^- \cdot \mathcal{N}_r$ (toujours grâce à la ramification totale en $\mathfrak{p}^\varrho$ dans F_∞^-/F_r^-). On conclut donc que la restriction $X/\omega_r X \to X_r$ est un isomorphisme (évidemment Galois-équivariant). Ceci achève la démonstration de la proposition 3.2.

On fixe alors un générateur topologique de Γ^- de la façon suivante. Soit γ l'élément de $\mathcal{G}$ image de $u = 1 + Np \in 1 + \mathfrak{f}\hat{\mathfrak{p}}$ dans le diagramme (3.1). C'est un générateur topologique de $\mathcal{G}$.

$$\text{Soit } \tau_0 \text{ l'unique élément de } \tilde{\Gamma} \text{ tel que } \tau_0^\varrho = \tau_0^{-1} \text{ et } \tau_0|F_\infty = \gamma^{1/2}. \tag{3.2}$$

On choisit $\tau_0|F_\infty^-$ pour générateur topologique de Γ^- et on fixe ainsi un isomorphisme:

$$\mathcal{O}_K[[\Gamma^-]] \to \Lambda_K$$

$$\tau_0|F_\infty^- \mapsto 1 + T.$$

Une fois cette identification posée, la proposition 3.2 nous permet de considérer une série caractéristique $\mathbb{F} \in \Lambda_K$ du module $X^{(\kappa)}$. Le théorème principal s'énonce alors:

THÉORÈME 3.3. *La série* $\mathbb{H}$ *divise* $\mathbb{F}(u^{-1}(1 + T) - 1)$ *dans* Λ_K.

Le reste de cet article est consacré à la démonstration de ce théorème.

Enonçons-en un corollaire.

Soit N_0 l'extension abélienne d'exposant p non-ramifiée hors de F. Soit $X_0 = \mathrm{Gal}(N_0/F)$. Rappelons que le nombre $H(\lambda) = L(\lambda\lambda^{\varrho}, k)/[\pi^k(U_\lambda U^\lambda)^{1/2}]$ est entier en $\mathfrak{P}|\mathfrak{p}$ si $p \nmid 6N\varphi(N)h$, $p > v + 1$ et p est décomposé en $\mathfrak{p}$ et $\mathfrak{p}^{\varrho}$ dans M. De plus Hida mentionne comme corollaire de son théorème 0.1 dans [8] le:

Corollaire 3.4. *Si* $\mathfrak{P}|H(\lambda)$, *on a* $X_0^{(\kappa)} \neq 0$.

On peut déduire très facilement ce corollaire des théorèmes 3.3 et 3.1: $\mathfrak{P}|H(\lambda)$ il résulte du théorème 3.1 que $\mathbb{H}$ n'est pas une unité de Λ_K, donc par le théorème 3.3, $\mathbb{F}$ n'est pas une unité donc $X^{(\kappa)} \neq 0$. Or, si $\mathfrak{M}$ désigne l'idéal maximal de Λ_K, on voit tout de suite que

$$X_0^{(\kappa)} = X^{(\kappa)}/\mathfrak{M} \cdot X^{(\kappa)}.$$

Par conséquent, le lemme de Nakayama nous assure que $X_0^{(\kappa)} \neq 0$.

§4. Construction de la représentation

On utilise les notations des paragraphes 1 et 2 concernant le module de congruences de la composante à multiplication complexe $\mathscr{K}$ ($\simeq \mathscr{L}_K$) définie dans la proposition 2.1 (notation (2.3)). On introduit les notations essentielles pour la suite:

$$\begin{aligned} R_1 &= \mathrm{Im}\,(R \xrightarrow{pr_1} \mathscr{K}), \quad & \mathfrak{c}_1 &= \mathrm{Ker}\,(R \xrightarrow{pr_2} \mathscr{B}) \\ R_2 &= \mathrm{Im}\,(R \xrightarrow{pr_2} \mathscr{B}), \quad & \mathfrak{c}_2 &= \mathrm{Ker}\,(R \xrightarrow{pr_1} \mathscr{K}). \end{aligned} \tag{4.1}$$

Rappelons que $pr_1 = \mathrm{X}$ et $R_1 = \Lambda_K$.

Lemme 4.1

(i) *L'idéal* $\mathfrak{c} = \mathfrak{c}_1 \oplus \mathfrak{c}_2$ *est le conducteur de l'ordre* $\tilde{R} = R_1 \oplus R_2$ *dans* R. *On a des isomorphismes induits par les inclusions* $R_1 \xrightarrow{i_1} \tilde{R} \xleftarrow{i_2} R_2$ *et les projections* $R_1 \xleftarrow{pr_1} R \xrightarrow{pr_2} R_2$:

$$R/\mathfrak{c} \xrightarrow[\sim]{pr_1} R_1/\mathfrak{c}_1 \xrightarrow[\sim]{i_1} R/\tilde{R} \xleftarrow[\sim]{i_2} R_2/\mathfrak{c}_2 \xleftarrow[\sim]{pr_2} R/\mathfrak{c}$$

(ii) R_2 *est une* Λ_K*-algèbre locale finie et plate. L'idéal* $\mathfrak{c}_2$ *de* R_2 *est au-dessus de* $\mathbb{H}\Lambda_K$ *dans le morphisme structural* $\Lambda_K \to R_2$.

Démonstration. (i) L'ensemble $\mathfrak{c}$ est simultanément un idéal des anneaux R et $\tilde{R}$. Il suffit de voir qu'il est maximal avec cette propriété. Soit $\mathfrak{a}$ un idéal de R qui est idéal de $\tilde{R}$. Soit e_i l'élément unité de R_i, $e_i \cdot \mathfrak{a} \subset \mathfrak{a} \cap R_i \subset \mathfrak{c}_i$, donc $\mathfrak{a} = e_1\mathfrak{a} \oplus e_2\mathfrak{a} \subset \mathfrak{c}$. Les isomorphismes de l'énoncé sont évidents.

(ii) Comme R_2 est l'image de R par pr_2, c'est une Λ_K-algèbre locale finie. Sa platitude utilise le théorème 2.2 disant que $R \simeq \mathrm{Hom}_{\Lambda_K}(R, \Lambda_K)$ par un isomorphisme R-linéaire (cf. [10] proposition 3.9): On part de la suite exacte de Λ_K-module

$$0 \to \mathfrak{c}_2 \to R \to \Lambda_K = R_1 \to 0$$

qu'on dualise en:

$$\begin{tikzcd}
0 \arrow[r] & \Lambda_K \arrow[r] & \mathrm{Hom}_{\Lambda_K}(R, \Lambda_K) \arrow[r] & \mathrm{Hom}_{\Lambda_K}(\mathfrak{c}_2, \Lambda_K) \arrow[r] & 0 \\
0 \arrow[r] & \mathscr{X} \arrow[r] \arrow[u] & \mathrm{R} \arrow[u, "d"'] & &
\end{tikzcd}$$

et

$$\mathscr{X} = \{r \in R, d(r) \cdot \mathfrak{c}_2 = 0\} = \{r \in R; r \cdot \mathfrak{c}_2 = 0\} = \mathfrak{c}_1.$$

Donc $\mathrm{Hom}_{\Lambda_K}(\mathfrak{c}_2, \Lambda_K) \xrightarrow{\sim} R/\mathfrak{c}_1 = R_2$, l'isomorphisme étant même R_2-linéaire. Comme $\mathfrak{c}_2$ est libre sur Λ_K, son dual linéaire aussi: R_2 est Λ_K-libre.

D'autre part, l'isomorphisme (de Λ_K-modules, *pas* d'algèbres):

$$R_1/\mathfrak{c}_1 \xrightarrow{\sim} R_2/\mathfrak{c}_2$$

s'identifie à $-\sigma$, où σ est le morphisme induit par réduction du morphisme structural $\Lambda_K \to R_2$. Il en résulte que $\mathfrak{c}_2$ est au-dessus de $\mathbb{H}\Lambda_K$.

Soit $X_r = X_1(Np^r)/\mathbb{Q}$ la courbe projective lisse de corps des fonctions égal à la partie fixe du corps des fonctions $\Gamma_1(Np^r)$-modulaires sous l'action de $\mathrm{Aut}(\mathbb{C})$ opérant sur le q-développement à l'infini. Cette courbe est géométriquement connexe. On note φ l'application holomorphe canonique du demi-plan de Poincaré $\mathfrak{h}$ vers $X_r(\mathbb{C})$. Soit $J_r = \mathrm{Pic}^0(X_r/\mathbb{Q})$ la jacobienne de X_r. On rappelle que le groupe $Z_r = (\mathbb{Z}/Np^r\mathbb{Z})^x/\{\pm 1\}$ opère fidèlement par automorphismes $\mathbb{Q}$-rationnels sur X_r. On note $a \mapsto \langle a \rangle_2$ cette action ("diamant de poids 2": cette appellation sera justifiée plus bas); Elle est caractérisée par la formule suivante: pour $a \in Z_r$ et $\sigma_a \in \Gamma_0(Np^r)$ telle que $\sigma_a \equiv \begin{pmatrix} a^{-1} & \\ & a \end{pmatrix}$ mod. Np^r on a pour tout $z \in \mathfrak{h}$

$$\langle a \rangle_2 \varphi(z) = \varphi(\sigma_a z).$$

On peut également définir pour chaque nombre premier ℓ une correspondance de Hecke $T(\ell)$ sur X_r rationnelle sur $\mathbb{Q}$ caractérisée par les formules:

$$T(\ell)\varphi(z) = \begin{cases} \sum_{i=0}^{\ell-1} \varphi\left(\dfrac{z+i}{\ell}\right) + \langle \ell \rangle_2 \varphi(\ell z) & \text{si } \ell \nmid Np \\ \sum_{i=0}^{\ell-1} \varphi\left(\dfrac{z+i}{\ell}\right) & \text{si } \ell \mid Np. \end{cases}$$

Grâce à la proposition 7.1 de [22] on peut noter, en accord avec le lemme 1.1, $h_{2,r}(\mathbb{Z})$ la $\mathbb{Z}$-algèbre d'endomorphismes de J_r engendrée par les correspondances de Hecke et les diamants de poids 2 opérant sur J_r par fonctorialité contravariante de Pic^0. Remarquons que sur l'espace tangent $S_2(\Gamma_1(Np^r))$ de J_r à l'origine, l'automorphisme $\langle a \rangle_2$ opère par $f \mapsto f|_2\sigma_a$. On note encore $h_{2,r} = h_{2,r}(\mathbb{Z}) \otimes \mathcal{O}_K$.

Considérons alors le groupe p-divisible $J_r[p^\infty]/\mathbb{Q}$. On munit le groupe de ses points algébriques d'une structure de $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module de la façon suivante.* Considérons le morphisme:

$$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_{Np^r})^+/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/Np^r\mathbb{Z})^\times/\{\pm 1\} \to h_{2,r}$$

composé de la restriction au sous-corps réel maximal de $\mathbb{Q}(\zeta_{Np^r})$ suivie de l'isomorphisme déduit du caractère d'action sur le groupe des racines $(Np^r)^{\text{ièmes}}$ de l'unité, suivi enfin par la représentation "diamant de poids 2". On note ce composé $\sigma \mapsto \langle \sigma \rangle_2$. On définit alors pour $\sigma \in G_{\mathbb{Q}}$, $P \in J_r[p^\infty](\bar{\mathbb{Q}})$:

$$\sigma_{\mathrm{Pic}} P = \langle \sigma \rangle_2 P^\sigma \tag{4.2}$$

où P^σ est l'action habituelle de $G_{\mathbb{Q}}$ sur les points algébriques d'une variété définie sur $\mathbb{Q}$.

Nota. On verra l'utilité du choix de cette action lorsqu'on écrira les relations d'Eichler–Shimura faisant intervenir les opérateurs de Hecke agissant de façon contravariante sur la jacobienne.

---

* Ce n'est pas l'action naturelle.

Il est clair que le groupe p-divisible

$$\mathcal{O}_K \otimes_{\mathbb{Z}_p} J_r[p^\infty](\bar{\mathbb{Q}}) \tag{4.3}$$

est un $h^0_{2,r}$-module et un $G_{\mathbb{Q}}$-module et que les deux actions commutent. Soit e_R l'élément unité de la composante locale R de h^0. Grâce à 2) du théorème 1.8, on peut appliquer e_R au groupe (4.3) et on définit ainsi un R_r-module et un $G_{\mathbb{Q}}$-module:

$$J_r(R) \quad = \quad e_R(\mathcal{O}_K \otimes_{\mathbb{Z}_p} J_r[p^\infty](\bar{\mathbb{Q}})).$$

Pour $r' \geqslant r$, on a un revêtement évident défini sur $\mathbb{Q}$: $X_{r'} \to X_r$ provenant de l'inclusion $\Gamma_1(Np^{r'}) \subset \Gamma_1(Np^r)$. Ceci donne un morphisme à noyau fini $J_r \to J_{r'}$ défini sur $\mathbb{Q}$ compatible avec les actions de $h_{2,r}$ et $h_{2,r'}$. Posons $J(R) = \varinjlim_r J_r(R)$. C'est un $G_{\mathbb{Q}}$-module et un R-module.

Hida a démontré dans [11], théorème 3.1, que:

THÉORÈME 4.2. *Les morphismes R-linéaires $J_r(R) \to J_{r'}(R)$ $r \leqslant r'$ sont injectifs et pour $\omega_{2,r} = (1 + T)^{p^{r-1}} - u^{2p^{r-1}} \in \Lambda_K \subset R$, on a*:

$$J(R)[\omega_{2,r}] \quad = \quad J_r(R).$$

Pour tout R-module at $G_{\mathbb{Q}}$-module $\mathcal{M}$, on munit son dual de Pontryagin $\mathcal{M}^* = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{M}; \mathbb{Q}_p/\mathbb{Z}_p)$ des structures de R-module et $G_{\mathbb{Q}}$-module définies de la manière suivante: si $x^* \in \mathcal{M}^*$, $r \in R$, $\sigma \in G_{\mathbb{Q}}$, rx^* et σx^* sont définis par les égalités:

$$\forall x \in \mathcal{M}, \langle x, rx^*\rangle \quad = \quad \langle rx, x^*\rangle, \langle \sigma x, \sigma x^*\rangle \quad = \quad \langle x, x^*\rangle.$$

Alors, grâce au théorème 2.2 ci-dessus et le théorème 9.4 de [11], on sait que le dual de Pontryagin de $J(R)$ est R-libre de rang 2:

$$J(R)^* \simeq R^2. \tag{4.4}$$

En particulier, $J(R)^*$ est Λ_K-libre donc $J(R)$ est Λ_K-divisible; ce qui donne un sens aux symboles $e_i \cdot J(R)$. En utilisant les formules d'orthogonalité en dualité de Pontryagin, on voit de plus que:

$$\begin{cases} e_1 \cdot J(R) \quad = \quad J(R)[\mathfrak{c}_2] \\ e_2 \cdot J(R) \quad = \quad J(R)[\mathfrak{c}_1]. \end{cases} \tag{4.5}$$

De même, on a les égalités de groupes p-divisibles:

$$\begin{cases} e_1 \cdot J_r(R) = J_r(R)[\mathfrak{c}_2] \\ e_2 \cdot J_r(R) = J_r(R)[\mathfrak{c}_1]. \end{cases} \tag{4.5.bis}$$

Explication. Il suffit de prendre la $\omega_{2,r}$-torsion de (4.5) et d'utiliser (4.4) pour obtenir (4.5.bis). On pose alors la

Notation 4.3.

$$A = e_1 \cdot J(R), \quad B = e_2 \cdot J(R)$$

$$A_r = e_1 \cdot J_r(R), \quad B_r = e_2 \cdot J_r(R).$$

On remarque que $A + B = J(R)$ et de même $A_r + B_r = J_r(R)$. De plus, il est clair que les modules A, B, A_r, B_r sont des $G_{\mathbb{Q}}$ et des R-modules. En fait, R opère sur A à travers $R \xrightarrow{pr_1} R_1$ et sur B à travers $R \xrightarrow{pr_2} R_2$. Si l'on note $\Lambda_r = \Lambda_K/\omega_{2,r}$, Λ_K, on voit de même que R opère sur A_r par $R \xrightarrow{pr_1 \bmod . \omega_{2,r}} R_1 \otimes \Lambda_r$ et sur B_r par $R \xrightarrow{pr_2 \bmod . \omega_{2,r}} R_2 \otimes \Lambda_r$. Rappelons que nous notons C le module de congruences défini au paragraphe 1 et posons $C_r = C \otimes \Lambda_r$.

Proposition 4.4. *On a des isomorphismes de R-modules*:

$$A^* \simeq \Lambda_K \oplus \Lambda_K \qquad A_r^* \simeq A^* \otimes \Lambda_r$$

$$B^* \simeq R_2 \oplus R_2 \qquad B_r^* \simeq B^* \otimes \Lambda_r$$

$$(A \cap B)^* \simeq C \oplus C \qquad (A_r \cap B_r)^* \simeq C_r \oplus C_r.$$

En particulier les duaux de Pontryagin de A et B sont Λ_K-libres donc A et B sont Λ_K-divisibles. De plus $A = \varinjlim_r A_r$, $B = \varinjlim_r B_r$, $A_r = A[\omega_{2,r}]$, $B_r = B[\omega_{2,r}]$.

Démonstration. On part de l'accouplement parfait de dualité de Pontryagin

$$J(R) \times R^2 \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Les formules d'orthogonalité en dualité de Pontryagin donnent $A^{\perp} = \mathfrak{c}_2 \oplus \mathfrak{c}_2$. Donc $A^* \simeq R \oplus R/\mathfrak{c}_2 \oplus \mathfrak{c}_2 = \Lambda_K \oplus \Lambda_K$. De même pour B. Enfin, on a:

$$(A \cap B)^{\perp} = A^{\perp} + B^{\perp} = \mathfrak{c} \oplus \mathfrak{c} \quad \text{où} \quad \mathfrak{c} = \mathfrak{c}_1 \oplus \mathfrak{c}_2$$

est le conducteur de l'ordre $\tilde{R}$ dans R comme dans le lemme 4.1. Donc le dual de $A \cap B$ s'identifie à $R/\mathfrak{c} \oplus R/\mathfrak{c} = C \oplus C$.

Les assertions analogues au niveau Np^r résultent des précédentes en prenant le quotient par $\omega_{2,r}$. De même pour les formules $A_r = A[\omega_{2,r}]$, $B_r = B[\omega_{2,r}]$.

COROLLAIRE 4.5. *On a* $A \cap B = A[\mathbb{H}] = B[\mathfrak{c}_2]$ *et* $A_r \cap B_r = A_r[\mathbb{H} \bmod. \omega_{2,r}] = B_r[\mathfrak{c}_2]$.

Démonstration du corollaire. Il suffit de calculer les duaux de Pontryagin dans les inclusions évidentes

$$A[\mathbb{H}] \supset A \cap B \subset B[\mathfrak{c}_2]$$

pour obtenir des égalités; idem pour $A_r \cap B_r$.

L'intérêt du corollaire 4.4 est d'égaler des morceaux des groupes Λ_K-divisibles A et B, alors que ces groupes sont très différents: A est de "type multiplication complexe par M" et B "de type sans multiplication complexe par M", ceci au sens vague de la proposition 2.4, mais aussi au sens plus précis de la proposition suivante.

Introduisons le caractère Φ: $G_M \to \Lambda_K^{\times}$, composé de la restriction au corps des rayons mod. $N\mathfrak{f} \cdot \mathfrak{p}^{\infty}$, suivi de l'isomorphisme inverse de la loi de réciprocité d'Artin, suivi de η:

$$G_M \xrightarrow{\text{Res}} \operatorname{Gal}(M_{N\mathfrak{f}\cdot\mathfrak{p}^{\infty}}/M) \xrightarrow{\sim} C\ell_{\mathfrak{f}\mathfrak{p}^{\infty}} \xrightarrow{\eta} \Lambda_K^{\times}.$$

REMARQUE 4.6. Si $\mathfrak{M}$ est l'idéal maximal de Λ_K, $\Phi \bmod. \mathfrak{M} = \tilde{\lambda}$ et en particulier, $\Phi \not\equiv \Phi^{\varrho} \bmod. \mathfrak{M}$ car $\tilde{\lambda}$ est ramifié en $\mathfrak{p}$ et $\tilde{\lambda}^{\varrho}$ ne l'est pas. Soit $\Lambda_K(\Phi)$ le Λ_K-module libre de rang 1 sur lequel G_M opère par le caractère Φ, et soit $V = \operatorname{Ind}_{\mathbb{Q}}^{M} \Lambda_K(\Phi)$ le $G_{\mathbb{Q}}$-module induit de M à $\mathbb{Q}$ par $\Lambda_K(\Phi)$ i.e., $V = \mathcal{O}_K[G_{\mathbb{Q}}] \otimes_{\mathcal{O}_K[G_M]} \Lambda_K(\Phi)$.

Soit V' le $G_{\mathbb{Q}}$-module contragrédient de V.

PROPOSITION 4.7

(i) *On a un isomorphisme de Λ_K et $G_{\mathbb{Q}}$-modules*:

$$A^* \simeq V'.$$

En particulier, le G_M-module A se décompose en somme de deux G_M-modules $A = X \oplus Y$, où G_M opère sur X par Φ et sur $\tilde{Y}$ par Φ^ϱ, et X et Y ont pour dual de Pontryagin le Λ_K-module C.

(ii) *Le module B^* ne contient aucun vecteur non-nul propre pour l'action de G_M.*

Démonstration. (i) On commence par montrer que les polynômes caractéristiques coïncident. Remarquons d'abord que d'après le théorème d'Igusa assurant que J_r a bonne réduction sur $\mathbb{Q}$ hors de Np, et le critère de Néron–Ogg–Shafarevitch, la représentation de $G_{\mathbb{Q}}$ sur A^* est non-ramifiée hors de Np. Soit donc $\ell \nmid Np$ et Frob_ℓ la classe de conjugaison de Frobenius en ℓ. Soit $r \geqslant 1$; les relations d'Eichler–Shimura reliant l'action naturelle de $G_{\mathbb{Q}}$ sur A_r aux correspondances de Hecke vues comme endomorphismes de J_r par fonctorialité covariante ([22] théorème 7.9) permettent de déduire que $\mathrm{Frob}_{\ell,\mathrm{Pic}}$ agissant sur $J_r[p^\infty](\bar{\mathbb{Q}})$ est annulé par le polynôme $X^2 - T(\ell)X + \ell\langle\ell\rangle_{2,r}$, les opérateurs de Hecke agissant sur J_r par fonctorialité contravariante comme convenu au début du paragraphe. Sur A_r, on voit donc que $\mathrm{Frob}_{\ell,\mathrm{Pic}}$ est annulé par $(X - \eta(\mathscr{L}))(X - \eta(\mathscr{L}^\varrho))$ mod. $\omega_{2,r}$ si ℓ est décomposé en $\mathscr{L}$ et $\mathscr{L}^\varrho$ dans M, et par $X^2 + \eta((\ell))^2$ mod. $\omega_{2,r}$ si ℓ est inerte dans M. Ceci est vrai pour tout entier $r \geqslant 1$. En utilisant alors la définition de l'action de $G_{\mathbb{Q}}$ sur $A^* = \varprojlim_r A_r^*$, ainsi que le théorème de densité de Čebotarev, on conclut que le polynôme caractéristique de σ_{Pic} sur A^* est égal à celui de σ agissant sur V'. On va en déduire l'isomorphisme souhaité. Tout d'abord, comme $\Phi \neq \Phi^\varrho$ et même $\Phi \not\equiv \Phi^\varrho$ mod. $\mathfrak{M}$, $\mathfrak{M}$ désignant l'idéal maximal de Λ_K, on voit que V', est irreductible (i.e., n'a pas de vecteur non-nul propre pour l'action de $G_{\mathbb{Q}}$) donc que $A^* \otimes \mathscr{L}_K$ et $V' \otimes \mathscr{L}_K$ sont isomorphes puisqu'elles ont même trace. On peut donc trouver un isomorphisme d'entrelacement Λ_K-linéaire, fournissant une inclusion $A^* \to V'$. Comme $\Phi \not\equiv \Phi^\varrho$ mod. $\mathfrak{M}$, pour tout élément irréductible P de Λ_K, $V'/P \cdot V'$ n'a pas de vecteurs propres non nuls pour $G_{\mathbb{Q}}$. Comme A^* est un sous-$G_{\mathbb{Q}}$-module de V' on voit en localisant en $P\Lambda_K$, de hauteur 1, que $A_P^* = P^{v_P} V_P'$ (car Λ_P est de valuation discrète). Or, comme A^* est libre sur Λ_K, $A^* = \bigcap_{ht(P)=1} A_P^*$, donc $A^* = f \cdot V'$ pour un $f \in \Lambda_K$, donc $A^* \simeq V'$, comme $\Lambda_K G_{\mathbb{Q}}$-modules.

(ii) Supposons par l'absurde que B^* contienne un vecteur non-nul x^* propre pour G_M. On peut supposer que $x^* \notin \omega_{2,1} \cdot B^*$. Soit $x_1^* \in B_1^*$

sa réduction, c'est encore un vecteur non nul propre pour G_M. Du fait que $p \nmid 6N\varphi(N)h$, on voit comme dans la proposition 2.4 que $F_2 = R_2 \otimes \Lambda_1 \otimes K$ est semi-simple, i.e. est produit de corps. Soit e_L l'idempotent correspondant à un facteur L de F_2. On sait que $B_1^* \otimes K \cong F_2 \oplus F_2$ comme modules (lemme 6.4 de [11]) et qu'on a un isomorphisme α $RG_{\mathbb{Q}}$-linéaire: $B_1^* \xrightarrow{\alpha} \mathrm{Hom}_{\mathcal{O}_K}(Ta(B_1), \mathcal{O}_K)$ où $Ta(B_1) = \mathrm{Hom}_{\mathcal{O}_K}(K/\mathcal{O}_K, B_1)$. On peut donc décomposer $G_{\mathbb{Q}}$-linéairement $B_1^* \otimes K = \oplus_L e_L(B_1^* \otimes K)$ où $F_2 = \Pi_L L$, et il existe L tel que $e_L x_1^* \neq 0$. L'image par α de cet élément fournit un sous-espace non-trivial du L-plan $e_L(Ta(B_1) \otimes K)$ stable par G_M. On sait que ce plan est l'espace de la représentation de $G_{\mathbb{Q}}$ associée à la forme modulaire propre pour les opérateurs de Hecke correspondant au caractère e_L: $h_2(\Gamma_1(Np), K) \to L$. Cette forme n'est pas du type $\theta(\lambda')$ pour un Grössencharakter λ' de M de conducteur $\mathfrak{f}'$ tel que $D \cdot \mathbf{N}\mathfrak{f}' = \mathbf{N}$ ou Np comme on l'a vu à la proposition 2.4. Mais ceci contredit le théorème 4.5 de Ribet [19]: l'existence d'une droit G_M-stable dans ce plan requiert l'existence d'un tel Grössencharakter.

On forme alors le G_M et R_2-module:

$$B^{(1)} = B/Y.$$

La structure de ce R_2-module est aisée à déterminer:

$$B^{(1)*} \simeq R_2 \oplus \mathfrak{c}_2.$$

Soit $X^{(1)}$ l'image de X dans $B^{(1)}$. On forme la suite exacte courte de G_M-modules qui définit $Y^{(1)}$:

$$0 \longrightarrow X^{(1)} \longrightarrow B^{(1)}[\mathfrak{c}_2] \xrightarrow{\pi} Y^{(1)} \longrightarrow 0. \tag{4.6}$$

LEMME 4.8
(i) *La suite de R_2-modules* (4.6) *est scindée.*
(ii) *L'action de G_M s'effectue sur $X^{(1)}$ via le caractère Φ et sur $Y^{(1)}$ via le caractère Φ^{ϱ}.*

Démonstration. Notons W, W_1, $\tilde{W}$, $\tilde{W}_1$ les duaux de Pontryagin respectifs de B, $B^{(1)}$, $B[\mathfrak{c}_2]$, $B^{(1)}[\mathfrak{c}_2]$. L'application $B \to B^{(1)}$ induit l'inclusion R_2G_M-linéaire $W_1 \subset W$. On voit aisément par le lemme de Nakayama qu'on peut choisir une base de W relevant une base de $\tilde{W}$ adaptée à la décomposition $\tilde{W} = X^* \oplus Y^*$. L'inclusion $W_1 \subset W$ s'identifie alors à $\mathfrak{c}_2 \oplus R_2 \subset R_2 \oplus R_2$. On peut donc identifier l'application $\tilde{W}_1 \to X^{(1)*}$ avec $C' \oplus C \xrightarrow{pr_2} C$ où $C' = \mathfrak{c}_2/\mathfrak{c}_2^2$. Ceci identifie donc le dual de Pontryagin de $Y^{(1)}$ avec $\ker pr_2$ d'où l'assertion (i).

Pour ce qui est de l'action de G_M sur $X^{(1)}$ on a déjà remarqué qu'elle était donnée par le caractère Φ. Pour l'étude de $Y^{(1)}$, dualisons la suite (4.6) et utilisons le base de W fixée ci-dessus pour former le diagramme commutatif:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y^{(1)*} & \longrightarrow & \tilde{W}_1 & \longrightarrow & X^{(1)*} & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ 0 & \longrightarrow & C' & \longrightarrow & C' \oplus C & \longrightarrow & C & \longrightarrow & 0. \end{array} \tag{4.6.bis}$$

Soit $\mathscr{L}$ un idéal premier de M de degré l'étranger à Np, les relations d'Eichler–Shimura nnous apprennent que $\sigma = \mathrm{Frob}_{\mathscr{L}} \in \mathrm{Aut}(W) = GL_2(R)$ est annulé par le polynôme réciproque de $X^2 - T_\ell X + \ell\langle\ell\rangle_2$. Or, on a:

$$X^2 - T_\ell X + \ell\langle\ell\rangle \equiv (X - \eta(\mathscr{L}))(X - \eta^\varrho(\mathscr{L})) \bmod . \, \mathfrak{c}_2 .$$

Donc, si $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on peut d'une part écrire l'automorphisme de $\tilde{W}_1$ qu'il induit sous la forme $\begin{pmatrix} \tilde{a} & \tilde{b} \\ 0 & \tilde{d} \end{pmatrix}$ et on sait d'autre part que dét $\sigma \equiv \eta^{-1}(\mathscr{L})\eta^{-\varrho}(\mathscr{L})$ mod. $\mathfrak{c}_2$. Comme on a vu plus haut que $\tilde{d} = \eta^{-1}(\mathscr{L})$ mod. $\mathfrak{c}_2$, on voit que $\tilde{a}$ est l'hypothétie de rapport $\eta^{-1}(\mathscr{L})$ sur C'. Par dualité, on obtient (ii). Fixons donc un scindage R_2-linéaire de la suite (4.6) (pour l'instant non spécifié).

Considérons alors l'application (qui dépend de ce scindage):

$$\begin{aligned} a\colon G_M &\to \mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)}) \\ \sigma &\longmapsto pr_{X^{(1)}} \circ \sigma_{\mathrm{Pic}}|_{Y^{(1)}} . \end{aligned} \tag{4.7}$$

REMARQUES

1) C'est l'analogue du coefficient en haut à droite dans la matrice $\pi(\sigma) = \begin{pmatrix} \chi & a \\ 0 & \chi^\varrho \end{pmatrix}$ du théorème 0.1 de Hida [8].
2) Il résulte du lemme 4.9 que $\mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)})$ est R_2-isomorphe au module de différentielles $C' = \mathfrak{c}_2/\mathfrak{c}_2^2$.

On a $a_P(\sigma\sigma') = a_P(\sigma)\Phi^\varrho(\sigma') + \Phi(\sigma)a_P(\sigma')$ pour tout couple (σ, σ') d'éléments de G_M. C'est donc une "binding function" au sens de [3] (73.17). Elle définit par restriction au sous-groupe de G_M fixant tous les corps de rayons mod. $N\mathfrak{f} \cdot p^r$, $r = 1, 2, \ldots$, un homomorphisme de groupes qui lui, ne dépend pas du scindage R_2-linéaire de (4.6) choisi (cf. paragraphe 5 ci-dessous)

$$a\colon G_{\tilde{F}_\infty} \to C' \tag{4.8}$$

où $\tilde{F}_\infty$ est la réunion des corps de rayons modulo $\mathrm{N}\mathfrak{f} \cdot p^r$: $\tilde{F}_r = M_{\mathrm{N}\mathfrak{f} \cdot p^r}$. Il est clair que a_P se factorise à travers le groupe de Galois de la p-extension abélienne maximale de $\tilde{F}_\infty$, et que pour tout σ fixant $\tilde{F}_\infty$ et tout $\tau \in \mathrm{Gal}(\tilde{F}_\infty/M)$, on a:

$$a(\sigma^\tau) = \frac{\Phi(\tau)}{\Phi(\tau^\varrho)} \cdot a(\sigma). \tag{4.9}$$

On va maintenant étudier les propriétés de ramification de a. On va utiliser pour cela les adhérences schématiques de groupes p-divisibles et de schémas en groupes finis définis sur $\mathbb{Q}$ ou sur M, liés à $J_r(R)$, A_r, B_r, $B_r^{(1)}$, X_r, Y_r. Il y a une petite difficulté technique pour les définir due au fait que nous avons étendu les scalaires de $\mathbb{Z}_p$ à $\mathcal{O}_K$ pour définir les objets énumérés ci-dessus, il fait donc s'assurer qu'ils proviennent d'objet "définis sur $\mathbb{Z}_p$" qui, eux, auront un sens géométrique naturel. C'est le but des remarques suivantes. Considérons dans $h^0(Np^\infty, \mathbb{Z}_p)$ l'unique composante locale $\mathbf{R}$ dont l'extension des scalaires à $\mathcal{O}_K$ s'identifie à R. La restriction à $h^0(Np^\infty, \mathbb{Z}_p)$ du caractère X à valeurs dans Λ_K se factorise à travers $\mathbf{R}$. Soit $\Lambda = \mathbb{Z}_p[[T]]$ l'algèbre d'Iwasawa sur $\mathbb{Z}_p$. Remarquons que la Λ-sous-algèbre de Λ_K engendrée par l'image de $\mathbf{R}$ par X est en fait égale à Λ_K. En effet, par définition, elle est égale à $\mathcal{O}'[[T]]$ où $\mathcal{O}'$ est l'ordre de $\mathcal{O}_K$ engendré sur $\mathbb{Z}_p$ par les éléments de $\hat{\lambda}(C\ell_{\mathfrak{f}\mathfrak{p}})$. Cet ordre est maximal: $\mathcal{O}' = \mathcal{O}_K$. Il suffit pour le voir d'adapter la démonstration de la proposition 4.4 de [8]: comme $K/\mathbb{Q}_p$ est non ramifée, elle est galoisienne et il suffit par Nakayama, de voir que si $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ vérifie $\hat{\lambda}(x_1) \equiv \hat{\lambda}(x_1)^\sigma$ modulo $\mathfrak{P}$ pour tout $x_1 \in C\ell_{\mathfrak{f}\mathfrak{p}}$, alors $\sigma = \mathrm{Id}_K$.

On tire de ces congruences que $\hat{\lambda} = \hat{\lambda}^\sigma$ car $p \nmid \# C\ell_{\mathfrak{f}\mathfrak{p}}$. Comme il est clair que K est engendré sur $\mathbb{Q}_p$ par les valeurs de $\hat{\lambda}$, on conclut $\sigma = \mathrm{Id}_K$.

Soit alors $\mathscr{L}$ le corps des fractions de Λ. Le caractère $\mathrm{X}|\mathbf{R}$ définit une décomposition:

$$\mathbf{R} \otimes_\Lambda \mathscr{L} \simeq \mathscr{L}_K \times \boldsymbol{\mathscr{B}} \tag{4.10}$$

où $\boldsymbol{\mathscr{B}}$ est une $\mathscr{L}$-algèbre finie (semi-simple), telle que

$$\boldsymbol{\mathscr{B}} \otimes_{\mathscr{L}} \mathscr{L}_K = \mathscr{B} \times \mathscr{B}'$$

où $\mathscr{B}$ est la $\mathscr{L}_K$-algèbre semi-simple de la proposition 2.3. De même

$$\mathscr{L}_K \otimes_{\mathscr{L}} \mathscr{L}_K = \mathscr{L}_K \times \mathscr{L}_K'$$

et l'extension des scalaires à $\mathscr{L}_K$ de (4.10) induit l'isomorphisme 2.5:

$$R \otimes \mathscr{L}_K \to \mathscr{L}_K \times \mathscr{B}.$$

On définit à partir de 4.10 des objets $\mathbf{R}_i$ et $\mathfrak{c}_i$ analogues à R_i et $\mathfrak{c}_i$ et on a:

$$\left.\begin{aligned} e_R(\mathbf{R}_i \otimes \mathcal{O}_K) &= R_i \\ e_R(\mathfrak{c}_i \otimes \mathcal{O}_K) &= \mathfrak{c}_i \end{aligned}\right. \qquad (i = 1, 2)$$

Notons que les remarques précédentes montrent:

$$\mathbf{R}_1 = \Lambda_K. \tag{4.10.bis}$$

Maintenant, posons:

$$\begin{aligned} J_r(\mathbf{R}) &= e_{\mathbf{R}} J_1(Np^r)[p^\infty] \\ J(\mathbf{R}) &= \varinjlim_r{}' J_r(\mathbf{R}) \\ \mathbf{A} &= J(\mathbf{R})[\mathfrak{c}_2] \\ \mathbf{B} &= J(\mathbf{R})[\mathfrak{c}_1] \\ \mathbf{A}_r &= J_r(\mathbf{R})[\mathfrak{c}_2] \\ \mathbf{B}_r &= J_r(\mathbf{R})[\mathfrak{c}_1]. \end{aligned}$$

On peut appliquer le critère 5.6 de [24] à $\mathbf{R}$ pour montrer qu'il est de Gorenstein comme au théorème 2.2.

Grâce à (4.10.bis), on peut appliquer la proposition 3.9 (ii) de [10] pour obtenir l'analogue de la proposition 4.4. La proposition 4.7 se transpose verbatim pour $\mathbf{A}^*$ et $\mathbf{B}^*$, ce qui permet de définir $\mathbf{X}$ et $\mathbf{Y}$ comme des G_M-modules, comme dans le corollaire 4.8, et on pose enfin:

$$\begin{cases} \mathbf{X}_r = \mathbf{X}[\omega_{2,r}] \\ \mathbf{Y}_r = \mathbf{Y}[\omega_{2,r}] \end{cases}$$

il est clair que $J_r(R)$, A_r, B_r, X_r, Y_r s'obtiennent en appliquant e_R à l'extension des scalaires de $\mathbb{Z}_p$ à $\mathcal{O}_K$ de $J_r(\mathbf{R})$, $\mathbf{A}_r$, $\mathbf{B}_r$, $\mathbf{X}_r$, $\mathbf{Y}_r$, et que les objets soulignés sont naturellement des sous-schémas en groupes de $J_1(Np^r)[p^\infty]$ définis sur $\mathbb{Q}$ ou M. Ce sont donc ces objets que nous allons utiliser sans prendre le soin de les souligner, leur sens étant désormais précisé.

C'est donc dans ce sens qu'il faudra entendre A_r et B_r lorsqu'on en prendra les adhérences schématiques. De même X_r et Y_r sont des sous-schémas en groupes finis définis sur $\mathbb{Q}$: $B_r[\mathfrak{c}_2]$. Il en est de même du groupe p-divisible $B_r^{(1)}$ défini sur M par $B_r^{(1)} = B_r/Y_r$.

D'abord, on traite le cas facile:

Proposition 4.9. *L'homomorphisme a est non-ramifié hors de p.*

Démonstration. En utilisant la notation 4.3 et (4.5.bis), on obtient les relations:

$$\begin{cases} B[\mathfrak{c}_2] = \varinjlim_r B_r[\mathfrak{c}_2]; & B_r[\mathfrak{c}_2] = B[\mathfrak{c}_2, \omega_{2,r}] \\ B^{(1)}[\mathfrak{c}_2] = \varinjlim_r B_r^{(1)}[\mathfrak{c}_2]; & B_r^{(1)}[\mathfrak{c}_2] = B^{(1)}[\mathfrak{c}_2, \omega_{2,r}]. \end{cases} \tag{4.11}$$

Les applications de transition des systèmes inductifs considérés étant naturellement déduites de $J_r(R) \to J_{r'}(R)$ pour $r \leqslant r'$, donc étant $R_2 G_M$-linéaires. Par conséquent, étant donnée une place v de $\tilde{F}_r$, $v \nmid Np$, il suffit de montrer qu'en la place v_r de $\tilde{F}_r$ induite par v, le module $B_r^{(1)}[\mathfrak{c}_2]$ est non ramifié. Or le théorème d'Igusa [12] nous apprend que $J_1(Np^r)$ a bonne réduction sur $\mathbb{Q}$ et v et le sens facile du critère de Néron–Ogg–Shaferevitch ([21]) nous permet de conclure à la non-ramification en v du groupe $\mathscr{C}_K$-divisible B_r, donc de $B_r^{(1)}$ qui lui est isogène. Ceci prouve que a est non ramifié en $v \nmid Np$. Si $v|N$, on utilise crucialement l'hypothèse $(\mathfrak{f}, \mathfrak{f}^{\varrho}) = 1$, qui nous permet de conclure que le Nebentypus ψ de $\theta(\lambda)$ est primitif modulo N. On introduit pour chaque entier $r \geqslant 1$, la sous-variété abélienne $\mathscr{A}_{r,\mathbb{Q}}$ de $J_1(Np^r)$ contenant $J_r(R)$, définie en 1.2 de [24]. Pour $q|N$, notons N_q la partie q-primaire de N. Par le théorème de bonne réduction de Langlands ([15] paragraphe 7 ou de Carayol [27] pour $q = 2$), cette variété a bonne réduction en $v|q$ sur $\mathbb{Q}(\zeta_{N_q})$. Si v est une place de $\tilde{F}_r = M_{N\mathfrak{f}\cdot p^r}$ au-dessus du facteur premier q de $N\mathfrak{f}$, on a $\mathbb{Q}(\zeta_{N_q}) \subset \tilde{F}_r$ $\forall r \geqslant 1$, donc le critère de Néron–Ogg–Shaferevitch montre que l'inertie en v agit trivialement sur $J_r(R)$, donc sur $B_r^{(1)}$; la non-ramification s'ensuit par le passage à la limite de (4.11). Si $v|q|D$, on forme les corps $\tilde{F}'_r = \tilde{F}_r(\zeta_{N_q})$ $r = 1, \ldots$ et on constate comme ci-dessus que pour chaque $r \geqslant 1$ l'inertie en une place v' de $\tilde{F}'_r$ au-dessus de v opère trivialement sur $J_r(R)$. Comme le degré de $\tilde{F}'_r$ sur $\tilde{F}_r$ divise l'entier $\varphi(N_q)$ qui est premier à p par l'hypothèse $p \nmid \varphi(N)$, et comme $C' = \mathfrak{c}_2/\mathfrak{c}_2^2$ est un pro-p-groupe, on voit que l'inertie en v dans $G_{\tilde{F}_r}$ est tuée par a. Q.E.D.

Reste à voir le cas d'une place v de $\tilde{F}_\infty$ au-dessus de $\mathfrak{p}^e$. Soit $\mathcal{O}_r$ l'anneau des entiers de la complétion v-adique de $\tilde{F}_r$. En utilisant le théorème 1.3.1 de [24] on peut, pour chaque entier $r \geqslant 1$ prolonger $B_r[\mathfrak{c}_2]$ (resp. $B_r^{(1)}[\mathfrak{c}_2]$) en un schéma fini et plat sur $\mathcal{O}_r$, en prenant son adhérence schématique dans le groupe p-divisible $J_r(R)/\mathcal{O}_r$ (resp. $(J_r(R)/Y_r)_{\mathcal{O}_r}$ où Y_r désigne le sous-module galoisien $Y_r = Y[\omega_{2,r}]$ de $B_r[\mathfrak{c}_2]$). On peut donc considérer les dévissages connexes-étales correspondants:

$$0 \longrightarrow \mathscr{C}_r/\mathcal{O}_r \longrightarrow B_r[\mathfrak{c}_2]/\mathcal{O}_r \xrightarrow{j} \mathscr{E}_r/\mathcal{O}_r \longrightarrow 0 \tag{4.12}$$

$$0 \longrightarrow \mathscr{C}_r^{(1)}/\mathcal{O}_r \longrightarrow B_r^{(1)}[\mathfrak{c}_2]/\mathcal{O}_r \xrightarrow{j^{(1)}} \mathscr{E}_r^{(1)}/\mathcal{O}_r \longrightarrow 0. \tag{4.13}$$

On omettra l'indice $\mathcal{O}_r$ lorsqu'on veut indiquer qu'on prend les points géométriques de la fibre générique. Les suites (4.12) et (4.13) fournissent des suites exactes sur les points géométriques pour chaque $r \geqslant 1$, et on obtient ainsi deux systèmes inductifs de suites exactes induits par les applications de transitions $J_r(R) \to J_{r+1}(R)$ $r = 1, 2, \ldots$.

Notation. On pose $X_r = X[\omega_{2,r}]$, $Y_r = Y[\omega_{2,r}]$. Ce sont des G_M-sous-modules finis de B_r. Soient X_r^- et Y_r^- les adhérences schématiques de X_r et Y_r dans $B_r[\mathfrak{c}_2]/\mathcal{O}_r$. Soit $D_{r,v}$, resp. D_v, le groupe de décomposition en v dans $G_{\tilde{F}_r}$ resp. $G_{\tilde{F}_\infty}$.

LEMME 4.10. *Les $D_{r,v}$-sous-modules de $B_r[\mathfrak{c}_2]$ X_r et Y_r satisfont: $Y_r = \mathscr{C}_r$, $X_r \xrightarrow{\sim} \mathscr{E}_r$. Par conséquent X_r^- est étale et Y_r^- est connexe.*

Démonstration. La structure sur R_r des composantes connexe C_r et étale E_r de $J_r(R)/\mathcal{O}_r$ est déterminée au théorème 4.4 de [23]. On a:

$$\begin{cases} E_r^* \simeq R_r \\ C_r^* \simeq \operatorname{Hom}(R_r, \mathbb{Z}_p). \end{cases}$$

Comme on sait de plus que R, donc R_r, est de Gorenstein, on a même $C_r^* \simeq R_r$. On va déduire les structures de $\mathscr{E}_r$ et $\mathscr{C}_r$. Rappelons pour cela que $B_r[\mathfrak{c}_2] = J_r(R)[\mathfrak{c}_r]$ où $\mathfrak{c}_r = \mathfrak{c}_1 \oplus \mathfrak{c}_2 \bmod .\ \omega_{2,r}$ est un idéal de $R_r = R \otimes \Lambda_r$ engendré par des isogénies définies sur $\mathbb{Q}$ de $J_r(R)$ (cf. (4.5.bis) et (4.11)). Ces isogénies se prolongent en des endomorphismes de $J_r(R)/\mathcal{O}_r$ par le propriété universelle du modèle de Néron.

On considère alors l'immersion fermée

$$B_r[\mathfrak{c}_2]/\mathcal{O}_r \to J_r(R)/\mathcal{O}_r$$

on en déduit par fonctorialité des composantes connexes et étales des immersions fermées

$$\mathscr{C}_r/\mathcal{O}_r \to C_r/\mathcal{O}_r \quad \text{et} \quad \mathscr{E}_r/\mathcal{O}_r \to E_r/\mathcal{O}_r$$

et par définition des noyaux:

$$\mathscr{C}_r/\mathcal{O}_r \to C_r[\mathfrak{c}_r]/\mathcal{O}_r \quad \text{et} \quad \mathscr{E}_r/\mathcal{O}_r \to E_r[\mathfrak{c}_r]/\mathcal{O}_r.$$

Or, si l'on note $I_{\bar{v}}$ le sous-groupe d'inertie de G_M et une place $\bar{v}|v$ de $\bar{\mathbb{Q}}$ au-dessus de $\mathfrak{p}^{\varrho}$, on peut définir une action de ce groupe sur tout les modules galoisiens $J_r(R)$, C_r, E_r, $B_r[\mathfrak{c}_2]$, $\mathscr{C}_r$, $\mathscr{E}_r$ dite action de "l'inertie géométrique" et définie par exemple dans [8] à la fin de la démonstration de la proposition 5.3. On démontre au corollaire 4.2 de [24] que cette action est triviale sur E_r et est donnée sur C_r par la formule:

pour tout $\sigma \in I_{\bar{v}}$ et tout P de C_r:

$$\sigma_{\mathrm{Pic}} P = \kappa(\sigma)\langle\kappa(\sigma)\rangle_{\mathrm{Pic}} \cdot P$$

où κ: $G_M \to \mathbb{Z}_p^{\times}$ désigne le caractère cyclotomique.

On remarque enfin que l'inclusion $\mathscr{E}_r \to \mathscr{E}_r[\mathfrak{c}_r]$ est équivariante sous I_v toujours par fonctorialité des composantes connexe et étale.

Soit maintenant $\sigma \in I_v$ et $y \in Y_r$, on a:

$$\sigma j(y) = j(y) = j(\sigma y) = \Phi^{\varrho}(\sigma) \cdot j(y).$$

Or, et c'est là intérêt de I_v, il existe $\sigma \in I_v$ tel que $\Phi^{\varrho}(\sigma) \not\equiv 1 \bmod. \mathfrak{M}$ ($\mathfrak{M}$ désignant l'idéal maximal de Λ_K). Par conséquent $j(Y_r) = 0$. De même, la projection de $\mathscr{C}_r$ dans X_r est nulle parce que Φ est non ramifié en $\mathfrak{p}^{\varrho}$, tandis que le caractère $\kappa \cdot \langle\kappa\rangle$ est non trivial (modulo $\mathfrak{M}$) sur I_v. On a donc $\mathscr{C}_r \subset Y_r$. Comme $\mathscr{C}_r = \operatorname{Ker} j$, on conclut $\mathscr{C}_r = Y_r$ et $X_r \xrightarrow{\stackrel{j}{\sim}} \mathscr{E}_r$. En particulier, il en résulte que $\mathscr{C}_r = C_r[\mathfrak{c}_r]$ et $\mathscr{E}_r = E_r[\mathfrak{c}_r]$, et que Y_r^- est connexe et X_r^- est étale.

On peut alors énoncer la proposition donnant la non-ramification de a en v.

PROPOSITION 4.11. *La suite exacte* (4.13) *de $D_{r,v}$-modules est scindée pour chaque $r \geqslant 1$. En fait, $B_r^{(1)}[\mathfrak{c}_2] = \mathscr{C}_r^{(1)} \oplus X_r^{(1)}$; $X_r^{(1)} \xrightarrow{\stackrel{j^{(1)}}{\sim}} \mathscr{E}_r/\mathcal{O}_r$. Les scindages ci-dessus sont compatibles avec les applications $B_r^{(1)}[\mathfrak{c}_2] \to B_{r'}^{(1)}[\mathfrak{c}_2]$ si $r \leqslant r'$, et en posant $\mathscr{C}^{(1)} = \varinjlim_r \mathscr{C}_r^{(1)}$, on a le scindage de D_v-modules*:

$$B^{(1)}[\mathfrak{c}_2] = \mathscr{C}^{(1)} \oplus X^{(1)},$$

et la restriction à $\mathscr{C}^{(1)}$ *de* π *dans* (4.6) *induit un isomorphisme de* D_v*-modules* $\pi\colon \mathscr{C}^{(1)} \xrightarrow{\sim} Y^{(1)}$.

REMARQUE IMPORTANTE. Soit $\mathscr{F}_r$ la complétion v-adique de $\tilde{F}_r$ (i.e., le corps des fractions de $\mathcal{O}_r$). Pour chaque $r \geqslant 1$, la fibre générique $\mathscr{C}_r^{(1)}/\mathscr{F}_r$ du schéma $\mathscr{C}_r^{(1)}/\mathcal{O}_r$ descend canoniquement à la complétion $M_{\mathfrak{p}^\varrho}$ de M en $\mathfrak{p}^\varrho$. De plus pour $r < r'$, on a une inclusion $\mathscr{C}_r^{(1)} \to \mathscr{C}_{r'}^{(1)}$ définie sur $M_{\mathfrak{p}^\varrho}$. Par conséquent le scindage:

$$B^{(1)}[\mathfrak{c}_2] \;=\; \mathscr{C}^{(1)} \oplus X^{(1)}$$

est en fait stable par le sous-groupe de décomposition D en une place $\bar{v}$ de $\bar{M}$ au-dessus de $\mathfrak{p}^\varrho$ dans le groupe de Galois absolu G_M de M.

En effet, comme $B_r^{(1)}[\mathfrak{c}_2]$ est un G_M-module, on voit grâce à la propriété universelle des composantes connexes que pour tout σ de D, il y a un unique isomorphisme de $\mathscr{F}_r$-schémas:

$$\mathscr{C}_r^{(1)^\sigma} \xrightarrow{\sim} \mathscr{C}_r^{(1)}$$

et les conditions de descente relatives à $\mathscr{F}_r/M_{\mathfrak{p}^\varrho}$ sont évidemment satisfaites.

Démonstration. Soit α l'isogénie de groupes p-divisibles définissant $B_r^{(1)}/M$ comme quotient de B_r/M par Y_r. Soit $X_r^{(1)^-}$ l'adhérence schématique de $X_r^{(1)}$ dans $B_r^{(1)}[\mathfrak{c}_2]/\mathcal{O}_r$. L'isogénie α induit un morphisme de schémas finis et plats:

$$\alpha_{\mathcal{O}_r}\colon X_r^- \to X_r^{(1)^-}.$$

Ce morphisme est surjectif car il est surjectif sur les fibres génériques et son noyau est un sous-schéma fermé de X_r^- et de Y_r^- (cette dernière assertion résulte de ce que $\alpha_{\mathcal{O}_r}$ est induite par le morphisme fidèlement plat, de noyau Y_r^-: $J_r(R)/\mathcal{O}_r \to (J_r(R)/Y_r)_{\mathcal{O}_r}$). Ce noyau est connexe et étale, par le lemme 4.10, il est donc nul. Ainsi $X_r^{(1)^-}$ est étale et isomorphe à $\mathscr{E}_r^{(1)}$. Comme le morphisme $\alpha_{\mathcal{O}_r}\colon B_r[\mathfrak{c}_2] \to B_r^{(1)}[\mathfrak{c}_2]/\mathcal{O}_r$ a pour noyau le schéma connexe Y_r^-, on voit que $X_r^{(1)^-}$ est isomorphe à $\mathscr{E}_r^{(1)}$ par $j_r^{(1)}$. Le scindage de (4.13) en résulte. Montrons que la décomposition $B_r^{(1)}[\mathfrak{c}_2] = \mathscr{C}_r^{(1)} \oplus X_r^{(1)}$ est respectée par les morphismes de transition du système inductif de (4.11). D'abord si $r \leqslant r'$, $\mathscr{C}_r^{(1)}$ s'envoie dans $\mathscr{C}_{r'}^{(1)}$ par fonctorialité de la composante connexe. De plus, on voit que $X_r^{(1)}$ s'envoie dans $X_{r'}^{(1)}$. On applique pour cela le lemme 4.8 (ii) et le fait que les morphismes de transition sont G_M-linéaires.

On tire évidemment de la proposition 4.11 que $a(D_v) = 0$ et a fortiori que $a(I_v) = 0$. Ce qui achève de prouver la non-ramification de a en $v|\mathfrak{p}^\varrho$.

Si on rassemble les résultats de non-ramification obtenus, on voit que l'homomorphisme (4.8) se factorise comme suit. Soit $\tilde{\mathcal{N}}$ la pro-p-extension abélienne maximale de $\tilde{F}_\infty$ non ramifiée hors de $\mathfrak{p}$. Notons que chaque place de $\tilde{F}_\infty$ au-dessus de $\mathfrak{p}^\varrho$ est totalement décomposée dans $\tilde{\mathcal{N}}$ car le degré résiduel de $\mathfrak{p}^\varrho$ dans $\tilde{F}_\infty/M$ est divisible par p^∞. Soit $\mathscr{X} = \mathrm{Gal}(\tilde{\mathcal{N}}/\tilde{F}_\infty)$. Notons que $\tilde{\mathcal{N}}$ est galoisien sur M et est abélien sur $\tilde{F}_\infty$ il y a une action naturelle de $\mathrm{Gal}(\tilde{F}_\infty/M) = \tilde{\Gamma} \times \Delta$ sur $\mathscr{X}$. On a montré la

PROPOSITION 4.12. *L'homomorphisme de groupes*

$$a\colon G_{\tilde{F}_\infty} \to C' = \mathfrak{c}_2/\mathfrak{c}_2^2 \tag{4.8}$$

se factorise en un homomorphisme $a_\infty\colon \mathscr{X} \to C'$ *tel que* $\forall x \in G_{\tilde{F}_\infty}$, $\forall \tau \in \mathrm{Gal}(\tilde{F}_\infty/M)$, $a(x^\tau) = (\Phi(\tau)/\Phi^\varrho(\tau)) \cdot a(x)$. *En particulier, avec les notations de* (3.1), *on a*:

$$\begin{cases} \forall x \in \mathscr{X}, \forall \delta \in \Lambda;\ a(x^\delta) = \kappa(\delta) \cdot a(x) \\ \qquad \forall \sigma \in \Gamma^+;\ a(x^\sigma) = a(x) \\ \text{et si } \tau_0 \text{ désigne l'élément de } \Gamma^- \text{ fixé dans (3.2) on a:} \\ \quad a(x^{\tau_0}) = u^{-1} \times (1 + T) \cdot a(x). \end{cases} \tag{4.9}$$

Nous considérons alors $a_\infty \otimes \mathrm{Id}_{\mathcal{O}_K}\colon \mathscr{X} \otimes \mathcal{O}_K \to C'$. Il est clair que ce morphisme $\mathcal{O}_K$-linéaire se factorise à travers $\mathscr{X}^{(\kappa)} = \{x \in \mathscr{X} \otimes \mathcal{O}_K;\ \forall \delta \in \Delta;\ x^\delta = \kappa(\delta) \cdot x\}$. Soit $\mathscr{X}^{(\kappa)}(1)$ le Λ_K-module obtenu en définissant la nouvelle action de $1 + T$ par:

$$(1 + T) \cdot x = u \cdot (1 + T) \cdot x.$$

COROLLAIRE 4.13. $a_\infty \otimes \mathrm{Id}_{\mathcal{O}_K}$ *définit un morphisme* Λ_K*-linéaire de* $\mathscr{X}^{(\kappa)}(1)$ *vers* C'.

Démonstration. Il résulte de la proposition 4.12 que $a(x^{u \cdot \tau_0}) = (1 + T) \cdot a(x)$ pour tout x de $\mathscr{X}$.

L'objet due prochain paragraphe est de montrer que $\mathrm{Im}(a_\infty \otimes \mathrm{Id}_{\mathcal{O}_K}) = C'$.

§5. Surjectivité de l'homomorphisme $a_\infty \otimes \mathrm{Id}_{\mathcal{O}_K}$

Notons encore $\tilde{\mathcal{N}}$ la pro-p-extension abélienne maximale de $\tilde{F}_\infty$ non ramifiée hors de $\mathfrak{p}$ (et donc totalement décomposée en chaque place v de $\tilde{F}_\infty$ au-dessus de $\mathfrak{p}^\varrho$). Posons

$$\mathscr{X} = \mathrm{Gal.}(\tilde{\mathcal{N}}/\tilde{F}_\infty), \quad G = \mathrm{Gal}(\tilde{\mathcal{N}}/M).$$

Il résulte de propositions 4.9 et 4.11 que l'action de G_M sur $B^{(1)}[\mathfrak{c}_2]$ se factorise à travers G.

La suite extracte courte de R_2G-modules:

$$0 \to X^{(1)} \to B^{(1)}[\mathfrak{c}_2] \to Y^{(1)} \to 0 \tag{5.1}$$

donne lieu à l'accouplement de Kummer–Wiles:

$$\begin{aligned} \langle\,,\rangle\colon \mathscr{X} \times Y^{(1)} &\to X^{(1)} \\ (\sigma, P) &\mapsto \sigma\tilde{P} - \tilde{P} \end{aligned} \tag{5.2}$$

où $\tilde{P} \in B^{(1)}[\mathfrak{c}_2]$ est un relèvement de $P \in Y^{(1)}$ arbitraire. Posons $\mathscr{H} = \mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)})$. On sait qu'il y a un isomorphisme de R_2-modules: $\mathscr{H} \cong C'$.

L'accouplement (5.2) induit un morphisme:

$$\begin{aligned} a_\infty\colon \mathscr{X} &\to \mathscr{H} \\ \sigma &\mapsto \langle\sigma, -\rangle. \end{aligned}$$

Ce morphisme coïncide avec celui induit par la restriction d'une fonction a donnée par (4.7) associée à un scindage R_2-linéaire quelconque de (4.6).

Soit

$$Z = \{y \in Y^{(1)}, \langle\sigma, y\rangle = 0, \forall\sigma \in \mathscr{X}\}.$$

On voit que $(\mathrm{Im}\, a_\infty) \otimes_{\mathbb{Z}_p} \mathcal{O}_K$ s'identifie au sous-module $Z^\perp_{\mathscr{H}} = \mathrm{Hom}_{R_2}(Y^{(1)}/Z, X^{(1)})$ de $\mathscr{H}$.

Il faut montrer que $Z = 0$.

Supposons par l'absurde que:

$$Z \neq 0. \tag{5.3}$$

Le R_2-module $Z^{\perp}_{\mathscr{H}}$ est naturellemment isomorphe au dual de Pontryagin de $Y^{(1)}/Z$ i.e., au noyau de la surjection naturelle $Y^{(1)*} \to Z^*$. On fixe désormais une base $\mathscr{B} = (e_1, e_2)$ de $W = B^*$ relevant une base $\bar{\mathscr{B}} = (\bar{e}_1, \bar{e}_2)$ de $\tilde{W} = B[\mathfrak{c}_2]^*$; on a vu dans la démonstration du lemme 4.8 qu'on peut alors identifier $Y^{(1)*}$ avec $C' = \mathfrak{c}_2/\mathfrak{c}_2^2$ et il est évident qu'il existe un idéal de R_2 compris entre $\mathfrak{c}_2^2$ et $\mathfrak{c}_2$ tel que dans cette identification, la suite duale de Pontryagin de

$$0 \to Z \to Y^{(1)} \to Y^{(1)}/Z \to 0$$

s'identifie à:

$$0 \to \mathfrak{a}/\mathfrak{c}_2^2 \to \mathfrak{c}_2/\mathfrak{c}_2^2 \to \mathfrak{c}_2/\mathfrak{a} \to 0.$$

On voit donc que l'inclusion (Im a_∞) $\otimes\ \mathcal{O}_K \subset \mathscr{H}$ s'identifie à l'inclusion $\mathfrak{a}/\mathfrak{c}_2^2 \subset C'$. L'hypothèse (5.3) équivaut donc à $\mathfrak{a} \subsetneqq \mathfrak{c}_2$.

Soit v une place de $\tilde{F}_\infty$ au-dessus de $\mathfrak{p}^\varrho$. On a vu dans la remarque importante qui suit la proposition 4.11, que pour $w\,|\,\mathfrak{p}^\varrho$ dans $\tilde{\mathscr{N}}$, en désignant par D_w un sous-groupe de G de décomposition en w la suite exacte (5.1) de D_w-modules est scindée:

$$B^{(1)}[\mathfrak{c}_2] \;=\; \mathscr{C}_w \oplus X^{(1)}. \tag{5.4}$$

L'homomorphisme π défini en (4.6) fournit un isomorphisme R_2D_w-linéaire $\pi\colon \mathscr{C}_w \xrightarrow{\sim} Y^{(1)}$. On note Z_w le sous-module de $\mathscr{C}_w$ isomorphe à Z par π.

Soit a_w l'application donnée en (4.7) associée au scindage (5.4) et soit b_w le 1-cocycle

$$b_w\colon G \to \mathscr{H}$$

défini par $b_w(\sigma) = a_w(\sigma)/\Phi^\varrho(\sigma)$.

Posons $H_w = \mathscr{X} \cdot D_w$.

LEMME 5.1. *Le groupe $\mathscr{X}$ est distingué dans G. Le groupe H_w est produit semi direct de $\mathscr{X}$ de D_w; de plus H_w est d'indice fini dans G.*

Démonstration. Il suffit de noter que $\mathscr{X} \cap D_w = 1$ par l'hypothèse de totale décomposition de v dans $\tilde{\mathscr{N}}$ et qu'au contraire, l'image de D_w dans $\mathrm{Gal}(\tilde{F}_\infty/M) = \tilde{\Gamma} \times \Delta$ par l'application de restriction est d'indice fini. En effet, on se ramène aisément à montrer que $\mathfrak{p}^\varrho$ est finiement décomposé dans la $\mathbb{Z}_p$-extension de M non-ramifiée hors de $\mathfrak{p}$ (il est totalement ramifié dans la $\mathbb{Z}_p$-extension non ramifiée hors de $\mathfrak{p}^\varrho$ grâce à l'hypothèse $p \nmid h$). Par la théorie du corps de classes global, cela revient à voir que l'idéal $\mathfrak{p}^\varrho$ définit une classe de rayons non triviale dans $Cl_{\mathfrak{f}\mathfrak{p}^r}$ pour chaque entier r assez grand. C'est clair car l'application évidente de l'ensembles des idéaux entiers de M premiers à ϱ^ϱ dans $\varprojlim C\ell_{\mathfrak{f}\mathfrak{p}^r}$ est injective.

Considérons alors $K_w = \ker b_w$. C'est un sous-groupe distingué de G contenant H_w. La suite exacte d'inflation-restriction:

$$0 \to H^1(G/K_w, \mathscr{H}^{K_w}) \to H^1(G, \mathscr{H}) \to H^1(K_w, \mathscr{H})$$

montre que la classe de cohomologie de b_w, $[b_w]$ est dans l'image de l'inflation. Or, on a le

LEMME 5.2. $\mathscr{H}^{K_w} = 0$.

Démonstration. Il y a $\sigma \in K_w$ dont la restriction à F est un générateur du groupe d'inertie en $\mathfrak{p}^\varrho$ dans $\Delta = \mathrm{Gal}(F/M)$. On a donc

$$\Phi(\sigma) \equiv 1 \text{ mod. } \mathfrak{M}$$

$$\Phi^\varrho(\sigma) \not\equiv 1 \text{ mod. } \mathfrak{M}$$

donc

$$\Phi(\sigma) - \Phi^\varrho(\sigma) \notin \mathfrak{M}.$$

Mais cet élément annule le R_2-module $\mathscr{H}^{K_w}$, d'où la conclusion.

On déduit de ce lemme que $[b_w] = 0$, c'est-à-dire qu'il existe $\xi \in \mathscr{H}$ tel que pour tout σ de G on ait: $b_w(\sigma) = \sigma \cdot \xi - \xi$. Et en particulier:

Pour tout y de Z_w, $a_w(\sigma)(y) = (\Phi^\varrho(\sigma) - \Phi(\sigma)) \cdot \xi\pi(y)$. Soit Z' l'image de Z_w dans $B^{(1)}[\mathfrak{c}_2]$ par l'application $y \mapsto Y + \xi\pi y$.

LEMME 5.3. *Les R_2-modules Z_w et Z' sont isomorphes et Z' est un G-sous-module de $B^{(1)}[\mathfrak{c}_2]$ sur lequel G opère par Φ^ϱ.*

Démonstration. Si $y \in Z_w$, $\pi y \in Z$ et $\xi\pi y \in X^{(1)} = \ker \pi$. Donc si $y + \xi\pi y = 0$, on a: $\pi y = 0$, donc $y = 0$. De plus, l'action de σ sur $z = y + \xi\pi y \in Z'$ est donnée matriciellement par:

$$\begin{pmatrix} \Phi(\sigma) & a_w(\sigma) \\ 0 & \Phi^\varrho(\sigma) \end{pmatrix} \begin{pmatrix} \mathrm{Id} & \xi\pi \\ & \mathrm{Id} \end{pmatrix} \begin{pmatrix} 0 \\ y \end{pmatrix} = \begin{pmatrix} \Phi(\sigma) & \Phi(\sigma) \cdot \xi\pi + a_w(\sigma) \\ 0 & \Phi^\varrho(\sigma) \end{pmatrix} \begin{pmatrix} 0 \\ y \end{pmatrix}.$$

Or $\Phi(\sigma)\xi\pi(y) + a_w(\sigma)(y) = \Phi^\varrho(\sigma)\xi\pi(y)$. On trouve donc: $\sigma \cdot z = \Phi^\varrho(\sigma) \cdot z$.

Notons que π induit maintenant un isomorphisme G-linéaire $Z' \xrightarrow{\sim} Z$.

Considérons alors l'image réciproque Y' de Z' dans B par l'application $B \to B^{(1)}$; c'est un G_M-module. On peut l'insérer dans le diagramme commutatif:

$$\begin{array}{ccccccccc} 0 & \to & Y & \to & Y' & \to & Z' & \to & 0 \\ & & \cap & & \cap & & \downarrow & & \\ 0 & \to & B[\mathfrak{c}_2] & \to & B[\mathfrak{c}_2^2] & \to & B[\mathfrak{c}_2^2]/B[\mathfrak{c}_2] & \to & 0. \end{array} \tag{5.5}$$

On tire aisément de la connaissance des structures des R_2-modules qui interviennent dans ce diagramme, qu'avec le choix de la base $\mathscr{B}$ de B^* effectué plus haut, on a un diagramme commutatif de R_2-modules:

$$\begin{array}{ccccccccc} 0 & \to & Z'^* & \to & Y'^* & \to & Y^* & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathfrak{c}_2/\mathfrak{a} & \to & R_2/\mathfrak{a} & \to & R_2/\mathfrak{c}_2 = C & \to & 0. \end{array}$$

On voit donc qu'en définissant le G_M-module $X^{(2)}$ par l'exactitude de la suite:

$$0 \to Y' \to B[\mathfrak{a}] \to X^{(2)} \to 0, \tag{5.6}$$

la suite des duaux de Pontryagin est scindée sur R_2 et fournit une représentation $\mathscr{R}$: $G_M \to GL_2(R_2/\mathfrak{a})$ triangulaire supérieure:

$$\mathscr{R}(\sigma) = \begin{pmatrix} \alpha(\sigma) & \beta(\sigma) \\ 0 & \delta(\sigma) \end{pmatrix}$$

On sait que les congruences suivantes ont lieu:

$$\begin{cases} \alpha \equiv \Phi^{-1} \bmod. \mathfrak{c}_2 \\ \delta \equiv \Phi^{-\varrho} \bmod. \mathfrak{c}_2. \end{cases} \tag{5.7}$$

On note désormais S l'anneau $R_2/\mathfrak{a}$. En fait, on va montrer que les congruences (5.7) proviennent des égalités analogues dans S.

LEMME 5.4. $\alpha^\varrho = \delta$.

Démonstration. La conjugaison complexe opère sur $B[\mathfrak{a}]$ et induit donc une matrice $\mathscr{R}(\varrho)$ dans $GL_2(S)$. De plus, pour tout $\sigma \in G_M$, on a:

$$\mathscr{R}(\varrho)\begin{pmatrix} \alpha(\sigma) & \beta(\sigma) \\ 0 & \delta(\sigma) \end{pmatrix} = \begin{pmatrix} \alpha^\varrho(\sigma) & \beta^\varrho(\sigma) \\ 0 & \delta^\varrho(\sigma) \end{pmatrix}\mathscr{R}(\varrho). \tag{5.8}$$

Or les congruences (5.5) montrent que si $\mathfrak{M}_S$ désigne l'idéal maximal de l'anneau local S, on a: $\alpha \not\equiv \alpha^\varrho$ mod. $\mathfrak{M}_S$. Par conséquent, la matrice $\mathscr{R}(\varrho)$ mod. $\mathfrak{M}_S$ ne peut être triangulaire supérieure: si $\mathscr{R}(\varrho) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, on a: $c \in S^\times$. En développant (5.8), on trouve alors:

$$c \cdot \alpha(\sigma) \quad = \quad c \cdot \delta^\varrho(\sigma)$$

d'où la conclusion: $\alpha = \delta^\varrho$, $\alpha^\varrho = \delta$.

On observe en outre que les caractères α et δ sont non-ramifiés hors de $N \cdot p$, grâce à la bonne réduction de $J_r(R)$ hors de Np et, plus précisement:

PROPOSITION 5.5
1) *Les conducteurs de* α *et* δ *divisent* $N \cdot p^\infty$.
2) *Le conducteur de* α *est* $\mathfrak{f} \cdot \mathfrak{p}^\infty$, *celui de* δ *est* $\mathfrak{f}^\varrho \cdot \mathfrak{p}^{\varrho\infty}$.

Commmentaire. Le sens à donner aux assertions ci-dessus est précisé dans la démonstration.

Démonstration. Notons encore α et δ les caractères des idèles de M déduits des avatars galoisiens. Soient α_r et δ_r les réductions modulo $\omega_{2,r}$ de ces caractères. On a Ker $\alpha = \bigcap_{r \geqslant 1}$ Ker α_r. Il suffit donc de montrer que Ker $\alpha_r \supset W_{Np^r}$ où W_{Np^r} est le sous-groupe des idèles de M qui sont des unités en chaque place de M et sont congrues à 1 mod $Np^r\mathcal{O}_v$ en chaque place v de M divisant Np^r. Si v est une telle place, elle est de degré 1 grâce à nos hypothèses sur N et p. Notons sa norme ℓ. Soit ℓ^ν la puissance exacte de ℓ divisant Np^r. Grâce à un théorème de Langlands déjà invoqué au paragraphe 4, le groupe $J_r(R)$ a bonne réduction au-dessus de ℓ sur $\mathbb{Q}(\zeta_{\ell^\nu})$. L'inertie en v dans G_M agit donc sur $J_r(R)$ à travers le quotient Gal$(M(\zeta_{\ell^\nu})/M)$. Si donc $x \in M_v^\times$, et $x \equiv 1$ mod. v^ν, on a $(x, M)|M(\zeta_{\ell^\nu}) = \mathrm{Id}$, donc $\alpha_r(x) = \delta_r(x) = 1$. Ceci prouve que Ker $\alpha \supset W_{N \cdot p^\infty} = \bigcap_{r \geqslant 1} W_{N \cdot p^r}$ et de même pour δ. Ce qui prouve 1). De plus, comme $\alpha \equiv \Phi^{-1}$ mod. $\mathfrak{c}_2$ et que Φ est de conducteur divisible par $\mathfrak{f}$, on voit que $\mathfrak{f}$ divise le conducteur de α (donc $\mathfrak{f}^\varrho$ le conducteur de $\delta = \alpha^\varrho$). On va montrer que α est non-ramifié hors de $\mathfrak{f} \cdot \mathfrak{p}$ Soit v une place divisant le conducteur de α et divisant aussi $\mathfrak{f}^\varrho \mathfrak{p}^\varrho \cdot D$. On note ℓ sa caractéristique résibuelle. Soit μ la valuation v-adique de $D\mathfrak{f}^\varrho\mathfrak{p}^\varrho$. Soit x une idèle de M de composantes égal à 1 en tout $w|Np$, et telle que:

$$\begin{cases} x \equiv 1 \text{ mod. } Np/v \\ x \not\equiv 1 \text{ mod. } v^\nu \end{cases}$$

$$\text{on aurait } \alpha(x) \neq 1 \in \begin{cases} \mu_{\ell-1} & \text{si } \nu = 1 \\ \mu_\ell & \text{si } \nu > 1 \end{cases}$$

et en réduisant modulo l'idéal maximal $\mathfrak{M}_S$ de S, grâce à l'hypothèse $p \nmid \ell(\ell - 1)$, on trouve

$$\alpha(x) \not\equiv 1 \text{ mod. } \mathfrak{M}_S$$

donc

$$\Phi(x) \not\equiv 1 \text{ mod. } \mathfrak{M}_S.$$

Ceci est impossible car le caractère Φ modulo $\mathfrak{M}_S$ coïncide avec $\tilde{\lambda}$ (réduction de λ mod. $\mathfrak{P}$) qui est de conducteur $\mathfrak{f}\mathfrak{p}$ comme on l'a vu au paragraphe 2. On a pratiqué même abus de langage pour Φ que pour α et δ à savoir d'identifier Φ au caractère des idèles de M qu'il définit.

On conclut donc que le caractère α définit un caractère du groupe $C\ell_{\mathfrak{f}\mathfrak{p}^\infty} \simeq C\ell_{\mathfrak{f}\mathfrak{p}} \times (1 + \mathfrak{f}\hat{\mathfrak{p}})$. Sa restriction à $C\ell_{\mathfrak{f}\mathfrak{p}}$ a même été identifiée dans le raisonnement ci-dessus:

pour $x = (x_1, x_2)$, on a vu que

$$\alpha^{-1}(x) = \hat{\lambda}(x_1) \cdot \alpha^{-1}(1, x_2).$$

Proposition 5.6. *$\alpha^{-1} = \Phi$ dans S.*

Démonstration. On doit montrer pour $x_2 \in 1 + \mathfrak{f}\hat{\mathfrak{p}}$, que $\alpha(1, x_2) = \eta^{-1}(x_2)$ car Φ est défini comme la composée de l'isomorphisme inverse de la loi d'Artin avec η. Pour cela, on utilise les relations d'Eichler–Shimura pour calculer le déterminant de la représentation $\mathscr{R}$: si v est une place de M de degré 1, de norme ℓ, $\ell \nmid Np$, on a:

$$\text{dét } \mathscr{R}(\text{Frob}_v) = (\ell \langle \ell \rangle_2)^{-1}.$$

Choisissons pour chaque entier $n \geqslant 1$ un tel idéal premmier $\mathscr{L}_n$ de degré 1 engendré par ξ_n tel que

$$\begin{cases} \xi_n \equiv x_2 \text{ mod. } \mathfrak{f} \cdot \mathfrak{p}^n \\ \xi_n \equiv 1 \text{ mod. } \sqrt{-D}\mathfrak{f}^{\varrho}\mathfrak{p}^{\varrho n}. \end{cases}$$

On construit un tel idéal par le théorème de Cebotarev en considérant la composée M_n' des corps de rayons de connducteur $\mathfrak{f}\mathfrak{p}^n$ et $\sqrt{-D}\mathfrak{f}^{\varrho}\mathfrak{p}^{\varrho n}$, disjoints au-dessus du corps de Hilbert $M_{(1)}$ de M: il y a σ dans $\mathrm{Gal}(M_n'/M)$ de restrictions:

$$\begin{cases} \sigma | M_{\mathfrak{f}\mathfrak{p}^n} = ((x_2), M_{\mathfrak{f}\mathfrak{p}^n}/M) \\ \sigma | M_{\sqrt{-D}\mathfrak{f}^\varrho \mathfrak{p}^{\varrho n}} = \mathrm{Id} \end{cases}$$

et il y a $\mathscr{L}_n$ de degré 1, de norme ℓ_n, tel que $(\mathscr{L}_n, M_n'/M) = \sigma$. On peut alors approximer x_2:

$$\xi_n \xi_n^\varrho \equiv x_2 \bmod. \mathfrak{f}\mathfrak{p}^n$$

donc

$$\alpha((\xi_n \xi_n^\varrho)) \to \alpha(x_2)$$

mais

$$\begin{aligned} \alpha(\xi_n \xi_n^\varrho) &= \alpha(L_n) \cdot \alpha(\mathscr{L}_n^\varrho) = \text{dét}\, \mathscr{R}(\mathrm{Frob}_{\mathscr{L}_n}) \\ &= (\ell_n^{-1} \langle \ell_n \rangle_0)^{-1} \to (x_2^{-1}[x_2])^{-1} = \eta^{-1}(1, x_2). \end{aligned}$$

Il résulte aussi de cette proposition que $\delta = \Phi^{-\varrho}$ dans S.

Proposition 5.7. *Sous l'hypothèse* 5.3, *on a les égalités suivantes dans* S:

$$T(\ell) = \begin{cases} \eta(\mathscr{L}) + \eta(\mathscr{L}^\varrho) & \textit{si } \ell \nmid Np \textit{ et } \ell \textit{ est décomposé en } \mathscr{L} \textit{ et } \mathscr{L}^\varrho \\ 0 & \textit{si } \ell \textit{ est inerte} \\ \eta(\mathscr{L}) & \textit{si } \ell \textit{ est ramifié ou est décomposé mais } \mathscr{L}^\varrho \to \mathfrak{f}\mathfrak{p}. \end{cases}$$

Démonstration. 1) Si $\ell | Np$ et ℓ est décomposé en $\mathscr{L}$ et $\mathscr{L}^\varrho$, les relations d'Eichler–Shimura nous donnent le polynôme caractéristique de $\mathrm{Frob}_{\mathscr{L}}$ sur B^*:

$$X^2 - (\ell \langle \ell \rangle_2)^{-1} T(\ell) \cdot X + (\ell \langle \ell \rangle_2)^{-1}.$$

En effet, pour chaque $r \geqslant 1$, la représentation sur B_r^*, donc sur $\mathbb{Q}_p \otimes B_r^*$, est la contragrédiente de celle sur le module de Tate $V_p B_r$ sur lequel les relations d'Eichler–Shimura habituelles sont de mise.

D'autre part, sur $B[\mathfrak{a}]^*$ on a:

$$\mathscr{R}(\mathrm{Frob}_{\mathscr{L}}) = \begin{pmatrix} \eta^{-1}(\mathscr{L}) & * \\ 0 & \eta^{-1}(\mathscr{L}^{\varrho}) \end{pmatrix}.$$

On tire de cela que $T(\ell) = \eta(\mathscr{L}) + \eta(\mathscr{L}^{\varrho})$ dans S.

2) Si $\mathscr{L} \nmid Np$ et ℓ est inerte dans M, le Frobenius absolu en ℓ définit un automorphisme de B^* et de $B[\mathfrak{a}]^*$. Notons-les σ. On a $\sigma^2 = \mathrm{Frob}_{\mathscr{L}}$. Donc $\mathscr{R}(\sigma^2) = \left(\begin{smallmatrix} \eta^{-1}(\ell) & * \\ 0 & \eta^{-1}(\ell) \end{smallmatrix}\right)$.

On sait toujours par Eichler–Shimura, que le polynôme caractéristique de σ sur B^* est $X^2 - (\ell\langle\ell\rangle_2)^{-1}T(\ell)X + (\ell\langle\ell\rangle_2)^{-1}$, donc $\eta((\ell))^2 \equiv (\ell\langle\ell\rangle_2)^2$ mod. $\mathfrak{a}$. Grâce à la proposition 4.7, on sait que $\eta((\ell)) \equiv -\ell\langle\ell\rangle_2$ mod. $\mathfrak{c}_2$ donc aussi

$$\eta((\ell)) \neq \ell\langle\ell\rangle_2 \text{ mod. } \mathfrak{M}_S \quad (\text{sinon } p = 2, \text{ ce qui est interdit})$$

d'où l'on tire que $\eta((\ell)) \equiv -\ell\langle\ell\rangle_2$ mod. $\mathfrak{c}_2$.

Donc en reportant dans le polynôme caractéristique: $\eta((\ell))\sigma^2 - T(\ell)\sigma + 1 = 0$ soit $T(\ell)\sigma = \eta((\ell))\sigma^2 - 1 = \left(\begin{smallmatrix} 0 & * \\ 0 & 0 \end{smallmatrix}\right)$. Comme d'autre part σ est de déterminant inversible, on voit que si $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, on a a et d inversibles ou bien b et c inversibles, donc on trouve que $T(\ell) = 0$ dans S.

3) $\ell \mid N$, on peut écrire $(\ell) = \mathscr{L}\mathscr{L}^{\varrho}$ où $\mathscr{L}^{\varrho} \mid \mathfrak{f}$ dans M, ou bien $(\ell) = \mathscr{L}^2$. Posons pour chaque entier $r \geqslant 1$:

$$Y'_r = Y'[\omega_{2,r}].$$

C'est un sous-G_M-module de $B_r[\mathfrak{a}]$, non-ramifié en $\mathscr{L}^{\varrho}$, sur lequel un Frobenius en $\mathscr{L}^{\varrho}$ opère par $\Phi^0(\mathrm{Frob}_{\mathscr{L}^{\varrho}}) = \eta(\mathscr{L})$. Or, rappelons que:

$$B_r \subset \sum_f A_f[p^\infty]$$

où A_f désigne la sous-variété abèlienne de $J_1(Np^r)$ attachée à une newform f pour $\Gamma_1(Np^r)$ par Shimura (cf. théorème 7.14 de [22]), f parcourant un ensemble maximal de newforms pour $\Gamma_1(Np^r)$ deux à deux non-conjuguées et congrues à $\theta(\lambda)$ mod. $\mathfrak{P}$. Or le théorème 2.1 de Carayol [27] nous apprend que pour $\ell \mid N$ (donc $\ell \neq p$), si I_ℓ est un groupe d'inertie en ℓ sur $\mathbb{Q}$, l'action de Frob_ℓ sur $A_f[p^\infty]^{I_\ell}$ est donnée par: $a(\ell, f)$, i.e., par $T(\ell)$. On voit donc que l'action de Frob_ℓ sur $B_r^{I_\ell}$ est donnée par $T(\ell)$. Comme $\mathrm{Frob}_{\mathscr{L}^{\varrho}} = \mathrm{Frob}_\ell$, aussi bien si ℓ est ramifié que décomposé, on voit que sur Y'_r, on a $\eta(\mathscr{L}) = T(\ell)$.

On passe alors à la limite en r, puis aux duaux de Pontryagin pour obtenir l'égalité dans S:

$$\eta(\mathscr{L}) = T(\ell).$$

4) $\ell = p$. On utilise toujours la sous-variété abélienne $\mathscr{A}_r$ de $J_1(Np^r)$. Soit w l'unique place de $M(\zeta_{p^r})$ au-dessus de $\mathfrak{p}^\varrho$. On sait que $\mathscr{A}_r$ a bonne réduction en w. Pour tout nombre premier $q \neq p$, on sait que Frob_w agissant sur le module de Tate de $\mathscr{A}_r$ en q est annulé par $(X - T(p))(X - T(p)^*\langle a_p\rangle_{2,r})$ où $a_p \equiv p$ mod. N, $a_p \equiv 1$ mod. p^r. Il en résulte, en notant $\tilde{\mathscr{A}}_r$ la fibre spéciale en w de $\mathscr{A}_r$, que dans $\mathrm{End}(\tilde{\mathscr{A}}_r)$ on a l'égalité

$$(\langle a_p\rangle\pi - T(p))\cdot(\langle a_p\rangle\pi - T(p)^*\langle a_p\rangle) = 0. \tag{5.9}$$

On forme alors l'adhérence schématique de $B_r[\mathfrak{a}]$ dans le modèle de Néron $\mathscr{A}_r/\mathscr{O}_r$ de $\mathscr{A}_r$ et on considére son dévissage connexe-étale:

$$0 \to \mathscr{C}_r' \to B_r[\mathfrak{a}] \to \mathscr{E}_r' \to 0. \tag{5.10}$$

Comparons-le avec le dévissage connexe-étale (4.12) de $B_r[\mathfrak{c}_2]$. Soit $\mathfrak{b} = \mathfrak{c}_1 \oplus \mathfrak{a}$ l'idéal de R analogue à l'idéal $\mathfrak{c} = \mathfrak{c}_1 \oplus \mathfrak{c}_2$ considéré au lemme 4.1. On a $B_r[\mathfrak{a}] = J_r(R)[\mathfrak{b}]$ on a donc les inclusions de suites exactes:

$$\begin{array}{ccccccc}
0 \to & \mathscr{C}_r & \to & B_r[\mathfrak{c}_2] & \to & \mathscr{E}_r & \to 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 \to & \mathscr{C}_r' & \to & B_r[\mathfrak{a}] & \to & \mathscr{E}_r' & \to 0 \\
& \downarrow & & \| & & \downarrow & \\
0 \to & \mathscr{C}_r[\mathfrak{b}] & \to & J_r(R)[\mathfrak{b}] & \to & E_r[\mathfrak{b}]. &
\end{array}$$

Passons à la limite en r et dualisons les flèches verticales. Posons:

$$\begin{cases} \mathscr{C}' = \varinjlim \mathscr{C}_r' \\ \mathscr{E}' = \varinjlim \mathscr{E}_r'. \end{cases}$$

On obtient alors:

$$\begin{cases} S \twoheadrightarrow \mathscr{C}'^* \twoheadrightarrow R_2/\mathfrak{c}_2 \\ S \twoheadrightarrow \mathscr{E}'^* \twoheadrightarrow R_2/\mathfrak{c}_2 \end{cases}$$

comme $B[\mathfrak{a}]^* \simeq S \oplus W$, on obtient aisément que

$$\begin{cases} \mathscr{C}'^* \simeq S \\ \mathscr{E}'^* \simeq S. \end{cases}$$

De plus, $\mathscr{E}'^*$ et $\mathscr{C}'^*$ sont des modules sur le groupe de décomposition en $\mathfrak{p}^\varrho$ dans G_M et en utilisant le corollaire 4.2 de [24], et on voit que l'action de ce groupe sur $\mathscr{E}'^*$ est donnée par Φ^{-1}. Comme $\Phi(\mathrm{Frob}_w) = \eta(\mathfrak{p}^\varrho)$, on conclut, en reportant dans la formule 5.9, que sur $\mathscr{E}'^*$, l'automorphisme de Frobenius $\mathrm{Frob}_{\mathfrak{p}^\varrho}$ opérant de façon covariante satisfait:

$$\begin{cases} \mathrm{Frob}_{\mathfrak{p}^\varrho} = \eta(\mathfrak{p}^\varrho) \\ (\mathrm{Frob}_{\mathfrak{p}^\varrho} - T(p)) \cdot (\mathrm{Frob}_{\mathfrak{p}^\varrho} - T(p)^*\langle a_p \rangle) = 0 \end{cases}$$

et comme $T(p)$ est inversible dans S et $T(p)T(p)^*\langle a_p\rangle = p$, on voit que $\eta(\mathfrak{p}^\varrho) - T(p)^*\langle a_p\rangle$ est une unité de S. Il en résulte que

$$\eta(\mathfrak{p}^\varrho) = T(p)$$

C.Q.F.D.

Dès lors, il est facile de terminer la démonstration du théorème 3.3. En effet, il résulte de la proposition 5.7 qu'il existe un isomorphisme d'anneaux j rendant commutatif le diagramme:

$$\begin{tikzcd} & R_1 = \Lambda_K \arrow[r] & \Lambda_K/(\mathfrak{a} \cap \Lambda_K) \arrow[d, "j", "\wr"'] \\ R \arrow[ur, "pr_1"] \arrow[dr, "pr_2"'] & & \\ & R_2 \arrow[r] & S \end{tikzcd}$$

On en déduit que $\mathfrak{c}_2$ est contenu dans $\mathfrak{a}$. En effet pr_1 est nulle sur $\mathfrak{c}_2$, donc l'image de $\mathfrak{c}_2$ dans S est nulle. On obtient donc

$$\mathfrak{c}_2 = \mathfrak{a}.$$

On voit donc que l'hypothèse 5.3 était absurde, donc que

$$a_\infty : \mathscr{X}^{(\kappa)} \otimes_{\mathbb{Z}_p} \mathcal{O}_K \to C'$$

est surjective. C.Q.F.D.

§6. Idéal de Fitting des différentielles – Conclusion

Nous avons ainsi établi la surjectivité du morphisme de Λ_K-modules:

$$a_\infty \otimes \mathrm{Id}_{\mathscr{C}_K}: \mathscr{X}^{(\kappa)}(1) \to C'.$$

Soit $\mathbb{H}'$ la série caractéristique de C', $\mathbb{F}'$ la série caractéristique de $\mathscr{X}^{(\kappa)}$. Il résulte immédiatement de la surjectivité de $a_\infty \otimes \mathrm{Id}_{\mathscr{C}_k}$ que

$$\mathbb{H}'(T) \mid \mathbb{F}'(u^{-1}(1 + T) - 1). \tag{6.1}$$

Nous nous intéressons en fait au lien entre la série caractéristique $\mathbb{H}$ du module de congruences, et la série caractéristique $\mathbb{F}$ du module d'Iwasawa $X^{(\kappa)}$ étudié dans la proposition 3.2. Nous allons établir

$$\mathbb{F}(T) = \mathbb{F}'(T) \tag{6.2}$$

et

$$\mathbb{H}(T) \mid \mathbb{H}'(T), \tag{6.3}$$

ce qui permettra grâce à (6.1) de conclure:

$$\mathbb{H}(T) \mid \mathbb{F}(u^{-1}(1 + T) - 1). \tag{6.4}$$

Lemme 6.1. *Il y a un homomorphisme de* $(\Delta \times \tilde{\Gamma})$*-modules*: $\mathscr{X} \to X$ *qui induit un isomorphisme de* Λ_K*-modules*: $\mathscr{X}^{(\kappa)} \xrightarrow{\sim} X^{(\kappa)}$. *En particulier, l'égalité* (6.2) *est vraie.*

Démonstration. Rappelons que $\mathscr{X} = \mathrm{Gal}(\tilde{\mathscr{N}}/\tilde{F}_\infty)$ et $X = \mathrm{Gal}(\mathscr{N}/F_\infty^-)$, où $\mathscr{N}$ (resp. $\tilde{\mathscr{N}}$) désigne la p-extension abélienne maximale non ramifiée hors de F_∞^- (resp. $\tilde{F}_\infty$). Comme $\tilde{F}_\infty/F_\infty^-$ est non ramifiée, nous avons les inclusions $\tilde{F}_\infty \subset \mathscr{N} \subset \tilde{\mathscr{N}}$. L'homomorphisme de restriction fournit alors la suite exacte:

$$\mathscr{X} \to X \to \Gamma^+ \to 1.$$

Commme Δ opère trivialement sur Γ^+, on obtient la surjection: $\mathscr{X}^{(\kappa)} \to X^{(\kappa)}$. Pour voir que c'est un isomorphisme, considérons l'idempotent e_{κ_0} de $\mathbb{Z}_p\Delta$ attaché au caractère rationnel κ_0 déduit de κ. Il est clair que κ_0

diffère du caractère trivial. Soit $\tilde{\mathcal{N}}^{(\kappa_0)}$ (resp. $\mathcal{N}^{(\kappa_0)}$) les sous-corps de $\tilde{\mathcal{N}}$ fixé par $(1 - e_{\kappa_0}) \cdot \mathcal{X}$ (resp. $1 - e_{\kappa_0})X$). On a la suite exacte de Δ-modules:

$$1 \to \mathcal{X}^{(\kappa_0)} \to \mathrm{Gal}\,(\tilde{\mathcal{N}}^{(\kappa_0)}/F_\infty^-) \to \Gamma^+ \to 1$$

et en prenant les parties correspondant au caractère trivial de Δ, on voit que Γ^+ possède un relèvement distingué dans $\mathrm{Gal}\,(\mathcal{N}^{(\kappa)}/F_\infty^-)$. Par conséquent $\tilde{\mathcal{N}}^{(\kappa_0)}$ est compositum de $\tilde{F}_\infty$ et $\mathcal{N}^{(\kappa_0)}$, qui sont linéairement disjoints sur F_∞^-. Donc

$$\mathcal{X}^{(\kappa_0)} \xrightarrow{\sim} X^{(\kappa_0)}$$

et enfin, en prenant les κ-parties:

$$\mathcal{X}^{(\kappa)} \xrightarrow{\sim} X^{(\kappa)}.$$

Nous avons défini au paragraphe 2 (cf. proposition 2.1) un caractère X: $h^0 \to \Lambda_K$ et Hida a associé à un tel caractère son module de différentielles $C(\mathrm{X})$ est son module de congruences $C(\mathrm{X})$ (cf. paragraphe 1 de [28]). Avec nos notations, nous avons:

$$\begin{cases} C_1(\mathrm{X}) = C' = \mathfrak{c}_2/\mathfrak{c}_2^2 \\ C_0(\mathrm{X}) = C = R_2/\mathfrak{c}_2 = \Lambda_K/(\mathbb{H}). \end{cases}$$

Rappelons que si M est un Λ_K-module de type fini et de torsion, de série caractéristique f et d'idéal de Fitting $F(M)$, l'idéal principal $f \cdot \Lambda_K$ coïncide avec l'enveloppe réflexive de $F(M)$ (pour les propriétés élémentaires de l'idéal de Fitting, cf. par exemple l'appendice de [31]). Il est alors clair que la divisibilité (6.3) équivaut à:

$$F(C_1(\mathrm{X})) \subset F(C_0(\mathrm{X})). \tag{6.3'}$$

En fait, l'égalité de ces idéaux a été conjecturée par Hida dans [28]. Le reste du paragraphe est consacré à la démonstratiion de (6.3'). La formation de l'idéal de Fitting commute à la localisation, il suffit donc de considérer successivement chaque facteur premier P de $\mathbb{H}$ et montrer l'analogue de (6.3') sur l'anneau de valuation discrète complet obtenu en localisant Λ_K en P. Considérons donc la situation plus générale suivante.

Soit D un anneau de valuation discrète complet de corps des fractions L, uniformisante π, corps résiduel k. Soit R une D-algèbre finie et plate, munie d'un caractère χ. $R \to D$ induisant un scindage générique

$$R \otimes_D L \xrightarrow{\sim} L \times B \tag{6.4}$$

où $pr_1 = \chi$ et B est une L-algèbre convenable. Notons η la restriction à R de la seconde projection:

$$pr_2 \colon R \otimes_D L \to B.$$

Soient $\mathfrak{a} = \operatorname{Ker} \chi$, $\mathfrak{b} = \operatorname{Ker} \eta$ et soit F_1 l'idéal de Fitting de $C_1(\chi) = \mathfrak{a}/\mathfrak{a}^2$ et F_0 l'idéal de Fitting de $C_0(\chi) = D/\chi(\mathfrak{b}) \cong \eta(R)/\eta(\mathfrak{a})$. L'énoncé général est alors:

PROPOSITION 6.2. *Sous les hypothèses générales précisée ci-dessus, on a*:

$$F_1 \subset F_0.$$

La démonstration de cette proposition m'a été communiquée par M. Raynaud. Elle comporte deux étapes. La première suppose que R est d'intersection complète relative sur D et la seconde consiste à ramener le cas général au cas d'intersection complète relative.

Soit $A = D[X_1, \ldots, X_d]$ l'algèbre des polynômes à d variables sur D.

DEFINITION 6.3. *Nous dirons qu'une suite $(f_1, \ldots, f_d)$ d'éléments de A est relativement régulière sur D si pour chaque $i = 1, \ldots, d$, la R-algèbre $A_i = A/(f_1, \ldots, f_i)$ est plate sur D et f_i ne divise pas 0 dans $A_{i-1} \otimes_R k$ ($A_0 = D$ par définition).*

DÉFINITION 6.4. *Si l'algèbre R possède une présentation*

$$0 \to I \to A \to R \to 0 \tag{6.5}$$

de sorte que l'idéal I soit engendré par une suite relativement régulière, nous dirons que R est d'intersection complète relative sur D.

1) Supposons que R est d'intersection complète relative sur D (en abrégé I.C.R.).

Dans ce cas, nous allons montrer l'égalité $F_0 = F_1$.

Grâce à la deuxième suite exacte fondamentale des différentielles de Kähler, on déduit de (6.5) la suite exacte:

$$I/I^2 \to \Omega_{A/D} \otimes_A R \to \Omega_{R/D} \to 0$$

et d'après l'hypothèse (I.C.R.), on voit que I/I^2 est libre de rang d sur R et que la première flèche est injective. De plus, on observe que le D-module $C_1(\chi)$ est isomorphe à $\Omega_{R/D} \otimes_{R,\chi} D$ où la structure de R-algèbre de D est donnée par χ: $R \to D$. On tire de ces remarques qu'on a une résolution libre de longueur 1 du D-module $C_1(\chi)$:

$$0 \to I/I^2 \otimes_{R,\chi} D \to \Omega_{A/D} \otimes_A R \otimes_{R,\chi} D \to C_1(\chi) \to 0.$$

L'idéal de Fitting F_1 de $C_1(\chi)$ est donc principal engendré par $\chi(j)$ où $j \in R$ est la spécialisation de A à R du jacobien dét $(\partial f_\alpha/\partial X_\beta)$. Soient j_1 et j_2 les composantes de j dans la décomposition (6.4), i.e., $j = (j_1, j_2)$ et $j_1 = \chi(j)$. sous l'hypothèse (I.C.R.), le R-module $\mathrm{Hom}(R, D)$ est libre de rang 1 et, plus précisément, j est une différente de R/D. C'est-à-dire qu'il y a une R-base $\{\lambda\}$ de $\mathrm{Hom}(R, D)$ telle que $\mathrm{Tr}_{R/D} = \lambda \cdot j$ (R opère à droite sur $\mathrm{Hom}(R, D)$ et $\mathrm{Tr}_{R/D}$ désigne la forme linéaire donnée par la trace) (cf. [30] théorème de l'appendice). Ainsi pour montrer l'égalité $F_0 = F_1$ il suffit de montrer que:

$$j_1 \cdot D = \{x_1 \in D;\, (x_1, 0) \in R\}.$$

Comme λ établit une autodualité de R, cela revient à voir que $x_1/j_1 \in D$ si et seulement si on a pour tout y de R, $\lambda((x_1, 0)\cdot y) \in D$. Or, grâce à l'égalité $(x_1, 0) = (x_1/j_1), 0)\cdot j$, on a $\lambda((x_1,0)y) = \mathrm{Tr}_{R/D}((x_1/j_1, 0)\cdot y)$. Comme $\mathrm{Tr}_{R/D} \otimes \mathrm{Id}_L$ induit l'identité sur le facteur L de la décomposition (6.4), on conclut à l'égalité annoncée.

2) Cas général.

Considérons une présentation de R par l'algèbre A comme en (6.5). Cette fois, on ne peut supposer que l'idéal I est engendré par une suite relativement régulière. Soit $\tilde{\mathfrak{a}}$ l'image reciproque dans A de $\mathfrak{a}$. La proposition suivante va nous ramener au cas 1:

Proposition 6.5. *Il existe un idéal I' de A contenu dans I et tel que*:

(i) *I' est engendré par une suite relativement régulière et $R' = A/I'$ est finie et plate sur D.*

(ii) *La surjection naturelle* γ: $R' \to R$ *induit un isomorphisme*:

$$\mathfrak{a}'/\mathfrak{a}'^2 \xrightarrow{\sim} \mathfrak{a}/\mathfrak{a}^2$$

où $\mathfrak{a}' = \tilde{\mathfrak{a}}/I'$.

(iii) *Le caractère naturel* χ': $R' \to D$ *de noyau* $\mathfrak{a}'$ *induit un scindage sur* L:

$$R' \otimes_D L \xrightarrow{\sim} L \times (\mathfrak{a}' \otimes_D L).$$

Démonstration. Considérons la suite exacte:

$$0 \to I/\tilde{\mathfrak{a}}^2 \cap I \to \tilde{\mathfrak{a}}/\tilde{\mathfrak{a}}^2 \to \mathfrak{a}/\mathfrak{a}^2 \to 0.$$

Grâce à l'isomorphisme D-linéaire:

$\tilde{\mathfrak{a}}/\tilde{\mathfrak{a}}^2 \xrightarrow{\sim} \Omega_{A/D} \otimes_A R \otimes_{R,\chi} D$, on voit que

le D-module $\tilde{\mathfrak{a}}/\tilde{\mathfrak{a}}^2$ est libre de rang d. Comme $\mathfrak{a}/\mathfrak{a}^2$ est un D-module de longueur finie, on conclut que le noyau $N = I/\tilde{\mathfrak{a}}^2 \cap I$ est libre de rang d. Pour construire une suite relativement régulière relevant une base de N, on va rréduire la situation modulo π et invoquer le résultat suivant d'algèbre commutative (cf. E.G.A.) 0_{III} (10.2.4) ou [29] 20.F Corollary 1):

> Soit D un anneau local noetherien de corps résiduel k; A une D-algèbre de type fini, M un A-module de type fini et $f \in A$. que M soit D-plat et que f ne *divise* pas zéro dans $M \otimes_D k$. Alors f ne divise pas zéro dans M et M/fM est plat sur R. (6.6)

Appliquons cet énoncé à notre situation. Nous en déduisons:

> Soit $(f_1, \ldots, f_d)$ une suite dans $A = D[X_1, \ldots, X_d]$ (6.7)
>
> dont la réduction modulo π est régulière dans $k[X_1, \ldots, X_d]$. Alors pour tout $i = 1, \ldots, d$, l'algèbre $A_i = A/(f_1, \ldots, f_i)$ est plate sur D de dimension relative d–i et f_i ne divise pas zéro dans A_{i-1}.

Pour utiliser ce dernier énoncé, nous construisons une suite régulière $(\tilde{f}_1, \ldots, f_d)$ dans $I \otimes k \subset A \otimes k$ relevant une base $(\tilde{e}_1, \ldots, \tilde{e}_d)$ de $N \otimes k$. Soit $\mathscr{J} = (\tilde{\mathfrak{a}}^2 \cap I) \otimes k$. C'est un idéal de $A \otimes k$ de hauteur d. On prend alors $\tilde{f}_1 \in I \otimes k$ relevant $\tilde{e}_1$. Si $d = 1$, on a fini. Sinon, les idéaux premiers minimaux $\mathfrak{p}_i^{(1)}$ contenant $\tilde{f}_1$ sont de hauteur $1 < d$; il existe donc $\tilde{f}_2$ tel que:

$$\begin{cases} \tilde{f}_2 \equiv \tilde{e}_2 \text{ mod. } \mathscr{I} \\ \tilde{f}_2 \notin \bigcup\limits_i \mathfrak{p}_i^{(1)}. \end{cases}$$

De nouveau si $d = 2$, on a fini; sinon, on poursuit la construction, ce qui est possible tant que haut. $(\tilde{f}_1, \ldots, \tilde{f}_i) = i < d$. Grâce à l'énoncé (6.7), on obtient ainsi une suite $(f_1, \ldots, f_d)$ relativement régulière contenue dans I et relevant une base de N. Soit I_1' l'idéal de A qu'elle engendre. L'algèbre $R_1' = A/I_1'$ est plate sur D et est d'intersection complète relative. L'idéal $\mathfrak{a}_1' = \tilde{\mathfrak{a}}/I_1'$ vérifie bien la condition (ii) de la proposition 6.5 car

$$I_1'/\tilde{\mathfrak{a}}^2 \cap I_1' \cong N$$

par définition de I_1'. Cependant l'algèbre R_1' n'est pas nécessairement finie sur D. On surmonte cette difficulté grâce au

SOUS-LEMME 6.6. *Soit R_1' une algèbre de type fini sur un anneau de valuation discrète complet D, telle que $R_1' \otimes k$ soit finie sur k et $R_1' \otimes L$ soit finie sur L. Il existe alors un isomorphisme de D-algèbres*:

$$R_1' \xrightarrow{\sim} R' \times R_0'$$

où R' est une D-algèbre finie
et R_0' est une K-algèbre finie.

Démonstration. On remarque d'abord que R_1' est semi-locale grâce aux hypothèses de finitude des fibres générique et spéciale.

De plus, R_1' s'injecte dans le produit de ses localisés aux idéaux maximaux. Soit $\mathfrak{M}$ un idéal maximal au-dessus de $\pi \cdot D$. L'anneau localisé en $\mathfrak{M}$ de R_1' est séparé pour la topologie $\mathfrak{M}$-adique. Il s'injecte donc dans son séparé complété. Ce dernier module est de type fini sur D grâce au lemme de Nakayama topologique (les topologies $\mathfrak{M}$-adique et π-adique du séparé complété sont équivalentes car $R_1' \otimes k$ est finie sur k). On en déduit que l'anneau localisé en $\mathfrak{M}$ de R' *coïncide* avec son complété. On définit alors R' (resp. R_0') commme le produit des localisés de R_1' aux idéaux maximaux au-dessus de $\pi \cdot D$ (resp. au-dessus de 0). Le lemme chinois montre que R_1'

se surjecte sur $R' \times R'_0$ et la démonstration est achevée car R' est finie sur D et R'_0 est finie sur K.

On peut alors terminer la démonstration de la proposition 6.5 en appliquant le lemme 6.6 à l'algèbre R'_1 construite ci-dessus. L'algèbre R' est l'algèbre finie et plate cherchée. Notons que sa fibre spéciale est la même que celle de R'_1, donc R' est encore intersection complète relative grâce à l'énoncé (6.7). En outre, l'idéal $\mathfrak{a}' = \mathfrak{a}'_1 \cap R'$ vérifie encore la condition (ii) de la proposition 6.5. Enfin, pour assurer que l'augmentation χ': $R' \to D$ est scindée sur L, nous considérons un élément e de $A \otimes L$ relevant l'idempotent de $R \otimes L$ correspondant à $\chi \otimes \mathrm{Id}_L$. Nous remarquons que $e^2 - e \in I \otimes L$ et $e^2 - e \notin \tilde{\mathfrak{a}}^2 \otimes L$. Si δ est un élément de D de valuation minimale tel que $e_0 = \delta \cdot e \in A$, on voit que $e_0^2 - \delta \cdot e_0 \notin \tilde{\mathfrak{a}}^2$ et même, par platitude de $A/\tilde{\mathfrak{a}}^2$, $e_0^2 - \delta \cdot e_0 \notin \tilde{\mathfrak{a}}^2 + \pi \cdot A$. Ceci permet de prendre $\tilde{f}_1 = e_0^2 - \delta \cdot e_0$ mod. π dans la construction de la suite régulière modulo π, puis de prendre $f_1 = e_0^2 - \delta \cdot e_0$ comme relèvement de $\tilde{f}_1$. Il est alors clair que l'augmentation χ'_1: $R'_1 \to D$ est scindée sur L, donc aussi l'augmentation χ': $R' \to D$. Q.E.D.

On applique alors la proposition 6.5 pour achever la démonstration de la proposition 6.2.

En effet, par construction de $\mathfrak{a}'$, on a égalité des idéaux de Fitting de $C_1(\chi)$ et $C_1(\chi')$. Par l'étude du cas 1, on a égalité des idéaux de Fitting de $C_0(\chi')$ et $C_1(\chi')$, et par fonctorialité évidente, on a $F(C_0(\chi')) \subset F(C_0(\chi))$. En fait si l'on considère le scindage:

$$(\chi', \eta'): R' \otimes L \xrightarrow{\sim} L \times B'$$

et

$$b' = \mathrm{Ker}(\eta': R' \to B')$$

on a: $F(C_0(\chi')) = \chi'(b') = \chi(\gamma(b')) \subset \chi(b) = F(C_0(\chi))$.

Ces relations impliquent l'inclusion $F_1 \subset F_0$. Remarquons que l'inclusion inverse, $F_0 \subset F_1$ conjecturée par Hida nécessite l'hypothèse que R est de Gorenstein (contrairement à l'inclusion que nous avons prouvé, qui n'utilise que les hypothèses de la proposition 6.2).

En effet, on peut trouver dans [28] un contre-exemple à $F_0 \subset F_1$ pour une $\mathbb{Z}_p$-algèbre finie et plate mais non de Gorenstein:

$$R = \{(x, y, z) \in \mathbb{Z}_p^3;\ x \equiv y \equiv z \text{ mod. } p\}$$

$$\chi = pr_1.$$

On a $F_0(p)$, $F_1 = (p^2)$.

Références

1. M. Atiyah et I. Macdonald, *Introduction to Commutative Algebra.* Addison-Wesley (1969).
2. J. Coates, p-adic L functions and Iwasawa theory, in *Algebraic Number Fields*, edited by A. Fröhlich, Academic Press (1977).
3. C. Curtis et I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Puublishers (1962).
4. K. Doi et M. Ohta, On some congruences between cusp forms on $\Gamma_0(N)$, in *Modular Functions of One Variable, Proceedings International Conference*, University of Bonn, L.N.M. 601, Springer-Verlag (1977) 91–105.
5. P. Gabriel, *Construction de Préschémas Quotients*, Exposé V in SGA 3 (Schémas en Groupes I), *Séminaire de Géométrie Algébrique du Bois Marie 1962/64*, dirigé par M. Demazure et A. Grothendieck, L.N.M. 151, Springer-Verlag (1970) 250–286.
6. H. Hida, Congruences of cusp forms and special values of their zeta functions. *Inv. Math.* 63 (1981) 225–261.
7. H. Hida, On congruence divisor of cusp forms as factors of the special values of their zeta functions. *Inv. Math.* 64 (1981) 221–262.
8. H. Hida, Kummer's criterion for the special values of Hecke L-functions of imaginary quadratic fields and congruences among cusp forms. *Inv. Math.* 66 (1982) 415–459.
9. H. Hida, A p-adic measure attached to the zeta functions associated with two elliptic modular forms, I. *Inv. Math.* 79 (1985) 159–195.
10. H. Hida, Iwasawa modules attached to congruences of cusp forms: *Ann. Scient. Ec. Norm. Sup.* 4ème série t. 19 (1986) 231–273.
11. H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms. *Inv. Math.* 85 (1986) 545–613.
12. J.I. Igusa, Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.* 81 (1959) 561–577.
13. N. Katz, Higher congruences between modular forms. *Ann. of Math.* 101 (1975) 332–367.
14. S. Lang, *Cyclotomic Fields I.* Springer-Verlag (1978).
15. R.-P. Langlands, Automorphic Forms and ℓ-adic representations, in *Proceedings International Summer School on Modular Functions of One Variable*, II, Antwerp 1972, L.N.M. 349, Springer-Verlag (1973) 361–500.
16. B. Mazur et A. Wiles, On p-adic analytic fammilies of Galois representations. *Comp. Math.* 59 (1986) 231–264.
17. B. Perrin-Riou, *Arithmétique des Courbes Elliptiques et Théorie d'Iwasawa*, Mémoires de la S.M.F. No 17, Nouvelle Série (1984).
18. K. Ribet, A Modular construction of unramified extensions of $\mathbb{Q}(\mu_p)$. *Inv. Math.* 34 (1976) 151–162.
19. K. Ribet, Galois representations attached to eigennforms with Nebentypus, in *Modular Functions of One Variable* V, L.N.M. 601, Springer-Verlag (1977) 17–52.
20. J.-P. Serre, *Représentations Linéaires des Groupes finis.* Hermann (1967).
21. J.-P. Serre et J. Tate, Good reduction of abelian varieties. *Ann. of Math.* 88 (1968) 492–517.
22. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Iwanami Shoten Publishers and Princeton University Press (1971).
23. G. Shimura, On Elliptic curves with complex multiplication as factors of the jacobians of modular function fields. *Nagoya Math. J.* 43 (1971) 199–208.
24. J. Tilouine, Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke (à paraître).

25. A. Weil, Ueber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.* 168 (1967) 149–156.
26. A. Wiles, Modular curves and the class-group of $\mathbb{Q}(\mu_p)$. *Inv. Math.* 58 (1980) 1–35.
27. H. Carayol, Sur les représentations ℓ-adiques attachées aux formes modulaires de Hilbert. *C.R. Acad Sc. Paris* 296 Série I (1985) 629–632.
28. H. Hida, *Hecke Algebras for GL_1 and GL_2*, Sém. de Théorie des Nombres de Paris (1985–86) 131–163.
29. H. Matsumara, *Commmutative Algebra*, Benjamin (1970).
30. B. Mazur et L. Roberts, Local Euler characteristics, *Inv. Math.* 9 (1970) 201–234.
31. B. Mazur et A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Inv. Math.* 76 (1984) 179–330.