GROUPE DE TRAVAIL
D'ANALYSE ULTRAMÉTRIQUE

JACQUES TILOUINE

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

Groupe de travail d'analyse ultramétrique, tome 13 (1985-1986), p. 99-112
<http://www.numdam.org/item?id=GAU_1985-1986__13__99_0>

THEORIE D'IWASAWA DE L'ALGEBRE DE HECKE ORDINAIRE ET THEORIE D'IWASAWA CLASSIQUE

Jacques Tilouine

1 - Nombre du type Hurwitz et critère d'irrégularité.

Soit M un corps quadratique imaginaire d'anneau des entiers $\mathcal{O}$, de discriminant $-D$, de nombre de classes h, de conjugaison complexe ρ. Soit λ un Grössencharakter de M de type $(\nu,0)$, $\nu \geq 1$, de conducteur $\mathfrak{f}$, i.e. $\lambda((\alpha)) = \alpha^{\nu}$ si $\alpha \in M^{\times}$, $\alpha \equiv 1 \bmod^{\times}.\mathfrak{f}$. On note $\lambda^{[\rho]}$ le Grössencharakter de M de type $(\nu,0)$ et conducteur $\mathfrak{f}^{\rho}$, défini par $\lambda^{[\rho]}(\mathfrak{a}) = \lambda(\mathfrak{a}^{\rho})^{\rho}$ si $(\mathfrak{a},\mathfrak{f}^{\rho}) = 1$.

Hecke et Shimura (voir [4] et [13]) ont montré que $\theta(\lambda) = \sum_{(\mathfrak{a},\mathfrak{f})=1} \lambda(\mathfrak{a})\, \mathbf{q}^{\mathbf{N}\mathfrak{a}}$ ($\mathbf{q} = e^{2i\pi z}$) est une forme parabolique de poids k et $\Gamma_1(N)$-modulaire ($k = \nu+1$, $N = D.\mathbf{N}\mathfrak{f}$) qui est propre pour tous les opérateurs de Hecke et vérifie $\theta(\lambda)|_k\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} = \varepsilon.\theta(\lambda^{[\rho]})$, où $\varepsilon \in \mathbb{C}^{\times}$ est de module 1. Elle est donc primitive au sens d'Atkin-Lehner-W.Li.

On peut attacher à cette forme des périodes U_{λ} et $U^{\lambda} \in \mathbb{C}^{\times}$ commensurables au carré de Petersson $\langle \theta(\lambda),\theta(\lambda) \rangle$ (cf. [7]) et on montre que le nombre

$$H(\lambda) = \frac{L(\lambda\lambda^{[\rho]},k)}{\pi^{k}(U_{\lambda}U^{\lambda})^{\frac{1}{2}}}$$

est algébrique et en fait que $H(\lambda)^2$ est dans le corps de nombres M_{λ} engendré par M et les valeurs de λ. Expliquons rapidement la définition de U_{λ}, U^{λ} dans le cas où $\nu = 1$: soit $X = X_1(N)$; les 1-formes $\omega_{\lambda} = \theta(\lambda)\,dz$ et $\overline{\omega}_{\lambda}$ définissent des classes de cohomologie dans $H^1(X,\mathbb{C})$. Soit W_{λ} le $\mathbb{C}$-sous-espace engendré par $B_{\lambda} = \{\omega_{\lambda},\overline{\omega}_{\lambda}\}$. Soit $\mathcal{O}_{M_{\lambda}}$ l'anneau des entiers de M_{λ}; $L = H^1(X,\mathcal{O}_{M_{\lambda}})$ est un réseau de $H^1(X,\mathbb{C})$ et $L = L \cap W_{\lambda}$ est un réseau de W_{λ} ainsi que $L^{\lambda} = 1_{\lambda}L$, où 1_{λ} est la projection sur W_{λ} orthogonale relativement au cup-produit de $H^1(X,\mathbb{C})$. En première approximation, on prend pour U_{λ}, resp. U^{λ}, le déterminant de la matrice de passage de B_{λ} à "un" système $\mathcal{O}_{M_{\lambda}}$-libre de L_{λ}, resp. L^{λ}. Une définition plus rigoureuse pour $\mathfrak{U}_{\lambda}$ (resp. $\mathfrak{U}^{\lambda}$) est le sous-$\mathcal{O}_{M_{\lambda}}$-module de $\mathbb{C}$ engendré par tous les déterminants de ce type. Ces modules sont projectifs de rang 1 et $H(\lambda)^2_{-}$ est un idéal fractionnaire de M_{λ}. La définition serait analogue pour $\nu > 1$ mais ferait intervenir l'espace de cohomologie $H^1(X,F_k)$ où F_k est un faisceau localement constant non constant.

Soit maintenant p premier, $p \nmid 6hN\varphi(N)$, et $\mathfrak{P}$ une place de $\overline{\mathbb{Q}}$ au-dessus de p.

Proposition 1. $H(\lambda)$ est entier en $\mathfrak{P}$.

On utilise ce nombre dans les critères suivants :

A. Critère de congruences : Soient $f = \sum_{n=1}^{\infty} a_n q^n$, $g = \sum_{n=1}^{\infty} b_n q^n$ des formes dans $S_k(\Gamma_1(M))$ propres et normalisées $(a_1 = b_1 = 1)$. Leurs coefficients sont des entiers algébriques (Shimura [13] 8.4). On note $f \equiv g \bmod. \mathfrak{P}$ la famille de congruences $a_n \equiv b_n \bmod. \mathfrak{P}, \forall n \geq 1$.

Proposition 2. (Ribet-Hida). $\mathfrak{P} | H(\lambda) \iff (\exists g$ propre normalisée $\in S_k(\Gamma_1(Np))$, $g \neq \theta(\lambda)^\sigma$ pour tout $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$ et $g \equiv \theta(\lambda) \bmod. \mathfrak{P})$.

B. Critère Kummérien : Il y a un lien de $H(\lambda)$ avec l'arithmétique de M. Ce critère dû à Hida ([5] Théorème 0.1) s'énonce comme suit :

Faisons les hypothèses :

D est impair, $\nu > 1$, $(\mathfrak{f},\mathfrak{f}^\rho) = 1$, $p \nmid 6N\varphi(N)h$ $p > k$ et p décomposé en $\mathfrak{p}$ et $\mathfrak{p}^\rho$ dans M.

Soit $\mathfrak{P}$ place de $\overline{\mathbb{Q}}$ au-dessus de $\mathfrak{p}$, ceci détermine un plongement de $\overline{\mathbb{Q}}$ dans $\mathbb{C}_p$. Notons K l'adhérence de M_λ dans $\mathbb{C}_p$, $\mathcal{O}_K$ son anneau des entiers, $\tilde{\mathcal{O}}_K$ sa réduction. Soit $\tilde{\lambda} = G_M \longrightarrow \mathcal{O}_K^\times$ (resp. $\tilde{\lambda} : G \longrightarrow \tilde{\mathcal{O}}_K^\times$ sa réduction), le caractère de Weil attaché à λ (cf. [16]), où G_L est le groupe de Galois absolu du corps L.

Théorème 3. Si $\mathfrak{P} | H(\lambda)$, il existe $\pi : G_M \longrightarrow GL_2(\tilde{\mathcal{O}}_K)$ telle que

(i) $\pi(\sigma) = \begin{pmatrix} \tilde{\lambda}(\sigma) & a(\sigma) \\ 0 & \tilde{\lambda}_\rho(\sigma) \end{pmatrix}$

(ii) π est non-semi-simple (i.e. $a(G_M) \neq 0$)

(iii) π est non-ramifié hors de $\mathfrak{p}$ sur le corps $M_{\mathfrak{N}\mathfrak{f}.p}$ des rayons de conducteur $\mathfrak{f}.p$.

Pour formuler en corollaire un résultat d'arithmétique de M, on introduit l'extension abélienne d'exposant p non-ramifiée hors de $\mathfrak{p}$ maximale de $M_{\mathfrak{N}\mathfrak{f}.p}$, soit N_0. Notons $X_0 = \mathrm{Gal}(N_0/M_{\mathfrak{N}\mathfrak{f}.p})$ et $\Delta = \mathrm{Gal}(M_{\mathfrak{N}\mathfrak{f}.p}/M)$. Considérons le caractère $\kappa = \frac{\tilde{\lambda}}{\tilde{\lambda}^\rho} : \Delta \longrightarrow \tilde{\mathcal{O}}_K$ et $X_0^{(\kappa)}$ la partie de $X_0 \otimes_{\mathbb{F}_p} \tilde{\mathcal{O}}_K$ sur laquelle Δ agit via le caractère κ. C'est alors un exercice facile de déduire du théorème 3 le

Corollaire 4. $\mathfrak{P} | H(\lambda) \Rightarrow X_0^{(\kappa)} \neq 0$.

On se propose de généraliser ce critère à la $\mathbb{Z}_p$-extension anticyclotomique de $M_{\mathfrak{N}\mathfrak{f}.p}$. L'ingrédient pour ça est la théorie d'Iwasawa de l'algèbre de Hecke ordinaire édifiée par H. Hida dans [6] et [7]. On en rappelle les principaux résultats dans le paragraphe suivant.

2 - Théorie d'Iwasawa de l'algèbre de Hecke ordinaire.

Soit $\Lambda_K = \mathcal{O}_K[[T]]$.

Soit $\ell \geq 1$, $r \geq 1$. On a une injection $\mathbb{C}$-linéaire $S(\Gamma_1(Np^r)) \longrightarrow \mathbb{C}[[\mathbf{q}]]$ donnée par le q-développement à l'infini. Soit $S_\ell(\Gamma_1(Np^r), \mathbb{Z})$ l'image réciproque de $\mathbb{Z}[[\mathbf{q}]]$. C'est un $\mathbb{Z}$-module libre de rang $\dim_{\mathbb{C}} S_\ell(\Gamma_1(Np^r))$. On pose

$$S_{\ell,r} = S_\ell(\Gamma_1(Np^r)) \otimes \mathcal{O}_K$$

Soit $r \geq 1$ fixé et $S_{\infty,r} = \mathcal{O}_K[[\mathbf{q}]] \cap \bigoplus_{\ell>0} (S_{\ell,r} \otimes K)$ (où $S_{0,r} = \mathcal{O}_K$). On munit $\mathcal{O}_K[[\mathbf{q}]]$ de la topologie de la valeur absolue $|\sum_{n=1}^{\infty} a_n q^n| = \operatorname{Sup}_{n>1} |a_n|_p$. N. Katz (cf. [8]) a montré que les inclusions $S_{\infty,r} \subset S_{\infty,r'}$, (pour $r \leq r'$) donnent des égalités par passage à l'adhérence dans la topologie induite par celle de $\mathcal{O}_K[[\mathbf{q}]]$: $\overline{S}_{\infty,r} = \overline{S}_{\infty,r'}$. On note $\overline{S}$ la valeur commune de ces espaces. On l'appelle espace des formes modulaires paraboliques p-adiques. Pour $\ell \geq 1$, $r \geq 1$ fixés, on a donc $S_{\ell,r} \subset \overline{S}$. Posons alors :

$$S_{\ell,\infty} = \bigcup_{r \geq 0} S_{\ell,r}.$$

Un théorème de Ohta (cf. [10]) montre en fait que $S_{\ell,\infty}$ est dense dans $\overline{S}$, nous n'en aurons cependant pas usage car nous nous cantonnerons aux parties ordinaires de ces modules sur lesquelles on a des résultats plus précis.

$$\text{Soit } Z = \varprojlim_r (\mathbb{Z}/Np^r\mathbb{Z})^\times = Z_1 \times \Gamma \quad \text{où} \quad \begin{cases} Z_1 & \text{est le facteur} \simeq (\mathbb{Z}/Np\mathbb{Z}) \\ \Gamma & \text{est le facteur} \simeq \mathbb{Z}_p^+ \end{cases}$$

On définit une action de Z sur $S_{\infty,r} \otimes K$ comme suit : Soit $z = (z_1, z_2)$ dans Z et $f \in S_{\ell,r} \otimes K$, soit $\sigma_z \in \Gamma_0(Np^r)$ telle que $\sigma_z \equiv \begin{pmatrix} z^{-1} & 0 \\ 0 & z \end{pmatrix}$ mod. Np^r, alors $f|\langle z\rangle_0 = z_2^\ell \times f|_\ell \sigma_z$. Katz a montré que cette action laisse stables $S_{\ell,r}$ et $S_{\infty,r}$. Par continuité on a donc une action de Z sur $\overline{S}$ (dite diamant de poids 0). On sait que les opérateurs de Hecke laissent stables les $S_{\ell,r} \otimes K$. Or pour q premier, $f = \sum_{n \geq 1} a(n,f)\mathbf{q}^n \in S_{\ell,r} \otimes K$.

$$\text{on a :} \quad a(n, f|T(q)) = \begin{cases} a(nq,f) + q^{-1} a(n/q, f|\langle q\rangle_0 & \text{si } q \nmid Np \\ a(nq,f) & \text{si } q \mid Np. \end{cases}$$

Par conséquent, les $T(q)$ laissent stables $S_{\ell,r}$ et $S_{\infty,r}$ et opèrent donc sur $\overline{S}$. On note $h_{\ell,r}$ (resp. $h = h_{\infty,r}$, pour $r \geq 1$) la $\mathcal{O}_K$-algèbre engendrée par les opérateurs de Hecke vus comme endomorphismes de $S_{\ell,r}$ (resp. de $\overline{S}$). On a la

Proposition 5.
$$\overline{S} \times h \longrightarrow \mathcal{O}_K$$
$$(f,T) \longmapsto \langle f,T\rangle = a(1,f|T)$$

est un accouplement $\mathcal{O}_K$-linéaire parfait tel que $\langle f|T,T'\rangle = \langle f,TT'\rangle$ induisant donc un isomorphisme de h-modules :

$$h \xrightarrow{\sim} \mathrm{Hom}(\overline{S},\mathcal{O}_K)$$
$$T \longmapsto (f \longmapsto \langle f,T\rangle)$$

Remarquons de plus que h contient l'image de $\mathbb{Z}$ par $z \longmapsto \langle z\rangle_0$. En particulier, h est un $\mathcal{O}_K[\Gamma]$-module compact, donc est un $\mathcal{O}_K[[\Gamma]]$-module. On identifie $\mathcal{O}_K[[\Gamma]]$ avec $\Lambda_K = \mathcal{O}_K[[T]]$ par $\langle 1+Np\rangle_0 \longrightarrow 1+T$. On notera $u = 1+Np$. Pour ℓ et r fixés, $h_{\ell,r}$ est finie et plate sur $\mathcal{O}_K$ donc est semi-locale. Comme $\mathcal{O}_K$ est complet, elle est produit de ses localisées aux idéaux maximaux. Soit $h^0_{\ell,r}$ le produit des composantes locales dans lesquelles $T(p)$ est inversible. Soit $e_{\ell,r}$ son élément unité, on l'appelle l'idempotent ordinaire de $h_{\ell,r}$. On définit de manière analogue l'idempotent ordinaire e de h et on note $h^0 = e.h$.

Théorème 6. h^0 est une $\mathcal{O}_K$-algèbre finie et plate.

De plus comme $\overline{S}_{\ell,\infty} \subset \overline{S}$ et que les opérateurs de Hecke laissent stable $S_{\ell,\infty}$, donc opèrent sur $\overline{S}_{\ell,\infty}$, en notant $h_{\ell,\infty}$ la $\mathcal{O}_K$-algèbre engendrée par tous les opérateurs de Hecke $T(q)$, q premier, on a un morphisme surjectif de Λ_K-algèbres : $h \xrightarrow{\alpha} h_{\ell,\infty}$ (c'est l'identité en utilisant Ohta). En utilisant des techniques élémentaires (du style du chapitre 8 de [13]), Hida [7] montre que α induit un isomorphisme

Théorème 7. $eh \xrightarrow{\underset{\sim}{\alpha}} eh_{\ell,\infty}$.

On note h^0 cette algèbre de Hecke.

Soit $\ell \geq 2$, ε un caractère de Γ de conducteur divisant p^r $(r \geq 0)$ et posons
$$S_{\ell,r}(\varepsilon) = \{f \in S_{\ell,r};\ \forall \gamma \in \Gamma,\ f|\langle\gamma\rangle_0 = \varepsilon(\gamma).f\}$$

$h_{\ell,\varepsilon} = \mathcal{O}_K$-algèbre engendrée par les opérateurs de Hecke comme endomorphismes de $S_{\ell,r}(\varepsilon)$.

Remarquons que $S_{\ell,r} \otimes K = \bigoplus_{\mathrm{Cond}(\varepsilon)|p^r} S_{\ell,r}(\varepsilon) \otimes K$ et $h_{\ell,r} \otimes K = \prod_{\mathrm{Cond}(\varepsilon)|p^r} h_{\ell,\varepsilon} \otimes K$.

Posons $P_{\ell,\varepsilon} = 1+T-\varepsilon(u)u^{\ell}$.

Théorème 8. (de contrôle) : L'inclusion $e\,S_{\ell,r}(\varepsilon) \subset e\,\overline{S}$ fournit un morphisme de $\mathcal{O}_K$-algèbres surjectif évident

$$h^o/P_{\ell,\varepsilon}\, h^o \longrightarrow h^o_{\ell,\varepsilon}.$$

C'est un isomorphisme.

Corollaire 9. Soit $\omega_{\ell,r} = (1+T)^{p^{r-1}} - u^{\ell p^{r-1}}$ si $r \geq 1$ l'inclusion $eS_{\ell,r} \subset e\,\overline{S}$ fournit un morphisme surjectif évident de $\mathcal{O}_K$-algèbres :

$$h^o/\omega_{\ell,r}\, h^o \longrightarrow h^o_{\ell,r}.$$

C'est un isomorphisme.

3 - Module de congruences adapté à notre situation.

Notons $C\ell_{\mathfrak{f}\mathfrak{p}^r}$ le groupe des classes de rayons de M de conducteur $\mathfrak{f}\mathfrak{p}^r$ pour $r \geq 1$ fixé. Soit $C\ell_{\mathfrak{f}\mathfrak{p}^\infty} = \varprojlim_r C\ell_{\mathfrak{f}\mathfrak{p}^r}$; comme $p \nmid h$, ce groupe profini admet une décomposition naturelle en produit de deux groupes :

$$\begin{array}{ccc} C\ell_{\mathfrak{f}\mathfrak{p}^\infty} & \xrightarrow{\sim} & C\ell_{\mathfrak{f}\mathfrak{p}} \times (1+\mathfrak{f}\hat{\mathfrak{p}}) \\ x & \longmapsto & (x_1, x_2) \end{array}$$

où $1 + \mathfrak{f}\hat{\mathfrak{p}} = \varprojlim_r (1+\mathfrak{f}\mathfrak{p})/(1+\mathfrak{f}\mathfrak{p}^r)$.

Il est clair de plus que l'ensemble I des idéaux de $\mathcal{O}$ premiers à $\mathfrak{f}\mathfrak{p}$ s'injecte dans $C\ell_{\mathfrak{f}\mathfrak{p}^\infty}$.

Soit
$$\begin{array}{rccl} \theta : & C(C\ell_{\mathfrak{f}\mathfrak{p}^\infty}, \mathcal{O}_K) & \longrightarrow & \overline{S} \\ & \varphi & \longmapsto & \sum_{a \in I} \varphi(a) q^{Na} \in \mathcal{O}_K[[q]] \end{array}$$

où $C(C\ell_{\mathfrak{f}\mathfrak{p}^\infty}, \mathcal{O}_K)$ désigne le $\mathcal{O}_K$-module des applications continues du groupe profini $C\ell_{\mathfrak{f}\mathfrak{p}^\infty}$ vers $\mathcal{O}_K$. L'image de θ est dans $\overline{S}$ car le $\mathcal{O}_K$-module engendré par les prolongements par continuité des Grössencharakter $I \longrightarrow M_\lambda$ de conducteur $|\mathfrak{f}\mathfrak{p}$ et de type $(\nu',0)$ $(\nu',0)$ $\nu' = 1,2\ldots$ est dense dans $C(C\ell_{\mathfrak{f}\mathfrak{p}^\infty}, \mathcal{O}_K)$ et le théorème de Hecke et Shimura cité au paragraphe 1 montre que son image est dans $\overline{S}$. Par dualité $\mathcal{O}_K$-linéaire et application de la Proposition 5 et du Théorème de Mahler [9], on obtient un morphisme de $\mathcal{O}_K$-algèbres :

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

$$T(q) \longmapsto \begin{cases} [\mathcal{Q}] + [\mathcal{Q}^\rho] & \text{si } q \text{ est décomposé en } \mathcal{Q}\mathcal{Q}^\rho \text{ et } (q,\mathfrak{f}\mathfrak{p}) = 1 \\ 0 & \text{si } q \text{ est inerte} \\ [\mathcal{Q}] & \text{si } q \text{ est ramifié ou décomposé en } \mathcal{Q},\mathcal{Q}^\rho \text{ et } \\ & \mathcal{Q}^\rho \mid \mathfrak{f}\mathfrak{p}. \end{cases}$$

En outre $\theta^*(\langle q\rangle_0) = (\frac{-D}{q}).q.[(q)]$. Notons de plus que $\theta^*(T(p)) = [\mathfrak{p}^\rho]$ qui est inversible.

Considérons le morphisme d'algèbres

$$\begin{aligned} \eta : \mathcal{O}_K[[C\ell_{\mathfrak{f}\mathfrak{p}^\infty}]] &\longrightarrow \Lambda_K \\ z = (z_1,z_2) &\longmapsto \hat{\lambda}(z_1)z_2^{-1}(1+T)^\alpha \\ z_2 = u^\alpha & \end{aligned}$$

Posons $\chi = \eta \circ \theta^*$. On a $\chi(T(p)) = \eta([\mathfrak{p}^\rho]) \in \Lambda_K^\times$. Or, l'algèbre h^0 jouit de la propriété universelle suivante (très facile à vérifier en utilisant la définition de h comme limite projective de $\mathcal{O}_K$-algèbres finies) pour toute $\mathcal{O}_K$-algèbre locale et tout morphisme α de $\mathcal{O}_K$-algèbres $\alpha : h \longrightarrow A$ tel que $\alpha(T(p)) \in A^\times$, il existe un unique morphisme de $\mathcal{O}_K$-algèbres $\alpha^0 : h^0 \longrightarrow A$ tel que $\alpha = \alpha^0 \circ e$, e désignant le morphisme $h \longrightarrow h^0$ de multiplication par l'idempotent ordinaire e. On applique ceci à $\alpha = \chi$ et on a en fait le résultat plus précis (où l'on note encore $\alpha^0 = \chi : h^0 \longrightarrow \Lambda_K$) :

<u>Proposition 10</u>. $\chi : h^0 \longrightarrow \Lambda_K$ est un morphisme de Λ_K-algèbres. Si $\mathcal{L}_K$ est le corps des fractions de Λ_K, on a $h^0 \otimes \mathcal{L}_K \simeq \mathcal{L}_K \oplus A$, la première projection s'identifiant à χ.

Comme d'autre part h^0 est une algèbre finie sur l'anneau local complet Λ_K, elle est semi-locale, produit de ses localisées aux idéaux maximaux. Soit R la composante locale à travers laquelle χ se factorise.

Il est clair que R est finie et plate et $R \otimes \mathcal{L}_K \simeq \mathcal{L}_K \oplus \mathcal{B}$.

<u>Notation 11</u>. Soient

$$\begin{aligned} R_1 &= \mathrm{Im}\,(R \xrightarrow{pr_1} \mathcal{L}_K) \\ \mathfrak{C}_1 &= \mathrm{Ker}(R \xrightarrow{pr_2} \mathcal{B}) \\ R_2 &= \mathrm{Im}\,(R \xrightarrow{pr_2} \mathcal{B}) \\ \mathfrak{C}_2 &= \mathrm{Ker}(R \xrightarrow{pr_1} \mathcal{L}_K). \end{aligned}$$

Soit $\mathfrak{C} = \mathfrak{C}_1 \oplus \mathfrak{C}_2$ et $R^* = R_1 \oplus R_2$. Remarquons que $pr_1 \times pr_2$ fournit une inclusion $R \hookrightarrow R_1 \oplus R_2 = R^*$

<u>Lemme 12</u>. L'idéal $\mathfrak{C}$ est le conducteur de l'ordre R^* dans R et on a des isomorphismes naturels de Λ_K-modules déduits des inclusions $R_1 \xhookrightarrow{i_1} R^* \xhookleftarrow{i_2} R_2$ et des

projections $R_1 \xleftarrow{pr_1} R \xrightarrow{pr_2} R_2$:

$$R/\mathfrak{C} \xrightarrow[\sim]{pr_1} R_1/\mathfrak{C}_1 \xrightarrow[\sim]{i_1} R^*/R \xleftarrow[\sim]{i_2} R_2/\mathfrak{C}_2 \xleftarrow[\sim]{pr_2} R/\mathfrak{C}.$$

Définition fondamentale. Le Λ_K-module décrit par les isomorphismes ci-dessus est appelé le module de congruences attaché au couple $(\lambda,\mathfrak{P})$ et noté C.

Proposition 13. Le Λ_K-module C est de type fini de torsion et est isomorphe à $\Lambda_K/H\Lambda_K$. Il n'a donc pas de sous-module-pseudo-nul non nul.

Preuve. On a $R_1 = \Lambda_K$ donc $\mathfrak{C}_1$ est un idéal de Λ_K. Or, $\mathfrak{C}_1 = L_K \cap R$ c'est donc l'intersection d'un sous-espace vectoriel de $R \otimes L_K$ avec un Λ_K-module réflexif : il est réflexif et donc libre sur l'anneau Λ_K régulier de dimension 2. Donc $\mathfrak{C}_1 = H\Lambda_K$.

Un élément H comme dans la proposition 13 est une série caractéristique de C. La série H satisfait les propriétés faibles d'interpolation suivantes (faibles car elles ne donnent que l'égalité des valuations p-adiques des deux membres). Si ε est un caractère de Dirichlet de M de conducteur $\mathfrak{p}^r$ et d'exposant p-primaire, on peut l'évaluer sur $u = 1 + Np$ vu comme générateur du p-Sylow de $C\ell_{\mathfrak{p}^r}$, et on a

Théorème 14 ([7] Théo. III).

(i) Si ε est non trivial,

$$(*) \qquad H(\varepsilon(u)u^k-1) \sim p^{2r-1} \frac{L(\lambda\lambda^{[\rho]}\varepsilon\varepsilon^{[\rho]},k)}{\pi^k(U_{\lambda\varepsilon}U^{\lambda\varepsilon})^{\frac{1}{2}}}$$

où le tilde signifie "différer par une unité p-adique" et où les périodes $U_{\lambda\varepsilon}U^{\lambda\varepsilon}$ ont une définition analogue à celle de U_λ, U^λ en remplaçant $\theta(\lambda)$ par $\theta(\lambda\varepsilon)$, et où en appelant $H(\lambda\varepsilon)$ le second membre de (*), on a : $H(\lambda\varepsilon)^2 \in M_{\lambda\varepsilon}$ engendré par M et les valeurs de $\lambda\varepsilon$.

(ii) Si ε est trivial

$$H(u^k-1) \sim H(\lambda).$$

Remarques : 1) On a évidemment, pour $P_{k,\varepsilon} = 1 + T - \varepsilon(u)u^k$,

$$(C : P_{k,\varepsilon}C)^2 \sim N_{K_\varepsilon/\mathbb{Q}_p} H(\lambda\varepsilon)^2$$

où K_ε est l'adhérence $\mathfrak{P}$-adique de $M_{\lambda\varepsilon}$ et le tilda signifie "diffère par une unité $\mathfrak{P}$-adique de".

2) En fait $C/P_{k,\varepsilon}C$ s'identifie au "module de congruences" attaché à $\theta(\lambda\varepsilon) \in S_k(\Gamma_1(Np^r),K)$ comme dans Doi-Ohta [3]. Le Λ_K-module C interpole donc les

groupes de congruences des $\theta(\lambda\varepsilon)$, ε variant. La proposition suivante explique alors en quel sens ce module généralise la Proposition 2 à la famille $\{\theta(\lambda\varepsilon)\}_\varepsilon$:

Proposition 15.

$$\mathfrak{p}|H(\lambda) \Longleftrightarrow C \neq 0 \Longleftrightarrow \mathfrak{p}|H(\lambda\varepsilon), \forall\varepsilon \Longleftrightarrow \begin{pmatrix} \forall\varepsilon, \exists g_\varepsilon \text{ propre normalisée dans } S_k(\Gamma_1(Np^r)) \text{ t.q.} \\ g_\varepsilon \neq \theta(\lambda\varepsilon)^\sigma \ \forall\sigma\in \mathrm{Aut}(\mathbb{C}) \text{ et } g_\varepsilon \equiv \theta(\lambda\varepsilon) \bmod. \mathfrak{p} \end{pmatrix}$$

Remarque : On doit considérer le couple (C,H) comme un analogue du couple (Y,G) où Y est le module analytique de Coates-Wiles-Yager, i.e. $\frac{\text{(unités semi-locales en } \mathfrak{p})}{\text{(adhérence des unités elliptiques)}}$, spécialisé à la $\mathbb{Z}_p$-extension cyclotomique du corps des rayons $M_{\mathfrak{N}f.p}$ et G est la spécialisation à la variable anticyclotomique de la série L p-adique à deux variables de Katz-Yager (cf. [2], [17]). L'étude des périodes de $U_{\lambda\varepsilon}$, $U^{\lambda\varepsilon}$ et de leur lien avec celles de Katz-Yager doit permettre de montrer au moins que les invariants λ et μ d'Iwasawa des séries H et G coïncident. L'objet du présent travail est d'exposer le résultat exprimant le lien du couple (C,H) et d'un couple (X,F) constitué d'un module d'Iwasawa galoisien lié à M et de sa série caractéristique définis au paragraphe suivant.

4 - Théorie d'Iwasawa classique.

Soit $\Delta = \mathrm{Gal}(M_{\mathfrak{N}f.p}/M)$, $\kappa : \dfrac{\hat\lambda}{\hat\lambda^\rho} : \Delta \longrightarrow \mathcal{O}_K^\times$.

Soit M_∞ la $\mathbb{Z}_p$-extension de M non ramifiée hors de $\mathfrak{p}$,
M_∞^- la $\mathbb{Z}_p$-extension de M anticyclotomique.

C'est-à-dire que c'est la pro-p-extension abélienne, diédrale sur $\mathbb{Q}$, maximale, de M.

Soit $M_{\mathfrak{N}f.p^\infty}$ la réunion des corps de rayons de M de conducteur $\mathfrak{N}f.p^r$, $r = 1,2\ldots$.

Soit $M'_\infty = M_\infty M_{\mathfrak{N}f.p}$ et $M'^-_\infty = M^-_\infty M_{\mathfrak{N}f.p}$. Soit $\Gamma^- = \mathrm{Gal}(M'^-_\infty/M_{\mathfrak{N}f.p})$.

Soit N la pro-p-extension abélienne non ramifiée hors de $\mathfrak{p}$ de M'^-_∞ et $X = \mathrm{Gal}(N/M'^-_\infty)$. Le groupe $\Delta\times\Gamma^-$ opère sur X. Soit $X^{(\kappa)}$ la partie de $X \otimes_{\mathbb{Z}_p} \mathcal{O}_K$ sur laquelle Δ opère par κ.

Proposition 16 (B. P.-R. [11]) $X^{(\kappa)}$ est un $\mathcal{O}_K[[\Gamma^-]]$-module de type fini et de torsion.

On identifie alors $\mathcal{O}_K[[\Gamma^-]]$ avec Λ_K de la manière suivante. Fixons pour générateur topologique de $\mathrm{Gal}(M'_\infty/M_{\mathfrak{N}f.p})$ l'élément γ image de $u \in C\ell_{\mathfrak{p}^\infty}$ par la Loi de Réciprocité d'Artin. Soit τ l'unique élément de $\mathrm{Gal}(M_{\mathfrak{N}f.p^\infty}/\mathfrak{N}f.p)$ tel que

$\tau^{\rho} = \tau^{-1}$ et $\tau|_{M'_\infty} = \gamma^{\frac{1}{2}}$. On prend $\tau|_{M'_\infty}$ pour générateur topologique et on l'envoie sur $1+T$.

Soit maintenant $F \in \Lambda_K$ une série caractéristique de $X^{(\kappa)}$. Le théorème qui nous occupe dans cet exposé est :

Théorème 17. Tout facteur premier de H dans Λ_K divise

$$F(u^{-1}(1+T)-1).$$

Lien avec le Corollaire 4 : On a $X_0^{(\kappa)} = X^{(\kappa)}/\mathfrak{m}X^{(\kappa)}$ où $\mathfrak{m}$ est l'idéal maximal de Λ_K. Donc d'après le théorème 17, (H non unité) $\Rightarrow$ (F non unité), ce qui entraîne le Corollaire 4.

5 - Schéma de la démonstration.

Rappelons que $C \simeq \Lambda_K/H\Lambda_K \longrightarrow R_2/\mathfrak{C}_2$.

L'idéal $\mathfrak{C}_2$ est donc au-dessus de $H\Lambda_K$ via le morphisme fini d'algèbres $\Lambda_K \longrightarrow R_2$. De plus, au-dessus d'un facteur premier P de H, il y a un unique idéal premier $\mathfrak{p}$ et la composante $\mathfrak{p}$-primaire de $\mathfrak{C}_2$ est donc bien définie (cf. [1] Théorème 4.9). On la note $\mathfrak{Q}$. Pour un tel $P|H$ fixé, on va construire un morphisme de groupes

$$a_P : \mathrm{Gal}(\overline{M}/M_{\mathbb{N}f.p^\infty}) \longrightarrow \mathfrak{Q}/_{\mathfrak{Q}^2} \quad \text{tel que}$$

(i) Pour $\tau \in \mathrm{Gal}(M_{\mathbb{N}f.p^\infty}/M_{\mathbb{N}f.p})$ l'élément défini précédemment, et pour tout $\sigma \in \mathrm{Gal}(\overline{M}/M_{\mathbb{N}f.p^\infty})$ on a $a_P(\sigma^\tau) = u^{-1}(1+T)a_P(\sigma)$.

Pour tout $\sigma \in \mathrm{Gal}(\overline{M}/M_{\mathbb{N}f.p^\infty})$ et tout $\delta \in \Delta$

$$a_P(\sigma^\delta) = \kappa(\delta).a_P(\sigma).$$

(ii) $\mathrm{Im}\, a_P$ n'est pas pseudo-nulle.

(iii) a_P est non-ramifiée hors des places au-dessus de $\mathfrak{p}$.

Noter l'analogie des assertions (i) (ii) (iii) avec les assertions (i) (ii) (iii) du Théorème 3.

Une fois cet homomorphisme construit, on peut le factoriser en un morphisme de Λ_K-algèbres, d'image non pseudo-nulle :

$$X^{(\kappa)}(1) \longrightarrow \mathfrak{Q}/_{\mathfrak{Q}^2}.$$

Or la série caractéristique de $\mathfrak{Q}/_{\mathfrak{Q}^2}$ est une puissance de P (c'est un quotient de

$C(P)^n$ où $C(P) = C/_{\mathbb{Q}}C = \Lambda_K/_{p^e\Lambda_K}$ si $p^e || H)$, tandis que la série caractéristique de $X^{(\kappa)}(1)$ est $F(u^{-1}(1+T)-1)$. Le Théorème 17 résulte donc de l'existence de a_p.

Remarquons encore, concernant la condition (ii) requise pour a_p, que la non-nullité de $\mathrm{Im}\, a_p$ ne serait pas suffisante pour notre objet car $\mathbb{Q}/_{\mathbb{Q}^2}$ peut contenir des sous R_2-modules pseudo-nuls non nuls.

Il se peut en effet que R_2 ne soit pas normal donc sûrement pas régulier (si $\mathbb{B}$ n'est pas un corps, R_2 n'est pas normal) et on a un exemple simple d'extension finie et plate de $\mathbb{Z}_p[[T]]$, normale et non régulière, avec un idéal primaire plat sur Λ_K dont le carré n'est pas plat sur Λ_K et tel que $\mathbb{Q}/_{\mathbb{Q}^2}$ contienne un sous-module pseudo-nul non-nul : $R_2 = \mathbb{Z}_p[[T,X]]/(X^2-pT)$, $\mathbb{Q} = (T,X)$, $\mathbb{Q}^2 = (T) \cap (p,T,X)^2$, $\mathbb{Q}^{(2)} = (T)$, $\mathbb{Q}^{(2)}$ désignant le carré symbolique de $\mathbb{Q}$ (cf. [1]) et $\mathbb{Q}^{(2)}/_{\mathbb{Q}^2}$ est non-nul et pseudo-nul.

La construction de a_p suit le plan que voici :

Soit $X_r = X_1(Np^r)/\mathbb{Q}$, $J_r = \mathrm{Pic}^0(X_r/\mathbb{Q})$

On introduit le $G_{\mathbb{Q}}$-module et h-module (les deux actions commutant) :

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

On prend la R-partie de ce module notée $J_r(R)$. C'est un R et un $G_{\mathbb{Q}}$-module. Notre point de départ est le module

$$J(R) = \varinjlim_r J_r(R),$$ la limite étant prise pour les revêtements $X_{r'} \longrightarrow X_r$ si $r' \geq r$, donnant par application de Pic^0 : $J_r \longrightarrow J_{r'}$.

<u>Proposition 18</u> (cf. [7] et [14]).

(1) R est de Gorenstein et R_2 est plat sur Λ_K.

(2) $J(R)$ est colibre de rang 2 sur R.

(3) Comme R est une Λ_K-algèbre, on peut parler de la $\omega_{2,r}$-torsion de $J(R)$, où $\omega_{2,r} = (1+T)^{p^{r-1}} - u^{2p^{r-1}}$ et on a :

$$\forall r \geq 1, \quad J_r(R) \longrightarrow J(R) \quad \text{et} \quad J_r(R) = J(R)[\omega_{2,r}]$$

Comme l'assertion 2, entraîne que $J(R)$ est Λ_K-divisible on peut appliquer les idempotents 1_i de R^*, élément unité de R_i. On pose

<u>Définition 19</u>. $A = 1_1\, J(R)$, $B = 1_2\, J(R)$.
Ce sont des $G_{\mathbb{Q}}$ et des R-modules, on a $A + B = J(R)$.

Notons M^* le dual de Pontryagin du R-module M. On a la

Proposition 20.
$$A^* \simeq \Lambda_K \oplus \Lambda_K$$
$$B^* \simeq R_2 \oplus R_2$$
$$(A \cap B)^* \simeq C \oplus C$$

En particulier $A \cap B = A[H] = B[\mathfrak{C}_2]$.

Cette dernière égalité est cruciale pour notre construction puisqu'elle égale deux morceaux des groupes Λ_K-divisibles A et B qu'on peut qualifier, le premier de type C.M. par M et le second de module sans multiplication complexe par M, au sens de la

Proposition 21. (i) $A^* \simeq (\mathrm{Ind}_{\mathbb{Q}}^{M} \Lambda_K(\phi))'$

(ii) B^* ne contient pas de vecteur propre non nul pour G_M.

Explication : Soit $\phi : G_M \xrightarrow{\mathrm{Res}} \mathrm{Gal}(M_{p^\infty}/M) \xrightarrow{\sim} C\ell_{\mathfrak{f}\mathfrak{p}^\infty} \xrightarrow{\eta} \Lambda_K^\times$.

$\Lambda_K(\phi)$ désigne le Λ_K-module libre de rang 1 sur lequel G_M opère par ϕ, et $\mathrm{Ind}_{\mathbb{Q}}^{M} \Lambda_K(\phi) = \Lambda_K G_{\mathbb{Q}} \otimes_{\Lambda_K G_M} \Lambda_K(\phi)$ est le Λ_K-module libre de rang 2 induit de M à $\mathbb{Q}$. Enfin le prime indique le passage à la contragrédiente et l'isomorphisme est $\Lambda_K G_{\mathbb{Q}}$-linéaire. Un corollaire évident de (i) est que sur G_M on a la décomposition de A^* en somme de deux Λ_K-droites stables avec action par ϕ^{-1} et $\phi^{-\rho}$. Au contraire, (ii) affirme que rien de tel ne se produit pour B. Pour la preuve, voir [15].

On déduit de la Proposition 20 que $B[\mathbb{Q}] = X \oplus Y$ où $X^* \simeq Y^* \simeq C(P)$ comme Λ_K-modules et l'action de G_M sur X (resp. Y) est via ϕ (resp. via ϕ^ρ défini par $\phi^\rho(\sigma) = \phi(\rho\sigma\rho)$). Au vu de la Proposition 21, ceci ne saurait durer pour la torsion de B tuée par un idéal plus petit que $\mathbb{Q}$. C'est pourquoi on forme $B^{(1)} = B/Y$.

C'est un $\left\{\begin{array}{l} G_M\text{-module} \\ R_2 \end{array}\right.$ et on a une suite exacte de G_M et R_2-modules :

$$(*) \qquad 0 \longrightarrow X^{(1)} \longrightarrow B^{(1)}[\mathbb{Q}] \longrightarrow Y^{(1)} \longrightarrow 0$$

où $X^{(1)}$ est l'image isomorphe de X dans $B^{(1)}$ et $Y^{(1)}$ est le quotient défini par (*).

Cette suite est scindée sur R_2 (facile), mais pas sur G_M (c'est ce qu'on va voir).

Définissons alors
$$a_P : G_M \longrightarrow \mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)})$$
$$\sigma \longmapsto pr_{X^{(1)}} \circ \sigma_{Y^{(1)}}$$

on a : $a_P(\sigma\sigma') = a_P(\sigma)\phi^\rho(\sigma') + \phi(\sigma)a_P(\sigma')$ d'où un morphisme de groupes par restriction :

$$a_P : G_{M_{\mathbf{N}f.p^\infty}} \longrightarrow \mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)})$$

satisfaisant la condition (i) requise pour a_P.

On montre facilement que $\begin{cases} X^{(1)*} \simeq C(P) \\ Y^{(1)*} \simeq \mathfrak{Q}/\mathfrak{Q}^2 \end{cases}$.

Donc $\mathrm{Hom}_{R_2}(Y^{(1)}, X^{(1)}) \simeq \mathfrak{Q}/\mathfrak{Q}^2$ sur R_2.

On traite alors la non-ramification de a_P hors de p à l'aide du critère de Néron-Ogg-Shafarevitch.

En $\mathfrak{P}_\rho | \mathfrak{p}^\rho$, on procède comme dans Ribet [12] en utilisant [14]. C'est ici qu'intervient le 3) de la Proposition 18.

L'assertion 2) enfin utilise la définition de $\mathfrak{C}$ comme conducteur de R^* dans R : Si Im a_P était pseudo-nulle, on construirait un idéal $\mathfrak{C}$ de R_2 tel que $\mathfrak{Q}^2 \subset \mathfrak{C}$ et $\mathfrak{C}/_{\mathfrak{Q}^2}$ est pseudo-nul, et un isomorphisme I faisant commuter le diagramme :

$$\begin{tikzcd}
 & R_1 \arrow[r] & R_1/\mathfrak{C} \cap R_1 \\
R \arrow[ur, "pr_1"] \arrow[dr, "pr_2"'] & & \\
 & R_2 \arrow[r] & R_2/\mathfrak{C} \arrow[uu, "\wr\ I"']
\end{tikzcd}$$

et par définition de $\mathfrak{C}_2$ on aurait $\mathfrak{C}|\mathfrak{C}_2$, ce qui est impossible car $\mathfrak{Q}$ est la partie $\mathfrak{P}$-primaire de $\mathfrak{C}_2$ donc on aurait dans $R_{2,\mathfrak{P}}$: $\mathfrak{Q}^2 = \mathfrak{Q}$ ce qui est impossible par Nakayama.

BIBLIOGRAPHIE

[1] M. Atiyah, I. Macdonald.- Notes on Commutative algebra, Math. Oxford Institute, 1966.

[2] J. Coates, A. Wiles.- On p-adic L functions and elliptic units, J. Austr. Math. Soc. (Series A) vol. 26 (1978), 1-25.

[3] K. Doi, M. Ohta.- On some congruences between cusp forms on $\Gamma_0(N)$ p. 91-105, in Modular Functions of one variable V, Bonn 1976, Lect. Notes in Math. vol. 601, Springer-Verlag, 1977.

[4] E. Hecke.- Ueber Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktenturcklung. II. Math. Ann. Bd. 114 (1937), 316-351, reproduit in Math. Werke, p. 672-707, Göttingen, Vandenhoek & Ruprecht, 1959.

[5] 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.

[6] H. Hida.- Iwasawa modules attached to congruences of cusp forms, à paraître dans Ann. Scient. de l'E.N.S.

[7] H. Hida.- Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, à paraître dans Inv. Math.

[8] N. Katz.- Higher congruences between modular forms, Ann. of Math. 101 (1975), 332-367.

[9] S. Lang.- Cyclotomic Fields, G.T.M., Springer-Verlag 1978.

[10] M. Ohta.- On ℓ-adic representations attached to automorphic forms, Japan. J. Math. 8 (1982), 1-47.

[11] B. Perrin-Riou.- Thèse d'Etat, Orsay 1984.

[12] K. Ribet.- A modular construction of unramified extensions of $\mathbb{Q}(\mu_p)$, Inv. Math. 34 (1976), 151-162.

[13] G. Shimura.- Introduction to the arithmetic Theory of automorphic functions, Princeton University Press, 1971.

[14] J. Tilouine.- Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke, à paraître au Bull. de la S.M.F.

[15] J. Tilouine.- Théorie d'Iwasawa classique et de l'algèbre de Hecke ordinaire, à paraître.

[16] A. Weil.- On a certain type of characters of the idèle-class group of an algebraic number field. 1955 c in Oeuvres Scientifiques vol. II, Springer-Verlag, 1980.

[17] R. Yager.- On p-adic L-functions with two variables, Ann. of Math. 115 (1982), 411-449.

Jacques TILOUINE
Mathématiques, Bât. 425
Université Paris-Sud
91405 ORSAY Cédex

[16] A. Weil.- On a certain type of characters of the idele-class groupe of an algebraic number field. 1955 c in Oeuvres Scientifiques vol. II, Springer-Verlag, 1980.

[17] R. Yager.- On p-adic L-functions with two variables, Ann. of Math. 115 (1982), 411-449.

Jacques Tilouine
Mathématiques, Bât. 425
Université Paris-Sud
91405 ORSAY CEDEX