ANNALES DE L'INSTITUT FOURIER

BERNADETTE PERRIN-RIOU

Systèmes d'Euler p-adiques et théorie d'Iwasawa

Annales de l'institut Fourier, tome 48, n° 5 (1998), p. 1231-1307

<http://www.numdam.org/item?id=AIF_1998__48_5_1231_0>

Ann. Inst. Fourier, Grenoble
48, 5 (1998), 1231–1307

SYSTÈMES D'EULER p-ADIQUES ET THÉORIE D'IWASAWA

par Bernadette PERRIN-RIOU

L'introduction des systèmes d'Euler par Kolyvagin en 1988 ([Ko90]) a eu des conséquences extrêmement importantes en arithmétique et théorie d'Iwasawa et a donné de nouvelles perspectives de démonstration. À partir d'une famille de nombres de $\mathbb{Q}(\mu_m)$ pour tout entier m vérifiant certaines relations de traces (on l'appelle système d'Euler cyclotomique, il s'agit simplement des $1-\zeta_m$ pour m entier, où ζ_m est une racine de l'unité d'ordre m et $\zeta_{mn}^n = \zeta_m$), Rubin a ainsi pu donner une démonstration élémentaire du théorème de Mazur-Wiles (conjecture d'Iwasawa) reliant la fonction ζ de Kubota-Leopoldt avec les groupes de classes d'idéaux des corps de nombres cyclotomiques. Kolyvagin a utilisé le système d'Euler des points de Heegner pour démontrer la finitude de certains groupes de Shafarevich-Tate. Récemment, Kato a annoncé la construction d'un système d'Euler des "éléments de Beilinson" associé à une courbe elliptique modulaire sur $\mathbb{Q}$, vivant dans la K-théorie de la courbe elliptique, et des conséquences sur la conjecture principale de Mazur dans le cas ordinaire.

D'autre part, depuis quelques années se développe l'idée que l'on peut avoir une connaissance partielle d'objets géométriques (disons même motiviques) par leurs propriétés p-adiques, propriétés qui se comprennent uniquement en termes de la représentation p-adique associée (Greenberg, Bloch et Kato, ...). Il est alors intéressant de séparer les constructions et théorèmes qui relèvent uniquement de la représentation p-adique et les constructions et théorèmes qui tirent leur existence de la géométrie arithmétique (disons des motifs). On peut ainsi parler de systèmes d'Euler "motiviques" et de systèmes d'Euler p-adiques (définis dans la cohomologie

Mots-clés : Représentation p-adique galoisienne – Théorie d'Iwasawa – Leopold – Systèmes d'Euler.
Classification math. : 11E95 – 11G40 – 11R23 – 11R42.

galoisienne de la réalisation p-adique). À un système d'Euler motivique, est associé un système d'Euler p-adique pour tout nombre premier p. Nous avons cherché ici à tirer les conséquences de l'existence d'un système d'Euler p-adique d'une représentation p-adique géométrique du groupe de Galois absolu de $\mathbb{Q}$. Les démonstrations sont inspirées de celles de [Ko90] et [Ru90]. Un travail similaire a été annoncé indépendamment par Kato et Rubin.

Aucun système d'Euler nouveau n'est construit dans ce texte. Cependant cette étude nous a permis de mieux comprendre cette notion. Insistons ici sur quelques points.

• Dans le cas du système d'Euler cyclotomique (et du système des points de Heegner aussi d'ailleurs), il est fait une utilisation essentielle des congruences $1-\zeta_{ml} \equiv 1-\zeta_m$ modulo les places divisant le nombre premier l. Comme l'a vu Rubin dans [Ru92], ces congruences peuvent en partie se déduire des relations globales de traces (en partie signifiant pour suffisamment de nombres premiers). Ces résultats se généralisent très bien aux systèmes d'Euler p-adiques généraux.

• Par les méthodes de [PR94] et [PR95], on associe à un système d'Euler p-adique d'une représentation p-adique V (avec certaines conditions) un quotient de fonctions analytiques sur $\mathrm{Gal}(\mathbb{Q}(\mu_{mp^\infty})/\mathbb{Q})$ à valeurs dans un certain $\mathbb{Q}_p$-espace vectoriel $\mathbf{D}_p(V)$ de dimension finie, ou ce qui revient au même un élément de $\mathcal{K}(G_\infty)[\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})] \otimes \mathbf{D}_p(V)$ où $\mathcal{K}(G_\infty)$ est l'anneau total des fractions d'une certaine algèbre $\mathcal{H}(G_\infty)$ contenant $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]$. Les relations de trace se traduisent alors par des relations entre ces "fonctions" reflétant la factorisation en produit eulérien des fonctions L classiques.

• Nous avons besoin de résultats généralisant les résultats sur le lien entre indépendance de points sur une courbe elliptique et groupe de Galois ([Ri79]). Ces résultats se déduisent de théorèmes généraux sur les ordres d'une $\mathbb{Q}_p$-algèbre semi-simple et la classification de leurs modules.

Donnons une idée du plan du texte et de son contenu. Dans le premier paragraphe, on introduit les systèmes d'Euler p-adiques et on donne un aperçu des théorèmes démontrés ensuite. Le second paragraphe est consacré aux propriétés locales des systèmes d'Euler. Dans le troisième paragraphe, on reprend la théorie de la dérivation de Kolyvagin et on l'applique aux systèmes d'Euler p-adiques. Dans le paragraphe 4, on rappelle des résultats bien connus sur l'image du groupe de Galois dans $GL(V)$, on montre quelques assertions de finitude sur certains groupes de cohomologie galoisienne, on étudie l'influence de l'indépendance linéaire de points sur le

groupe de Galois engendré par ces points, puis on donne des applications de théorème de Chebotarev. Dans le paragraphe 5, on utilise ce qui précède pour démontrer des résultats de finitude et la divisibilité de certaines séries caractéristiques en théorie d'Iwasawa.

Nous avons ajouté des appendices. Le premier donne la démonstration complète d'une loi explicite de réciprocité pour $l \neq p$ qui est certainement bien connue. Dans le second, nous avons précisé le lien entre deux notions de systèmes d'Euler. Dans le troisième et quatrième, nous avons donné quelques précisions techniques.

Plan.

1. Généralités.

1.1. Préliminaires.

1.1.1. On fixe une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$. Toutes les extensions algébriques de $\mathbb{Q}$ sont supposées contenues dans $\bar{\mathbb{Q}}$. Si F est une extension algébrique de $\mathbb{Q}$ (donc contenue dans $\bar{\mathbb{Q}}$), on note G_F le groupe de Galois de $\bar{\mathbb{Q}}/F$. Si v est une place de F, on choisit une place de $\bar{\mathbb{Q}}$ au-dessus de v et on note abusivement G_v le sous-groupe de décomposition en v de G_F, I_v le sous-groupe d'inertie en v et $\mathrm{Frob}_v \in G_v/I_v$ l'homomorphisme de Frobenius arithmétique associé à v. Si m est un entier, on note μ_m le groupe des racines de l'unité d'ordre divisant m. Pour l nombre premier, pour m entier premier à l, la restriction de Frob_l à $\mathbb{Q}(\mu_m)$ est donnée par $\zeta \to \zeta^l$ pour $\zeta \in \mu_m$. On note $\Delta_m = \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$.

Soit p un nombre premier impair. Soit $\mathbb{Q}(\mu_{p^\infty})$ l'extension cyclotomique de $\mathbb{Q}$ de groupe de Galois $G_\infty \cong \mathbb{Z}_p^\times$. On note $\mathbb{Q}_\infty$ la sous-$\mathbb{Z}_p$-extension de $\mathbb{Q}(\mu_{p^\infty})$, $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ et $\mathbb{Q}_n$ la sous-extension de degré p^n. Si F est une extension de $\mathbb{Q}$, on pose $F_n = F\mathbb{Q}_n$.

Si F est une extension algébrique de $\mathbb{Q}$ et S un ensemble fini de places contenant p et l'infini, on note $G_{S,F}$ le groupe de Galois sur F de la plus grande extension de F contenue dans $\bar{\mathbb{Q}}$, non ramifiée en dehors des places de S.

On reprend les notations usuelles de cohomologie galoisienne. Si L/F est une extension finie, on note $Tr_{L/F}$ l'application de corestriction, encore appelée trace. Si v est une place de F ne divisant pas p et si M est un $\mathbb{Z}_p[G_{F_v}]$-module, on pose

$$H^1_{\mathrm{br}}(F_v, M) = H^1(G_{F_v}/I_v, M^{I_v}) \subset H^1(F_v, M);$$

un élément de $H^1_{\mathrm{br}}(F_v, M)$ est alors dit non ramifié ou ayant bonne réduction. Si Σ est un ensemble de places contenant les places au-dessus de p, on note $H^1_{\mathrm{br},\Sigma}(F, M)$ l'ensemble des éléments de $H^1(F, M)$ dont le localisé en toute place n'appartenant pas à Σ est non ramifié. Pour $v|p$, nous utiliserons (très occasionnellement) les H^1_f introduits par Bloch et Kato.

1.1.2. Soit $\mathcal{E}$ une extension finie de $\mathbb{Q}_p$ et $\mathcal{O}$ son anneau d'entiers. Soit V une représentation $\mathcal{E}$-adique de $G_\mathbb{Q}$, c'est-à-dire un $\mathcal{E}$-espace vectoriel de dimension finie d, muni d'une action linéaire et continue de $G_\mathbb{Q}$, non ramifiée en dehors d'un ensemble fini de nombres premiers de $\mathbb{Q}$

et potentiellement semi-stable en p. Une telle représentation est appelée représentation géométrique. Soit $\Sigma(V)$ l'ensemble des places l de $\mathbb{Q}$ où V n'a pas bonne réduction (on dit que V a bonne réduction en l si V est non ramifiée en l lorsque $l \neq p$ et cristalline en l lorsque $l = p$). On note $\rho = \rho_V$ l'homomorphisme de $G_{\mathbb{Q}}$ dans $GL(V)$ associé et pour $l \neq p$, $\varphi_l = \rho_V(\mathrm{Frob}_l)$ l'endomorphisme de V^{I_l} image de Frob_l. On note en fait de même φ_l agissant sur $V^*(1)^{I_l}$ avec $V^*(1) = \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$ et $\mathbb{Q}_p(1) = \mathbb{Q}_p \otimes \varprojlim_n \mu_{p^n}$, le contexte disant duquel il s'agit. Soit $P_l(V^*(1), X)$ le facteur d'Euler en l de $V^*(1)$: on a donc pour l premier à p

$$P_l(V^*(1), X) = \det(1 - \varphi_l^{-1} X | V^*(1)^{I_l}).$$

En particulier, lorsque V a bonne réduction en l, on a

$$P_l(V^*(1), X) = \det(1 - l^{-1}\varphi_l X | V).$$

Pour $l = p$, on définit $P_p(V^*(1), X)$ par

$$P_p(V^*(1), X) = \det(1 - \varphi X | \mathbf{D}(V^*(1))).$$

où $\mathbf{D}(V^*(1)) = (B_{\mathrm{cris}} \otimes V^*(1))^{G_p}$ est le φ-module filtré associé à $V^*(1)$. Nous nous servirons très peu de ce facteur.

On note $d_\pm = d_\pm(V)$ la dimension du sous-espace vectoriel de V sur lequel une conjugaison complexe c agit par ± 1 (la dimension ne dépend pas de c).

1.1.3. Soit F une extension algébrique finie de $\mathbb{Q}$. Fixons un $\mathcal{O}$-réseau T de V stable par $G_{\mathbb{Q}}$. Soit S un ensemble fini de places de F contenant les places divisant $\Sigma(V)$, p et l'infini. La limite projective $H^1_\infty(F, T)$ des $H^1(G_{S,F_n}, T)$ pour les applications de corestriction ne dépend pas de S. On note $H^2_{\infty,S}(F, T)$ la limite projective des $H^2(G_{S,F_n}, T)$ et $H^2_\infty(F, T)$ le noyau de l'homomorphisme

$$H^2_{\infty,S}(F, T) \to \bigoplus_{v \in S} Z^2_\infty(F_v, T).$$

où $Z^2_\infty(F_v, T)$ est la limite projective des $\bigoplus_{w|v} H^2(F_{n,w}, T)$ pour les homomorphismes de corestrictions.

1.1.4. Le groupe de Galois $G_{\infty,m} = \mathrm{Gal}(\mathbb{Q}(\mu_{mp^\infty})/\mathbb{Q})$ est isomorphe à $\Delta_{pm} \times \Gamma$ avec

$$\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{mp^\infty})/\mathbb{Q}(\mu_{pm})) \cong \mathbb{Z}_p,$$

pour m premier à p ; il opère sur les $\mathcal{O}$-modules $H^i_\infty(\mathbb{Q}(\mu_m), T)$ qui sont ainsi munis d'une structure de $\Lambda[\Delta_m]$-modules avec $\Lambda = \mathcal{O}[[G_\infty]]$ et $G_\infty = G_{\infty,1}$. En tant que Λ-modules, ils sont de type fini.

Si ξ est un caractère de Δ_{mp}, si $\mathcal{O}(\xi)$ est l'anneau engendré sur $\mathcal{O}$ par les valeurs de ξ et $\mathcal{M}$ un $\mathcal{O}[\Delta_m]$-module, on note $\mathcal{M}^{(\xi)}$ le $\mathcal{O}(\xi)$-module formé des $x \in \mathcal{O}(\xi) \otimes_{\mathcal{O}} \mathcal{M}$ tel que $\delta x = \xi(\delta)x$ pour tout $\delta \in \Delta_{mp}$. Si ξ_p est la p-composante de ξ, c'est-à-dire la restriction de ξ à Δ_p, on note $\epsilon(\xi) = \epsilon(\xi_p)$ le signe de $\xi_p(c)$ où c est une conjugaison complexe de $\bar{\mathbb{Q}}/\mathbb{Q}$. L'image Λ_ξ de $\mathcal{O}(\xi)[[G_{\infty,m}]]$ par le caractère ξ est isomorphe à $\mathcal{O}(\xi)[[\Gamma]]$ et donc à l'anneau des séries formelles en 1 variable à coefficients dans $\mathcal{O}(\xi)$.

Si $\mathcal{M}$ est un Λ-module, on dit abusivement que $\mathcal{M}$ est de Λ-torsion si $\mathcal{M}^{(\xi)}$ est un Λ_ξ-module de torsion pour tout caractère ξ de Δ_{mp}, c'est-à-dire si $\mathcal{M}$ est un $\mathbb{Z}_p[[\Gamma]]$-module de torsion. On note

$$\mathcal{M}_+ = \bigoplus_{\epsilon(\xi)=+} \mathcal{M}^{(\xi)} \quad , \quad \mathcal{M}_- = \bigoplus_{\epsilon(\xi)=-} \mathcal{M}^{(\xi)}.$$

Rappelons ([P-R95] par exemple) que si m est premier à p et si ξ est un caractère de Δ_{mp}, on a

$$rg_{\Lambda_\xi} H^1_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)} - rg_{\Lambda_\xi} H^2_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)} = d_{-\epsilon(\xi)}.$$

1.1.5. Conjecture. — *Le Λ-module $H^2_\infty(\mathbb{Q}(\mu_m), T)$ est un Λ-module de torsion.*

De manière équivalente, $H^1_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)}$ est un Λ_ξ-module de rang $d_{-\epsilon(\xi)}$ pour tout caractère ξ de Δ_{pm}. Nous référons à la conjecture relative à ξ comme la conjecture Leop(V, ξ).

1.2. Systèmes d'Euler p-adiques.

1.2.1. Soit Σ un ensemble fini de places de $\mathbb{Q}$. Si m est un entier, on dit que m est premier à Σ si m est une unité en toutes les places de Σ. Si F est une extension algébrique de $\mathbb{Q}$, on note Σ_F ou abusivement Σ l'ensemble des places de F au-dessus des places de Σ.

Définition. — *On appelle système d'Euler p-adique de rang 1 une famille d'éléments $c(m) \in H^1(\mathbb{Q}(\mu_m), T)$ pour m entier premier à Σ et sans facteurs carrés vérifiant*

(1.2.1)

$$Tr_{\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)}(c(ml)) = \begin{cases} P_l(V^*(1), \mathrm{Frob}_l^{-1})c(m) & \text{si } l \text{ est premier à } m \\ c(m) & \text{si } l \text{ divise } m \end{cases}$$

pour l nombre premier et premier à Σ.

Ici, Frob_l est vu comme un élément de Δ_m.

DÉFINITION. — *On appelle système d'Euler-Iwasawa p-adique de rang 1 une famille d'éléments $c(m) \in H^1(\mathbb{Q}(\mu_m), T)$ pour m de la forme $m'p^n$ avec m' entier premier à Σ et sans facteurs carrés et n entier, vérifiant*

(1.2.2)

$$\mathrm{Tr}_{\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)}(c(ml)) = \begin{cases} P_l(V^*(1), \mathrm{Frob}_l^{-1})c(m) & \text{si } l \text{ est premier à } m \\ c(m) & \text{si } l \text{ divise } m \end{cases}$$

pour l nombre premier et premier à Σ.

Dans l'un et l'autre cas, si $c(m)$ est défini, on dit que m est admissible. Remarquons que si m est admissible et si l est un nombre premier, premier à m et à Σ (admissible), ml est admissible.

Si $c = (c(m))_m$ est un système d'Euler-Iwasawa p-adique, on a, pour $n \geqslant 1$ et m admissible

$$\mathrm{Tr}_{\mathbb{Q}(\mu_{mp^{n+1}})/\mathbb{Q}(\mu_{mp^n})} c(mp^{n+1}) = c(mp^n).$$

Ainsi, les $(c(mp^{n+1}))_n$ forment un système projectif pour la corestriction que l'on note $c_p(m)$. Nous verrons en 2.1.2 que nécessairement $c_p(m)$ appartient à $H^1_\infty(\mathbb{Q}(\mu_m), T)$ et que l'image $c(mp^n)$ de $c_p(m)$ dans $H^1(\mathbb{Q}(\mu_{mp^n}), T)$ est non ramifiée en dehors de p pour $n \geqslant 1$. Par contre, il n'est pas toujours possible de reconstruire $c(m)$ pour m premier à p à partir des $c_p(m')$: comme

$$\mathrm{Tr}_{\mathbb{Q}(\mu_l)/\mathbb{Q}} c(l) = P_l(V^*(1), \mathrm{Frob}_l^{-1})c(1) = P_l(V^*(1), 1)c(1),$$

si $P_l(V^*(1), 1) = 0$ (resp. $P_p(V^*(1), 1) = 0$), $c(1)$ ne se déduit pas de $c(l)$ (resp. de $c_p(1)$).

Si l est un nombre premier et F une extension galoisienne de $\mathbb{Q}$ non ramifiée en l, notons Tr_l la trace de $\mathrm{Tr}_{F(\mu_l)/F}$. Pour tout nombre premier l premier à Σ et pour tout entier m premier à l et admissible, on a donc

$$\mathrm{Tr}_l(c(ml)) = P_l(V^*(1), \mathrm{Frob}_l^{-1})c(m).$$

1.2.2. Pour m' multiple de m (premier à p), la projection $\Delta_{m'} \to \Delta_m$ induit un morphisme naturel d'anneaux

$$\Lambda[\Delta_{m'}] = \mathcal{O}[[\mathrm{Gal}(\mathbb{Q}(\mu_{m'p^\infty})/\mathbb{Q})]] \to \mathcal{O}[[\mathrm{Gal}(\mathbb{Q}(\mu_{mp^\infty})/\mathbb{Q})]] = \Lambda[\Delta_m].$$

On note $\pi_l : \Lambda[\Delta_{ml}] \to \Lambda[\Delta_m]$. Si M est un $\Lambda[\Delta_m]$-module, on a alors une flèche naturelle entre l'algèbre extérieure de M en tant que $\Lambda[\Delta_{m'}]$-module et son algèbre extérieure en tant que $\Lambda[\Delta_m]$-module. Nous laissons l'ambiguïté. Soit r un entier. On désigne par $\mathrm{Tr}_l^r = \wedge^r(\mathrm{Tr}_l)$ l'application de

$$\wedge^r H^1_\infty(\mathbb{Q}(\mu_{ml}), T) \to \wedge^r H^1_\infty(\mathbb{Q}(\mu_m), T)$$

induite par $\mathrm{Tr}_l \in \mathbb{Z}_p[\Delta_{ml}]$. Nous utiliserons la notation commode suivante : si $\underline{r} = (r_+, r_-)$ et si $\mathcal{M}$ est un $\mathcal{O}[[G_\infty]]$-module, on note

$$\wedge^{\underline{r}}\mathcal{M} = \wedge^{r_+}\mathcal{M}_+ \oplus \wedge^{r_-}\mathcal{M}_-$$

(respectivement $\wedge^{r_+}\mathcal{M}_+$, $\wedge^{r_-}\mathcal{M}_-$ si $r_- = 0$, $r_+ = 0$). On pose $\underline{d}_\pm = (d_\pm, d_{-\pm})$. On note $\mathrm{Tr}_l^{\underline{r}} = \mathrm{Tr}_l^{r_+} \oplus \mathrm{Tr}_l^{r_-}$ relativement à la décomposition précédente.

DÉFINITION. — *On appelle système d'Euler-Iwasawa p-adique une famille d'éléments $c_p(m)$ de $\wedge^{\underline{d}-} H^1_\infty(\mathbb{Q}(\mu_m), T)$ pour m entier sans facteurs carrés, premier à un ensemble fini Σ et à p telle que pour tout nombre premier l premier à Σ et à p et pour tout entier m premier à lp et à Σ,*

$$\mathrm{Tr}_l^{\underline{d}-}(c_p(ml)) = P_l(V^*(1), \mathrm{Frob}_l^{-1}) c_p(m). \tag{1.2.3}$$

Ici, Frob_l est vu comme un élément de $\mathrm{Gal}(\mathbb{Q}(\mu_{mp^\infty})/\mathbb{Q})$. Pour $n \geqslant 1$, on note $c(mp^n)$ la projection de $c_p(m)$ dans $\wedge^{\underline{d}-} H^1(\mathbb{Q}(\mu_{mp^n}), T)$. Si m est premier à p et ξ un caractère de Δ_{mp} à valeurs dans $\bar{\mathbb{Q}}_p^\times$ étendu de manière naturelle en un caractère ξ' de Δ_{mpl}, on a alors

$$\begin{aligned} e_{\xi'}^{d_{-\epsilon(\xi)}} c_p(ml)) &= P_l(V^*(1), \xi(\mathrm{Frob}_l)^{-1}) e_\xi^{d_{-\epsilon(\xi)}} c_p(m) \\ &= P_l(V^*(1), \xi(l)^{-1}) e_\xi^{d_{-\epsilon(\xi)}} c_p(m) \end{aligned}$$

avec $e_\xi^r = \wedge^r(e_\xi)$.

1.2.3. Expliquons comment obtenir à partir d'un système d'Euler-Iwasawa p-adique un système d'Euler-Iwasawa p-adique de rang 1 d'après une idée de Rubin (ce qui suit n'a bien sûr d'intérêt que si d_+ ou d_- sont supérieurs ou égaux à 2). Dans la suite, l est un nombre premier, m et l

sont supposés admissibles, premiers entre eux et premiers à p. Considérons l'homomorphisme Tr_l :

$$\mathrm{Hom}_{\Lambda[\Delta_{ml}]}(H^1_\infty(\mathbb{Q}(\mu_{ml}),T),\Lambda[\Delta_{ml}]) \to \mathrm{Hom}_{\Lambda[\Delta_m]}(H^1_\infty(\mathbb{Q}(\mu_m),T),\Lambda[\Delta_m])$$

induit par l'application de restriction

$$H^1_\infty(\mathbb{Q}(\mu_m),T) \to H^1_\infty(\mathbb{Q}(\mu_{ml}),T)$$

et par l'application

$$\Lambda[\Delta_{ml}]^{\mathrm{Gal}(\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m))} \to \Lambda[\Delta_m]$$

qui envoie $\sum_{\tau\in\mathrm{Gal}(\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m))} \tau$ sur 1. On comprend mieux cette application si on utilise le fait que si M est un $A[\Delta]$-module où Δ est un groupe fini abélien (ici $A=\Lambda$), il y a un isomorphisme canonique

$$\mathrm{Hom}_{A[\Delta]}(M,A[\Delta]) \cong \mathrm{Hom}_A(M,A)^\iota$$

où ι revient à changer l'action de Δ par $\delta \to \delta^{-1}$ pour $\delta\in\Delta$ (cf. 4.7.1). L'application Tr_l est alors simplement l'application induite par l'application de restriction

$$H^1_\infty(\mathbb{Q}(\mu_m),T) \to H^1_\infty(\mathbb{Q}(\mu_{ml}),T).$$

On vérifie facilement l'identité

$$\mathrm{Tr}_l(\psi)(\mathrm{Tr}_l(x)) = \pi_l \circ \psi(x)$$

pour $x\in H^1_\infty(\mathbb{Q}(\mu_{ml}),T)$ et $\psi\in\mathrm{Hom}_{\Lambda[\Delta_{ml}]}(H^1_\infty(\mathbb{Q}(\mu_{ml}),T),\Lambda[\Delta_{ml}])$.

Soit $\Phi=(\Phi_m)_m$ un élément de la limite projective des

$$\wedge^{r-1}\mathrm{Hom}_{\Lambda[\Delta_m]}(H^1_\infty(\mathbb{Q}(\mu_m),T),\Lambda[\Delta_m])$$

relativement aux applications Tr_l^{r-1} induites par les Tr_l. On définit à partir de Φ_m un homomorphisme de $\wedge^r H^1_\infty(\mathbb{Q}(\mu_m),T)$ dans $H^1_\infty(\mathbb{Q}(\mu_m),T)$ noté encore Φ_m :

$$\Phi_m(\omega_1\wedge\ldots\wedge\omega_r) = \sum_{i=1}^{r}(-1)^i\Phi_m(\omega_1\wedge\ldots\wedge\omega_{i-1}\wedge\omega_{i+1}\wedge\ldots\wedge\omega_r)\omega_i.$$

LEMME. — *Soit $c_p=(c_p(m))_m$ un système d'Euler-Iwasawa p-adique. Soit (Φ_m) un système compatible d'éléments de*

$$\wedge^{\underline{d}_-{}^{-1}}\mathrm{Hom}_{\Lambda[\Delta_m]}(H^1_\infty(\mathbb{Q}(\mu_m),T),\Lambda[\Delta_m]) \cong \wedge^{\underline{d}_-{}^{-1}}\mathrm{Hom}_\Lambda(H^1_\infty(\mathbb{Q}(\mu_m),T),\Lambda)^\iota.$$

Alors, les $\Phi_m(c_p(m))$ *vérifient pour* $m \in \mathbb{N}$ *et* l *premier et premier à* m *admissibles,*

$$\text{Tr}_l(\Phi_{ml}((c_p(ml))) = P_l(V^*(1), \text{Frob}_l^{-1})\Phi_m(c_p(m)) \tag{1.2.4}$$

et forment donc un système d'Euler-Iwasawa p-adique de rang 1.

Démonstration. — On a $\Phi_m(\text{Tr}_l^{\frac{d}{-}-1}(x)) = \pi_l \circ \Phi_{ml}(x)$, d'où

$$\begin{aligned} P_l(V^*(1), \text{Frob}_l^{-1})\Phi_m(c_p(m)) &= \Phi_m(P_l(V^*(1), \text{Frob}_l^{-1})c_p(m)) \\ &= \Phi_m(\text{Tr}_l^{\frac{d}{-}-1}(c_p(ml))) \\ &= \pi_l(\Phi_{ml}(\text{Tr}_l^{\frac{d}{-}-1}(c_p(ml))) \\ &= \text{Tr}_l(\Phi_{ml}((c_p(ml))). \end{aligned}$$

□

Nous montrons dans l'appendice B que pour tout caractère ξ fixé de Δ_{mp}, il existe un système compatible Φ_ξ d'éléments $\Phi_{\xi,mm'}$ de

$$\wedge^{d-\epsilon(\xi)-1}\text{Hom}_{\Lambda_\xi}(H^1_\infty(\mathbb{Q}(\mu_{mm'}), T)^{(\xi)}, \Lambda)$$

pour m' premier à mp tel que $\Phi_{\xi,m}(c_{p,\xi}(m))$ soit non nul.

1.3. Énoncés de quelques théorèmes.

1.3.1. Nous supposons désormais que V est une représentation $\mathcal{E}$-adique irréductible de $G_\mathbb{Q}$, non ramifiée en dehors d'un nombre fini de places et de Hodge-Tate en p. Le déterminant $\det(V)$ est donné par un caractère de la forme $\epsilon < \chi >^r$ où ϵ est un caractère d'ordre fini, $r \in \mathbb{Z}$ et $< \chi >$ est la p-composante du caractère cyclotomique : $< \chi >: G_\mathbb{Q} \to 1+p\mathbb{Z}_p$.

Introduisons des conditions techniques :

(Tech$_m$) il existe un élément $g \in GL(T)$ appartenant à l'image de $G_{\mathbb{Q}(\mu_{mp^\infty})}$, tel que $V/(g-1)V$ soit de dimension 1 et dont les valeurs propres autre que 1 ne sont pas des racines de l'unité.

(Tech$_\infty$) il existe un élément $g \in GL(T)$ appartenant à l'image de $G_{\mathbb{Q}^{\text{ab}}}$ avec $\mathbb{Q}^{\text{ab}}$ la plus grande extension abélienne de $\mathbb{Q}$, tel que $V/(g-1)V$ soit de dimension 1 et dont les valeurs propres autre que 1 ne sont pas des racines de l'unité.

(H) pour presque tout nombre premier l, $P_l(V, 1) \neq 0$.

Remarquons que si m est premier à $\Sigma(V)$, il suffit de demander que g soit dans l'image de $G_{\mathbb{Q}(\mu_{p^\infty})}$. En effet, $\mathbb{Q}(\mu_m)$ et le corps de définition de V sont alors linéairement disjoints sur $\mathbb{Q}$. D'autre part, quitte à remplacer g par une puissance, on peut en fait supposer que le déterminant de g est 1. Si (Tech$_m$) est vrai, pour un m, (Tech$_{ml_1\dots l_r}$) est vrai pour tous nombres premiers $l_1,\dots, l_r$ distincts premiers à m et à $\Sigma(V)$. Remarquons enfin que ces hypothèses (en fait (Tech$_1$)=(Tech)) impliquent que V est absolument irréductible sur $G_{\mathbb{Q}}$ et que sa restriction à tout sous-groupe fermé distingué de $G_{\mathbb{Q}}$ est somme directe de représentations absolument irréductibles (cf. l'appendice D). D'autre part, alors que les conditions (Tech$_m$) sont invariantes par twist par $\mathbb{Z}_p(1)$, il n'en est pas de même de la condition (H) que l'on peut donc "forcer" par twist.

Si l'on se donne un système d'Euler p-adique c ou un système d'Euler-Iwasawa p-adique c_p (resp. et tel que (Tech) est vérifié), on dit que m est fortement admissible si m est admissible et si $V^{G_{\mathbb{Q}(\mu_m)}} = 0$ ou si $V^{G_{\mathbb{Q}(\mu_{mp^\infty})}} = 0$ (resp. et si (Tech$_m$) est vérifié).

THÉORÈME. — *Supposons que V vérifie* (Tech) *et* (H). *Soit c_p un système d'Euler-Iwasawa p-adique de rang 1 pour V. Soit m un entier fortement admissible premier à p et ξ un caractère de Δ_{mp} tel que $d_-(\xi) \neq 0$. Si $c_{p,\xi}(m) \overset{\text{déf}}{=} e_\xi c_p(m) \in H^1_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)}$ n'est pas de Λ_ξ-torsion,* Leop(V,ξ) *est vraie.*

1.3.2. Supposons les hypothèses du théorème vérifiées pour le caractère ξ. Par les théorèmes de structure, il existe un homomorphisme de Λ_ξ-modules

$$H^1_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)}/{}_*c_{p,\xi}(m) \to \Lambda_\xi/(\mathcal{F}(c_{p,\xi}(m))) \oplus \Lambda_\xi^{\,d_{-\epsilon(\xi)}-1}$$

à noyau et conoyau finis annulés par un idéal de Λ_ξ de hauteur 2. D'autre part, comme Leop(V,ξ) est vraie, $H^2_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)}$ est un Λ_ξ-module de torsion et il existe un Λ_ξ-homomorphisme injectif

$$\oplus_{i=1}^r \Lambda_\xi/(f_i) \to H^2_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)}$$

à conoyau fini annulé par un idéal de hauteur 2. Posons $f_\xi(m) = f_1 \dots f_r \in \Lambda_\xi$.

1.3.3. THÉORÈME. — *Soit V une représentation $\mathcal{E}$-adique de $G_{\mathbb{Q}}$ irréductible, non ramifiée en dehors d'un nombre fini de places, vérifiant* (Tech). *Soit c_p un système d'Euler-Iwasawa p-adique de rang 1. Alors, pour m entier fortement admissible et tel que $V^*(1)^{G_{\mathbb{Q}(\mu_{mp^\infty})_v}} = 0$ pour toute*

place v divisant p, il existe un entier positif μ_m tel que

$$f_\xi(m)|p^{\mu_m}\mathcal{F}(c_{p,\xi}(m)).$$

Remarque. — Sous des hypothèses supplémentaires sur V, il est possible de montrer que l'on peut prendre $\mu_m = 0$ (cf. 5.3.6).

1.3.4. Supposons qu'il existe un système c_p d'Euler-Iwasawa p-adique. Soit $\mathcal{F}_m(c_{p,\xi})$ un élément de Λ_ξ tel qu'il existe un homomorphisme de Λ_ξ-modules

$$\wedge^{d-\epsilon(\xi)} H^1_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)}/\Lambda_\xi c_{p,\xi}(m) \to \Lambda_\xi/(\mathcal{F}_m(c_{p,\xi}))$$

à noyau et conoyau finis près pour ξ caractère de Δ_{mp} (on le prend égal à 0 si le premier module n'est pas de torsion) et soit $\mathcal{F}_m(c_p)$ un élément de $\mathbb{Q}_p \otimes \Lambda[\Delta_m]$ tel que $\xi(\mathcal{F}_m(c_p)) = \mathcal{F}_m(c_{p,\xi})$. Soit d'autre part un élément f_m de $\mathbb{Q}_p \otimes \Lambda[\Delta_m]$ tel que $f_\xi(m) = \xi(f_m)$.

On déduit alors du théorème 1.3.3 le théorème suivant :

1.3.5. THÉORÈME. — *Soit V une représentation $\mathcal{E}$-adique de $G_\mathbb{Q}$, irréductible, non ramifiée en dehors d'un nombre fini de places et vérifiant* (Tech). *Soit c_p un système d'Euler-Iwasawa p-adique de V. Alors, si m est fortement admissible tel que $V^*(1)^{G_{\mathbb{Q}(\mu_m p^\infty)_v}}$ soit nul pour toute place v divisant p, il existe un entier positif μ_m tel que*

$$f_m|p^{\mu_m}\mathcal{F}_m(c_p).$$

Ce théorème se déduit du théorème 1.3.3 en remarquant qu'il existe un système compatible $(\Phi_{\xi,mm'})$ comme en 1.2.3 tel que $\mathcal{F}(\Phi_{\xi,m}(c_p(m))) = \mathcal{F}_m(c_{p,\xi})$ (la démonstration est faite dans l'appendice B). On peut alors faire la conjecture suivante :

Conjecture. — Il existe un système d'Euler-Iwasawa p-adique $c_p^{\text{spéc}}$ tel que

$$f(m)\Lambda[\Delta_m] = \mathcal{F}_m(c_p^{\text{spéc}})\Lambda[\Delta_m].$$

D'autres résultats à un niveau fini sont obtenus dans le paragraphe 5.

1.4. Lien avec les fonctions L p-adiques.

1.4.1. On choisit pour tout entier m une racine de l'unité ζ_m d'ordre m telle que $\zeta_{mn}^n = \zeta_m$ pour tous entiers m et n. On note ζ ce choix de racines

de l'unité. On a alors un homomorphisme de $\mathcal{O}[\Delta_m]$-modules $\Psi_m^\zeta : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{O}[\Delta_m] = \mathcal{E}[\Delta_m] \to \mathcal{E} \otimes_{\mathbb{Q}} \mathbb{Q}(\mu_m)$ donné par $\sum_{\delta\in\Delta_m} a_\delta\delta \mapsto \sum_{\delta\in\Delta_m} a_\delta\delta(\zeta_m)$. On en déduit un homomorphisme noté encore $\Psi_m^\zeta : \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p[\Delta_m] \to \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}(\mu_m)$.

On note toujours π_l la projection de Δ_{ml} sur Δ_m pour l nombre premier ne divisant pas m.

LEMME. — *On a* $\mathrm{Tr}_l \circ \Psi_{ml}^\zeta = -\Psi_m^\zeta \circ \mathrm{Frob}_l^{-1}\pi_l = -\mathrm{Frob}_l^{-1}\Psi_m^\zeta \circ \pi_l$.

Démonstration. — On a

$$\mathrm{Tr}_l \circ \Psi_{ml}^\zeta\left(\sum_{\delta\in\Delta_{ml}} a_\delta\delta\right) = \sum_{\delta'\in\Delta_{ml},\pi_l(\delta')=1}\ \sum_{\delta\in\Delta_{ml}} a_\delta\delta'\delta(\zeta_{ml})$$

Or $\sum_{\delta'\in\Delta_{ml},\pi_l(\delta')=1} \delta'(\zeta_{ml}) = \sum_{i \bmod ml,(i,l)=1,i\equiv 1 \bmod m} \zeta_{ml}^i$. On écrit $1 = mu + lv$ et $j \equiv ui \bmod l$ et on obtient

$$\sum_{\delta'\in\Delta_l,\pi_l(\delta')=1} \delta'(\zeta_{ml}) = \sum_{j \bmod l,\ (j,l)=1} \zeta_l^j\zeta_m^v = -\zeta_m^{l^{-1}},$$

car $v \equiv l^{-1} \bmod m$. Donc

$$\begin{aligned}\mathrm{Tr}_l \circ \Psi_{ml}^\zeta\left(\sum_{\delta\in\Delta_{ml}} a_\delta\delta\right) &= -\sum_{\delta\in\Delta_{ml}} a_\delta\delta.\mathrm{Frob}_l^{-1}\zeta_m \\ &= -\mathrm{Frob}_l^{-1}\pi_l\left(\sum_{\delta\in\Delta_{ml}} a_\delta\delta)(\zeta_m\right) \\ &= -\Psi_m^\zeta \circ \mathrm{Frob}_l^{-1}\pi_l\left(\sum_{\delta\in\Delta_{ml}} a_\delta\delta\right).\end{aligned}$$

□

1.4.2. Lorsque V est cristalline en p, il est construit dans [PR94] pour tout entier h un homomorphisme de $\Lambda[\Delta_m]$-modules

$$\mathcal{L}_{V,\mathbb{Q}(\mu_m),h}^\zeta : H_\infty^1(\mathbb{Q}(\mu_m),T)/T^{G_{\mathbb{Q}(\mu_{mp^\infty})}} \to \mathbb{Q}(\mu_m) \otimes_{\mathbb{Q}} \mathcal{K}(G_\infty) \otimes_{\mathbb{Q}_p} \mathbf{D_p(V)}$$

(pour la définition de $\mathcal{K}(G_\infty)$, voir [PR94]; $\mathbf{D_p(V)}$ est le φ-module filtré associé à V par Fontaine). En utilisant l'isomorphisme Ψ_m^ζ, on en déduit un homomorphisme de $\Lambda[\Delta_m]$-modules

$$\underline{L}_{V,\mathbb{Q}(\mu_m),h}^\zeta : H_\infty^1(\mathbb{Q}(\mu_m),T)/T^{G_{\mathbb{Q}(\mu_{mp^\infty})}} \to \mathcal{K}(G_\infty)[\Delta_m] \otimes \mathbf{D_p(V)} \ :$$

on a $\underline{L}^{\zeta}_{V,\mathbb{Q}(\mu_m),h}\cdot\zeta_m = \mathcal{L}^{\zeta}_{V,\mathbb{Q}(\mu_m),h}$. On pose $\mathcal{L}_{V,\mathbb{Q}(\mu_m)} = (\mathcal{L}^{\zeta}_{V,\mathbb{Q}(\mu_m),h})_h$, et $\underline{L}_{V,\mathbb{Q}(\mu_m)} = (\underline{L}_{V,\mathbb{Q}(\mu_m),h})_h$.

1.4.3. Lemme. — *Soit c_p un système d'Euler-Iwasawa p-adique. Pour tout m admissible, pour tout l premier à m et à Σ, on a*

$$\pi_l(\underline{L}_{V,\mathbb{Q}(\mu_{ml})}(c_p(ml))) = P_l(V^*(1),\mathrm{Frob}_l^{-1})(-\mathrm{Frob}_l)^{\underline{d}-}\underline{L}_{V,\mathbb{Q}(\mu_m)}(c_p(m)).$$

Démonstration. — Pour tout $x \in H^1_{\infty}(\mathbb{Q}(\mu_{ml}),T)$, on a

$$\mathcal{L}^{\zeta}_{V,h}(\mathrm{Tr}_l(x)) = \mathrm{Tr}_l(\mathcal{L}^{\zeta}_{V,h}(x)).$$

On déduit alors du lemme 1.4.1 que

$$\pi_l(\underline{L}^{\zeta}_{V,\mathbb{Q}(\mu_{ml}),h}(x) = (-\mathrm{Frob}_l)^{\underline{d}-}\underline{L}^{\zeta}_{V,\mathbb{Q}(\mu_m),h}(\mathrm{Tr}_l^{\underline{d}-}(x)).$$

On déduit alors de la relation (1.2.3) que

$$\pi_l(\underline{L}^{\zeta}_{V,\mathbb{Q}(\mu_{ml}),h}(c_p(ml))) = (-\mathrm{Frob}_l)^{\underline{d}-}P_l(V^*(1),\mathrm{Frob}_l^{-1})\underline{L}^{\zeta}_{V,\mathbb{Q}(\mu_m),h}(c_p(m)).$$

□

1.4.4. Notons $\Sigma(m)$ l'ensemble des nombres premiers divisant m. On fixe un élément non nul e_T de $\det_{\mathcal{E}}\mathbf{D}_p(V)$ (on peut faire des choix plus précis mais c'est inutile ici). Si c_p est un système d'Euler-Iwasawa p-adique, on considère l'élément $\Lambda^{p,\Sigma(pm)}_{p,\infty}(\mathcal{M})$ de $\mathcal{K}(G_\infty)[\Delta_m]\otimes\wedge^{\underline{d}_+(V)}\mathbf{D}_p(V^*(1))$ défini pour $n \in \wedge^{\underline{d}_+(V)}\mathbf{D}_p(V)$ par

$$\Lambda^{p,\Sigma(pm)}_{p,\infty}(c_p)(n)e_T = \prod_{j>-h} l_{-j}^{\dim_{\mathbb{Q}_p}\mathrm{Fil}^j\mathbf{D}_p(V)}\underline{L}^{\epsilon}_{V,\mathbb{Q}(\mu_m),h}(c_p(m))\wedge n$$

où $\mathrm{Fil}^j\mathbf{D}_p(V)$ est la filtration sur $\mathbf{D}_p(V)$ et où $l_j = \dfrac{\log(\chi(\gamma)^j\gamma^{-1})}{\log\chi(\gamma)}$ pour γ d'ordre infini de Γ.

1.4.5. Lemme. — *Soit c_p un système d'Euler-Iwasawa p-adique. On a*

$$\pi_l(\Lambda^{p,\Sigma(pml)}_{p,\infty}(c_p)) = (-\mathrm{Frob}_l)^{\underline{d}-}P_l(V^*(1),\mathrm{Frob}_l^{-1})\Lambda^{p,\Sigma(pm)}_{p,\infty}(c_p).$$

Démonstration. — Comme Frob_l agit trivialement sur $\mathbf{D}_p(V)$, on a

$$P_l(V^*(1),\mathrm{Frob}_l^{-1})[\Lambda^{p,\Sigma(pm)}_{p,\infty}(c_p)(n)] = P_l(V^*(1),\mathrm{Frob}_l^{-1})(\Lambda^{p,\Sigma(pm)}_{p,\infty}(c_p))(n).$$

On peut alors utiliser le lemme 1.4.3. □

1.5. Exemples.

1.5.1. On prend $V = \mathbb{Q}_p(1)$. Par la théorie de Kummer, $H^1(F, \mathbb{Z}_p(1))$ est le complété p-adique $\varprojlim_n F^\times/F^{\times p^n}$ du groupe multiplicatif $F^\times$ de F. Prenons alors pour $c(m)$ l'image de $1-\zeta_m$ dans $H^1(F, \mathbb{Z}_p(1))$ où les ζ_m sont des racines de l'unité d'ordre m vérifiant $\zeta_{mn}^n = \zeta_m$. Vérifions que les $c(m)$ forment bien un système d'Euler p-adique de rang 1. Pour cela, soit l un nombre premier, premier à m et écrivons $1 = ul + vm$. On a alors $\zeta_{ml} = \zeta_m^u \zeta_l^v$ et

$$\begin{aligned} N_{\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)}(1-\zeta_{ml}) &= N_{\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)}(1-\zeta_m^u\zeta_l^v) = \prod_{i=1}^{l-1}(1-\zeta_m^u\zeta_l^i) \\ &= \frac{\prod_{i=0}^{l-1}(1-\zeta_m^u\zeta_l^i)}{1-\zeta_m^u} = \frac{1-\zeta_m^{ul}}{1-\zeta_m^u} \\ &= \frac{1-\zeta_m}{1-\zeta_m^{\mathrm{Frob}_l^{-1}}} = (1-\mathrm{Frob}_l^{-1})(1-\zeta_m). \end{aligned}$$

Comme $P_l(V^*(1), X) = 1-X$, la relation de normes est bien vérifiée. Enfin, lorsque l divise m, on a

$$N_{\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)}(1-\zeta_{ml}) = \prod_{i=0}^{l-1}(1-\zeta_{ml}\zeta_l^i) = 1-\zeta_{ml}^l = 1-\zeta_m.$$

1.5.2. Soit E une courbe elliptique modulaire définie sur $\mathbb{Q}$ et $V_p(E)$ la représentation p-adique associée construite à partir de ses points de p^n-torsion. Kato a construit récemment un système d'Euler-Iwasawa relatif à $V_p(E)(1)$ à partir d'une construction de Beilinson. On renvoie à [Ka ?].

1.5.3. Rappelons que le choix d'un système de racines de l'unité compatibles d'ordre une puissance de p permet de définir un opérateur de twist

$$Tw_{V,j} : H^1_\infty(F, T) \cong H^1_\infty(F, T(j))$$

pour tout entier j. Il est obtenu par passage à la limite projective des isomorphismes

$$H^1(G_{S,F(\mu_{p^n})}, T/p^nT) \cong H^1(G_{S,F(\mu_{p^n})}, T/p^nT \otimes \mu_{p^n}^{\otimes j}).$$

Soit c_p un système d'Euler-Iwasawa p-adique (resp. un système d'Euler-Iwasawa p-adique de rang 1) relatif à V. Il est facile de vérifier

que les $Tw_{V,j}(c_p(m))$ forment un système d'Euler-Iwasawa p-adique (resp. un système d'Euler-Iwasawa p-adique de rang 1) relatif à $V(j)$: en effet, $Tw_{V,j}(c_p(m)) \in H^1_\infty(\mathbb{Q}(\mu_m), T(j))$ et

$$\begin{aligned}\mathrm{Tr}_l(Tw_{V,j}(c_p(ml))) &= Tw_{V,j}(\mathrm{Tr}_l(c_p(m))) \\ &= Tw_{V,j}(P_l(V^*(1), \mathrm{Frob}_l^{-1})(c_p(m))) \\ &= P_l(V^*(1), l^j \mathrm{Frob}_l^{-1}) Tw_{V,j}(c_p(m)) \\ &= P_l(V(j)^*(1), \mathrm{Frob}_l^{-1}) Tw_{V,j}(c_p(m)).\end{aligned}$$

On peut donc à partir d'un système d'Euler-Iwasawa p-adique (resp. un système d'Euler-Iwasawa p-adique de rang 1) pour une représentation V en construire un pour tout twist cyclotomique $V(j)$ de V.

1.5.4. Soit E une courbe elliptique à multiplication complexe par l'anneau des entiers d'un corps quadratique imaginaire K, p un nombre premier totalement décomposé dans K et $\mathfrak{p}$ un idéal premier de K au-dessus de p. Alors, si $\mathfrak{p}^h = (\pi)$ et si $T_\mathfrak{p}(E)$ est la limite projective des E_{π^n} relativement à la multiplication par π, $V_\mathfrak{p}(E) = \mathbb{Q}_p \otimes T_\mathfrak{p}(E)$ est une représentation $K_\mathfrak{p}$-adique. Il est alors naturel d'introduire les corps $F(\mathfrak{a}) = F(E_\mathfrak{a})$ pour $\mathfrak{a}$ idéal de K. À partir des unités elliptiques, on construit un système d'Euler relatif à cette famille de corps de nombres *mutatis mutandis* et les résultats sont similaires et de toute façon déjà démontrés par Rubin.

2. Systèmes d'Euler p-adiques.

2.1. Retour sur les définitions.

2.1.1. Définition. — *Soit Σ un ensemble fini de places de $\mathbb{Q}$. Soit R_l une famille de polynômes de $\mathcal{O}[X]$ pour $l \notin \Sigma$. On appelle système p-adique de rang 1 relatif aux R_l une famille d'éléments $c(m) \in H^1(\mathbb{Q}(\mu_m), T)$, pour $m \in \mathbb{N}$ de la forme $m'p^n$ avec m' premier à Σ sans facteurs carrés, vérifiant pour tout nombre premier l premier à Σ et pour tout entier m premier à l et à Σ,*

(2.1.1)

$$\mathrm{Tr}_{\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)}(c(ml)) = \begin{cases} R_l(\mathrm{Frob}_l^{-1})c(m) & \text{si } l \text{ ne divise pas } m \\ c(m) & \text{si } l \text{ divise } m. \end{cases}$$

2.1.2. Si $(c(m))$ est un système p-adique de rang 1, on pose pour tout m admissible (c'est-à-dire pour lequel les $c(mp^n)$ sont définis)

$$c_p(m) = \varprojlim_n c(mp^n),$$

où Frob_l est vu comme un élément de Δ_m.

PROPOSITION. — *Pour tout entier m admissible, $c(mp)$ est non ramifié en dehors de p. Ainsi, $c_p(m)$ appartient à $H^1_\infty(\mathbb{Q}(\mu_m), T)$.*

Démonstration. — Les $c(mp^n)$ forment un système compatible pour les applications de corestriction. Soit v une place ne divisant pas p. Alors $c_p(m)_v$ appartient à la limite projective des $H^1(\mathbb{Q}(\mu_{mp^n})_v, T)$, ce qui est aussi égale à la limite projective des $H^1_{\mathrm{br}}(\mathbb{Q}(\mu_{mp^n})_v, T)$. Donnons rapidement la démonstration. Par la suite exacte inflation-restriction et en posant $K_n = \mathbb{Q}(\mu_{mp^{n+1}})_v$, il suffit de montrer que la limite projective des $H^1(K_n^{nr}, T)^{\mathrm{Gal}(K_n^{nr}/K_n)}$ relative aux traces est nulle. On remarque que comme K_n/K_0 est non ramifié, on a $K_n^{nr} = K_0^{nr}$ et que $\mathrm{Gal}(K_n^{nr}/K_n) = \mathrm{Gal}(K_n^{nr}/K_0)^{p^n}$; comme $H^1(K_0^{nr}, T)$ est un $\mathcal{O}$-module de type fini, la suite des modules $H^1(K_n^{nr}, T)^{\mathrm{Gal}(K_n^{nr}/K_n)}$ est stationnaire et pour n assez grand, l'application de transition de K_{n+1} à K_n est simplement la multiplication par p et la limite projective est nulle. Ainsi, la projection $c(mp^n)$ de $c_p(m)$ est non ramifiée en dehors de p et on en déduit la proposition. □

2.1.3. *Exemple trivial.* — Supposons que $H^0(\mathbb{Q}(\mu_{p^\infty}), T) = T^{G_{\mathbb{Q}(\mu_{p^\infty})}}$ soit non nul. Alors, il existe un tel système p-adique. En effet, l'action de G_∞ sur $H^0(\mathbb{Q}(\mu_{p^\infty}), T)$ est donnée par des caractères $\chi^{j_1}, \ldots, \chi^{j_r}$ où χ est le caractère cyclotomique. Soit $c \in H^0(\mathbb{Q}(\mu_{p^\infty}), T)$ tel que l'action de G_∞ sur c soit donnée par χ^j pour un entier j. Alors, les $c_p(m) = m^{-1}c$ pour m premier à p forment un système p-adique de rang 1 relatif aux polynômes $R_l(X) = 1 - l^{j-1}X$. On a en effet :

$$\mathrm{Tr}_l(c_p(ml)) = (l-1)m^{-1}l^{-1}c = (1-l^{-1})c = (1 - l^{j-1}\mathrm{Frob}_l^{-1})c$$

puisque $\mathrm{Frob}_l^{-1}(c) = l^{-j}c$. Rappelons que l'on a une injection de $H^0(\mathbb{Q}(\mu_{mp^\infty}), T)$ dans $H^1_\infty(\mathbb{Q}(\mu_m), T)$ et que $H^0(\mathbb{Q}(\mu_{mp^\infty}), T)$ en est le sous-module de torsion. Ainsi, le système construit est «de torsion».

2.2. Propriétés locales des systèmes d'Euler p-adiques.

2.2.1. Les résultats de ce paragraphe ont leur inspiration dans [Ru92] et dans des conversations avec K. Rubin. Il s'agit de déduire certaines

relations locales des relations globales de trace qu'un système d'Euler vérifie.

Soit l un nombre premier différent de p et tel que V soit non ramifié en l, F une extension abélienne de $\mathbb{Q}$ et soit λ une place de F au-dessus de l. Notons ev_λ l'isomorphisme

$$H^1_{\mathrm{br}}(F_\lambda, T) \cong T/(1-\varphi_\lambda)T$$

suivant : à $[x]$ élément de $H^1_{\mathrm{br}}(F_\lambda, T)$ dont un représentant dans $Z^1(G_{F_\lambda}, T)$ est x, on associe l'image de $x(\mathrm{Frob}_\lambda) \in T$ dans $T/(1-\varphi_\lambda)T$ qui ne dépend pas du choix de x :

$$\mathrm{ev}_\lambda([x]) \equiv x(\mathrm{Frob}_\lambda) \bmod (\varphi_\lambda - 1)T.$$

2.2.2. Si N est un entier, on note $S(N)$ l'ensemble des nombres premiers l congrus à 1 mod N. Ainsi, pour $l \in S(N)$, l est totalement décomposé dans $\mathbb{Q}(\mu_N)$ et Frob_l laisse fixe $\mathbb{Q}(\mu_N)$. Si f est un élément de $GL(T)$, M une puissance de p et N un entier, on note $S_{f,M}(N)$ le sous-ensemble de $S(N)$ formé des l tel que la réduction de φ_l modulo M coïncide avec la réduction de f^{-1} modulo M sur T/MT.

Considérons la condition (**) portant sur un endomorphisme $f \in GL(T)$: *Il existe une puissance M_0 de p telle que* $(f^{M_0}-1)T \subset p(f-1)T$. Si f vérifie (**), pour toute puissance M de p, il existe une puissance M' de p telle que $(f^{M'}-1)T \subset M(f-1)T$. Il suffit pour cela de montrer que si $(f^{M'}-1)T \subset M(f-1)T$, alors $(f^{M'p}-1)T \subset pM(f-1)T$. Or, $f^{M'p}-1 = (f^{M'}-1)\sum_{i=0}^{p-1} f^{M'i}$. Comme $f^{M'}t - t \in MT$ pour tout $t \in T$, on a $\sum_{i=0}^{p-1} f^{M'i}t - pt \in MT$ et donc $\sum_{i=0}^{p-1} f^{M'i}t \in pT$. Donc,

$$(f^{M'p}-1)T \subset p(f^{M'}-1)T \subset pM(f-1)T.$$

Soit $f \in GL(T)$ tel qu'il existe un entier s pour lequel que $(f-1)^s T \subset pT$ (ce que signifie que $f-1$ est nilpotent sur T/pT). Nous allons montrer que f vérifie alors la condition (**). On a l'identité

$$\begin{aligned}\sum_{i=0}^{M-1} f^i &= \sum_{k=0}^{M-1}\sum_{i=k}^{M-1}\binom{i}{k}(f-1)^k \\ &= \sum_{k=0}^{M-1}\binom{M}{k+1}(f-1)^k\end{aligned}$$

car $\sum_{i=k}^{M-1} \binom{i}{k} = \binom{M}{k+1}$ pour $k \geqslant 0$. On a alors

$$\binom{M}{k+1}(f-1)^k T \subset p^{[\frac{k}{s}]} \frac{M}{k+1} T.$$

Il existe un entier k_0 tel que $[\frac{k}{s}] \geqslant ord_p(k+1)$ pour $k > k_0$. Notons α le ppcm des dénominateurs des $\dfrac{p^{[k/s]}}{k+1}$ pour $k \leqslant k_0$. Alors, $\sum_{i=0}^{M-1} f^i T \subset \frac{M}{\alpha} T$ et f vérifie la condition (**).

On note $S_*(N)$ l'ensemble des nombres premiers $l \in S(N)$, non ramifiés pour V et tels qu'il existe $f \in GL(T)$ vérifiant la condition (**) et tel que $\varphi_l^{-1} \equiv f \bmod l-1$. Ainsi, si $l \in S_*(N)$, il existe une puissance M de p telle que

$$(\varphi_l^M - 1)T \subset (l-1)(\varphi_l - 1)T.$$

On note $S_{*,M}(MN)$ l'ensemble des nombres premiers $l \in S(MN)$ tels qu'il existe $f \in GL(T)$ vérifiant la condition (**) et tel que $\varphi_l \equiv f^{-1} \bmod M$.

2.2.3. Soit $\mathcal{B}(m)$ l'idéal de $\mathcal{O}[\Delta_m]$ engendré par les $\det(1 - \gamma X | V^*(1))_{|X=\delta}$ pour $g \in G_{\mathbb{Q}(\mu_{p^\infty})}$ dont l'image dans $GL(T^*(1))$ est γ et la restriction à $\mathbb{Q}(\mu_m)$ est δ. Remarquons que si m est premier à $\Sigma(V)$, δ et γ peuvent être choisis indépendamment. D'autre part, l'idéal $\mathcal{B}(1)$ est engendré par les $\det(1 - \gamma | V^*(1))$ pour γ dans l'image de $G_{\mathbb{Q}(\mu_{p^\infty})}$. Il est non nul si et seulement s'il existe $g \in G_{\mathbb{Q}(\mu_{p^\infty})}$ tel que 1 ne soit pas valeur propre de g agissant sur $V^*(1)$.

2.2.4. On note $Z(\lambda)$ l'opérateur de T donné par $(l-1)^{-1} P_l(V^*(1), \varphi_\lambda^{-1})$: il est bien défini car par le théorème de Cayley-Hamilton, $P_l(V^*(1), l\varphi_\lambda^{-1})x = 0$ pour $x \in T$ et

$$P_l(V^*(1), l\varphi_\lambda^{-1})x \equiv P_l(V^*(1), \varphi_\lambda^{-1})x \bmod (l-1)T$$

($P_l(V^*(1), X)$ est à coefficients entiers p-adiques).

On considère un système d'Euler p-adique c de rang 1.

2.2.5. Proposition. — i) *Pour m admissible, pour $l \in S_*(m)$ tel que $c(ml)$ soit non ramifié en l,*

$$(c(ml)_\lambda - Z(\lambda)c(m)_\lambda)_\lambda \in \prod_{\lambda | l} H^1_{\mathrm{br}}(\mathbb{Q}(\mu_m)_\lambda, T)$$

est annulé par $\mathcal{B}(m)$ (le produit est pris sur les places λ de $\mathbb{Q}(\mu_m)$ au-dessus de l).

ii) *Si c est de plus un système d'Euler-Iwasawa p-adique de rang 1 et si m est divisible par p, on a*

$$c(ml)_\lambda = Z(\lambda)c(m)_\lambda$$

pour λ place de $\mathbb{Q}(\mu_m)$ divisant l.

La démonstration de (i) qu'on ne fera que pour m premier à p utilise la donnée des $c(n)$ pour n premier à p et sans facteurs carrés. La démonstration de (ii) utilise la donnée des $c(mp^n)$ pour $n \geqslant 1$. Nous allons commencer par le cas où m est premier à p. On fixe M une puissance de p telle que $(\varphi_\lambda^M - 1)T \subset (l-1)(\varphi_\lambda - 1)T$ pour λ place de $\mathbb{Q}(\mu_m)$ au-dessus de l. On note $\mathbb{Q}(T/MT)$ le corps de définition de T/MT.

2.2.6. Lemme. — *Soient γ un élément de $\mathrm{Gal}(\mathbb{Q}(T/MT)/\mathbb{Q}(\mu_M) \cap \mathbb{Q}(T/MT))$ et δ un élément de $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ tel que γ et δ coïncident sur $\mathbb{Q}(\mu_m) \cap \mathbb{Q}(T/MT)$. Il existe un nombre premier q et un prolongement $\mathfrak{Q}$ à $\mathbb{Q}(\mu_m)$ vérifiant les conditions suivantes :*

(1) $q \equiv 1 \bmod M$;

(2) *les actions de φ_q et de γ sur T/MT coïncident ;*

(3) *les places de $\mathbb{Q}(\mu_{ml})$ divisant l sont indécomposées dans la sous-p-extension de $\mathbb{Q}(\mu_{mlq})/\mathbb{Q}(\mu_{ml})$;*

(4) *la restriction de $\mathrm{Frob}_\mathfrak{Q}$ à $\mathbb{Q}(\mu_m)$ est δ.*

Démonstration. — Posons $F = \mathbb{Q}(\mu_M, \sqrt[l]{p})$. C'est une extension de degré p de $\mathbb{Q}(\mu_M)$. Soit σ un générateur de $\mathrm{Gal}(F/\mathbb{Q}(\mu_M))$. Les corps $\mathbb{Q}(T/MT)$ et F sont linéairement indépendants sur $K = \mathbb{Q}(\mu_M) \cap \mathbb{Q}(T/MT)$. En effet, $\mathbb{Q}(T/MT)/K$ est non ramifié aux places divisant l et $F/\mathbb{Q}(\mu_M)$ est totalement ramifiée aux places divisant l. D'autre part, soit $H \subset F(T/MT) \cap \mathbb{Q}(\mu_m)$ de degré premier sur $H_0 = \mathbb{Q}(T/MT) \cap \mathbb{Q}(\mu_m)$. Il existe λ' divisant m tel que H/H_0 est totalement ramifié en λ'. Or $F/\mathbb{Q}$ est non ramifié en λ'. Donc $H = H_0$ et $F(T/MT)$ et $\mathbb{Q}(\mu_m)$ sont linéairement indépendants sur $\mathbb{Q}(T/MT) \cap \mathbb{Q}(\mu_m)$. On en déduit qu'il existe un nombre premier q et un prolongement $\mathfrak{Q}$ à $\bar{\mathbb{Q}}$ tels que le Frobenius $\mathrm{Frob}_\mathfrak{Q}$ coïncide avec

(i) σ sur F,

(ii) γ sur $\mathbb{Q}(T/MT)$,

(iii) δ sur $\mathbb{Q}(\mu_m)$.

La condition (i) implique la condition (1). La condition (ii) implique la condition (2). La condition (iii) implique la condition (4). Il reste à montrer que la condition (3) est vérifiée. Pour cela, on remarque que par la théorie du corps de classes, l'image de Frob_l par l'isomorphisme $\mathrm{Gal}(\mathbb{Q}(\mu_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ est la classe de l (ou l^{-1} selon les conventions). La condition (i) implique que l n'est pas une puissance p-ième dans $(\mathbb{Z}/q\mathbb{Z})^\times$, ce qui implique la condition (3). □

2.2.7. Posons pour simplifier $Q_q(X) = P_q(V^*(1), X)$. Soit λ une place de $\mathbb{Q}(\mu_{ml})$ divisant l. Choisissons un nombre premier q comme dans le lemme 2.2.6. On a alors

$$\begin{aligned} \mathrm{Tr}_q c(mq) &= Q_q(\mathrm{Frob}_q^{-1})c(m), \\ \mathrm{Tr}_q c(mlq) &= Q_q(\mathrm{Frob}_q^{-1})c(ml). \end{aligned} \tag{2.2.1}$$

Notons M' la plus grande puissance de p divisant $q-1$ (M' est divisible par M). Notons d'autre part F_q^p la sous-p-extension maximale de $\mathbb{Q}(\mu_q)/\mathbb{Q}$, Tr'_q la trace de $F(\mu_q)/FF_q^p$ et $\mathrm{Tr}_q^{(p)}$ la trace de $FF_q^{(p)}/F$ pour toute extension F telle que $F \cap \mathbb{Q}(\mu_q) = \mathbb{Q}$: on l'utilise dans la suite pour $F = \mathbb{Q}(\mu_m)$ ou $\mathbb{Q}(\mu_{ml})$ et on a $M' = [FF_q^{(p)} : F] = M'$. Posons enfin $c'(mq) = \mathrm{Tr}'_q(c(mq))$ pour tout m premier à q. On déduit de (2.2.1) que

$$\begin{aligned} \mathrm{Tr}_q^{(p)} c'(mq) &= Q_q(\mathrm{Frob}_q^{-1})c(m), \\ \mathrm{Tr}_q^{(p)} c'(mlq) &= Q_q(\mathrm{Frob}_q^{-1})c(ml). \end{aligned} \tag{2.2.2}$$

Soit λ une place de $\mathbb{Q}(\mu_m)$ divisant l et notons de même son prolongement à $\mathbb{Q}(\mu_{ml})$. La condition (3) du lemme 2.2.6 implique que Frob_λ est un générateur de $\mathrm{Gal}(\mathbb{Q}(\mu_{ml})F_q^p/\mathbb{Q}(\mu_{ml}))$. Grâce à la définition explicite de la corestriction d'un cocycle, on a pour λ divisant l

$$\begin{aligned} \mathrm{Tr}_q^{(p)}(c'(mlq))(\mathrm{Frob}_\lambda) &\equiv c'(mlq)(\mathrm{Frob}_\lambda^{M'}) \bmod (\varphi_\lambda - 1)T \\ \mathrm{Tr}_q^{(p)}(c'(mq))(\mathrm{Frob}_\lambda) &\equiv c'(mq)(\mathrm{Frob}_\lambda^{M'}) \bmod (\varphi_\lambda - 1)T. \end{aligned} \tag{2.2.3}$$

D'où,

(2.2.4)

$$\prod_\lambda c'(mlq)(\mathrm{Frob}_\lambda^{M'}) \equiv Q_q(\varphi_q^{-1}) \prod_\lambda c(ml)(\mathrm{Frob}_\lambda) \bmod \prod_\lambda (\varphi_\lambda - 1)T$$

$$\prod_\lambda c'(mq)(\mathrm{Frob}_\lambda^{M'}) \equiv Q_q(\varphi_q^{-1}) \prod_\lambda c(m)(\mathrm{Frob}_\lambda) \bmod \prod_\lambda (\varphi_\lambda - 1)T.$$

On déduit d'autre part de la relation

$$\mathrm{Tr}_l c'(mlq)(\mathrm{Frob}_\lambda) \equiv Q_l(\varphi_\lambda^{-1})c'(mq)(\mathrm{Frob}_\lambda) \bmod (\varphi_\lambda - 1)T$$

et du fait que l'action de l'inertie en l est triviale sur T que

$$(2.2.5)\quad (l-1)c'(mlq)(\mathrm{Frob}_\lambda^{M'}) \equiv Q_l(\varphi_\lambda^{-1})c'(mq)(\mathrm{Frob}_\lambda^{M'}) \bmod (\varphi_\lambda^{M'}-1)T.$$

L'hypothèse sur l implique que

$$(\varphi_\lambda^{M'}-1)T \subset (\varphi_\lambda^{M}-1)T \subset (l-1)_p(\varphi_\lambda-1)T.$$

D'autre part, $Q_l(\varphi_\lambda^{-1})T \subset (l-1)_pT$. L'équation (2.2.5) devient donc

$$c'(mlq)(\mathrm{Frob}_\lambda^{M'}) \equiv Z(\lambda)c'(mq)(\mathrm{Frob}_\lambda^{M'}) \bmod (\varphi_\lambda-1)T.$$

En utilisant (2.2.4), on obtient

$$Q_q(\varphi_q^{-1})\Big(\prod_\lambda c(ml)(\mathrm{Frob}_\lambda) - Z(\lambda)c(m)(\mathrm{Frob}_\lambda)\Big) \in \prod_\lambda (\varphi_\lambda-1)T.$$

On en déduit que $Q_q(\varphi_q^{-1})\Big(\prod_\lambda c(ml)_\lambda - Z(\lambda)c(m)_\lambda\Big)$ est nul dans $\prod_\lambda H^1_{\mathrm{br}}(\mathbb{Q}(\mu_{ml})_\lambda, T) = \prod_\lambda H^1_{\mathrm{br}}(\mathbb{Q}(\mu_m)_\lambda, T)$. Maintenant, l'action de φ_q sur $\prod_\lambda H^1_{\mathrm{br}}(\mathbb{Q}(\mu_{ml})_\lambda, T)$ est induite par sa restriction Frob_q à $\mathbb{Q}(\mu_m)$ et est donc égale à δ. Quand à $Q_q(X)$, grâce à la condition (2) du lemme 2.2.6, il est égal à $Q_\gamma(X) = \det(1-\gamma X|T^*(1))$. Les $Q_\gamma(\delta)$ engendrent un idéal contenant l'idéal $\mathcal{B}(m)$. Ce qui termine la démonstration.

Démontrons l'assertion (ii) de la proposition 2.2.5. — On change les notations : on suppose maintenant que m est premier à p et on démontre la proposition pour mp. Soit r un entier $\geqslant 0$ tel que l soit totalement décomposé dans $\mathbb{Q}(\mu_{mp^r})$ et ne le soit pas dans $\mathbb{Q}(\mu_{mp^{r+1}})$ et soit λ une place de $\mathbb{Q}(\mu_{mp^r})$ au-dessus de l. Alors, Frob_λ engendre le groupe de Galois de $F(\mu_{p^{r+n}})/F(\mu_{p^r})$ pour $F = \mathbb{Q}(\mu_m)$ ou $\mathbb{Q}(\mu_{ml})$. Prenons $M = p^n$ tel que $(\varphi_\lambda^M-1)T \subset (l-1)(\varphi_\lambda-1)T$. Notons pour simplifier Tr la trace de $F(\mu_{mp^{r+n}})/F(\mu_{mp^r})$ et de $F(\mu_{lmp^{r+n}})/F(\mu_{lmp^r})$. On a

$$(2.2.6)\quad \begin{aligned} \mathrm{Tr}(c(mlp^{r+n}))(\mathrm{Frob}_\lambda) &= c(mlp^{r+n})(\mathrm{Frob}_\lambda^M) \bmod (\varphi_\lambda-1)T \\ \mathrm{Tr}(c(mp^{r+n}))(\mathrm{Frob}_\lambda) &= c(mp^{r+n})(\mathrm{Frob}_\lambda^M) \bmod (\varphi_\lambda-1)T. \end{aligned}$$

D'où,

$$(2.2.7)\quad \begin{aligned} c(mlp^{r+n})(\mathrm{Frob}_\lambda^M) &\equiv c(mlp^r)(\mathrm{Frob}_\lambda) \bmod (\varphi_\lambda-1)T \\ c(mp^{r+n})(\mathrm{Frob}_\lambda^M) &\equiv c(mp^r)(\mathrm{Frob}_\lambda) \bmod (\varphi_\lambda-1)T. \end{aligned}$$

On déduit d'autre part de la relation

$$\mathrm{Tr}_l c(mlp^{r+n})(\mathrm{Frob}_\lambda^M) \equiv Q_l(\varphi_\lambda^{-1})c(mp^{r+n})(\mathrm{Frob}_\lambda^M) \bmod (\varphi_\lambda^M-1)T$$

et du fait que l'action de l'inertie en l est triviale sur T que

(2.2.8)

$$(l-1)c(mlp^{r+n})(\mathrm{Frob}_\lambda^M) \equiv Q_l(\varphi_\lambda^{-1})c(mp^{r+n})(\mathrm{Frob}_\lambda^M) \bmod (\varphi_\lambda^M - 1)T.$$

Donc, grâce à l'inclusion $(\varphi_\lambda^M - 1)T \subset (l-1)(\varphi_\lambda - 1)T$, on a

$$c(mlp^{r+n})(\mathrm{Frob}_\lambda^M) \equiv Z(\lambda)c(mp^{r+n})(\mathrm{Frob}_\lambda^M) \bmod (\varphi_\lambda - 1)T$$

et donc

$$c(mlp^r)(\mathrm{Frob}_\lambda) \equiv Z(\lambda)c(mp^r)(\mathrm{Frob}_\lambda) \bmod (\varphi_\lambda - 1)T.$$

On en déduit que $c(mlp^r)_\lambda = Z(\lambda)c(mp^r)_\lambda$ dans $H^1_{\mathrm{br}}(\mathbb{Q}(\mu_{mlp^r})_\lambda, T)$ et en appliquant la corestriction de $\mathbb{Q}(\mu_{mlp^r})$ à $\mathbb{Q}(\mu_{mlp})$ que $c(mpl)_\lambda = Z(\lambda)c(mp)_\lambda$. □

3. Dérivation de Kolyvagin.

Dans ce paragraphe, on reprend la construction de la dérivation de Kolyvagin en privilégiant la définition cohomologique qui permet de tout décrire en termes de la représentation p-adique. Nous nous sommes inspirés des démonstrations de Nekovář ([Ne92]).

3.1. Situation générale.

3.1.1. Soit G un groupe profini et H un sous-groupe fermé distingué de G tel que G/H soit cyclique d'ordre N. On fixe un générateur σ de G/H et un relèvement $\tilde{\sigma}$ de σ dans G. On note Tr la trace relativement à G/H : $\mathrm{Tr} = \sum_{i=0}^{N-1} \sigma^i$. L'opérateur de Kolyvagin est l'opérateur $D = D_\sigma = \sum_{i=0}^{N-1} i\sigma^i$. Il vérifie la relation

$$(\sigma - 1)D = N - \sum_{i=0}^{N-1} \sigma^i = N - \mathrm{Tr}.$$

Soit A un G-module discret tué par N. Si x est un cocycle de H à valeurs dans A, on note $[x]$ sa classe dans $H^1(H, A)$. On définit un élément $D(x) = D_{\tilde{\sigma}}(x) \in Z^1(H, A)$ par

$$D(x)(h) = \sum_{i=0}^{N-1} i\tilde{\sigma}^i(x)(h)$$

où $\tau(x)(h) = \tau(x(\tau^{-1}h\tau))$ si $\tau \in G$. Supposons que $\mathrm{cores}([x]) \in H^1(G, A)$ est nulle. Alors, la classe $D[x] = [D(x)]$ de $D(x)$ dans $H^1(H, A)$ est invariante par σ, c'est-à-dire par G/H. Si A^G est nul, il en est de même de $H^1(G/H, A^H)$ car G/H est cyclique et l'application restriction $H^1(G, A) \to H^1(H, A)^{G/H}$ est un isomorphisme. Ainsi, $D[x]$ est l'image par restriction d'un unique élément de $H^1(G, A)$ que l'on note $\mathrm{kol}_H([x]) = \mathrm{kol}([x])$ (il dépend du choix de σ).

3.1.2. Soyons plus explicite. On ne suppose plus que A^G est nul. Soit $x \in Z^1(H, A)$ un cocycle de classe $[x]$ dans $H^1(H, A)$. Soit $\mathrm{cores}(x)$ l'élément de $Z^1(G, A)$ défini par :

$$\mathrm{cores}(x)(g) = \begin{cases} \sum_{i=0}^{N-1} \tilde{\sigma}^i(x)(g) & \text{si } g \in H \\ x(\tilde{\sigma}^N) & \text{si } g = \tilde{\sigma}. \end{cases} \tag{3.1.1}$$

La classe de $\mathrm{cores}(x)$ est égale à $\mathrm{cores}[x]$. Comme $\mathrm{cores}[x] = 0$, il existe $\alpha \in A$ tel que

$$\mathrm{cores}(x)(g) = (g-1)(\alpha) \text{ pour tout } g \in G$$

et α est bien défini modulo A^G. D'autre part,

$$\tilde{\sigma}(Dx)(h) - (Dx)(h) = -(h-1)\tilde{\sigma}\alpha.$$

L'application $f : G \to A$ définie par

$$\begin{cases} f(h) & = \mathrm{D(x)(h)} \text{ pour } h \in H \\ f(\tilde{\sigma}) & = -\tilde{\sigma}\alpha \end{cases}$$

se prolonge de manière unique en un élément de $Z^1(G, A)$ dont la restriction à H est $D(x)$. Si $x' = x + \delta(\beta)$ où $\delta(\beta)(h) = (h-1)\beta$, f est changé en f' avec

$$f' - f - \delta(D(\beta)) \in Z^1(G, A^G).$$

On en déduit que si a est un entier tel que $aA^G = 0$, $\mathrm{kol}_H^{(a)}([x]) \overset{\text{déf}}{=} a[f] \in H^1(G, aA)$ est indépendant du choix de x. Si $a = 1$, c'est l'élément $\mathrm{kol}([x])$ défini précédemment.

3.1.3. Lemme. — *Soit H' un sous-groupe de H, distingué dans G et tel que G/H' soit cyclique d'ordre N'. Soit A un G-module annulé par N' ; soient $\pi : A \to A/NA$ la projection naturelle et* Tr *l'application de corestriction de H' à H. Alors, si $x \in H^1(H', A)$, on a*

$$\pi(\mathrm{kol}_{H'}([x])) = \mathrm{kol}_H(\pi(\mathrm{Tr}([x]))).$$

Démonstration. — Faisons la démonstration dans le cas où $A^G = 0$. L'élément $\mathrm{kol}_{H'}([x])$ est calculé à l'aide d'un générateur $\sigma' \in G/H'$ dont l'image dans G/H est σ ; prenons pour $\tilde{\sigma}$ un relèvement de σ' (donc de σ). On a avec $N' = Nm$,

$$\sum_{i=0}^{N'-1} iX^i = \sum_{j=0}^{N-1}\sum_{k=0}^{m-1}(j+Nk)X^{j+Nk} \equiv \sum_{j=0}^{N-1} jX^j \sum_{k=0}^{m-1} X^{Nk} \bmod N.$$

On en déduit que

$$\pi\left(\sum_{i=0}^{Nm-1} i\sigma^i([x])\right) = \sum_{j=0}^{N-1} j\sigma^j\pi(\mathrm{Tr}[x]).$$

D'où la conclusion. □

3.1.4. Supposons donné un sous-groupe fermé G_0 de G tel que si $H_0 = H \cap G_0$, G_0/H_0 soit encore cyclique d'ordre N de générateur σ_0. On suppose que

i) on a une surjection

$$\pi : G_0 \twoheadrightarrow \prod_{q\neq l} \mathbb{Z}_q(1) \ltimes \hat{\mathbb{Z}}$$

de noyau premier à p, le produit semi-direct étant donné par la relation $\varphi\tau\varphi^{-1} = \tau^l$ avec l premier à p, pour φ un générateur topologique de $\hat{\mathbb{Z}}$ et τ un générateur topologique $\prod_{q\neq l} \mathbb{Z}_q(1)$; on note I_0 le noyau de $G_0 \to \hat{\mathbb{Z}}$;

ii) l'image de H_0 par π est $N\prod_{q\neq l} \mathbb{Z}_q(1) \ltimes \hat{\mathbb{Z}}$ et l'image de σ_0 est τ modulo N ;

iii) G agit continûment sur un $\mathcal{O}$-module libre T de type fini et G_0 agit sur T par son quotient $\hat{\mathbb{Z}}$.

On pose

$$\begin{aligned} H^1_{\mathrm{br}}(G_0,T) &= H^1(G_0/I_0,T) \\ H^1_{\mathrm{br}}(H_0,T) &= H^1(H_0/(I_0\cap H_0),T) \\ H^1_{/br}(G_0,T/MT) &= H^1(G_0,T/MT)/H^1_{\mathrm{br}}(G_0,T/MT). \end{aligned}$$

On a un isomorphisme canonique $H^1_{\mathrm{br}}(G_0,T) \cong H^1_{\mathrm{br}}(H_0,T)$. Ainsi, $H^1_{\mathrm{br}}(G_0,T) = H^1(\hat{\mathbb{Z}},T)$ et par évaluation sur le générateur φ de $\hat{\mathbb{Z}}$, on obtient un isomorphisme

$$\mathrm{ev} : H^1_{\mathrm{br}}(G_0,T) \cong T/(\varphi-1)T.$$

Comme I_0 agit trivialement sur T et pour $M|l-1$, on a un homomorphisme

$$\mathrm{Ev}_\tau : H^1(G_0, T/MT) \to \mathrm{Hom}(I_0, T/MT)^{\varphi=1} \to (T/MT)^{\varphi=1},$$

la dernière application étant induite par l'évaluation sur τ (comme M divise $l-1$, φ agit trivialement sur I_0/MI_0). On en déduit une application

$$H^1(G_0/H_0, (T/MT)^{H_0}) \to (T/MT)^{\varphi=1}$$

que l'on note encore $\mathrm{Ev}_{\sigma_0} : \mathrm{Ev}_{\sigma_0}([z_0]) = z_0(\sigma_0)$ pour z_0 cocycle représentant $[z_0]$.

Remarque. — Si $\mathrm{Hom}_{\mathcal{O}}(I_0, T)^{\hat{\mathbb{Z}}} = 0$, c'est-à-dire si l^{-1} n'est pas valeur propre de φ agissant sur T, $H^1_{\mathrm{br}}(G_0, T)$ est en fait égal à $H^1(G_0, T)$.

3.1.5. Supposons que $V^G = 0$ avec $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$, ce qui est équivalent à ce que $(V/T)^G$ est fini et soit un entier a annulant $(V/T)^G$ et donc $(T/MT)^G$ pour toute puissance M de p. Soit M une puissance de p divisant N et $l-1$ et soit $[y] \in H^1(H, T)$ tel que $\mathrm{cores}([y])$ soit divisible par M dans $H^1(G, T)$: $\mathrm{cores}([y]) = M[x]$ avec $[x] \in H^1(G, T)$. On peut appliquer la construction de Kolyvagin à $A = T/MT$. Il existe donc un élément $[z] = \mathrm{kol}^{(a)}_{H,M}([y]) = \mathrm{kol}^{(a)}_H([y] \bmod M)$ de $H^1(G, aT/MT)$ tel que la restriction de $[z]$ à H soit $aD([y] \bmod M)$. On enlèvera H de la notation s'il n'y a pas de confusion possible.

Soit $[z_0]$ la restriction de $[z]$ à G_0. Comme σ_0 agit trivialement sur T, l'opérateur de Kolyvagin D agit sur T et sur $Z^1(H_0, T)$ par $\frac{1}{2}N(N-1)$. On en déduit que la restriction de $[z_0]$ à H_0 est nul. Donc $[z_0]$ est l'image par inflation d'un élément $[z_0']$ de $H^1(G_0/H_0, (aT/MT)^{H_0})$. On peut donc calculer $\mathrm{Ev}_{\sigma_0}([z_0'])$ que l'on note avec un léger abus de notation $\mathrm{Ev}_{\sigma_0}(\mathrm{kol}^{(a)}([y]))$.

3.1.6. Proposition (Nekovář). — *Soit $[y]$ un élément de $H^1(H, T)$ dont l'image par restriction à H_0 appartient à $H^1_{\mathrm{br}}(H_0, T)$. On suppose que* $\mathrm{cores}([y])$ *est divisible par M dans $H^1(G, T)$: $\mathrm{cores}([y]) = M[x]$ et que la restriction de $[x]$ à $H^1(H_0, T)$ appartient à $H^1_{\mathrm{br}}(H_0, T)$. Alors, on a*

(3.1.2)

$$\frac{\varphi-1}{M}.\mathrm{Ev}_{\sigma_0}(\mathrm{kol}^{(a)}_M([y])) \equiv a\Big(\frac{\mathrm{ev}(\mathrm{cores}([y])}{M} - \frac{N}{M}\mathrm{ev}([y])\Big) \bmod (\varphi-1)T$$
$$\equiv a\Big(\mathrm{ev}([x]) - \frac{N}{M}\mathrm{ev}([y])\Big) \bmod (\varphi-1)T.$$

Démonstration. — Vérifions d'abord que cela a bien un sens : $\mathrm{Ev}_{\sigma_0}(\mathrm{kol}^{(a)}_M([y]))$ est défini modulo MT et donc $\dfrac{\varphi-1}{M}\mathrm{Ev}_{\sigma_0}(\mathrm{kol}^{(a)}_M([y]))$ est

défini modulo $(\varphi - 1)T$, ev($[x]$) et ev($[y]$) sont définis modulo $(\varphi - 1)T$, enfin $N/M \in \mathcal{O}$. On note x et y des cocycles de $Z^1(\hat{\mathbb{Z}}, T)$ représentant les images de $[x]$ et $[y]$ dans $H^1(\hat{\mathbb{Z}}, T)$. Alors,

$$\text{cores}(y)(g) = Mx(g) + (g-1)\alpha \tag{3.1.3}$$

avec $\alpha \in T$. Par définition de $[z]$, on a

$$\text{Ev}_{\sigma_0}([z]) \equiv -a\alpha \bmod MT.$$

Il s'agit donc de calculer α mod MT. En évaluant (3.1.3) en φ et en remarquant que $\tilde{\sigma}_0(y)(\varphi) = y(\varphi)$, on obtient

$$Ny(\varphi) = Mx(\varphi) + (\varphi - 1)\alpha \bmod (M, N)T.$$

Comme N est divisible par M, on en déduit la formule (3.1.2). □

3.2. Dérivations des systèmes d'Euler p-adiques.

3.2.1. Remarquons que si $V^H = 0$ pour un sous-groupe fermé H de $G_{S,\mathbb{Q}}$, $(V/T)^H$ est fini. D'autre part, pour tout sous-groupe H fermé distingué dans $G_{\mathbb{Q}}$, V^H est stable par G/H et est donc une sous-représentation de V ; comme V est une représentation irréductible de $G_{\mathbb{Q}}$, cela implique que $V^H = 0$ ou $V^H = V$. Ainsi s'il existe un entier m tel que $V^{G_{\mathbb{Q}(\mu_{mp^\infty})}}$ soit non nul, l'action de $G_{\mathbb{Q}}$ se factorise par $G_{\mathbb{Q}^{\text{ab}}}$ où $\mathbb{Q}^{\text{ab}} = \bigcup_m \mathbb{Q}(\mu_m)$ la plus grande extension abélienne de $\mathbb{Q}$. Comme V est irréductible, elle est alors de dimension 1. Dans ce cas, elle est donnée par un caractère de $G_{\mathbb{Q}}$ à valeurs dans $\mathcal{O}^\times$. Si ce caractère n'est pas d'ordre fini, $V^{G_{\mathbb{Q}(\mu_m)}} = 0$ est toujours vrai et les $(V/T)^{G_{\mathbb{Q}(\mu_m)}} = 0$ sont d'ordre borné à condition de prendre m divisible au plus par une puissance de p fixée. Si le caractère est d'ordre fini et de conducteur $m_0 \neq 1$, les conditions précédentes sont vérifiées à condition de se restreindre aux entiers m premiers à m_0, c'est-à-dire à $\Sigma(V)$.

On déduit de ces remarques que :

(1) Pour tout entier m (premier à $\Sigma(V)$ si V est de dimension 1), $V^{G_{\mathbb{Q}(\mu_m)}} = 0$; il existe donc un entier $a_m(T)$ annulant $(V/T)^{G_{\mathbb{Q}(\mu_m)}}$ et $(T/MT)^{G_{\mathbb{Q}(\mu_m)}}$ pour toute puissance M de p ;

(2) les $a_m(T)$ (pour m premier à $\Sigma(V)$ si V est de dimension 1) sont bornés par un entier $a(T)$.

Ainsi, la condition $V^{G_{\mathbb{Q}(\mu_m)}} = 0$ imposée pour que m soit fortement admissible est presque toujours vérifiée. On fixe $a = a(T)$ (on a en fait besoin, à m fixé, d'un entier annulant $(V/T)^{G_{\mathbb{Q}(\mu_m)}}$ et les $(V/T)^{G_{\mathbb{Q}(\mu_{ml_1\dots l_r})}}$ pour l_i des nombres premiers distincts premiers à mp et à $\Sigma \cup \Sigma(V)$, ce qui existe dès que m est fortement admissible).

3.2.2. Choisissons une famille de racines de l'unité $\zeta = (\zeta_n)_{n\in\mathbb{N}}$, avec ζ_n d'ordre n, telles que $\zeta_{nn'}^{n'} = \zeta_n$ (voir 1.4.1). Notons $\mathbb{Q}^{ab,l}$ la réunion des $\mathbb{Q}(\mu_m)$ pour m premier à l. On note σ_l l'élément de $\mathrm{Gal}(\mathbb{Q}^{ab,l}(\mu_l)/\mathbb{Q}^{ab,l})$ défini par

$$\frac{\sigma_l(\sqrt[l-1]{\Pi})}{\sqrt[l-1]{\Pi}} = \zeta_{l-1}$$

pour Π uniformisante de $\mathbb{Q}^{ab,l}$ (par exemple l) et $\sigma_l^{(m)}$ sa restriction à $\mathbb{Q}(\mu_{ml})$ (c'est donc un élément d'ordre $l-1$ de $\mathrm{Gal}(\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m))$. Si λ est une place au-dessus de l, on note $\sigma_\lambda = \sigma_\lambda^{(m)}$ son prolongement à $\mathbb{Q}(\mu_{ml})_\lambda$.

3.2.3. Soit c un système d'Euler p-adique ou d'Euler-Iwasawa p-adique de rang 1. Soit $l \in S(m)$. L'homomorphisme Frob_l agit trivialement sur $\mathbb{Q}(\mu_m)$ et on a

$$\mathrm{Tr}_l(c(ml)) = P_l(V^*(1), \mathrm{Frob}_l^{-1})c(m) = P_l(V^*(1), 1)\ c(m).$$

Comme $P_l(V^*(1), 1)$ est divisible par $l-1$, on est dans la situation du paragraphe 3.1 avec $G = G_{\mathbb{Q}(\mu_m)}$ et $H = G_{\mathbb{Q}(\mu_{ml})}$ et $N = l-1$ et M une puissance de p divisant $l-1$. On note

$$d_M^{(a)}(m; l) = \mathrm{kol}_{H,M}^{(a)}(c(ml))$$

avec $\sigma = \sigma_l^{(m)}$ et

$$d^{(a)}(m; l) = d_{H,(l-1)_p}^{(a)}(m; l)$$

(si N est un entier, on note N_p la plus grande puissance de p divisant N).

3.2.4. Proposition. — *Pour toute place v de $\mathbb{Q}(\mu_m)$ ne divisant pas p ou l et telle que $c(ml)$ est non ramifié en v, $d^{(a)}(m; l)$ est non ramifié : son image $d^{(a)}(m; l)_v$ par localisation en v appartient à*

$$H^1_{\mathrm{br}}(\mathbb{Q}(\mu_m)_v, T/(l-1)T) \overset{\text{déf}}{=} H^1(\mathbb{Q}(\mu_m)_v^{nr}/\mathbb{Q}(\mu_m)_v, T/(l-1)T)$$

où $\mathbb{Q}(\mu_m)_v^{nr}$ est la plus grande extension non ramifiée de $\mathbb{Q}(\mu_m)_v$.

Démonstration. — On utilise d'une part le fait que $\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)$ est non ramifiée en v et donc que le noyau de l'application restriction

$$H^1(\mathbb{Q}(\mu_m)_v, T/(l-1)T) \to H^1(\mathbb{Q}(\mu_{ml})_v, T/(l-1)T)$$

est contenu dans $H^1_{\mathrm{br}}(\mathbb{Q}(\mu_m)_v, T/(l-1)T)$ et d'autre part le fait que les composantes de $D^{(a)}_{\sigma_l}(c(ml))$ appartiennent, de même que $c(ml)$, à $H^1_{\mathrm{br}}(\mathbb{Q}(\mu_{lm})_v, T/(l-1)T)$. □

3.2.5. Soit λ une place de $\mathbb{Q}(\mu_m)$ au-dessus de l. On désire calculer le localisé de $d(m;l)$ en λ. Pour cela, on applique les paragraphes 3.1.4 et suivants avec pour G_0 le groupe de décomposition de λ. Notons $\mathrm{Ev}_{\lambda,\sigma_\lambda}$, ev_λ les applications Ev_{σ_0} et ev correspondant à la place λ. Enfin, posons

$$\tilde{P}_l(V^*(1), X) = \frac{P_l(V^*(1), X) - P_l(V^*(1), 1)}{X - 1}.$$

3.2.6. Proposition. — i) *L'idéal $\mathcal{B}(m)$ annule*

$$\prod_{\lambda|l}(\mathrm{Ev}_{\lambda,\sigma_\lambda}(d^{(a)}(m;l)) - a\varphi_\lambda^{-1}\tilde{P}_l(V^*(1), \varphi_\lambda^{-1})\mathrm{ev}_\lambda(c(m)))$$

pour tout entier m et pour tout $l \in S_*(m)$ tels que $c(ml)$ soit non ramifié en l et $P_l(V,1) \neq 0$.

ii) *Si de plus p divise m et c d'Euler-Iwasawa, on a*

$$\mathrm{Ev}_{\lambda,\sigma_\lambda}(d^{(a)}(m;l)) = a\varphi_\lambda^{-1}\tilde{P}_l(V^*(1), \varphi_\lambda^{-1})\mathrm{ev}_\lambda(c(m)).$$

Démonstration. — On fait la démonstration de (i). Posons $Q_l(X) = P_l(V^*(1), X)$. D'après l'équation (3.1.2), on a

$$\frac{\varphi_\lambda - 1}{l-1}\mathrm{Ev}_{\lambda,\sigma_\lambda} d^{(a)}(m;l) = a\Big(\frac{Q_l(1)}{l-1}\mathrm{ev}_\lambda(c(m)) - \mathrm{ev}_\lambda(c(ml))\Big).$$

Soit b un élément de $\mathcal{B}(m)$. Comme

$$b\prod_\lambda \mathrm{ev}_\lambda(c(ml)) = b\prod_\lambda Z(\lambda)\mathrm{ev}_\lambda(c(m)) \in \prod_\lambda T/(\varphi_\lambda - 1)T$$

avec $Z(\lambda) = \dfrac{Q_l(\varphi_\lambda^{-1})}{l-1}$, on a

$$b\prod_\lambda \frac{\varphi_\lambda - 1}{l-1}\mathrm{Ev}_{\lambda,\sigma_\lambda} d(m;l)$$

$$= -ba\prod_\lambda \frac{Q_l(\varphi_\lambda^{-1}) - Q_l(1)}{l-1}\mathrm{ev}_\lambda(c(m)) \in \prod_\lambda T/(1-\varphi_\lambda)T.$$

En multipliant par $(l-1)(\varphi_l-1)^{-1}$, on obtient dans $\prod_\lambda T/(l-1)T$,

$$b\prod_\lambda \mathrm{Ev}_{\lambda,\sigma_\lambda} d(m;l) = ba\prod_\lambda \tilde{Q}_l(\varphi_\lambda^{-1})\varphi_\lambda^{-1}\mathrm{ev}_\lambda(c(m)).$$

La démonstration est identique dans le cas (ii) (on peut alors prendre $b=1$). □

3.2.7. Posons $H^1_{/br}(F_\lambda, A) = H^1(F_\lambda, A))/H^1_{\mathrm{br}}(F_\lambda, A)$ pour A G_{F_λ}-module continu. Notons

$$< .,. >_\lambda : H^1_{\mathrm{br}}(F_\lambda, T) \times H^1_{/br}(F_\lambda, V^*(1)/T^*(1)) \to \mathcal{E}/\mathcal{O}$$

l'accouplement de dualité locale et pour M un entier,

$$< .,. >_\lambda^{(M)} : H^1_{\mathrm{br}}(F_\lambda, T/MT) \times H^1_{/br}(F_\lambda, T^*(1)/MT^*(1)) \to \mathcal{O}/M\mathcal{O}$$

l'accouplement qui s'en déduit. Notons

$$[.,.]_\zeta^{(M)} : T/MT \times T^*(1)/MT^*(1) \to \mathcal{O}/M\mathcal{O}$$

l'accouplement induit par l'accouplement naturel

$$T/MT \times T^*/MT^* \to \mathcal{O}/M\mathcal{O}$$

et par l'isomorphisme

$$\begin{array}{ccc} \mathbb{Z}/M\mathbb{Z} \cong & \mu_M & = \mathbb{Z}(1)/M\mathbb{Z}(1) \\ x \mapsto & \zeta_M^x & \mod M. \end{array}$$

Si $g \in G_{\mathbb{Q}}$, on a $[ga, gb]_\zeta^{(M)} = \chi(g)[a,b]_\zeta^{(M)}$. En particulier, pour $l \in S(Mm)$ et λ divisant l, $[\varphi_\lambda a, b]_\zeta^{(M)} = [a, \varphi_\lambda^{-1} b]_\zeta^{(M)}$.

3.2.8. Lemme. — *Soient $x \in H^1(\mathbb{Q}(\mu_m)_\lambda, T/MT)$ et $y \in H^1_{\mathrm{br}}(\mathbb{Q}(\mu_m)_\lambda,)$ $T^*(1)/MT^*(1)$. Alors*

$$< x, y >_\lambda^{(M)} = [\mathrm{Ev}_{\lambda,\sigma_l}(x), \mathrm{ev}_\lambda(y)]_\zeta^{(M)}.$$

Pour une démonstration, voir l'appendice A.

3.2.9. Proposition. — *Soit $l \in S_*(m)$. On suppose toujours $P_l(V,1) \neq 0$ et $c(ml)$ non ramifié en l. Soit M un diviseur de $l-1$ et soit $y \in H^1_{\mathrm{br}}(\mathbb{Q}(\mu_m)_\lambda, T^*(1)/MT^*(1))$. Alors,*

(3.2.1)

$$(< d_M^{(a)}(m,l)_\lambda, y >_\lambda^{(M)} - a[\tilde{P}_l(V^*(1), \varphi_\lambda^{-1})\varphi_\lambda^{-1}\mathrm{ev}_\lambda(c(m)_\lambda), \mathrm{ev}_\lambda(y)]_\zeta^{(M)})_\lambda$$

est annulé par l'idéal $\mathcal{B}(m)$ et est nul si m est divisible par p et c d'Euler-Iwasawa (λ parcourt les places de $\mathbb{Q}(\mu_m)$ au-dessus de l).

Démonstration. — La dernière expression a un sens : comme $\mathrm{ev}_\lambda(c(m))$ est défini modulo $(\varphi_\lambda - 1)T$, $\tilde{P}_l(V^*(1), \varphi_\lambda^{-1})\varphi_\lambda^{-1}\mathrm{ev}_\lambda(c(m))$ est défini modulo $P_l(V^*(1), \varphi_\lambda^{-1})(T)$ qui est contenu dans $(l-1)T$; $\mathrm{ev}_\lambda(y)$ est défini modulo $(\varphi_\lambda - 1)T^*(1) + MT^*(1)$ et comme $[\varphi_\lambda a, b]_\zeta^{(M)} = [a, \varphi_\lambda^{-1} b]_\zeta^{(M)}$, on est ramené au calcul précédent. La proposition se déduit des lemmes 3.2.6 et 3.2.8. □

3.3. Généralisation.

3.3.1. Si m est un entier sans facteurs carrés, on pose $D_m = \prod_{l|m} D_{\sigma_l}$.

LEMME. — *Soit c un système d'Euler p-adique de rang 1. Soient m un entier admissible, M_m la puissance de p maximale divisant les $l-1$ pour $l|m$ et m_0 un entier premier à m et fortement admissible. Alors, l'image de $D_m(c(mm_0))$ dans $H^1(\mathbb{Q}(\mu_{mm_0}), T/M_mT)$ est invariante par $\Delta_m \cong \mathrm{Gal}(\mathbb{Q}(\mu_{mm_0})/\mathbb{Q}(\mu_{m_0}))$.*

Démonstration. — Cela se démontre par récurence sur le nombre de l premiers divisant m. Ecrivons $m = lm'$. On a

$$\begin{aligned}(\sigma_l - 1)D_{m'}(c(m_0m'l)) &= (l-1)c(m_0m'l) - \mathrm{cores}_{\Delta_l}(D_{m'}(c(m_0m'l))) \\ &= (l-1)c(m_0m'l) - P_l(V^*(1), \varphi_l^{-1})(D_{m'}(c(m_0m'))).\end{aligned}$$

Comme $D_{m'}(c(m_0m'))$ est invariant par $\Delta_{m'}$ dans $H^1(\mathbb{Q}(\mu_{m_0m'}), T/M_mT)$ par hypothèse de récurence et que φ_l appartient à $\Delta_{m'}$, on en déduit que

$$P_l(V^*(1), \varphi_l^{-1})(D_{m'}(c(m_0m'))) \equiv P_l(V^*(1), 1)D_{m'}(c(m_0m')) \bmod M_m.$$

Comme M_m divise $P_l(V^*(1), 1)$, on en déduit le lemme. □

Si M est une puissance de p divisant M_m, on note $d_M^{(a)}(m_0; m) \in H^1(\mathbb{Q}(\mu_{m_0}, T/MT)$ l'élément dont la restriction à $H^1(\mathbb{Q}(\mu_{mm_0}), T/MT)$ est l'image de $aD_m(c(mm_0))$.

3.3.2. LEMME. — *On suppose vérifiées les conditions du lemme 3.3.1. Soit M une puissance de p divisant M_m. On suppose que pour $l|m$, $c(mm_0)$ est non ramifié en l et $P_l(V, 1) \neq 0$. Alors, $d_M^{(a)}(m_0; m)$ est non ramifié en dehors des nombres premiers divisant m et pour $l|m$*

$$(\mathrm{Ev}_{\lambda,\sigma_\lambda}(d_M^{(a)}(m_0; m)) - \tilde{P}_l(V^*(1), \varphi_\lambda^{-1})\mathrm{ev}_\lambda(d_M^{(a)}(m_0; m/l)))_{\lambda|l}$$

est annulé par l'idéal $\mathcal{B}(m_0)$ et est nul si p divise m_0 et c d'Euler-Iwasawa.

3.4. Réinterprétation.

3.4.1. Soit f un endomorphisme de V laissant stable T, de déterminant 1 et tel que $V/(f-1)V$ soit de dimension 1. Soit $Q'(X) = X\det(f-X)$, $\tilde{Q}'(X) = Q'(X)/(X-1)$. On a donc $(f-1)\tilde{Q}'(f) = 0$. Dès que V est de dimension > 1, $\tilde{Q}'(f) \neq 0$. Comme $\ker(f-1)$ est de dimension 1 et que $\mathrm{Im}\ \tilde{Q}'(f)$ est contenu dans $\ker(f-1)$, les sous-espaces vectoriels $\mathrm{Im}\ \tilde{Q}'(f)$ et $\ker(f-1) = V^{f=1}$ sont égaux. L'homomorphisme $\tilde{Q}'(f)$ induit un isomorphisme d'espaces vectoriels $V/(1-f)V \to \tilde{Q}'(f)V = V^{f=1}$. Si on le restreint à T, il induit un homomorphisme de $\mathcal{O}$-modules à noyau et conoyau finis $T/(1-f)T \to T^{f=1}$. Enfin, par passage au quotient par MT pour M une puissance de p, on obtient un homomorphisme à noyau et conoyau finis d'ordre borné par rapport à M

$$T/(1-f, M)T \to (T/MT)^{f=1},$$

(le conoyau de $T^{f=1}/MT^{f=1} \to (T/MT)^{f=1}$ est $MT \cap (f-1)T/(f-1)MT$ qui est fini d'ordre borné par rapport à M, son noyau est nul).

3.4.2. Soit maintenant l un nombre premier, $l \in S_{f,M}(Mm)$: pour une place λ de $\mathbb{Q}(\mu_{Mm})$ au-dessus de l, φ_λ^{-1} agit sur T/MT comme f. On prend $F = \mathbb{Q}(\mu_m)$ ou $F = \mathbb{Q}(\mu_{mM})$. L'opérateur $f\tilde{Q}'(f) \equiv \varphi_\lambda^{-1}\tilde{Q}(\varphi_\lambda^{-1}) \bmod M$ avec $Q(X) = \det(f - X)$ induit un homomorphisme de $\mathcal{O}$-modules à noyau et conoyau finis d'ordre borné par rapport à M

$$T/(\varphi_\lambda - 1, M)T \to (T/MT)^{\varphi_\lambda = 1}.$$

En utilisant les homomorphismes ev_λ et Ev_λ, on en déduit un homomorphisme

$$\mathrm{Dér}_{\lambda,M} : H^1_{\mathrm{br}}(F_\lambda, T/MT) \to H^1_{/br}(F_\lambda, T/MT)$$

à noyaux et conoyaux finis d'ordre borné par rapport à M et ne dépendant que de f. Remarquons que comme $\det(f) = 1$, on a

$$\det(1 - Xf|V^*(1)) = \det(1 - Xf|V^*) = \det(1 - Xf^{-1}|V) = \det(f - X|V).$$

Ainsi, dans l'expression $\varphi_\lambda^{-1}\tilde{Q}(\varphi_\lambda^{-1}) \bmod M$, on peut remplacer Q par $P_l(V^*(1), X)$ et $\tilde{Q}$ par $P_l(V^*(1), X)/(X-1)$.

Les résultats des paragraphes 3.2 et 3.3 se résument alors en la proposition suivante.

3.4.3. Proposition. — *Soit c un système d'Euler p-adique (resp. un système d'Euler-Iwasawa p-adique) de rang 1. Soit f un endomorphisme*

laissant stable T, de déterminant 1, tel que $V/(f-1)V$ soit de dimension 1 et vérifiant la condition (**). On suppose vérifiées les conditions du lemme 3.3.1. Soit $l \in S_{f,M}(Mm)$ tel que $P_l(V,1) \neq 0$ et $c(lmm_0)$ soit non ramifié en l. Alors,

$$(d_M^{(a)}(m_0;ml) - \mathrm{Dér}_{\lambda,M} d_M^{(a)}(m_0;m))_\lambda$$

est annulé par $\mathcal{B}(m_0)$ (resp. est nul si p divise m_0) pour λ parcourant les places de $\mathbb{Q}(\mu_m)$ au-dessus de l. Ainsi, dans le deuxième cas pour $\lambda|l$, pour $p|m_0$, pour tout $y \in H^1_{\mathrm{br}}(F_\lambda, T^*(1)/MT^*(1))$,

$$\begin{aligned} < d_M^{(a)}(m_0;ml)_\lambda, y >_\lambda^{(M)} &=< \mathrm{Dér}_{\lambda,M} d_M^{(a)}(m_0;m), y >_\lambda^{(M)} \\ &= [\mathrm{Ev}_\lambda \mathrm{Dér}_{\lambda,M} d_M^{(a)}(m_0;m), \mathrm{ev}_\lambda(y)]_M^{(\zeta)}. \end{aligned}$$

4. Quelques résultats de cohomologie galoisienne.

4.1. Rappels sur l'image du groupe de Galois dans $GL(T)$.

4.1.1. Soit F une extension finie de $\mathbb{Q}$. On note $F(M)$ le corps $F\mathbb{Q}(M)$ avec $Q(M) = \mathbb{Q}(T/MT)$ et $F(p^\infty)$ la réunion des $F(M)$ pour M puissance de p. On pose $F'(M) = F(M)(\mu_M)$. Notons $G_F(T)$ l'image de G_F dans $GL(V) = GL_V(\mathcal{E})$; elle est en fait contenue dans $GL(T) = GL_T(\mathcal{O})$ et s'identifie à $\mathrm{Gal}(F(p^\infty)/F)$. Comme G_F est un groupe compact, son image $G_F(T)$ dans $GL(T)$ est un sous-groupe de Lie p-adique du groupe linéaire $GL(T)$. L'algèbre de Lie $\mathcal{G}$ de $G_F(T)$ ne dépend pas de l'extension finie F de $\mathbb{Q}$. Notons $\tilde{\mathcal{G}}$ l'algèbre de Lie de $G_{F(\mu_{p^\infty})}(T)$. Soit $G_{V,F}^{\mathrm{alg}}$ le groupe algébrique linéaire adhérence de Zariski de $G_F(T)$ dans GL_V. Rappelons quelques propriétés de ces groupes (voir en particulier [S67], [S76], [S94]).

4.1.2. (A_1) La représentation V est non ramifiée en dehors d'un ensemble fini de places et que sa restriction au groupe de décomposition en p est de Hodge-Tate. Par exemple, si V est géométrique, V vérifie ces conditions. Par un théorème de Bogomolov ([Bo80]), l'algèbre de Lie $\mathcal{G}$ est algébrique (cf. aussi [He81]). En particulier, l'algèbre de Lie de $G_{V,F}^{\mathrm{alg}}$ est égale à $\mathcal{G}$. On en déduit que $G_F(T)$ est ouvert dans $G_{V,F}^{\mathrm{alg}}(\mathcal{E})$ pour toute extension F finie de $\mathbb{Q}$. Ainsi, si l'on note $G_{T,F}^{\mathrm{alg}}(\mathcal{O}) = G_{V,F}^{\mathrm{alg}}(\mathcal{E}) \cap GL(T)$, l'image $G_F(T)$ de G_F est contenue dans $G_{T,F}^{\mathrm{alg}}(\mathcal{O})$ et y est d'indice fini. Enfin, la composante connexe $G_V^{alg,o}$ de $G_{V,F}^{\mathrm{alg}}$ ne dépend pas de F et est égale à $G_{V,F}^{\mathrm{alg}}$ pour une extension finie F de $\mathbb{Q}$ convenable.

Rappelons d'autre part que si G est un groupe de Lie p-adique compact et si A est un G-module fini, les groupes de cohomologie $H^i(G, A)$ sont finis ([L65]), ce qu'on appliquera à $G = G_F(T)$.

4.1.3. (A_2) Supposons de plus que V est une représentation linéaire semi-simple de $G_{\mathbb{Q}}$. Pour toute extension galoisienne F de $\mathbb{Q}$, les groupes $G_{V,F}^{\mathrm{alg}}$ sont réductifs. L'algèbre de Lie $\mathcal{G}$ est réductive de même que l'algèbre de Lie $\tilde{\mathcal{G}}$ de $G_{\mathbb{Q}(\mu_{p^\infty})}$ (qui est aussi l'algèbre de Lie de $G_{\mathbb{Q}(\mu_{mp^\infty})}$ pour tout entier m).

4.1.4. (A_3) Avec les hypothèses précédentes (essentiellement V de Hodge-Tate en p), le déterminant $\det(V)$ est donné par un caractère de la forme $\epsilon < \chi >^r$ où $r \in \mathbb{Z}$, ϵ est un caractère d'ordre fini et $< \chi >$ est la p-composante du caractère cyclotomique : $< \chi >: G_{\mathbb{Q}} \to 1 + p\mathbb{Z}_p$. Ainsi, si $r \neq 0$, la $\mathbb{Z}_p$-extension cyclotomique $\mathbb{Q}_\infty$ est contenue dans $F(p^\infty)$. Si $r = 0$ et V est irréductible, par contre, la $\mathbb{Z}_p$-extension cyclotomique $\mathbb{Q}_\infty$ n'est pas contenue dans $F(p^\infty)$.

4.1.5. (A_4) On dit que V est une représentation pure de poids w si elle est géométrique et si pour presque toute place v de $\mathbb{Q}$ différente de p, les coefficients du polynôme caractéristique de l'endomorphisme de Frobenius agissant sur V sont dans $\mathbb{Q}$ et ses racines sont des nombres de Weil de poids w (ainsi, si α est une telle valeur propre, toutes ses valeurs absolues archimédiennes sont égales à $Nv^{-w/2}$) ; on dispose d'un morphisme poids w du groupe multiplicatif $\mathbb{G}_{\geqslant}$ dans la composante connexe du centre de G_V^{alg} donné par

$$w(t) = t^w \mathrm{Id}_V.$$

Il est démontré [S76] que $w(\mathbb{G}_m)$ est contenu dans $G_V^{alg,o}$ et même dans la composante neutre du centre de $G_F(T)$. En particulier, pour toute extension finie F de $\mathbb{Q}$, $G_F(T)$ contient un sous-groupe d'indice fini de $w(\mathbb{Z}_p^\times)$. On a $\det(V) = \epsilon < \chi >^{-wd/2}$.

Les propriétés d'algébricité ne seront pas utiles dans la suite. Elles le sont par contre quand il s'agit de vérifier l'hypothèse (Tech). Ainsi, par exemple, si $G_{V,\mathbb{Q}}^{\mathrm{alg}}$ est le groupe des similitudes symplectiques ou des similitudes orthogonales relatives à une forme bilinéaire symétrique non dégénérée, l'hypothèse (Tech) est alors vérifiée.

4.2. Finitude de groupes de cohomologie.

Nous supposons que V est irréductible sur $G_{\mathbb{Q}}$.

4.2.1. Nous avons en vue de montrer sous certaines conditions que les groupes $H^i(F(M)/F, T/MT)$ sont d'ordre borné par rapport à M, puis d'étudier leur variation lorsque F parcourt les sous-extensions finies de $\mathbb{Q}(\mu_{mp^\infty})$. Dans la suite, M est toujours une puissance de p.

4.2.2. PROPOSITION. — *Soit F une extension finie galoisienne de $\mathbb{Q}$ et $\tilde{F} = F$ ou F_∞. Les $\mathcal{E}$-espaces vectoriels $H^i(G_{\tilde{F}}(T), V)$ sont nuls pour $i \leqslant 2$.*

Démonstration. — Soit $\mathcal{G}'$ l'algèbre de Lie de $G_{\tilde{F}}(T)$ (elle est égale à $\mathcal{G}$ si $\tilde{F} = F$ et à $\tilde{\mathcal{G}}$ si $\tilde{F} = F_\infty$). Supposons le centre de $\mathcal{G}'$ non trivial. Quitte à remplacer F par une extension finie galoisienne sur $\mathbb{Q}$, on peut supposer que le centre $Z_{\tilde{F}}$ de $G_{\tilde{F}}(T)$ est non trivial. Il est alors distingué dans $G_{\mathbb{Q}}(T)$: en effet, $G_{\tilde{F}}(T)$ est distingué dans $G_{\mathbb{Q}}(T)$ et si $g \in G_{\mathbb{Q}}(T)$, $z \in Z_F$ et $h \in G_{\tilde{F}}(T)$, on a

$$gzg^{-1}hgz^{-1}g^{-1}h^{-1} = gz(g^{-1}hg)z^{-1}g^{-1}h^{-1} = gg^{-1}hgg^{-1}h^{-1} = 1.$$

On en déduit que $V^{Z_{\tilde{F}}}$ est stable par $G_{\mathbb{Q}}(T)$ et donc, comme V est irréductible sur $\mathbb{Q}$, soit $V^{Z_{\tilde{F}}} = 0$, soit $V^{Z_{\tilde{F}}} = V$. Comme de plus $G_{\tilde{F}}(T)$, et donc $Z_{\tilde{F}}$, s'injecte dans $GL(T)$, on en déduit que $V^{Z_{\tilde{F}}} = 0$.

Soit maintenant α un élément de $Z_{\tilde{F}}$ différent de 1. Alors, $V^{\alpha=1}$ est stable par $G_{\tilde{F}}$. Si V est irréductible sur $G_{\tilde{F}}$, on a encore nécessairement $V^{\alpha=1} = 0$ et on en déduit que les $H^i(G_{\tilde{F}}(T), V)$ sont nuls : comme le sous-groupe $< \alpha >$ engendré par α est distingué dans $G_{\tilde{F}}(T)$, par la suite spectrale de Hochschild-Serre, il suffit de vérifier que $V^{\alpha=1} = 0$ et $H^1(< \alpha >, V) \cong V/(\alpha - 1)V = 0$. Dans le cas général, écrivons $V = \oplus W_i$ où les W_i sont irréductibles (la restriction de V à $G_{\tilde{F}}$ est semi-simple). Comme $V^{Z_{\tilde{F}}} = 0$, pour tout i, il existe $\alpha \in Z_{\tilde{F}}$ tel que $W_i^{\alpha=1} = 0$. On en déduit comme précédemment que $H^i(G_{\tilde{F}}(T), W_i) = 0$ et donc que $H^i(G_{\tilde{F}}(T), V) = 0$ pour tout $i \geqslant 0$.

Supposons maintenant que le centre de $\mathcal{G}'$ est trivial. Comme V est irréductible, $\mathcal{G}'$ est semi-simple. Par un résultat de Lazard ([L65], cf. [S67] dans le cas où $i = 1$), l'application naturelle $H^i(G_{\tilde{F}}(T), V)$ dans $H^i(\mathcal{G}', V)$ est injective (les groupes de cohomologie $H^i(G_{\tilde{F}}(T), V)$ pouvant être calculés indifféremment avec des cocycles continus ou analytiques). Un théorème de Chevalley-Eilenberg ([CH48]) affirme alors que, comme $\mathcal{G}'$ est une algèbre de Lie semi-simple, $H^i(\mathcal{G}', V)$ est nul pour $i = 1, 2$ (et, mais nous n'en aurons pas besoin, que si la représentation triviale n'intervient pas dans le $\mathcal{G}'$-module V, $H^i(\mathcal{G}', V)$ est nul aussi pour $i \geqslant 3$). On en déduit la nullité des $H^i(G_{\tilde{F}}(T), V)$. □

Remarque. — On a en fait montré que si le centre de $\mathcal{G}'$ est non trivial ou si la représentation trivale n'intervient pas dans le $\mathcal{G}'$-module V, les $H^i(G_{\tilde{F}}(T), V)$ sont nuls pour tout i.

4.2.3. Corollaire. — *Si F est une extension finie galoisienne de $\mathbb{Q}$ et si $\tilde{F} = F$ ou F_∞, les $H^i(G_{\tilde{F}}(T), T/MT)$ sont finis d'ordre borné.*

Démonstration. — On utilise le fait que

$$\mathbb{Q}_p \otimes H^i(G_{\tilde{F}}(T), T) = H^i(G_{\tilde{F}}(T), V)$$

([Tate]), que les $H^i(G_{\tilde{F}}(T), T)$ sont de type fini et que l'on a la suite exacte

$$0 \to H^i(G_{\tilde{F}}(T), T)/M \to H^i(G_{\tilde{F}}(T), T/MT) \to H^{i+1}(G_{\tilde{F}}(T), T)_M \to 0.$$

□

4.2.4. Proposition. — *Supposons que F est une extension finie galoisienne de $\mathbb{Q}$. Les $H^1(F(M)/F, T/MT)$ sont finis d'ordre borné. Si de plus, la restriction de V à G_F n'est pas la représentation triviale, les $H^1(F'(M)/F, T/MT)$ sont finis d'ordre borné.*

Remarque. — Si V est la représentation triviale,

$$\begin{aligned} H^1(F'(M)/F, T/MT) &= H^1(F(\mu_M)/F, \mathcal{O}/M\mathcal{O}) \\ &= \mathrm{Hom}(\mathrm{Gal}(F(\mu_M)/F), \mathcal{O}/M\mathcal{O}), \end{aligned}$$

ce qui est non borné par rapport à M.

Démonstration. — La première assertion se déduit de l'injectivité de l'application inflation $H^1(F(M)/F, T/MT) \to H^1(G_F(T), T/MT)$. Montrons la seconde. Lorsque F_∞ est contenu dans $F(p^\infty)$, cela est clair car $F'(M)/F(M)$ est de degré premier à p. Lorsque F_∞ n'est pas contenu dans $F(p^\infty)$, posons $F_0 = F_\infty \cap F(p^\infty)$. Ainsi, $\mathrm{Gal}(F(\mu_M)/F_0)$ agit trivialement sur $(T/MT)^{G_{F(\mu_M)}}$. Il suffit alors de montrer que les $H^1(F(\mu_M)/F_0, (T/MT)^{G_{F_0}})^{\mathrm{Gal}(F_0/F)}$ sont finis d'ordre borné. C'est clairement le cas lorsque $V^{G_{F_0}}$ est nul. Dans le cas contraire, $V = V^{G_{F_0}}$; cela implique que V est de dimension 1 donné par un caractère d'ordre fini ϵ trivial sur F_0. On a

$$\begin{aligned} &H^1(F(\mu_M)/F_0, (T/MT)^{G_{F_0}})^{\mathrm{Gal}(F_0/F)} \\ &\qquad \cong \mathrm{Hom}(\mathrm{Gal}(F(\mu_M)/F_0), (T/MT)^{G_F}). \end{aligned}$$

Si ϵ n'est pas trivial sur G_F, ces groupes sont finis d'ordre borné par rapport à M. □

4.2.5. Soit M' un entier divisant M. La suite exacte

$$0 \to M'T/MT \to T/MT \to T/M'T \to 0 \tag{4.2.1}$$

induit la suite exacte

$$(T/MT)^{G_F} \to (T/M'T)^{G_F} \to H^1(F'(M)/F, M'T/MT) \to H^1(F'(M)/F, T/MT).$$

En particulier, si $V^{G_F} = 0$ (ce qui est le cas si V n'est pas la représentation triviale sur G_F), $H^1(F'(M)/F, M'T/MT)$ est d'ordre borné par rapport à M. Ainsi, pour tout entier M'' divisant M, les $H^1(F'(M)/F, T/M''T)$ sont d'ordre borné. On note s_F un entier divisible par l'ordre de $H^1(F'(M)/F, T/MT)$ et de $H^1(F'(M)/F, T/M'T)$ pour $M'|M$ ainsi que de $H^1(F'(M)/F, T^*(1)/MT^*(1))$.

Remarquons que $s_{\mathbb{Q}(\mu_m)}$ est fini sous les mêmes conditions que $a_m(T)$ (cf. 3.2.1).

4.2.6. *Remarque.* — Supposons que T/pT est absolument irréductible et n'est pas isomorphe à la représentation adjointe de G_F sur $\mathcal{G}/p\mathcal{G}$ et que $H^1(F(p)/F, T/pT) = 0$. Alors, $s_F = 1$. En effet, on a $(T/pT)^{G_F} = 0$ et il en est donc de même pour $(T/MT)^{G_F} = 0$. Par utilisation de la suite exacte de cohomologie déduite de (4.2.1) pour $M' = M/p$, la nullité de $\mathrm{Hom}(\mathrm{Gal}(F(M)/F(p), T/pT)^{G_F}$ implique celle de $H^1(F(M)/F, T/MT)$. On remarque alors que $\mathrm{Gal}(F(M)/F(p)) \cong \mathcal{G}/M'\mathcal{G}$ en tant que représentation de G_F (cf. l'appendice C). Dans [Fl92], le cas où V est la représentation adjointe d'une représentation de dimension 2 est traité (voir un résumé dans l'appendice C).

4.3. Variation avec $F_n \subset F_\infty$.

LEMME. — *Pour $F/\mathbb{Q}$ une extension finie galoisienne, les $H^1(F_n(M)/F_n, T/MT)$ sont finis d'ordre borné par rapport à n et M. Si de plus V ne se factorise pas par une extension finie de G_{F_∞}, les $H^1(F'_n(M)/F_n, T/MT)$ sont finis d'ordre borné par rapport à n et M.*

Démonstration. — La deuxième assertion se déduit de la première en reprenant la démonstration de la proposition 4.2.4 pour F_n contenu dans F_∞. Montrons la première assertion. Supposons d'abord que $V^{G_{F_\infty}} = 0$. D'après le corollaire 4.2.3 pour F extension finie galoisienne de $\mathbb{Q}$, les $H^1(G_{F_\infty}(T), T/MT)$ sont finis et d'ordre borné par rapport à M. On a

la suite exacte inflation-restriction :

$$O \to H^1(F_\infty/F_n, (T/MT)^{G_{F_\infty}}) \to H^1(G_{F_n}(T), T/MT) \\ \to H^1(G_{F_\infty}(T), T/MT)^{\mathrm{Gal}(F_\infty/F_n)}.$$

Comme $V^{G_{F_n}} = 0$, les $(T/MT)^{G_{F_n}}$ sont finis d'ordre borné par rapport à M ; comme $V^{G_{F_\infty}} = 0$, ils sont d'ordre borné par rapport à n et M. Il en est donc de même des $H^i(F_\infty/F_n, (T/MT)^{G_{F_\infty}})$. On en déduit que les $H^1(G_{F_n}(T), T/MT)$ sont finis d'ordre borné par rapport à n et M. L'injectivité de l'application inflation

$$H^1(F_n(M)/F_n, T/MT) \to H^1(G_{F_n}(T), T/MT)$$

démontre le lemme dans ce cas. Supposons maintenant que $V = V^{G_{F_\infty}}$. Comme V est irréductible, elle est de dimension 1. On a alors $V = \mathcal{E}(\epsilon < \chi >^r)$ pour un caractère ϵ d'ordre fini. Pour $r \neq 0$, il suffit de montrer le lemme pour une extension finie F galoisienne telle $V \cong \mathcal{E}(\chi^r) = \mathcal{E} \otimes \mathbb{Z}_p(r)$ en tant que G_F-module. Pour $r \neq 0$, $F(M)$ diffère alors de $F(\mu_M)$ par une extension de degré borné et $H^i(F(\mu_M)/F(\mu_{p^n}), \mu_M^{\otimes r})$ est d'ordre borné par rapport à M. Lorsque $r = 0$, on a $F_n(M) = F_n K_\epsilon$ où K_ϵ est le corps fixé par le noyau de ϵ et l'assertion est claire. □

4.4. Étude des $\mathcal{O}[G_F]$-modules.

4.4.1. On suppose dans ce paragraphe que W est une représentation $\mathcal{E}$-adique semi-simple de $G_{S,F}$ telle que $W = \bigoplus_{i=1}^{s} V_i$ avec V_i des représentations irréductibles de $G_{S,F}$ non isomorphes. Pour tout i, on pose $\mathcal{K}_F^{(i)} = \mathrm{End}_{G_F}(V_i)$ et $\mathfrak{O}_F^{(i)} = \mathrm{End}_{G_F}(T_i)$. On pose $\mathcal{K}_F = \prod \mathcal{K}_F^{(i)}$, $\mathfrak{O}_F = \prod \mathfrak{O}_F^{(i)}$. Si $\underline{r} = (r_1, \ldots, r_s)$, on pose $W^{\underline{r}} = \oplus V_i^{r_i}$, $\mathcal{K}_F^{\underline{r}} = \prod \mathcal{K}_F^{(i)^{r_i}}$ et $\mathfrak{O}_F^{\underline{r}} = \prod \mathfrak{O}_F^{(i)^{r_i}}$. On a alors $\mathrm{End}_{G_F}(W^{\underline{r}}) = \prod_{i=1}^{s} M_{r_i}(\mathcal{K}_F^{(i)})$. On le note aussi $M_{\underline{r}}(\mathcal{K}_F)$. On pose $GL_{\underline{r}}(\mathcal{K}_F) = M_{\underline{r}}(\mathcal{K}_F)^* = \prod_{i=1}^{s} GL_{r_i}(\mathcal{K}_F^{(i)})$. On pose de même $M_{\underline{r}}(\mathfrak{O}_F) = \prod_{i=1}^{s} M_{r_i}(\mathfrak{O}_F^{(i)})$.

On désigne par G_F-réseau $\mathcal{W}$ de W un $\mathcal{O}$-réseau de W (c'est-à-dire un sous-$\mathcal{O}$-module libre de type fini contenu dans W et tel que $\mathcal{E} \otimes \mathcal{W} = W$) stable par G_F. On fixe un G_F-réseau U de W et on pose $U_i = U \cap W_i$ et $U^{\underline{r}} = \oplus U_i^{r_i}$. Ainsi, $U^{\underline{r}}$ est un G_F-réseau de $W^{\underline{r}}$ et est muni d'une structure de $\mathfrak{O}_F$-module commutant avec l'action de G_F.

LEMME. — *Il existe un élément non nul $m(U)$ de $\mathcal{O}$ telle que pour tout $\underline{r}$, pour tout G_F-réseau $\mathcal{W}$ de $W^{\underline{r}}$, il existe un G_F-réseau $\mathcal{W}'$ de $W^{\underline{r}}$ équivalent à $U^{\underline{r}}$ pour l'action de $GL_{\underline{r}}(\mathcal{K}_F)$ tel que $m(U)\mathcal{W}' \subset \mathcal{W} \subset \mathcal{W}'$.*

Remarque. — Il existe un nombre fini de G_F-réseaux de $W^{\underline{r}}$ à équivalence près par l'action de $GL_{\underline{r}}(\mathcal{K}_F)$.

Démonstration. — Nous allons utiliser le théorème suivant (voir par exemple [Re, Theorem 18.7]) : Si A est une $\mathcal{E}$-algèbre semi-simple et $\bar{\mathfrak{O}}$ un ordre maximal de A, deux $\bar{\mathfrak{O}}$-modules (à gauche) $\mathcal{W}_1$ et $\mathcal{W}_2$ tels que $\mathcal{E} \otimes_{\mathcal{O}} \mathcal{W}_1 = \mathcal{E} \otimes_{\mathcal{O}} \mathcal{W}_2$ et qui sont libres de type fini en tant que $\mathcal{O}$-module sont isomorphes.

Prenons pour A la sous-$\mathcal{E}$-algèbre de $\mathrm{End}(W)$ engendrée par l'image de G_F dans $\mathrm{End}(W)$ et soit $\mathfrak{O}$ l'ordre de A engendré sur $\mathcal{O}$ par l'image de G_F dans $\mathrm{End}(U)$. Comme W est un A-module semi-simple et que A est contenu dans $\mathrm{End}(W) = \mathrm{End}_{\mathcal{E}}(W)$, l'algèbre A est semi-simple ([Bo, chap. 8, §9, 2]). D'autre part, $W^{\underline{r}}$ est naturellement un A-module et tout G_F-réseau de $W^{\underline{r}}$ contenu dans $U^{\underline{r}}$ est un $\mathfrak{O}$-module. Supposons d'abord que $\mathfrak{O}$ est un ordre maximal de A. On peut alors appliquer le théorème cité. Si $\mathcal{W}$ est un G_F-réseau de $W^{\underline{r}}$ (donc un sous-$\mathfrak{O}$-module de $W^{\underline{r}}$), il existe un automorphisme g de $W^{\underline{r}}$ commutant avec $\mathfrak{O}$, c'est-à-dire avec l'action de G_F et tel que $\mathcal{W} = g(U^{\underline{r}})$. Comme $\mathrm{End}_{G_F}(W^{\underline{r}}) = \mathrm{End}_A(W^{\underline{r}}) = M_{\underline{r}}(\mathcal{K}_F)$, les deux G_F-réseaux $\mathcal{W}$ et $U^{\underline{r}}$ sont équivalents par $GL_{\underline{r}}(\mathcal{K}_F)$ et la constante $m(U)$ peut être prise égale à 1. Si $\mathfrak{O}$ n'est pas maximal, il est contenu dans un ordre maximal $\bar{\mathfrak{O}}$; notons α l'indice de $\mathfrak{O}$ dans $\bar{\mathfrak{O}}$. Soit $\bar{\mathcal{W}} = \bar{\mathfrak{O}}\mathcal{W} \subset W^{\underline{r}}$ le $\bar{\mathfrak{O}}$-module engendré par $\mathcal{W}$ dans $\mathcal{E} \otimes_{\mathcal{O}} \mathcal{W} = W^{\underline{r}}$. Soit de même $\bar{U}^{\underline{r}} = \bar{\mathfrak{O}}U^{\underline{r}}$. Les deux $\bar{\mathfrak{O}}$-modules $\bar{U}^{\underline{r}}$ et $\bar{\mathcal{W}}$ étant deux $\mathcal{O}$-modules libres et vérifiant $\mathcal{E} \otimes_{\mathcal{O}} \bar{U}^{\underline{r}} = \mathcal{E} \otimes_{\mathcal{O}} \bar{\mathcal{W}}$, ils sont isomorphes en tant que $\bar{\mathfrak{O}}$-modules et donc équivalents sous l'action de $GL_{\underline{r}}(\mathcal{K}_F)$. Soit $g \in GL_{\underline{r}}(\mathcal{K}_F)$ tel que $\bar{\mathcal{W}} = g(\bar{U}^{\underline{r}})$; comme l'indice de $\mathfrak{O}$ dans $\bar{\mathfrak{O}}$ est α, les exposants de $\bar{\mathcal{W}}/\mathcal{W}$ et de $\bar{U}^{\underline{r}}/U^{\underline{r}}$ divisent α. On en déduit que $\mathcal{W}$ est contenu dans $g'(U^{\underline{r}})$ avec $g' = \alpha^{-1}g$ et que l'exposant de $g'(U^{\underline{r}})/\mathcal{W}$ divise α^2. On peut donc prendre pour $m(U)$ le carré de l'indice de $\mathfrak{O}$ dans $\bar{\mathfrak{O}}$. Ce qui termine la démonstration. □

4.4.2. Pour $\underline{a} = (\underline{a}_1, \ldots, \underline{a}_s) \in \mathcal{K}_F^{\underline{r}}$ et pour $\underline{w} = (\underline{w}_1, \ldots, \underline{w}_s) \in W^{\underline{r}}$, on pose $\underline{a}.\underline{w} = \left(\sum_{j=1}^{r_i} a_{ij} w_{ij} \right)_i$ avec $\underline{a}_i = (a_{ij})$ et $\underline{w}_i = (w_{ij})$. Soit $\mathcal{W}$ un G_F-réseau de $W^{\underline{r}}$ contenu dans $U^{\underline{r}}$ et contenant $MU^{\underline{r}}$. On pose

$$\mathfrak{a}_M(\mathcal{W}) = \{\underline{a} \in \mathfrak{O}_F^{\underline{r}} \text{ tq } \underline{a}.\underline{w} \in MU \text{ pour tout } \underline{w} \in \mathcal{W}\},$$
$$\mathfrak{b}_M(\mathcal{W}) = \{\underline{b} \in U^{\underline{r}} \text{ tq } \underline{a}.\underline{b} \in MU \text{ pour tout } \underline{a} \in \mathfrak{a}_M(\mathcal{W})\}.$$

4.4.3. Lemme. — *Soit $\mathcal{W} \subset U^{\underline{r}}$ un G_F-réseau de $W^{\underline{r}}$ contenant $MU^{\underline{r}}$. On a*

$$m(U)\mathfrak{b}_M(\mathcal{W}) \subset \mathcal{W} \subset \mathfrak{b}_M(\mathcal{W}).$$

Autrement dit, si $\underline{t} \in U^{\underline{r}}$ vérifie $\underline{a}.\underline{t} \in MU$ pour tout $\underline{a} \in \mathfrak{a}_M(\mathcal{W})$, $m(U)t$ appartient à $\mathcal{W}$.

Démonstration. — Il est clair que l'on a $\mathcal{W} \subset \mathfrak{b}_M(\mathcal{W})$. Soit $\mathcal{W}' = g(U^{\underline{r}})$ un G_F-réseau équivalent à $U^{\underline{r}}$ et tel que

$$m(U)\mathcal{W}' \subset \mathcal{W} \subset \mathcal{W}'.$$

Calculons $\mathfrak{a}_M(\mathcal{W}')$ puis $\mathfrak{b}_M(\mathcal{W}')$. On remarque que $\underline{a}.\underline{w} \in MU$ pour tout $\underline{w} \in \mathcal{W}'$ si et seulement si $\underline{a}g(\underline{t}) \in MU$ pour tout $\underline{t} \in U^{\underline{r}}$. Comme $\underline{a}g(\underline{t}) = {}^t g\underline{a}.\underline{t}$, $\underline{a} \in \mathfrak{a}_M(\mathcal{W}')$ si et seulement si ${}^t g\underline{a} \in M\mathfrak{O}_F^{\underline{r}}$ et donc $\mathfrak{a}_M(\mathcal{W}') = M{}^t g^{-1}\mathfrak{O}_F^{\underline{r}}$. Le même calcul montre que $\underline{t} \in \mathfrak{b}_M(\mathcal{W}')$ si et seulement si $\underline{t} \in g(U^{\underline{r}})$ et donc que $\mathfrak{b}_M(\mathcal{W}') = \mathcal{W}'$. Des inclusions (4.4.1), on déduit successivement que $\mathfrak{a}_M(\mathcal{W}') \subset \mathfrak{a}_M(\mathcal{W})$ et $\mathfrak{b}_M(\mathcal{W}) \subset \mathfrak{b}_M(\mathcal{W}') = \mathcal{W}'$. Donc, $m(U)\mathfrak{b}_M(\mathcal{W}) \subset m(U)\mathcal{W}' \subset \mathcal{W}$. □

Donnons la conséquence suivante du lemme 4.4.3. La représentation $V \oplus V^*(1)$ de G_F vue comme représentation p-adique (i.e comme $\mathbb{Q}_p$-espace vectoriel muni d'une action de G_F) s'écrit sous la forme $\overset{s}{\underset{i=1}{\oplus}} W_i^{s_i}$ où les W_i sont irréductibles sur G_F et non isomorphes. Soit $U_i = W_i \cap (T \oplus T^*(1))$ et $U = \oplus U_i$. Si r et s sont des entiers, on écrit $V^r \oplus V^*(1)^s = \oplus W_i^{r_i(r,s)}$ et $\underline{r}_{r,s} = (r_i(r,s))$. En appliquant ce qui précède à $W = \oplus W_i$, on peut montrer la proposition :

4.4.4. Proposition. — *Il existe une constante $\tilde{m}_F$ avec la propriété suivante : Soit $\mathcal{W}$ un $\mathbb{Z}_p[G_F]$-réseau contenu dans $T^r \oplus T^*(1)^s$ et contenant $M(T^r \oplus T^*(1)^s)$ et soit $\underline{w} \in T^r$ et $\underline{w}' \in T^*(1)^s$ tels que pour tous $\underline{a} \in \mathfrak{O}_F^{\underline{r}_{r,s}}$ vérifiant $\underline{a}.\mathcal{W} \subset MU$, on ait $\underline{a}.(\underline{w}, \underline{w}') \in MU$. Alors, $\tilde{m}_F(\underline{w}, \underline{w}') \in \mathcal{W}$.*

Remarque. — Si T/pT est absolument irréductible, $\mathfrak{O}$ est un ordre maximal et on a $m(T) = 1$. En effet, la $\mathbb{Z}/p\mathbb{Z}$-algèbre engendrée par l'image de G_F dans $GL(T/pT)$ est alors égale à $\mathrm{End}(T/pT)$. On en déduit par le lemme de Nakayama que $\mathfrak{O} = \mathrm{End}(T)$ et que $\mathfrak{O}$ est un ordre maximal de $A = \mathcal{E} \otimes_{\mathcal{O}} \mathfrak{O}$. Si de plus T/pT et $T^*(1)/pT^*(1)$ sont disjointes dès que V et $V^*(1)$ le sont, on a $\tilde{m}_F = 1$.

4.4.5. Lemme. — *Si F est une extension finie galoisienne de $\mathbb{Q}$, les $\tilde{m}_{F_n}$ sont bornés lorsque F_n varie dans la $\mathbb{Z}_p$-extension cyclotomique de F.*

Démonstration. — La représentation V reste semi-simple comme représentation de G_{F_∞} et on applique la proposition 4.4.4 à F_∞. On a alors $\tilde{m}_{F_n} \leqslant \tilde{m}_{F_\infty}$. □

4.5. Indépendance linéaire et groupes de Galois.

4.5.1. Rappelons que $F'(M) = F(T/MT, \mu_M)$. On suppose que V et $V^*(1)$ ne sont pas isomorphes à la représentation triviale sur F.

Soient

$$\delta_M = \delta_{M,F} : H^1(F, T/MT) \to \mathrm{Hom}_{\mathbb{Z}}(G_{F'(M)}(p), T/MT)^{\mathrm{Gal}(F'(M)/F)}$$
$$\delta_M^* = \delta_{M,F}^* : H^1(F, T^*(1)/MT^*(1)) \to \mathrm{Hom}_{\mathbb{Z}}(G_{F'(M)}(p), T^*(1)/MT^*(1))^{\mathrm{Gal}(F'(M)/F)}$$

les applications de restriction ($G(p)$ désignant la p-partie du groupe profini G). Les noyaux de $\delta_{M,F}$ et de $\delta_{M,F}^*$ sont égaux respectivement à $H^1(F'(M)/F, T/MT)$ et à $H^1(F'(M)/F, T^*(1)/MT^*(1))$; ces groupes d'après 4.2.5 sont finis d'ordre borné par s_F.

Si $X \subset H^1(F, T/MT)$ et $Y \subset H^1(F, T^*(1)/MT^*(1))$ sont des sous-$\mathcal{O}$-modules, on déduit de δ_M et de δ_M^* un homomorphisme invariant par G_F

$$\delta_M(X,Y) : G_{F'(M)} \to \mathrm{Hom}_{\mathcal{O}}(X, T/MT) \times \mathrm{Hom}_{\mathcal{O}}(Y, T^*(1)/MT^*(1)),$$
$$g \mapsto ((x,y) \mapsto (\delta_M(x)(g), \delta_M^*(y)(g))).$$

Si $x \in H^1(F, T/MT)$ ou $H^1(F, T^*(1)/MT^*(1))$, on note $\mathfrak{a}_M(x)$ son annulateur dans $\mathcal{O}$ et $\mathfrak{b}_M(x)$ l'ensemble des $b \in \mathcal{O}$ tel que $b\mathfrak{a}_M(x) \subset M\mathcal{O}$. Plus généralement, si X est un sous-$\mathcal{O}$-module de $H^1(F, T/MT)$ et $\underline{X} = (\hat{X} \to X)$ un couple formé d'un $\mathcal{O}$-module libre de type fini $\hat{X}$ et d'une surjection $\hat{X} \to X$, on note $\mathfrak{a}_M(\underline{X})$ le noyau de $\hat{X} \to X$ et $\mathfrak{b}_M(\underline{X})$ l'ensemble des éléments ψ de $\hat{X}^* = \mathrm{Hom}_{\mathcal{O}}(\hat{X}, \mathcal{O})$ tels que $\psi(\mathfrak{a}_M(\underline{X})) \subset M\mathcal{O}$. Avec des notations similaires pour Y, notons $\mathcal{W}'$ l'image réciproque de $\mathrm{Hom}_{\mathcal{O}}(X, T/MT) \times \mathrm{Hom}_{\mathcal{O}}(Y, T^*(1)/MT^*(1))$ dans $\mathrm{Hom}_{\mathcal{O}}(\hat{X} \times \hat{Y}, T \times T^*(1))$. Soit $\mathcal{W}_{\mathrm{gal}}(\underline{X} \times \underline{Y})$ le sous-$\mathbb{Z}_p$-module libre de $\mathrm{Hom}_{\mathcal{O}}(\hat{X} \times \hat{Y}, T \times T^*(1))$, image réciproque dans $\mathrm{Hom}_{\mathcal{O}}(\hat{X} \times \hat{Y}, T \times T^*(1))$ de l'image de l'application

$$G_{F'(M)} \to \mathrm{Hom}_{\mathcal{O}}(X, T/MT) \times \mathrm{Hom}_{\mathcal{O}}(Y, T^*(1)/MT^*(1))$$
$$\to \mathrm{Hom}_{\mathcal{O}}(\hat{X} \times \hat{Y}, T/MT \times T^*(1)/MT^*(1)).$$

On a donc $\mathcal{W}_{\mathrm{gal}}(\underline{X} \times \underline{Y}) \subset \mathcal{W}'$. On note alors $\mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X} \times \underline{Y}))$ (resp. $\mathfrak{a}_M(\mathcal{W}')$) l'ensemble des $(x, y) \in \hat{X} \times \hat{Y}$ tel que $\psi(x, y) \in MT \times MT^*(1)$ pour tout $\psi \in \mathcal{W}_{\mathrm{gal}}(\underline{X} \times \underline{Y})$ (resp. pour tout $\psi \in \mathcal{W}'$). Si on choisit un isomorphisme de $\mathcal{O}$-modules de $\hat{X}$ avec $\mathcal{O}^r$, $\mathcal{W}_{\mathrm{gal}}(\underline{X})$ s'identifie à un $\mathbb{Z}_p$-réseau $\mathcal{W}$ de V^r stable par G_F et on retrouve par ces identifications les définitions de 4.4.2.

4.5.2. Lemme. — *On a les inclusions*

$$s_F \mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X} \times \underline{Y})) \subset \mathfrak{a}_M(\mathcal{W}') \subset \mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X} \times \underline{Y})).$$

Démonstration. — Faisons pour simplifier $Y = 0$. Choisissons une base e_i du $\mathcal{O}$-module libre $\hat{X}$ et faisons les identifications qui en résultent : ainsi, on identifie $\mathrm{Hom}_{\mathcal{O}}(\hat{X}, T)$ avec T^r. On déduit la deuxième inclusion de ce que $\mathcal{W}_{\mathrm{gal}}(X) \subset \mathcal{W}'$. Montrons la première. Il est clair que $\mathfrak{a}_M(\mathcal{W}') = \mathfrak{a}_M(\underline{X})$. Si $(a_1, \ldots, a_r) \in \mathfrak{a}_M(\underline{X})$, on a $\sum_i a_i x_i = 0$ pour tout $(x_1, \cdots, x_r) \in X$, d'où pour tout $g \in G_{F'(M)}$

$$\sum_i a_i \delta_M(x_i)(g) = 0$$

et donc $\sum_i a_i w_i \in MT$ pour tout $(w_1, \ldots, w_r) \in \mathcal{W}_{\mathrm{gal}}(\underline{X})$. Donc $\mathfrak{a}_M(\underline{X}) \subset \mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X}))$. Réciproquement si $(a_1, \ldots, a_r) \in \mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X}))$, on a $\sum_i a_i w_i = 0$ pour tout $(w_1, \ldots, w_r) \in \mathcal{W}_{\mathrm{gal}}(\underline{X})$, d'où $\delta_M(\sum_i a_i x_i) = 0$ pour tout $(x_1, \cdots, x_r) \in X$. Comme le noyau de δ_M est annulé par s_F, on en déduit que $s_F \sum_i a_i x_i = 0$. Donc, $s_F \mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X})) \subset \mathfrak{a}_M(\underline{X})$. □

4.5.3. *Remarque.* — Soit $\psi \in \mathfrak{b}_M(\underline{X})$. L'image de ψ dans $\mathrm{Hom}_{\mathcal{O}}(\hat{X}, \mathcal{O}/M\mathcal{O})$ se factorise par X (on la note ψ_M) et définit un élément de $\mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O}/M\mathcal{O})$. Réciproquement, si $\psi_M \in \mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O}/M\mathcal{O})$, l'image réciproque de ψ dans $\mathrm{Hom}_{\mathcal{O}}(\hat{X}, \mathcal{O})$ est contenue dans $\mathfrak{b}_M(\underline{X})$.

4.5.4. Proposition. — *Soient X un sous-$\mathcal{O}$-module de $H^1(F, T/MT)$ et Y un sous-$\mathcal{O}$-module de $H^1(F, T^*(1)/MT^*(1))$. Si (ψ, ψ^*) appartient à*

$$\mathrm{Hom}_{\mathcal{O}}(X, T/MT) \times \mathrm{Hom}_{\mathcal{O}}(Y, T^*(1)/MT^*(1)),$$

$s_F \tilde{m}_F(\psi, \psi^*)$ appartient à l'image de $G_{F'(M)}$.

Démonstration[1]. — On a $s_F\mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X}\times\underline{Y})) \subset \mathfrak{a}_M(\mathcal{W}') \subset \mathfrak{a}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X}\times\underline{Y}))$. On en déduit par le lemme 4.4.3 (appliqué aux représentations vues comme représentations p-adiques, voir aussi la proposition 4.4.4) que

$$s_F\mathcal{W}' \subset s_F\mathfrak{b}_M(\mathcal{W}') \subset \mathfrak{b}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X}\times\underline{Y}))$$

et

$$\tilde{m}_F s_F\mathcal{W}' \subset \tilde{m}_F\mathfrak{b}_M(\mathcal{W}_{\mathrm{gal}}(\underline{X}\times\underline{Y})) \subset \mathcal{W}_{\mathrm{gal}}(\underline{X}\times\underline{Y}),$$

ce qui permet de conclure. □

4.5.5. Lemme. — *Soit X un sous-$\mathcal{O}$-module de $H^1(F,T/MT)$. Si $Z^1(G_F,\, T/MT)$ est le module des cocycles de G_F à valeurs dans T/MT, il existe un homomorphisme $X \to Z^1(G_F,T/MT)$ tel que le composé $X \to Z^1(G_F,T/MT) \to H^1(F,T/MT)$ soit la multiplication par s_F.*

Démonstration. — Commençons par démontrer l'assertion lorsque X est de rang 1. Il s'agit alors de démontrer les faits suivants : Soit $x \in H^1(F,T/MT)$; l'image de $\delta_M(x)$ est contenue dans $\mathfrak{b}_M(x)T/MT$ et s_Fx appartient à l'image de $H^1(F,\mathfrak{b}_M(x)T/MT)$ dans $H^1(F,T/MT)$, i.e. on peut choisir un cocycle x' représentant x tel que s_Fx' soit à valeurs dans $\mathfrak{b}_M(x)T$ modulo MT.

La première assertion est claire : si $\alpha x = 0$, on a $\alpha\delta_M(x)(g) = 0$ pour tout $g \in G_{F'(M)}$, ce qui signifie que si t est un relèvement dans T d'un élément de l'image de $\delta_M(x)$, on a $\mathfrak{a}_M(x)t \subset MT$ et $t \in \mathfrak{b}_M(x)T$. Pour la deuxième assertion, on remarque que l'image de x dans

$$H^1(F(M),T/b(x)T) = \mathrm{Hom}_{\mathcal{O}}(G_{F(M)}(p),T/b(x)T)$$

est nulle. Donc l'image de x dans $H^1(F,T/b(x)T)$ provient de $H^1(F(M)/F,\, T/b(x)T)$. Ainsi, s_Fx appartient à l'image de $H^1(F,b(x)T/MT)$, d'où le lemme pour X monogène. Dans le cas général, on choisit un isomorphisme $X \cong \oplus\mathcal{O}/\pi^{n_i}$ (π uniformisante de $\mathcal{O}$) et des éléments $x_1,\ldots,x_r$ tels que l'image de x_i soit $(0,\ldots,0,1,0,\ldots,0)$ et on applique ce qui précède à chacun des x_i. Comme il n'y a pas d'autres relations entre les x_i que $\pi^{n_i}x_i = 0$, on peut conclure.

□

[1] Je remercie ici le rapporteur de m'avoir signalé une erreur : j'avais regardé initialement le $\mathcal{O}$-module engendré par l'image de Galois, ce qui permet uniquement de montrer que $s_F\tilde{m}_F(\psi,\psi^*)$ appartient à l'image de $\mathcal{O}/M\mathcal{O} \otimes G_{F'(M)}$.

4.6. Applications du théorème de Chebotarev.

4.6.1. On se donne un élément $g \in GL(T)$ tel que

(1) $\det(g) = 1$;

(2) est valeur propre de g et $V^{g=1}$ est de dimension 1 ;

(3) les valeurs propres autres que 1 de g ne sont pas des racines de l'unité.

On suppose de plus que g appartient à l'image de $G_{\mathbb{Q}(\mu_{mp^\infty})}$. On se donne d'autre part une puissance α de p. Nous la choisirons plus tard égale à $\alpha = \tilde{m}_F s_F$. La condition (3) implique que l'endomorphisme $1+\ldots+g^{\alpha-1}$ de V est bijectif; on note α' une puissance de l'uniformisante π de $\mathcal{O}$ telle que $\alpha' T \subset (1+\ldots g^{\alpha-1})T$. Enfin, quitte à prendre une puissance convenable de g de manière à ce que les valeurs propres différentes de 1 de g soient congrues à 1 modulo p, g^α vérifie la condition (**) : il existe une puissance m_0 de p telle que $(g^{m_0}-1)T \subset p(g^\alpha - 1)T$. Nous supposons désormais que g^α vérifie la condition (**).

Soit enfin un polynôme $\tilde{R}(X)$ tel que $R(X) = (X-1)\tilde{R}(X)$ annule g^α et tel que $\tilde{R}(g^\alpha)$ ne soit pas nul. Par exemple, le polynôme $X\det(X - g^\alpha)$ convient pour $R(X)$ (car g^α n'est pas l'identité lorsque $\dim_{\mathcal{E}} V > 1$). On note alors t_0 un élément de T engendrant $V/(g^\alpha - 1)V$ et non divisible par π dans T et soit α_3 une puissance de π telle que $\alpha_3 t \in \tilde{R}(g)T$. On pose $\alpha_1 = \alpha\alpha' = \tilde{m}_F s_F^2 \alpha'$, $\alpha_2 = s_F \alpha'$.

On note dans la suite $F = \mathbb{Q}(\mu_m)$. On note $S_{g^\alpha, M}(Nm)$ l'ensemble des nombres premiers l congrus à 1 modulo Nm et tels que pour une place $\lambda_0 | l$, la restriction de $\mathrm{Frob}_{\lambda_0}^{-1}$ à $F'(M)$ coïncide avec la réduction de g^α modulo M.

4.6.2. Proposition. — *Soit S un ensemble fini de places contenant $\Sigma(V)$, p et l'infini. Soient $x \in H^1(G_{S,F}, T/MT)$, $y \in H^1(G_{S,F}, T^*(1)/MT^*(1))$. Soient $a \in T/MT$ appartenant à l'image de $\tilde{R}(g^\alpha)\mathfrak{b}_M(x)T$ et $a^* \in \mathfrak{b}_M(y)T^*(1)/MT^*(1)$. Il existe un nombre premier $l \in S_{g^\alpha, M}(Mm) - S$ et une place λ de F divisant l tels que*

$$\alpha_2^2[\tilde{R}(\varphi_\lambda^{-1})(\mathrm{ev}_\lambda(x)), \mathrm{ev}_\lambda(y)]_\zeta^{(M)} = \alpha_1^2[a, a^*]_\zeta^{(M)}.$$

Remarquons que $\mathrm{ev}_\lambda(x) = x(\mathrm{Frob}_\lambda)$ est déterminé modulo $(M, g^\alpha - 1)T$ et que $\tilde{R}(\varphi_\lambda^{-1})(\mathrm{ev}_\lambda(x))$ est déterminé modulo $(M, g^\alpha - 1)\tilde{R}(g^\alpha)T \subset MT$. D'autre part comme $y(\mathrm{Frob}_\lambda)$ est déterminé modulo $(M, (g^\alpha -$

$1))T^*(1)$ et que

$$[\tilde{R}(g^\alpha)b, (g^\alpha - 1)b^*]_\zeta^{(M)} = [(g^\alpha - 1)\tilde{R}(g^\alpha)b, b^*]_\zeta^{(M)} = 0,$$

le premier membre de l'égalité a bien un sens.

4.6.3. Pour le corollaire suivant, on prend $R(X) = Q(g^\alpha, X) = X\det(g^\alpha - X)$; on remarque que pour $l \in S_{g^\alpha,M}(Mm)$, $P_l(V^*(1), X) \equiv \det(g^\alpha - X) \bmod M$.

4.6.4. COROLLAIRE. — *Pour $x \in H^1(G_{S,F}, T/MT)$ et $y \in H^1(G_{S,F}, T^*(1)/MT^*(1))$, l'ensemble des*

$$\alpha_2^2[\varphi_\lambda^{-1}\tilde{P}_l(V^*(1), \varphi_\lambda^{-1})(\mathrm{ev}_\lambda(x)), \mathrm{ev}_\lambda(y)]_\zeta^{(M)}$$

pour l nombre premier dans $S_{g^\alpha,M}(Mm)$ contient $\alpha_1^2\alpha_3\mathfrak{b}_M(x)\mathfrak{b}_M(y)$ modulo M.

Démonstration. — On prend $a = \alpha_3 t_0$ et on choisit $a^{*\prime}$ de manière à ce que $[t_0, a^{*\prime}]_\zeta^{(M)} = 1$ et $a^* \in \mathfrak{b}_M(y)a^{*\prime}$. □

Démonstration de la proposition 4.6.2. — On commence par choisir un élément $\gamma \in G_{F(\mu_M)}$ dont l'image dans $GL(T)$ est g. Écrivons $a = \tilde{R}(g^\alpha)(a')$ avec $a' \in \mathfrak{b}_M(x)T$ et $\alpha = \tilde{m}_F s_F$ (voir la proposition 4.5.4). Soit x' (resp. y') un cocycle représentant $s_F x$ (resp. $s_F y$) et à valeurs dans $\mathfrak{b}_M(x)T/MT$ (resp. dans $\mathfrak{b}_M(y)T^*(1)/MT^*(1)$). Comme $a' - x'(\gamma) \in \mathfrak{b}_M(x)T/MT$ et que $a^* - y'(\gamma) \in \mathfrak{b}_M(x)T^*(1)/MT^*(1)$, on peut appliquer la proposition 4.5.4; il existe $h \in G_{F'(M)}$ tel que

$$\begin{aligned} x'(h) &= \alpha(a' - x'(\gamma)) \\ y'(h) &= \alpha(a^* - y'(\gamma)). \end{aligned}$$

Comme h agit trivialement sur T/MT, on a

$$\begin{aligned} x'(h\gamma^\alpha) &\equiv \alpha x'(\gamma) + x'(h) \equiv \alpha a' \bmod (M, (g-1)T) \\ y'(h\gamma^\alpha) &\equiv \alpha y'(\gamma) + y'(h) \equiv \alpha a^* \bmod (M, (g-1)T^*(1)). \end{aligned}$$

Posons $\gamma' = h\gamma^\alpha$. Par le théorème de Chebotarev, il existe un nombre premier l et une place λ au-dessus de l tel que Frob_λ coïncide avec γ'^{-1} sur le corps de définition de x et y sur $F(M)$. L'action de γ' sur T/MT coïncide avec celle de g^α. On a alors

$$\begin{aligned} s_F\tilde{R}(\varphi_\lambda^{-1})\mathrm{ev}_\lambda(x) &\equiv -\alpha a \bmod (M, \tilde{R}(g^\alpha)(g-1))T) \\ s_F\mathrm{ev}_\lambda(y) &\equiv -\alpha a^* \bmod (M, g-1)T^*(1). \end{aligned}$$

Comme $\alpha'(g-1)T \subset (M, g^\alpha - 1)T$ et $\alpha'(g-1)T^*(1) \subset (M, g^\alpha - 1)T^*(1)$, on en déduit que

$$\alpha' s_F \tilde{R}(\varphi_\lambda^{-1})\mathrm{ev}_\lambda(x) \equiv -\alpha'\alpha a \bmod M\tilde{R}(\varphi_\lambda^{-1})T$$
$$\alpha' s_F \mathrm{ev}_\lambda(y) \equiv -\alpha'\alpha a^* \bmod (M, \varphi_\lambda - 1)T^*(1)$$

et

$$\alpha'^2 s_F^2 [\tilde{R}(\varphi_\lambda^{-1})\mathrm{ev}_\lambda(x), \mathrm{ev}_\lambda(y)]_\zeta^{(M)} = \alpha'^2\alpha^2 [a, a^*]_\zeta^{(M)},$$

d'où la proposition. □

4.6.5. Proposition. — *Soit S un ensemble fini de places contenant $\Sigma(V)$, p et l'infini. Soient*

$$\psi \in \mathrm{Hom}_{\mathcal{O}}(H^1(G_{S,F}, T/MT), \mathcal{O}/M\mathcal{O})$$
$$\psi^* \in \mathrm{Hom}_{\mathcal{O}}(H^1(G_{S,F}, T^*(1)/MT^*(1)), \mathcal{O}/M\mathcal{O}).$$

Il existe un nombre premier $l \in S_{g^\alpha, M}(Mm) - S$ et une place λ de F divisant l tels que

$$\alpha_2^2 [\varphi_\lambda^{-1}\tilde{P}_l(V^*(1), \varphi_\lambda^{-1})(\mathrm{ev}_\lambda(x)), \mathrm{ev}_\lambda(y)]_\zeta^{(M)} = \alpha_1^2\alpha_3\psi(x)\psi^*(y)$$

pour tous $x \in H^1(G_{S,F}, T/MT)$, $y \in H^1(G_{S,F}, T^*(1)/MT^*(1))$.

La démonstration est identique à la précédente.

4.7. Version algèbre de groupes.

4.7.1. Soit Δ le groupe de Galois de l'extension abélienne $F/\mathbb{Q}$. On note π_1 l'application $\mathcal{O}$-linéaire de $\mathcal{O}[\Delta]$ dans $\mathcal{O}$ qui envoie l'unité de Δ sur 1 et $g \neq 1$ sur 0. Soit $\mathcal{M}$ un $\mathcal{O}[\Delta]$-module. A $\psi \in \mathrm{Hom}_{\mathcal{O}}(\mathcal{M}, \mathcal{O}/M\mathcal{O})$, on associe naturellement un homomorphisme $\tilde{\psi}$ de $\mathcal{O}[\Delta]$-modules par la formule

$$\tilde{\psi}(x) = \sum_{\tau \in G} \psi(\tau^{-1}x)\tau$$

pour $x \in \mathcal{M}$. On a alors $\pi_1(\tilde{\psi}) = \psi$. Si A est un $\mathcal{O}$-module avec action triviale de Δ, on obtient ainsi un isomorphisme naturel de $\mathcal{O}[\Delta]$-modules

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{M}, A)^\iota \cong \mathrm{Hom}_{\mathcal{O}[\Delta]}(\mathcal{M}, A[\Delta]),$$

l'action de $\tau \in \Delta$ sur $\mathrm{Hom}_{\mathcal{O}[\Delta]}(M, A[\Delta])$ est donné par $f \mapsto \tau.f$ (on a $f(\tau x) = \tau.f(x)$), l'action de Δ sur $\mathrm{Hom}_{\mathcal{O}}(\mathcal{M}, A)^\iota$ est donnée par $f \mapsto (x \to f(\tau x))$ (on note M^ι le Δ-module dont le $\mathcal{O}$-module sous-jacent

est M et où l'action de Δ est changée par $\delta \mapsto \delta^{-1}$). Remarquons que le produit sur le premier correspond à la convolution sur le second. Si ξ est un caractère de Δ à valeurs dans $\bar{\mathbb{Q}}_p^\times$, on a la formule

$$\xi(\tilde{\psi}(x)) = \psi(e_\xi(x))$$

avec $e_\xi = \sum_{\tau\in\Delta} \xi(\tau)^{-1}\tau$ et ψ étendu par linéarité à l'anneau $\mathcal{O}(\xi)$ engendré sur $\mathcal{O}$ par les valeurs de ξ.

4.7.2. Si l est un nombre premier que l'on suppose désormais totalement décomposé dans F, on choisit une place λ_0 de F au-dessus de l; si λ est une autre place au-dessus de l, il existe un unique élément de Δ noté τ_λ tel que $\tau_\lambda\lambda_0 = \lambda$. On a un isomorphisme naturel de $\mathcal{O}[\Delta]\otimes H^1(F_{\lambda_0}, T/MT)$ sur $\prod_{\lambda|l} H^1(F_\lambda, T/MT)$ donné par $\sum_{\tau\in\Delta} \tau\otimes x_\tau \mapsto (\tau_\lambda x_{\tau_\lambda})_\lambda$.

On pose pour $x = (x_\lambda) \in \prod_{\lambda|l} H^1(F_\lambda, T/MT)$

$$\mathrm{ev}_{l,\Delta}(x) = \sum_{\lambda|l} \mathrm{ev}_\lambda(x_\lambda)\tau_\lambda = \sum_{\lambda|l} \mathrm{ev}_{\lambda_0}(\tau_\lambda^{-1}x_\lambda)\tau_\lambda = \sum_{\tau\in\Delta} \mathrm{ev}_{\lambda_0}(\tau^{-1}x_{\tau(\lambda_0)})\tau,$$

et de même pour $\mathrm{Ev}_{l,\Delta}$. On prolonge l'accouplement $[\ ,\ ]_\zeta^{(M)}$ en un accouplement $\mathcal{O}[\Delta]$-linéaire en la première variable et anti-linéaire en la seconde variable pour l'involution de $\mathcal{O}[\Delta]$ induite par $\delta \mapsto \delta^{-1}$ pour $\delta \in \Delta$.

4.7.3. Si $\tilde{x} \in \mathcal{O}[\Delta] \otimes H^1(F_{\lambda_0}, T/MT)$ et $\tilde{y} \in \mathcal{O}[\Delta] \otimes H^1(F_{\lambda_0}, T^*(1)/MT^*(1))$, on définit un accouplement de $\mathcal{O}[\Delta]$-modules $<\ ,\ >_{l,\Delta}^{(M)}$ par

$$<\tilde{x},\tilde{y}>_{l,\Delta}^{(M)} = \sum_{\delta\in\Delta}\sum_{\tau\in\Delta} <\tilde{x}_\tau, \tilde{y}_{\delta^{-1}\tau}>_{\lambda_0}^{(M)} \delta$$

avec $\tilde{x} = \sum_{\tau\in\Delta} \tau\otimes\tilde{x}_\tau$ et $\tilde{y} = \sum_{\tau\in\Delta} \tau\otimes\tilde{y}_\tau$. On en déduit par projection sur $\mathcal{O}$ par π_1 un accouplement de $\mathcal{O}$-modules $<\ ,\ >_l^{(M)} = \pi_1 <\ ,\ >_{l,\Delta}^{(M)}$:

$$<\tilde{x},\tilde{y}>_l^{(M)} = \sum_{\tau\in\Delta} <\tilde{x}_\tau, \tilde{y}_\tau>_{\lambda_0}^{(M)}$$

ou

$$<(x_\lambda),(y_\lambda)>_l^{(M)} = \sum_{\lambda|l} <x_\lambda, y_\lambda>_\lambda^{(M)}.$$

Si $x \in H^1(F, T/MT)$ et $y \in H^1(F, T^*(1)/MT^*(1))$ et si $\tilde{x} = \sum_{\tau \in \Delta} \tau \otimes \tau^{-1} x_{\tau(\lambda_0)}$, $\tilde{y} = \sum_{\tau \in \Delta} \tau \otimes \tau^{-1} y_{\tau(\lambda_0)}$, on a alors

$$< \tilde{x}, \tilde{y} >_l^{(M)} = \sum_{\lambda | l} < x_\lambda, y_\lambda >_\lambda^{(M)} = \sum_{\lambda | l} < x, y >_\lambda^{(M)} .$$

4.7.4. Soit $l \in S_{*,M}(Mm)$. On déduit des considérations de 3.4.2 une application

$$\text{Dér}_{l,\Delta} : \mathcal{O}[\Delta] \otimes H^1_{\text{br}}(F_{\lambda_0}, T/MT) \to \mathcal{O}[\Delta] \otimes H^1_{/br}(F_{\lambda_0}, T/MT)$$

donnée par $x \mapsto \sum_{\tau \in \Delta} \text{Dér}_{\lambda_0}(x_{\tau^{-1}})\tau$, ou ce qui revient au même

$$\text{Dér}_{l,\Delta} : \prod_{\lambda | l} H^1_{\text{br}}(F_\lambda, T/MT) \to \prod_{\lambda | l} H^1_{/br}(F_\lambda, T/MT),$$

dont le noyau et conoyau sont finis d'exposant borné par rapport à M.

4.7.5. Proposition. — *Soit X (resp. Y) un sous-$\mathcal{O}[\Delta]$-module de $H^1(G_{S,F}, T/MT)$ (resp. de $H^1(G_{S,F}, T^*(1)/MT^*(1))$). Soient*

$$\psi \in \text{Hom}_{\mathcal{O}}(X, \mathcal{O}/M\mathcal{O}), \quad \psi^* \in \text{Hom}_{\mathcal{O}}(Y, \mathcal{O}/M\mathcal{O}).$$

Soient $t_0 \in T$ appartenant à l'image de $\tilde{Q}(g^\alpha, g)V$ comme en 4.6.1. (avec $\alpha_3 t_0 \in \tilde{Q}(g^\alpha, g)T$) et t_0^* un élément de $T^*(1)$. Il existe un nombre premier $l \in S_{g^\alpha,M}(Mm) - S$ et une place λ_0 de F au-dessus de l tels que

$$\alpha_2 \text{Ev}_{l,\Delta} \text{Dér}_{l,\Delta}(x) \equiv -\alpha_1 \alpha_3 \tilde{\psi}(x) t_0 \bmod M \quad \text{pourtout } x \in X$$
$$\alpha_2 ev_{l,\Delta}(y) \equiv -\alpha_1 \tilde{\psi}^*(y) t_0^* \bmod M \quad \text{pourtout } y \in Y,$$

ce qui implique

$$\alpha_2^2 < \text{Dér}_{l,\Delta}(x), \tilde{y} >_{l,\Delta}^{(M)} = \alpha_3 \alpha_1^2 \tilde{\psi}(x) \tilde{\psi}^*(y)^\iota [t_0, t_0^*]_\zeta^{(M)}.$$

C'est une reformulation de la proposition 4.6.5 et des formules (4.6.1) (rappelons que $\tilde{y} = \sum_{\delta \in \Delta} \delta \otimes \delta^{-1} y$). En particulier, en appliquant π_1, on a

$$\alpha_2^2 \sum_{\lambda | l} < \text{Dér}_\lambda(x), y >_\lambda^{(M)} = \alpha_1^2 \alpha_3 \sum_{\delta \in \Delta} \psi(\delta^{-1} x) \psi^*(\delta y) [t_0, t_0^*]_\zeta^{(M)}.$$

On peut aussi appliquer e_ξ pour ξ caractère de Δ. On obtient alors

$$\alpha_2^2 < \text{Dér}_\lambda(e_\xi(x)), e_{\xi^{-1}} y >_l^{(M)} = \alpha_1^2 \alpha_3 \psi(e_\xi(x)) \psi^*(e_{\xi^{-1}}(y)) [t_0, t_0^*]_\zeta^{(M)}$$

pour tous x et y.

5. Démonstrations.

5.1. Quelques résultats de finitude.

5.1.1. On fait les hypothèses

(Tech) il existe un élément $g \in GL(T)$ appartenant à l'image de $G_{\mathbb{Q}(\mu_{p^\infty})}$ de déterminant 1, tel que $V/(g-1)V$ soit de dimension 1 et dont les valeurs propres autre que 1 ne sont pas des racines de l'unité.

(H) Pour presque tout l, $P_l(V,1) \neq 0$.

On se donne un système d'Euler p-adique c de rang 1 non ramifié en dehors de p et un entier m fortement admissible. Si ξ est un caractère de Δ_m, on note $c_\xi(m) = e_\xi c(m)$. On note $H^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))$ le noyau de l'application de localisation en p :

$$H^1_{\mathrm{br}}(F, T^*(1)/MT^*(1)) \to \prod_{v|p} H^1(F_v, T^*(1)/MT^*(1)).$$

5.1.2. Proposition. — *Soit ξ un caractère de Δ_m et tel que $\xi(\mathcal{B}(m)) \neq 0$ si p ne divise pas m. Supposons $c_\xi(m)$ d'ordre infini.*

Si $V \not\cong V^*(1)$ ou si $\xi^2 \neq 1$, $H^1_{\mathrm{br},0}(\mathbb{Q}(\mu_m), T^*(1)/MT^*(1))^{(\xi^{-1})}$ est d'ordre borné par rapport à M et $H^1_{\mathrm{br},0}(\mathbb{Q}(\mu_m), V^*(1)/T^*(1))^{(\xi^{-1})}$ est fini. Si $V \cong V^*(1)$ et si $\xi^2 = 1$, alors $H^1_{\mathrm{br},0}(\mathbb{Q}(\mu_m), T)^{(\xi)}$ est de rang

$$\begin{cases} 1 & \text{si } c_\xi(m) \in H^1_{\mathrm{br},0}(F,V)^{(\xi)} \\ 0 & \text{si } c_\xi(m) \notin H^1_{\mathrm{br},0}(\mathbb{Q}(\mu_m), V)^{(\xi)}. \end{cases}$$

Démonstration. — Supposons V et $V^*(1)$ non isomorphes. Soit

$$y \in H^1_{\mathrm{br},0}(\mathbb{Q}(\mu_m), T^*(1)/MT^*(1))^{(\xi^{-1})}.$$

Soit $b \in \mathfrak{b}_M(c_\xi(m))$ et $b^* \in \mathfrak{b}_M(y)$. D'après le corollaire 4.6.4, il existe un nombre premier $l \in S_{g^\alpha, M}(Mm)$ et une place λ de $F = \mathbb{Q}(m)$ au-dessus de l tel que

$$\alpha_2^2 < \mathrm{Dér}_\lambda(c_\xi(m)), y >_l^{(M)} = \alpha_1^2 \alpha_3 b b^*. \tag{5.1.1}$$

Si β est un élément de $\mathcal{B}(m)$ si p ne divise pas m et 1 sinon, on a

$$\xi(\beta) < d^{(a)}_{M,\xi}(m; l), y >_{l,M} = \xi(\beta) a < e_\xi \mathrm{Dér}_\lambda(c(m)), y >_{l,}^{(M)} \tag{5.1.2}$$

avec $e_\xi d_M^{(a)}(m;l) = d_{M,\xi}^{(a)}(m;l)$. La loi de réciprocité implique

$$\sum_v < d_M^{(a)}(m;l)_v, y_v >_v^{(M)} = 0. \tag{5.1.3}$$

Comme $d_M^{(a)}(m;l)_v \in H^1_{\mathrm{br}}(F_v, T/MT)$ pour toute place v de F ne divisant pas p et l, que l'image de y est dans $H^1_{\mathrm{br}}(F_v, T^*(1)/MT^*(1))$ pour v ne divisant pas p et nulle pour v divisant p, les termes du premier membre de (5.1.3) sont nuls pour v ne divisant pas l. Comme $\delta(y) = \xi^{-1}(\delta)y$, on déduit de (5.1.3) que

$$< d_{M,\xi}^{(a)}(m;l), y >_l^{(M)} = 0.$$

En mettant ensemble avec (5.1.1) et (5.1.2), on en déduit qu'il existe une constante C non nulle indépendante de $c_\xi(m)$ et de y telle que $Cbb^* \in M\mathcal{O}(\xi)$. Donc, $\mathfrak{a}_M(y) \supset C\mathfrak{b}_M(c_\xi(m))$. On en déduit la proposition. Le cas où V et $V^*(1)$ sont isomorphes se traite de la même manière. □

Donnons quelques précisions supplémentaires. On suppose $c_\xi(m)$ d'ordre infini et soit $m_\xi(1)$ la puissance de π engendrant $\mathfrak{b}_M(c_\xi(m))$ pour M assez grand. C'est aussi la plus grande puissance de π telle que $c_\xi(m) \in m_\xi(1)H^1(\mathbb{Q}(\mu_m), T)^{(\xi)}$. Distinguons les deux cas suivants :

(I) : $V \not\cong V^*(1)$ ou $\xi^2 \neq 1$, **(II)** : $V \cong V^*(1)$ et $\xi^2 = 1$.

Cas (I)

(1) $H^1_{\mathrm{br},\{p\}}(\mathbb{Q}(\mu_m), V^*(1))^{(\xi^{-1})}$ s'injecte dans $H^1(\mathbb{Q}(\mu_m)_p, V^*(1))^{(\xi^{-1})}$;

(2) le noyau de $H^1_{\mathrm{br},\{p\}}(\mathbb{Q}(\mu_m), V^*(1)/T^*(1))^{(\xi^{-1})} \to H^1(\mathbb{Q}_p, V^*(1))/T^*(1)^{(\xi^{-1})}$ est annulé par $Cm_\xi(1)$ où C est une constante qui se calcule explicitement et ne dépend pas du système d'Euler c.

(3) Si $c_\xi(m)$ a bonne réduction en p (le localisé en p est dans $H^1_f(\mathbb{Q}(\mu_m)_p, V)^{(\xi)}$), $H^1_f(\mathbb{Q}(\mu_m), V^*(1))^{(\xi^{-1})}$ est nul et $H^1_f(\mathbb{Q}(\mu_m), V^*(1))/T^*(1)^{(\xi^{-1})}$ est fini. La même démonstration s'applique en remarquant que dans la formule 5.1.3, le terme en p s'annule encore sous ces hypothèses.

Cas (II)

(1) Si le localisé $c_\xi(m)_p$ en p est d'ordre infini, $H^1_{\mathrm{br},\{p\}}(\mathbb{Q}(\mu_m), V^*(1))^{(\xi)}$ s'injecte dans $H^1(\mathbb{Q}(\mu_m)_p, V^*(1))^{(\xi)}$;

(2) Si $c_\xi(m)$ a bonne réduction en p, $H^1_f(\mathbb{Q}(\mu_m), V^*(1))^{(\xi)}$ est de rang 1.

Dans tous les cas, la dimension de $H^1_f(\mathbb{Q}(\mu_m), V^*(1))^{(\xi^{-1})}$ est inférieure ou égale à 1. Supposons l'espace tangent de $V^*(1)$ nul (dans ce cas $V^*(1)$ et V ne peuvent pas être isomorphes) et $P_p(V^*(1), \xi(p)) \neq 0$ (ce qui implique que $H^1_f(\mathbb{Q}(\mu_m)_v, V^*(1))^{(\xi)}$ est nul pour tout $v|p$). Alors $H^1_f(\mathbb{Q}(\mu_m), V^*(1))^{(\xi^{-1})} = 0$. On en déduit que $H^1_f(\mathbb{Q}(\mu_m), V)^{(\xi)}$ est de dimension $d_{-\epsilon(\xi)}$ car on a ([PR95])

$$\dim_{\mathcal{E}(\xi)} H^1_f(\mathbb{Q}(\mu_m), V)^{(\xi)} - \dim_{\mathcal{E}(\xi)} H^1_f(\mathbb{Q}(\mu_m), V^*(1))^{(\xi^{-1})} = d_{-\epsilon(\xi)}.$$

5.1.3. Si Σ est un ensemble de nombres premiers contenant p, rappelons qu'on note $H^1_{\mathrm{br},\Sigma}(F, T^*(1)/MT^*(1))$ le sous-$\mathcal{O}$-module de $H^1(F, T^*(1))/MT^*(1)$ formé des éléments non ramifiés pour $l \notin \Sigma$. Pour l nombre premier, on note $H^1_*(F_l, A) = \prod_{v|l} H^1_*(F_v, A)$. On suppose dans le reste du paragraphe 5.1. que ξ est un caractère d'ordre premier à p.

LEMME. — *Soit ξ un caractère de $\mathrm{Gal}(F/\mathbb{Q})$. Soient M une puissance de p, $l_1, \ldots, l_s$ des nombres premiers tels que $H^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))^{(\xi^{-1})}$ s'injecte dans $\prod_i H^1_{\mathrm{br}}(F_{l_i}, T^*(1)/MT^*(1))^{(\xi^{-1})}$. Posons $\Sigma_i = \{l_0, l_1, \ldots, l_i\}$ avec $l_0 = p$. Alors, le cardinal de $H^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))^{(\xi^{-1})}$ est borné par*

$$\prod_{i=1}^{r} \sharp\mathrm{coker}(H^1_{\mathrm{br},\Sigma_i}(F, T/MT)^{(\xi)} \to H^1_{/br}(F_{l_i}, T/MT)^{(\xi)}).$$

Démonstration. — Notons

$$X_0 = H^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))^{(\xi^{-1})}$$

$$X_i = \{x \in H^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))^{(\xi^{-1})} \text{ tel que } x_v = 0 \text{ pour } v|l \in \Sigma_i\}$$

(une notation plus compliquée serait $H^{1\ (0,\Sigma_i)}_{\mathrm{br}}(F, T^*(1)/MT^*(1))^{(\xi^{-1})}$). L'homomorphisme naturel $X_{i-1}/X_i \to H^1_{\mathrm{br}}(F_{l_i}, T^*(1)/MT^*(1))^{(\xi^{-1})}$ est injectif. Soit $y \in H^1_{\mathrm{br},\Sigma_i}(F, T/MT)^{(\xi)}$ et $x \in X_{i-1}$. On a $\sum_{v|l\in\Sigma_i} < x, y >_v^{(M)} = 0$ et donc

$$\sum_{l\in\Sigma_i} < x, y >_l^{(M)} = 0.$$

Comme $x \in X_{i-1}$, cette égalité se réduit à $< x, y >_{l_i}^{(M)} = 0$. On en déduit que x_{l_i} est orthogonal à l'image de $H^1_{\mathrm{br},\Sigma_i}(F, T/MT)^{(\xi)}$ dans

$H^1_{/br}(F_{l_i}, T/MT)^{(\xi)}$ (rappelons que x_{l_i} est de toute façon orthogonal à $H^1_{\mathrm{br}}(F_{l_i}, T/MT)^{(\xi)}$) et donc que

$$\sharp X_{i-1}/X_i \leqslant \sharp\mathrm{coker} \to (H^1_{\mathrm{br},\Sigma_i}(F, T/MT)^{(\xi)} \to H^1_{/br}(F_{l_i}, T/MT)^{(\xi)}).$$

On fait alors le produit sur i en remarquant que $X_0 = H^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))^{(\xi^{-1})}$ et que $X_r = 0$. □

5.1.4. Soit m un entier divisible par p tel que le degré de $F = \mathbb{Q}(\mu_m)$ sur $\mathbb{Q}$ soit premier à p. Nous supposons dans ce paragraphe que les constantes α_1, α_2, α_3 et $a_m(T)$ sont égales à 1. Plus précisément, on suppose les conditions suivantes :

(1) $s_{\mathbb{Q}(\mu_m)} = 1$: c'est-à-dire

$$\begin{cases} H^1(\mathbb{Q}(\mu_{mM})(M)/\mathbb{Q}(\mu_m), T/M'T)^{(\xi)} = 0 & \text{pour } M'|M \\ H^1(\mathbb{Q}(\mu_{mM})(M)/\mathbb{Q}(\mu_m), T^*(1)/MT^*(1))^{(\xi^{-1})} & = 0; \end{cases}$$

par exemple, cela est vrai si T/pT est absolument irréductible, si

$$H^1(\mathbb{Q}(\mu_m)(p)/\mathbb{Q}(\mu_m), T/pT) = 0,$$
$$H^1(\mathbb{Q}(\mu_m)(p)/\mathbb{Q}(\mu_m), T^*(1)/pT^*(1)) = 0$$

et si T/pT et $T/pT^*(1)$ sont disjointes avec la représentation adjointe $\mathcal{G}/p\mathcal{G}$;

(2) $\tilde{m}_{\mathbb{Q}(\mu_m)} = 1$, par exemple T/pT et $T^*(1)/pT^*(1)$ sont absolument irréductibles sur $\mathbb{Q}(\mu_m)$ et isomorphes si et seulement si V et $V^*(1)$ le sont ;

(3) ξ est d'ordre premier à p ;

(4) Si m est premier à p, $\xi(\mathcal{B}(m)) = \mathcal{O}(\xi)$;

(5) il existe un élément g de $GL(T)$ appartenant à l'image de $G_{\mathbb{Q}(\mu_{mp^\infty})}$ tel que 1 soit valeur propre simple de g agissant sur T/pT ;

(6) $(T/pT)^{G_{\mathbb{Q}^{\mathrm{ab}}}} = 0$.

5.1.5. Proposition. — *Supposons les conditions de 5.1.4 vérifiées. Soit m un entier fortement admissible et ξ un caractère de $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ tel que $c_\xi(m)$ soit d'ordre infini. On suppose V et $V^*(1)$ non isomorphes ou $\xi^2 \neq 1$. Alors,*

$$\sharp H^1_{\mathrm{br},0}(\mathbb{Q}(\mu_m), T^*(1)/MT^*(1))^{(\xi^{-1})} \leqslant m_\xi(1).$$

Démonstration. — On pose toujours $F = \mathbb{Q}(\mu_m)$. On fixe une puissance M_0 de π suffisamment grande : $M_0 > Mm_\xi(1)^R$ avec $R =$

$\sharp(H^1_{\mathrm{br},0}(F,T^*(1)/MT^*(1))^{(\xi^{-1})})$. On pose $M_i = M_0/m_\xi(1)^i$. Nous allons choisir successivement des nombres premiers $l_1,\dots,l_R$. On posera alors $L_0 = 1$, $\Sigma_0 = \{p\}$, $L_i = l_1\dots l_i$, $\Sigma_i = \{p,l_1,\dots,l_i\}$ pour $i \geqslant 1$ et $c_\xi(m) = m_\xi(L_0)Z_0$, $d_{M_i,\xi}(m,L_i) = m_\xi(L_i)Z_i$ où $Z_i \in H^1(F,T/M_iT)^{(\xi)}$ n'est pas divisible par p. Ainsi, on a $\mathfrak{b}_{M_i}(c_\xi(m)) = m_\xi(L_0)\mathcal{O}(\xi)$, $\mathfrak{b}_{M_i}(d_{M_i,\xi}(m,L_i)) = m_\xi(L_i)\mathcal{O}(\xi)$. On note aussi S_i l'ordre du conoyau de

$$H^1_{\mathrm{br},\Sigma_i}(F,T/MT)^{(\xi)} \to H^1_{/br}(F_{l_i},T/MT)^{(\xi)}.$$

On énumère les éléments de $H^1_{\mathrm{br}}(F_{l_i},V^*(1)/T^*(1))^{(\xi)} : y_1,\dots,y_R$. On choisit $l_1 \in S_{g,M_0}(M_0m)$ comme dans la proposition 4.6.2 pour $x = Z_0$, $y = y_1$. Plus précisément,

- $\mathrm{Dér}_{l_1,\xi}(Z_0) = U_{l_1}$ engendre $H^1_{/\mathrm{br}}(F_{l_1},T/M_0T)^{(\xi)}$;
- $\mathrm{ev}_{l_1}(Z_0)$ n'est pas divisible par π dans $H^1_{\mathrm{br}}(F_{l_1},T/M_0T)^{(\xi)}$;
- $\mathrm{ev}_{l_1}(y_1)$ n'est divisible par π dans $H^1_{\mathrm{br}}(F_{l_1},T^*(1)/M_0T^*(1))^{(\xi^{-1})}$.

Ainsi, on a $m_\xi(L_0)U_{l_1} = m_\xi(L_1)(Z_1)_{l_1}$. En écrivant

$$(Z_1)_{l_1} = m_{l_1}(L_1)U_{l_1}$$

dans $H^1_{/\mathrm{br}}(F_{l_1},T/M_0T)^{(\xi)}$, on en déduit que $m_\xi(L_0) \equiv m_\xi(L_1)m_{l_1}(L_1)$ mod M_0, c'est-à-dire que $m_\xi(L_1)$ divise $m_\xi(L_0)$ et que

$$\frac{m_\xi(L_0)}{m_\xi(L_1)}U_{l_1} = (Z_1)_{l_1}$$

dans $H^1_{/\mathrm{br}}(F_{l_1},T/M_1T)^{(\xi)}$ avec $M_1 = M_0/m_\xi(L_1)$ et donc dans $H^1_{/\mathrm{br}}(F_{l_1},)$ $T/MT^{(\xi)}$. L'image de $H^1_{\mathrm{br},\Sigma_0}(F,V/T)^{(\xi)}$ dans $H^1_{/\mathrm{br}}(F_{l_1},T/MT)^{(\xi)}$ contient

$$\frac{m_\xi(L_0)}{m_\xi(L_1)}H^1_{/\mathrm{br}}(F_{l_1},T/MT)^{(\xi)}$$

et S_1 divise $m_\xi(L_0)/m_\xi(L_1)$. La condition relative à y_1 implique que y_1 n'appartient pas au noyau de localisation en l_1.

On choisit $l_2 \in S_{g,M_1}(M_1ml_1)$ comme dans la proposition 4.6.2 avec $x = Z_1$, $y = y_2$. On a alors

- $\mathrm{Dér}_{l_1,\xi}(Z_1) = U_{l_2}$ engendre $H^1_{/\mathrm{br}}(F_{l_2},T/M_1T)^{(\xi)}$;
- $\mathrm{ev}_{l_2}(Z_1)$ n'est pas divisible par π dans $H^1_{\mathrm{br}}(F_{l_2},T/M_1T)^{(\xi)}$;

• $\mathrm{ev}_{l_2}(y)$ n'est divisible par π dans $H^1_{\mathrm{br}}(F_{l_2}, T^*(1)/M_1T^*(1))^{(\xi^{-1})}$.

On en déduit comme précédemment que y_2 n'appartient pas au noyau de localisation en l_2, que $m_\xi(L_2)$ divise $m_\xi(L_1)$ et que l'image de $H^1_{\mathrm{br},\Sigma_1}(F, T/M_2T)^{(\xi)}$ dans $H^1_{/\mathrm{br}}(F_{l_2}, T/M_2T)^{(\xi)}$ contient

$$m_\xi(L_1)/m_\xi(L_2)H^1_{/br}(F_{l_2}, T/M_2T)^{(\xi)}$$

avec $M_2 = M_1/m_\xi(L_0)$; ce qui implique que S_2 divise $m_\xi(L_1)/m_\xi(L_2)$.

On continue jusqu'à R ; l'homomorphisme

$$H^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))^{(\xi^{-1})} \to \prod_i H^1_{\mathrm{br}}(F_{l_i}, T^*(1)/MT^*(1))^{(\xi^{-1})}$$

est injectif et pour tout i

$$S_i \Big| \frac{m_\xi(L_{i-1})}{m_\xi(L_i)}.$$

On peut appliquer le lemme 5.1.3 : le cardinal de $h^1_{\mathrm{br},0}(F, T^*(1)/MT^*(1))^{(\xi^{-1})}$ est inférieur à $m_\xi(L_0)$. □

5.2. Théorie d'Iwasawa, préliminaires.

On suppose que V vérifie (Tech). On se donne maintenant un système d'Euler-Iwasawa c p-adique de rang 1 et m un entier fortement admissible.

5.2.1. Théorème. — *On suppose* $c_{p,\xi}(m) = e_\xi c_p(m) \in H^1_\infty(\mathbb{Q}(\mu_m),)$ $T^{(\xi)}$ *d'ordre infini. Alors,* $\mathrm{Leop}(V, \xi)$ *est vraie.*

Démonstration. — $\mathrm{Leop}(V, \xi)$ est vraie si et seulement si $\mathrm{Leop}(V(j), \xi)$ est vraie pour $j \equiv 0 \bmod p-1$. Il existe un entier j tel que

(1) l'espace tangent de $V(j)^*(1)$ soit nul,

(2) $V^{G_{\mathbb{Q}(\mu_{mp})}} = 0$, $V^*(1)^{G_{\mathbb{Q}(\mu_{mp})}} = 0$,

(3) $V^{G_{\mathbb{Q}(\mu_{mp})_v}} = 0$ pour tout $v \in S$,

(4) l'image de $Tw_{j,V}c_{p,\xi}(m) \in H^1_\infty(\mathbb{Q}(\mu_m), T(j))^{(\xi)}$ dans $h^1(\mathbb{Q}(\mu_m), V(j))^{(\xi)}$ est d'ordre infini.

Les propriétés des systèmes d'Euler-Iwasawa se conservant par twist, on peut ainsi supposer que l'espace tangent de $V^*(1)$ est nul et que $c_{p,\xi}(m)$

est d'ordre infini. Donc, $H^1_{\mathrm{br},0}(\mathbb{Q}(\mu_{mp}), V^*(1))^{(\xi^{-1})} = 0$, c'est-à-dire par la dualité de Poitou-Tate,

$$H^2(G_{S,\mathbb{Q}(\mu_{mp})}, V)^{(\xi)} = 0.$$

D'où la nullité de $H^2(G_{S,\mathbb{Q}(\mu_{mp})}, V)^{(\xi)}$, $H^1(G_{S,\mathbb{Q}(\mu_m}, V)^{(\xi)}$ est de dimension $d_{-\epsilon(\xi)}(V)$ et la conjecture $\mathrm{Leop}(V,\xi)$ est démontrée (cf. la démonstration de la proposition 1.3.2 de [PR95]). □

5.2.2. Si ξ est un caractère de Δ_{mp}, on note maintenant $\Lambda = \mathcal{O}[[\mathrm{Gal}(\mathbb{Q}(\mu_{mp^\infty})/\mathbb{Q}]]_\xi$ (il s'agit d'un $\mathcal{O}(\xi)$-module). Si γ est un générateur de $\mathrm{Gal}(\mathbb{Q}(\mu_{mp^\infty})/\mathbb{Q}(\mu_{mp}))$, on pose $\Lambda_n = \Lambda/(\gamma^{p^n}-1)\Lambda$, $\Lambda_{n,M} = \Lambda_n/M\Lambda_n$. On dit qu'une famille de $\Lambda_{n,M}$-homomorphismes $f_{n,M}$ est contrôlée s'il existe un idéal de hauteur 2 annulant les noyaux et conoyaux des $f_{n,M}$. On note $Tw_j : \Lambda \to \Lambda$ l'opérateur de twist induit par $\gamma \to \chi^j(\gamma)\gamma - 1$. Si $G \in \Lambda$ est un élément non nul, pour presque tout entier $j \equiv 0 \bmod p-1$, $\Lambda_n/(Tw_j(G))\Lambda_n = \Lambda/(Tw_j(G), \gamma^{p^n}-1)\Lambda$ est fini pour tout entier n.

5.2.3. Soit $\mathcal{M}$ un Λ-module de type fini et de torsion et $\mathcal{M}_{n,M}$ des Λ_n/M-modules munis d'homomorphismes de Λ-modules $\Lambda_{n,M} \otimes \mathcal{M} \to \mathcal{M}_{n,M}$ contrôlés. Par le théorème de structure des Λ-modules, il existe un homomorphisme injectif de $\overset{s}{\underset{i=1}{\oplus}} \Lambda/f_i\Lambda \to \mathcal{M}$ à conoyau fini.

Lemme. — *Supposons $\Lambda_n/f_i\Lambda_n$ fini pour tout i et posons $M(\mathcal{M},n) = \prod_i \sharp\Lambda_n/f_i\Lambda_n$. Il existe un idéal $\mathfrak{N}$ de hauteur 2 et pour tout entier n, pour tout $M > M(\mathcal{M},n)$ des éléments $\psi_{1,n,M},\dots,\psi_{s,n,M}$ de $\mathcal{M}_{n,M}$ tels que l'annulateur $\mathfrak{A}'_{n,M}(\psi_{i,n,M}) \subset \Lambda_n$ de $\psi_{i,n,M}$ dans $\mathcal{M}_{n,M}/\sum_{j<i}\Lambda_{n,M}\psi_{j,n,M}$ vérifie*

$$\mathfrak{N}\mathfrak{A}'_{n,M}(\psi_{i,n,M}) \subset f_i\Lambda_n \subset \mathfrak{A}'_{n,M}(\psi_{i,n,M}).$$

Démonstration. — On prend pour $\psi_{i,n,M}$ l'image d'un générateur u_i de $\Lambda/f_i\Lambda$ dans $\mathcal{M}_{n,M}$ (par exemple 1). Les homomorphismes de Λ_n-modules

$$\oplus_i \Lambda_n/(f_i, M)\Lambda_n \to \mathcal{M}_{n,M}$$

sont contrôlés. On en déduit que $\mathfrak{N}\mathfrak{A}'_{n,M}(\psi_{i,n,M}) \subset \mathfrak{A}_{n,M}(u_{i,n,M})$ avec $u_{i,n,M}$ l'image de u_i dans $\Lambda_n/(f_i,M)\Lambda_n$ et $\mathfrak{N}$ un idéal de hauteur 2 ($\mathfrak{A}_{n,M}(x)$ désignant l'idéal de Λ_n annulateur de x). En utilisant le fait que $\mathfrak{A}_{n,M}(u_{i,n,M}) = f_i\Lambda_n$, on en déduit la première inclusion. La seconde est claire. □

5.2.4. Soit $\mathcal{M}$ un Λ-module de type fini sans torsion. On se donne de nouveau des $\Lambda_{n,M}$-modules $\mathcal{M}_{n,M}$ et des homomorphismes de Λ-modules compatibles $\Lambda_{n,M} \otimes \mathcal{M} \to \mathcal{M}_{n,M}$ contrôlés. Soit x un élément de $\mathcal{M}$ et $x_{n,M}$ son image dans $\mathcal{M}_{n,M}$. Alors, il existe un Λ-homomorphisme $\mathcal{M}/\Lambda x \to \Lambda^{r-1} \oplus \Lambda/(F_x)\Lambda$ à noyau et conoyau annulés par un idéal de hauteur 2. On note $\mathfrak{B}_{n,M}(x_{n,M})$ l'ensemble des éléments ρ' de Λ_n tels que si $\rho x_{n,M} = 0$ dans $\mathcal{M}_{n,M}$, $\rho'\rho \in M\Lambda_n$, c'est-à-dire tels que $\rho'\mathfrak{A}_{n,M}(x_{n,M}) \subset M\Lambda_n$.

LEMME. — *On suppose que, pour tout n, $\Lambda_n/F_x\Lambda_n$ est fini d'ordre $M_{x,n}$. Alors, il existe un idéal $\mathfrak{N}$ de hauteur 2 tel que pour $M > M_{x,n}$, $\mathfrak{N}.F_x\Lambda_n \subset \mathfrak{B}_{n,M}(x_{n,M})$.*

Démonstration. — Posons $\mathcal{C} = \Lambda x$. Les suites qui suivent sont des complexes et sont exactes à des groupes finis près d'ordre borné indépendamment de n et de M (on dira quasi-exacte contrôlée). De la suite quasi-exacte

$$0 \to \mathcal{C} \to \mathcal{M} \to \Lambda^{r-1} \oplus \Lambda/F_x\Lambda \to 0,$$

on déduit successivement les suites quasi-exactes contrôlées

$$0 \to \Lambda_n \otimes \mathcal{C} \to \Lambda_n \otimes \mathcal{M} \to \Lambda_n^{r-1} \oplus \Lambda_n/F_x\Lambda_n \to 0$$

(on utilise le fait que $\Lambda_n/F_x\Lambda_n$ est fini, ce qui implique $(\Lambda/F_x\Lambda)^{\Gamma_n} = 0$),

$$0 \to \Lambda_n/F_x\Lambda_n \xrightarrow{\delta} \Lambda_{n,M} \otimes \mathcal{C} \to \Lambda_{n,M} \otimes \mathcal{M} \to \Lambda_{n,M}^{r-1} \oplus \Lambda_n/F_x\Lambda_n \to 0$$

(on utilise là le fait que M annule $\Lambda_n/F_x\Lambda_n$). Notons ici x_n (resp. $x_{n,M}$) l'image de x dans $\Lambda_n \otimes \mathcal{M}$ (resp. $\Lambda_{n,M} \otimes \mathcal{M}$). Soit $\mathfrak{N}'$ un idéal de hauteur 2 contrôlant les suites précédentes (c'est-à-dire annulant les groupes de cohomologies de ces suites vues comme complexes) et soit ν un élément quelconque de $\mathfrak{N}'$. Soit ρ appartenant à l'annulateur $\mathfrak{A}_{n,M}(x_{n,M})$ de $x_{n,M}$ dans $\Lambda_{n,M}$. Alors, $\nu\rho x_n$ appartient à l'image de δ et donc $\nu F_x \alpha x_n \in M\Lambda_n \otimes \mathcal{C}$ et $\nu^2 F_x \rho \in M\Lambda_n$. On en déduit que $\nu^2 F_x\Lambda_n \subset \mathfrak{B}_{n,M}(x_{n,M})$ et donc que $F_x\mathfrak{N} \subset \mathfrak{B}_{n,M}(x_{n,M})$ avec $\mathfrak{N} = \mathfrak{N}'^2$. □

5.2.5. Pour L extension de $\mathbb{Q}$ et A un $G_{S,L}$-module topologique, notons $H^2_{0,S}(L, A)$ le noyau de localisation

$$H^2(G_{S,L}, A) \to \oplus_{v \in S} H^2(L_v, A).$$

Notons $H^1_{\mathrm{br},0,S}(L, A)$ le noyau de

$$H^1_{\mathrm{br},\{p\}}(L, A) \to \oplus_{v \in S} H^1(L_v, A).$$

Par la dualité de Tate, les groupes $H^2_{0,S}(L,T/MT)$ et $H^1_{\mathrm{br},0,S}(L,M^{-1}T^*(1)/T^*(1))$ sont en dualité et par passage à la limite sur les extensions finies F_n contenues dans F_∞, on en déduit une dualité de Pontryagin de $\Lambda[\Delta_{mp}]$-modules

$$H^2_\infty(F,T)\times H^1_{\mathrm{br},0,S}(F_\infty,V^*(1)/T^*(1))\to\mathcal{E}/\mathcal{O}.$$

Sous l'hypothèse que $V^*(1)^{G_{F_\infty}}=0$, les applications

$$H^1(G_{S,F_n},M^{-1}T^*(1)/T^*(1))\to H^1(G_{S,F_n},V^*(1)/T^*(1))_M$$

sont contrôlées (cela se déduit de la suite exacte associée à $0\to M^{-1}T^*(1)/T^*(1)\to V^*(1)/T^*(1)\to V^*(1)/T^*(1)\to 0$:

$$\begin{aligned}0\to(V^*(1)/T^*(1))^{G_{F_n}}/M\to H^1(G_{S,F_n},M^{-1}T^*(1)/T^*(1))\\ \to H^1(G_{S,F_n},V^*(1)/T^*(1))_M\to 0\end{aligned}$$

et de ce que $(V^*(1)/T^*(1))^{G_{F_n}}$ est fini d'ordre borné (annulé par $a(T)$)). Notons $\mathcal{H}_{n,M}$ l'image réciproque de $H^1_{\mathrm{br},0,S}(F_n,V^*(1)/T^*(1))_M$ dans $H^1(G_{S,F_n},M^{-1}T^*(1)/T^*(1))$.

5.2.6. Lemme. — *Supposons que pour tout entier n et pour toute place $v\in S$ de F_n, $V^*(1)^{G_{F_{n,v}}}=0$. Les homomorphismes naturels*

$$\Lambda_{n,M}\otimes_\Lambda H^2_\infty(F,T)\to H^2_{0,S}(F_n,T)/M$$

sont contrôlés. De manière équivalente, l'application restriction

$$H^1_{\mathrm{br},0,S}(F_n,V^*(1)/T^*(1))_M\to H^1_{\mathrm{br},0,S}(F_\infty,V^*(1)/T^*(1))^{\Gamma_n}_M$$

a un noyau et conoyau fini d'ordre borné par rapport à n et M.

Si de plus $V^{G_{F_\infty}}=0$, les homomorphismes naturels

$$\Lambda_{n,M}\otimes_\Lambda H^2_\infty(F,T)\to\mathrm{Hom}_{\mathcal{O}}(\mathcal{H}_{n,M},\mathcal{E}/\mathcal{O})$$

sont contrôlés. De manière équivalente, l'application naturelle

$$\mathcal{H}_{n,M}\to H^1_{\mathrm{br},0,S}(F_\infty,V^*(1)/T^*(1))^{\Gamma_n}_M$$

a un noyau et conoyau fini d'ordre borné par rapport à n et M.

Il suffit de remplacer V par un twist convenable $V(j)$ avec $j\equiv 0 \bmod p-1$ pour que les conditions locales soient vérifiées.

Démonstration. — On a le diagramme commmutatif exact

$$\begin{array}{ccccccccc} 0 & \to & H^1(\Gamma_n, A) & \to & H^1(G_{S,F_n}, \mathcal{W}) & \to & H^1(G_{S,F_\infty}, \mathcal{W})^{\Gamma_n} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \prod_{v\in S} H^1(\Gamma_{n,v}, A_v) & \to & \prod_{v\in S} H^1(F_{n,v}, \mathcal{W}) & \to & \prod_{v\in S} H^1(F_{\infty,v}, \mathcal{W})^{\Gamma_n} & \to & 0 \end{array}$$

où $A = (V^*(1)/T^*(1))^{G_{F_\infty}}$, $A_v = (V^*(1)/T^*(1))^{G_{F_{\infty,v}}}$ et $\mathcal{W} = V^*(1)/T^*(1)$. On remarque alors que $H^1(\Gamma_{n,v}, A_v)$ et $H^1(\Gamma_n, A)$ sont finis d'ordre borné : en posant $L = F_\infty$ ou $F_{\infty,v}$, $K_n = F_n$ ou $F_{n,v}$ et $B = A$ ou A_v, on a une suite exacte de $\mathrm{Gal}(L/K_n)$-modules

$$0 \to V^*(1)^{G_L}/T^*(1)^{G_L} \to B \to H^1(L, T^*(1))_{\mathrm{tors}} \to 0 \ ;$$

Comme le premier groupe est divisible et que $H^1(L/K_n, V^*(1)^{G_L}/T^*(1)^{G_L})$ en est un quotient, ce dernier est nul si et seulement si $V^*(1)^{G_{K_n}}$ est nul. Dans ce cas, $H^1(L/K_n, B) = H^1(L/K_n, C)$ où $C = H^1(L, T^*(1))_{\mathrm{tors}}$ est un groupe fini indépendant de n.

Ainsi, dans le diagramme, les groupes de la première colonne sont finis d'ordre borné indépendamment de n. On en déduit facilement le lemme en remarquant que les noyaux des deux dernières flèches verticales sont exactement $H^1_{\mathrm{br},0,S}(F_n, V^*(1)/T^*(1))$ et $H^1_{\mathrm{br},0,S}(F_\infty, V^*(1)/T^*(1))^{\Gamma_n}$. Par dualité, on obtient la première assertion. La deuxième assertion s'en déduit en utilisant la définition de $\mathcal{H}_{n,M}$ et la remarque précédant le lemme. □

5.2.7. Lemme. — *Supposons toujours que* $V^*(1)^{G_{F_\infty}} = 0$ *et que* $V^*(1)^{G_{F_{\infty,v}}} = 0$ *pour* v *divisant* p. *Alors, les*

$$H^1_{\mathrm{br},0,S}(F_n, M^{-1}T^*(1)/T^*(1)) \cap \mathcal{H}_{n,M} \to \mathcal{H}_{n,M}$$

sont contrôlés (i.e le conoyau est fini et d'ordre borné par rapport à M *et* n*).*

Démonstration. — Posons $\mathcal{T} = T^*(1)$ et $\mathcal{V} = V^*(1)$. On déduit du diagramme commutatif et exact

$$\begin{array}{ccccccccc} 0 & \to & (\mathcal{V}/\mathcal{T})^{G_{F_n}} & \to & H^1(G_{S,F_n}, M^{-1}\mathcal{T}/\mathcal{T}) & \to & H^1(G_{S,F_n}, \mathcal{V}/\mathcal{T})_M & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \prod_{v\in S}(\mathcal{V}/\mathcal{T})^{G_{F_{n,v}}} & \to & \prod_{v\in S} H^1(F_{n,v}, M^{-1}\mathcal{T}/\mathcal{T}) & \to & \prod_{v\in S} H^1(F_{n,v}, \mathcal{V}/\mathcal{T})_M & \to & 0 \end{array}$$

que l'image par localisation en $v \in S$ d'un élément de $\mathcal{H}_{n,M}$ appartient à $(\mathcal{V}/\mathcal{T})^{G_{F_{n,v}}}$.

Supposons d'abord que v ne divise pas p. L'image de $(\mathcal{V}/\mathcal{T})^{G_{F_{n,v}}}/M$ dans

$$H^1(F_{n,v}, M^{-1}\mathcal{T}/\mathcal{T})/H^1_{\mathrm{br}}(F_{n,v}, M^{-1}\mathcal{T}/\mathcal{T}) = H^1(I_v, \mathcal{T}/M\mathcal{T})$$

est contenue dans $H^1(I_v, \mathcal{T})_{\text{tors}}$: en effet, l'application

$$(\mathcal{V}/\mathcal{T})^{G_{F_{n,v}}} \to H^1(F_{n,v}, M^{-1}\mathcal{T}/\mathcal{T})$$

se factorise par $H^1(F_{n,v}, \mathcal{T})$. Les $\mathbb{Z}_p$-modules de torsion $H^1(I_{F_{n,v}}, \mathcal{T})_{\text{tor}}$ sont finis d'ordre borné par rapport à n ([PR92, 2.2]) ; d'autre part, lorsque v divise p, les groupes $(\mathcal{V}/\mathcal{T})^{G_{F_{n,v}}}$ sont finis d'ordre borné par rapport à n. Finalement, il existe une constante c (liée aux nombres de Tamagawa de V et à l'ordre de $(\mathcal{V}/\mathcal{T})^{G_{F_{n,v}}}$ telle que $c\mathcal{H}_{n,M}$ soit contenu dans dans le noyau de localisation en $v \in S$, c'est-à-dire dans $H^1_{\text{br},0,S}(F_n, M^{-1}T^*(1)/T^*(1))$. □

5.2.8. On fixe un entier m et un caractère ξ de Δ_{mp} et on pose $F = \mathbb{Q}(\mu_{mp})$. On suppose que m est fortement admissible et que V vérifie les hypothèses du théorème 1.3.3. En particulier, $V^{G_{F_\infty}}$ est nul ainsi que $V^*(1)^{G_{F_{\infty,v}}}$ pour toute place v divisant p (on n'a en fait besoin de ces hypothèses que pour les ξ-parties à condition de rajouter la nullité de $(V^*(1)^{G_{F_\infty}})^{(\xi^{-1})}$).

On fait désormais l'hypothèse que $c_{p,\xi}(m) = e_\xi c_p(m) \in H^1_\infty(\mathbb{Q}(\mu_m), T)^{(\xi)}$ n'est pas de Λ_ξ-torsion. D'après 5.2.1, le Λ_ξ-module $H^1_\infty(F,T)^{(\xi)}$ est de Λ_ξ-rang $d_{-\epsilon(\xi)}$ et le Λ_ξ-module $H^2_\infty(F,T)^{(\xi)}$ est de Λ_ξ-torsion. De plus, on peut définir comme en 5.2.4 un élément $\mathcal{F}_\xi = F_{c_{p,\xi}(m)}$ de Λ non nul. Rappelons ([PR95, proposition 3.4.2]) que l'application naturelle

$$H^1_\infty(F,V)_{\Gamma_n} \to H^1(F_n, V)$$

est injective. Comme $H^1_\infty(F,T)^{(\xi)}$ est sans Λ_ξ-torsion, le sous-$\mathcal{O}(\xi)$-module de torsion de $H^1_\infty(F,T)^{(\xi)}_{\Gamma_n}$ est fini et d'ordre borné et il en est de même du noyau de

$$H^1_\infty(F,T)^{(\xi)}_{\Gamma_n} \to H^1(F_n, T)^{(\xi)}.$$

L'application

$$H^1_{\text{br},\{p\}}(F_n, T)/M \to H^1_{\text{br},\{p\}}(F_n, T/M)$$

est d'autre part injective. On en déduit que si $H^1_{f,\{p\}}(F_n, T/MT)_0$ désigne l'image de $H^1_\infty(F,T)$ dans $H^1(F_n, T/MT)$, les homomorphismes de $\Lambda_{\xi,n,M}$-modules

$$\Lambda_{\xi,n,M} \otimes H^1_\infty(F,T)^{(\xi)} \to H^1_{\text{br},\{p\}}(F_n, T/MT)^{(\xi)}_0 \tag{5.2.1}$$

sont contrôlés.

5.2.9. Nous prenons ici $\Lambda_n = \Lambda_{n,\xi}$ pour simplifier les notations. Soit f_ξ une série caractéristique de $H^2_\infty(F,T)^{(\xi)}$. Si $\mathcal{C}_\xi$ est le sous-Λ-module de $H^1_\infty(F,T)^{(\xi)}$ engendré par $c_{p,\xi}(m)$, soit $\mathcal{F}_\xi$ une série caractéristique du sous-module de torsion de $H^1_\infty(F,T)^{(\xi)}/\mathcal{C}_\xi$.

En remplaçant V par un twist $V(j)$ avec $j \equiv 0 \bmod p-1$, on peut supposer que :

(1) pour tout entier n, $\Lambda_n/\mathcal{F}_\xi\Lambda_n$ est fini, c'est-à-dire $\eta(\mathcal{F}_\xi) \neq 0$ pour tout caractère η d'ordre fini de Γ;

(2) pour tout $v \in S$, pour tout entier n, $V^*(1)^{G_{F_{n,v}}} = 0$;

(3) $\Lambda_n \otimes H^2_\infty(F,T)^{(\xi)}$ est fini pour tout entier n, i.e. $\eta(f_\xi) \neq 0$ pour tout caractère η d'ordre fini de Γ.

On a alors les propriétés suivantes :

(1) si $\mathcal{M}_{n,M} = \mathrm{Hom}_{\mathcal{O}}(\mathcal{H}_{n,M}, \mathcal{E}/\mathcal{O})^{(\xi)}$, par le lemme 5.2.6, les homomorphismes

$$\Lambda_{n,M} \otimes H^2_\infty(\mathbb{Q}(\mu_m),T)^{(\xi)} \to \mathcal{M}_{n,M} \tag{5.2.2}$$

sont contrôlés; il existe un idéal $\mathfrak{N}_0$ de hauteur 2 tel que

$$\mathfrak{N}_0 \mathcal{H}_{n,M}^{(\xi^{-1})} \subset H^1_{\mathrm{br},0,S}(F_n, M^{-1}T^*(1)/T^*(1)); \tag{5.2.3}$$

(2) $\mathcal{M}_{n,M}$ est fini et d'ordre borné par rapport à M. On peut appliquer le lemme 5.2.3 à $\mathcal{M} = H^2_\infty(F,T)^{(\xi)}$ et $\mathcal{M}_{n,M}$: on a

$$\hat{\mathcal{M}} = H^1_{\mathrm{br},0,S}(F_\infty, V^*(1)/T^*(1))^{(\xi^{-1})}, \hat{\mathcal{M}}_{n,M} = \mathcal{H}_{n,M}^{(\xi^{-1})}.$$

On note f_i des éléments de Λ tels que $H^2_\infty(F,T)^{(\xi)}$ est isomorphe à $\bigoplus_{i=1}^{s} \Lambda/(f_i)$ à un groupe fini près. D'après le lemme 5.2.3, il existe

$$\psi^*_{i,M} \in \mathrm{Hom}_{\mathcal{O}}(\mathcal{H}_{n,M}^{(\xi^{-1})}, \mathcal{O}/M\mathcal{O})$$

tel que si $M_1(n) \geqslant \prod_{i=1}^{r} \sharp\Lambda_n/f_i\Lambda_n$, pour tout entier n, pour tout $M > M_1(n)$ l'annulateur $\mathfrak{A}'_{n,M}(\psi^*_{i,M}) \subset \Lambda_n$ de $\psi^*_{i,M}$ dans $\mathcal{M}_{n,M}/\sum_{j<i} \Lambda_{n,M}\psi^*_{j,M}$ vérifie

$$\mathfrak{N}_1 \mathfrak{A}'_{n,M}(\psi^*_{i,M}) \subset f_i\Lambda_n \tag{5.2.4}$$

pour $\mathfrak{N}_1$ un idéal de hauteur 2. On peut prendre $M_1(n)$ supérieur aux cardinaux des $\mathcal{M}_{n,M}$ pour tout M.

(3) On peut appliquer le lemme 5.2.4 à $H^1_\infty(\mathbb{Q},T)^{(\xi)}$, $H^1_{f,\{p\}}(F_n,T/MT)^{(\xi)}_0$ et $x=c_{p,\xi}(m)$. Ainsi, on a $\mathcal{F}_\xi=F_x$ et il existe un idéal $\mathfrak{N}_2$ de hauteur 2 tel que pour $M>M_2(n)=\sharp(\Lambda_n/\mathcal{F}_\xi\Lambda_n)$, on ait

$$\mathfrak{N}_2\mathcal{F}_\xi\Lambda_n\subset\mathfrak{B}_{n,M}(c_\xi(mp^{n+1})) \tag{5.2.5}$$

où $\mathfrak{B}_{n,M}(c_\xi(mp^{n+1}))$ est l'ensemble des ρ' de Λ_n tels que si $\rho c_{p,\xi}(mp^{n+1})=0$ dans $H^1_{f,\{p\}}(F_n,T/MT)^{(\xi)}_0$, $\rho'\rho\in M\Lambda_n$.

5.3.

5.3.1. D'après les lemmes 4.4.5 et 4.3 , les $\tilde{m}_{F_n}$ et les s_{F_n} sont bornés lorsque F_n parcourt les sous-extensions de F_∞. Notons $\tilde{m}$ (resp. s) des puissances de p divisibles par tous les $\tilde{m}_{F_n}$ (resp. par les s_{F_n}) et posons $\alpha=\tilde{m}s$. On choisit un élément g de $GL(T)$ tel que $V/(g^\alpha-1)V$ soit de dimension 1, appartenant à l'image de $G_{\mathbb{Q}(\mu_{mp^\infty})}$ et tel que g^α vérifie la condition (**). On note t_0 un élément de T, non divisible par p, dont l'image dans $V/(g^\alpha-1)V$ en est une base, α_3 un élément de $\mathcal{O}$ tel que $\alpha_3 t_0\in\tilde{Q}(g^\alpha,g)T$. On pose comme en 4.6.1 $\alpha_1=\alpha\alpha'$, $\alpha_2=s\alpha'$ avec $\alpha'T\subset(1+\dots g^{\alpha-1})T$. On choisit aussi un idéal $\mathfrak{N}$ de hauteur 2 annulant $a=a(T)$ annulant $(V/T)^{G_{\mathbb{Q}(\mu_{mp^\infty})}}$ et contenu dans les idéaux $\mathfrak{N}_0$, $\mathfrak{N}_1$ et $\mathfrak{N}_2$ de hauteur 2 rencontrés dans (5.2.3), (5.2.4) et (5.2.5). On prend $\nu\in\mathfrak{N}$ premier à $\gamma^{p^n}-1$ pour tout entier n.

On fixe un entier n. Soient $M_1(n)$ comme dans (5.2.4) et $M_2(n)$ comme dans (5.2.5). Soit d'autre part $M_3(n)$ une puissance de p supérieure à $\sharp(\Lambda_n/\nu\Lambda_n)$. Enfin, M est une puissance de p sur laquelle on donnera des conditions à chaque étape.

Tous les nombres premiers choisis dans la suite appartiennent à $S_{g^\alpha,M}(Mm)$. On dispose alors d'un opérateur

$$\mathrm{Dér}_{\lambda,n}=\mathrm{Dér}_{\lambda,\mathrm{Gal}(F_n/F)}:\oplus_{\lambda|l}H^1_{\mathrm{br}}(F_{n,\lambda},T/MT)\to\oplus_{\lambda|l}H^1_{/br}(F_{n,\lambda},T/MT).$$

Le noyau et le conoyau de $\mathrm{Dér}_{\lambda,n}$ sont annulés par α_3 qui est indépendant de n. On note $\mathrm{Ev}_{t_0,l,n}(x)$ l'élément de $\Lambda_n/M\Lambda_n$ tel que $\mathrm{Ev}_{l,\mathrm{Gal}(F_n/F)}(x)=\mathrm{Ev}_{t_0,l,n}(x)\otimes t_0$ pour $x\in\oplus_{\lambda|l}H^1_{/br}(F_{n,\lambda},T/MT)$. Enfin, on note $<\ ,\ >_{l,n}=<\ ,\ >_{l,\mathrm{Gal}(F_n/F)}$.

5.3.2. Prenons pour l'instant $M>M_1(n)$.

Étape 1 : *Il existe un nombre premier* $l_1 \in S_{g^\alpha,M}(Mm) - S$ *et une place* λ_1 *au-dessus de* l_1 *tels que*

$$\begin{aligned} \alpha_2 \mathrm{Ev}_{l_1,n} \mathrm{Dér}_{l_1,n}(c_\xi(mp^{n+1})) &\equiv \nu\alpha_1\alpha_3\mathcal{F}_\xi \otimes t_0 \bmod M\Lambda_n \otimes T \\ \alpha_2[t_0, \mathrm{ev}_{l_1,n}(y)]_\zeta^{(M)} &= \nu\alpha_1\tilde{\psi}^*_{1,M}(y) \end{aligned} \tag{5.3.1}$$

pour tout $y \in \mathcal{H}_{n,M}$.

La première équation implique que

$$\alpha_2 \mathrm{Ev}_{t_0,l_1,n}(d^{(\nu)}_{M,\xi}(mp^{n+1}, l_1))) \equiv \nu^2\alpha_1\alpha_3\mathcal{F}_\xi \bmod M\Lambda_n. \tag{5.3.2}$$

Démonstration. — On choisit $t_0^* \in T^*(1)$ tel que $[t_0, t_0^*]^{(M)} = 1$ et on applique la proposition 4.7.5 en utilisant le fait que $\nu\mathcal{F}_\xi \in \mathfrak{B}_{n,M}(c_\xi(mp^{n+1}))$ par (5.2.5). □

5.3.3. On a

$$\begin{aligned} \alpha_2^2 < d^{(\nu)}_{M,\xi}(mp^{n+1}, l_1), y >^{(M)}_{l_1,n} &= \alpha_2^2\nu < \mathrm{Dér}_{l_1,n} c_\xi(mp^{n+1}), y >^{(M)}_{l_1,n} \\ &= \nu^3\alpha_1^2\alpha_3(\mathcal{F}_\xi\psi^*_{1,M})(y). \end{aligned}$$

La loi de réciprocité appliquée à $d^{(\nu)}_{M,\xi}(mp^{n+1}, l_1)$ et à νy pour $y \in \mathcal{H}_{n,M}$ implique que

$$\nu^4\alpha_3\alpha_1^2\mathcal{F}_\xi\psi^*_{1,M} = 0,$$

car $\nu\mathcal{H}^{(\xi^{-1})}_{n,M}$ est contenu dans $H^1_{\mathrm{br},0,S}(F_n, M^{-1}T^*(1)/T^*(1))^{(\xi^{-1})}$ et l'image de $\nu^4\alpha_3\alpha_1^2\mathcal{F}$ dans Λ_n appartient à $\mathfrak{A}_{n,M}(\psi^*_{1,M}) = \mathfrak{A}'_{n,M}(\psi^*_{1,M})$. Comme M est un multiple de $\sharp(\Lambda_n/f_1\Lambda_n)$, M appartient à $f_1\Lambda_n$ et par (5.2.4), $\nu^5\alpha_4\mathcal{F}_\xi \in f_1\Lambda_n$ avec $\alpha_4 = \alpha_3\alpha_1^2$. On écrit $\nu^5\alpha_4\mathcal{F}_\xi = f_1\mathcal{F}_1$ dans Λ_n.

Lemme. — *Prenons* $M = M_1^2$ *avec* $M_1 > \alpha_1\alpha_3^2M_1(n)M_2(n)M_3(n)$. *Alors,* $\mathcal{F}_1$ *appartient à* $\mathfrak{B}_{M_1,n}(d^{(\nu)}_{M_1,\xi}(mp^{n+1}, l_1))$.

Démonstration. — On a

$$\nu^2\alpha_1\alpha_2\mathrm{Ev}_{t_0,l_1,n}(d_M) \equiv f_1\mathcal{F}_1 \bmod M.$$

La projection de $d_M = d^{(\nu)}_{M,\xi}(mp^{n+1}, l_1)$ dans $H^1_{\mathrm{br},\{l_1,p\}}(F_n, T/M_1T)$ est égale à $d_{M_1} = d^{(\nu)}_{M_1,\xi}(mp^{n+1}, l_1)$. Montrer que $\mathcal{F}_1 \in \mathfrak{B}_{M_1,n}(d_{M_1})$ est équivalent à montrer que si $\rho d_{M_1} = 0$ pour $\rho \in \Lambda_n$, alors $\rho\mathcal{F}_1 \in M_1\Lambda_n$. Soit donc $\rho \in \Lambda_n$ tel que $\rho d_{M_1} = 0$. On a alors $\rho d_M = M_1 d'$ avec $d' \in H^1(G_{S\cup\{l_1\},F_n}, M_1^{-1}T/T)^{(\xi)}$. La loi de réciprocité implique que

$$\nu < d', y >^{(M_1)}_{l_1,n} = 0 \tag{5.3.3}$$

pour tout $y \in \mathcal{H}_{n,M_1}$ car $\nu y \in H^1_{\mathrm{br},0,S}(F_n, T^*(1)/M_1T^*(1))^{(\xi^{-1})}$, On en déduit que $\mathrm{Ev}_{t_0,l_1,n}(d')$ annule $\nu\psi^*_{1,M_1}$ et donc que $\nu^2\mathrm{Ev}_{t_0,l_1,n}(d') = f_1\alpha$ avec $\alpha \in \Lambda_n$. Comme $\rho\mathrm{Ev}_{t_0,l_1,n}(d_M) \equiv M_1\mathrm{Ev}_{t_0,l_1,n}(d')$ mod M et $\nu^2\alpha_1\alpha_2\mathrm{Ev}_{t_0,l_1,n}(d_M) \equiv f_1\mathcal{F}_1$ mod M, on obtient

$$\begin{aligned}\alpha_1\alpha_2M_1f_1\alpha \equiv \alpha_1\alpha_2M_1\nu^2\mathrm{Ev}_{t_0,l_1,n}(d') &= \nu^2\rho\alpha_1\alpha_2\mathrm{Ev}_{t_0,l_1,n}(d_M)\\ &= \rho\mathcal{F}_1f_1 \text{ mod } M_1^2\Lambda_n.\end{aligned}$$

La multiplication par f_1 étant injective sur Λ_n et M_1 appartenant à $f_1\Lambda_n$, on en déduit que $\rho\mathcal{F}_1$ appartient à $M_1\Lambda_n$, ce qui termine la démonstration.

□

5.3.4. Grâce à $\mathcal{F}_1 \in \mathfrak{B}_{n,M_1}(d^{(\nu)}_{M_1,\xi}(mp^{n+1}, l_1))$, on peut appliquer de nouveau la proposition 4.7.5. :

Étape 2 : *Il existe* $l_2 \in S_{g^\alpha,M_1}(M_1m) - S$ *tel que*

$$\begin{aligned}\alpha_2\mathrm{Dér}_{l_2,n}(d^{(\nu)}_{M_1,\xi}(mp^{n+1}, l_1)) &\equiv \alpha_1\alpha_3\mathcal{F}_1 \otimes t_0 \text{ mod } M_1\Lambda_n \otimes T\\ \alpha_2[t_0, \mathrm{ev}_{l_2,n}(y)]^{(M_1)}_\zeta &= \nu\alpha_1\tilde{\psi}^*_{2,M_1}(y)\end{aligned} \tag{5.3.4}$$

pour $y \in \mathcal{H}_{n,M_1}$.

On a donc comme précédemment

$$\begin{aligned}\alpha_2^2 < d^{(\nu)}_{M_1,\xi}(mp^{n+1}, l_1l_2), y >^{(M_1)}_{l_2,n}&\\ = \alpha_1^2\alpha_3 < \mathrm{Dér}_{l_2,n}(d^{(a)}_{M_1,\xi}(mp^{n+1}, l_1)), y >^{(M_1)}_{l_2,n} &= \nu\alpha_4\mathcal{F}_1\tilde{\psi}^*_{2,M_1}(y).\end{aligned}$$

D'autre part, $< d^{(\nu)}_{M_1,\xi}(mp^{n+1}, l_1l_2), y >^{(M_1)}_{l_1,n} = \alpha[t_0, \mathrm{ev}_{l_1,n}(y)]^{(M_1)}_\zeta = \nu\alpha\alpha_2$ $\tilde{\psi}^*_{1,M_1}(y)$. En utilisant de nouveau la loi de réciprocité, on en déduit que $\nu\alpha_4\mathcal{F}_1\psi^*_{2,M_1} \in \Lambda_n\psi^*_{1,M_1}$, et par (5.2.4) que

$$\nu^2\alpha_4\mathcal{F}_1 \in (f_2, M_1)\Lambda_n.$$

Comme M_1 est un multiple de $\sharp(\Lambda_n/f_2\Lambda_n)$, $M_1 \in f_2\Lambda_n$ et $\nu^2\alpha_4\mathcal{F}_1 \in f_2\Lambda_n$: $\nu^2\alpha_4\mathcal{F}_1 = f_2\mathcal{F}_2$ avec $\mathcal{F}_2 \in \Lambda_n$.

Lemme. — *Prenons* $M_1 = M_2^2$ *avec* $M_2 > \alpha_1\alpha_3^2M_1(n)M_2(n)M_3(n)$. *Alors,* $\mathcal{F}_2$ *appartient à* $\mathfrak{B}_{M_2,n}(d^{(\nu)}_{M_2,\xi}(mp^{n+1}, l_1l_2))$.

Démonstration. — La démonstration se fait comme dans le lemme 5.3.3. Soit $\rho \in \Lambda_n$ tel que $\rho d^{(\nu)}_{M_2,\xi}(mp^{n+1}, l_1l_2) = 0$ pour $\rho \in \Lambda_n$. On a $\rho d^{(\nu)}_{M_2,\xi}(mp^{n+1}, l_1l_2) = d'$ avec $d' \in H^1(G_{S\cup\{l_1,l_2\},F_n}, T/M_2T)^{(\xi)}$. La loi de réciprocité implique que

$$\nu < d', y >^{(M_2)}_{l_1,n} + \nu < d', y >^{(M_2)}_{l_2,n} = 0 \tag{5.3.5}$$

pour tout $y \in \mathcal{H}^{(\xi^{-1})}_{n,M_2}$. D'où, $\nu \mathrm{Ev}_{t_0,l_2,n}(d')\psi^*_{2,M_2} \in \psi^*_{1,M_2}\Lambda_n$ et par (5.2.4), $\nu^2 \mathrm{Ev}_{t_0,l_2,n}(d') = f_1\lambda \bmod M_2$ avec $\lambda \in \Lambda_n$. On en conclut encore que $\rho\mathcal{F}_1 \in M_2\Lambda_n$, ce qui termine la démonstration. □

5.3.5. Les étapes suivantes sont identiques. On prend maintenant M' quelconque supérieur à $\alpha_2\alpha_3^2 M_1(n)M_2(n)M_3(n)$ et $M = M'^{2^r}$, $M_i = M'^{2^{r-i}}$. On construit ainsi des éléments $\mathcal{F}_1, \ldots, \mathcal{F}_r$ de Λ_n vérifiant

$$\begin{aligned}
\nu^5\alpha_4\mathcal{F}_\xi &\equiv f_1\mathcal{F}_1 \bmod M'\Lambda_n \\
\nu^2\alpha_4\mathcal{F}_1 &\equiv f_2\mathcal{F}_2 \bmod M'\Lambda_n \\
&\cdots \\
\nu^2\alpha_4\mathcal{F}_{r-2} &\equiv f_{r-1}\mathcal{F}_{r-1} \bmod M'\Lambda_n \\
\nu^2\alpha_4\mathcal{F}_{r-1} &\equiv f_r\mathcal{F}_r \bmod M'\Lambda_n.
\end{aligned}$$

Donc,

$$\nu^{2r+3}\alpha_4^r\mathcal{F}_\xi \equiv \mathcal{F}_r f_r \ldots f_1 \equiv \mathcal{F}_r f_\xi \bmod M'\Lambda_n.$$

Comme $M' \in f_r \ldots f_1\Lambda_n$, on en déduit que $\nu^r\alpha_4^r\mathcal{F}_\xi \in f_\xi\Lambda_n$ pout tout entier n, donc $\nu^r\alpha_4^r\mathcal{F}_\xi \in f_\xi\Lambda$. L'élément ν a été choisi dans un idéal de hauteur 2. En faisant deux choix de ν premiers entre eux, on obtient le résultat final :

$$\alpha_4^r\mathcal{F}_\xi \in f_\xi\Lambda.$$

5.3.6. Lorsque $\alpha_4 = 1$, on a $\mathcal{F}_\xi \in f_\xi\Lambda$. Cela se produit si $\alpha_1 = \alpha_3 = 1$, c'est-à-dire si $\tilde{m} = 1$, $s = 1$ et si l'espace propre relatif à la valeur propre 1 pour g agissant sur T/pT est de dimension 1.

Appendice A. Loi de réciprocité pour $l \neq p$.

On donne la démonstration détaillée du lemme 3.2.8 (voir aussi la thèse de E. Frossart (Orsay)).

Soit l un nombre premier différent de p, K une extension finie de $\mathbb{Q}_l$, A un G_K-module fini annulé par une puissance M de p. On note I_K le groupe d'inertie, Π une uniformisante de K et pour $\sigma \in I_K$,

$$\zeta_\sigma = \frac{\sigma(\sqrt[M]{\Pi})}{\sqrt[M]{\Pi}} \in \mu_M = \mathbb{Z}_p(1)/M\mathbb{Z}_p(1).$$

Lemme. — *Notons* $\mathrm{ev} : H^1_{\mathrm{br}}(K, \hat{A}(1)) \to \hat{A}(1)/(\varphi-1)\hat{A}(1)$ *l'évaluation sur* Frob *et* Ev_σ *l'évaluation sur* σ *pour* $\sigma \in I_K$. *Si* $< , >$ *est l'accouplement*

local

$$H^1(K,A)\times H^1(K,\hat{A}(1))\to H^2(K,\mu_M)\overset{\text{inv}}{\cong}\mathbb{Z}/M\mathbb{Z}$$

et

$$[\ ,\ ]: A\times\hat{A}(1)\to\mathbb{Z}(1)/M\mathbb{Z}(1)$$

l'accouplement naturel, on a pour tout $\sigma\in I_K$

$$<x,y>\zeta_\sigma=[\mathrm{Ev}_\sigma(x),\mathrm{ev}(y)]$$

pour $x\in H^1(K,A)$ *et* $y\in H^1_{\mathrm{br}}(K,\hat{A}(1))$.

Pour passer au lemme 3.2.8 , on remarque que $[\ ,\ ]_\zeta^{(M)}=[\ ,\ ].\zeta^{-1}$ et que $\zeta_{\sigma_\lambda}=\zeta$.

Rappelons quelques généralités cohomologiques bien connues. Soit G un groupe profini, I un sous-groupe fermé distingué de p-dimension cohomologique 1 et A un G-module topologique annulé par une puissance de p. Il existe des applications

$$r_{i-1}: H^i(G,A)\to H^{i-1}(G/I,H^1(I,A))$$

telles que la suite suivante soit exacte

$$H^i(G/I,A^I)\overset{\text{inf}}{\to}H^i(G,A)\overset{r_{i-1}}{\to}H^{i-1}(G/I,H^1(I,A))\to H^{i+1}(G/I,A^I).$$

Ce résultat se trouve dans [H-S] et utilise les suites spectrales de Hochschild-Serre. On peut décrire explicitement l'homomorphisme r_{i-1}. Pour r_0, il s'agit simplement de restreindre un cocycle de G à I. Dans les autres cas, on a besoin du fait suivant :

LEMME. — *Soit* a *un* i*-cocycle de* G *à valeurs dans* A*; si* $i=1$*, on a* $a(1)=0$*. Si* $i\geqslant 2$*, il existe un* i*-cocycle* a' *cohomologue à* a *tel que* $a'(g,h_2,\ldots,h_i)=0$ *pour tout* $g\in G$ *et* $h_j\in I$*. On dit que* a' *est un cocycle normalisé.*

Démonstration. — Pour $i=1$, on a $a(g)=a(g.1)=ga(1)+a(g)$, d'où $a(1)=0$. Démontrons l'assertion suivante uniquement pour $i=2$ qui est le seul cas dont nous aurons besoin. Comme $(h,h')\to a(h,h')$ est un 2-cocycle de I à valeurs dans A, c'est un cobord : $a(h,h')=hb(h')-b(hh')+b(h)$ avec $b: I\to A$. Fixons un système de représentants $(g_j)_{j\in J}$ de G/I et des éléments $b_j\in A$ pour $j\in J$ et définissons une fonction b sur G à valeurs dans A par la formule

$$b(g_jh)=b_j+g_ib(h)-a(g_i,h).$$

On pose alors $a'(g,g') = a(g,g') - gb(g') + b(gg') - b(g)$. C'est un 2-cocycle de G cohomologue à a et on vérifie facilement par le calcul que $a'(g,h) = 0$ pour $h \in I$. □

Donnons alors la définition de r_{i-1} pour $i = 1$ et 2. Soit a un 1-cocycle, on a

$$\begin{aligned}(g-1)(a)(h) &= ga(g^{-1}hg) - a(h) = gg^{-1}ha(g) + ga(g^{-1}h) - a(h)\\ &= ha(g) + a(h) + ga(g^{-1}) - a(h)\\ &= (h-1)a(g) + ga(g^{-1}) + a(g)\\ &= (h-1)a(g) + a(1) = (h-1)a(g).\end{aligned}$$

Donc la classe de $h \to a(h)$ dans $H^1(I,A)$ est invariante par G/I, c'est l'image par r_0 de la classe de a.

Soit a un 2-cocycle normalisé. On déduit de l'identité de cocycle :

$$ga(g',h) - a(gg',h) + a(g,g'h) - a(g,g') = 0$$

et de la nullité des deux premiers termes que $a(g,g'h) = a(g,g')$ pour $h \in I$. Comme I est distingué dans G, on a aussi $a(g,hg') = a(g,g')$. On vérifie ensuite que $h \to a(h,g)$ est un 1-cocycle de I :

$$\begin{aligned}&h'a(h,g) - a(h'h,g) + a(h',g)\\ &\qquad = -a(h',hg) - a(h',h) + a(h',g) - a(h',g) + a(h',g) = 0.\end{aligned}$$

On vérifie alors que $g \to a_g(h) = a(h,g)$ vérifie la relation de 1-cocycles modulo les 1-cobords de I :

$$\begin{aligned}g'(a_g)(h) - a_{g'g}(h) + a_{g'}(h) &= g'a(g'^{-1}hg',g) - a(h,g'g) + a(h,g')\\ &= a(hg',g) - a(g',g'^{-1}hg'g) + a(g',g'^{-1}hg') - a(h,g'g) + a(h,g')\\ &= a(hg',g) - a(g',g) - a(h,g'g) + a(h,g')\\ &= (h-1)a(g',g) - ha(g',g) + a(hg',g) - a(h,g'g) + a(h,g')\\ &= (h-1)a(g',g).\end{aligned}$$

Ainsi, si $\alpha(g)$ est la classe dans $H^1(I,A)$ de a_g, $g \to \alpha(g)$ est un 1-cocycle de G/I à valeurs dans $H^1(I,A)$; sa classe dans $H^1(G/I, H^1(I,A))$ est l'image par r_1 de la classe de a.

De manière générale, soit a un i-cocycle normalisé. Si $a_{g_2,\dots,g_i}(h) = a(h,g_2,\dots,g_i)$ et si $\alpha(g_2,\dots,g_i)$ est la classe dans $H^1(I,A)$ de $a_{g_2,\dots,g_i}$, $(g_2,\dots,g_i) \to \alpha(g_2,\dots,g_i)$ est un $i-1$-cocycle de G/I à valeurs dans

$H^1(I,A)$; sa classe dans $H^{i-1}(G/I, H^1(I,A))$ est l'image par r_{i-1} de la classe de a.

LEMME. — *On a le diagramme commutatif suivant :*

$$\begin{array}{ccccc} H^i(G,A) & \otimes & H^j(G,B) & \to & H^{i+j}(G, A\otimes B) \\ \downarrow r_{i-1} & & \uparrow \inf & & \downarrow r_{i+j-1} \\ H^{i-1}(G/I, H^1(I,A)) & \otimes & H^j(G/I, B^I) & \to & H^{i+j-1}(G/I, H^1(I, A\otimes B)) \end{array}$$

où la première flèche horizontale est donnée par le cup-produit relatif à G, la seconde flèche horizontale par le cup produit relatif à G/I :

$$H^{i-1}(G/I, A') \otimes H^j(G/I, B') \to H^{i+j-1}(G/I, A'\otimes B')$$

avec $A' = H^1(I,A)$ et $B' = H^0(I,B)$ puis à I :

$$H^1(I,A)\otimes H^0(I,B) \to H^1(I, A\otimes B)),$$

autrement dit,

$$r_{i-1}(a)\cup b = r_{i+j-1}(a\cup \inf(b))$$

pour $a\in H^i(G,A)$ et $b\in H^j(G/I,B^I)$. On vérifie facilement la commutativité du diagramme en utilisant la description de r_{i-1} qui a été faite.

Prenons maintenant A annulé par M, $B = \hat{A}(1) = \mathrm{Hom}_{\mathcal{O}}(A, \mu_M)$, $i = j = 1$. En composant avec $A\otimes B \to \mu_M$, on obtient le diagramme commutatif

$$\begin{array}{ccccc} H^1(G,A) & \otimes & H^1(G,B) & \to & H^2(G,\mu_M) \\ \downarrow & & \uparrow & & \downarrow \\ H^0(G/I, H^1(I,A)) & \otimes & H^1(G/I, B^I) & \to & H^1(G/I, H^1(I,\mu_M)). \end{array}$$

Prenons maintenant pour $G = G_K$ le groupe de Galois absolu d'une extension finie K de $\mathbb{Q}_l$ avec $l\neq p$ et pour $I = I_K$ son sous-groupe d'inertie ; soit Π une uniformisante de K et v la valuation de K normalisée par $v(\Pi) = 1$. Rappelons que l'on a une surjection $\epsilon = \lim\limits_{\leftarrow n} \epsilon_{p^n} : I_K \to \mathbb{Z}_p(1)$ de G_K-modules dont le noyau est d'ordre (profini) premier à p donné par

$$h\in I_K \mapsto \lim_n \frac{h(\sqrt[p^n]{\Pi})}{\sqrt[p^n]{\Pi}}.$$

On en déduit un isomorphisme $\gamma : H^1(I_K, \mu_M) = \mathrm{Hom}(I_K, \mu_M) \cong \mathbb{Z}/M\mathbb{Z}$ vérifiant $\gamma(b)\epsilon_M(h) = b(h)$. On a alors un isomorphisme naturel $\theta = \mathrm{ev}\circ\gamma$:

$$\begin{aligned} H^1(G_K/I_K, H^1(I_K,\mu_M)) &= H^1(G_K/I_K, \mathbb{Z}/M\mathbb{Z}) \\ &= \mathrm{Hom}(G_K/I_K, \mathbb{Z}/M\mathbb{Z}) \cong \mathbb{Z}/M\mathbb{Z}. \end{aligned}$$

Soit d'autre part l'isomorphisme inv : $H^2(G_K, \mu_M) \to \mathbb{Z}/M\mathbb{Z}$ provenant de la théorie du corps de classes. La propriété suivante le caractérise : Si $\xi \in H^1(G_K, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_K, \mathbb{Q}/\mathbb{Z})$, $\alpha \in K$ et si $\delta(\alpha)$ est l'image de α dans $H^1(G_K, \mu_M)$, alors

$$\mathrm{inv}(\delta(\alpha) \cup \xi) = \xi(\sigma_\alpha) \tag{A.07}$$

où σ_α est un élément de G_K construit par la théorie du corps de classes local et dont la restriction à $K_{nr}^\times$ est $\mathrm{Frob}^{v(\alpha)}$. On en déduit que si $\xi \in H^1(G_K/I_K, \mathbb{Q}/\mathbb{Z})$, on a

$$\mathrm{inv}(\delta(\alpha) \cup \xi) = v(\alpha)\xi(\mathrm{Frob}).$$

Notons ev l'évaluation en Frob. Le diagramme

$$\begin{array}{ccccc}
H^1(G_K, \mu_M) & \otimes & H^1(G_K, \mathbb{Z}/M\mathbb{Z}) & \to & H^2(G_K, \mu_M) \\
\downarrow r_0 & & \uparrow & & \downarrow r_1 \\
H^0(G_K/I_K, H^1(I_K, \mu_M)) & \otimes & H^1(G_K/I_K, \mathbb{Z}/M\mathbb{Z}) & \to & H^1(G_K/I_K, H^1(I_K, \mu_M)) \\
\downarrow \gamma & & \| & & \downarrow \gamma \\
\mathbb{Z}/M\mathbb{Z} & \otimes & H^1(G_K/I_K, \mathbb{Z}/M\mathbb{Z}) & \to & H^1(G_K/I_K, \mathbb{Z}/M\mathbb{Z}) \\
 & & & & \downarrow \mathrm{ev} \\
 & & & & \mathbb{Z}/M\mathbb{Z}
\end{array}$$

est commutatif, étant un cas particulier du diagramme (A.0.6). L'application $\gamma \circ r_0$ est donnée par $\delta(\alpha) \mapsto v(\alpha)$ pour $\alpha \in K$: En effet, le cocycle associé à α est $g \to \delta(\alpha)(g) = \dfrac{g(\sqrt[M]{\alpha})}{\sqrt[M]{\alpha}}$. Si l'on prend $h \in I_K$ et si $\alpha = u.\Pi^{v(\alpha)}$ avec u une unité, on a

$$\delta(\alpha)(h) = \left(\frac{h(\sqrt[M]{\Pi})}{\sqrt[M]{\Pi}} \right)^{v(\alpha)}$$

et $\gamma \circ r_0 \circ \delta(\alpha) = v(\alpha)$. Le cup produit

$$H^0(G_K/I_K, H^1(I_K, \mu_M)) \otimes H^1(G_K/I_K, \mathbb{Z}/M\mathbb{Z}) \to H^1(G_K/I_K, H^1(I_K, \mu_M)) \xrightarrow{\mathrm{ev}} \mathbb{Z}/M\mathbb{Z}$$

est donné par $\beta \otimes \xi \mapsto \gamma(\beta)\xi(\mathrm{Frob})$. On en déduit que

$$\mathrm{ev} \circ \gamma \circ r_1(\delta(\alpha) \cup \xi) = \mathrm{ev}(\gamma \circ r_0 \circ \delta(\alpha) \cup \xi) = \mathrm{ev}(v(\alpha)\xi) = v(\alpha)\xi(\mathrm{Frob})$$

et par la propriété (A.0.7) de l'invariant que $\theta \circ r_1 = \mathrm{inv}$.

Démonstration de la proposition 3.2.8. — Il ne reste plus qu'à calculer explicitement la flèche

$$H^0(G_K/I_K, H^1(I_K, A)) \otimes H^1(G_K/I_K, \hat{A}(1)) \to H^1(G_K/I_K, H^1(I_K, \mu_M)) \to \mathbb{Z}/M\mathbb{Z}$$

pour $A = T/MT$ et $B = \hat{A}(1) = T^*(1)/MT^*(1)$ lorsque I_K agit trivialement sur A et B. Soit $a \in H^1(G_K, A)$ et $b \in H^1(G_K/I_K, B)$. On a

$$< a, \inf(b) >= \mathrm{inv}(a \cup \inf(b)) = \theta \circ r_1(a \cup \inf(b)) = \theta \circ (r_0(a) \cup b) \ .$$

D'où, pour tout $\sigma \in I_K$, $< a, \inf(b) > \zeta_\sigma = [a(\sigma), b(\mathrm{Frob})] = [\mathrm{Ev}_\sigma(a), \mathrm{ev}(b)]$ et le lemme. □

Appendice B.
Système d'Euler-Iwasawa et système d'Euler-Iwasawa de rang 1.

On complète ici les démonstrations de l'existence de systèmes compatibles (Φ_m).

Soit $\mathcal{V}$ une famille d'extensions finies abéliennes d'un corps F_0 (F_0 corps de nombres ou corps p-adique). Si $F \in \mathcal{V}$, on note Δ_F le groupe de Galois de F sur F_0. Soit A un anneau local noetherien régulier complet (ici, $\mathcal{O}[[\Gamma]]$, Λ_ξ ou $\mathcal{O}$). On se donne pour chaque $F \in \mathcal{V}$ un $A[\Delta_F]$-module M_F de type fini. On suppose que

(1) M_F est sans A-torsion;

(2) Pour toute extension $F \subset F'$ d'éléments de $\mathcal{V}$, $M_F = M_{F'}^{\mathrm{Gal}(F'/F)}$.

Posons $M_F^* = \mathrm{Hom}_A(M_F, A) \cong \mathrm{Hom}_{A[\Delta_F]}(M, A[\Delta_F])^\iota$.

LEMME. — *Sous les hypothèses précédentes, la limite projective $M_{\mathcal{V}}^*$ des M_F^* est non nulle et l'application naturelle $M_{\mathcal{V}}^* \to M_F^*$ est surjective pour tout $F \in \mathcal{V}$.*

Démonstration. — Montrons que si $F \subset F'$, $M_{F'}/M_F$ est un A-module sans torsion. En effet, soit $x \in M_{F'}$ tel que $ax \in M_F = M_{F'}^{\mathrm{Gal}(F'/F)}$ avec $a \in A$ non nul. Pour tout $\delta \in \mathrm{Gal}(F'/F)$, on a $a(\delta - 1)x = 0$; comme $M_{F'}$ n'a pas de A-torsion, $(\delta - 1)x = 0$ et $x \in M_F$. On en déduit que $\mathrm{Ext}_A^1(M_{F'}/M_F, A) = 0$ et donc que l'application $M_{F'}^* \to M_F^*$ est surjective. Comme les M_F^* sont compacts, l'application $M_{\mathcal{V}}^* \to M_F^*$ est surjective. □

Comme M_F est un A-module sans torsion, M_F^* est un A-module libre. Soit r son rang et s un entier $\leqslant r$. Les $A[\Delta_F]$-modules $\wedge^s M_F^*$ forment un système projectif. On peut aussi considérer le $\varprojlim_{F \in \mathcal{V}} A[\Delta_F]$-module $\wedge^s M_{\mathcal{V}}^*$ et on a $\wedge^s M_{\mathcal{V}}^* = \varprojlim_{F \in \mathcal{V}} \wedge^s M_F^*$. On déduit de ce qui précède que les applications

naturelles $\wedge^s M_F^* \to \wedge^s M_{F_0}^*$ sont surjectives et qu'il en est de même de l'application $\varprojlim_{F \in \mathcal{V}} \wedge^s M_F^* \to \wedge^s M_{F_0}^*$.

Prenons m un entier premier à p, $\mathcal{V}_{mp}$ l'ensemble des extensions de $\mathbb{Q}(\mu_{mp})$, abéliennes sur $\mathbb{Q}$ et de conducteur $m'mp$ avec m' premier à mp et à $\Sigma(V)$ (ce qui est en bijection avec les extensions abéliennes de $\mathbb{Q}$ de conducteur premier à mp et à $\Sigma(V)$). Soit ξ un caractère de Δ_{mp}. On peut alors appliquer ce qui précède à $M_F = H^1_{\mathrm{br},\{p\}}(F,T)$ ou $M_F = H^1_\infty(F,T)^{(\xi)}$ à condition de vérifier les hypothèses.

LEMME. — *Soit F'/F une extension abélienne finie.*

i) *Si $(V/T)^{G_{F'}} = 0$ et si $V^{G_{F'_v}} = 0$ pour v ramifiée dans F'/F, $H^1_{\mathrm{br},\{p\}}(F,T)$ et $H^1_{\mathrm{br},\{p\}}(F',T)$ sont sans $\mathcal{O}$-torsion et l'application restriction*

$$H^1_{\mathrm{br},\{p\}}(F,T) \to H^1_{\mathrm{br},\{p\}}(F',T)^{\mathrm{Gal}(F'/F)}$$

est un isomorphisme.

ii) *On suppose que $F' \in \mathcal{V}_{mp}$, $F \in \mathcal{V}_{mp}$. Alors, si $H^0(F'(\mu_{p^\infty}),V) = 0$, $H^1_\infty(F,T)$ et $H^1_\infty(F',T)$ sont sans $\mathcal{O}[[\Gamma]]$-torsion et l'application restriction*

$$H^1_\infty(F,T) \to H^1_\infty(F',T)^{\mathrm{Gal}(F'/F)}$$

est un isomorphisme.

Démonstration. — Démontrons (i). Les sous-$\mathcal{O}$-modules de torsion de $H^1_{\mathrm{br},\{p\}}(F,T)$ et de $H^1_{\mathrm{br},\{p\}}(F',T)$ sont respectivement contenus dans $(V/T)^{G_F}$ et dans $(V/T)^{G_{F'}}$. La première assertion est donc claire. Prenons S contenant $\Sigma(V)$, p et les places de $\mathbb{Q}$ ramifiées dans F'. Comme $T^{G_{F'}} = 0$, on a $H^1(G_{S,F},T) \cong H^1(G_{S,F'},T)^{\mathrm{Gal}(F'/F)}$.

Si v est une place de F' ne divisant pas p et non ramifié dans F'/F, on a la suite exacte

$$0 \to H^1(F'_v/F_v, T^{G_{F'_v}}) \to H^1_{\mathrm{br}}(F_v,T) \to H^1_{\mathrm{br}}(F'_v,T)^{\mathrm{Gal}(F'_v/F_v)} \to H^2(F'_v/F_v, T^{G_{F'_v}}).$$

D'où par une chasse au diagramme

$$H^1_{/br}(F_v,T) \cong H^1(F'_v,T)^{\mathrm{Gal}(F'_v/F_v)}/H^1_{\mathrm{br}}(F'_v,T)^{\mathrm{Gal}(F'_v/F_v)} \subset H^1_{/br}(F'_v,T)^{\mathrm{Gal}(F'_v/F_v)}.$$

Si v est ramifié dans F'/F, comme $T^{G_{F'_v}} = 0$, on a une injection de $H^1_{/br}(F_v,T)$ dans $H^1_{/br}(F'_v,T)^{\mathrm{Gal}(F'_v/F_v)}$. Il est facile d'en déduire (chasse

au diagramme) que

$$H^1_{\mathrm{br},\{p\}}(F,T) \cong H^1_{\mathrm{br},\{p\}}(F',T)^{\mathrm{Gal}(F'/F)}.$$

Démontrons maintenant (ii). Le sous-$\mathcal{O}[[\Gamma]]$ module de torsion de $H^1_\infty(F',T)$ est $H^0(F'(\mu_{p^\infty}),T)$. Par hypothèse, il est donc nul. Le fait que l'homomorphisme restriction $H^1_\infty(F,T) \to H^1_\infty(F',T)^{\mathrm{Gal}(F'/F)}$ est un isomorphisme se déduit du fait qu'on a déjà pour tout entier n un isomorphisme

$$H^1(G_{S,F'(\mu_{p^n})},T) \cong H^1(G_{S,F(\mu_{p^n})},T)^{\mathrm{Gal}(F'/F)}$$

car $H^0(F'(\mu_{p^n}),T) = 0$. □

Remarques. — i) Le fait que $H^1_\infty(F,T) \to H^1_\infty(F',T)^{\mathrm{Gal}(F'/F)}$ est un isomorphisme est vrai même sans l'hypothèse que $V^{G_{F(\mu_{p^\infty})}} = 0$. En effet, on se ramène au cas où F'/F est cyclique. On a

$$H^1(F'(\mu_{p^n})/F(\mu_{p^n}),T^{G_{F'(\mu_{p^n})}}) \subset T^{G_{F'(\mu_{p^n})}}/(\delta-1)T^{G_{F'(\mu_{p^n})}}$$

où δ est un générateur de $\mathrm{Gal}(F'/F)$. Les $T^{G_{F'(\mu_{p^n})}}$ forment une suite de sous-$\mathcal{O}$-modules de type fini de T qui est donc stationnaire et leur limite projective pour la corestriction est nulle. De même, le conoyau est contenu dans la limite projective des $H^2(F'(\mu_{p^n})/F(\mu_{p^n}),T^{G_{F'(\mu_{p^n})}})$ qui est nulle (ces groupes sont des quotients de $T^{G_{F(\mu_{p^n})}}$).

ii) On a le même genre de résultats pour la famille des $Z^1_\infty(F,T)$ pour F parcourant les extensions finies abéliennes de $\mathbb{Q}_p$ non ramifiées en p. Si $V^{G_{F'(\mu_{p^\infty})}} = 0$, $Z^1_\infty(F,T)$ et $Z^1_\infty(F',T)$ sont sans $\mathcal{O}[[\Gamma]]$-torsion et l'homomorphisme restriction

$$Z^1_\infty(F,T) \to Z^1_\infty(F',T)^{\mathrm{Gal}(F'/F)}$$

est un isomorphisme.

Supposons désormais que V est une représentation irréductible non abélienne (on a donc $V^{G_{\mathbb{Q}^{\mathrm{ab}}}} = 0$, il suffit de supposer que V est de dimension > 1). Les hypothèses du premier lemme de l'appendice sont alors vérifiées pour $\mathcal{V} = \mathcal{V}_{mp}$ et pour $M_F = H^1_\infty(F,T)^{(\xi)}$. Rappelons que le Λ_ξ-module $H^1_\infty(\mathbb{Q}(\mu_m,T)^{(\xi)}$ est un Λ_ξ-module de rang supérieur ou égal à $d_{-\epsilon(\xi)}$. On obtient alors que (pour $d_{-\epsilon(\xi)} > 1$), pour tout élément $\Phi_{m,\xi} \in \wedge^{d_{-\epsilon(\xi)}-1}(H^1_\infty(\mathbb{Q}(\mu_m,T)^{(\xi)})^*$, il existe un système compatible $(\Phi_{mm',\xi})_{m'm}$ (pour m' premier à mp) d'éléments

$$\Phi_{mm',\xi} \in \wedge^{d_{-\epsilon(\xi)}-1}(H^1_\infty(\mathbb{Q}(\mu_{mm'},T)^{(\xi)})^*.$$

PROPOSITION. — *Supposons que V est une représentation irréductible $\mathcal{E}$-adique de $G_{\mathbb{Q}}$, non ramifiée en dehors d'un nombre fini de places et vérifiant la condition* (Tech). *Supposons qu'il existe un système d'Euler-Iwasawa p-adique c_p relatif à V non nul. Soit m un entier fortement admissible premier à p et ξ un caractère de Δ_{mp} tels que $c_{p,\xi}(m)$ soit un élément non nul de $\wedge^{d_{-\epsilon(\chi)}} H^1_\infty(\mathbb{Q}(\mu_m),T)^{(\xi)}$. Alors,* Leop$(V,\xi)$ *est vraie et il existe un entier μ tel que f_ξ divise $p^\mu \mathcal{F}_\xi(c_p)$.*

Démonstration. — Si M est un Λ_ξ module sans torsion de rang r, on le plonge dans un module libre avec conoyau fini, par exemple M^{**}. Les Λ_ξ-modules $\det(M)$ et $\det(M^{**})$ sont alors égaux et libres de rang 1. Soit N un sous-module de $\det(M)$ tel que $\det(M)/N$ soit de torsion. Si $e_1,\dots,e_r$ est une base de M^{**}, on a $N = \Lambda_\xi \mathcal{F} e_1 \wedge \dots \wedge e_r$. Il est alors clair que si $\Phi = e_1 \wedge \dots \wedge e_{r-1}$, $\Phi(\mathcal{F}e_1 \wedge \dots \wedge e_r) = \pm \mathcal{F} e_r$.

Ainsi, il existe un élément $\Phi_{m,\xi}$ de $\wedge^{d_{-\epsilon(\xi)}-1}(H^1_\infty(\mathbb{Q}(\mu_m),T)^{(\xi)})^*$ tel que

$$\Phi_{m,\xi}(c_{p,\xi}(m)) \neq 0$$

et on a $\mathcal{F}_\xi(c_p) = \mathcal{F}_\xi(\Phi_{m,\xi}(c_p))$ (on peut supposer $d_{-\epsilon(\xi)} > 1$). On choisit un système compatible $(\Phi_{mm',\xi})_{mm'}$ pour m' premier à mp redonnant $\Phi_{m,\xi}$ pour $m' = 1$. On peut alors appliquer le théorème 5.2.1 au système d'Euler-Iwasawa p-adique $\Phi_\xi(c_p) = (\Phi_{mm',\xi}(c_{p,\xi}(mm')))_{mm'}$ de rang 1. Le Λ_ξ-module $H^1_\infty(\mathbb{Q}(\mu_m),T)^{(\xi)}$ est donc de rang $d_{-\epsilon(\xi)}$. On applique alors le théorème 1.3.3. □

Appendice C.
Étude complémentaire des $H^1(F(p)/F, T/pT)$.

Il s'agit de donner quelques informations supplémentaires sur la constante s_F intervenant dans le texte et des conditions suffisantes pour que s_F soit égal à 1. Le calcul et l'étude de la nullité des groupes $H^i(F(p)/F, T/pT)$ pour certaines $\mathbb{F}_p$-représentations se trouve dans [CPS]. On note $\bar{V}$ une $\mathbb{F}_p$-représentation de G_F et $F(\bar{V}) = F(p)$ le corps de définition de $\bar{V}$. Le cas qui nous intéresse est bien sûr $\bar{V} = T/pT$.

C.1. Dans [No87], Nori démontre qu'en général ces groupes sont nuls. Plus précisément, il existe des constantes $c_3(d)$ pour d entier tel que si $p > c_3(d)$ et si $\bar{V}$ est une $\mathbb{F}_p$-représentation linéaire de dimension d d'un groupe profini, $H^i(F(\bar{V})/F, \bar{V})$ est nul pour $i = 1, 2$. Ainsi, à dimension

fixée, la condition

$$H^1(F(\bar{V})/F, \bar{V}) = 0$$

est vérifiée pour tout nombre premier p sauf un nombre fini.

C.2. LEMME. — *S'il existe dans le centre de* $\mathrm{Gal}(F(\bar{V})/F)$ *un élément non trivial n'ayant pas de point fixes dans* $\bar{V}$, *les* $H^i(F(\bar{V})/F, \bar{V})$ *pour* $i = 1, 2$ *sont nuls.*

En parallèle (et en reprenant les notations du texte principal), on a le lemme :

LEMME. — *On suppose qu'il existe dans le centre de* $G_F(T)$ *un élément non trivial n'ayant pas de point fixes dans* T/pT. *Alors les* $H^i(F(M)/F, T/MT)$ *pour* $i = 1, 2$ *sont nuls.*

Démonstration. — Soit α un élément comme dans le lemme. Comme $\bar{V}^{\alpha=1} = 0$, les $(T/MT)^{\alpha=1}$ sont nuls. Si Z_α est l'image du groupe engendré par α dans $\mathrm{Gal}(F(M)/F) \subset GL(T/MT)$, Z_α est dans le centre de $\mathrm{Gal}(F(M)/F)$. Les $(T/MT)^{Z_\alpha} = (T/MT)^{\alpha=1}$ étant nuls, les $H^i(Z_\alpha, T/MT)$ sont d'ordre borné par rapport à M et même nuls car Z_α est cyclique et agit sur T/MT par homothéties. On utilise alors la suite spectrale de Hochschild-Serre pour obtenir les isomorphismes

$$H^i(\mathrm{Gal}(F(M)/F)/Z_\alpha, (T/MT)^{Z_\alpha}) \cong H^i(F(M)/F, T/MT).$$

Ainsi, les $H^i(F(M)/F, T/MT)$ sont nuls. □

Par exemple, si les valeurs propres de α sont des racines de l'unité d'ordre premier à p, les $H^i(F(M)/F, T/MT)$ sont tous nuls. On obtient d'autre part les corollaires suivants.

C.3. COROLLAIRE. — *Si* $\bar{V}$ *est irréductible et s'il existe une homothétie non triviale dans* $\mathrm{Gal}(F(\bar{V})/F)$, $H^1(F(\bar{V})/F, \bar{V}) = 0$.

Par exemple, supposons que

(1) V est une représentation irréductible, pure de poids w;

(2) $w(\mathbb{F}_p^\times)$ appartient à l'image de G_F dans $GL(T/pT)$ et est non nul;

(3) T/pT est irréductible.

Alors, $H^1(F(p)/F, T/pT) = 0$ et $H^1(F(M)/F, T/MT) = 0$.

C.4. *Exemple.* — Prenons pour V la représentation p-adique associée à une courbe elliptique. On a $w = -1$ et $d = 2$. Dès que l'image de G_F contient un élément non trivial de $(\mathbb{Z}/p\mathbb{Z})^\times$, les $H^i(F_n(E_M)/F_n, E_M)$ sont

nuls. En effet, il suffit de montrer que cet élément est aussi contenu dans l'image de G_{F_n}. Mais le déterminant de V est isomorphe à $\mathbb{Z}_p(1)$. Donc si $g \in G_F$, on a $\det(g) = \chi(g)$ et g laisse stable F_∞ si et seulement si $\det(g) \in \mu_{p-1}$, c'est-à-dire $\det(g)^{p-1} = 1$, ce qui est le cas si g appartient à l'image de $(\mathbb{Z}/p\mathbb{Z})^\times$. Par exemple, si -1 appartient à l'image de G_F dans $GL(T)$, $H^i(F_n(E_M)/F_n, E_M) = 0$.

C.5. La nullité de $H^1(F(M)/F, T/MT) = 0$ pour une puissance M de p implique celle de $H^1(F(p)/F, T/pT)$. Réciproquement, supposons T/pT irréductible et

$$H^1(F(p)/F, T/pT) = 0.$$

Supposons de plus l'application

$$\text{(C.5.1)} \quad \mathrm{Hom}(\mathrm{Gal}(F(M)/F(p)), T/pT)^{\mathrm{Gal}(F(p)/F)} \to H^2(F(p)/F, T/pT)$$

injective. Alors les $H^1(F(M)/F, T/MT)$ sont tous nuls. En effet, on déduit de l'injectivité de (C.5.1) et de la suite exacte inflation-restriction que

$$H^1(F(p)/F, T/pT) \cong H^1(F(M)/F, T/pT)$$

et donc que $H^1(F(M)/F, T/pT) = 0$. On démontre ensuite par récurrence sur $M'|M$ que $H^1(F(M)/F, T/M'T) = 0$ en utilisant la suite exacte

$$H^1(F(M)/F, pT/M'T) \to H^1(F(M)/F, T/M'T) \to H^1(F(M)/F, T/pT).$$

Revenons à l'injectivité de (C.5.1). Il est clair que si T/pT est disjointe de la représentation adjointe de G_F sur $\mathcal{G}/p\mathcal{G}$, $\mathrm{Hom}(\mathrm{Gal}(F(M)/F(p)), T/pT)^{\mathrm{Gal}(F(p)/F)} = \mathrm{Hom}(\mathcal{G}/p\mathcal{G}, T/pT)^{\mathrm{Gal}(F(p)/F)} = 0$ et (C.5.1) est bien sûr injective. Montrons que si T/pT et $\mathcal{G}/p\mathcal{G}$ sont irréductibles et isomorphes et si $\mathrm{Gal}(F(p^2)/F)$ n'est pas un produit semi-direct de $\mathrm{Gal}(F(p)/F)$ par $\mathcal{G}/p\mathcal{G}$, (C.5.1) est injective. Un élément de $\mathrm{Hom}(\mathcal{G}/p\mathcal{G}, T/pT)^{\mathrm{Gal}(F(p)/F)}$ est soit nul, soit un isomorphisme. L'application (C.5.1) se décrit de la manière suivante : soit c la classe de l'extension de groupes de $\mathrm{Gal}(F(p)/F)$ par $\mathcal{G}/p\mathcal{G}$ donée par $\mathrm{Gal}(F(p^2)/F)$. Par hypothèse, $c \neq 0$. Si $f \in \mathrm{Hom}(\mathcal{G}/p\mathcal{G}, T/pT)^{\mathrm{Gal}(F(p)/F)}$, l'image de f dans $H^2(F(p)/F, T/pT)$ est $f^*(c)$. Ainsi, si f est non nul, c'est un isomorphisme et $f^*(c)$ est non nul.

Exemple. — Soit U une représentation $\mathbb{Z}_p$-adique de rang 2 de déterminant χ et $T = sl_2(U)$ la sous-représentation de la représentation adjointe de U formée de éléments de trace nulle (cf. [Fl92]). Supposons de plus que $G_F \to GL(U)$ est surjective; on a alors $G_F(T) \cong PGL(U)$ et T/pT est irréductible. L'extension $PGL(\mathbb{Z}/p^2\mathbb{Z})$ de $PGL(\mathbb{F}_p)$ par $\mathcal{G}/p\mathcal{G} =$

$(1+p\mathrm{End}(U))/(1+p\mathbb{F}_p)$ est non scindée et $\mathcal{G}/p\mathcal{G}$ est isomorphe à $T/pT = sl(U/pU)$ comme représentation de $PGL(U/pU)$ par l'isomorphisme induit par $1+pa \mapsto a - \frac{1}{2}\mathrm{tr}(a)$ (au moins si $p \neq 2$). Les $H^1(F(M)/F, T/MT)$ sont donc nuls si $H^1(F(p)/F, T/pT)$ l'est. Montrons comme dans [Fl92, Lemma 1.2] que $H^1(F(p)/F, T/pT) = H^1(PGL_2(\mathbb{F}_p), sl(T/pT)) = 0$. On montre même que

$$H^1(GL_2(\mathbb{F}_p), sl(T/pT)) = 0,$$

ce qui impliquera de la même manière que précédemment que $H^1(F'(M)/F, T/MT) = 0$ avec $F'(M) = F(M)(\mu_M)$. Soit $\mathfrak{U}$ le sous-groupe de $GL(T) \cong GL_2(\mathbb{F}_p)$ formé des matrices $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$; c'est un p-groupe de Sylow de $GL_2(\mathbb{F}_p)$ et $H^1(GL_2(\mathbb{F}_p), T/pT)$ est le sous-groupe de $H^1(\mathfrak{U}, T/pT)$ formé des éléments invariants par $GL_2(\mathbb{F}_p)$, ($x \in H^1(\mathfrak{U}, T/pT)$ est invariant par $GL_2(\mathbb{F}_p)$ si et seulement si pour tout $g \in GL_2(\mathbb{F}_p)$ tel que $g\mathfrak{U}g^{-1} \cap \mathfrak{U} \neq 1$, les restrictions de x et de $g(x)$ à $g\mathfrak{U}g^{-1} \cap \mathfrak{U}$ sont égales). Comme $\mathfrak{U}$ est cyclique, il est facile de calculer explicitement $H^1(\mathfrak{U}, sl_2(\mathbb{F}_p))$ et on trouve que c'est le groupe des matrices de la forme $\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$. Soit $g = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ une matrice diagonale. Elle normalise $\mathfrak{U}$ et on a $g \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} g^{-1} = \begin{pmatrix} 0 & 0 \\ \lambda^{-1}\mu c & 0 \end{pmatrix}$. Il n'y a donc pas d'éléments non nuls de $H^1(\mathfrak{U}, sl_2(\mathbb{F}_p))$ invariants par $GL_2(\mathbb{F}_p)$. Remarquons que, contrairement à ce qui est écrit dans [Fl92, Lemma 1.2], les $H^1(GL_2(\mathbb{Z}_p/p^n\mathbb{Z}_p), M_2(\mathbb{Z}/p^n\mathbb{Z}))$ ne sont pas nuls. En effet, il suffit de montrer la non nullité de $H^1(GL_2(\mathbb{Z}_p/p^n\mathbb{Z}_p), \mathbb{Z}/p^n\mathbb{Z}) = \mathrm{Hom}(GL_2(\mathbb{Z}_p/p^n\mathbb{Z}_p), \mathbb{Z}/p^n\mathbb{Z})$ et $x \mapsto p^{n-2} < \det(x) > -1) \bmod p^n\mathbb{Z}_p$ en est un élément non nul.

Appendice D.

LEMME. — *Soit V une représentation irréductible $\mathcal{E}$-adique de G_F. On suppose que l'image de G_F dans $GL(V)$ contient un élément f tel que $V^{f=1}$ soit de dimension 1. Alors, V est absolument irréductible.*

Démonstration. — Notons G l'image de G_F dans $GL(V)$. Soit $h \in \mathrm{End}_{G_F}(V)$. Soit e_1 un vecteur propre de f de valeur propre 1. Comme $h \in GL(V)$ commute avec f, $h(e_1) \in V^{f=1}$ et est donc proportionnel à e_1. D'autre part, si g appartient à $GL(V)$, $V^{gfg^{-1}=1}$ est de dimension 1 et admet comme base $g(e_1)$. En particulier, si $g \in G$, h commute avec gfg^{-1},

et $h(ge_1)$ est proportionnel à $g(e_1)$. Ainsi, pour tout $g \in G$, $h(ge_1) = \lambda_g ge_1$ avec $\lambda_g \in \mathbb{Q}_p$. On déduit alors de $hgf = gfh$ que

$$hgf(e_1) = hg(e_1) = \lambda_g ge_1 = gfh(e_1) = \lambda_1 ge_1$$

et donc que λ_g est indépendant de g. Ainsi, h est une homothétie sur le $\mathcal{E}[G_F]$-module engendré par e_1. Comme V est irréductible, h est une homothétie sur V. On a donc montré que $\mathrm{End}_{G_F} V = \mathcal{E}$ et donc que V est absolument irréductible. □

On démontre de même le lemme suivant :

LEMME. — *Soit V une représentation irréductible de G_F. Soit L une extension galoisienne finie de F. On suppose que l'image de G_L dans $GL(V)$ contient un élément f tel que $V^{f=1}$ soit de dimension 1. Alors, V est absolument irréductible et la restriction de V à G_L est somme directe de représentations absolument irréductibles.*

BIBLIOGRAPHIE

[Bo80] F. BOGOMOLOV, Sur l'algébricité des représentations l-adiques, C.R. Acad. Sc., Paris, 290 (1980), 701-703.

[Bo] BOURBAKI, Algèbre.

[CE56] H. CARTAN et S. EILENBERG, Homological Algebra, Princeton Math. Series 19 (1956), Princeton.

[ChE48] C. CHEVALLEY et S. EILENBERG, Cohomology theory of Lie groups and Lie algebras, Trans. Amer. Math. Soc., 63 (1948), 85-124.

[CPS] E. CLINE, B. PARSHALL et L. SCOTT, Cohomology of finite groups of Lie type I, Publ. Math. IHES, 45 (1975), 169-191.

[Fl92] M. FLACH, A finiteness theorem for the symmetric square of an elliptic curve, Invent. Math., 109 (1992), 307–327.

[FP-R94] J.-M. FONTAINE et B. PERRIN-RIOU, Autour des conjectures de Bloch et Kato : cohomologie galoisienne et valeurs de fonctions L, dans Motives (Seattle) Proceedings of Symposia in Pure Mathematics, vol. 55, part 1 (1994), pp. 599-706.

[He81] G. HENNIART, Représentations l-adiques abéliennes, Séminaire de théorie des nombres 1980-81, Birkhäuser, 107-126.

[HS] HOCHSCHILD et J.-P. SERRE, Cohomology of groups extensions, Trans. Am. Math. Soc., 74 (1953), 110-134.

[Ka] K. KATO, Euler systems, Iwasawa theory and Selmer groups, prépublication (1995).

[Ka ?] K. KATO, Iwasawa theory of modular forms, en préparation.

[Ko90] V.A. KOLYVAGIN, Euler systems, The Grothendieck Festschrift, vol. 2, Prog. in Math. 87, Birkhäuser, Boston, 1990, pp. 436–483.

[L65] M. LAZARD, Groupes analytiques p-adiques, Publ. Math. IHES, 26 (1965), 1-219.

[No87] M. V. NORI, On subgroups of $GL_n(\mathbb{F}_p)$, Invent. Math., 88 (1987), 257-275.

[Ne92] J. NEKOVÁŘ, Kolyvagin's method for Chow groups of Kuga-Sato varieties, Invent. Math., 107 (1992), 99-125.

[P-R92] B. PERRIN-RIOU, Théorie d'Iwasawa et hauteurs p-adiques, Invent. Math., 109 (1992), 137-185.

[P-R94] B. PERRIN-RIOU, Théorie d'Iwasawa des représentations p-adiques sur un corps local, Invent. Math., 115 (1994), 81-149.

[P-R95] B. PERRIN-RIOU, Fonctions L p-adiques des représentations p-adiques, Astérisque, 229, (1995).

[P-R96] B. PERRIN-RIOU, Systèmes d'Euler p-adiques et théorie d'Iwasawa, Prépublications d'Orsay 96-04 (1996).

[Re] C. REINER, Maximal orders

[Ri79] K. RIBET, Kummer theory on extensions of abelian varieties by tori, Duke Math. J., 46 (1979), 745-761.

[Ru88] K. RUBIN, On the main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. Math., 93 (1988), 701-719 .

[Ru90] K. RUBIN, The main conjecture, Appendix to Cyclotomic fields (seconde édition) par S. Lang, Graduate Texts in Math. 121, Springer-Verlag (1990).

[Ru91] K RUBIN, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math., 103 (1991), 25-68.

[Ru92] K. RUBIN, Stark's units and Kolyvagin's "Euler systems", J. reine angew. Math., 425 (1992), 141-154.

[R] K. RUBIN, A Stark conjecture "over $\mathbb{Z}$" for abelian L-functions with multiple zeros, prépublication.

[S64] J.-P. SERRE, Sur les groupes de congruence des variétés, Izv. Akad. Nauk. SSSR 28 (1964), 3-18; II : 35 (1971), 731-735.

[S67] J.-P. SERRE, Sur les groupes de Galois attachés aux groupes p-divisibles, Proc. of a conference on local fields, Nuffic Summer School at Driebergen, Springer, Berlin (1967), pp. 118–131.

[S76] J.-P. SERRE, Représentations l-adiques, Algebraic Number Theory, Int. Symp. Kyoto (1976), 177-193.

[S94] J.-P. SERRE, Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques, dans Motives (Seattle) Proceedings of Symposia in Pure Mathematics, vol. 55, part 1 (1994), pp. 377-400.

[So92] D. SOLOMON, On a construction of p-units in abelian fields, Ivent. Math., 109 (1992), 329-350.

[T76] J. TATE, Relations between K_2 and Galois cohomology, Invent. Math., 36 (1976), 257-274.

Manuscrit reçu le 23 mars 1998,
accepté le 6 mai 1998.

Bernadette PERRIN-RIOU,
Université Paris-Sud
Mathématiques
Bâtiment 425
F-91405 Orsay Cedex (France).