BULLETIN DE LA S. M. F.

BERNADETTE PERRIN-RIOU

Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner

Bulletin de la S. M. F., tome 115 (1987), p. 399-456

<http://www.numdam.org/item?id=BSMF_1987__115__399_0>

Bull. Soc. math. France,
115, 1987, p. 399-456.

FONCTIONS L p-ADIQUES, THÉORIE D'IWASAWA ET POINTS DE HEEGNER

PAR

BERNADETTE PERRIN-RIOU (*)

RÉSUMÉ. — On interprète (en partie conjecturalement) en termes de modules d'Iwasawa et de leurs séries caractéristiques le lien existant entre points de Heegner et dérivées de fonctions L. En appendice, on étudie la variation par isogénie de la fonction L p-adique algébrique.

ABSTRACT. — We give (at least conjecturally) the relation between Heegner points and derivatives of L functions in terms of Iwasawa modules and characteristic series. In the appendix, we study the variation by isogeny of the algebraic p-adic L function.

Soit E une courbe elliptique définie sur $\mathbb{Q}$ et k un corps quadratique imaginaire. Dans le cas où E est modulaire et sous certaines hypothèses sur le conducteur de E, Heegner a construit des points de E rationnels sur k. Dans le cas où $E(k)$ est de rang 1, Birch et Stephens ont observé que l'indice des points de Heegner dans $E(k)$ est essentiellement la racine carrée du cardinal du groupe de Tate-Shafarevitch. Ce fait empirique se déduit maintenant de la conjecture de Birch et Swinnerton-Dyer grâce au théorème de Gross et Zagier. Nous cherchons ici à donner une explication de ce fait en termes de théorie d'Iwasawa, ce qui fait apparaître de manière déterminante la $\mathbb{Z}_p$-extension de k qui est diédrale sur $\mathbb{Q}$.

Dans un premier paragraphe, nous énoncerons nos conjectures et les théorèmes montrés dans le reste du texte. Dans le second paragraphe, nous appliquerons les idées de [9] à l'étude de la fonction L p-adique algébrique au voisinage d'une $\mathbb{Z}_p$-extension où elle est nulle. Dans le troisième paragraphe, indépendant du précédent, nous construirons un module d'Iwasawa associé aux points de Heegner et qui intervient dans

(*) Texte reçu le 30 avril 1986

Bernadette PERRIN-RIOU, L.M.F., U.E.R. n° 48, Université Pierre-et-Marie-Curie, 4, place Jussieu, 75230 Paris Cedex 05, France

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE - 0037-9484/1987/04 399 58 $7.80

les conjectures et nous montrerons en particulier qu'il est soit nul, soit libre de rang 1 sur l'algèbre d'Iwasawa de l'extension diédrale de k. Enfin, dans le dernier paragraphe, nous complèterons les démonstrations des énoncés du paragraphe 1. Auparavant, nous avons réuni dans un paragraphe 0 un certain nombre de définitions et notations. Dans l'appendice, nous étudierons la variation de la fonction L p-adique algébrique par isogénie.

L'idée de la construction du module d'Iwasawa associé aux points de Heggner revient à B. Mazur (cours à Harvard en 1982-1983), [8]). Je tiens d'autre part à remercier J. Coates pour son constant encouragement.

PLAN

0. *Quelques notations et définitions.*
1. *Énoncé des résultats et conjectures.*
2. *Théorie d'Iwasawa.*
   2.1. Situation étudiée.
   2.2. Λ-modules, normes universelles, groupes de Selmer.
   2.3. Hauteurs p-adiques attachées à un caractère de $G(\bar{F}/D_\infty)$.
   2.4. Groupes de Selmer et séries caractéristiques.
   2.5. Conséquence sur le module de torsion de $\widehat{S_p(D_\infty)}$.
   2.6. Cas où la courbe E est définie sur $\mathbf{Q}$.
3. *Points de Heegner et $\mathbf{Z}_p$-extensions.*
   3.1. Généralités
   3.2. $\mathbf{Z}_p$-extensions et corps de classes.
   3.3. Points de Heegner relatifs à la $\mathbf{Z}_p$-extension D_∞/k.
   3.4. Modules d'Iwasawa associés aux points de Heegner.
4. *Fin des démonstrations.*

Appendice. Variation de la fonction L p-adique algébrique par isogénie.

0. Quelques notations et définitions

Si G est un $\mathbf{Z}_p$-module, on note Λ_G son algèbre de groupe

$$\Lambda_G = \mathbf{Z}_p[[G]] = \varprojlim \mathbf{Z}_p[G/U]$$

où la limite projective est prise sur les sous-groupes ouverts U de G. Si M est un Λ_G-module, on note M^G (resp. M_G) le plus grand sous-$\mathbf{Z}_p$-module (resp. $\mathbf{Z}_p$-module quotient) de M sur lequel G agit trivialement. Le dual

de Pontryagin de M est noté $\hat{M}$:

$$\hat{M} = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p).$$

Enfin, on notera $\dot{M}$ le Λ_G-module dont le $\mathbb{Z}_p$-module sous-jacent est celui de M et tel que l'action de G soit

$$g.m = g^{-1}m.$$

Il existe un $\mathbb{Z}_p$-homomorphisme naturel de Λ_G dans l'espace des fonctions définies sur les caractères de G (à valeurs dans $\mathbb{Z}_p^\times$) et à valeurs dans $\mathbb{Z}_p$ prolongeant

$$g \in G \mapsto (\varphi \mapsto \varphi(g)).$$

L'image de Λ_G est l'algèbre d'Iwasawa $\mathrm{Iw}(G)$ de G sur $\mathbb{Z}_p$. Si G est isomorphe à $\mathbb{Z}_p^r$, Λ_G et $\mathrm{Iw}(G)$ sont isomorphes. Lorsque G est le groupe de Galois d'une extension L/F, on notera

$$\Lambda_{L/F} = \Lambda_{G(L/F)}$$
$$\mathrm{Iw}(L/F) = \mathrm{Iw}(G(L/F)).$$

Soit F un corps de nombres. Si v est une place de F, le complété de F en v est noté F_v, le corps résiduel de F_v est noté $\tilde{F}_v$. Si L est une extension (finie ou non) de F, on désigne par L_v la réunion des complétions des F'_v pour F' extension finie de F contenue dans L.

Soit E une courbe elliptique définie sur F. Si v est une place de F où E a bonne réduction, on note par $\tilde{E}_v$ la courbe réduite de E modulo v.

Finalement, définissons les groupes de Selmer. Le groupe de Selmer de E/L relatif à p^n est défini comme le noyau des homomorphismes de restriction

$$0 \to S(L)^{(p^n)} \to H^1(L, E_{p^n}) \to \prod_v H^1(L_v, E).$$

On définit de même le groupe de Selmer $S_p(L)$ de E/L relatif à p^∞ :

$$0 \to S_p(L) \to H^1(L, E_{p^\infty}) \to \prod_v H^1(L_v, E).$$

On définit à partir de ces groupes de Selmer des $\mathbb{Z}_p$-modules compacts : si L est une extension finie de F, notons $\check{S}_p(L)$ la limite projective des groupes de Selmer $S(L)^{(p^n)}$, les homomorphismes de transition étant induits

par la multiplication par p. Si L est une extension de F, notons $\tilde{S}_p(L)$ la limite projective des $\check{S}_p(F')$ où F' parcourt les sous-extensions finies de L/F et où les homomorphismes de transition sont induits par la corestriction (norme). Ce dernier $\mathbb{Z}_p$-module sera essentiel ici.

Si L/F est une extension finie de corps, on notera $\mathrm{tr}_{L/F}$ la trace de L/F.

Enfin, si a et b sont deux éléments non nuls d'un anneau tels que $a=ub$ avec u unité, on écrira $a \sim b$. On utilisera la même notation pour désigner un quasi-isomorphisme (c'est-à-dire à noyau et conoyau finis).

1. Enoncé des résultats et conjectures

Soit k un corps quadratique imaginaire et p un nombre premier impair. Il existe une unique extension k_∞ de k dont le groupe de Galois est topologiquement isomorphe à $\mathbb{Z}_p^2$. L'action de l'automorphisme non trivial τ de $G(k/\mathbb{Q})$ sur le groupe de Galois de k_∞/k décompose ce groupe en somme de deux sous-espaces propres pour les valeurs propres $+1$ et -1 et met donc en évidence deux $\mathbb{Z}_p$-extensions particulières : la $\mathbb{Z}_p$-extension cyclotomique C_∞ de k et la $\mathbb{Z}_p$-extension diédrale D_∞; cette dernière peut être définie comme l'unique $\mathbb{Z}_p$-extension de k galoisienne sur $\mathbb{Q}$ et dont le groupe de Galois sur $\mathbb{Q}$ est pro-p-diédrale.

D'autre part, soit E une courbe elliptique définie sur $\mathbb{Q}$ ayant bonne réduction ordinaire en p. Soit $S_p(k_\infty)$ le groupe de Selmer de E sur k_∞ relatif à p^∞. Son dual de Pontryagin $\widehat{S_p(k_\infty)}$ est un $\Lambda_{k_\infty/\mathbb{Q}}$-module de type fini compact. Considérons les deux hypothèses suivantes :

HYPOTHÈSE (*). — *Le $\Lambda_{k_\infty/k}$-module $\widehat{S_p(k_\infty)}$ est de torsion.*

HYPOTHÈSE (**) *Pour toute extension finie k' de k contenue dans k_∞, le $\Lambda_{k'C_\infty/k'}$-module $\widehat{S_p(k'C_\infty)}$ est de torsion.*

L'hypothèse (**) implique l'hypothèse (*). Nous ne ferons pour l'instant que l'hypothèse (*) qui est fondamentale. Nous aurons besoin de l'hypothèse (**) un peu plus tard. Remarquons qu'il est montré que si la hauteur p-adique relative à l'extension cyclotomique est non dégénérée sur $\check{S}_p(k)$, le $\Lambda_{C_\infty/k}$-module $\widehat{S_p(C_\infty)}$ est de torsion.

Nous sommes intéressés ici par la série caractéristique $\mathscr{L}_p(E/k_\infty)$ de $\widehat{S_p(k_\infty)}$ en tant que $\Lambda_{k_\infty/k}$-module. C'est une fonction d'Iwasawa sur le

$\mathbb{Z}_p$-module $\Delta(k_\infty/k)$ des caractères continus de $\Theta = G(k_\infty/k)$ à valeurs dans $\mathbb{Z}_p^\times$; elle n'est définie qu'à une unité près. La restriction de $\mathscr{L}_p(E/k_\infty)$ à $\Delta(D_\infty/k)$ est la série caractéristique de $\widehat{S_p(D_\infty)}$ en tant que $\Lambda_{D_\infty/k}$-module (paragraphe 2). De plus, au moins dans le cas où E a multiplication complexe par un corps quadratique imaginaire et sous l'hypothèse (**) (mais cela reste certainement vrai dans le cas général), $\mathscr{L}_p(E/k_\infty)$ vérifie une équation fonctionnelle au sens suivant. Soit ν (resp. ρ) un caractère cyclotomique (resp. diédral) c'est-à-dire dont le noyau est $G(k_\infty/C_\infty)$ (resp. $G(k_\infty/D_\infty)$) et soit ι l'involution de $\mathrm{Iw}(k_\infty/k)$ défini par

$$f^\iota(\nu^a \rho^b) = f(\nu^{-a} \rho^b).$$

Alors, il existe un représentant $\mathscr{L}_p(E/k_\infty)$ de la série caractéristique vérifiant

$$\mathscr{L}_p(E/k_\infty)^\iota = \varepsilon_p \mathscr{L}_p(E/k_\infty)$$

avec $\varepsilon_p = \pm 1$. En particulier, si $\varepsilon_p = -1$, la restriction de $\mathscr{L}_p(E/k_\infty)$ à $\Delta(D_\infty/k)$ est nulle et $\widehat{S_p(D_\infty)}$ n'est pas de $\Lambda_{D_\infty/k}$- torsion.

Exemples 1. — On montrera en utilisant les tables de [1] dans le paragraphe 2.6 que :

$$\begin{aligned}
E:\ y^2 = x^3 - x, \qquad & k = \mathbb{Q}(\sqrt{-7}), \qquad \varepsilon_{13} = \varepsilon_{17} = 1 \\
E:\ y^2 = x^3 + x, \qquad & k = \mathbb{Q}(\sqrt{-7}), \qquad \varepsilon_5 = -1 \\
E:\ y^2 = x^3 - x, \qquad & k = \mathbb{Q}(\sqrt{-11}), \qquad \varepsilon_5 = \varepsilon_{13} = \varepsilon_{17} = 1 \\
& k = \mathbb{Q}(\sqrt{-13}), \qquad \varepsilon_5 = \varepsilon_{17} = -1 \\
& k = \mathbb{Q}(\sqrt{-3}), \qquad \varepsilon_5 = \varepsilon_{17} = -1.
\end{aligned}$$

Pour les courbes précédentes, si l'on suppose que le groupe de Shafarevitch-Tate de E sur k est fini, la valeur de ε_p est en fait indépendante de p pour tout nombre premier p ordinaire pour E; d'autre part, toujours pour les exemples précédents, on montrera que $\widehat{S_p(D_\infty)}$ est de rang 0 si $\varepsilon_p = 1$ et de rang 1 si $\varepsilon_p = -1$.

Nous aimerions montrer que, de manière générale, ε_p est en fait égal au signe ε_∞ de l'équation fonctionnelle complexe c'est-à-dire que

$$\varepsilon_p = \varepsilon_\infty = -\varepsilon(N)$$

si N est le conducteur de E et ε le caractère quadratique associé à l'extension quadratique $k/\mathbb{Q}$ (au moins lorsque N ne se ramifie pas dans k).

Revenons à la situation générale. Dans le cas où $S_p(D_\infty)$ n'est pas de $\Lambda_{D_\infty/k}$-torsion, il est intéressant de donner une interprétation de la dérivée de $\mathscr{L}_p(E/k_\infty)$ dans la direction de D_∞. Par un raffinement des méthodes de [9], dans le cas où E est à multiplication complexe, on reliera au paragraphe 3 cette dérivée à la série caractéristique $\mathscr{T}_p(E/D_\infty)$ du $\Lambda_{D_\infty/k}$-module de torsion de $\widehat{S_p(D_\infty)}$. Énonçons le théorème obtenu dans ce cas particulier. Nous définirons une forme bilinéaire sur $\tilde{S}_p(D_\infty)$ à valeurs dans $\mathrm{Iw}(D_\infty/k)$ attachée à tout caractère ν_∞ de $G(k_\infty/D_\infty)$ à valeurs dans $\mathbb{Z}_p$; on la note $\ll\ ,\ \gg_{\nu_\infty,\,p}$.

Plus précisément, soient $\underline{x}=(x_n)$ et $\underline{y}=(y_n)$ deux éléments de $\tilde{S}_p(D_\infty)$ Posons

$$\ll \underline{x},\ \underline{y} \gg_{\nu_\infty,\,p} = \left(\frac{1}{[D_n : k]} \sum_{s,\ t \in G(D_n/k)} \langle sx_n,\ ty_n \rangle_{\nu_n,\,p}\, st^{-1} \right)_n$$

où ν_n est un caractère de $G(k_\infty/D_n)$ dont la restriction à $G(k_\infty/D_\infty)$ est ν_∞ et où $\langle\ ,\ \rangle_{\nu_n,\,p}$ est la hauteur p-adique attachée à E et à ν_n. On vérifie que ceci est bien un élément de $\Lambda_{D_\infty/k}$ et donc de $\mathrm{Iw}(D_\infty/k)$.

THÉORÈME 1. — *Soit r_{D_∞} le rang des normes universelles de $\tilde{S}_p(k)$ dans $\tilde{S}_p(D_\infty)$. Pour tout caractère ρ de $\Delta(k_\infty/k)$ se factorisant par $G(D_\infty/k)$ et pour tout caractère ν de $\Delta(k_\infty/k)$ non trivial sur $G(k_\infty/D_\infty)$,*

(i) *la fonction $\mathscr{L}_p(E/k_\infty)(\nu^s\rho)$ a un zéro de multiplicité supérieure ou égale à r_{D_∞};*

(ii) *ce zéro est de multiplicité exactement r_{D_∞} si et seulement si la forme bilinéaire $\ll\ ,\ \gg_{\nu_\infty,\,p}$ est non dégénérée (ν_∞ est ici la restriction de ν à $G(k_\infty D_\infty)$);*

(iii) *on a dans ce cas*

$$\lim_{s \to 0} \frac{\mathscr{L}_p(E/k_\infty)(\nu^s\rho)}{s^{r_{D_\infty}}} \sim \mathrm{disc}_{\tilde{S}_p(D_\infty)} \ll\ ,\ \gg_{\nu_\infty,\,p}(\rho)\, \mathscr{T}_p(E/D_\infty)(\rho).$$

Supposons maintenant que E est une courbe modulaire de conducteur N c'est-à-dire qu'il existe un morphisme π non trivial de $X_0(N)$ dans E rationnel sur $\mathbb{Q}$. Notons c_E la constante de Manin associée à la paramétrisation π de E (si ω est une forme différentielle de Néron sur la courbe

elliptique E, $\pi^*\omega/2i\pi c_E dz$ est une forme modulaire normalisée). Supposons désormais que N vérifie la condition suivante que l'on appellera *hypothèse de Heegner* :

tout diviseur de N se décompose dans k.

Pour toute sous-extension finie D_n de D_∞/k, on construit des points de Heegner appartenant à $E(D_n)$. Nous construirons à l'aide de ces points un $\Lambda_{D_\infty/k}$-module $\mathbf{H}_\infty$ (dépendant du choix de la paramétrisation π de E) et nous montrerons.

PROPOSITION 2. — *Le $\Lambda_{D_\infty/k}$-module $\mathbf{H}_\infty$ est libre de rang inférieur ou égal à* 1.

Ce $\Lambda_{D_\infty/k}$-module $\mathbf{H}_\infty$ est un sous-module de $\tilde{S}_p(D_\infty)$. Nous construirons deux éléments de $\mathrm{Iw}(D_\infty/k)$ à partir de $\mathbf{H}_\infty$. Le premier, de nature arithmétique, est la série caractéristique $I(\mathbf{H}_\infty)$ du quotient de $\tilde{S}_p(D_\infty)$ par $\mathbf{H}_\infty$ en tant que $\Lambda_{D_\infty/k}$-module; il est non nul si et seulement si $\mathbf{H}_\infty$ et $\tilde{S}_p(D_\infty)$ sont de même rang égal à 1.

Le second élément de $\mathrm{Iw}(D_\infty/k)$, de nature analytique, est construit à l'aide des hauteurs p-adiques associées à E et à un caractère non trivial ν_∞ de $G(k_\infty/D_\infty)$ dans $\mathbb{Z}_p^\times$. Notons

$$\mathrm{disc}_{\mathbf{H}_\infty} \ll\ ,\ \gg_{\nu_\infty,\,p}$$

le discriminant de $\ll\ ,\ \gg_{\nu_\infty,\,p}$ sur le $\Lambda_{D_\infty/k}$-module $\mathbf{H}_\infty$ (défini à une unité près) vu comme élément de $\mathrm{Iw}(D_\infty/k)$.

Nous proposons alors les conjectures suivantes :

CONJECTURE A. — Sous l'hypothèse de Heegner et pour tout élément ρ de $\Delta(k_\infty/k)$ se factorisant par $G(D_\infty/k)$

$$\mathrm{A}_1 \qquad \mathscr{L}_p(E/k_\infty)(\rho)=0$$

$$\mathrm{A}_2 \qquad \lim_{s\to 0}\frac{\mathscr{L}_p(E\,k_\infty)(\rho\nu^s)}{s}\sim\frac{1}{c_E^2u^2}\,\mathrm{disc}_{\mathbf{H}_\infty}\ll\ ,\ \gg_{\nu_\infty,\,p}(\rho)$$

dans l'algèbre d'Iwasawa $\mathrm{Iw}(D_\infty/k)$ pour tout caractère ν de $\Delta(k_\infty/k)$ dont la restriction ν_∞ à $G(k_\infty/D_\infty)$ est non triviale.

($2u$ est le nombre de racines de l'unité de k.)

CONJECTURE B. — Si les $\Lambda_{D_\infty/k}$-modules $\mathbf{H}_\infty$ et $\widehat{S_p(D_\infty)}$ sont de rang 1,

$$\mathscr{T}_p(E/D_\infty)(\rho)\sim I(\mathbf{H}_\infty)(\rho)\,I(\mathbf{H}_\infty)(\rho^{-1})/c_E^2u^2$$

dans $\mathrm{Iw}(D_\infty/k)$.

On peut aussi écrire la conjecture A_2 en utilisant les caractères finis de $G(D_\infty/k)$. Soit $(h_n)_n$ un générateur de $\mathbf{H}_\infty$ (le module $\mathbf{H}_\infty$ est construit comme limite projective de $\mathbb{Z}_p[G(D_n/k)]$-modules $\mathbf{H}_n$). On voit alors facilement que la conjecture A_2 est équivalente à

$$A_2(\chi):\quad \lim_{s\to 0}\frac{\mathscr{L}_p(E/k_\infty)(\chi\nu^s)}{s}\sim\sum_{\gamma\in G(D_n/k)}\bar{\chi}(\gamma)\langle\gamma h_n,\ h_n\rangle_{v_n,\ p}/c_E^2u^2$$

pour tout caractère χ de $G(D_\infty/k)$ d'ordre fini (et se factorisant par $G(D_n/k)$).

Les conjectures A et B sont essentiellement équivalentes. Malheureusement, nous ne montrerons complétement les théorèmes suivants que dans le cas où *E est à multiplication complexe et sous l'hypothèse* (**), bien que nous pensons qu'ils sont vrais dans le cas général (cela car nous maitrisons mal la théorie d'Iwasawa dans le cas sans multiplication complexe).

THÉORÈME 3. — *Si les* $\Lambda_{D_\infty/k}$*-modules* $\mathbf{H}_\infty$ *et* $\widehat{S_p(D_\infty)}$ *sont de rang* 1, *les conjectures* A *et* B *sont équivalentes.*

Examinons d'un peu plus près ces conjectures. Pour montrer que A_1 est vraie, il suffit de montrer que le signe ε_p est -1. Le signe ε_∞ de l'équation fonctionnelle complexe est égal à -1 sous l'hypothèse de Heegner. Malheureusement, nous ne savons pas lier ε_p et ε_∞. Rappelons cependant que la fonction L p-adique qui interpole les valeurs de la fonction L de E/k tordue par un caractère en $s=1$ admet une équation fonctionnelle dont le signe est bien ε_∞ [10]. Cette fonction est conjecturalement liée à notre fonction $\mathscr{L}_p(E/k_\infty)$ bien qu'aucune conjecture précise n'ait été pour l'instant écrite. Nous y reviendrons à la fin de ce paragraphe. Pour montrer que A_1 est vraie, nous pouvons aussi montrer que $\tilde{S}_p(D_\infty)$ ou $\mathbf{H}_\infty$ sont nuls (*cf.* exemples numériques 1). En utilisant le module $\mathbf{H}_\infty$ de Heegner, on obtient par exemple :

si E *vérifie l'hypothèse de Heegner et est ordinaire en p, si k est égal à* $\mathbb{Q}(\sqrt{-p})$ *et est principal alors* A_1 *est vraie car* $\mathbf{H}_\infty$ *est non trivial.*

Ces conditions sont en fait très restrictives et excluent le cas où E a multiplication complexe.

Exemples 2. — Donnons pour les courbes suivantes tirées de [12] les valeurs de p vérifiant les hypothèses précédentes

11 B $\qquad y^2+y=x^3-x^2-10x-20, \qquad p=3,\ 43$

17 C $\quad y^2+xy+y=x^3-x^2-x-14, \qquad p=7,\ 19,\ 43,\ 67.$

Nous allons maintenant étudier la consistence de ces conjectures avec la conjecture de Birch et Swinnerton-Dyer.

THÉORÈME 4.1. — *Si la fonction de Hasse-Weil $L(E/k, s)$ de E/k a un zéro simple en $s=1$, la conjecture A_1 est vraie.*

2. *Supposons de plus que $E(k)$ est de rang 1. Alors la conjecture de Birch et Swinnerton-Dyer implique que la conjecture $A_2(1)$ est vraie si 1 est le caractère trivial de $G(D_\infty/k)$.*

Plus précisément, notons e_1 un point de Heegner sur E défini sur le corps de Hilbert H de k. L'étude précise du module $\mathbf{H}_\infty$ et de son module de coinvariants par le groupe de Galois de D_∞/k permet d'écrire la conjecture $A_2(1)$ sous la forme

$$A_2(1): \quad \lim_{s\to 0} \frac{\mathscr{L}_p(E/k_\infty)(v^s)}{s} \sim u^{-2} c_E^{-2} \mathscr{E}_p^2 \langle \mathrm{tr}_{H/k}(e_1), \mathrm{tr}_{H/k}(e_1)\rangle_{v,\,p}$$

où $\mathscr{E}_p$ désigne le facteur d'Euler de E sur $\mathbb{Q}$ en p. On montre alors que si $E(k)$ est de rang 1, si $L(E/k, s)$ a un zéro simple en $s=1$ et si la p-composante du groupe de Shafarevitch-Tate $Ш(k)$ est finie, la conjecture $A_2(1)$ est équivalente à

$$[E(k)\otimes_{\mathbb{Z}} Z_p : Z_p \mathrm{tr}_{H/k} e_1] \sim \mathfrak{M}_{\mathbb{Q}} \sqrt{\#(Ш(k)(p))}\, u^2 c_E^2$$

avec des notations que nous allons préciser. Auparavant, rappelons que cette formule se déduit de la conjecture de Birch et Swinnerton-Dyer grâce au théorème démontré par GROSS et ZAGIER [5]. Ici, $\mathfrak{M}_{\mathbb{Q}}$ est le produit des nombres de Tamagawa de E sur $\mathbb{Q}$:

$$\mathfrak{M}_{\mathbb{Q}} = \prod_\ell [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)].$$

Remarquons que la condition que la fonction $L(E/k, s)$ a un zéro simple en $s=1$ est équivalente au fait que $\mathrm{tr}_{H/k}(e_1)$ n'est pas de torsion.

Remarque. — Comme il a déjà été dit, nous ne montrerons ce théorème que lorsque E a multiplication complexe (dans ce cas, uc_E est toujours une unité (pour $p\neq 2, 3$)). Dans le cas général, il faudrait rajouter l'hypothèse que la hauteur p-adique relative à l'extension cyclotomique d'un point de $E(k)$ est non nulle, ce qui, dans le cas C.M., a été montré par D. BERTRAND [2].

Donnons une conséquence de ces conjectures.

PROPOSITION 5. — *Si la conjecture* A *est vraie, l'une des affirmations suivantes est vraie* :

$$\mathrm{tr}_{H/k}(e_1) \quad \textit{n'est pas de torsion}$$

ou

$$Ш(k)(p) \quad \textit{est infini}$$

ou

$$\textit{le rang de } E(k) \textit{ est strictement supérieur à } 1.$$

Faisons finalement quelques remarques sur le lien entre ces conjectures et celles présentées dans [10] sur la fonction L p-adique notée $L_p(E/k)$. Rappelons-en rapidement la définition. Soit f la forme modulaire normalisée associée à E. On a donc

$$\pi^* \omega = c_E 2i\pi f(z)\,dz.$$

Posons

$$\Omega_f = 8\pi^2 \int_{\chi_0(N)} |f(z)|^2\,dx\,dy.$$

On choisit des plongements de $\bar{\mathbb{Q}}$ dans $\bar{\mathbb{Q}}_p$ et dans $\mathbb{C}$ et on considère abusivement un caractère d'ordre fini de $G(k_\infty/k)$ dans $\bar{\mathbb{Q}}^\times$ comme une fonction sur les idéaux de k. La fonction $L_p(E/k)$ est alors un élément de $d^{-1}\mathrm{Iw}(k_\infty/k)$ (pour un certain entier d de $\mathbb{Z}_p$) vérifiant pour tout caractère χ d'ordre fini de $G(k_\infty/k)$ à valeurs dans $\bar{\mathbb{Q}}^\times$ (et de conducteur $\mathfrak{f}$)

$$L_p(E/k)(\chi) = \bar{\chi}(\mathfrak{D})\,\mathrm{N}\mathfrak{f}^{1/2}\,\alpha_{\mathrm{N}\mathfrak{f}}^{-1}\,V_p(\chi)\,|D|^{1/2}\,W(\chi)\,\frac{L(E,k,\bar{\chi},1)}{\Omega_f}.$$

Ici, $L(E,k,\chi,s)$ est la fonction de Hasse-Weil de E/k tordue par le caractère χ, $\mathfrak{D}$ est la différente de k et D son discriminant; $W(\chi)$ est l'« Artin Root number » associé à χ. Quand à α_p, c'est la racine qui est une unité du polynôme caractéristique de l'endomorphisme de Frobenius agissant sur $\tilde{E}_p(\mathbb{F}_p)$. Enfin, $V_p(\chi)$ est un facteur du type facteur d'Euler (nous le retrouverons de manière naturelle dans l'étude des modules $\mathcal{H}_\infty$ sous la notation $\delta_p(\chi)$ dans le paragraphe 3). On montrera que $V_p(1)$ et δ_p^2 ont même valuation.

Il est alors naturel de proposer le lien suivant entre $L_p(E/k)$ et $\mathscr{L}_p(E/k_\infty)$:

$$L_p(E/k)\Omega_f|D|^{-1/2} \sim \mathscr{L}_p(E/k_\infty)\Omega_E|D|^{-1/2}$$

où Ω_E est la période complexe de E :

$$\Omega_E = \int_{E(\mathbb{C})} \omega \wedge i\bar{\omega}$$

(rappelons que Ω_E/Ω_f est un rationnel égal à $c_E^2/\deg \pi$). Toutes ces conjectures mettent en évidence le fait que la fonction d'Iwasawa $\mathscr{L}_p(E/k_\infty)$ n'est pas invariante par isogénie (alors que la fonction $L_p(E/k)$ l'est de manière évidente par définition). C'est en effet le cas. Plus précisément, on montre (*voir* l'appendice pour une formulation plus générale et la démonstration) :

PROPOSITION 6. — *Soient deux courbes elliptiques E et E' définies sur $\mathbb{Q}$ et isogènes ayant bonne réduction ordinaire en p. Alors, on a*

$$\Omega_{E'}\mathscr{L}_p(E'/k_\infty) \sim \Omega_E \mathscr{L}_p(E/k_\infty).$$

Exemple 3. — Soit E la courbe elliptique modulaire $X_0(11)$ (de conducteur 11) et E_1 et E_2 les deux courbes isogènes à E de conducteur 11 :

$$E_1 = E/\mu_5 \qquad \text{et} \qquad E_2 = E/(\mathbb{Z}/5\mathbb{Z}).$$

Ces courbes ont bonne réduction ordinaire en $p=5$ et on a

$$\Omega_E = \Omega_f, \qquad \Omega_{E_1} = 5\Omega_f, \qquad \Omega_{E_2} = \frac{1}{5}\Omega_f.$$

On en déduit que 5 divise $\mathscr{L}_5(E/k_\infty)$ et que 25 divise $\mathscr{L}_5(E_2/k_\infty)$.

Remarquons que les résultats du paragraphe 3 sont différents de ceux annoncés dans [8] : des facteurs d'Euler s'introduisent dans le calcul des coinvariants du module des points de Heegner, facteurs dont la présence est tout à fait attendue dans la théorie p-adique.

2. Théorie d'Iwasawa

2.1. Situation étudiée

Expliquons d'abord le but de ce paragraphe. Soit E une courbe elliptique définie sur un corps de nombres F et ayant bonne réduction ordinaire en toute place au-dessus de p. Soit F_∞/F une $\mathbb{Z}_p^2$-extension. Le $\Lambda_{F_\infty/F}$-module $\widehat{S_p(F_\infty)}$ est un $\Lambda_{F_\infty/F}$-module compact de type fini. Faisons l'hypothèse

Hypothèse (*). — Le $\Lambda_{F_\infty/F}$-module $\widehat{S_p(F_\infty)}$ est de $\Lambda_{F_\infty/F}$-torsion.

Soit $\mathscr{L}_p(E/F_\infty)$ sa série caractéristique dans $\mathrm{Iw}(F_\infty/F)$ (définie à une unité près). Elle est donc non nulle par hypothèse. Supposons maintenant qu'il existe une $\mathbb{Z}_p$-extension D_∞ de F contenue dans F_∞ telle que $\widehat{S_p(D_\infty)}$ ne soit pas de $\Lambda_{D_\infty/F}$-torsion (par exemple dans la situation du paragraphe 1, cela peut se produire si D_∞ est la $\mathbb{Z}_p$-extension diédrale d'un corps quadratique imaginaire). Cette hypothèse se traduit de la manière suivante: pour tout caractère ρ de $G(F_\infty/F)$ à valeurs dans $\mathbb{Z}_p^\times$ définissant D_∞ (c'est-à-dire tel que le noyau de ρ soit égal à $G(F_\infty/D_\infty)$), la fonction $\mathscr{L}_p(E/F_\infty)$ est nulle en ρ. On désire alors l'étudier plus précisément dans la direction de ρ, en particulier relier le début de son développement dans la direction de ρ à des invariants arithmétiques de E sur D_∞. Ces invariants arithmétiques seront le sous-module de torsion $t(D_\infty)$ de $\widehat{S_p(D_\infty)}$ et sa série caractéristique $\mathscr{T}_p(E/D_\infty)$ dans $\mathrm{Iw}(D_\infty/F)$ en tant que $\Lambda_{D_\infty/F}$-module, le rang r_{D_∞} des normes universelles de $\check{S}_p(F)$ dans les $\check{S}_p(D_n)$ (pour D_n extension finie de F contenue dans D_∞) et la hauteur p-adique $\ll , \gg_{v_\infty, p}$ attachée à un caractère v_∞ de $G(F_\infty/D_\infty)$ définie sur $\tilde{S}_p(D_\infty)$. Sans plus définir les notations, on peut énoncer (avec les restrictions qui suivront le théorème):

Théorème 1. — (i) *Soit r_{D_∞} le rang des normes universelles de $\check{S}_p(F)$ dans $\tilde{S}_p(D_\infty)$: la fonction d'Iwasawa $\mathscr{L}_p(E/F_\infty)$ a un zéro en ρ de multiplicité supérieure ou égale à r_{D_∞} pour tout caractère ρ de $G(F_\infty/F)$ dont le noyau est $G(F_\infty/D_\infty)$.*

(ii) *Ce zéro est de multiplicité r_{D_∞} si et seulement si la forme bilinéaire $\ll , \gg_{v_\infty, p}$ est non dégénérée sur $\tilde{S}_p(D_\infty)$.*

(iii) *On a dans ce cas*

$$\lim_{s \to 0} \frac{\mathscr{L}_p(E/F_\infty)(\rho v^s)}{s^{r_{D_\infty}}} \sim \mathrm{disc}_{\tilde{S}_p(D_\infty)} \ll , \gg_{v_\infty, p}(\rho)\, \mathscr{T}_p(E/D_\infty)(\rho).$$

pour tout caractère ν *de* $G(F_\infty/F)$ *dont la restriction* ν_∞ *à* $G(F_\infty/D_\infty)$ *est non triviale.*

Nous ne montrerons malheureusement pas ce qui précède en toute généralité, mais seulement dans le cadre de la multiplication complexe. Cependant, le théorème 1 se montre à partir de quelques faits que nous ne savons pas montrer dans le cas général mais qui sont certainement vrais. Nous allons donc les énoncer de manière indépendante de la démonstration du théorème. La démonstration de ces faits utilise le point de vue de [9]: les hauteurs p-adiques se déduisent de pseudo-isomorphismes entre groupes de Selmer relatifs à des $\mathbb{Z}_p$ ou $\mathbb{Z}_p^2$-extensions.

Nous supposerons donc que E est une courbe elliptique définie sur F à multiplication complexe par l'anneau des entiers d'un corps quadratique imaginaire K et que E a bonne réduction ordinaire en toute place au-dessus de p. Dans le cas particulier que nous avons en vue, la $\mathbb{Z}_p^2$-extension F_∞ de F contient la $\mathbb{Z}_p$-extension cyclotomique C_∞ de F et il y a un nombre fini de places de F_∞ au-dessus de p. Nous le supposerons donc; dans l'énoncé des faits qui suivent, L_∞ sera une $\mathbb{Z}_p$-extension de F contenue dans F_∞, ramifiée en toute place de F au-dessus de p mais nous ne démontrerons ces faits que dans le cas où L_∞ est la $\mathbb{Z}_p$-extension cyclotomique C_∞.

Nous devons faire les hypothèses suivantes:

HYPOTHÈSE (**). — *Pour toute extension finie* F' *contenue dans* F_∞, *le* $\Lambda_{L_\infty F'/F'}$*-module* $\widehat{S_p(L_\infty F')}$ *est de* $\Lambda_{L_\infty F'/F'}$*-torsion.*

HYPOTHÈSE DE LEOPOLDT. — *La conjecture de Leopoldt relative à chacun des deux idéaux du corps de multiplication complexe au-dessus de p est vraie pour toute extension finie contenue dans* $KF(E_{p^\infty})$.

FAIT *a.* — *Soit* M_∞ *une extension de* F *contenue dans* F_∞ *telle que* $G(F_\infty/M_\infty)$ *soit isomorphe à* $\mathbb{Z}_p$; *on suppose que* M_∞/F *est ramifiée en toute place divisant p. Alors l'homomorphisme de restriction.*

$$S_p(M_\infty) \to S_p(F_\infty)^{G(F_\infty/M_\infty)}$$

est un quasi-isomorphisme. De plus, les noyaux et conoyaux sont d'ordre borné lorsque M_∞ *varie dans* F_∞.

Démonstration. — La démonstration se fait comme celle de la proposition II.12 de [9]. On utilise les faits que les groupes

$H^i(F_\infty/M_\infty, E_{p^\infty}(F_\infty))$ sont finis (et d'ordre borné) de même que les groupes $H^1(F_{\infty,v}/M_{\infty,v}, E(F_{\infty,v}))$ si v est une place de M_∞ ramifiée dans F_∞.

Avant d'énoncer le fait b, rappelons comment ayant choisi un générateur topologique γ de $\Gamma' = G(L_\infty/F)$, on peut construire un homomorphisme de $\mathbb{Z}_p$-modules

$$\check{S}_p(F) \to a_{\Lambda_{\Gamma'}}(\widehat{S_p(L_\infty)})^{\Gamma'} \tag{1}$$

où $a_{\Lambda_{\Gamma'}}(\widehat{S_p(L_\infty)})$ est l'adjoint de $\widehat{S_p(L_\infty)}$ c'est-à-dire par définition

$$\mathrm{Ext}^1_{\Lambda_{\Gamma'}}(\widehat{S_p(L_\infty)}, \Lambda_{\Gamma'})$$

(on le notera aussi $a_{L_\infty}(\widehat{S_p(L_\infty)})$. Pour cela, soit $\mathcal{U}$ l'image de $\widehat{S_p(L_\infty)}$ dans le quotient de $\widehat{S_p(F)}$ par son $\mathbb{Z}_p$-module de torsion; de la suite exacte de $\Lambda_{\Gamma'}$-modules

$$0 \to \Lambda_{\Gamma'} \xrightarrow{\gamma - 1} \Lambda_{\Gamma'} \to \mathbb{Z}_p \to 0,$$

on déduit l'isomorphisme de $\mathbb{Z}_p$-modules

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{U}, \mathbb{Z}_p) \xrightarrow{\simeq} a_{\Lambda_{\Gamma'}}(\mathcal{U})^{\Gamma'};$$

l'homomorphisme cherché est alors obtenu par composition des homomorphismes suivants :

$$\check{S}_p(F) \to \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{U}, \mathbb{Z}_p) \to a_{\Lambda_{\Gamma'}}(\mathcal{U})^{\Gamma'} \to a_{\Lambda_{\Gamma'}}(\widehat{S_p(L_\infty)})^{\Gamma'}.$$

Finalement, soit ν un caractère non trivial de $G(L_\infty/F)$ à valeurs dans $\mathbb{Z}_p^\times$.

FAIT b. — *Il existe un quasi-isomorphisme Φ_{L_∞} injectif*

$$\widehat{S_p(L_\infty)} \to a_{L_\infty}(\widehat{S_p(L_\infty)})$$

induisant sur $\check{S}_p(F) \times \check{S}_p(F)$ la hauteur p-adique analytique $\langle\ ,\ \rangle_{\nu,p}$.

Expliquons ce que signifie le fait b. Soit γ un générateur topologique de $G(L_\infty/F) = \Gamma'$; des homomorphismes

$$\begin{array}{ccc} \widehat{S_p(L_\infty)}^{\Gamma'} & \xrightarrow{\sim} & a_{L_\infty}(\widehat{S_p(L_\infty)})^{\Gamma'} \\ \downarrow & & \uparrow (1) \\ \widehat{S_p(F)} & & \check{S}_p(F) \\ \downarrow & & \\ \mathrm{Hom}_{\mathbb{Z}_p}(S_p(F), \mathbb{Z}_p) & & \end{array}$$

on déduit une forme bilinéaire $\{\ ,\ \}_{\gamma,p}$ sur $\check{S}_p(F)$ à valeurs dans $\mathbb{Q}_p$ telle que

$$\langle\ ,\ \rangle_{v,p} = \frac{1}{\log_p v(\gamma)} \{\ ,\ \}_{\gamma,p}$$

ne dépend que de v. Le fait *b* est alors que $\langle\ ,\ \rangle_{v,p}$ restreinte à $E(F)\otimes_{\mathbb{Z}}\mathbb{Z}_p$ est exactement la forme bilinéaire *p*-adique définie dans [7] (*voir* aussi [9], paragraphe III).

Démonstration. — Dans le cas où F contient le corps de multiplication complexe K, cela est démontré dans [9] pour toute $\mathbb{Z}_p$-extension L_∞ de F contenue dans $F(E_{p^\infty})$ telle que $\widehat{S_p(L_\infty)}$ soit de $\Lambda_{L_\infty/F}$-torsion (corollaire 3 du paragraphe V, paragraphe V.4) et donc en particulier pour $L_\infty = C_\infty$. Lorsque F ne contient pas le corps de multiplication complexe, on introduit le corps $F' = FK$ et on fait la théorie avec F' comme corps de base. On en déduit le résultat pour la $\mathbb{Z}_p$-extension L_∞ de F en remarquant que le groupe de Galois $G(F'/F)$ agit sur toute la situation et que $\widehat{S_p(L_\infty)}$ est le sous-module de $\widehat{S_p(L_\infty F')}$ fixé par $G(F'/F)$ (le nombre premier p est ici supposé impair).

Le quasi-isomorphisme Φ_{L_α} est fonctoriel par extension du corps de base, c'est-à-dire que si F' est une extension finie de F, le diagramme suivant est commutatif, la flèche de gauche est induite par la restriction, celle de droite par la corestriction.

$$\begin{array}{ccc} \widehat{S_p(F' L_\gamma)} & \xrightarrow{\Phi_{L_\gamma F'}} & \dot{a}_{L_\gamma F'}(\widehat{S_p(F' L_\gamma)}) \\ \downarrow & & \downarrow \\ \widehat{S_p(L_\gamma)} & \xrightarrow{\Phi_{L_\gamma}} & \dot{a}_{L_\gamma}(\widehat{S_p(L_\gamma)}); \end{array}$$

Si M est un $\Lambda_{F_\alpha/F}$-module, notons

$$a_{F_\alpha}(M) = \mathrm{Ext}^1_{\Lambda_{F_\alpha/F}}(M, \Lambda_{F_\alpha/F}).$$

FAIT c. — *Les homomorphismes* Φ_{L_∞} *induisent un* $\Lambda_{F_\infty/F}$*-pseudo-isomorphisme injectif* Φ_{F_∞} :

$$\widehat{S_p(F_\infty)} \xrightarrow{\Phi_{F_\infty}} \dot{a}_{F_\infty}(\widehat{S_p(F_\infty)}).$$

De plus, son conoyau $T(F_\infty)$ *vérifie que* $T(F_\infty)^H$ *et* $T(F_\infty)_H$ *sont finis pour tout sous-groupe* H *de* $G(F_\infty/F)$ *dont le corps des invariants est ramifié sur* F *en toute place divisant* p.

Démonstration. — Par passage à la limite projective des homomorphismes $\Phi_{F' L_\infty}$ pour F' contenu dans F_∞, on obtient un $\Lambda_{F_\infty/F}$-homomorphisme injectif

$$\widehat{S_p(F_\infty)} \to \varprojlim \dot{a}_{L_\infty F'}(\widehat{S_p(L_\infty F')}).$$

Montrons que ce dernier $\Lambda_{F_\infty/F}$-module est presque $\dot{a}_{F_\infty}(S_p(F_\infty))$. Du fait a, on déduit que l'on a la suite exacte :

$$0 \to a_{L_\infty F'}(\widehat{S_p(L_\infty F')}) \to a_{L_\infty F'}(\widehat{S_p(F_\infty)}_{G(F_\infty/L_\infty F')})$$
$$\to (\text{fini d'ordre borné}) \to 0.$$

Par passage à la limite projective, le dernier terme donne un $\Lambda_{F_\infty/F}$-module fini. Quant au second terme, il est égal à $a_{\Lambda_{F_\infty/F}}(\widehat{S(F_\infty)})$ grâce au lemme suivant (*cf.* corollaire I. 13 de [9]).

LEMME 2. — *Soit* M *un* Λ*-module de type fini compact de torsion. Soit* $\mathfrak{L}_i$ *une suite décroissante d'idéaux de hauteur* 1 *premiers à la série caractéristique de* M. *Alors*

$$a_\Lambda(M) = \varprojlim a_{\Lambda/\mathfrak{L}_i}(M/\mathfrak{L}_i M).$$

Démonstration. — De la suite exacte de Λ-modules

$$0 \to \Lambda \xrightarrow{f_i} \Lambda \to \Lambda/\mathfrak{L}_i \to 0$$

(avec $\mathfrak{L}_i = (f_i)$) et du lemme I. 10 de [9], on déduit la suite exacte

$$0 \to a_\Lambda(M)\,\mathfrak{L}_i\, a_\Lambda(M) \to a_{\Lambda/\mathfrak{L}_i}(M/\mathfrak{L}_i M) \to \mathrm{Ext}^2_\Lambda(M, \Lambda)_{\mathfrak{L}_i}$$

(le dernier terme est le noyau de la multiplication par f_i sur $\mathrm{Ext}^2_\Lambda(M, \Lambda)$). Il suffit alors de montrer que la limite projective des $\mathrm{Ext}^2_\Lambda(M, \Lambda)_{\mathfrak{Q}_i}$ relativement à la multiplication par f_{i+1}/f_i est nulle. Comme f_{i+1}/f_i appartient à l'idéal maximal $\mathcal{M}$ de Λ, cela se déduit du fait que, comme M est compact, on a

$$\bigcap \mathcal{M}^n M = 0.$$

Nous ne donnerons pas les détails de la démonstration des propriétés relatives au conoyau $T(F_\infty)$ (*voir* [9], paragraphe V. 1).

Remarque 3. — Si maintenant M_∞/F est une $\mathbb{Z}_p$-extension contenue dans F_∞ (que l'on supposera pour simplifier ramifiée en toute place au-dessus de p), on déduit comme au fait b une forme bilinéaire $\langle\ ,\ \rangle_{\lambda, p}$ sur $\check{S}_p(F)$ attachée à un caractère λ de $G(F_\infty/F)$ dont le noyau est $G(F_\infty/M_\infty)$. Plus précisément on construit un homomorphisme naturel

$$\check{S}_p(F) \to (\hat{a}_{F_\infty}(\widehat{S_p(F_\infty)})_{G(F_\infty/M_\infty)})^{G(M_\infty/F)}$$

dépendant du choix d'un générateur topologique γ de $G(M_\infty/F)$ (*cf.* [9], V 2, (7)), d'où comme pour le fait b une forme bilinéaire $\{\ ,\ \}_{\gamma, p}$ sur $\check{S}_p(F)$ à valeurs dans $\mathbb{Q}_p$ telle que

$$\langle\ ,\ \rangle_{\lambda, p} = \frac{1}{\log_p \lambda(\gamma)} \{\ ,\ \}_{\gamma, p}$$

ne dépend que de λ.

Les propriétés du conoyau $T(F_\infty)$ de Φ_{F_∞} impliquent que les formes bilinéaires $\langle\ ,\ \rangle_{\lambda', p}$ sont à valeurs dans $\mathbb{Z}_p$ sur un sous-groupe de $\check{S}_p(F')$ d'indice fini borné lorsque F' parcourt les sous-extensions de M_∞/F et que λ' est la restriction de λ à $G(F_\infty/F')$.

2.2. Λ-modules. normes universelles. groupes de Selmer

Soit Γ un $\mathbb{Z}_p$-module isomorphe à $\mathbb{Z}_p$; rappelons que Λ_Γ est l'anneau $\mathbb{Z}_p[[\Gamma]]$ et $\Gamma_n = \Gamma^{p^n}$. Soit M un Λ_Γ-module compact de type fini. Posons $M_n = M_{\Gamma_n}$.

Lemme 4. — (i) *Les Λ_Γ-rangs de M et de $\mathrm{Hom}_{\Lambda_\Gamma}(M, \Lambda_\Gamma)$ sont égaux.*
(ii) *Le Λ_Γ-module $\mathrm{Hom}_{\Lambda_\Gamma}(M, \Lambda_\Gamma)$ est égal à la limite projective des*

$$\mathrm{Hom}_{\mathbb{Z}_p}(M_n, \mathbb{Z}_p)$$

relativement aux homomorphismes de normes

$$M_n \to M_{n+1}.$$

(iii) *Le $\mathbb{Z}_p$-module des coinvariants pour Γ de $\mathrm{Hom}_{\Lambda_\Gamma}(M, \Lambda_\Gamma)$ est un sous-$\mathbb{Z}_p$-module de $\mathrm{Hom}_{\mathbb{Z}_p}(M_0, \mathbb{Z}_p)$.*

Démonstration. — (i) est évident. Pour (ii), on remarque que $\mathrm{Hom}_{\mathbb{Z}_p}(M_n, \mathbb{Z}_p)$ est canoniquement isomorphe à

$$\mathrm{Hom}_{\Lambda_\Gamma}(M, \mathbb{Z}_p[\Gamma/\Gamma_n])$$

par l'homomorphisme

$$\varphi_n \mapsto (x \mapsto \textstyle\sum_{\gamma \in \Gamma/\Gamma_n} \varphi_n(\gamma^{-1}x)\gamma)$$

et que l'homomorphisme de normes correspond par cet isomorphisme à la projection canonique

$$\mathbb{Z}_p[\Gamma/\Gamma_{n+1}] \to \mathbb{Z}_p[\Gamma/\Gamma_n].$$

Comme Λ_Γ est par définition la limite projective des $\mathbb{Z}_p[\Gamma/\Gamma_n]$, on en déduit la partie (ii).

Montrons maintenant (iii). Soit f un élément de $\mathrm{Hom}_{\Lambda_\Gamma}(M, \Lambda_\Gamma)$ dont l'image f_0 dans $\mathrm{Hom}_{\mathbb{Z}_p}(M_0, \mathbb{Z}_p)$ est nulle; on a donc si $m \in M$

$$0 = f_0(m \text{ modulo } TM) = f(m) \text{ modulo } T\Lambda_\Gamma$$

si $T = \gamma - 1$ pour un générateur topologique γ de Γ. On en déduit un unique élément $g(m)$ de Λ_Γ tel que

$$f(m) = Tg(m).$$

La fonction g sur M est un élément de $\mathrm{Hom}_{\Lambda_\Gamma}(M, \Lambda_\Gamma)$. D'où (iii).

L'image de $\mathrm{Hom}_{\Lambda_\Gamma}(M, \Lambda_\Gamma)$ dans $\mathrm{Hom}_{\mathbb{Z}_p}(M_0, \mathbb{Z}_p)$ est le sous-$\mathbb{Z}_p$-module des normes universelles de $\mathrm{Hom}_{\mathbb{Z}_p}(M_0, \mathbb{Z}_p)$ relativement à M. C'est aussi l'intersection des projections des $\mathrm{Hom}_{\mathbb{Z}_p}(M_n, \mathbb{Z}_p)$ dans $\mathrm{Hom}_{\mathbb{Z}_p}(M_0, \mathbb{Z}_p)$. Son $\mathbb{Z}_p$-rang est égal au Λ_Γ-rang de M.

Revenons à notre situation arithmétique. Le dual de Pontryagin $\widehat{S_p(F_\infty)}$ de $S_p(F_\infty)$ est muni d'une structure de $\Lambda_{F_\infty/F}$-module compact de type fini. L'hypothèse (*) implique que $\widehat{S_p(F_\infty)}$ est un $\Lambda_{F_\infty/F}$-module de torsion grâce au fait a. Soit $\mathscr{L}_p(E/F_\infty)$ sa série caractéristique dans $\mathrm{Iw}(F_\infty/F)$. Soit

maintenant D_∞ une $\mathbb{Z}_p$-extension de F contenue dans F_∞ ramifiée en toute place v de F et vérifiant les deux propriétés équivalentes suivantes :

(i) $\widehat{S_p(D_\infty)}$ *n'est pas de* $\Lambda_{D_\infty/F}$*-torsion.*

et

(ii) $\mathscr{L}_p(E/F_\infty)$ *est nulle sur tout caractère* ρ *dont le noyau contient* $G(F_\infty/D_\infty)$ (l'équivalence de (i) et (ii) se déduit du lemme I.4 de [9]).

On introduit les $\Lambda_{D_\infty/F}$-modules suivant associés à $\widehat{S_p(D_\infty)}$. Soient d'abord $t(D_\infty)$ le sous-$\Lambda_{D_\infty/F}$-module de torsion de $\widehat{S_p(D_\infty)}$ et $R(D_\infty)$ le quotient de $\widehat{S_p(D_\infty)}$ par $t(D_\infty)$. Nous avons associé un autre $\Lambda_{D_\infty/F}$-module sans torsion qui est $\tilde{S}_p(D_\infty)$. Le lien entre $R(D_\infty)$ et $\tilde{S}_p(D_\infty)$ est donné dans le lemme suivant.

LEMME 5. — (i) *Le* $\Lambda_{D_\infty/F}$*-module* $\tilde{S}_p(D_\infty)$ *est isomorphe à*

$$\mathrm{Hom}_{\Lambda_{D_\infty/F}}(R(D_\infty), \Lambda_{D_\infty/F})$$

et (non canoniquement) à

$$\mathrm{Ext}^1_{\Lambda_{F_\infty/F}}(R(D_\infty), \Lambda_{F_\infty/F}).$$

(ii) *Le* $\Lambda_{D_\infty/F}$*-module* $R(D_\infty)$ *s'injecte dans*

$$\mathrm{Hom}_{\Lambda_{D_\infty/F}}(\tilde{S}_p(D_\infty), \Lambda_{D_\infty/F})$$

avec un conoyau pseudo-nul.

Dans toutes les démonstrations qui suivent, nous poserons $\Lambda = \Lambda_{F_\infty/F}$, $\Gamma = G(D_\infty/F)$.

Démonstration. — L'homomorphisme

$$(\widehat{S_p(D_\infty)})_{\Gamma_n} \to \widehat{S_p(D_n)}$$

a un noyau et un conoyau finis et d'ordre bornés (ici D_n est le corps fixé par Γ_n).

Il en est de même de l'homomorphisme

$$\tilde{S}_p(D_n) \to T_p(S_p(D_n))$$

où $T_p(S_p(D_n))$ désigne le module de Tate de $S_p(D_n)$ relativement à la multiplication par p. On en déduit les égalités :

$$\begin{aligned}\tilde{S}_p(D_\infty) &= \varprojlim \mathrm{Hom}_{\mathbb{Z}_p}\widehat{(S_p(D_n)}, \mathbb{Z}_p) \\ &= \varprojlim \mathrm{Hom}_{\mathbb{Z}_p}\widehat{(S_p(D_\infty)_{\Gamma_n}}, \mathbb{Z}_p) \\ &= \mathrm{Hom}_{\Lambda_\Gamma}\widehat{(S_p(D_\infty)}, \Lambda_\Gamma) \\ &= \mathrm{Hom}_{\Lambda}(R(D_\infty), \Lambda_\Gamma).\end{aligned}$$

Finalement, de la suite exacte

$$0 \to \Lambda \xrightarrow{h-1} \Lambda \to \Lambda_\Gamma \to 0$$

(dépendant du choix du générateur topologique h de $G(F_\infty/D_\infty)$), on déduit que

$$\mathrm{Hom}_\Lambda(R(D_\infty), \Lambda_\Gamma) \xrightarrow{\simeq} \mathrm{Ext}^1_\Lambda(R(D_\infty), \Lambda)$$

et la partie (i) du lemme.

Pour (ii), on utilise l'isomorphisme

$$\tilde{S}_p(D_\infty) \simeq \mathrm{Hom}_{\Lambda_\Gamma}(R(D_\infty), \Lambda_\Gamma).$$

On sait d'autre part par la théorie générale des Λ_Γ-modules que $R(D_\infty)$ s'injecte dans

$$\mathrm{Hom}_{\Lambda_\Gamma}(\mathrm{Hom}_{\Lambda_\Gamma}(R(D_\infty), \Lambda_\Gamma), \Lambda_\Gamma)$$

avec un conoyau pseudo-nul, ce qui termine la démonstration.

2.3. Hauteurs p-adiques attachées a un caractère de $G(\bar{F}/D_\infty)$

On déduit des propriétés fonctorielles des homomorphismes Φ_{L_∞} le lemme suivant (*voir* aussi [7], 3.4.5). On désigne par $N_{L/F}$ la norme de $\check{S}(L)$ à $\check{S}(F)$.

Lemme 6. — *Soit L/F une extension finie et v un homomorphisme de $G(F_\infty/F)$ dans $\mathbb{Z}_p^*$. Si v' est la restriction de v à $G(\bar{F}/L)$, on a*

(i) $\langle x, y\rangle_{v,p} = \langle x, N_{L/F}(y)\rangle_{v',p}$ pour $x \in \check{S}_p(F)$, $y \in \check{S}_p(L)$.

(ii) $\langle x, y\rangle_{v,p} = \langle N_{L/F}(x), y\rangle_{v',p}$ pour $x \in \check{S}_p(L)$, $y \in \check{S}_p(F)$.

Revenons à la $\mathbb{Z}_p$-extension D_∞ telle que $\widehat{S_p(D_\infty)}$ ne soit pas de $\Lambda_{D_\infty/F}$-torsion. On note ici D_n le sous-corps de degré p^n sur F, ρ un caractère définissant D_∞. Si ν est un caractère de $G(F_\infty/F)$ (par exemple définissant L_∞), on note ν_n sa restriction à $G(F_\infty/D_n)$.

LEMME 7. — *Soit* (x_n) *un élément de* $\tilde{S}_p(D_\infty)$, *alors*

$$\langle x_n, y \rangle_{\rho_n, p} = 0$$

pour tout n et tout y appartenant à $\check{S}_p(D_n)$.

Démonstration. — Grâce au lemme précédent, on a

$$\langle x_n, y \rangle_{\rho_n, p} = \langle x_m, y \rangle_{\rho_m, p}$$

pour tout $m \geqslant n$. De plus, comme $\log_p \rho_m$ est à valeurs dans $p^m \mathbb{Z}_p$, la forme bilinéaire

$$\langle \ , \ \rangle_{\rho_m, p}$$

est à valeurs dans $p^{m-c}\mathbb{Z}_p$ où c ne dépend pas de m grâce à la remarque 3. On en déduit que $\langle x_n, y \rangle_{\rho_n, p}$ appartient à $p^m \mathbb{Z}_p$ pour tout m et donc est nul.

Les formes bilinéaires $\langle \ , \ \rangle_{\rho_n, p}$ étant peu intéressantes pour l'étude de $\tilde{S}_p(D_\infty)$, nous allons nous occuper maintenant de $\langle \ , \ \rangle_{\nu_n, p}$.

LEMME ET DÉFINITION 8. — *Soit* ν *un homomorphisme de* $G(F_\infty/F)$ *à valeurs dans* $\mathbb{Z}_p^\times$ *et* ν_∞ *sa restriction à* $G(F_\infty/D_\infty)$. *Soit* $\underline{x} = (x_n)$ *et* $\underline{y} = (y_n)$ *deux éléments de* $\tilde{S}_p(D_\infty)$. *Alors le système d'éléments de* $\mathbb{Z}_p[\Gamma/\Gamma_n]$ (*avec* $\Gamma/\Gamma_n = G(D_n/F)$)

$$(2) \qquad \frac{1}{[D_n : F]} \sum_{s,\, t \in \Gamma/\Gamma_n} \langle s(x_n), t(y_n) \rangle_{\nu_n, p} s^{-1} t$$

est compatible avec les homomorphismes de projection $\mathbb{Z}_p[\Gamma/\Gamma_n] \to \mathbb{Z}_p[\Gamma/\Gamma_{n-1}]$ *et définit un élément de* $\mathbb{Z}_p[[\Gamma]]$ *qui ne dépend de* ν *que par* ν_∞ *et que l'on note*

$$\ll \underline{x}, \underline{y} \gg_{\nu_\infty, p}$$

Démonstration. — Montrons d'abord que les éléments (2) appartiennent bien à $\mathbb{Z}_p[\Gamma/\Gamma_n]$.

On a

$$\sum_{s,\, t \in \Gamma/\Gamma_n} \langle sx_n,\, ty_n \rangle_{v_n,\, p}\, s^{-1} t = [D_n :\, F] \sum_{\gamma \in \Gamma/\Gamma_n} \langle \gamma^{-1} x_n,\, y_n \rangle_{v_n,\, p}\, \gamma.$$

La forme bilinéaire $\langle\, , \rangle_{v_n,\, p}$ est à valeurs dans $\mathbb{Z}_p$ sur un sous-groupe S_n d'indice fini borné par rapport à n de $\check{S}_p(D_n)$. Donc on a

$$\varprojlim S_n = \varprojlim \check{S}_p(D_n) = \tilde{S}_p(D_\infty)$$

et l'élément (2) appartient à $\mathbb{Z}_p[\Gamma/\Gamma_n]$.

Ensuite la compatibilité se déduit du fait que

$$\langle x_{n-1},\, y_{n-1} \rangle_{v_n,\, p} = [D_n : D_{n-1}] \langle x_{n-1},\, y_{n-1} \rangle_{v_{n-1},\, p}.$$

Finalement, si v et v' ont même restriction à $G(F_\infty/D_\infty)$, on a

$$v = v'\, \rho^a$$

avec $a \in \mathbb{Z}_p$ et la dernière affirmation du lemme se déduit alors du lemme précédent.

Nous venons donc de définir une forme bilinéaire $\ll\, ,\, \gg_{v_\infty,\, p}$ sur $\tilde{S}_p(D_\infty)$ de manière analytique dans la mesure où les $\langle\, ,\, \rangle_{v_n,\, p}$ sont analytiques au moins sur $E(D_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Nous allons maintenant passer à une construction algébrique en utilisant le pseudo-isomorphisme Φ_{F_∞}.

2.4. Groupes de Selmer et séries caractéristiques

Nous fixons un générateur h de $G(F_\infty/D_\infty) = H$. On identifiera $\Lambda_{F_\infty/F}$ avec $\Lambda_{D_\infty/F}[[S]]$ par $h \leftrightarrow S + 1$. Nous noterons f_{F_∞} la série caractéristique de $\widehat{S_p(F_\infty)}$ vu comme élément de $\mathrm{Iw}(D_\infty/F)[[S]]$. Soit r_{D_∞} le rang de $\widehat{S_p(D_\infty)}$ en tant que $\Lambda_{D_\infty/F}$-module. On a alors le fait trivial suivant.

Lemme 9. — *La série caractéristique de $R(D_\infty)$ en tant que $\Lambda_{F_\infty/F}$-module est $S^{r_{D_\infty}}$.*

Le $\Lambda_{D_\infty/F}$-module $\widehat{S_p(F_\infty)_H}$ est quasi-isomorphe à $\widehat{S_p(D_\infty)}$ grâce au fait a et l'homomorphisme

$$\widehat{S_p(F_\infty)} \to R(D_\infty)$$

est donc quasi-surjectif. On en déduit un homorphisme

$$\alpha : \widehat{S_p(F_\infty)}^H \to R(D_\infty).$$

PROPOSITION 10. — (i) *La série caractéristique* f_{F_α} *de* $\widehat{S_p(F_\alpha)}$ *est divisible par* $S^{r_{D_\infty}}$;

(ii) *Elle est exactement divisible par* $S^{r_{D_\infty}}$ *si et seulement si le conoyau de* α *est de* $\Lambda_{D_\infty/F}$*-torsion ;*

(iii) *Si cela est vérifié,* α *est injective et on a*

$$f_{F_\infty}(S) \sim S^{r_{D_\alpha}} \mathscr{T}_p(E/D_\infty)\,[[R(D_\infty) : \widehat{S_p(F_\infty)}^H]]_{\mathrm{Iw}(D_\infty/F)}$$

modulo $S^{r_{D_\alpha}} \mathrm{Iw}(D_\alpha/F)$

où $\mathscr{T}_p(E/D_\infty)$ *est la série caractéristique du* $\Lambda_{D_\infty/F}$*-module* $t(D_\infty)$ *et où* $[[R(D_\infty) : \widehat{S_p(F_\infty)}^H]]_{\mathrm{Iw}(D_\infty/F)}$ *désigne la série caractéristique du* $\Lambda_{D_\infty/F}$*-module* $R(D_\infty)/\widehat{S_p(F_\infty)}^H$ *(vue comme élément de* $\mathrm{Iw}(D_\infty/F)$*).*

Démonstration. — Soit B_α le noyau de l'homomorphisme

$$\widehat{S_p(F_\infty)} \to R(D_\infty).$$

La proposition se déduit alors des suites exactes à modules finis près

$$0 \to B_\infty^H \to \widehat{S_p(F_\infty)}^H \to R(D_\infty) \to (B_\infty)_H \to \widehat{S_p(F_\infty)}_H \to R(D_\infty) \to 0$$

et

$$0 \to t(D_\infty) \to \widehat{S_p(F_\infty)}_H \to R(D_\infty) \to 0.$$

On remarque en particulier que $(B_\alpha)_H$ est de $\Lambda_{D_\infty/F}$-torsion si et seulement si f_{F_α} est exactement divisible par $S^{r_{D_\alpha}}$.

Il reste maintenant à interpréter l'indice

$$[[R(D_\alpha) : \widehat{S_p(F_\alpha)}^H]]_{\mathrm{Iw}(D_\infty/F)}$$

comme le discriminant d'une forme bilinéaire à valeurs dans $\mathrm{Iw}(D_\alpha/F)$.

LEMME 11. — (i) *Le pseudo-isomorphisme* Φ_{F_α} *induit un quasi-isomorphisme de* $\Lambda_{D_\alpha/F}$*-modules*

$$\widehat{S_p(F_\alpha)}^H \to \mathrm{Ext}^1_{\Lambda_{F_\alpha/F}}(R(D_\alpha), \Lambda_{F_\alpha/F})$$

sous l'hypothèse que $S^{r_{D_\alpha}}$ *divise exactement* f_{F_α}.

Démonstration. — De la suite exacte

$$0 \to B_\infty \to \widehat{S_p(F_\infty)} \to R(D_\infty) \to \text{fini} \to 0,$$

on déduit la suite exacte

$$0 \to \text{Ext}^1_\Lambda(R(D_\infty), \Lambda) \to \text{Ext}^1_\Lambda(\widehat{S_p(F_\infty)}), \Lambda) \to \text{Ext}^1_\Lambda(B_\infty, \Lambda).$$

Comme $S^{r_{D_\infty}}$ divise exactement f_{F_∞} et que le Λ-module $\text{Ext}^1_\Lambda(B_\infty, \Lambda)$ n'a pas de sous-module pseudo-nul non nul, $\text{Ext}^1_\Lambda(B_\infty, \Lambda)^H$ est nul. Donc

$$\text{Ext}^1_\Lambda(R(D_\infty), \Lambda) \simeq \text{Ext}^1_\Lambda(\widehat{S_p(F_\infty)}), \Lambda)^H. \tag{3}$$

Du pseudo-isomorphisme $\Phi(F_\infty)$, on déduit le quasi-isomorphisme

$$\widehat{S_p(F_\infty)}^H \to \text{Ext}^1_\Lambda(\widehat{S_p(F_\infty)}), \Lambda)^H. \tag{4}$$

En combinant (3) et (4), on en déduit le lemme 11.

En utilisant le lemme 5, on obtient ainsi le diagramme suivant

$$\begin{array}{ccc} \widehat{S_p(F_\infty)}^H & \xrightarrow{\sim} & \text{Ext}^1_{\Lambda_{F_\infty/F}}(R(D_\infty), \Lambda_{F_\infty/F}) \\ \downarrow & & \uparrow \sim \\ R(D_\infty) & & \tilde{S}_p(D_\infty) \\ \downarrow & & \\ \text{Hom}_{\Lambda_{D_\infty, F}}(\tilde{S}_p(D_\infty), \Lambda_{D_\infty/F}) & & \end{array}$$

On en déduit une forme bilinéaire sur $\tilde{S}_p(D_\infty)$ à valeurs dans $p^{-\mu}\Lambda_{D_\infty/F}$ où μ est un entier positif. Notons-la $B_{D_\infty, h}$ (elle dépend en fait du choix du générateur h de $G(F_\infty/D_\infty)$ car l'homomorphisme

$$\tilde{S}_p(D_\infty) \to \text{Ext}^1_{\Lambda_{F_\infty, F}}(R(D_\infty), \Lambda_{F_\infty/F})$$

en dépend). Il nous reste à comparer $B_{D_\infty, h}$ avec la forme bilinéaire $\ll\ ,\ \gg_{v_\infty, p}$.

LEMME 12. — *Les deux formes bilinéaires* $\ll\ ,\ \gg_{v_\infty, p}$ *et* $B_{D_\infty, h}$ *sont proportionnelles :*

$$\ll\ ,\ \gg_{v_\infty, p} = \log_p v_\infty(h) B_{D_\infty, h}.$$

Démonstration. — Par construction, on a le diagramme suivant :

$$\begin{array}{ccccc} R(D_\infty) & \longleftarrow & \widehat{S_p(F_\infty)^H} & \xrightarrow{\Phi_{F_\infty}} & \mathrm{Ext}^1_\Lambda(\widehat{S_p(F_\infty)}, \Lambda)^H = \mathrm{Ext}^1_\Lambda(R(D_\infty), \Lambda) \\ \| & & & & \downarrow \sim \\ \varprojlim \mathrm{Hom}_{\mathbb{Z}_p}(\check{S}_p(D_n), \mathbb{Q}_p) & \xleftarrow{\Psi_{D_\infty}} & \varprojlim \check{S}_p(D_n) & = & \check{S}_p(D_\infty) \end{array}$$

Par définition même de Φ_{F_∞}, Ψ_{D_∞} est obtenu comme limite d'homomorphismes

$$\Psi_n : \quad \check{S}_p(D_n) \to \mathrm{Hom}_{\mathbb{Z}_p}(\check{S}_p(D_n), \mathbb{Q}_p)$$

tels que

$$\Psi_n(y_n)(x_n) = \frac{1}{\log_p \nu_n(h)} \langle x_n, y_n \rangle_{\nu_n, p}.$$

En utilisant l'isomomorphisme canonique décrit dans le lemme 4 entre

$$\mathrm{Hom}_{\mathbb{Z}_p}(\check{S}_p(D_n), \mathbb{Z}_p)$$

et

$$\mathrm{Hom}_{\mathbb{Z}_p[\Gamma/\Gamma_n]}(\check{S}_p(D_n), \mathbb{Z}_p[\Gamma/\Gamma_n]),$$

et la formule (2), on en déduit le lemme 12.

Afin d'énoncer précisément le théorème 1, nous avons encore besoin d'une notation. Si M est un A-module compact de type fini (où A sera ici $\mathbb{Z}_p$ ou $\mathrm{Iw}(D_\infty/F)$), le discriminant d'une forme bilinéaire B sur M est défini par

$$\mathrm{disc}_M B = \frac{\det((B(x_i, x_j)))}{[M : \Sigma A x_i]^2}$$

si (x_i) est un système libre maximal de M.

Le théorème 1 se déduit alors de la proposition 10, du fait que

$$[[R(D_\infty) : \widehat{S_p(F_\infty)^H}]]_{\mathrm{Iw}(D_\infty/F)} \sim \mathrm{disc}_{\tilde{S}_p(D_\infty)} B_{D_\infty, h}$$

et du lemme 12 (on rappelle que le lien entre f_{F_∞} et $\mathscr{L}_p(E/F_\infty)$ est donné par

$$\mathscr{L}_p(E/F_\infty)(\nu^s \rho^t) = f_{F_\infty}(\rho^t)(\nu_\infty(h)^s - 1)).$$

2.5. CONSÉQUENCE SUR LE MODULE DE TORSION DE $\widehat{S_p(D_\infty)}$

On donne ici une conséquence concernant le module de torsion de $\widehat{S_p(D_\infty)}$ ou plutôt sa série caractéristique $\mathscr{T}_p(E/D_\infty)$. On aura besoin pour cela de la formule suivante qui lie $\mathscr{L}_p(E/F_\infty)$ avec les hauteurs p-adiques $\langle\ ,\ \rangle_{\lambda,p}$ définies précédemment :

$$(5)\quad \mathscr{L}_p(E/F_\infty)(\rho^s \nu^{s'}) \sim \mathscr{M}_F \mathscr{E}_p^2 \sharp(Ш(F)(p)/\mathrm{div})\ \mathrm{disc}_{\tilde{S}_p(F)}(\langle\ ,\ \rangle_{p,p} s + \langle\ ,\ \rangle_{\nu,p} s') \text{ modulo } (s, s')^{t_F+1}.$$

Ici, t_F est le $\mathbb{Z}_p$-rang de $\check{S}_p(F)$, $\mathscr{E}_p$ le facteur d'Euler en p

$$\mathscr{E}_p = \prod_{v|p} \sharp(\tilde{E}_v(\tilde{F}_v)),$$

$\mathscr{M}_F$ le produit des nombres de Tamagawa aux places de mauvaise réduction de E/F. Enfin, $Ш(F)(p)/\mathrm{div}$ est le quotient de $Ш(F)(p)$ par son sous-$\mathbb{Z}_p$-module divisible maximal. Cette formule se déduit formellement de la définition des formes bilinéaires $\langle\ ,\ \rangle_{\lambda,p}$ telle qu'elle a été présentée au paragraphe 2.1 et du fait que la formule (5) est vraie pour $s=0$ (démontrée dans [9], V.5 lorsque F contient le corps de multiplication complexe K, le cas général s'en déduit facilement) : plus précisément, on montre comme dans le paragraphe V.3.2 de [8] que

$$\lim_{s\to 0} \frac{\mathscr{L}_p(E/F_\infty)(\lambda^s)}{s^{t_F}} \sim C\,\mathrm{disc}_{\tilde{S}_p(F)}\langle\ ,\ \rangle_{\lambda,p}$$

où C est une constante indépendante de λ; la constante C est alors déterminée par le cas où $\lambda = \nu$.

Remarquons que dans le cas de multiplication complexe, le facteur $\mathscr{M}_F$ est toujours une unité : en effet, $\mathscr{M}_F$ est une puissance de 2 sauf si $K = \mathbb{Q}(\sqrt{-3})$ où $\mathscr{M}_F$ peut avoir aussi le facteur premier 3 mais 3 n'est pas ordinaire pour une courbe elliptique à multiplication complexe par $\mathbb{Q}(\sqrt{-3})$ (*cf.* par exemple [4], proposition 4.5).

Finalement, introduisons la notation suivante : si B est une forme bilinéaire symétrique sur un $\mathbb{Z}_p$-module M et si κ est le noyau de la forme

bilinéaire B, on notera

$$\widetilde{\mathrm{disc}}_M B = \begin{cases} \mathrm{disc}_{M/\kappa} B & \text{si } M \neq \kappa, \\ 1 & \text{si } M = \kappa. \end{cases}$$

Grâce au diagramme commutatif

$$\begin{array}{ccc} S_p(D_\chi)_\Gamma & \longrightarrow & \tilde{S}_p(F) \text{ modulo torsion} \\ & \searrow \quad \swarrow \sim & \\ & \widehat{\mathrm{Hom}_{\mathbb{Z}_p}(S_p(D_\chi)_\Gamma, \mathbb{Z}_p)} & \end{array}$$

on voit que le $\mathbb{Z}_p$-module U_ρ des normes universelles de $\tilde{S}_p(F)$ pour les $\tilde{S}_p(D_n)$ est isomorphe à $\tilde{S}_p(D_\chi)_\Gamma$. Notons κ_ρ le noyau de la forme bilinéaire $\langle \ , \ \rangle_{\rho, \rho}$.

Proposition 13. — *Supposons que :*

(i) *les $\mathbb{Z}_p$-modules U_ρ et κ_ρ ont même rang r_{D_χ},*

(ii) *le discriminant de $\langle \ , \ \rangle_{\rho, \rho}$ sur κ_ρ est non nul.*

Alors, on a

$$\lim_{s \to 0} \frac{\mathscr{F}_p(E/D_\chi)(\rho^s)}{s^{t_F - r_{D_\chi}}} \sim \mathscr{M}_F \mathscr{E}_p^2 \sharp(Ш(F)(p)/\mathrm{div}) \frac{\mathrm{disc}_{\tilde{S}_p(F)} \langle \ , \ \rangle_{\rho, \rho}}{[\kappa_\rho : U_\rho]^2}$$

et

$$\lim_{s \to 0} \frac{\mathscr{F}_p(E/D_\chi)(\rho^s)}{s^n} = 0 \qquad \text{si } n < t_F - r_{D_\chi}.$$

On utilisera pour la démonstration le lemme trivial suivant.

Lemme 14. — *Soient B_1 et B_2 deux formes bilinéaires (symétriques) sur un $\mathbb{Z}_p$-module M de rang t. Soit κ le noyau de B_2 et r son $\mathbb{Z}_p$-rang. Alors le coefficient de $\lambda^r \mu^{t-r}$ dans*

$$\mathrm{disc}_M(\lambda B_1 + \mu B_2)$$

est égal à

$$\mathrm{disc}_\kappa B_1 \cdot \widetilde{\mathrm{disc}}_M B_2.$$

Démonstration de la proposition 13. — Il suffit de mettre ensemble le lemme 14, la formule (5), le théorème 1 et la formule suivante

$$\lim_{s \to 0} \mathrm{disc}_{\tilde{S}_p(D_\infty)} \ll\ ,\ \gg_{v_\infty, p}(\rho^s) = \mathrm{disc}_{U_\rho} \langle\ ,\ \rangle_{v, p}.$$

2.6. Cas où la courbe E est définie sur $\mathbb{Q}$

Supposons ici que E est définie sur $\mathbb{Q}$, que $F = k$ est un corps quadratique imaginaire, que $F_\infty = k_\infty$ est la $\mathbb{Z}_p^2$-extension de k, et que D_∞ est l'extension pro-p-diédrale de $\mathbb{Q}$ contenant k (plus généralement, on pourrait supposer que F est de type C.M. et que E est définie sur son sous-corps maximal totalement réel).

Du pseudo-isomorphisme Φ_{k_∞}, on déduit l'équation fonctionnelle

$$\mathscr{L}_p(E/k_\infty)(\lambda^s) \sim \mathscr{L}_p(E/k_\infty)(\lambda^{-s}) \tag{6}$$

si λ est un caractère de $G(k_\infty/k)$ à valeurs dans $\mathbb{Z}_p^\times$ (cela est d'ailleurs vrai en toute généralité). De plus sous les hypothèses précédentes, la conjugaison complexe τ induit un automorphisme sur $\widehat{S_p(F_\infty)}$. Si ν est le caractère cyclotomique de $G(k_\infty/k)$ et ρ le caractère diédral (on a donc $\mathrm{Ker}\,\nu = G(k_\infty/C_\infty)$ et $\mathrm{Ker}\,\rho = G(k_\infty/D_\infty)$), τ agit sur ν et ρ par

$$\tau(\nu) = \nu, \qquad \tau(\rho) = \rho^{-1}.$$

Notons ι l'involution de $\Lambda_{k_\infty/k}$ définie par la formule

$$f^\iota(\nu^a \rho^b) = f(\nu^{-a} \rho^b).$$

Alors $\mathscr{L}_p(E/k_\infty)$ vérifie l'équation fonctionnelle

$$\mathscr{L}_p(E/k_\infty)^\iota = u\, \mathscr{L}_p(E/k_\infty)$$

où u est une unité de $\Lambda_{k_\infty/k}$. En suivant une idée de Greenberg (non publiée à ma connaissance), on peut alors définir le signe de l'équation fonctionnelle de $\mathscr{L}_p(E/k_\infty)$.

Pour cela, on énonce le lemme suivant.

Lemme 15. — *Le groupe de cohomologie*

$$H^1(\{1, \iota\}, \Lambda_{k_\infty/k}^\times)$$

est d'ordre 2 ; *la classe non triviale admet* -1 *comme représentant.*

Comme conséquence, il existe un représentant de la série caractéristique de $\widehat{S_p(k_\infty)}$, que l'on notera encore $\mathscr{L}_p(E/k_\infty)$, vérifiant

$$\mathscr{L}_p(E/k_\infty)^\iota = \varepsilon_p \mathscr{L}_p(E/k_\infty) \tag{7}$$

avec $\varepsilon_p = \pm 1$, ou encore en explicitant ι

$$\mathscr{L}_p(E/k_\infty)(\nu^{-s'}\rho^s) = \varepsilon_p \mathscr{L}_p(E/k_\infty)(\nu^{s'}\rho^s). \tag{7}'$$

Sous certaines hypothèses de non dégénérescence, ε_p peut être facilement lié à certains invariants de la courbe.

PROPOSITION 16. — (i) *Si* $\langle\ ,\ \rangle_{v,p}$ *est non dégénérée sur* $\check{S}_p(k)$, *alors* $\varepsilon_p = (-1)^{t_k}$.

(ii) *Si* $\ll\ ,\ \gg_{v_\infty,p}$ *est non dégénérée sur* $\check{S}_p(D_\infty)$, *alors*

$$\varepsilon_p = (-1)^{r_{D_\infty}}.$$

Démonstration. — La partie (i) se déduit de la formule (5) prise en $s=0$ et de (7)'. La partie (ii) se déduit de l'équation fonctionnelle (7)' et de la formule (iii) du théorème 1.

Remarque. — Dans le cas où E est à multiplication complexe par $K=k$, on voit facilement que t_k et r_{D_α} sont pairs. On peut cependant dans ce cas utiliser la décomposition de $S_p(k_\infty)$ en $S_\mathfrak{p}(k_\infty) \oplus S_{\mathfrak{p}^*}(k_\infty)$ si $p = \mathfrak{p}\mathfrak{p}^*$ dans k et définir le signe à l'aide de l'équation fonctionnelle liant $\widehat{S_\mathfrak{p}(k_\infty)}$ et $\widehat{S_{\mathfrak{p}^*}(k_\infty)}$. Nous n'entrerons pas ici dans les détails.

COROLLAIRE 17. — *Si* ε_p *est égal à* -1, *le* $\Lambda_{D_\alpha/k}$*-rang de* $\widehat{S_p(D_\alpha)}$ *est supérieur à* 1 *et* $\mathscr{L}_p(E/D_\alpha)$ *est nulle.*

Revenons aux exemples 1 du paragraphe 1. Le calcul de ε_p se déduit de la proposition 16, (i) (l'étude de $y^2 = x^3 - dx$ sur $\mathbf{Q}(\sqrt{-D})$ se ramenant à celles de $y^2 = x^3 - dx$ et de $y^2 = x^3 + dDx$ sur $\mathbf{Q}$). Dans tous ces exemples, le rang de $E(k)$ est égal à 0 ou 1 et la composante p-primaire du groupe de Shafarevitch-Tate est finie (*cf.* [1]). De plus $\langle\ ,\ \rangle_{v,p}$ (ainsi que $\ll\ ,\ \gg_{v_\infty,p}$) est non nulle car la hauteur d'un point qui n'est pas de torsion est non nulle grâce à [2]. Donc r_{D_α} et t_k sont égaux par la proposition 16, (ii) et on a donc

$$r_{D_\alpha} = \Lambda_{D_\alpha/k}\text{-rang de } \widehat{S_p(D_\alpha)} = \begin{cases} 1 & \text{si } \varepsilon_p = -1 \\ 0 & \text{si } \varepsilon_p = 1 \end{cases}.$$

Dans tous les exemples précédents, en appliquant la proposition 13, on trouve que $\mathscr{T}_p(E/D_\infty)$ est une unité c'est-à-dire que le sous $\Lambda_{D_\infty/k}$-module de torsion de $\widehat{S_p(D_\infty)}$ est fini.

Donnons des exemples dans le cas où le corps F est le corps de multiplication complexe K de E. Soit la courbe $y^2=x^3-226x$ et $p=5$. Le corps K est $\mathbb{Q}(\sqrt{-1})$. Le rang de $E(\mathbb{Q})$ est 3 et on montre de la même manière que $\mathscr{T}_p(E/D_\infty)(\rho^s)$ est égale à s^4 à une unité près. Pour la courbe $y^2=x^3+3x$, $p=5$, on a $t_K=2$. Le calcul numérique montre que $\mathscr{T}_p(E/D_\infty)$ est une unité. Mais $\widehat{S_p(D_\infty)}$ n'a pas de sous-modules finis non nuls grâce à [8] (le $\Lambda_{K_\infty/K}$-module $\widehat{S_p(k_\infty)}$ est de dimension projective inférieure à 1 et $\widehat{S_p(D_\infty)}$ est égal à $\widehat{S_p(k_\infty)}_{G(k_\infty/D_\infty)}$). Donc $\widehat{S_p(D_\infty)}$ est sans torsion et même libre car $\widehat{S_p(D_\infty)}_{G(D_\infty/K)}$ est isomorphe à $\mathbb{Z}_p$. En particulier, si $Ш(D_n)(p)$ est fini pour tout n, le rang de $E(D_n)$ tend vers l'infini et $Ш(D_n)(p)$ est nul ainsi que $Ш(D_\infty)(p)$.

3. Points de Heegner et $\mathbb{Z}_p$-extensions

3.1. Généralités [4]

Soit k un corps quadratique imaginaire de discriminant D. Soit $\mathcal{O}$ l'anneau des entiers de k et si c est un entier positif, on note $\mathcal{O}_c$ l'ordre de $\mathcal{O}$ de conducteur c; on a donc $\mathcal{O}_c=\mathbb{Z}+c\mathcal{O}$. Soit H_c le Ringklassenkörper de k de conducteur c. Le groupe de Galois de H_c sur k est donc isomorphe au groupe des classes Pic $(\mathcal{O}_c)$ de $\mathcal{O}_c$. En particulier, $H=H_1$ est le corps de Hilbert de k.

Soit N un entier positif. On suppose vérifiée la condition qui assure l'existence de points de Heegner :

Il existe un $\mathcal{O}_c$-idéal $\mathcal{N}$ contenu dans $\mathcal{O}_c$ tel que $\mathcal{O}_c/\mathcal{N}$ soit cyclique d'ordre N.

Lorsque N est premier à c, cette condition est équivalente à :

Il existe un $\mathcal{O}$-idéal $\mathcal{N}$ contenu dans $\mathcal{O}$ tel que $\mathcal{O}/\mathcal{N}$ soit cyclique d'ordre N.

Cela est encore équivalent à :

Tout diviseur premier l de $\mathcal{N}$ se décompose dans k ou se ramifie et dans ce dernier cas l^2 ne divise pas $\mathcal{N}$.

Nous ferons en fait l'hypothèse :

HYPOTHÈSE DE HEEGNER. — *Tout diviseur premier de N se décompose dans k.*

Si $\mathfrak{A}$ est un $\mathcal{O}_c$-idéal propre et si $\sigma_{\mathfrak{A}}$ désigne son image dans Pic $(\mathcal{O}_c)$, l'élément de $X_0(N)$ $(\mathbb{C})$ défini comme la classe d'isomorphismes de l'isogénie cyclique de degré N

$$\mathbb{C}/\mathfrak{A} \to \mathbb{C}/N^{-1}\mathfrak{A}$$

appartient en fait à $X_0(N)$ (H_c) et est noté

$$[\mathcal{O}_c, N, [\mathfrak{A}]].$$

C'est un point de Heegner de niveau c. L'action de l'automorphisme complexe τ est donnée par

$$[\mathcal{O}_c, N, [\mathfrak{A}]]^{\tau} = [\mathcal{O}_c, N^{\tau}, [\mathfrak{A}]^{-1}],$$

celle du groupe de Galois de H_c/k est donnée par

$$[\mathcal{O}_c, N, [\mathfrak{A}]]^{\sigma_{\mathfrak{B}}} = [\mathcal{O}_c, N, [\mathfrak{A}\mathfrak{B}^{-1}]]$$

si $\sigma_{\mathfrak{B}}$ est l'élément du groupe de Galois de H_c/k associé à l'$\mathcal{O}_c$-idéal propre $\mathfrak{B}$.

Soit y_c l'image de l'un des points de Heegner $[\mathcal{O}_c, N, [\mathfrak{A}]]$ dans la jacobienne $J_0(N)$ de $X_0(N)$:

$$y_c = ([\mathcal{O}_c, N, [\mathfrak{A}]]) - (\infty)$$

où (∞) désigne la classe dans $X_0(N)$ de la pointe à l'infini. On notera $2u$ le cardinal des racines de l'unité de k et on pose

$$\delta = \begin{cases} u & \text{si } c = 1 \\ 1 & \text{si } c \neq 1 \end{cases}.$$

PROPOSITION 1. — *Soit y_c un point de Heegner de niveau c. Alors, si $T(p)$ est l'opérateur de Hecke agissant sur $J_0(N)$,*

(i) *si* $(p, c)=1$, *on a*

$$T(p)y_c=\begin{cases}\delta\,\mathrm{tr}_{H_{cp}/H_c}(y_{cp}) & \text{si } p \text{ est inerte dans } k.\\ \delta\,\mathrm{tr}_{H_{cp}/H_c}(y_{cp})+\sigma_{\mathfrak{p}}y_c & \text{si } p \text{ est ramifié dans } k : p=\mathfrak{p}^2\\ \delta\,\mathrm{tr}_{H_{cp}/H_c}(y_{cp})+\sigma_{\mathfrak{p}}y_c+\sigma_{\mathfrak{p}^*}y_c & \text{si } p \text{ se décompose dans } k : p=\mathfrak{p}\mathfrak{p}^*.\end{cases}$$

(ii) *Si* p *divise* c, *il existe un point de Heegner* $y_{c/p}$ *de niveau* c/p *tel que*

$$T(p)y_c=y_{c/p}+\mathrm{tr}_{H_{cp}/H_c}(y_{cp}).$$

3.2. $\mathbb{Z}_p$-EXTENSIONS ET CORPS DE CLASSES

Fixons désormais un entier c et un nombre premier p premier à cN. Considérons la tour d'extensions de k formée des H_{cp^n} pour $n\geqslant 0$ et soit H_{cp^∞} la réunion des H_{cp^n}. Par la théorie du Ringklassenkörper, le groupe de Galois de H_{cp^∞}/H_{cp} est isomorphe à $\mathbb{Z}_p$. Rappelons quelques formules de nombres de classes. Soit $h(\mathcal{C}_m)$ le nombre de classes de $\mathcal{C}_m$. On a

$$h(\mathcal{C}_m)=h\frac{m}{[\mathcal{C}^\times:\mathcal{C}_m^\times]}\prod_{l\mid m}\left(1-\left(\frac{D}{l}\right)\frac{1}{l}\right)$$

si h est $h(\mathcal{C})$. Remarquons que

$$[\mathcal{C}^\times:\mathcal{C}_m^\times]=\begin{cases}u & \text{si } m\neq 1\\ 1 & \text{si } m=1\end{cases}.$$

En particulier, on a

$$\frac{h(\mathcal{C}_{cp})}{h(\mathcal{C}_c)}=\begin{cases}p-\left(\dfrac{D}{p}\right) & \text{si } c\neq 1\\ \dfrac{1}{u}\left(p-\left(\dfrac{D}{p}\right)\right) & \text{si } c=1.\end{cases}\tag{1}$$

Le groupe de Galois de H_{cp^∞}/k admet donc un quotient isomorphe à $\mathbb{Z}_p$. Soit D_∞ la $\mathbb{Z}_p$-extension de k correspondante. C'est l'unique $\mathbb{Z}_p$-extension de k prodiédrale sur $\mathbb{Q}$, c'est-à-dire telle que l'automorphisme non trivial τ de $G(k/\mathbb{Q})$ agit sur $G(D_\infty/k)$ par $\sigma\to\sigma^{-1}$. En général, H_{cp} et D_∞ ne

sont pas linéairement disjointes sur k. On pose pour $n \geqslant 0$

$$D_n = H_{cp^n} \cap D_\infty.$$

Alors $G(H_{cp^n}/D_n)$ est isomorphe à $G(H_{cp}/D_1)$ et le degré de D_n sur D_1 est p^{n-1}. Lorsque p est non ramifié dans k, D_1 et D_0 sont égales. Lorsque p ne divise pas le nombre de classes de k, D_1 (resp. D_0) est égal à k lorsque p ne se ramifie pas dans k (resp. lorsque p se ramifie dans k). En effet, dans toute sous-extension de H_c/H_1, il existe au moins une place ne divisant pas p et se ramifiant. Par contre, on peut montrer que si $k = \mathbb{Q}(\sqrt{-23})$ et si p est égal à 3, H_1 est contenue dans D_∞. Enfin, comme nous l'avons déjà dit, le groupe de Galois de H_{cp^∞}/H_{cp} est isomorphe à $\mathbb{Z}_p$. Lorsque p est non ramifié, c'est le plus grand sous-groupe de $G(H_{cp^\infty}/k)$ isomorphe à $\mathbb{Z}_p$. Lorsque p est ramifié et $p>3$ l'extension H_{cp^∞}/H_c est aussi une $\mathbb{Z}_p$-extension. Il suffit de montrer pour cela que $G(H_{cp^n}/H_c)$ est cyclique d'ordre p^n. Or, par la théorie du corps de classes, ce groupe de Galois est isomorphe à

$$(\mathcal{O}/p^n\mathcal{O})^\times/(\mathbb{Z}/p^n\mathbb{Z})^\times \quad \text{(image des unités globales de } \mathcal{C}_c),$$

qui est d'ordre p^n et engendré par

$$1+\sqrt{D} \qquad (\text{car } \operatorname{ord}_p(\sqrt{D}) > \operatorname{ord}_p(p)/(p-1)).$$

Nous supposerons désormais p strictement supérieur à 3 si p est ramifié dans k car pour $p=2$ et 3, il peut se produire que H_{cp^∞}/H_c n'est pas une $\mathbb{Z}_p$-extension; cependant, la modification à faire est minime mais augmenterait les notations (l'hypothèse est en fait que H_{cp^∞}/H_c est une $\mathbb{Z}_p$-extension si p est ramifié dans k).

Finalement, nous noterons $\Gamma = G(D_\infty/k)$.

3.3. Points de Heegner relatifs a la $\mathbb{Z}_p$-extension D_∞/k

Fixons une courbe elliptique E définie sur $\mathbb{Q}$, de conducteur N tel qu'il existe un morphisme de degré fini de $X_0(N)$ dans E rationnel sur $\mathbb{Q}$ que l'on peut supposer de degré minimal et notons e_{cp^n} l'image de y_{cp^n} dans

$E(H_{cp^n})$. Soit a_p la trace de l'endomorphisme de Frobenius sur $E/\mathbb{Q}$ modulo p. L'opérateur de Hecke $T(p)$ sur $J_0(N)$ correspond à la multiplication par a_p sur les points de E. On réécrit alors la proposition 1.

LEMME 2. — *Soit b_p l'élément de $\mathbb{Z}_p[G(H_c/k)]$ défini par*

$$b_p = \begin{cases} a_p & \text{si } p \text{ est inerte} \\ a_p - \sigma_{\mathfrak{p}} & \text{si } (p) = \mathfrak{p}^2 \\ a_p - \sigma_{\mathfrak{p}} - \sigma_{\mathfrak{p}^*} & \text{si } (p) = \mathfrak{p}\mathfrak{p}^*, \quad \mathfrak{p} \neq \mathfrak{p}^*. \end{cases}$$

On a alors les relations

(i) $a_p e_{cp^{n+1}} = e_{cp^n} + \mathrm{tr}_{H_{cp^{n+2}}/H_{cp^{n+1}}}(e_{cp^{n+2}})$ *pour* $n \geqslant 0$;

(ii) $b_p e_c = \delta \, \mathrm{tr}_{H_{cp}/H_c}(e_{cp})$.

PROPOSITION 3. — 1. *Il existe des éléments γ_n de $\mathbb{Z}_p[G(H_c/k)]$ tels que*

$$\mathrm{tr}_{H_{cp^n}/H_c}(e_{cp^n}) = \delta^{-1} \gamma_n e_c$$

avec

$$\gamma_0 = \delta$$

$$\gamma_1 = b_p$$

$$\gamma_2 = a_p \gamma_1 - \delta_c \delta$$

$$\gamma_n = a_p \gamma_{n-1} - p \gamma_{n-2} \qquad \text{pour} \quad n \geqslant 3$$

(on a posé $\delta_c = [H_{cp} : H_c]$).

2. *Si p est non ramifié dans k et si ξ est un caractère non trivial de*

$$\Delta_c' = G(H_{cp}/H_c),$$

il existe des éléments β_n de $\mathbb{Z}_p$ (indépendants de ξ) tels que

$$\mathrm{tr}_{H_{cp^n}/H_{cp}}\left(\sum_{\sigma \in \Delta_c'} \xi(\sigma)\, \sigma\, e_{cp^n}\right) = \beta_n \sum_{\sigma \in \Delta_c'} \xi(\sigma)\, \sigma\, e_{cp}$$

avec

$$\beta_1 = 1$$

$$\beta_2 = a_p$$

$$\beta_3 = a_p \beta_{n-1} - p \beta_{n-2} \qquad \text{pour} \quad n \geqslant 3.$$

Cette proposition se déduit facilement du lemme 2.

Nous allons maintenant étudier les éléments γ_n et exploiter les relations de récurrence. Disons un mot du but recherché. On désire calculer « l'indice » de la trace de H_{cp^n} à H_c du $\mathbb{Z}_p[G(H_{cp^n}/k)]$-module engendré par e_{cp^n} dans le $\mathbb{Z}_p[G(H_c/k)]$-module engendré par e_c et de le comparer à certains facteurs d'Euler généralisés.

Plus précisément, l'extension H_c/k est non ramifiée aux places divisant p. Aussi le groupe fini

$$\tilde{E}_p(\widetilde{H_c \otimes_{\mathbb{Q}} \mathbb{Q}_p})(p) = \prod_{v \mid p} \tilde{E}_v(\tilde{H}_{c,\,v})(p)$$

(où le produit est pris sur les places v de H_c au-dessus de p) est muni canoniquement d'une structure de $\mathbb{Z}_p[G(H_c/k)]$-module; on peut le décrire plus canoniquement comme

$$\prod_{\mathfrak{p} \mid p} \tilde{E}_{v_\mathfrak{p}}(\tilde{H}_{c,\,v_\mathfrak{p}})(p) \otimes_{\mathbb{Z}_p[G(H_c/k)_{v_\mathfrak{p}}]} \mathbb{Z}_p[G(H_c/k)]$$

où $\mathfrak{p}$ parcourt les places de k au-dessus de p et où $v_\mathfrak{p}$ est une place fixée de H_c au-dessus de $\mathfrak{p}$. Il est annulé par l'élément suivant de $\mathbb{Z}_p[G(H_c/k)]$:

$$\Phi_p = \prod_{\mathfrak{p} \mid p} (N\mathfrak{p} - a_{N\mathfrak{p}}\,\sigma_\mathfrak{p} + \sigma_\mathfrak{p}^2)$$

si $\sigma_\mathfrak{p}$ est l'automorphisme d'Artin associé à $\mathfrak{p}$ dans $G(H_c/k)$. Plus explicitement, on a

$$(2)\quad \Phi_p = \begin{cases} p^2 - a_{p^2} + 1 = p^2 + 1 + p - a_p^2 & \text{si } p \text{ est inerte} \\ p - a_p\sigma_\mathfrak{p} + \sigma_\mathfrak{p}^2 & \text{si } (p) = \mathfrak{p}^2 \\ (p - a_p\sigma_\mathfrak{p} + \sigma_\mathfrak{p}^2)(p - a_p\sigma_{\mathfrak{p}^*} + \sigma_{\mathfrak{p}^*}^2) & \text{si } (p) = \mathfrak{p}\mathfrak{p}^*,\quad \mathfrak{p} \neq \mathfrak{p}^*. \end{cases}$$

Remarquons que dans le cas décomposé, $\sigma_{\mathfrak{p}^*}$ est égal à $\sigma_\mathfrak{p}^{-1}$.

Posons

$$\Phi'_p = \begin{cases} p^2 + 1 + 2p - a_p^2 & \text{si } p \text{ est inerte dans } k \\ \Phi_p & \text{sinon.} \end{cases}$$

On vérifie facilement que l'on a

$$\Phi'_p = \prod_{\mathfrak{p} \mid p} (\sigma_\mathfrak{p} - \alpha_{N\mathfrak{p}})(\sigma_\mathfrak{p} - \beta_{N\mathfrak{p}})$$

où α_p et β_p sont les racines du polynôme

$$X^2 - a_p X + p$$

et où α_{p^r} et β_{p^r} sont définis par multiplicativité. En particulier,

$$\Phi'_p \sim \prod_{\mathfrak{p} \mid p} \left(1 - \frac{\sigma_{\mathfrak{p}}}{\alpha_{N\mathfrak{p}}}\right)$$

si a_p est une unité et α_p la racine qui est une unité. C'est Φ'_p qui intervient naturellement dans le calcul des γ_n. On vérifie cependant facilement que Φ_p et Φ'_p ont même valuation p-adique (lorsque a_p est une unité) : le cas non trivial est celui où $a_p{}^2 \equiv 1 \bmod p$ et les inégalités de Weil impliquent alors que $a_p{}^2$ vaut 1; il suffit alors de calculer Φ_p et Φ'_p.

LEMME 4. — *Les éléments γ_n de $\mathbb{Z}_p[G(H_c/k)]$ vérifient*

$$\gamma_n = q_n \Phi'_p + p^{n-1} r_n$$

où q_n et r_n appartiennent à $\mathbb{Z}_p[G(H_c/k)]$ et où les q_n vérifient

$$q_{n+1} \equiv a_p q_n \text{ modulo } p \qquad \textit{pour} \quad n \geqslant 2.$$

et

$$q_2 = \begin{cases} \varepsilon(p) & \textit{si } p \textit{ est non ramifié} \\ a_p \sigma_{\mathfrak{p}}^{-1} & \textit{si } p \textit{ est ramifié.} \end{cases}$$

Démonstration. — La démonstration se fait par récurrence en utilisant la proposition 3.

Nous donnerons seulement les valeurs ou les relations vérifiées par r_n :

1. *Cas inerte*

$$r_{2n} = (p+1)$$

$$r_{2n+1} = a_p$$

$$q_2 = -1$$

$$q_{n+1} \equiv a_p q_n \text{ modulo } p \qquad (n \geqslant 2).$$

2. *Cas décomposé*

$$r_n = s_n(p - a_p \sigma_{\mathfrak{p}} + \sigma_{\mathfrak{p}}^2) + \sigma_{\mathfrak{p}}^{-(n-1)}(a_p - \sigma_{\mathfrak{p}} - \sigma_{\mathfrak{p}}^{-1})$$

avec

$$s_{n+1} = \sigma_p s_n - \sigma_p^{-(n-1)} \qquad \text{et} \qquad s_1 = 0$$

$$q_{n+1} \equiv a_p q_n \text{ modulo } p \qquad (n \geqslant 2)$$

$$q_2 = 1.$$

3. *Cas ramifié*

$$r_n = p\,\sigma_p^{-n} \qquad (n \geqslant 1)$$

$$q_1 = \sigma_p^{-1}$$

$$q_{n+1} \equiv a_p q_n \bmod p \qquad (n \geqslant 1).$$

COROLLAIRE 5. — *Si a_p est une unité de $\mathbb{Z}_p$ et si M est un $\mathbb{Z}_p[G(H_c/k)]$-module de type fini compact, l'intersection des $\gamma_n M$ pour $n \geqslant 2$ est égale à $\Phi'_p M$.*

On déduit aussi du lemme 2 les relations suivantes

$$\text{(3)} \qquad \operatorname{tr}_{H_{cp^{n+k}}/H_{cp^k}}(e_{cp^{n+k}}) = \beta_{n+1} e_{cp^k} - \beta_n e_{cp^{k-1}}$$

pour $k \geqslant 1$ où les β_n vérifient les relations de récurrence

$$\beta_0 = 0$$

$$\beta_1 = 1$$

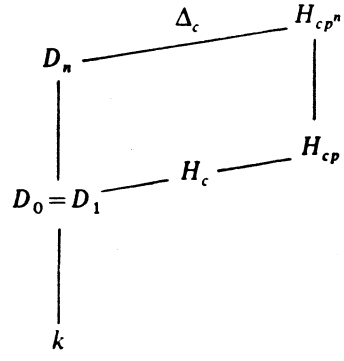
$$\beta_n = a_p \beta_{n-1} - p\,\beta_{n-2} \qquad (n \geqslant 2)$$

(ce sont donc les mêmes que ceux de la proposition 3). On montre facilement que si a_p est une unité, les entiers β_n sont des unités en p pour $n \geqslant 1$.

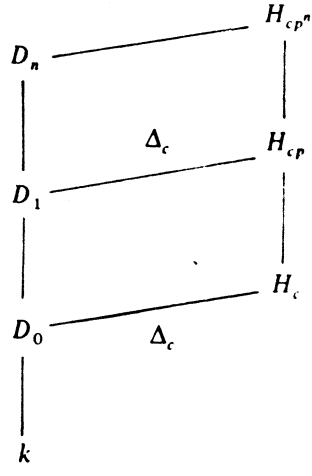
3.4. MODULES D'IWASAWA ASSOCIÉS AUX POINTS DE HEEGNER

Nous allons dans ce paragraphe donner la construction détaillée du module $\mathbf{H}_\infty$ qui intervient dans les conjectures du premier paragraphe. Un peu plus généralement, nous construirons des modules $\mathscr{H}_{\infty,c}^{(\xi)}$ dépendant d'un caractère ξ et d'un entier c (premier à p), le cas particulier $\mathbf{H}_\infty$ étant obtenu pour $c = 1$ et pour ξ caractère trivial.

Rappelons les diagrammes suivants de corps



Cas non ramifié



Cas ramifié

On posera

$$\Delta_c = G(H_{cp}/D_1)$$

$$\Delta_c' = \begin{cases} G(H_{cp}/H_c) & \text{si } p \text{ est non ramifié} \\ 1 & \text{si } p \text{ est ramifié} \end{cases}$$

(l'ordre de Δ_c' est donc toujours premier à p).

Pour simplifier, nous supposerons désormais que l'on est dans une des deux situations suivantes :

(i) $G(H_{cp}/k)$ est le produit direct de $G(D_1/k)$ avec Δ_c et ξ est un caractère de Δ_c (prolongé par le caractère trivial sur $G(D_1/k)$)

(ii) ξ est le caractère trivial de $G(H_{cp}/D_1)$.

On notera $\mathbb{Z}_p[\xi]$ l'anneau obtenu en rajoutant à $\mathbb{Z}_p$ les valeurs du caractère ξ et $\Lambda_{D_\infty/k}^{(\xi)} = \mathbb{Z}_p[\xi][[G(D_\infty/k)]]$.

Dans le cas (i), le groupe $G(H_{cp^n}/k)$ se décompose aussi en produit direct

$$G(H_{cp^n}/k) = G(D_n/k) \times \Delta_c;$$

si M est un $\mathbb{Z}_p[G(H_{cp^n}/k)]$-module et m un élément de M, on pose

$$m_\xi = \sum_{\sigma \in \Delta_c} \xi(\sigma)\, \sigma m.$$

Si $M^{(\xi)}$ *est le* $\mathbb{Z}[\xi]$-module engendré par les éléments m_ξ pour m appartenant à M, on considère $M^{(\xi)}$ comme un $\mathbb{Z}_p[\xi][G(D_n/k)]$-module grâce à cette décomposition. D'autre part, si ξ est trivial sur Δ_c' et si γ est un élément de $\mathbb{Z}_p[G(H_c/k)]$, on note $\gamma(\xi)$ l'image de γ dans $\mathbb{Z}_p[\xi][G(D_0/k)]$ par le $\mathbb{Z}_p$-homomorphisme induit par

$$G(H_c/k) = G(D_0/k) \times \Delta_c/\Delta_c' \to \mathbb{Z}_p[\xi][G(D_0/k)]$$
$$(\sigma, \tau) \mapsto \xi(\tau)\sigma$$

Enfin, on appelera cas I le cas où ξ est trivial sur Δ_c' et cas II le cas où ξ n'est pas trivial sur Δ_c'. Ce dernier cas ne peut se produire que si p est non ramifié (dans k) et l'entier n sera alors toujours supérieur ou égal à 1.

Considérons maintenant le $\mathbb{Z}_p[GH_{cp^n}/k)]$-module $\mathscr{H}'_{n,c}$ engendré par e_{cp^n} pour $n \geqslant 0$. Notons $\mathscr{H}'^{(\xi)}_{n,c}$ le $\mathbb{Z}_p[\xi][G(D_n/k)]$-module engendré par $e_{cp^n,\xi}$ pour $n \geqslant 1$ et par

$$e_{c,\xi} = \sum_{\sigma \in G(H_c/D_0)} \xi(\sigma)\sigma e_c$$

pour $n = 0$ (uniquement dans le cas (II); la notation est abusive puisqu'elle n'a pas toujours la même signification que pour $e_{cp^n,\xi}$ avec $n \geqslant 1$:

$$e_{cp^n,\xi} = \sum_{\sigma \in G(H_{cp}/D_1)} \xi(\sigma)\sigma e_{cp^n}).$$

D'autre part, dans le cas où ξ est le caractère trivial, on notera aussi les objets correspondant par des lettres grasses : $\mathbf{H}_{n,c}$, $\mathbf{H}_{\infty,c}$.

D'après (3), on a

$$\mathrm{tr}_{D_n/D_l}(\mathscr{H}'^{(\xi)}_{n,c}) \subset \mathscr{H}'^{(\xi)}_{l,c} + \mathscr{H}'^{(\xi)}_{l-1,c}$$

On pose

$$\mathscr{H}_{n,c} = \sum_{0 \leqslant l \leqslant n} \mathscr{H}'_{l,c}$$
$$\mathscr{H}^{(\xi)}_{n,c} = \sum_{0 \leqslant l \leqslant n} \mathscr{H}'^{(\xi)}_{l,c}$$

On a alors le lemme.

LEMME 6. — *La trace de* D_m *sur* D_n *induit un morphisme de* $\mathscr{H}^{(\xi)}_{m,c}$ *dans* $\mathscr{H}^{(\xi)}_{n,c}$.

Soit $\mathscr{H}^{(\xi)}_{\infty,\,c}$ la limite projective des $\mathscr{H}^{(\xi)}_{n,\,c}$ relativement aux morphismes de trace. C'est un sous-$\Lambda^{(\xi)}_{D_\infty/k}$-module de $\tilde{S}(H_{cp^\infty})^{(\xi)}$. En particulier, il est sans torsion par le lemme 5, paragraphe 2. Nous désirons maintenant calculer le module de ses coinvariants par $G(D_\infty/k)$ afin de calculer son $\Lambda^{(\xi)}_{D_\infty/k}$-rang.

LEMME 7. — *On a*

$$\bigcap_{n\geq 1} \mathrm{tr}_{D_n/k}(\mathscr{H}^{(\xi)}_{n,\,c}) = \begin{cases} \mathscr{E}'_{p,\,\xi}\,\mathbb{Z}_p[\xi]\,\mathrm{tr}_{D_0/k}(e_{c,\,\xi}) & (\textit{cas I}) \\ \mathbb{Z}_p[\xi]\,\mathrm{tr}_{D_1/k}(e_{cp,\,\xi}) & (\textit{cas II}) \end{cases}$$

où $\mathscr{E}'_{p,\,\xi}$ est l'image par ξ de Φ'_p (dans $\mathbb{Z}_p[\xi]$) dans le cas I.

Démonstration. — On a

$$\bigcap_{n\geq 1} \mathrm{tr}_{D_n/D_0}(\mathscr{H}^{(\xi)}_{n,\,c}) = \begin{cases} \bigcap_{n\gg 0} \gamma_n(\xi)\,\mathscr{H}^{(\xi)}_{0,\,c} & (\text{cas I}) \\ \bigcap_{n\gg 0} \beta_n\,\mathscr{H}^{(\xi)}_{1,\,c} & (\text{cas II}) \end{cases}$$

(proposition 3). D'après le corollaire 5 et la remarque qui suit concernant les β_n, cela vaut

$$\begin{cases} \Phi'_p(\xi)\,\mathscr{H}^{(\xi)}_{0,\,c} & (\text{cas I}) \\ \mathscr{H}^{(\xi)}_{1,\,c} & (\text{cas II}). \end{cases}$$

La projection de l'élément $\Phi'_p(\xi)$ de $\mathbb{Z}_p[\xi][G(D_0/k)]$ dans $\mathbb{Z}_p[\xi]$ (par l'homomorphisme

$$\sigma \in G(D_0/k) \mapsto 1)$$

est $\mathscr{E}'_{p,\,\xi}$. D'où le lemme 7.

Remarque. — Lorsque ξ est le caractère trivial, le lemme 7 devient

$$\bigcap_{n\geq 1} \mathrm{tr}_{D_n/k}(\mathbf{H}_n) = \mathscr{E}_p\,\mathbb{Z}_p\,\mathrm{tr}_{H_c\,k}(e_c)$$

où $\mathscr{E}_p$ est le facteur d'Euler en p usuel :

$$\mathscr{E}_p = \#(\textstyle\prod_{\mathfrak{p}\mid p} \tilde{E}_{\mathfrak{p}}(\tilde{k}_{\mathfrak{p}})(p))$$

(le produit est pris sur les places $\mathfrak{p}$ de k au-dessus de p).

Les $\mathbb{Z}_p[\xi]$-modules $\mathscr{H}^{(\xi)}_{n,\,c}$ étant compacts, l'homomorphisme naturel

$$\mathscr{H}^{(\xi)}_{\infty,\,c} \to \bigcap_n \mathrm{tr}_{D_n/k}(\mathscr{H}^{(\xi)}_{n,\,c})$$

est surjectif et se factorise par $(\mathscr{H}^{(\xi)}_{\infty,c})_{G(D_\infty/k)}$. Nous allons commencer par étudier un cas où cette factorisation est un isomorphisme.

PROPOSITION 8. — *Supposons que* $\mathrm{tr}_{D_0/k}(e_{c,\xi})$ *dans le cas* (I) (*resp.* $\mathrm{tr}_{D_1/k}(e_{cp,\xi})$ *dans le cas* II) *est d'ordre infini. Alors l'homomorphisme*

$$(\mathscr{H}^{(\xi)}_{\infty,c})_{G(D_\infty/k)} \to \bigcap_n \mathrm{tr}_{D_n/k}(\mathscr{H}^{(\xi)}_{n,c})$$

est un isomorphisme (de $\mathbb{Z}_p[\xi]$*-modules).*

Démonstration. — Nous ne donnerons les détails de la démonstration que dans le cas (I) et nous oublierons le c et le ξ dans les notations. L'homomorphisme considéré est simplement

$$(x_n) \to \mathrm{tr}_{D_0/k} x_0 \qquad (= \mathrm{tr}_{D_n/k}(x_n) \text{ pour tout } n)$$

(dans le cas non ramifié, on a $D_1 = D_0$ et $x_1 = x_0$). Calculons son noyau. Soit σ un générateur de $G(D_\infty/k)$; nous noterons de la même manière sa projection dans $G(D_n/k)$. Soit (x_n) un élément de $\mathscr{H}_\infty = \varprojlim \mathscr{H}_n$ tel que $\mathrm{tr}_{D_n/k} x_n = 0$. Nous voulons montrer qu'il appartient à $(\sigma-1)\mathscr{H}_\infty$: il suffit pour cela de montrer que x_n appartient à $(\sigma-1)\mathscr{H}_n$ pour tout n. Grâce aux relations (3), on voit que

$$\mathscr{H}_n = \mathscr{H}'_n + \mathscr{H}'_{n-1}$$

et donc on peut écrire

$$x_n = a_n e_{cp^n,\xi} + b_n e_{cp^{n-1},\xi} + (\sigma-1) z_n$$

avec a_n et b_n dans $\mathbb{Z}_p[\xi]$ et z_n dans $\mathscr{H}_n$. Notons δ_n la projection de $\gamma_n(\xi)$ dans $\mathbb{Z}_p[\xi]$. On a donc

$$\mathrm{tr}_{D_n/k}(e_{cp^n,\xi}) = \delta_n \mathrm{tr}_{D_0/k}(e_{c,\xi});$$

grâce à l'hypothèse que $\mathrm{tr}_{D_0/k}(e_{c,\xi})$ est d'ordre infini, la relation

$$\mathrm{tr}_{D_n/k}(x_n) = 0$$

se traduit par

$$a_n \delta_n + p b_n \delta_{n-1} = 0.$$

D'où

$$\delta_n x_n = b_n(-p\delta_{n-1} e_{cp^n,\xi} + \delta_n e_{cp^{n-1},\xi}) + (\sigma-1) z_n. \tag{4}$$

L'élément

$$h_n = -p\,\delta_{n-1}\,e_{cp^n,\xi} + \delta_n\,e_{cp^{n-1},\xi}$$

de $\mathscr{H}_n$ vérifie

(5) $\qquad \mathrm{tr}_{D_n D_{n-1}}(h_n) = p h_{n-1} \qquad$ pour n assez grand

(par exemple $n \geqslant 3$) grâce aux relations vérifiées par les δ_n :

$$\delta_n = a_p\,\delta_{n-1} - p\,\delta_{n-2}.$$

Finalement, comme δ_n est de valuation constante pour n assez grand (par le lemme 4), que l'on a

$$\mathrm{tr}_{D_{n+k} D_n}(x_{n+k}) = x_n,$$

on montre grâce à (4) et (5) que, pour tout $k \gg 0$, x_n appartient à

$$(p^{k-k_0}, \sigma - 1)\,\mathscr{H}_n$$

où k_0 ne dépend pas de k. Donc x_n appartient à $(\sigma-1)\,\mathscr{H}_n$, ce qui montre que x_∞ appartient à $(\sigma-1)\,\mathscr{H}_\infty$ et finit la démonstration de la proposition.

Remarque. — La condition que $\mathrm{tr}_{D_0/k}(e_{c,\xi})$ est d'ordre infini est équivalente à ce que l'annulateur de $e_{c,\xi}$ dans $\mathbb{Z}_p[\xi][G(D_0/k)]$ soit contenu dans l'idéal d'augmentation de $\mathbb{Z}_p[\xi][G(D_0/k)]$ c'est-à-dire dans l'idéal $(\sigma-1)\,\mathbb{Z}_p[\xi][G(D_0/k)]$.

COROLLAIRE 9. — *Sous les hypothèses de la proposition* 8, $\mathscr{H}^{(\xi)}_{\alpha,c}$ *est un* $\Lambda^{(\xi)}_{D_\infty,k}$*-module libre de rang* 1 *et l'on a*

$$(\mathscr{H}^{(\xi)}_{\infty,c})_{G(D_\infty/k)} = \begin{cases} \mathscr{E}'_{p,\xi}\,\mathbb{Z}_p[\xi]\,\mathrm{tr}_{D_0/k}(e_{c,\xi}) \\ \mathbb{Z}_p[\xi]\,\mathrm{tr}_{D_1/k}(e_{cp,\xi}). \end{cases}$$

Démonstration. — Si M est un $\Lambda^{(\xi)}_{D_\infty/k}$-module de type fini sans torsion et tel que M_Γ soit isomorphe à $\mathbb{Z}_p[\xi]$, il est libre de rang 1. En effet, il existe une suite exacte

$$0 \to M \to \Lambda^{(\xi)r}_{D_\infty,k} \to T \to 0$$

avec T fini. On en déduit la suite exacte

$$0 \to T^\Gamma \to M_\Gamma \to \mathbb{Z}_p[\xi]^r \to T_\Gamma \to 0.$$

D'où T^Γ donc T sont nuls et r est égal à 1. On peut appliquer ce résultat à $M=\mathscr{H}^{(\xi)}_{\infty,c}$; le lemme 7 et la proposition 8 permettent de calculer M_Γ.

Nous allons maintenant envisager le cas général.

PROPOSITION 10. — *S'il existe un entier n tel que $e_{cp^n,\xi}$ est d'ordre infini, le $\Lambda^{(\xi)}_{D_\infty/k}$-module $\mathscr{H}^{(\xi)}_{\infty,c}$ est libre de rang 1; il est nul sinon.*

Démonstration. — Toujours pour simplifier les notations, nous nous placerons dans le cas (I). Supposons d'abord qu'il existe un entier n tel que $e_{cp^n,\xi}$ est d'ordre infini et soit l le plus petit de ces entiers. Toujours pour simplifier nous supposerons que $l\geqslant 1$ ($l\geqslant 2$ dans le cas non ramifié) (dans le cas contraire il faudrait introduire les sous-corps intermédiaires de D_0/k). Soit s un entier annulant les points de torsion $e_{cp^n,\xi}$ pour $n<l$. Posons $T_n=s\mathscr{H}^{(\xi)}_{n,c}$ et soit T_∞ la limite projective des T_n. Alors la multiplication par s induit un homomorphisme de $\mathscr{H}^{(\xi)}_{\infty,c}$ dans T_∞ surjectif par la compacité des T_n et injectif car $\mathscr{H}^{(\xi)}_{\infty,c}$ n'a pas de $\Lambda^{(\xi)}_\Gamma$-torsion. C'est donc un isomorphisme. C'est donc T_∞ que nous étudierons et pour s'implifier les notations, nous supposerons en fait que $s=1$ (sinon, il faudrait multiplier toutes les relations par s). Les relations (3) deviennent en particulier

$$\mathrm{tr}_{D_{n+l}/D_l}(e_{cp^{n+l},\xi})=\beta_n e_{cp^l,\xi}$$

et β_n est une unité de $\mathbb{Z}_p$. Donc $e_{cp^l,\xi}$ appartient à l'intersection des traces de D_{n+l} à D_l de T_{n+l} et il existe un élément y_∞ de T_∞ tel que si $y_\infty=(y_l)$, $y_l=e_{cp^l,\xi}$. Remarquons d'autre part que T_n est nul pour $n<l$. Soit $\mathscr{M}=(p,\sigma-1)$ l'idéal maximal de $\Lambda^{(\xi)}_\Gamma$ (où σ est un générateur topologique de $G(D_\infty/k)$). Nous allons montrer que $T_\infty=\Lambda^{(\xi)}_\Gamma y_\infty+\mathscr{M}T_\infty$. On en déduira par le lemme de Nakayama que T_∞ est égal à $\Lambda^{(\xi)}_\Gamma y_\infty$. Un $\Lambda^{(\xi)}_\Gamma$-module compact de type fini sans torsion et monogène étant libre de rang 1, on en déduira la proposition.

Considérons donc un élément $t_\infty=(t_n)$ de T_∞. Nous allons montrer que t_n appartient à $\mathbb{Z}_p[\xi][G(D_n/k)]y_n+\mathscr{M}T_n$. La démonstration est tout à fait semblable à celle de la proposition 8. Comme $T_l=\mathbb{Z}_p[\xi][G(D_l/k)]y_l$, il existe un élément λ de $\Lambda^{(\xi)}_{D_\infty/k}$ tel que la l-ième composante de $t_\infty-\lambda y_\infty$ soit nulle. Si $s_n=t_n-\lambda y_n$, il suffit donc de montrer que s_n appartient à $\mathscr{M}T_n$. On écrit s_n sous la forme

$$s_n=a_n e_{cp^n,\xi}+b_n e_{cp^{n-1},\xi}+(\sigma-1)r_n$$

avec $a_n \in \mathbb{Z}_p[\xi]$, $b_n \in \mathbb{Z}_p[\xi]$ et $r_n \in T_n$. La relation

$$\mathrm{tr}_{D_n/D_l}(s_n) = 0$$

se traduit donc par

$$(a_n \beta_{n-l} + p b_n \beta_{n-l-1}) e_{cp^l,\xi} + (\sigma - 1)\,\mathrm{tr}_{D_n/D_l}(r_n) = 0.$$

Comme $\mathrm{tr}_{D_n/D_l}(r_n)$ est un multiple de $e_{cp^l,\xi}$ (par un élément de $\Lambda^{(\xi)}_{D_\infty/k}$), on en déduit qu'il existe un élément μ de $\Lambda^{(\xi)}_{D_\infty/k}$ tel que

$$a_n \beta_{n-l} + p b_n \beta_{n-l-1} + (\sigma - 1)\mu$$

appartient à l'annulateur de $e_{cp^l,\xi}$.

Comme $e_{cp^l,\xi}$ est d'ordre infini, celui-ci est contenu dans l'idéal maximal $\mathcal{M}$ de $\Lambda^{(\xi)}_{D_\infty/k}$. On en déduit donc facilement que

$$s_n \equiv \frac{b_n}{\beta_{n-l}} h_n \text{ modulo } \mathcal{M}\, T_n$$

avec $h_n = -p\,\beta_{n-l-1}\, e_{cp^n,\xi} + \beta_{n-l} e_{cp^{n-1},\xi}$

En utilisant le fait que

$$\mathrm{tr}_{D_{n+1}/D_n}(h_{n+1}) = p h_n$$

et que

$$\mathrm{tr}_{D_{n+1}/D_n}(s_{n+1}) = s_n,$$

on voit que s_n appartient à $\mathcal{M}\, T_n$, ce qu'il fallait démontrer.

Pour la seconde partie de la proposition, on remarque que le sous-$\mathbb{Z}$-module de torsion de $E(H_{cp^\infty})$ est fini. Comme $\mathcal{H}^{(\xi)}_{\infty,c}$ est sans torsion, il ne peut être que nul.

Remarque. — On a toujours une surjection

$$(\mathcal{H}^{(\xi)}_{\infty,c})_{G(D_\infty/D_l)} \longrightarrow \bigcap_{n \geq l} \mathrm{tr}_{D_n/D_l}(S\mathcal{H}^{(\xi)}_{n,c}) = S\mathcal{H}^{(\xi)}_{l,c}$$

On en déduit une surjection

$$(\mathcal{H}^{(\xi)}_{\infty,c})_{G(D_\infty/k)} \to (S\mathcal{H}^{(\xi)}_{l,c})_{G(D_l/k)}.$$

Ce dernier $\mathbb{Z}_p[\xi]$-module est en fait isomorphe à $\mathbb{Z}_p[\xi]/p\,\mathbb{Z}_p[\xi]$ lorsque les hypothèses de la proposition 8 ne sont pas vérifiées mais que $\mathscr{H}^{(\xi)}_{\infty,c}$ est cependant non nul.

Nous allons maintenant récapituler certains des résultats précédents. Notons $I^{(\xi)}(\mathscr{H}_{\infty,c})$ la série caractéristique du $\Lambda^{(\xi)}_{D_\infty/k}$-module quotient de $\tilde{S}_p(H_{cp^\infty})^{(\xi)}$ par $\mathscr{H}^{(\xi)}_{\infty,c}$. On notera **1** le caractère trivial de $G(D_\infty/k)$ et rappelons que Δ'_c est $G(H_{cp}/H_c)$ si p est non ramifié et 1 si p est ramifié dans k.

PROPOSITION 11. — (i) *Si les points $e_{cp^n,\xi}$ sont de torsion pour tout n, $\mathscr{H}^{(\xi)}_{\infty,c}$ est nul.*

(ii) *Si $\mathrm{tr}_{D_0/k}(e_{c,\xi})$ lorsque ξ est trivial sur Δ'_c (resp. $\mathrm{tr}_{D_1/k}(e_{cp,\xi})$ si ξ est non trivial sur Δ'_c) n'est pas de torsion, $\mathscr{H}^{(\xi)}_{\infty,c}$ est de $\Lambda^{(\xi)}_{D_\infty/k}$-rang 1; si de plus le $\Lambda^{(\xi)}_{D_\infty/k}$-rang de $S_p(H_{cp^\infty})^{(\xi)}$ est égal à 1, on a*

$$I^{(\xi)}(\mathscr{H}_{\infty,c})(\mathbf{1}) \sim \mathscr{E}'_{p,\xi}[\mathbb{Z}_p[\xi]P_{un,\xi} : \mathbb{Z}_p[\xi]\,\mathrm{tr}_{D_0/k}(e_{c,\xi})]$$

(resp.

$$I^{(\xi)}(\mathscr{H}_{\infty,c})(\mathbf{1}) \sim [\mathbb{Z}_p[\xi]P_{un,\xi} : \mathbb{Z}_p[\xi]\,\mathrm{tr}_{D_1/k}(e_{cp,\xi})])$$

où $P_{un,\xi}$ est un générateur de $(\tilde{S}_p(H_{cp^\infty})^{(\xi)})_{G(D_\infty/k)}$.

(iii) *Sinon, le $\Lambda^{(\xi)}_{D_\infty/k}$-module $\mathscr{H}^{(\xi)}_{\infty,c}$ est de rang égal à 1 et si le $\Lambda^{(\xi)}_{D_\infty/k}$-rang de $\tilde{S}_p(H_{cp^\infty})^{(\xi)}$ est aussi égal à 1, on a*

$$I^{(\xi)}(\mathscr{H}_{\infty,c})(\mathbf{1}) = 0$$
$$I^{(\xi)}(\mathscr{H}_{\infty,c}) \neq 0.$$

Nous n'utiliserons dans le paragraphe 4 que le cas où ξ est le caractère trivial. Nous allons réécrire dans ce cas la proposition 11 en modifiant la définition de la série caractéristique $I^{(\xi)}(\mathscr{H}_{\infty,c})$.

Notons $I(\mathbf{H}_{\infty,c})$ la série caractéristique du $\Lambda_{D_\infty/k}$-module quotient de $\tilde{S}_p(D_\infty)$ par $\mathbf{H}_{\infty,c}$ et soit P_{un} un générateur de $\tilde{S}_p(D_\infty)_{G(D_\infty/k)}$. Grâce aux lemmes 4 et 5 du paragraphe 2, c'est un élément de $\check{S}_p(k)$ qui est une norme universelle pour les $\check{S}_p(D_n)$ (*voir* aussi paragraphe 2.5).

PROPOSITION 11'. — (i) *Si les points $\mathrm{tr}_{H_{cp^n}D_n}(e_{cp^n})$ sont de torsion pour tout n, $\mathbf{H}_{\infty,c}$ est nul;*

(ii) *si $\mathrm{tr}_{H_c/k}(e_c)$ n'est pas de torsion, $\mathbf{H}_{\infty,c}$ est libre de $\Lambda_{D_\infty/k}$-rang égal à 1; si le $\Lambda_{D_\infty/k}$-rang de $\tilde{S}_p(D_\infty)$ est aussi égal à 1, on a*

$$I(\mathbf{H}_{\infty,c})(\mathbf{1}) \sim \mathscr{E}_p[\mathbb{Z}_p P_{un} : \mathbb{Z}_p\,\mathrm{tr}_{H_c/k}(e_c)];$$

(iii) *sinon, le* $\Lambda_{D_\infty/k}$*-module* $\mathbf{H}_{\infty,c}$ *est libre de* $\Lambda_{D_\infty/k}$*-rang égal à* 1 *et si le* $\Lambda_{D_\infty/k}$*-rang de* $\tilde{S}_p(D_\infty)$ *est aussi égal à* 1, *on a*

$$I(\mathbf{H}_{\infty,c})(\mathbf{1}) = 0$$
$$I(\mathbf{H}_{\infty,c}) \neq 0.$$

Démonstration de la proposition 11′ (la proposition 11 se démontrant de la même manière). — Compte tenu de la proposition 10, il ne reste plus qu'à calculer $I(\mathbf{H}_{\infty,c})(\mathbf{1})$ en supposant $\mathbf{H}_{\infty,c}$ et $\tilde{S}_p(D_\infty)$ de $\Lambda_{D_\infty/k}$-rang 1. Notons Z_∞ le $\Lambda_{D_\infty/k}$-module défini par la suite exacte

$$0 \to \mathbf{H}_{\infty,c} \to \tilde{S}_p(D_\infty) \to Z_\infty \to 0.$$

On en déduit la suite exacte de $\mathbb{Z}_p$-modules

$$0 \to Z_\infty^\Gamma \to (\mathbf{H}_{\infty,c})_\Gamma \to \tilde{S}_p(D_\infty)_\Gamma \to (Z_\infty)_\Gamma \to 0.$$

Dans le cas (ii), $(\mathbf{H}_{\infty,c})_\Gamma$ est isomorphe à

$$\cap\, \mathrm{tr}_{D_n/k}(\mathbf{H}_{n,c})$$

d'après la proposition 8. Comme on a la factorisation

$$\begin{array}{ccc} (\mathbf{H}_{\infty,c})_\Gamma & \longrightarrow & \tilde{S}_p(D_\infty)_\Gamma \\ \wr\downarrow & & \downarrow \\ \cap\, \mathrm{tr}_{D_n/k}(\mathbf{H}_{n,c}) & \hookrightarrow & \tilde{S}_p(k) \text{ modulo torsion,} \end{array}$$

le Z_p-module $(Z_\infty)^\Gamma$ est nul et $(Z_\infty)_\Gamma$ est fini. On a alors

$$I(\mathbf{H}_{\infty,c})(\mathbf{1}) = \#((Z_\infty)_\Gamma).$$

On en déduit (ii) à l'aide du lemme 7.

Dans le cas (iii), l'homomorphisme

$$(\mathbf{H}_{\infty,c})_\Gamma \to \cap\, \mathrm{tr}_{D_n/k}(\mathbf{H}_{n,c})$$

est nul. On en déduit que Z_∞^Γ est isomorphe à $(\mathbf{H}_{\infty,c})_\Gamma$ donc à $\mathbb{Z}_p$, c'est-à-dire que $I(\mathbf{H}_{\infty,c})(\mathbf{1})$ est nul.

Remarque — Lorsque le $\Lambda_{D_\infty/k}$-rang de $\tilde{S}_p(D_\infty)$ est strictement supérieur à 1, on peut encore conclure que la série caractéristique du sous-$\Lambda_{D_\infty/k}$-module de torsion de $\tilde{S}_p(D_\infty)/\mathbf{H}_{\infty,c}$ est nulle en 1 dans le cas (iii) et

non nulle en 1 dans le cas (ii). En effet, on a de même

$$\mathrm{rg}_{\mathbf{Z}_p}(Z_\infty^\Gamma)=\mathrm{rg}_{\mathbf{Z}_p}(\mathrm{tors}(Z_\infty)^\Gamma)=\begin{cases}0 & \text{dans le cas (ii)}\\ 1 & \text{dans le cas (iii)}\end{cases}.$$

Cela prouve en particulier dans le cas (iii) que ce sous-module de torsion est non trivial.

Nous allons maintenant examiner les exemples 2 où $\mathbf{H}_\infty$ est non nul. D'après [6], le module $\mathcal{H}_{\infty,c}$ (défini sur le Ringklassenkörper H_{cp^∞} de k de conducteur cp^∞) est non nul. Donc, lorsque H_{cp^∞} est égal à D_∞, le $\Lambda_{D_\infty/k}$-module $\mathbf{H}_{\infty,c}$ est non nul, ce qui a lieu lorsque k est principal et que p est ramifié dans k et c égal à 1.

4. Fin des démonstrations

Ce dernier paragraphe complète le premier en présentant les démonstrations des théorèmes énoncés dans le premier. Nous ferons donc les mêmes hypothèses, c'est-à-dire que la courbe elliptique E est à multiplication complexe par l'anneau des entiers d'un corps quadratique imaginaire et vérifie l'hypothèse (**) et l'hypothèse de Heegner. Le sous-$\Lambda_{D_\infty/k}$-module $\mathbf{H}_\infty$ est le module noté $\mathbf{H}_{\infty,1}$ dans le paragraphe 3.

Le théorème 1 a été montré dans le paragraphe 2. La proposition 2 a été montrée dans le paragraphe 3.4 (proposition 10). Donnons donc la démonstration du théorème 3.

Sous l'hypothèse que le $\Lambda_{D_\infty/k}$-module $\widehat{S_p(D_\infty)}$ est de rang 1, la conjecture A_1 est vraie. D'après le théorème 1 du paragraphe 1, on a

$$(1)\quad \lim_{s\to 0}\frac{\mathcal{L}_p(E/k_\infty)(\rho,s)}{s}\sim \mathrm{disc}_{\widehat{S_p(D_\infty)}}\ll\ ,\ \gg_{\nu_\infty,p}(\rho)\,\mathcal{T}_p(E/D_\infty)(\rho).$$

En utilisant la formule

$$\ll \gamma x,\ y\gg_{\nu_\infty,p}=\ll x,\ \gamma^{-1}y\gg_{\nu_\infty,p}=\gamma\ll x,\ y\gg_{\nu_\infty,p}$$

dès que $\gamma\nu_\infty=\nu_\infty$, on voit facilement que

$$(2)\qquad I(\mathbf{H}_\infty)I(\mathbf{H}_\infty)\mathrm{disc}_{\mathbf{H}_\infty}\ll\ ,\ \gg_{\nu_\infty,p}\sim\mathrm{disc}_{\widehat{S_p(D_\infty)}}\ll\ ,\ \gg_{\nu_\infty,p}$$

où $\check{I}(\mathbf{H}_\infty)(\rho)=I(\mathbf{H}_\infty)(\rho^{-1})$. De (1) et de (2), on déduit l'équivalence de A_2 et de B et donc le théorème 3.

Montrons maintenant le théorème 4. D'après le théorème énoncé dans [5], si $L(E/k, s)$ a un zéro simple en $s=1$, le point de Heegner $\mathrm{tr}_{H/k}(e_1)$ n'est pas de torsion (E vérifie l'hypothèse de Heegner). On en déduit par la proposition 10 de 3.5 que $\mathbf{H}_\infty$ est de $\Lambda_{D_\infty/k}$-rang égal à 1 et donc que $\widehat{S_p(D_\infty)}$ n'est pas de $\Lambda_{D_\infty/k}$-torsion. On en déduit la conjecture A_1 et r_{D_∞} est supérieur à 1. Sous l'hypothèse supplémentaire que le rang de $E(k)$ est 1 et que $\text{Ш}(k)(p)$ est fini, le nombre t_k est égal à 1 et r_{D_∞} est nécessairement égal à 1. D'après [2], la hauteur d'un générateur P_{un} des normes universelles de $\check{S}_p(k)$ pour les $\check{S}_p(D_n)$ relativement au caractère cyclotomique ν est non nulle. En appliquant la proposition 13 (paragraphe 2.2), on a

$$\mathscr{T}_p(E/D_\infty)(1)\sim\frac{\mathscr{M}_k\mathscr{E}_p^2\#(\text{Ш}(k)(p))}{[E(k)\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}_p P_{un}]^2}$$

Par la proposition 11 (paragraphe 3.5), on a

$$I(\mathbf{H}_\infty)(1)\sim\mathscr{E}_p[\mathbb{Z}_p P_{un}:\mathbb{Z}_p\,\mathrm{tr}_{H/k}(e_1)].$$

On en déduit que la conjecture B (donc A_2) est vraie pour le caractère trivial **1** si et seulement si

$$[E(k)\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}_p\,\mathrm{tr}_{H/k}(e_1)]^2\sim\mathscr{M}_k\#(\text{Ш}(k)(p))u^2c_E^2.$$

Cette formule est une conséquence de la conjecture de Birch et Swinnerton-Dyer et du théorème de Gross et Zagier déjà cité. En remarquant que

$$\mathscr{M}_k=\mathscr{M}_{\mathbb{Q}}^2$$

(car toutes les places de $\mathbb{Q}$ de mauvaise réduction pour E se décomposent dans k), cette formule peut aussi s'écrire

$$[E(k)\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}_p\,\mathrm{tr}_{H/k}(e_1)]\sim\mathscr{M}_{\mathbb{Q}}\sqrt{\#(\text{Ш}(k)(p))}\,uc_E$$

Démontrons enfin la proposition 5 en la précisant.

Supposons d'abord que $\mathbf{H}_\chi$ est nul. Dans ce cas, $\mathrm{tr}_{H/k}(e_1)$ en particulier est un point de torsion. La conjecture A_2 signifie que

$$\lim_{s \to 0} \frac{\mathscr{L}_p(E/k_\chi)(\rho v^s)}{s} = 0.$$

D'après le théorème 1, cela signifie donc que r_{D_χ} est supérieur à 2, c'est-à-dire que le $\mathbb{Z}_p$-module des normes universelles contenues dans $\check{S}_p(F)$ est de rang supérieur à 2. Donc soit $Ш(k)(p)$ est infini, soit le rang de $E(k)$ est strictement supérieur à 1.

Supposons maintenant que $\mathbf{H}_\chi$ est non nul et supposons que $\mathrm{tr}_{H/k}(e_1)$ est de torsion. On a donc

$$I(\mathbf{H}_\chi)(\mathbf{1}) = 0.$$

D'autre part, si $Ш(k)(p)$ est fini et si le rang de $E(k)$ est égal à 1, on a

$$r_{D_\chi} = t_k = 1.$$

Les hypothèses de la proposition 13 de 2.5 sont vérifiées. Donc $\mathscr{T}_p(E/D_\chi)(\mathbf{1})$ est non nul. Ce qui est contradictoire avec la conjecture B.

BIBLIOGRAPHIE

[1] BERNARDI (D.), GOLDSTEIN (C.) et STEPHENS (N.). – Notes p-adiques sur les courbes elliptiques, *J. reine angew. Math.*, t. 351, 1984, p. 129-170.

[2] BERTRAND (D.). – Propriétés arithmétiques de fonctions thêta à plusieurs variables, *Journées arithmétiques de Leiden*, 1983.

[3] GROSS (B. H.). – On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication, dans *Number Theory related to Fermat's Last Theorem: Progress in Math.*, t. 26, 1982, p. 219-236.

[4] GROSS (B. H.). – Heegner points on $X_0(N)$, dans *Modular forms*, RANKIN (R. A.) éd., Ellis Horwood Limited, 1984, p. 87-105.

[5] GROSS (B. H.) et ZAGIER (D.). – Points de Heegner et dérivées de fonctions L, *C.R. Acad. Sci. Paris*, t. 297, 1983, p. 85-87.

[6] KURCANOV (P. F.). – Elliptic curves of infinite rank over Γ-extensions, *Math. Sbornik*, t. 90, (132), 1973; *Math. U.S.S.R. Sbornik*, vol. 19, n° 2, 1973, p. 320-324.

[7] MAZUR (B.) et TATE (J.). – Canonical height pairings via biextensions, vol. dédié à Shafarevich, *Progress in Math.*, t. 35-36, 1983, p. 195-237.

[8] MAZUR (B.). – Modular curves and arithmetic, *Proc. Int. congress*, Warszawa, 1983, p. 185-211.

[9] PERRIN-RIOU (B.). — *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mémoire 17, S.M.F., supplément au fascicule IV, t. 112, 1984.

[10] PERRIN-RIOU (B.). — Fonctions L p-adiques attachées à une courbe elliptique modulaire et à un corps quadratique imaginaire, *Lond. Math. Soc.* (à paraître).

[11] PERRIN-RIOU (B.). — Fonctions L p-adiques et points de Heegner, *Journées arithmétiques de Besançon*, Société Mathématique de France, *Astérisque*, n° 147-148, 1987, p. 151-171.

[12] Modular functions of one variable IV, *Springer Lectures Notes*, vol. 476, p. 82-113.

APPENDICE

Variation de la fonction L p-adique algébrique par isogénie

Contrairement à la fonction L p-adique analytique, la fonction L p-adique algébrique attachée à une courbe elliptique n'est pas invariante par isogénie lorsque le degré n'est pas premier à p. Nous allons ici en examiner la dépendance. Avant d'énoncer le théorème, fixons quelques notations. Soient E et E' deux courbes elliptiques définies sur un corps de nombres F et f une isogénie de E dans E' définie sur F dont le degré est une puissance de p. Si v est une place de F, on note $\tilde{F}_v$ le corps résiduel de F en v et $\bar{\mathbf{F}}_v = \bar{\tilde{F}}_v$ une clôture algébrique séparable de $\tilde{F}_v$. Nous supposerons que E (donc E') a bonne réduction ordinaire en toute place au-dessus de p. Soit C le noyau de l'isogénie f. Si v est une place au-dessus de p, la réduction de C modulo v est notée $\tilde{C}_v$. C'est un $G(\bar{\mathbf{F}}_v/\tilde{F}_v)$-module (c'est d'ailleurs aussi un $G(\bar{F}_v/F_v)$-module); on note $C_{1,v}$ le noyau de réduction modulo v.

Soit F_∞/F une $\mathbb{Z}_p^r$-extension (avec $r \geqslant 1$). Notons $S_p(E/F_\infty)$ le groupe de Selmer de E F_∞ relatif à p^∞ et $\mathscr{L}_p(E/F_\infty)$ une série caractéristique de son dual de Pontryagin en tant que $\mathrm{Iw}(F_\infty/F)$-module. Nous supposerons qu'elle est non nulle c'est-à-dire que $\widehat{S_p(E/F_\infty)}$ est de $\mathrm{Iw}(F_\infty/F)$-torsion. On suppose que les places de F où E (donc E') à mauvaise réduction ne se décomposent pas totalement dans F_∞.

THÉORÈME. — *On a*

$$\mathscr{L}_p(E'/F_\infty) \sim p^{m(f)}\,\mathscr{L}_p(E/F_\infty)$$

avec

$$m(f)=\sum_{v\mid\infty}\operatorname{ord}_p(\#(C(F_v)))$$
$$+\sum_{v\mid p}[F_v:\mathbb{Q}_p]\operatorname{ord}_p(\#(\tilde{C}_v))-[F:\mathbb{Q}]\operatorname{ord}_p(\#(C))$$
$$=\sum_{v\mid\infty}\operatorname{ord}_p(\#(C(F_v)))-\sum_{v\mid p}[F_v:\mathbb{Q}_p]\operatorname{ord}_p(\#(C_{1,v})).$$

Commençons par une remarque simple. Si M est un $\mathrm{Iw}(F_\infty/F)$-module compact de type fini de torsion, on peut écrire une de ses séries caractéristiques $\mathscr{L}(M)$ sous la forme

$$\mathscr{L}(M)=p^{\mu(M)}R(M)$$

où la fonction d'Iwasawa $R(M)$ n'est pas divisible par p et ne dépend que de la structure de $\mathrm{Iw}(F_\infty/F)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$-module de $M\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$. Il est facile de voir que les $\mathrm{Iw}(F_\infty/F)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$-modules

$$\widehat{S_p(E/F_\infty)}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p \qquad \text{et} \qquad \widehat{S_p(E'/F_\infty)}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$$

sont isomorphes c'est-à-dire que

$$R(\widehat{S_p(E'/F_\infty)})=R(\widehat{S_p(E/F_\infty)}).$$

En posant pour simplifier $\mu(\hat{M})=\mu(M)$, on est donc ramené à montrer que

$$m(f)=\mu(S_p(E'/F_\infty))-\mu(S_p(E/F_\infty)). \tag{1}$$

Nous montrerons la relation (1) en restant dans le cadre de la cohomologie galoisienne (P. Schneider m'a indiqué une démonstration utilisant la définition de groupes de Selmer par la cohomologie plate). Nous utiliserons les théorèmes de dualité locale [4] et de dualité globale de Tate-Poitou [5] et les formules de caractéristiques d'Euler-Poincaré correspondantes. Nous aurons aussi besoin d'un théorème de Cassels [2].

Commençons par quelques définitions. Soit L une extension de F, éventuellement infinie. On note $M(L)$ l'ensemble des places de L où E a mauvaise réduction et des places archimédiennes. $P(L)$ l'ensemble des places de L au-dessus de p et $T(L)$ la réunion de $M(L)$ et de $P(L)$. Soit F_T la plus grande extension de F non ramifiée au dehors de $T(F)$. Toutes les extensions L de F considérées seront contenues dans F_T. Il est bien

connu [1] que $S_p(E/L)$ est un sous-groupe de $H^1(F_T/L, E_{p^\infty})$. Posons

$$X^i_v(E/L) = H^i(L_w, (\widetilde{E_{p^\infty}})_v) \quad \text{si} \quad v \in P(L)$$
$$Y^i_v(E/L) = H^i(L_w, E)(p) \quad \text{si} \quad v \in T(L).$$

On définit alors trois homomorphismes de localisation

$$\alpha_i(E/L): \quad H^i(F_T/L, E_{p^\infty}) \to \prod_{v \in T(L)} H^i(L_w, E_{p^\infty})$$
$$\beta_i(E/L): \quad H^i(F_T/L, E_{p^\infty}) \to \prod_{v \in T(L)} H^i(L_w, E)(p) \left(= \prod_{v \in T(L)} Y^i_v(E/L)\right)$$
$$\gamma_i(E/L): \quad H^i(F_T/L, E_{p^\infty}) \to \prod_{v \in M(L)} Y^i_v(E/L) \prod_{v \in P(L)} X^i_v(E/L).$$

Le noyau de $\beta_1(E/L)$ est par définition égal à $S_p(E/L)$. Quant à $\alpha_i(E/L)$, c'est l'homomorphisme de localisation intervenant dans les théorèmes de dualité globale. Tous les groupes de cohomologie intervenant sont nuls en dimension supérieure ou égale à 3.

PROPOSITION 1. — *Supposons que* $\widehat{S_p(E/F_\infty)}$ *est un* $\mathrm{Iw}(F_\infty/F)$*-module de torsion. Alors, il en est de même de* $\ker \gamma_i(E/F_\infty)$ *et de* $\operatorname{coker} \gamma_i(E/F)$. *De plus, on a*

$$\mu(S_p(E/F_\infty)) = \mu(\ker \gamma_1(E/F_\infty)) - \mu(\operatorname{coker} \gamma_1(F_\infty)) + \mu\left(\prod_{v \in P(F_\infty)} X^0_v(E/F_\infty)\right); \tag{2}$$

$$0 = \mu(\ker \gamma_2(E/F_\infty)) - \mu(\operatorname{coker} \gamma_2(E/F_\infty)); \tag{3}$$

$$\mu(\ker \gamma_0(E/F_\infty)) = 0 \tag{4}$$

et

$$\mu(\operatorname{coker} \gamma_0(E/F_\infty)) = \mu\left(\prod_{v \in P(F_\infty)} X^0_v(E/F_\infty)\right).$$

COROLLAIRE 2. — *On a la formule*

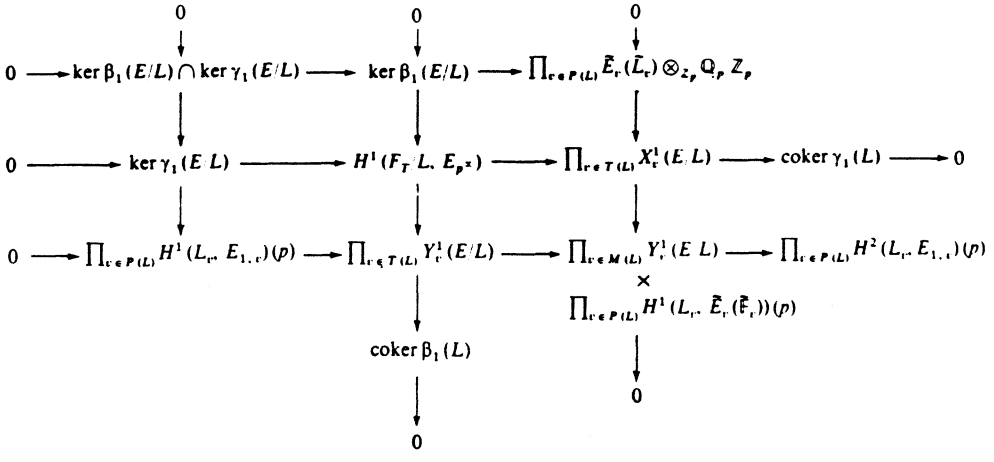
$$-\mu(S_p(E/F_\gamma)) = \sum_{i=0}^{2} (-1)^i (\mu(\ker \gamma_i(E/F_\gamma)) - \mu(\operatorname{coker} \gamma_i(E/F_\gamma))). \tag{5}$$

Démonstration. — Notons $E_{1,v}$ le noyau de réduction de E modulo v. On a les deux suites exactes courtes de $G(\bar{F}_v/F_v)$-modules (pour $v \in P(L)$)

$$0 \to E_{1,v}(\bar{F}_v) \to E(\bar{F}_v) \to \tilde{E}_v(\bar{F}_v) \to 0$$

$$0 \to \tilde{E}_v(\bar{F}_v)_{p^n} \to \tilde{E}_v(\bar{F}_v) \xrightarrow{p^n} \tilde{E}_v(\bar{F}_v) \to 0.$$

On en déduit le diagramme commutatif exact suivant (noté (6)) :



Le 0 vient de ce que la suite suivante est exacte (grâce à l'hypothèse de bonne réduction en v appartenant à $P(L)$) :

$$0 \to E_{1,v}(L_v) \to E(L_v) \to \tilde{E}_v(\tilde{L}_v) \to 0.$$

Énonçons maintenant les deux lemmes suivants.

LEMME 3. — *Soit v une place de F_∞ au-dessus de p. On a*

$$H^1(F_{\infty,v}, E_{1,v})(p) = \begin{cases} 0 & \text{si } F_{\infty,v}/F_v \text{ est ramifiée (i)} \\ \mathbb{Q}_p/\mathbb{Z}_p & \text{si } F_{\infty,v}/F_v \text{ est non ramifiée et infinie (ii)} \\ \mathbb{Z}_p/\#(\tilde{E}_v(\tilde{F}_{\infty,v}))\mathbb{Z}_p & \text{si } F_{\infty,v}/F_v \text{ est non ramifiée et finie (iii);} \end{cases}$$

$$H^2(F_{\infty,v}, E_{1,v})(p) = 0.$$

LEMME 4. — *Le conoyau de $\beta_1(E/F_\infty)$ est nul.*

On déduit du diagramme 6 et des lemmes 3 et 4 les conclusions suivantes :

(*a*) $\widehat{\ker \gamma_1(E/F_\infty)}$ et $\widehat{\operatorname{coker} \gamma_1(E/F_\infty)}$ sont des $Iw(F_\infty/F)$-modules de torsion;

(*b*) $\mu(\ker \beta_1(E/F_\infty)) = \mu(\ker \gamma_1(E/F_\infty)) - \mu(\operatorname{coker} \gamma_1(E/F_\infty)) + \mu(\prod_{v \in P(F_\infty)} X_v^0(E/F_\infty))$

(on remarque en particulier que

$$\prod_{v \in P(F_\infty)} H^1(F_{\infty,v}, E_{1,v})(p)$$

et

$$\prod_{v \in P(F_\infty)} \tilde{E}_v(\tilde{F}_{\infty,v})(p)$$

ont même μ invariant).

Démonstration du lemme 3. — Posons ici $L = F_\infty$. Soient T la complétion de la plus grande extension non ramifiée de F_v et M_v la plus grande extension non ramifiée de F_v contenue dans L_v. Posons $L'_v = L_v T$. La courbe elliptique étant ordinaire en v, il existe un isomorphisme de groupes formels défini sur l'anneau des entiers de T entre $E_{1,v}$ et le groupe $U_{1,v}$ des unités fondamentales : $s : E_{1,v} \to U_{1,v}$. Si φ est l'endomorphisme de Frobenius de M_v, il existe un élément u de $\mathbb{Z}_p^\times$ tel que

$$s^\varphi s^{-1} = u.$$

On en déduit que $E_{1,v}(L_v)$ est isomorphe à l'ensemble des α appartenant à $U_{1,v}(L'_v)$ tels que $\varphi(\alpha) = u\alpha$.

Supposons d'abord que L_v est à valuation discrète (cas (ii) et (iii)). Dans ce cas, M_v et L_v sont égales. On déduit de l'exercice 2, chapitre XII de [23] que

$$H^1(L'_v, U_{1,v})(p) = H^1(L'_v, U_v)(p) = \mathbb{Q}_p/\mathbb{Z}_p,$$
$$H^2(L'_v, U_{1,v})(p) = H^2(L'_v, U_v)(p) = 0.$$

De plus, φ agissant trivialement sur L_v, l'endomorphisme $\varphi - u$ agissant sur $H^1(L'_v, U_{1,v})(p)$ correspond à la multiplication par $1-u$ sur $\mathbb{Q}_p/\mathbb{Z}_p$. Donc $H^2(L_v, E_{1,v})(p)$ est nul et $H^1(L_v, E_{1,v})(p)$ est égal au noyau de la multiplication par $u-1$ sur $\mathbb{Q}_p/\mathbb{Z}_p$ (en utilisant le fait que $H^i(L'_v/L_v, E(L'_v))$ est nul pour $i \geqslant 1$). Dans le cas (ii), u est égal à 1. Dans le cas (iii), la valuation p-adique de $u-1$ est égale à celle de $\#(\tilde{E}_v(\tilde{L}_v)(p))$.

Supposons maintenant que L_v contient une $\mathbb{Z}_p$-extension ramifiée (cas (i)). Alors, $H^1(L'_v, U_{1,v})(p)$ est la limite projective sur les extensions finies $L_{n,v}$ contenues dans L_v des

$$H^i(L_{n,v}, T, U_{1,v})(p) = \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & \text{si } i=1 \\ 0 & \text{si } i=2 \end{cases}$$

(les flèches de transition étant induites par la multiplication par l'indice de ramification). On en déduit que $H^i(L'_v, U_{1,v})(p)$ est nul pour $i \geqq 1$. D'où la nullité des $H^i(L_v, E_{1,v})(p)$ pour $i \geqq 1$.

Démonstration du lemme 4. — Nous utiliserons ici le théorème de CASSELS ([2], *voir* aussi [1]) qui décrit le conoyau de $\beta_1(E/L)$ pour une extension finie L de F. Le dual de ce conoyau est isomorphe à l'image de $\tilde{S}_p(E/L)$ dans le $\mathbb{Z}_p$-module

$$\prod_{v \in T(L)} \varprojlim_{\times p} E(L_v)/p^n E(L_v).$$

Le dual de $\operatorname{coker}\beta_1(E/F_\infty)$ est donc un quotient de $\tilde{S}_p(E/F_\infty)$. Ce dernier $\mathrm{Iw}(F_\infty/F)$-module est nul si $\widehat{S_p(E/F_\infty)}$ est de $\mathrm{Iw}(F_\infty/F)$-torsion (*voir* paragraphe 2.2 pour une propriété analogue). On en déduit donc le lemme 4.

Passons maintenant aux groupes de cohomologie de dimension 2.

Les groupes de cohomologie $H^2(L_v, E)$ et $H^2(L_v, E_{p^\infty})$ pour v appartenant à $T(L)$ ainsi que $H^2(L_v, \widetilde{(E_{p^\infty})}_v)$ pour v appartenant à $P(L)$ sont nuls. On en déduit la nullité du conoyau de $\gamma_2(E/F_\infty)$ et l'égalité des noyaux de $\alpha_2(E/F_\infty)$ et de $\gamma_2(E/F_\infty)$.

On utilise alors les théorèmes de dualité de Tate-Poitou pour montrer que $\widehat{\ker\alpha_2(E/F_\infty)}$ est un sous-$\mathrm{Iw}(F_\infty/F)$-module de $\tilde{S}_p(E/F_\infty)$ (et est donc nul). On en déduit la nullité de $\mu(\ker\alpha_2(E/F_\infty)$ et l'égalité (3).

Quant aux égalités (4), elles sont immédiates par définition de $\gamma_0(E/F_\infty)$.

Nous allons maintenant déduire le théorème de la proposition 1 et de son corollaire. On a les suites exactes longues

$$\begin{array}{ccccccc}
\cdots \to & H^i(F_T/F, C) & \longrightarrow & H^i(F_T/F_\infty, E_{p^\infty}) & \longrightarrow & H^i(F_T/F, E'_{p^\infty}) & \to \cdots \\
 & \downarrow & & \downarrow & & \downarrow & \\
\cdots \to & \prod_{v \in M(F_\gamma)} H^i(F_{\gamma,v}, C) & & \prod_{v \in M(F_\gamma)} Y'_v(E/F_\gamma) & & \prod_{v \in M(F_\gamma)} Y'_v(E'/F_\gamma) & \to \cdots \\
 & \times & \longrightarrow & \times & \longrightarrow & \times & \\
 & \prod_{v \in P(F_\gamma)} H^i(F_{\gamma,v}, \tilde{C}_v) & & \prod_{v \in P(F_\gamma)} X'_v(E/F_\gamma) & & \prod_{v \in P(F_\gamma)} X'_v E'/F_\gamma) &
\end{array}$$

Les $\mathrm{Iw}(F_\alpha/F)$-modules $H^i(F_T/F_\alpha, C)$ et

$$\prod_{v \in M(F_\alpha)} H^i(F_{\alpha,v}, C) \times \prod_{v \in P(F_\alpha)} H^i(F_{\alpha,v}, \tilde{C}_v)$$

sont de torsion. On déduit alors du diagramme et du corollaire 2 la formule

$$(7) \qquad m(f) = \mu(S_p(E'/F_\alpha)) - \mu(S_p(E/F_\gamma)) = \mu_{\text{global}} - \mu_{\text{local}}.$$

avec

$$\mu_{\text{global}} = \sum_i (-1)^i \mu(H^i(F_T/F_\infty, C))$$

et

$$\mu_{\text{local}} = \sum_i (-1)^i \mu\left(\prod_{v \in P(F_\infty)} H^i(F_{\infty,v}, \tilde{C}_v)\right).$$

Rappelons que si M est un $\mathrm{Iw}(F_\infty/F)$-module compact de type fini de torsion tel que

$$\mathrm{ord}_p(\#(M_{G(F_\infty/F_n)}) = \mu[F_n : F] + o([F_n : F])$$

pour n assez grand, l'entier μ est exactement égal à $\mu(M)$. Grâce à la suite exacte inflation-restriction, les $\mathbb{Z}_p[G(F_n/F)]$-modules

$$\left(\prod_{v \in P(F_\infty)} H^i(F_{\infty,v}, \tilde{C}_v)\right)^{G(F_\infty/F_n)}$$

et

$$\prod_{v \in P(F_n)} H^i(F_{n,v}, \tilde{C}_v)$$

sont isomorphes à un groupe fini près d'ordre borné. On est donc ramené à un calcul de caractéristique d'Euler-Poincaré locale [4] : on a donc

$$\mu_{\text{local}} = -\sum_{v \in P(F)} [F_v : \mathbb{Q}_p] \mathrm{ord}_p(\#(\tilde{C}_v)).$$

Le μ-invariant de $H^i(F_T/F_\infty, C)$ se calcule de même en utilisant la caractéristique d'Euler-Poincaré globale [5] :

$$\mu_{\text{global}} = -[F : \mathbb{Q}] \mathrm{ord}_p(\#(C)) + \sum_{v \mid \infty} \mathrm{ord}_p(\#(C(F_v))).$$

La formule (1) se déduit de la formule (7) et de l'expression précédente de μ_{global} et de μ_{local}.

Remarquons que les calculs précédents (et donc le théorème) sont tout à fait valables pour une variété abélienne ordinaire en toute place de F au-dessus de p.

Rappelons la définition du nombre de Tamagawa de E à l'infini. Pour simplifier, supposons que E admet une forme différentielle ω invariante

minimale partout sur l'anneau des entiers de F. Pour toute place archimédienne v de F, on pose

$$\Omega_v = \begin{cases} \displaystyle\int_{E(F_v)} \omega & \text{si } v \text{ est réelle} \\ \displaystyle\int_{E(F_v)} \omega \wedge i\varpi & \text{si } v \text{ est complexe.} \end{cases}$$

On pose alors

$$\Omega(E/F) = \prod_{v \mid \infty} \Omega_v.$$

Le lemme suivant est bien connu (avec les hypothèses et notations du théorème précédent).

LEMME. — *Le nombre $\Omega(E'/F)/\Omega(E/F)$ est un rationnel et on a*

$$\mathrm{ord}_p(\Omega(E'/F)/\Omega(E/F)) = -m(f).$$

On en déduit que $\Omega(E/F)\mathscr{L}_p(E/F_\infty)$ est un invariant d'isogénie.

Démonstration du lemme. — Si ω' est une forme différentielle minimale de E'/F, on a

$$f^*\omega' = c(f)\omega$$

où $c(f)$ est un entier de F. On voit alors facilement que

$$\Omega'_v/\Omega_v = \begin{cases} \sigma_v(c(f)) \cdot \#(C(F_v)) & \text{si } v \text{ est réelle} \\ |\sigma_v(c(f))|^2 \cdot \#(C(F_v)) & \text{si } v \text{ est complexe} \end{cases}$$

où σ_v désigne un plongement de F dans F_v associé à v. On en déduit que

$$\Omega(E'/F)/\Omega(E/F) = N_{F/\mathbb{Q}}(c(f)) \cdot \prod_{v \mid \infty} \#(C(F_v))$$

d'où

$$\mathrm{ord}_p(\Omega(E'/F)/\Omega(E/F)) = -\sum_{v \mid \infty} \mathrm{ord}_p(\#(C(F_v))) + \sum_{v \mid p} [F_v : \mathbb{Q}_p] \mathrm{ord}_p(\sigma_v(c(f))).$$

On doit donc montrer que $\mathrm{ord}_p(\sigma_v(c(f)))$ est égal à $\#(C_{1,v})$. Cela se voit facilement si f est étale en v, donc si l'isogénie duale de f est étale. Comme nous avons supposé que E est ordinaire en v, le cas général se déduit de ces deux cas précédents.

BIBLIOGRAPHIE

[1] BASHMAKOV (M. I.). – The cohomology of abelian varieties over a number field, *Russian Math. Surveys*, vol. 27, 1972, p. 25-70.

[2] CASSELS (J. W. S.). – Arithmetic on curves of genus 1, *J. Reine angew. Math.* (*VII*), t. 216, 1964, p. 150-158.

[3] SERRE (J.-P.). – *Corps locaux*, Hermann, Paris, 1968.

[4] SERRE (J.-P.). – Cohomologie galoisienne, *Lect. Notes in Math.*, 5, Springer-Verlag, 1973.

[5] TATE (J.). – Duality theorems in Galois cohomology over number fields, *Proc. Int. Congress*, Stockholm, 1962, p. 288-295.