Werk

Titel: Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication...

Autor: Perrin-Riou, Bernadette

PURL: https://resolver.sub.uni-goettingen.de/purl?356556735_0070|log33

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Invent. math. 70, 369–398 (1983)

Inventiones mathematicae
© Springer-Verlag 1983

Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe

Bernadette Perrin-Riou

Université Pierre et Marie Curie, L.M.F. 45–46, 3éme étage - U.E.R. 48,
4, place Jussieu, F-75230 Paris Cedex 05, France

Il n'a été encore prouvé aucun lien entre le déterminant de la forme bilinéaire de Néron-Tate sur le groupe des points rationnels d'une courbe elliptique sur un corps de nombres et le comportement de la fonction de Hasse-Weil de la courbe elliptique au point $s=1$, bien que la conjecture de Birch et Swinnerton-Dyer ne le prédise. Le but de cet article est d'établir un analogue p-adique partiel d'un tel lien dans le cas spécial où la courbe elliptique est à multiplication complexe.

Donnons un énoncé précis des résultats obtenus. Soient K un corps quadratique imaginaire, F une extension finie de K et E une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathcal{O}$ de K, définie sur F. Soit p un nombre premier impair vérifiant les deux propriétés suivantes:

(i) p se décompose dans K en deux idéaux premiers distincts $\mathfrak{p}$ et $\mathfrak{p}^*$; $(p)=\mathfrak{p}\mathfrak{p}^*$;

(ii) E a bonne réduction en toute place de F au dessus de $\mathfrak{p}$.

Ces deux conditions expriment que E a bonne réduction ordinaire en toute place de F au dessus de $\mathfrak{p}$. Soit h_F la hauteur $\mathfrak{p}$-adique sur $E(F)$ définie dans [10] (la définition en est rappelée dans le paragraphe 1). C'est une fonction quadratique à valeurs dans $K_{\mathfrak{p}}$, donnée par une formule analytique et vérifiant $h_F(\alpha P)=\deg\alpha\ h_F(P)$ si P appartient à $E(F)$, α à $\mathcal{O}$ et si $\deg\alpha$ désigne la norme de K sur $\mathbb{Q}$ de α. On note α^* le conjugué de α. On suppose dans tout ce texte le corps K plongé dans $K_{\mathfrak{p}}$ par le plongement $\mathfrak{p}$-adique. Il existe une unique forme bilinéaire (notée $\langle\ ,\ \rangle_{F,\mathfrak{p}}$) sur $E(F)$ à valeurs dans $K_{\mathfrak{p}}$ vérifiant

(i) $\langle P, P\rangle_{F,\mathfrak{p}}=h_F(P)$,

(ii) $\langle\alpha P, Q\rangle_{F,\mathfrak{p}}=\langle P, \alpha^* Q\rangle_{F,\mathfrak{p}}=\alpha\langle P, Q\rangle_{F,\mathfrak{p}}$

pour P et Q appartenant à $E(F)$ et α à $\mathcal{O}$.

D'autre part, on construit ici une forme bilinéaire algébrique $\{\ ,\ \}_{F,\mathfrak{p}}$ sur $E(F)$ à valeurs dans $K_{\mathfrak{p}}$ que l'on peut qualifier de kummerienne car elle est obtenue grâce à l'emploi conjugué de la théorie de Kummer multiplicative et de la théorie de Kummer sur la courbe elliptique (paragraphe 3). Le premier théorème obtenu est que as deux formes bilinéaires, ainsi construites selon des

0020-9910/83/0070/0369/$ 06.00

points de vue différents, sont égales à un coefficient de proportionnalité près:

$$\{P, Q\}_{F,\mathfrak{p}} = t_{\mathfrak{p}}(F)^{-1}\langle P, Q\rangle_{F,\mathfrak{p}},$$

(théorème 4.1).

Soit K_∞ l'unique extension galoisienne de K, non ramifiée au dehors de $\mathfrak{p}$ et dont le groupe de Galois sur K est topologiquement isomorphe à $\mathbb{Z}_p$. Appelons N_∞ le composé de F et de K_∞ et Γ le groupe de Galois de N_∞ sur F. Soit $S(N_\infty)$ le groupe de Selmer de E sur N_∞ relatif à la descente pour $\mathfrak{p}^\infty$ (pour la définition précise, voir 2.1). Alors $S(N_\infty)$ est un module discret sur lequel Γ opère de manière continue. Sous une hypothèse que l'on appellera $\mathfrak{p}$-adique faible de Leopoldt et qui sera précisée au paragraphe 2.2, le dual de Pontryagin $\widehat{S(N_\infty)}$ de $S(N_\infty)$ est un module compact de type fini et de torsion sur l'algèbre d'Iwasawa $\mathbb{Z}_p[\![\Gamma]\!]$ (qui est isomorphe à l'algèbre des séries formelles à une variable à coefficients dans $\mathbb{Z}_p$). L'hypothèse $\mathfrak{p}$-adique faible de Leopoldt est en fait vérifiée pour un grand nombre de courbes elliptiques, en particulier pour celles telles que $F(E_\mathfrak{p})$ est abélien sur K (par un théorème de Baker). Par la théorie classique de la multiplication complexe, $N_\infty(E_\mathfrak{p})$ est égal à $F(E_{\mathfrak{p}^\infty})$. On identifie Γ avec le groupe de Galois de $F(E_{\mathfrak{p}^\infty})$ sur $F(E_\mathfrak{p})$. Notons κ le caractère de Γ à valeurs dans $\mathcal{O}_\mathfrak{p}$ donné par l'action de Γ sur $E_{\mathfrak{p}^\infty}$. Soit γ un générateur topologique de Γ; on pose $T=\gamma-1$ et $u=\kappa(\gamma)$. Soit $f(E/F, T)$ une série caractéristique de $\widehat{S(N_\infty)}$. On considère alors la fonction de variable s dans $\mathbb{Z}_p$ définie par

$$\mathscr{L}_\mathfrak{p}(E/F, s)=\begin{cases} f(E/F, u^{s-1}-1)/(u^s-1) & \text{si } F \text{ contient } E_\mathfrak{p} \\ f(E/F, u^{s-1}-1) & \text{sinon.}\end{cases}$$

On s'intéresse au comportement de $\mathscr{L}_\mathfrak{p}(E/F, s)$ au point $s=1$. Notons $\Psi_{E/F}$ le Grössencharakter de E/F et $\Omega(F)$ le groupe de torsion de $E(F)$. Si v est une place de F, Nv désigne le cardinal du corps résiduel k_v de F en v.

Théorème. *On suppose vérifiée l'hypothèse $\mathfrak{p}$-adique faible de Leopoldt pour F.*

(1) *La fonction $\mathscr{L}_\mathfrak{p}(E/F, s)$ a un zéro en $s=1$ de multiplicité supérieure au rang $n_{E/F}$ sur $\mathcal{O}$ de $E(F)$.*

(2) *Cette multiplicité est égale à $n_{E/F}$ si et seulement si la composante $\mathfrak{p}$-primaire $Ш(F)(\mathfrak{p})$ du groupe de Shafarevitch et Tate est finie et si la forme bilinéaire $\langle\ ,\ \rangle_{F,\mathfrak{p}}$ est non dégénérée sur $E(F)/\Omega(F)$.*

(3) *Si cette multiplicité est $n_{E/F}$, la valeur de*

$$\mathscr{L}_\mathfrak{p}(E/F, s)/(s-1)^{n_{E/F}}$$

en $s=1$ est égale (à une unité près) à

$$\prod_{v/\mathfrak{p}}\left(1-\frac{\Psi_{E/F}(v)}{Nv}\right)\#(Ш(F)(\mathfrak{p}))\,\frac{\det((\langle P_i, P_j\rangle_{F,\mathfrak{p}}))}{[E(F):\sum \mathcal{O}P_i]}$$

où $P_1, \ldots, P_{n_{E/F}}$ désigne un système indépendant de $n_{E/F}$ points de $E(F)/\Omega(F)$.

On obtient d'autre part comme résultat intermédiaire le résultat suivant qui ne semblait pas être connu avant.

Proposition. *Supposons vérifiée l'hypothèse* $\mathfrak{p}$*-adique faible de Leopoldt. Alors les* $\mathbb{Z}_p$*-rangs des duaux de Pontryagin de* $Ш(F)(\mathfrak{p})$ *et de* $Ш(F)(\mathfrak{p}^*)$ *sont égaux. En particulier,* $Ш(F)(\mathfrak{p})$ *est fini si et seulement si* $Ш(F)(\mathfrak{p}^*)$ *est fini.*

Dans le premier paragraphe, on définit la hauteur $\mathfrak{p}$-adique h_F sur $E(F)$. Dans le second paragraphe, on rappellera les techniques de la théorie d'Iwasawa et on commencera le calcul de la série caractéristique en $T=0$. Dans le troisième paragraphe, on construira la forme bilinéaire $\{\,,\}_{F,\mathfrak{p}}$ qui permet d'interpréter une partie du premier coefficient non nul du développement de la série caractéristique en puissance de T. Dans le quatrième paragraphe, on montrera le lien entre $\{\,,\}_{F,\mathfrak{p}}$ et $\langle\,,\rangle_{F,\mathfrak{p}}$. Un cinquième paragraphe est consacré à des exemples numériques.

Une construction analogue à celle de $\{\,,\}_{F,\mathfrak{p}}$ pour l'extension cyclotomique a été faite depuis par P. Schneider dans un cadre différent et sous des hypothèses de finitude de groupes de Shafarevitch-Tate [11]. Signalons d'autre part que *B.* Gross a donné une conjecture sur le premier coefficient non nul du développement de Taylor en $s=1$ de la fonction L de Hecke $L(\bar{\Psi}_{E/F}, s)$ (pour s complexe) qui précise la conjecture de Birch et Swinnerton-Dyer [7]. Enfin, dans le cas où le corps obtenu en rajoutant à F le groupe des points d'ordre fini de E est abélien sur K, il existe une conjecture principale reliant la fonction $\mathscr{L}_{\mathfrak{p}}$ à une fonction L p-adique $L_{\mathfrak{p}}$ interpolant certaines valeurs des fonctions complexes $L(\bar{\Psi}^k_{E/F}, s)$ (voir [3] dans le cas $F=K$ et [4] dans le cas général). Des calculs faits par D. Bernardi et N. Stephens sur la fonction L p-adique (article en préparation) donnent des «évidences numériques» pour cette conjecture. La formule démontrée ici permet alors de faire une conjecture sur la fonction $L_{\mathfrak{p}}$ tout à fait analogue à celle de B. Gross dans le cas complexe.

Je tiens à remercier J. Coates pour les nombreuses remarques et suggestions qu'il m'a faites.

1. Hauteur $\mathfrak{p}$-adique analytique

Différentes constructions d'une hauteur p-adique analogue à la hauteur canonique de Néron et Tate ont été données ([1, 8], cf. aussi [9]). On rappelle ici la construction de la forme quadratique attachée à la courbe E et à $\mathfrak{p}$ (ou plutôt à la $\mathbb{Z}_p$-extension N_∞) donnée dans [10] et tout à fait analogue à celle de D. Bernardi.

Soit L une extension finie de F. On utilisera un modèle de Weierstrass de E sur l'anneau des entiers de L ayant bonne réduction aux places au dessus de $\mathfrak{p}$, c'est-à-dire une équation de la forme

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$$

(où les a_i appartiennent à l'anneau des entiers de L) et de discriminant Δ premier à $\mathfrak{p}$. Définissons les fonctions suivantes sur la courbe:

$$\gamma(P,Q)=\Delta^{-1}(x(P)-x(Q))^6,$$

$$\gamma_\alpha(P)=\prod_{r\in E_\alpha-\{0\}}\Delta^{-1}(x(P)-x(r))^6$$

pour α appartenant à $\mathcal{O}$. Elles ne dépendent pas du modèle choisi.

Si v est une place de L, soit v_L la valuation associée telle que $v_L(L^\times)=\mathbb{Z}$. D'après un théorème de Néron-Tate, il existe une unique fonction $\lambda_{L,v}$ de $E(L_v)-\{O\}$ dans $\mathbb{Q}$ (muni de la topologie usuelle sur $\mathbb{R}$), continue pour la topologie v-adique, telle que:

(i) la limite, pour P tendant vers $\lambda_{L,v}(P)-v_L(t(P))$ existe pour un (donc pour tout) paramètre uniformisant t de E à l'origine;

(ii) pour tout couple (P, Q) de points de $E(L_v)-\{O\}$ tel que $P\pm Q\neq O$, on a

$$\lambda_{L,v}(P+Q)+\lambda_{L,v}(P-Q)=2\lambda_{L,v}(P)+2\lambda_{L,v}(Q)+\tfrac{1}{6}v_L(\gamma(P,Q)). \tag{1}$$

La fonction $\lambda_{L,v}$ vérifie aussi la propriété suivante pour α appartenant à $\mathcal{O}$ et P et αP non nuls:

$$\lambda_{L,v}(\alpha P)=\deg\alpha\,\lambda_{L,v}(P)+\tfrac{1}{12}v_L(\gamma_\alpha(P)\,\alpha^{12}). \tag{2}$$

Cette formule servira de manière essentielle dans le paragraphe 4 et les fonctions $\prod_r (x(P)-x(r))$ où le produit est pris sur les éléments r non nuls du noyau de l'endomorphisme α permettront de faire le lien entre la forme bilinéaire «algébrique» définie dans le paragraphe 3 et la hauteur $\mathfrak{p}$-adique analytique dont la définition va suivre. On aura aussi besoin du lemme.

Lemme 1.1. *Soit v une place de L où E a bonne réduction et (x, y) les coordonnées de points de E dans un modèle ayant bonne réduction en v. Alors,*

$$\lambda_{L,v}(P)=\mathrm{Sup}(0,\ -\tfrac{1}{2}v_L(x(P))).$$

En particulier, $\lambda_{L,v}(P)$ est un entier qui est non nul si et seulement si P appartient au noyau de réduction modulo v.

Soient v une place de L au dessus de $\mathfrak{p}$ et $E_{1,v}$ le noyau de la réduction modulo v. Alors, $t=-x/y$ est un paramètre uniformisant de E en O. Soient $\mathscr{L}_v$ le logarithme de $E_{1,v}$ et φ_v la série entière réciproque de $\mathscr{L}_v$. Alors, $z=\mathscr{L}_v(t)$ est un paramètre uniformisant du groupe formel additif. On définit alors les séries formelles:

$$\mathfrak{P}_v(z)=x(\varphi_v(z))+(a_1^2+4a_2)/12=1/z^2+\sum_2^\infty \gamma_k z^{2k-2},$$

$$\Theta_v(z)=\Delta z^{12}\exp\left(-6s_2 z^2-12\sum_2^\infty \gamma_k z^{2k}/2k(2k-1)\right).$$

Donnons la définition de s_2 et montrons en même temps l'invariance de Θ_v par rapport au modèle.

Pour chaque plongement de L dans la clôture algébrique de $\mathbb{Q}$ contenue dans $\mathbb{C}$, on a une équation de E sur $\mathbb{C}$ et un réseau $\mathscr{L}$. Soit alors

$$s_2(\mathscr{L})=\lim_{s\to 0^+}\sum_{\substack{\omega\in\mathscr{L}\\ \omega\neq 0}}\omega^{-2}|\omega|^{-2s}.$$

Comme E est à multiplication complexe, il est bien connu que $s_2(\mathscr{L})$ est un entier algébrique, image par le plongement d'un élément de L qui ne dépend

pas du plongement et que l'on note s_2. Il en est de même pour les γ_k qui sont reliés de manière analogue aux séries d'Eisenstein $E_{2k}(\mathscr{L})$. L'étude du comportement de s_2, γ_k, t par changement de modèle montre facilement que $\Theta_v(\mathscr{L}_v(t(P)))$ est indépendant du modèle choisi. Remarquons que l'on peut calculer s_2 de la manière suivante. Soit α un élément de $\mathcal{O}$ qui n'est pas dans $\mathbb{Z}$. Alors,

$$(\alpha^2 - \alpha\alpha^*)\, s_2 = \sum_{\substack{r \in E_{\overline{\mathfrak{p}}} \\ r \neq O}} (x(r) + (a_1^2 + 4a_2)/12).$$

La série $\Theta_v(z)$ converge dans L_v pour $v_L(z) > v_L(p)/(p-1)$. Soit n'importe quel prolongement $\log_{\mathfrak{p}}$ à $K_{\mathfrak{p}}$ du logarithme p-adique usuel sur les unités de $K_{\mathfrak{p}}$ congrues à 1 modulo $\mathfrak{p}$. Notons $N_{L_v/K_{\mathfrak{p}}}$ (resp. $\mathrm{tr}_{L_v/K_{\mathfrak{p}}}$) la norme (resp. la trace) de $L_v/K_{\mathfrak{p}}$. On a alors le lemme suivant.

Lemme 1.2. *Soit v une place de L au dessus de $\mathfrak{p}$. Il existe une et une seule fonction $\eta_{L,v}$ de $E_{1,v}(L_v) - \{O\}$ à valeurs dans $K_{\mathfrak{p}}$, continue et vérifiant les deux propriétés suivantes:*

(i) $\eta_{L,v}(P+Q) + \eta_{L,v}(P-Q) = 2\eta_{L,v}(P) + 2\eta_{L,v}(Q) + \frac{1}{6}\log_{\mathfrak{p}} N_{L_v/K_{\mathfrak{p}}}\gamma(P,Q)$,

(ii) $\eta_{L,v}(\alpha P) = \deg\alpha\, \eta_{L,v}(P) + \frac{1}{12}\log_{\mathfrak{p}} N_{L_v/K_{\mathfrak{p}}}(\gamma_\alpha(P)\,\alpha^{12})$

pour α appartenant à $\mathcal{O}$.

Démonstration. Les propriétés usuelles de la fonction Θ permettent de montrer que sur un sous-groupe de $E_{1,v}(L_v)$, par exemple pour les points P vérifiant

$$v_L(t(P)) > v_L(p)/(p-1),$$

la fonction

$$\tfrac{1}{12}\log_{\mathfrak{p}} N_{L_v/K_{\mathfrak{p}}}\, \Theta_v(\mathscr{L}_v(t(P)))$$

convient. On montrera que la série formelle en t

$$R_v(t) = \log[\Theta_v(\mathscr{L}_v(t))/\Delta\mathscr{L}_v(t)^{12}]$$

converge pour $v_L(t) > 0$. La fonction

$$\eta_{L,v}(P) = \tfrac{1}{12}[\mathrm{tr}_{L_v/K_{\mathfrak{p}}} R_v(t(P)) + \log_{\mathfrak{p}} N_{L_v/K_{\mathfrak{p}}}(\Delta\mathscr{L}_v(t(P))^{12})]$$

conviendra alors. Revenons à la convergence de la série formelle R_v. Elle vérifie l'équation différentielle

$$\left(\frac{R_v'(t)}{\mathscr{L}_v'(t)}\right)' = -12(x(t) - \mathscr{L}_v(t)^{-2} + (a_1^2 + 4a_2)/12 - s_2).$$

De même que $\mathscr{L}_v'(t)$, le second membre est une série formelle convergent pour $v_L(t) > 0$. On en déduit que $R_v(t)$ s'obtient par intégrations successives de séries convergeant pour $v_L(t) > 0$ et donc converge pour $v_L(t) > 0$.

L'unicité se montre grâce au lemme suivant.

Lemme 1.3. *Soient v une place de L au dessus de $\mathfrak{p}$ et D une fonction sur $E_{1,v}(L_v) - \{O\}$ à valeurs dans $\mathbb{Z}_p$, continue et vérifiant $D(\alpha P) = \deg\alpha\, D(P)$ pour tout α appartenant à $\mathcal{O}$. Alors, D est identiquement nulle.*

Démonstration. Soit α un élément de $\mathcal{O}$ qui n'est pas dans $\mathbb{Z}$. Soit k_n une suite d'entiers de $\mathbb{Z}$ dont la limite dans $\mathcal{O}$ est α et telle que $k_n P$ soit non nul. Alors, αP est la limite de la suite $k_n P$ dans $E_{1,v}(L_v)$. Donc

$$D(\alpha P) = \lim_{n\to\infty} D(k_n P) = \lim_{n\to\infty} k_n^2 D(P) = \alpha^2 D(P).$$

D'autre part, $D(\alpha P)$ est égal à $\deg\alpha\ D(P)$. Cela implique que D est identiquement nulle.

L'idéal $N_{L/K} v$ est principal pour toute place v car L contient le corps de Hilbert de K par la théorie de la multiplication complexe. Soit τ_v un générateur de $N_{L/K} v$. Le nombre $\log_{\mathfrak{p}} \tau_v$ ne dépend que de v. Soit $E_1(L)$ l'ensemble des points de $E(L)$ dont la réduction modulo toute place de L au dessus de $\mathfrak{p}$ est nulle. C'est un sous-groupe d'indice fini de $E(L)$. On pose alors

$$h_L(P) = \sum_v \lambda_{L,v}(P) \log_{\mathfrak{p}} \tau_v - \sum_{v/\mathfrak{p}} \eta_{L,v}(P)$$

pour P élément non nul de $E_1(L)$. Cette définition ne dépend en fait pas du choix du logarithme $\mathfrak{p}$-adique. On a la proposition suivante.

Proposition 1.4. *La fonction h_L est une fonction quadratique sur $E_1(L)$, c'est-à-dire qu'elle vérifie*

$$h_L(P+Q) + h_L(P-Q) = 2h_L(P) + 2h_L(Q).$$

On a de plus les propriétés suivantes:

(i) $h_L(\alpha P) = \deg\alpha\ h_L(P)$ si $\alpha \in \mathcal{O}$;

(ii) *si L' est une extension finie de L de degré $[L':L]$, on a*

$$h_{L'}(P) = [L':L]\, h_L(P)$$

pour P appartenant à $E_1(L)$.

Démonstration. Par le lemme 1.2, on a les formules

$$\sum_{v/\mathfrak{p}} [\eta_{L,v}(P+Q) + \eta_{L,v}(P-Q) - 2\eta_{L,v}(P) - 2\eta_{L,v}(Q)] = \tfrac{1}{6} \log_{\mathfrak{p}} N_{L/K}\, \gamma(P, Q),$$

$$\sum_{v/\mathfrak{p}} [\eta_{L,v}(\alpha P) - \deg\alpha\ \eta_{L,v}(P)] = \tfrac{1}{12} \log_{\mathfrak{p}} N_{L/K}(\alpha^{12} \gamma_\alpha(P)).$$

D'autre part, les équations (1) et (2) permettent de montrer le même type de formules pour l'expression

$$\sum_v \lambda_{L,v}(P) \log_{\mathfrak{p}} \tau_v$$

grâce à la «formule du produit»

$$(N_{L/K}(a)) = \left(\prod_v \tau_v^{v_L(a)}\right).$$

(où le produit est pris sur les places finies de L) pour tout élément a de $L^\times$. Ce qui démontre la quadraticité de h_L et (i). On démontre de même facilement la formule (ii).

La formule (i) est fondamentale par la suite; remarquons de plus que si $\Omega(L)$ est le groupe de torsion de $E(L)$, h_L se prolonge naturellement à $E(L)/\Omega(L)$.

On attache maintenant à h_L une forme bilinéaire.

Lemme 1.5. *Soit h une forme quadratique sur $E(L)$ à valeurs dans $K_\mathfrak{p}$ vérifiant*

$$h(\alpha P)=\deg \alpha\, h(P) \quad \textit{pour } \alpha\in\mathcal{O}.$$

Il existe une unique forme bilinéaire B sur $E(L)$ vérifiant les trois propriétés suivantes:

(i) $B(P,P)=h(P)$,

(ii) $B(\alpha P,Q)=\alpha B(P,Q)$,

(iii) $B(P,\alpha Q)=\alpha^* B(P,Q)$

pour $\alpha\in\mathcal{O}$, $P\in E(L)$ et $Q\in E(L)$.

Démonstration. Soient deux formes bilinéaires sur $E(L)$ vérifiant (i), (ii) et (iii) et D leur différence. On a alors

$$D(P,Q)+D(Q,P)=0.$$

D'où

$$D(\alpha P,Q)=-D(Q,\alpha P)=-\alpha^* D(Q,P)=\alpha^* D(P,Q).$$

Le membre de gauche étant d'autre part égal à $\alpha D(P,Q)$, D est identiquement nulle.

Soient S la forme bilinéaire symétrique associée à h et β n'importe quel élément de $\mathcal{O}$ qui n'est pas dans $\mathbb{Z}$. Montrons que la forme bilinéaire B donnée par la formule

$$B(P,Q)=\frac{2}{\beta-\beta^*}(\beta S(P,Q)-S(P,\beta Q))$$

vérifie les propriétés (i), (ii) et (iii). La forme S vérifie

$$S(\alpha P,\alpha Q)=\deg\alpha\, S(P,Q);$$

d'où

$$S(\alpha P,Q)=S(P,\alpha^* Q). \tag{3}$$

On a donc

$$S(P,\beta P)=S(P,\beta^* P)=S\left(P,\frac{\beta+\beta^*}{2}P\right)=\frac{\beta+\beta^*}{2}S(P,P),$$

d'où

$$B(P,P)=\frac{2}{\beta-\beta^*}\left(\beta S(P,P)-\frac{\beta+\beta^*}{2}S(P,P)\right)=S(P,P)=h(P).$$

Ensuite, pour montrer (ii), il suffit de le faire pour un seul élément de $\mathcal{O}$ qui n'est pas dans $\mathbb{Z}$, par exemple β. De l'égalité

$$S(P,(\beta+\beta^*)Q)=(\beta+\beta^*)S(P,Q),$$

on tire que

$$B(P,Q)=\frac{2}{\beta^*-\beta}[\beta^* S(P,Q)-S(P,\beta^* Q)]. \tag{4}$$

On a alors

$$\begin{aligned} B(\beta P,Q)&=\frac{2}{\beta-\beta^*}[\beta S(\beta P,Q)-S(\beta P,\beta Q)]\\ &=\frac{2\beta}{\beta-\beta^*}[S(\beta P,Q)-\beta^* S(P,Q)]\\ &=\beta B(P,Q)\end{aligned}$$

grâce à (3) et (4), ce qui donne (ii). Quant à (iii), il se déduit de (3) et de (ii).

On note $\langle\ ,\ \rangle_{L,\mathfrak{p}}$ la forme bilinéaire ainsi associée à la forme quadratique h_L.

2. Théorie d'Iwasawa

Les résultats de cette partie sont donnés sans démonstration ([2] et [10]).

2.1. *Groupes de Selmer*

Donnons d'abord quelques notations. Si L est un corps, on note G_L le groupe de Galois sur L d'une clôture algébrique. Si B est un G_L-module discret, $H^i(L,B)$ désigne le groupe de cohomologie de G_L sur B. De plus, si B est le groupe des points de E à valeurs dans la clôture algébrique $\bar{L}$ de L, on notera ce groupe de cohomologie $H^i(L,E)$. Si L est une extension de $\mathbb{Q}$ et w une place non archimédienne de L, on définit L_w comme la réunion des complétés en w des extensions finies de $\mathbb{Q}$ contenues dans L. Choisissons un élément π de $\mathcal{O}$ tel que $\mathfrak{p}^h=(\pi)$ pour un entier $h\geqq 1$. Si M est un $\mathcal{O}$-module et α un élément de $\mathcal{O}$, M_α désigne le noyau de α sur M et $M(\alpha)$ la réunion des M_{α^n} pour $n\in\mathbb{N}$. En particulier, on note $M(\mathfrak{p})=M(\pi)$, $E_{\mathfrak{p}^\infty}=E(\bar{F})(\mathfrak{p})$. Soit L une extension de F. On définit alors le groupe de Selmer $S(L)^{(\alpha)}$ relatif à L et à α comme le noyau de l'application canonique

$$H^1(L,E_\alpha)\to\prod_v H^1(L_v,E)$$

où le produit est pris sur toutes les places de L. On n'utilisera en fait que les groupes de Selmer relatifs à π^n ou à π^{*n}. Soit $S(L)$ la limite inductive des $S(L)^{(\pi^n)}$ prise relativement aux applications induites par l'inclusion de E_{π^n} dans $E_{\pi^{n+1}}$. Rappelons que le groupe de Shafarevitch-Tate $Ш(L)$ est défini comme le noyau de l'application restriction

$$H^1(L,E)\to\prod_v H^1(L_v,E).$$

On a alors la suite exacte

$$0\to E(L)\otimes_{\mathcal{O}} D_{\mathfrak{p}}\to S(L)\to Ш(L)(\mathfrak{p})\to 0$$

où l'on a posé $D_{\mathfrak{p}}=K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$.

Pour des raisons techniques, on doit introduire d'autres groupes. On notera $S'(L)$ le noyau de

$$H^1(L, E_{\mathfrak{p}^\infty}) \to \prod_{v \not| \mathfrak{p}} H^1(L_v, E),$$

$Ш'(L)$ le noyau de

$$H^1(L, E) \to \prod_{v \not| \mathfrak{p}} H^1(L_v, E),$$

où les produits sont pris sur les places v de L ne divisant pas $\mathfrak{p}$, et $\Sigma(L)^{(\pi^{*n})}$ le noyau de l'application restriction

$$S(L)^{(\pi^{*n})} \to \prod_{v/\mathfrak{p}} H^1(L_v, E_{\pi^{*n}}).$$

Rappelons que l'on a noté $E_1(F)$ le noyau de l'application

$$E(F) \to \prod_{v/\mathfrak{p}} \tilde{E}_v(k_v)$$

où $\tilde{E}_v$ désigne la courbe réduite en v et k_v le corps résiduel de F en v.

Proposition 2.1. (1) *Les groupes $Ш'(N_\infty)(\mathfrak{p})$ et $Ш(N_\infty)(\mathfrak{p})$ sont égaux.*

(2) *Le groupe $Ш(F)(\mathfrak{p})$ est d'indice fini dans $Ш'(F)(\mathfrak{p})$. Si $Ш(F)(\mathfrak{p}^*)$ est fini, cet indice est égal (à une unité près) à*

$$\prod_{v/\mathfrak{p}} \left(1 - \frac{\Psi_{E/F}(v)}{Nv}\right) [E(F) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*} : E_1(F) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}]^{-1}.$$

Proposition 2.2. *L'application canonique de restriction de $S'(F)$ dans $S(N_\infty)^{G(N_\infty/F)}$ est un isomorphisme.*

2.2. *Λ-modules*

Rappelons que l'extension $\mathcal{N}_\infty = F(E_{\mathfrak{p}^\infty})$ peut s'interpréter comme le composé de $F(E_\mathfrak{p})$ et de K_∞. Soit Γ le groupe de Galois de N_∞/F que l'on peut identifier au groupe de Galois de $\mathcal{N}_\infty/F(E_\mathfrak{p})$. Soit κ le caractère de Γ à valeurs dans $\mathcal{O}_\mathfrak{p}$ donné par l'action de Γ sur $E_{\mathfrak{p}^\infty}$. On fait le choix d'un générateur topologique γ de Γ et on pose $u = \kappa(\gamma)$. On identifie l'algèbre $\mathbb{Z}_p[\![\Gamma]\!]$ avec l'algèbre Λ des séries formelles à une variable à coefficients dans $\mathbb{Z}_p$: $\gamma = 1 + T$. Le groupe de Selmer $S(N_\infty)$ est alors muni d'une structure naturelle de Λ-module discret. Donnons d'autre part l'énoncé de l'hypothèse p-adique faible de Leopoldt. Si L est une extension finie de K et v une place de L, soit $U(L_v)$ le groupe des unités locales du complété L_v de L en v. Soient $\mathscr{E}_L$ le groupe des unités globales de L et i_L l'injection diagonale

$$\mathscr{E}_L \to \prod_{v/\mathfrak{p}} U(L_v).$$

On note $\delta(L)$ la différence entre le $\mathbb{Z}_p$-rang de la clôture de $i_L(\mathscr{E}_L)$ pour la topologie p-adique et le $\mathbb{Z}$-rang de $\mathscr{E}_L$.

Hypothèse p*-adique faible de Leopoldt: les nombres entiers* $\delta(L)$ *sont bornés lorsque* L *parcourt les extensions finies de* F *contenues dans* $\mathcal{N}_\infty = F(E_{\mathfrak{p}\infty})$.

En combinant la proposition 2.1 avec un résultat de Greenberg ([6]), on trouve le résultat suivant concernant le dual de Pontryagin $Y(N_\infty)$ de $S(N_\infty)$,

$$Y(N_\infty) = \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(S(N_\infty), D_\mathfrak{p}).$$

Théorème. *Sous l'hypothèse* p*-adique faible de Leopoldt, le* Λ*-module* $Y(N_\infty)$ *est un* Λ*-module compact de type fini de* Λ*-torsion, n'ayant pas de sous-*Λ*-modules finis non nuls.*

On note $f(E/F, T)$ «la» série caractéristique de $Y(N_\infty)$ (définie à une unité près de Λ). La définition de $\mathscr{L}_\mathfrak{p}$ a été donnée dans l'introduction. La limite de $\mathscr{L}_\mathfrak{p}(E/F, s)/(s-1)^{n_{E/F}}$ lorsque s tend vers 1 est égale à une unité près à la valeur de

$$f(E/F, T)\, T^{-n_{E/F}}\, t_\mathfrak{p}(F)^{n_{E/F}} \#(E(F)(\mathfrak{p}))^{-1}$$

en $T=0$ ($t_\mathfrak{p}(F)$ est le cardinal de la composante p-primaire de $E(F(E_\mathfrak{p}))$; il a même valuation p-adique que $u-1$). Désormais, nous écrirons les résultats obtenus en terme de la série $f(E/F, T)$.

Rappelons les notations et le lemme classique suivants: si M est un Λ-module de type fini, on note M^Γ (resp. M_Γ) le plus grand sous-groupe (resp. quotient) de M sur lequel Γ agit trivialement et $\hat{M}$ le dual de Pontryagin de M.

Lemme 2.3. *Soit* M *un* Λ*-module compact de type fini et de* Λ*-torsion et* f *sa série caractéristique. Alors* $f(0)$ *est non nul si et seulement si* M_Γ *est fini, ce qui est encore équivalent à* M^Γ *fini. Dans ce cas, on a*

$$f(0) \sim \#(M_\Gamma)/\#(M^\Gamma).$$

On a noté $a \sim b$ pour a et b appartenant à $\mathbb{Q}_p^\times$ si et seulement si a/b est une unité de $\mathbb{Z}_p$.

L'application $Y(N_\infty) \to E(F) \underset{\mathcal{O}}{\otimes} D_\mathfrak{p}$ est surjective comme composé de deux applications surjectives:

$$Y(N_\infty) \to \widehat{S'(F)}$$

(par la proposition 2.2) et

$$\widehat{S'(F)} \to E(F) \underset{\mathcal{O}}{\otimes} D_\mathfrak{p}.$$

On en déduit que $T^{n_{E/F}}$ divise $f(E/F, T)$. Soit Z_∞ le Λ-module défini par l'exactitude de la suite

$$0 \to Z_\infty \to Y(N_\infty) \to \widehat{E(F) \underset{\mathcal{O}}{\otimes} D_\mathfrak{p}} \to 0.$$

Par le lemme du serpent, on a la suite exacte

$$0 \to Z_\infty^\Gamma \to Y(N_\infty)^\Gamma \to \widehat{E(F) \underset{\mathcal{O}}{\otimes} D_\mathfrak{p}} \to (Z_\infty)_\Gamma \to Y(N_\infty)_\Gamma \to \widehat{E(F) \underset{\mathcal{O}}{\otimes} D_\mathfrak{p}} \to 0.$$

Notons α_F l'homomorphisme

$$\alpha_F : Y(N_\infty)^\Gamma \to \widehat{E(F) \underset{\mathcal{O}}{\otimes} D_\mathfrak{p}}.$$

Une conséquence de la proposition 2.2 est que l'image de $(Z_\infty)_\Gamma$ dans $Y(N_\infty)_\Gamma$ est le dual de Pontryagin de $Ш'(F)(\mathfrak{p})$. En utilisant le fait que $Y(N_\infty)$ n'a pas de sous-Λ-modules finis non nuls, il est alors facile d'en déduire le résultat suivant, résultat intermédiaire en vue du théorème principal.

Proposition 2.4. (i) *La multiplicité de T dans $f(E/F, T)$ est égale à $n_{E/F}$ si et seulement si $Ш(F)(\mathfrak{p})$ est fini et si le conoyau* $\operatorname{coker} \alpha_F$ *de α_F est fini.*

(ii) *Dans ce cas, α_F est injective et la valeur de $f(E/F, T)/T^{n_{E/F}}$ en $T=0$ est à une unité près*

$$\#(Ш'(F)(\mathfrak{p}))\,\#(\operatorname{coker} \alpha_F).$$

3. Construction algébrique d'une forme bilinéaire

3.1. Enoncé des résultats

On note $\mathcal{N}_n$ le corps $F(E_{\pi^n})$. Soit $\mathcal{J}_n$ le groupe des idèles de $\mathcal{N}_n$, $U_n^{(\mathfrak{p})}$ le sous-groupe des idèles de $\mathcal{N}_n$ dont les composantes sont égales à 1 en toute place divisant $\mathfrak{p}$ et une unité ailleurs. On pose

$$\mathcal{C}_n = \mathcal{J}_n / U_n^{(\mathfrak{p})}\, \mathcal{N}_n^\times.$$

Soit $\mathcal{M}_n$ la p-extension abélienne non ramifiée au dehors de $\mathfrak{p}$ maximale de $\mathcal{N}_n$ et X_n le groupe de Galois de $\mathcal{M}_n/\mathcal{N}_n$. L'application d'Artin $(\ , \mathcal{M}_n/\mathcal{N}_n)$ induit un homomorphisme surjectif de $\mathcal{J}_n/\overline{U_n^{(\mathfrak{p})}\, \mathcal{N}_n^\times}$ sur X_n de noyau fini d'ordre premier à p. Soit X_∞ la limite projective des X_n et $T_\mathfrak{p}$ la limite projective des E_{π^n} relativement à la multiplication par π. On a alors l'interprétation suivante de $Y(N_\infty)$ ([2]).

Proposition 3.1. *Les Λ-modules $Y(N_\infty)$ et* $\operatorname{Hom}_{\mathbf{Z}_p}(T_\mathfrak{p}, X_\infty)^{G(\mathcal{N}_\infty/N_\infty)}$ *sont canoniquement isomorphes.*

Rappelons que l'on a noté $\Sigma(F)^{(\pi^{*n})}$ le sous-groupe du groupe de Selmer rendant la suite suivante exacte

$$0 \to \Sigma(F)^{(\pi^{*n})} \to S(F)^{(\pi^{*n})} \to \prod_{v/\mathfrak{p}} H^1(F_v, E_{\pi^{*n}}).$$

Ces groupes forment un système projectif pour $n \geqq 1$ avec comme applications de transition la multiplication par π^*. Le résultat suivant est le résultat principal de cette section.

Théorème 3.2. *Sous l'hypothèse $\mathfrak{p}$-adique faible de Leopoldt pour F, il existe un isomorphisme naturel Φ_F entre* $\varprojlim \Sigma(F)^{(\pi^{*n})}$ *et* $Y(N_\infty)^\Gamma$.

Remarque. Si l'on n'impose pas l'hypothèse $\mathfrak{p}$-adique faible de Leopoldt, l'homomorphisme Φ_F de $\varprojlim \Sigma(F)^{(\pi^{*n})}$ dans $Y(N_\infty)^\Gamma$ est seulement surjectif.

Les trois corollaires suivants sont donnés sous cette hypothèse.

Corollaire 3.3. *Les rangs des $\mathbb{Z}_p$-modules $\widehat{Ш(F)(\mathfrak{p})}$ et $\widehat{Ш(F)(\mathfrak{p}^*)}$ sont égaux. En particulier, $Ш(F)(\mathfrak{p})$ est fini si et seulement si $Ш(F)(\mathfrak{p}^*)$ est fini.*

Démonstration. On a la suite exacte

$$0 \to E_1(F) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*} \to \varprojlim \Sigma(F)^{(\pi^{*n})} \to \varprojlim Ш(F)_{\pi^{*n}} \tag{5}$$

et le conoyau de la dernière flèche est un sous-groupe du conoyau de l'application

$$E(F) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*} \to \prod_{v/\mathfrak{p}} E(F_v) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*}.$$

Mais $E(F_v) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*}$ est fini pour toute place v divisant $\mathfrak{p}$. Donc le rang sur $\mathbb{Z}_p$ de $\varprojlim \Sigma(F)^{(\pi^{*n})}$ est égal à la somme de $n_{E/F}$ et du rang sur $\mathbb{Z}_p$ de $\widehat{Ш(F)(\mathfrak{p}^*)}$. D'autre part, comme $Y(N_\infty)$ est de Λ-torsion, les $\mathbb{Z}_p$-rangs de $Y(N_\infty)_\Gamma$ et de $Y(N_\infty)^\Gamma$ sont égaux, et égaux à la somme de $n_{E/F}$ et du rang sur $\mathbb{Z}_p$ de $\widehat{Ш(F)(\mathfrak{p})}$. L'isomorphisme Φ_F entre $\varprojlim \Sigma(F)^{(\pi^{*n})}$ et $Y(N_\infty)^\Gamma$ permet alors de terminer la démonstration.

Corollaire 3.4. *Le dual de Pontryagin de $\varinjlim S(N_\infty)^{(\pi^{*n})}$ est un Λ-module de type fini et de Λ-torsion.*[1]

Démonstration. Par le corollaire 3.3, pour toute extension finie L de F contenue dans N_∞, les $\mathbb{Z}_p$-rangs de $\widehat{Ш(L)(\mathfrak{p})}$ et de $\widehat{Ш(L)(\mathfrak{p}^*)}$ sont égaux. On peut d'autre part facilement montrer que l'homomorphisme de restriction

$$\varinjlim S(L)^{(\pi^{*n})} \to (\varinjlim S(N_\infty)^{(\pi^{*n})})^{G(N_\infty/L)}$$

a un noyau et un conoyau finis. La suite exacte

$$0 \to E(L) \underset{\mathcal{O}}{\otimes} D_{\mathfrak{p}^*} \to \varinjlim S(L)^{(\pi^{*n})} \to Ш(L)(\mathfrak{p}^*) \to 0$$

et les théorèmes généraux sur les Λ-modules de type fini permettent alors de conclure (on rappelle que $E(N_\infty)$ modulo torsion est un groupe abélien de type fini, [10]).

Corollaire 3.5. *Si $Ш(F)(\mathfrak{p})$ est fini, les $\mathbb{Z}_p$-modules $E_1(F) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*}$ et $Y(N_\infty)^\Gamma$ sont isomorphes canoniquement.*

Démonstration. L'hypothèse implique que $\varprojlim Ш(F)_{\pi^{*n}}$ est nul (à l'aide du corollaire 3.3). On utilise alors la suite exacte (5) et le théorème 3.2.

---

[1] Note. On peut en fait montrer qu'il existe un pseudo-isomorphisme entre le dual de Pontryagin de $\varinjlim S(N_\infty)^{(\pi^{*n})}$ et $\widehat{Y(N_\infty)}$ (l'action de Λ étant modifiée par $\gamma \mapsto \gamma^{-1}$). Cela permet alors de montrer un théorème analogue au théorème donné dans l'introduction pour la fonction caractéristique du groupe de Selmer relatif à N_∞ et à p^∞, la forme bilinéaire $\langle , \rangle_{F,\mathfrak{p}}$ étant en particulier remplacée par la forme bilinéaire symétrique associée à h_F

Remarquons que le dual de Pontryagin de $D_\mathfrak{p}$ est $\mathcal{O}_\mathfrak{p}$. Donc celui de $E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{p}$ est

$$\mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{p}, \mathcal{O}_\mathfrak{p}).$$

De l'homomorphisme $\alpha_F \circ \Phi_F$

$$E_1(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*} \to \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{p}, \mathcal{O}_\mathfrak{p}),$$

on déduit la forme bilinéaire $\{\ ,\ \}_{F,\mathfrak{p}}$ donnée par la formule

$$\{z, z'\}_{F,\mathfrak{p}} = \alpha_F \circ \Phi_F(z')(z)$$

sur $E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{p} \times E_1(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*}$ et prolongée à $E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{p} \times E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*}$. On donnera en 3.3 quelques propriétés de cette forme bilinéaire. Notons cependant dès maintenant que la remarque suivant le théorème 3.2 entraine la proposition suivante, vraie sans aucune hypothèse de Leopoldt.

Proposition 3.6. *Les rangs des formes bilinéaires* $\{\ ,\ \}_{L,\mathfrak{p}}$ *sont bornés lorsque* L *parcourt les extensions finies de* N_∞/F.

Démonstration. Le rang de $\{\ ,\ \}_{L,\mathfrak{p}}$ est majoré par le $\mathbb{Z}_p$-rang de $Y(N_\infty)^{G(N_\infty/L)}$ qui est borné lorsque L parcourt les sous-extensions finies de N_∞/F.

Imposons de nouveau l'hypothèse p-adique faible de Leopoldt et de plus la finitude de $Ш(F)(\mathfrak{p})$; alors $\{\ ,\ \}_{F,\mathfrak{p}}$ est non dégénérée si et seulement si le conoyau de α_F est fini et on a

$$\#(\mathrm{coker}\ \alpha_F) \sim \frac{\det\{z_i, z'_j\}_{F,\mathfrak{p}}\,[B(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*} : E_1(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*}]}{[B(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{p} : \sum \mathcal{O}_\mathfrak{p} z_i]\,[B(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*} : \sum \mathcal{O}_{\mathfrak{p}^*} z'_j]}$$

où $(z_1, \ldots, z_{n_{E/F}})$ (resp. $(z'_1, \ldots, z'_{n_{E/F}})$) forme un système $\mathcal{O}_\mathfrak{p}$ (resp. $\mathcal{O}_{\mathfrak{p}^*}$)-linéairement indépendant d'éléments de $B(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{p}$ (resp. $B(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*}$) avec $B(F) = E(F)/\Omega(F)$. En particulier, en choisissant z_i et z'_i sous la forme

$$z_i = P_i \otimes 1 \qquad z'_i = P_i \otimes 1$$

avec P_i appartenant à $E(F)$, et en posant

$$\{P, Q\}_{F,\mathfrak{p}} = \{P \otimes 1, Q \otimes 1\}_{F,\mathfrak{p}}$$

pour P et Q appartenant à $E(F)$, on a

$$\#(\mathrm{coker}\ \alpha_F) \sim \frac{\det\{P_i, P_j\}_{F,\mathfrak{p}}\,[E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*} : E_1(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_{\mathfrak{p}^*}]}{[E(F) : \sum \mathcal{O} P_i]} \#(\Omega(F)(\mathfrak{p})).$$

D'où la formule

$$\mathscr{L}_\mathfrak{p}(E/F, s)/(s-1)^{n_{E/F}}|_{s=1} \sim \prod_{v/\mathfrak{p}} \left(1 - \frac{\Psi_{E/F}(v)}{Nv}\right) \frac{t_\mathfrak{p}(F)^{n_{E/F}} \det\{P_i, P_j\}_{F,\mathfrak{p}}}{[E(F) : \sum \mathcal{O} P_i]} \#(Ш(F)(\mathfrak{p})). \tag{6}$$

3.2. Construction

Commençons par donner une idée de la construction de l'homomorphisme Φ_F. L'idée due à Weil ([12]) consiste à comparer théorie de Kummer sur la courbe elliptique et théorie de Kummer multiplicative. C'est la descente classique. Elle est tout à fait essentielle pour montrer que le groupe de Selmer d'une courbe elliptique sur un corps de nombres relatif à une isogénie est fini. Le principe est le suivant. La division d'un point de $E(F)$ par π^{*n} sur le corps $\mathscr{F}_n = F(E_{q^n})$ (où $q = \pi\pi^*$) permet par la théorie de Kummer multiplicative d'obtenir un élément de $\mathscr{F}_n^\times$ et même de $\mathscr{N}_n^\times$ modulo les puissances q^n-ièmes. L'idéal engendré par cet élément est alors la puissance q^n-ième d'un idéal de $\mathscr{N}_n$. On pourrait alors associer au point l'image de cet idéal par l'application de réciprocité d'Artin dans le groupe de Galois du corps de Hilbert de $\mathscr{N}_n$. Cependant, en se limitant aux points de $E_1(F)$, il est possible de lui associer par une méthode plus fine un élément du groupe de Galois X_n. Il reste encore à préciser cette idée par

– l'étude des actions de $G(\mathscr{N}_n/F)$ sur les différents éléments considérés,
– leur compatibilité lorsqu'on effectue la descente relativement à chacun des $\pi^{*n}(n \geqq 1)$ et le passage à la limite projective.

3.2.1. Accouplement de Weil. Soit l'accouplement de Weil W_n

$$W_n : E_{\pi^n} \times E_{\pi^{*n}} \to \mu_{q^n}$$

défini de la manière suivante: soient u un élément de E_{π^n}, v un élément de $E_{\pi^{*n}}$ et u' l'élément de E_{π^n} tel que $\pi^{*n} u' = u$. Il existe une fonction $f_{n,u}$ (resp. $g_{n,u}$) rationnelle sur $\mathscr{N}_n$ de diviseur

$$q^n((u) - (O))$$

(resp.

$$\sum_{r \in E_{\pi^{*n}}} (u' + r) - (r)).$$

On a évidemment la relation

$$\operatorname{div}(f_{n,u} \circ \pi^{*n}) = q^n \operatorname{div}(g_{n,u});$$

donc quitte à changer $f_{n,u}$ par une constante, on a l'égalité

$$f_{n,u}(\pi^{*n} P) = g_{n,u}(P)^{q^n}.$$

On pose alors

$$W_n(u, v) = g_{n,u}(P + v)/g_{n,u}(P). \tag{7}$$

Propriétés 3.7. (1) *L'accouplement W_n définit un isomorphisme de G_F-modules*

$$E_{\pi^{*n}} \to \operatorname{Hom}(E_{\pi^n}, \mu_{q^n})$$
$$v \mapsto (u \mapsto W_n(u, v)).$$

(2) *Si α appartient à $\mathcal{O}$,*

$$W_n(\alpha u, v) = W_n(u, \alpha^* v).$$

(3) *Si u appartient à E_{π^n} et v à $E_{\pi^{*n+1}}$,*

$$W_{n+1}(u, v) = W_n(u, \pi^* v).$$

Démonstration de (3). La comparaison des diviseurs de $g_{n+1,u}$ et de $g_{n,u}$ montre que

$$g_{n+1,u}(P) = C g_{n,u}(\pi^* P)$$

où C est une constante. D'où

$$\begin{aligned} W_{n+1}(u, v) &= g_{n+1,u}(P+v)/g_{n+1,u}(P) \\ &= g_{n,u}(\pi^* P + \pi^* v)/g_{n,u}(\pi^* P) \\ &= W_n(u, \pi^* v). \end{aligned}$$

3.2.2. Construction (niveau fini).

Lemme 3.8. *On a un isomorphisme de $G(\mathcal{N}_n/F)$-modules*

$$H^1(\mathcal{N}_n, E_{\pi^{*n}}) \to \mathrm{Hom}(E_{\pi^n}, \mathcal{N}_n^\times / \mathcal{N}_n^{\times q^n}).$$

On notera $f \to \tilde{f}$ cet isomorphisme.
On a besoin pour la démonstration du lemme général.

Lemme 3.9. *Soient A un groupe cyclique d'ordre une puissance d'un nombre premier impair et Δ un groupe d'automorphismes de A. Alors $H^i(\Delta, A)$ est nul pour $i \geqq 1$.*

Démonstration. Le groupe Δ est cyclique, il suffit donc de calculer $H^i(\Delta, A)$ pour $i=1$ et 2 et cela peut se faire tout à fait explicitement (voir par exemple G. Poitou, Conditions globales pour les problèmes de plongement à noyau abélien, Ann. Inst. Fourier, t. 29 (1979), 1-14).

Démonstration du lemme 3.8. Le lemme 3.9. montre la nullité de

$$H^i(\mathcal{F}_n/\mathcal{N}_n, E_{\pi^{*n}})$$

pour $i \geqq 1$ (avec toujours $\mathcal{F}_n = F(E_{q^n})$). On en déduit que la restriction

$$H^1(\mathcal{N}_n, E_{\pi^{*n}}) \to H^1(\mathcal{F}_n, E_{\pi^{*n}})^{G(\mathcal{F}_n/\mathcal{N}_n)}$$

est un isomorphisme. Mais l'on a

$$H^1(\mathcal{F}_n, E_{\pi^{*n}}) = \mathrm{Hom}(G(\bar{F}/\mathcal{F}_n), E_{\pi^{*n}}).$$

L'accouplement de Weil W_n induit alors un isomorphisme

$$H^1(\mathcal{F}_n, E_{\pi^{*n}}) \to \mathrm{Hom}(E_{\pi^n}, H^1(\mathcal{F}_n, \mu_{q^n})).$$

Par le lemme 3.9., les groupes $H^1(\mathscr{F}_n, \mu_{q^n})^{G(\mathscr{F}_n/\mathscr{N}_n)}$ et $H^1(\mathscr{N}_n, \mu_{q^n})$ sont isomorphes car $\mathscr{F}_n = \mathscr{N}_n(\mu_{q^n})$. La théorie de Kummer multiplicative donne alors un isomorphisme de $H^1(\mathscr{N}_n, \mu_{q^n})$ avec $\mathscr{N}_n^\times / \mathscr{N}_n^{\times q^n}$. D'où le lemme 3.8.

On peut de même établir un isomorphisme analogue dans le cas local.

Lemme 3.10. *Pour toute place v de $\mathscr{N}_n$, on a un isomorphisme canonique*

$$H^1(\mathscr{N}_{n,v}, E_{\pi^{*n}}) \to \mathrm{Hom}(E_{\pi^n}, \mathscr{N}_{n,v}^\times / \mathscr{N}_{n,v}^{\times q^n}).$$

Par définition, un élément h de $H^1(\mathscr{N}_n, E_{\pi^{*n}})$ appartient à $\Sigma(\mathscr{N}_n)^{(\pi^{*n})}$ si et seulement si ses images par localisation appartiennent à $E(\mathscr{N}_{n,v})/\pi^{*n} E(\mathscr{N}_{n,v})$ pour v ne divisant pas $\mathfrak{p}$ et sont nulles pour v divisant $\mathfrak{p}$. Donc, pour toute place v divisant $\mathfrak{p}$, $\tilde{h}(u)$ appartient à $\mathscr{N}_{n,v}^{\times q^n}$ $(u \in E_{\pi^n})$. Le lemme suivant permet de comprendre quelle propriété locale vérifie $\tilde{h}(u)$ pour une place ne divisant pas $\mathfrak{p}$. On conviendra de noter $U(k)$ le groupe des unités d'un corps local k et d'identifier $U(k)/U(k)^{q^n}$ à son image dans $k^\times / k^{\times q^n}$.

Lemme 3.11. *Soit v une place de $\mathscr{N}_n$ ne divisant pas* $\mathfrak{p}$. *On a l'isomorphisme*

$$E(\mathscr{N}_{n,v})/\pi^{*n} E(\mathscr{N}_{n,v}) \to \mathrm{Hom}(E_{\pi^n}, U(\mathscr{N}_{n,v})/U(\mathscr{N}_{n,v})^{q^n}).$$

Démonstration. Une première démonstration séparait les cas où v ne divise pas p et où v divise $\mathfrak{p}^*$ et utilisait une étude précise du groupe formel dans le second cas. La démonstration qui suit, plus simple, m'a été indiquée par J. Oesterlé. Considérons les deux suites exactes

$$0 \to E(\mathscr{N}_{n,v})/\pi^n E(\mathscr{N}_{n,v}) \to H^1(\mathscr{N}_{n,v}, E_{\pi^n}) \to H^1(\mathscr{N}_{n,v}, E)_{\pi^n} \to 0,$$
$$0 \to E(\mathscr{N}_{n,v})/\pi^{*n} E(\mathscr{N}_{n,v}) \to H^1(\mathscr{N}_{n,v}, E_{\pi^{*n}}) \to H^1(\mathscr{N}_{n,v}, E)_{\pi^{*n}} \to 0.$$

Les deux groupes du milieu sont en dualité exacte et l'orthogonal de

$$E(\mathscr{N}_{n,v})/\pi^{*n} E(\mathscr{N}_{n,v})$$

est exactement

$$E(\mathscr{N}_{n,v})/\pi^n E(\mathscr{N}_{n,v}).$$

Soit $\mathscr{N}_{n,v}^{nr}$ l'extension non ramifiée maximale de $\mathscr{N}_{n,v}$. Comme v ne divise pas $\mathfrak{p}$, la suite

$$0 \to E_{\pi^n} \to E(\mathscr{N}_{n,v}^{nr}) \to E(\mathscr{N}_{n,v}^{nr}) \to 0$$

est exacte. On déduit alors de la nullité de

$$H^1(\mathscr{N}_{n,v}^{nr}/\mathscr{N}_{n,v}, E(\mathscr{N}_{n,v}^{nr}))$$

l'isomorphisme

$$E(\mathscr{N}_{n,v})/\pi^n E(\mathscr{N}_{n,v}) \xrightarrow{\sim} H^1(\mathscr{N}_{n,v}^{nr}/\mathscr{N}_{n,v}, E_{\pi^n}).$$

L'orthogonal de ce dernier groupe dans

$$H^1(\mathscr{N}_{n,v}, E_{\pi^{*n}}) \xrightarrow{\sim} \mathrm{Hom}(E_{\pi^n}, \mathscr{N}_{n,v}^\times / \mathscr{N}_{n,v}^{\times q^n})$$

est alors exactement par la théorie du corps de classes

$$\mathrm{Hom}(E_{\pi^n}, U(\mathscr{N}_{n,v})/U(\mathscr{N}_{n,v})^{q^n}).$$

Rappelons que si h est un élément de $H^1(\mathcal{N}_n, E_{\pi^{*n}})$, $\tilde{h}$ est son image dans $\mathrm{Hom}(E_{\pi^n}, \mathcal{N}_n^\times/\mathcal{N}_n^{\times q^n})$. Le lemme 3.11 a comme corollaire le lemme suivant.

Lemme 3.12. *h appartient à $\Sigma(\mathcal{N}_n)^{(\pi^{*n})}$ si et seulement si $\tilde{h}(u)$ appartient à $\mathcal{N}_{n,v}^{\times q^n}$ pour toute place v divisant $\mathfrak{p}$ et si $v_{\mathcal{N}_n}(\tilde{h}(u))$ est divisible par q^n pour toute place v (pour u quelconque dans E_{π^n}).*

Posons $G_n = G(\mathcal{N}_n/F)$ et rappelons que l'on a noté $\mathcal{C}_n$ le groupe $\mathcal{J}_n/\mathcal{N}_n^\times U_n^{(\mathfrak{p})}$. Posons d'autre part

$$\Omega_n = \prod_{v/\mathfrak{p}} \mu_{q^n}(\mathcal{N}_{n,v}).$$

C'est un groupe d'ordre borné. On a un homomorphisme naturel

$$\mathrm{Hom}(E_{\pi^n}, \Omega_n) \to \mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n)$$

dont le noyau est $\mathrm{Hom}(E_{\pi^n}, \mu_{q^n}(\mathcal{N}_n))$. Nous allons maintenant donner l'analogue du théorème 3.2 à un niveau fini.

Proposition 3.13. *Il existe une suite exacte naturelle*

$$\mathrm{Hom}(E_{\pi^n}, \Omega_n)^{G_n} \to \mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n)^{G_n} \xrightarrow{\eta_n} \Sigma(F)^{(\pi^{*n})} \to 0.$$

Remarque. Le noyau de la première application est bien sûr

$$\mathrm{Hom}(E_{\pi^n}, \mu_{q^n}(\mathcal{N}_n))^{G_n}$$

qui est isomorphe par l'accouplement de Weil à $E_{\pi^{*n}}(F)$.

Démonstration. Nous allons donner une description complète de l'homomorphisme η_n. Cependant, cela entre très certainement dans le cadre des théorèmes de dualité globale.

On note d_n la projection sur $\bar{F}^\times$ du produit direct $\bar{F}^\times U_n^{(\mathfrak{p})}$ considéré comme sous-groupe de la réunion des groupes d'idèles des extensions finies de F contenues dans $\bar{F}$. Soit f un élément de $\mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n)^{G_n}$. Si u appartient à E_{π^n}, soit f'_u un représentant de $f(u)$ dans $\mathcal{J}_n$. Alors,

$$d_n(f_u'^{q^n}) = a_u \quad \text{avec } a_u \in \mathcal{N}_n^\times ;$$

a_u est défini modulo $\mathcal{N}_n^{\times q^n}$ et vérifie les propriétés du lemme 3.12. Il existe donc un élément h de $\Sigma(\mathcal{N}_n)^{(\pi^{*n})}$ tel que

$$\tilde{h}(u) \equiv a_u \text{ modulo } \mathcal{N}_n^{\times q^n}.$$

A défaut d'avoir encore trouvé $\eta_n(f)$, on a pour le moment construit la restriction de l'élément cherché à $G(\bar{F}/\mathcal{N}_n)$. Cela suffit dans le cas où $E_{\pi^{*n}}(F_v)$ est nul pour toute place v divisant $\mathfrak{p}$, car on a alors l'égalité entre $\Sigma(F)^{(\pi^{*n})}$ et $\Sigma(\mathcal{N}_n)^{(\pi^{*n})G_n}$. Dans le cas général, il faut reprendre cette construction facile en la précisant.

Considérons la suite d'applications

$$\mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n) \to \mathrm{Ext}^1(E_{\pi^n}, \mathcal{N}_n^\times U_n^{(\mathfrak{p})}) \xrightarrow{d_n} \mathrm{Ext}^1(E_{\pi^n}, \mathcal{N}_n^\times)$$

et soit g l'image de f dans le dernier groupe. C'est par exemple par définition la classe de

$$(u, v) \to d_n(f'_{u+v}/f'_u\, f'_v).$$

On a d'autre part la suite exacte

$$\mathrm{Hom}(E_{\pi^n}, \bar{F}^\times) \to \mathrm{Hom}(E_{\pi^n}, \bar{F}^\times/\mathcal{N}_n^\times) \to \mathrm{Ext}^1(E_{\pi^n}, \mathcal{N}_n^\times) \to \mathrm{Ext}^1(E_{\pi^n}, \bar{F}^\times).$$

Le dernier groupe est nul car $\bar{F}^\times$ est p-divisible. Donc, il existe un élément β de $\mathrm{Hom}(E_{\pi^n}, \bar{F}^\times/\mathcal{N}_n^\times)$ dont l'image est g, ce qui veut dire qu'il existe des représentants β'_u de $\beta(u)$ dans $\bar{F}^\times$ tels que l'application $u \to f'_u\, \beta'^{-s}_u$ soit un homomorphisme de E_{π^n} à valeurs dans $\mathcal{J}_n \bar{F}^\times/U_n^{(\mathfrak{p})}$. De plus deux tels choix de β'_u diffèrent d'un homomorphisme de E_{π^n} dans $\bar{F}^\times$. D'autre part, comme f est invariant par $G(\bar{F}/F)$, l'idèle

$$\sigma f'_{\sigma^{-1}u} f'^{-1}_u\, \sigma \beta'^{-1}_{\sigma^{-1}u} \beta'_u$$

appartient à $\bar{F}^\times U_n^{(\mathfrak{p})}$ pour $\sigma \in G(\bar{F}/F)$. Notons $t_u(\sigma)$ sa projection sur $\bar{F}^\times$. Alors $u \to t_u(\sigma)$ est un homomorphisme de E_{π^n} dans $\bar{F}^\times$ (donc dans μ_{q^n}). Il existe donc un élément $s(\sigma)$ de $E_{\pi^{*n}}$ tel que

$$W_n(u, s(\sigma)) = t_u(\sigma).$$

De la relation

$$t_u(\sigma\tau) = \sigma t_{\sigma^{-1}u}(\tau)\, t_u(\sigma),$$

on déduit que s est un 1-cocycle de $G(\bar{F}/F)$ à valeurs dans $E_{\pi^{*n}}$. Un choix différent des représentants f'_u et β'_u modifie s par un cobord. Soit $\bar{s}$ la classe de s dans $H^1(F, E_{\pi^{*n}})$. La restriction de $\bar{s}$ à $H^1(\mathcal{N}_n, E_{\pi^{*n}})$ est exactement l'élément h de $\Sigma(\mathcal{N}_n)^{(\pi^{*n})}$. Comme $H^1(\mathcal{N}_{n,v}/F_v, E)$ est nul pour toute place v ne divisant pas $\mathfrak{p}$, la restriction de $\bar{s}$ à $H^1(F_v, E)$ est nulle pour une telle place. Si v est une place au dessus de $\mathfrak{p}$,

$$u \mapsto (f'_u)_v\, \beta'^{-1}_u$$

est un homomorphisme de E_{π^n} dans μ_{q^n} qui est associé par l'accouplement de Weil à un élément w de $E_{\pi^{*n}}$. La restriction de s à $G(\bar{F}_v/F_v)$ est le cobord $(\sigma \to \sigma w - w)$. En posant

$$\eta_n(f) = \bar{s},$$

on définit ainsi un homomorphisme η_n

$$\eta_n : \mathrm{Hom}(E_{\pi^n}, \mathscr{C}_n)^{G_n} \to \Sigma(F)^{(\pi^{*n})}.$$

Le calcul du noyau de η_n se fait aisément: si s est un cobord, quitte à changer le choix des β'_u, on peut supposer que

$$\sigma \beta'_{\sigma^{-1}u} \beta'^{-1}_u = d_n(\sigma f'_{\sigma^{-1}u} f'^{-1}_u).$$

Si σ appartient à $G(\bar{F}/\mathcal{N}_n)$, le terme de droite vaut 1, donc β'_u appartient à $\mathcal{N}_n^\times$ et l'on peut remplacer f'_u par $\beta'^{-1}_u f'_u$. Comme $f'^{q^n}_u$ appartient alors à $U_n^{(\mathfrak{p})}$, on peut modifier f'_u par un élément de $U_n^{(\mathfrak{p})}$ de manière à ce que $u \mapsto f'_u$ soit un élément de

$$\mathrm{Hom}(E_{\pi^n}, \Omega_n)^{G_n}.$$

Le noyau de η_n contenant trivialement l'image de ce groupe, il est donc égal à cette image.

Il reste à montrer la surjectivité. Soit $\bar{s}$ un élément de $\Sigma(F)^{(\pi^* n)}$ et s un cocycle le représentant. Posons

$$t_u(\sigma) = W_n(u, s(\sigma)) \quad \text{pour } \sigma \in G(\bar{F}/F).$$

Il existe $\beta'_u \in \bar{F}^\times$ tel que $t_u(\sigma) = \sigma\,\beta'_u/\beta'_u$ pour $\sigma \in G(\bar{F}/\mathcal{N}_n)$. De plus,

$$a_u = \beta'^{q^n}_u$$

appartient à $\mathcal{N}_{n,v}^{\times q^n}$ pour toute place divisant $\mathfrak{p}$ et est de valuation divisible par q^n pour les autres places par le lemme 3.12. D'autre part, la restriction de s à $G(\bar{F}_v/F_v)$ étant un cobord pour v divisant $\mathfrak{p}$, on a

$$t_u(\sigma) = \sigma\,\zeta_v(\sigma^{-1}u)\,\zeta_v(u)^{-1} \qquad (\sigma \in G(\bar{F}_v/F_v))$$

avec ζ_v dans $\mathrm{Hom}(E_{\pi^n}, \mu_{q^n})$. Posons

$$c_{\sigma,u} = \sigma\,\beta'_{\sigma^{-1}u}\,\beta'^{-1}_u\,t_u(\sigma)^{-1}.$$

Alors, pour toute place v de F divisant $\mathfrak{p}$, si l'on choisit un prolongement v_0 de v à $\bar{F}$, on a

$$c_{\sigma,u} = \sigma(\beta'_{\sigma^{-1}u}\,\zeta_v(\sigma^{-1}u)^{-1})/(\beta'_u\,\zeta_v(u)^{-1}) \qquad (\sigma \in G(\bar{F}_{v_0}/F_v)). \tag{8}$$

On définit maintenant un idèle f'_u de $\mathcal{N}_n$ par

$$\begin{aligned}
(f'_u)_w &= 1 && \text{si } w/\infty,\\
w_{\mathcal{N}_n}((f'_u)_w) &= w_{\mathcal{N}_n}(a_u)/q^n && \text{si } w\not/\mathfrak{p},\ w\not/\infty,\\
(f'_u)_{v_0} &= \zeta_v(u)^{-1}\,\beta'_u && \text{si } v/\mathfrak{p},\\
(f'_u)_w &= \sigma(f'_{\sigma^{-1}u})_{v_0}\,c^{-1}_{\sigma,u} && \text{si } w/\mathfrak{p},\ w = \sigma v_0.
\end{aligned}$$

La relation (8) assure que f'_u appartient à $\mathcal{J}_n$, que sa classe $f(u)$ dans $\mathcal{C}_n$ ne dépend pas des choix de v_0 et de σ et que $u \mapsto f(u)$ est un élément de

$$\mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n)^{G_n}$$

tel que $\eta_n(f) = \bar{s}$, ce qui termine la démonstration de la proposition 3.13.

3.2.3. Comparaison des différents niveaux. Soit $N_{n,n-1}$ la norme de $\mathcal{N}_n$ à $\mathcal{N}_{n-1}$ (sur $\mathcal{C}_n$ ou sur $\mathcal{N}_n^\times$).

Lemme 3.14. *Pour n assez grand, il existe une unique application t_n:*

$$t_n\colon \mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n)^{G_n} \to \mathrm{Hom}(E_{\pi^{n-1}}, \mathcal{C}_{n-1})^{G_{n-1}}$$

vérifiant

$$t_n(h)(q\,u) = N_{n,n-1}(h(u)).$$

On a pour cela besoin du lemme.

Lemme 3.15. *Soit i_n l'application de $\mathcal{C}_{n-1}$ dans $\mathcal{C}_n$ induite par l'inclusion $\mathcal{J}_{n-1} \to \mathcal{J}_n$. Alors, pour n assez grand, i_n est injective sur $(\mathcal{C}_{n-1})_{q^n}$.*

Démonstration. Soit x un élément de $\mathscr{J}_{n-1}$ tel que

$$x^{q^n} = a\, y (a \in \mathscr{N}_{n-1}^{\times},\ y \in U_{n-1}^{(\mathfrak{p})}),$$
$$x = b\, z (b \in \mathscr{N}_n^{\times},\ z \in U_n^{(\mathfrak{p})}).$$

Alors, a est égal à b^{q^n} et a appartient à $\mathscr{N}_{n-1,v}^{\times q^n}$ pour toute place v divisant p. Mais le noyau de l'application restriction

$$H^1(\mathscr{N}_n/\mathscr{N}_{n-1}, \mu_{q^n}(\mathscr{N}_n)) \to \prod_{v/\mathfrak{p}} H^1(\mathscr{N}_{n,v}/\mathscr{N}_{n-1,v}, \mu_{q^n}(\mathscr{N}_{n,v}))$$

est nul pour n assez grand. Cela implique que a appartient à $\mathscr{N}_{n-1}^{\times q^n}$ et que x appartient à $\mathscr{N}_{n-1}^{\times} U_{n-1}^{(\mathfrak{p})}$.

Démonstration du lemme 3.14. Il suffit de voir que si l'on définit $t_n(h)$ par

$$t_n(h)(qu) = N_{n,n-1}(h(u)),$$

il ne dépend pas du choix de u, c'est-à-dire que si u appartient à E_π, $N_{n,n-1}(h(u))$ est égal à 1. D'après le lemme 3.15, il suffit de montrer que

$$i_n(N_{n,n-1}(h(u))) = 1.$$

Mais cela est égal à

$$\prod_{\sigma \in G(\mathscr{N}_n/\mathscr{N}_{n-1})} \sigma\, h(u) = h(u)^q = 1.$$

Lemme 3.16. *Soit r_n l'application*

$$r_n : \Sigma(F)^{(\pi^{*n})} \to \Sigma(F)^{(\pi^{*n-1})}$$

induite par la multiplication par π^*. On a

$$r_n \circ \eta_n = \eta_{n-1} \circ t_n \quad (\textit{pour } n \textit{ assez grand}).$$

Démonstration. Il suffit de reprendre la construction de η_n. Soit f un élément de

$$\mathrm{Hom}(E_{\pi^n}, \mathscr{C}_n)^{G_n}$$

et $h = t_n(f)$. En remarquant que

$$i_n \circ t_n(f)(qu) = f(u)^q,$$

on voit que l'on peut choisir les représentants de $f(u)$ et de $h(u)$ de manière à ce que

$$h'_{qu} f'^{-q}_u = y_u \alpha_u \quad (y_u \in U_n^{(\mathfrak{p})},\ \alpha_u \in \mathscr{N}_n^{\times}),$$
$$\beta'^{(h)}_{qu} = \beta'^{(f)}_u \alpha_u$$

et on en déduit que

$$t^{(h)}_{qu}(\sigma) = t^{(f)}_u(\sigma)^q$$

et

$$W_n(u, \eta_n(f)(\sigma))^q = W_{n-1}(qu, \eta_{n-1}(h)(\sigma)),$$

c'est-à-dire grâce aux propriétés 3.7,

$$r_n \circ \eta_n(f) = \eta_{n-1}(h) = \eta_{n-1} \circ t_n(f).$$

Soit η'_n l'application déduite de η_n par passage au quotient par le noyau de η_n et posons

$$\Xi_n = \delta^{-1}\, \pi^{*-n}\, \eta'^{-1}_n$$

où δ est le degré de l'extension $F(E_\mathfrak{p})/F$.

Proposition 3.17. *Les homomorphismes Ξ_n forment un système compatible d'homomorphismes qui induisent un isomorphisme Ξ_F*

$$\Xi_F : \varprojlim \Sigma(F)^{(\pi^{*n})} \to \mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p}, \varprojlim \mathscr{C}_n(p))^{G(\mathscr{N}_\infty/F)}$$

où la limite projective des $\mathscr{C}_n(p)$ est prise relativement à la norme.

Démonstration. La première partie de la proposition se déduit du lemme 3.16. On a en effet

$$N_{n,n-1}(\Xi_n(h)(u)) = \Xi_{n-1}(r_n(h))(\pi u).$$

Comme $\mathrm{Hom}(E_{\pi^n}, \Omega_n)^{G_n}$ est un groupe fini d'ordre borné par rapport à n (isomorphe à

$$\prod_{v/\mathfrak{p}} E_{\pi^{*n}}(F_v)),$$

l'ensemble d'arrivée de Ξ_F est isomorphe à

$$\varprojlim \mathrm{Hom}(E_{\pi^n}, \mathscr{C}_n)^{G(\mathscr{N}_\infty/F)}.$$

Mais ce $\mathbb{Z}_p$-module est aussi isomorphe à

$$\varprojlim \mathrm{Hom}(T_\mathfrak{p}, (\mathscr{C}_n)_{q^n})^{G(\mathscr{N}_\infty/F)} = \varprojlim \mathrm{Hom}(T_\mathfrak{p}, \mathscr{C}_n(p))^{G(\mathscr{N}_\infty/F)}.$$

En effet, si (f_n) est un élément de ce dernier groupe, l'image de f_n dans $\mathscr{C}_n$ est nécessairement d'ordre divisant q^n car f_n est invariant par $G(\mathscr{N}_\infty/\mathscr{N}_n)$:

$$\gamma f_n = f_n = f_n^{\kappa(\gamma)} \quad \text{pour } \gamma \in G(\mathscr{N}_\infty/\mathscr{N}_n)$$

et $\kappa(\gamma)$ est exactement congru à 1 modulo q^n, pour γ générateur de $G(\mathscr{N}_\infty/\mathscr{N}_n)$. D'où la proposition.

3.2.4. Fin de la démonstration du théorème 3.2. Pour finir la démonstration du théorème 3.2, il ne reste plus qu'à faire le lien entre

$$\varprojlim \mathrm{Hom}(T_\mathfrak{p}, \mathscr{C}_n(p))^\Gamma$$

et

$$\mathrm{Hom}(T_\mathfrak{p}, X_\infty)^\Gamma.$$

Soient $\mathscr{E}_n$ le groupe des unités globales de $\mathscr{N}_n$ congrues à 1 modulo toute place v au dessus de $\mathfrak{p}$ et $\bar{\mathscr{E}}_n$ son adhérence dans $\prod_{v/\mathfrak{p}} U(\mathscr{N}_{n,v})$. Rappelons que l'on a noté $\mathscr{M}_n$ la p-extension abélienne non ramifiée au dehors de $\mathfrak{p}$ maximale

de $\mathcal{N}_n$, X_n le groupe de Galois de $\mathcal{M}_n/\mathcal{N}_n$ et X_∞ la limite projective des X_n. Le $\mathbb{Z}_p$-module $\bar{\mathcal{E}}_n/\mathcal{E}_n$ est p-divisible car $\bar{\mathcal{E}}_n=\mathcal{E}_n\bar{\mathcal{E}}_n^{p^r}$ pour tout $r\in\mathbb{N}$. On a donc la suite exacte

$$0\to\bar{\mathcal{E}}_n/\mathcal{E}_n(p)\to\mathcal{C}_n(p)\to(\mathcal{J}_n/\overline{\mathcal{N}_n^\times U_n^{(\mathfrak{p})}})(p)\to 0.$$

Les applications d'Artin $(\ ,\mathcal{M}_n/\mathcal{N}_n)$ induisent un homomorphisme surjectif A

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},\varprojlim\mathcal{C}_n(p))\to\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},\varprojlim X_n(p)).$$

On remarque que l'on a l'égalité

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},\varprojlim X_n(p))^{G(\mathcal{N}_\infty/F)}=\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},X_\infty)^{G(\mathcal{N}_\infty/F)},$$

un élément de ce dernier groupe étant toujours d'ordre fini. Le composé $\Phi_F=A\circ\Xi_F$ est donc un homomorphisme surjectif de $\varprojlim\Sigma(F)^{(\pi^{*n})}$ sur

$$Y(N_\infty)^\Gamma=\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},X_\infty)^{G(\mathcal{N}_\infty/F)}.$$

Pour montrer que, dans le cas où l'hypothèse p-adique faible de Leopoldt est vérifiée, Φ_F est un isomorphisme, c'est-à-dire le théorème 3.2, il suffit maintenant de montrer:

Lemme 3.18. *Sous l'hypothèse* p*-adique faible de Leopoldt, les $\mathbb{Z}_p$-modules suivants sont égaux*

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},\varprojlim\mathcal{C}_n(p))^\Gamma=\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},\varprojlim X_n(p))^\Gamma.$$

Démonstration. Si M est un $\mathbb{Z}_p$-module, posons

$$M(-1)=\mathrm{Hom}_{\mathbb{Z}_p}(T_\mathfrak{p},M).$$

Le lemme est trivial lorsque la conjecture p-adique de Leopoldt est vraie pour tous les corps $\mathcal{N}_n$, car $\bar{\mathcal{E}}_n/\mathcal{E}_n$ n'a alors pas de torsion. Dans le cas général, $\bar{\mathcal{E}}_n/\mathcal{E}_n(p)(-1)_\Gamma$ est nul car si γ appartient à G_n, $\kappa(\gamma)^{-1}\gamma-1$ agit sur $\bar{\mathcal{E}}_n/\mathcal{E}_n$ comme une puissance de p à un automorphisme près et $\bar{\mathcal{E}}_n/\mathcal{E}_n$ est p-divisible. Pour montrer le lemme, il suffit donc de montrer que

$$\varprojlim\bar{\mathcal{E}}_n/\mathcal{E}_n(-1)^\Gamma=0.$$

Si $\mathcal{E}'_n$ est le quotient de $\mathcal{E}_n$ par son sous-groupe de torsion, on a

$$\bar{\mathcal{E}}_n/\mathcal{E}_n(-1)^\Gamma=\bar{\mathcal{E}}_n/\mathcal{E}_n(-1)^\Gamma_{q^n}=\bar{\mathcal{E}}'_n/\mathcal{E}'_n(-1)^\Gamma_{q^n}.$$

Nous allons montrer que si r est un entier tel que le défaut $\delta(\mathcal{N}_n)$ de la conjecture p-adique de Leopoldt soit constant pour $n\geqq r$ (et égal à δ), on a

$$(\bar{\mathcal{E}}'_n/\mathcal{E}'_n)_{q^n}=(\bar{\mathcal{E}}'_r/\mathcal{E}'_r)_{q^n}. \tag{9}$$

Cela montrera que la limite projective (relativement à la norme ou ce qui revient au même à la multiplication par q) de $(\bar{\mathcal{E}}'_n/\mathcal{E}'_n)_{q^n}$ est bien définie, que $(\bar{\mathcal{E}}'_n/\mathcal{E}'_n)(-1)^\Gamma$ est fini d'ordre borné par rapport à n et donc que la limite projective des $(\bar{\mathcal{E}}'_n/\mathcal{E}'_n)(-1)^\Gamma$ est nulle.

Revenons à (9). Soit $(e_1, \ldots, e_{h_n})$ une base du $\mathbb{Z}$-module $\mathscr{E}'_n$ telle que $e'_1 = e_1^{a_1}, \ldots, e'_h = e_h^{a_h}$ soit une $\mathbb{Z}$-base de $\mathscr{E}'_r$. On pose $s = a_1 \ldots a_h$. On peut extraire de $(e'_1, \ldots, e'_h)$ un système $\mathbb{Z}_p$-libre maximal, par exemple supposons que c'est $(e'_{\delta+1}, \ldots, e'_h)$. Alors $(e_{\delta+1}, \ldots, e_{h_n})$ est un système $\mathbb{Z}_p$-libre maximal de $\mathscr{E}'_n$.

Soit x un élément de $\bar{\mathscr{E}}'_n$ tel que x^{q^n} appartient à $\mathscr{E}'_n$:

$$x = \lim_{j \to \infty} \prod_{i=1}^{h_n} e_i^{\alpha_{i,j}} \qquad (\alpha_{i,j} \in \mathbb{Z}),$$

$$x^{q^n} = \prod_{i=1}^{h_n} e_i^{\beta_i} \qquad (\beta_i \in \mathbb{Z}).$$

On a une relation du type

$$\lim_{j \to \infty} \prod_{i=\delta+1}^{h} e_i^{y_{i,j}} \prod_{i=h+1}^{h_n} e_i^{u(\alpha_{i,j} q^n - \beta_i)} = 1.$$

Comme $(e_{\delta+1}, \ldots, e_{h_n})$ est $\mathbb{Z}_p$-libre, β_i est divisible par q^n pour $i > h$. Donc x peut s'écrire de la façon suivante:

$$x = y \prod_{i=h+1}^{h_n} e_i^{\beta'_i}$$

avec $y^s \in \bar{\mathscr{E}}'_r$, $\beta'_i \in \mathbb{Z}$. Comme $\bar{\mathscr{E}}'_r / \mathscr{E}'_r$ est un $\mathbb{Z}_p$-module p-divisible, on en déduit que x est congru un élément de $\bar{\mathscr{E}}'_r$ modulo $\mathscr{E}'_n$. D'où le lemme 3.18.

3.3. *Formules explicites pour la forme bilinéaire* $\{\ ,\ \}_{F,\mathfrak{p}}$ *et propriétés*

Revenons à la définition de la forme bilinéaire kummérienne $\{\ ,\ \}_{F,\mathfrak{p}}$. Le groupe $E_1(F) \underset{\mathscr{O}}{\otimes} \mathscr{O}_{\mathfrak{p}^*}$ s'injecte de manière naturelle dans $\varprojlim \Sigma(F)^{(\pi^{*n})}$ et l'on rappelle que l'on a posé

$$\{z, z'\}_{F,\mathfrak{p}} = \alpha_F \circ \Phi_F(z')(z).$$

La construction faite permet de donner des formules «explicites» pour $\{P, Q\}_{F,\mathfrak{p}}$ si P appartient à $E(F)$ et Q à $E_1(F)$. Soit ρ_n le composé de Φ_F avec la projection

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_{\mathfrak{p}}, \varprojlim \mathscr{C}_n(p))^{\Gamma} \to \mathrm{Hom}(E_{\pi^n}, \mathscr{J}_n / \overline{\mathscr{N}_n^{\times} U_n^{(\mathfrak{p})}})^{\Gamma}$$

et $\pi^{n(u)}$ l'ordre de l'élément u de E_{π^n}.

Lemme 3.19. 1. *Pour tout* $u \in E_{\pi^n}$, *on a*

$$\{P, Q\}_{F,\mathfrak{p}} u = (\rho_n(Q)(u), \mathscr{M}_n / \mathscr{N}_n)(P_n) - P_n \tag{10}$$

si P_n *est un point de* $E(\bar{F})$ *tel que* $\pi^n P_n = P$.

2. *(Décomposition locale). Soient* $S_{n,u}(Q)$ *un représentant de* $\eta_n'^{-1}(Q)(u)$ *dans* $\mathscr{J}_n$ *et* $\{P, Q\}_{n,v}^{(u)}$ *l'unique élément de* $\mathscr{O}/\pi^{n(u)}\mathscr{O}$ *tel que*

$$\{P, Q\}_{n,v}^{(u)} u = (S_{n,u}(Q)_v, \mathscr{M}_{n,v} / \mathscr{N}_{n,v})(P_n) - P_n$$

pour tout $u \in E_{\pi^n}$. *Alors*

$$\delta \pi^{*n} \{P, Q\}_{F,\mathfrak{p}} \equiv \sum_v \{P, Q\}_{n,v}^{(u)} \text{ modulo } \pi^{n(u)} \mathcal{O}_{\mathfrak{p}} \tag{11}$$

où v *parcourt les places finies de* $\mathcal{N}_n$.

Remarque. On verra par la suite qu'il est possible de choisir $S_{n,u}(Q)$ de manière à ce que l'application $Q \to S_{n,u}(Q)_v$ soit continue sur $E_1(F)$ pour la topologie v-adique $(v/\mathfrak{p})$.

Démonstration. 1. La formule (10) provient immédiatement du diagramme commutatif exact suivant

$$\begin{array}{ccccc} E_1(F) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*} & \xrightarrow{\Phi_F} & Y(N_\infty)^\Gamma & \xrightarrow{\alpha_F} & \mathrm{Hom}(E(F) \underset{\mathcal{O}}{\otimes} D_{\mathfrak{p}}, D_{\mathfrak{p}}) \\ \downarrow & & \downarrow & & \downarrow \\ E_1(F)/\pi^{*n} E_1(F) & \longrightarrow & \mathrm{Hom}(E_{\pi^n}, \mathcal{J}_n/\overline{U_n^{(\mathfrak{p})} \mathcal{N}_n^{\times}})^\Gamma & \longrightarrow & \mathrm{Hom}(E(F)/\pi^n E(F), \mathcal{O}/\pi^n \mathcal{O}). \end{array}$$

La seconde application de la ligne inférieure est

$$f \mapsto (P \bmod \pi^n E(F) \mapsto (u \mapsto (f(u), \mathcal{M}_n/\mathcal{N}_n)(P_n) - (P_n)))$$

où l'on a identifié canoniquement $\mathcal{O}/\pi^n \mathcal{O}$ et $\mathrm{Hom}(E_{\pi^n}, E_{\pi^n})$ par

$$\beta \mapsto (u \to \beta u).$$

2. La formule (11) provient de la décomposition du symbole d'Artin par la théorie du corps de classes

$$(y, \mathcal{M}_n/\mathcal{N}_n) = \prod_v (y_v, \mathcal{M}_{n,v}/\mathcal{N}_{n,v}) \quad \text{si } y \in \mathcal{J}_n.$$

Propriétés 3.20. *Si* α *appartient à* $\mathcal{O}$, *on a*

$$\alpha \{z, z'\}_{F,\mathfrak{p}} = \{\alpha z, z'\}_{F,\mathfrak{p}}$$
$$\{\alpha z, z'\}_{F,\mathfrak{p}} = \{z, \alpha^* z'\}_{F,\mathfrak{p}}.$$

Démonstration. La première formule se voit immédiatement sur (10). La deuxième se déduit du fait que

$$\Xi_F(x)(\beta u) = \Xi_F(\beta^* x)(u)$$

pour $x \in \varprojlim \Sigma(F)^{(\pi^{*n})}$, qui provient lui-même de la propriété analogue de l'accouplement de Weil

$$W_n(u, \beta^* u') = W_n(\beta u, u').$$

4. Comparaison des deux formes bilinéaires

Théorème 4.1. *Les deux formes bilinéaires* $\{\ ,\ \}_{F,\mathfrak{p}}$ *et* $\langle\ ,\ \rangle_{F,\mathfrak{p}}$ *sur* $E(F)$ *sont proportionnelles:*

$$\{\ ,\ \}_{F,\mathfrak{p}} = t_{\mathfrak{p}}(F)^{-1} \langle\ ,\ \rangle_{F,\mathfrak{p}}$$

où $t_{\mathfrak{p}}(F)$ *est le cardinal de la composante* $\mathfrak{p}$*-primaire de* $E(F(E_{\mathfrak{p}}))$.

La démonstration occupe tout le paragraphe. Les deux formes bilinéaires vérifiant les propriétés (ii) et (iii) du lemme 1.5, il suffit de montrer que si P est un point de $E(F)$, l'expression $t_{\mathfrak{p}}(F)\{P,P\}_{F,\mathfrak{p}}$ est égale à $h_F(P)=\langle P,P\rangle_{F,\mathfrak{p}}$. On remarque ensuite qu'il suffit de vérifier cela pour un sous-groupe d'indice fini de $E(F)$, par exemple pour $E_1(F)$. On commence alors par calculer $\{P,P\}_{n,v}^{(u)}$ pour toute place v ne divisant pas p (proposition 4.4). On montre ensuite que l'on peut éviter de le calculer pour les places divisant $\mathfrak{p}^*$ (lemme 4.5) puis grâce à un résultat d'unicité analogue au lemme 1.3 pour les places divisant $\mathfrak{p}$.

Rappelons que la fonction $f_{n,u}$ est de diviseur

$$q^n((u)-(O)),$$

que $g_{n,u}$ est de diviseur

$$\sum_{r\in E_{\pi^{*n}}}(u'+r)-(r) \qquad (\pi^{*n}u'=u)$$

et que les deux fonctions sont reliées par

$$f_{n,u}(\pi^{*n}P)=g_{n,u}(P)^{q^n}.$$

Lemme 4.2. *Soit P un point de $E_1(F)$ qui n'est pas de torsion et $h_{n,p}$ le cocycle associé dans $H^1(F,E_{\pi^{*n}})$. Alors, l'homomorphisme correspondant $\tilde{h}_{n,P}$ dans* $\mathrm{Hom}(E_{\pi^n},\mathscr{N}_n^{\times}/\mathscr{N}_n^{\times q^n})$ *est donné par*

$$\tilde{h}_{n,P}(u)\equiv f_{n,u}(P) \text{ modulo } \mathscr{N}_n^{\times q^n}.$$

Démonstration. Soit P_n^* un point de $E(\bar{F})$ tel que $\pi^{*n}P_n^*=P$. On a alors

$$h_{n,P}(\sigma)=\sigma P_n^*-P_n^*$$

et on cherche un élément $\tilde{h}_{n,P}(u)$ de $\mathscr{N}_n^{\times}$ tel que si

$$a^{q^n}=\tilde{h}_{n,P}(u),$$

on ait

$$\sigma a/a=W_n(u,h_{n,P}(\sigma)).$$

Mais, par définition de W_n, on a

$$\begin{aligned}W_n(u,h_{n,P}(\sigma))&=g_{n,u}(P_n^*+\sigma P_n^*-P_n^*)/g_{n,u}(P_n^*)\\&=\sigma\, g_{n,u}(P_n^*)/g_{n,u}(P_n^*)\end{aligned}$$

et $g_{n,u}(P_n^*)^{q^n}$ étant égal à $f_{n,u}(P)$, le lemme est démontré.

Posons

$$F_{n,u}(P)=\prod_r\frac{x(P-u')-x(r)}{x(P)-x(r)}$$

où le produit est étendu aux classes r de $E_{\pi^{*n}}-\{O\}$ modulo $+1$ et où u' est toujours l'unique élément de E_{π^n} tel que $\pi^{*n}u'=u$. Cette fonction ne dépend pas du modèle de Weierstrass choisi. Remarquons que l'on a

$$F_{n,u}(P)^{12}=\gamma_{\pi^{*n}}(P-u')/\gamma_{\pi^{*n}}(P).$$

et que l'on a l'égalité des diviseurs suivants

$$\operatorname{div} g_{n,u} = \operatorname{div} F_{n,u} + q^n((u') - (O)).$$

On pose

$$t_{n,u} = F_{n,u} f_{n,u'}, \qquad a_{n,u}(P) = t_{n,u}(P_n^*)^{q^n}.$$

On a donc

$$\tilde{h}_{n,P}(u) \equiv a_{n,u}(P) \text{ modulo } \mathscr{N}_n^{\times q^n}.$$

Lemme 4.3. *Supposons que v ne divise pas p. Alors,*

$$v_{\mathscr{N}_n}(a_{n,u}(P))/q^n \equiv \lambda_{\mathscr{N}_n,v}(P-u) - \lambda_{\mathscr{N}_n,v}(P) \bmod q^n \mathbb{Z}.$$

Démonstration. Soit $\Omega_n = \mathscr{F}_n(P_n^*)$. L'extension $\Omega_n/\mathscr{N}_n$ est non ramifiée en v d'où

$$v_{\mathscr{N}_n}(a_{n,u}(P))/q^n = v_{\Omega_n}(F_{n,u}(P_n^*)) + v_{\Omega_n}(f_{n,u'}(P_n^*)) \bmod q^n \mathbb{Z}.$$

D'après (1), on a

$$\begin{aligned} v_{\Omega_n}(F_{n,u}(P_n^*)) &= \lambda_{\Omega_n,v}(P-u) - \lambda_{\Omega_n,v}(P) \\ &\quad - q^n[\lambda_{\Omega_n,v}(P_n^* - u') - \lambda_{\Omega_n,v}(P_n^*)] \\ &\equiv \lambda_{\mathscr{N}_n,v}(P-u) - \lambda_{\mathscr{N}_n,v}(P) \bmod q^n \mathbb{Z}. \end{aligned}$$

D'autre part, on a

$$f_{n,u'}(P_n^*) = g_{n,u'}(P_{2n}^*)^{q^n} \quad \text{avec } \pi^{*n} P_{2n}^* = P_n^*$$

et l'extension $\mathscr{N}_n(P_{2n}^*)/\mathscr{N}_n$ est de nouveau non ramifiée en v. D'où

$$v_{\Omega_n}(f_{n,u'}(P_n^*)) \equiv 0 \bmod q^n \mathbb{Z}.$$

Cela termine la démonstration du lemme.

On considère désormais les expressions $\{\ ,\ \}_{n,v}^{(u)}$ (lemme 3.19) calculées à partir de l'idèle $S_{n,u}(P)$ vérifiant

$$\begin{aligned} S_{n,u}(P)_v &= \begin{cases} 1 & \text{si } v/\infty \\ t_{n,u}(P_{n,v}^*) & \text{si } v/\mathfrak{p} \end{cases} \\ v_{\mathscr{N}_n}(S_{n,u}(P)_v) &= v_{\mathscr{N}_n}(a_{n,u}(P))/q^n \quad \text{sinon} \end{aligned} \tag{12}$$

où $P_{n,v}^*$ est l'unique élément de $E_{1,v}(\mathscr{N}_{n,v})$ tel que $\pi^{*n} P_{n,v}^* = P$ (l'existence et l'unicité viennent de ce que π^* est un automorphisme sur $E_{1,v}(\mathscr{N}_{n,v})$). L'application $P \mapsto S_{n,u}(P)_v$ est alors continue pour la topologie v-adique si v est au dessus de $\mathfrak{p}$.

Proposition 4.4. *Supposons que v ne divise pas p. Alors, pour P appartenant à $E_1(F)$ et qui n'est pas de torsion, on a*

$$\{P, P\}_{n,v}^{(u)} u = \pi^{-n} \lambda_{\mathscr{N}_n,v}(P-u) \log_{\mathfrak{p}} \Psi_{E/\mathscr{N}_n}(v)\, u \tag{13}$$

pour tout $u \in E_{\pi^n}$.

Démonstration. Pour simplifier les notations, on posera $\Psi = \Psi_{E/\mathscr{N}_n}$. Par définition, si ω_v est une uniformisante de $\mathscr{N}_n$ en v, on a

$$\{P, P\}_{n,v}^{(u)} u = v_{\mathscr{N}_n}(a_{n,u}(P))/q^n[(\omega_v, \mathscr{M}_{n,v}/\mathscr{N}_{n,v})(P_n) - P_n]$$

où $\pi^n P_n = P$. Notons $P \mapsto \tilde{P}$ la réduction modulo v sur $E(\mathcal{N}_n(P_n)_v)$. Elle induit une injection sur E_{π^n}. D'autre part, par définition du Grössencharakter, on a

$$(\omega_v, \mathcal{M}_{n,v}/\mathcal{N}_{n,v})(\tilde{P}_n) = \Psi(v)\,\tilde{P}_n.$$

Comme $\mathcal{N}_n$ contient E_{π^n}, $\Psi(v)$ est congru à 1 modulo π^n et $\log_{\mathfrak{p}} \Psi(v)$ est congru à $\Psi(v)-1$ modulo π^{2n}. D'où:

$$\begin{aligned}\{P, P\}^{(u)}_{n,v}\, u &= q^{-n}\, v_{\mathcal{N}_n}(a_{n,u}(P))\, \pi^{-n}(\Psi(v)-1)\,\tilde{P} \\ &= [\lambda_{\mathcal{N}_n, v}(P-u) - \lambda_{\mathcal{N}_n, v}(P)]\, \pi^{-n} \log_{\mathfrak{p}} \Psi(v)\,\tilde{P},\end{aligned}$$

(la première ligne est vraie dès que v ne divise pas $\mathfrak{p}$). D'autre part, par le lemme 1.1, $\lambda_{\mathcal{N}_n, v}(P)\,\tilde{P}$ est toujours nul, de même que $\lambda_{\mathcal{N}_n, v}(P-u)(\tilde{P}-\tilde{u})$. D'où:

$$\{P, P\}^{(u)}_{n,v}\,\tilde{u} = \lambda_{\mathcal{N}_n, v}(P-u)\,\pi^{-n} \log_{\mathfrak{p}} \Psi(v)\,\tilde{u}$$

et la proposition.

Lemme 4.5. *Choisissons un entier m_0 tel que π^{m_0} annule $E(F_w)(\mathfrak{p})$ pour toute place w de F au dessus de $\mathfrak{p}^*$. Alors pour tout $n > m_0$ et pour toute place v de $\mathcal{N}_n$ au dessus de $\mathfrak{p}^*$, on a*

(i) $\pi^{m_0}\{P, P\}^{(u)}_{n,v} \equiv 0$ *modulo* $\pi^{n(u)}\mathcal{O}_{\mathfrak{p}}$

(ii) $\lambda_{\mathcal{N}_n, v}(P-u) = 0$ *pour tout* $u \in E_{\pi^n} - E_{\pi^{m_0}}$.

Démonstration. Le début du calcul fait dans la démonstration du lemme précédent montre que $\{P, P\}^{(u)}_{n,v}\,\tilde{u}$ est un multiple de $\tilde{P}$ et donc appartient à $\tilde{E}(k_w)(p)$. Comme $\tilde{E}(k_w)(p)$ est isomorphe à $E(F_w)(\mathfrak{p})$, π^{m_0} annule $\{P, P\}^{(u)}_{n,v}$ modulo $\pi^{n(u)}$. Quant à (ii), i. se déduit du lemma 1.1. En effet, la réduction d'un point P de $E(F)$ en une place w au dessus de $\mathfrak{p}^*$ est dans $\tilde{E}_w(k_w)$ et ne peut donc être égal à la réduction d'un point annulé par π^n et non par π^{m_0}.

On peut réécrire (ii) de la manière suivante:

$$\pi^{m_0}\,\lambda_{\mathcal{N}_n, v}(P-u)\,u = O \quad \text{pour tout} \quad u \in E_{\pi^n}.$$

Effectuons le calcul de $\{P, P\}_{F,\mathfrak{p}}$ en utilisant la formule (11). Choisissons un entier m supérieur à m_0 et tel que

$$\pi^m\, t_{\mathfrak{p}}(F)^{-1}\, h_F(P)$$

soit à valeurs entières pour $P \in E(F)$. Comme on a

$$\begin{aligned}h_{\mathcal{N}_n}(P-u) = h_{\mathcal{N}_n}(P) &= [\mathcal{N}_n : F]\, h_F(P) \\ &= \delta q^n\, t_{\mathfrak{p}}(F)^{-1}\, h_F(P),\end{aligned}$$

$\pi^m h_{\mathcal{N}_n}(P-u)/\pi^n$ est aussi à valeurs entières ainsi que tous les termes de la formule qui suit et qui provient d'autre part du lemme 4.5, de la définition de $h_{\mathcal{N}_n}$ et de la proposition 4.4:

$$\begin{aligned}&\delta \pi^m \pi^{*n}\{P, P\}_{F,\mathfrak{p}}\, u \\ &\quad = \pi^m \sum_{v/\mathfrak{p}} [\{P, P\}^{(u)}_{n,v} - \pi^{-n}(\eta_{\mathcal{N}_n, v}(P-u) - \lambda_{\mathcal{N}_n, v}(P-u) \log_{\mathfrak{p}} \Psi_{E/\mathcal{N}_n}(v))]\, u \\ &\qquad + \pi^{m-n}\, h_{\mathcal{N}_n}(P-u)\, u.\end{aligned}$$

D'où une égalité du type

$$\{P, P\}_{F,\mathfrak{p}} - t_{\mathfrak{p}}(F)^{-1} h_F(P) \equiv D_n(P) \bmod \pi^{n-m} \mathcal{O}_{\mathfrak{p}}$$

où $D_n(P)$ est une fonction quadratique sur $E_1(F)$ à valeurs dans $\mathcal{O}_{\mathfrak{p}}/\pi^{n-m}\mathcal{O}_{\mathfrak{p}}$ vérifiant

$$D_n(\alpha P) = \deg \alpha D_n(P)$$

pour $\alpha \in \mathcal{O}$ et continue pour la topologie induite par l'inclusion

$$E_1(F) \to \prod_{v/\mathfrak{p}} E_{1,v}(F_v).$$

Par un lemme tout à fait analogue au lemme 1.3, D_n est donc identiquement nulle.

Cela termine la démonstration du théorème 4.1. Ensuite, la proposition 2.4, la formule (6) et le théorème 4.1 permettent de finir la démonstration du second théorème annoncé dans l'introduction.

5. Exemples numériques

Nous allons d'abord donner quelques exemples de calculs de hauteurs. Toutes les courbes elliptiques considérées ont une équation de la forme $y^2 = x^3 - dx$ avec $d \in \mathbb{Z}$, ont bonne réduction en 5 et sont telles que le groupe des points rationnels sur $\mathbb{Q}$ est de rang 1. Elles sont donc définies sur $\mathbb{Q}$, à multiplication complexe par l'anneau des entiers de $\mathbb{Q}(i)$ (avec $i^2 = -1$). On prend comme nombre premier $p = 5$, $\mathfrak{p} = (-1+2i)$. Soit $|\ |_5$ la valeur absolue 5-adique sur $\mathbb{Q}_5$ normalisée par $|5|_5^{-1} = 5$ et posons:

$$c = \left| \left(1 - \frac{\Psi_{E/K}(\mathfrak{p})}{5}\right) h_K(P)/5 \right|_5^{-1}$$

où P est un point de $E(K)$ engendrant un sous-groupe d'indice premier à 5. Comme $E(K)$ n'a pas de 5-torsion, $c\#(Ш(K)(\mathfrak{p}))$ est la valeur du coefficient non nul de $f(E/K, T)/T$. Notons $\tilde{E}_5$ la courbe réduite en 5. On a alors:

$$c = |\#(\tilde{E}_5(\mathbb{F}_5))\, h_K(P)/5|_5^{-1}$$

Le nombre $\#(\tilde{E}_5(\mathbb{F}_5))$ est premier à 5 si et seulement si d n'est pas congru à 2 modulo 5. Par exemple:

$$y^2 = x^3 - 14x, \quad P = (8, 20), \quad c = 1;$$
$$y^2 = x^3 - 124x, \quad P = (18, 60), \quad c = 5.$$

Donnons deux exemples où $\#(\tilde{E}_5(\mathbb{F}_5))$ est divisible par 5 (en fait égal à 10):

$$y^2 = x^3 - 2x, \quad P = (-1, 1), \quad c = 1;$$

dans ce cas, $|h_K(P)/5|_5^{-1}$ est égal à $\frac{1}{5}$. La forme bilinéaire $t_{\mathfrak{p}}(K)^{-1}\langle\ ,\ \rangle_{K,\mathfrak{p}}$ n'est donc pas à valeurs entières et l'indice de $E_1(K)$ dans $E(K)$ est exactement

divisible par 5.

$$y^2=x^3-2662x, \qquad P=(-50, 90), \qquad c=5;$$

ici, on vérifie facilement que P n'est pas divisible par $-1+2i$ mais que $2P$ appartient à $E_1(K)$. On voit donc que l'indice de $E_1(K)$ dans $E(K)$ est premier à 5. Quant à $\frac{1}{5}\langle P, P\rangle_{K,\mathfrak{p}}$, il est égal à une unité.

Montrons sur un exemple comment il est possible de calculer une hauteur p-adique. On considère le cas de la courbe $y^2=x^3-2x$, du point $P=(-1, 1)$. Posons $Q=5P$. Alors $x(Q)=-\dfrac{1803649}{5^4\times 61^2}$. On écrit $x(Q)=\dfrac{a}{e^2}$, $y(Q)=\dfrac{b}{e^3}$ avec $e=25\times 61$. La courbe a bonne réduction partout sauf en 2. On a alors

$$\lambda_v(Q)=\begin{cases}1 & \text{si } v/61\\ 2 & \text{si } v/5\\ \dfrac{1}{12}v(\Delta) & \text{si } v/2\\ 0 & \text{sinon.}\end{cases}$$

On a d'autre part

$$\eta_{\mathfrak{p}}(Q)=\frac{1}{12}\log_{\mathfrak{p}}\frac{\Theta_{\mathfrak{p}}(\mathscr{L}_{\mathfrak{p}}(t(Q)))}{\Delta\, t(Q)^{12}}+\frac{1}{12}\log_{\mathfrak{p}}\Delta+\log_{\mathfrak{p}} t(Q).$$

Une étude précise de la série définissant le premier terme montre qu'il est congru à 0 mod 5^3 pour $t(Q)=\dfrac{a}{b}e$. On a donc

$$h_K(Q)\equiv\log_{\mathfrak{p}} e\,t(Q)^{-1}\equiv\log_{\mathfrak{p}} b/a \bmod 5^3$$

Mais a et b vérifient: $b^2\equiv a^3 \bmod 5^3$.

On a donc

$$h_K(Q)\equiv\tfrac{1}{2}\log_{\mathfrak{p}} a \bmod 5^3.$$

En remarquant que a^2 est congru à 1 module 25 et non modulo 125, on en déduit que:

$$h_K(Q)\sim 5^2$$
$$h_K(P)\sim 1.$$

Soit G_1 la série d'Iwasawa associé à la fonction L p-adique ([3]). Dans tous les cas cités (et dans d'autres) des calculs faits par D. Bernardi et N. Stephens montrent que la valeur de $G_1(u(1+T)-1)/T$ en $T=0$ est à une unité près égale à c. La composante p-primaire de $Ш(K)$ devrait donc être nulle. Nous allons citer deux exemples où il est possible de le montrer.

Soit la courbe d'équation $y^2=x^3-12x$. Le corps $K(E_{\mathfrak{p}})$ est égal à $K(\sqrt[4]{27(-1+2i)})$. On vérifie facilement que 2 divise son nombre de classes mais que par les minorations d'Odlysko ([5]), 10 ne le divise pas. On en déduit que le nombre de classes de $K(E_{\mathfrak{p}})$ est premier à 5. Par un théorème important de Coates et Wiles ([3]), on en déduit que $f(E/K, T)$ divise $G_1(u(1+T)-1)$.

Mais, le calcul montre que la valeur de $G_1(u(1+T)-1)/T$ en $T=0$ est 1 (à une unité près). On en déduit que la conjecture principale est vraie, c'est-à-dire que $G_1(u(1+T)-1)$ et $f(E/K, T)$ sont égaux à une unité près (et égaux à T), que le rang de $E(N_\infty)$ modulo torsion est égal à 1, que $Ш(N_\infty)(5)$ est égal à 1, de même que $Ш(K)(5)$.

Pour la courbe d'équation $y^2=x^3-36x$, on peut de la même manière montrer que $f(E/K, T)$ divise $G_1(u(1+T)-1)$. Mais la valeur de $G_1(u(1+T)-1)/T$ en $T=0$ est égale à 5 à une unité près. Donc $G_1(u(1+T)-1)$ est égale au produit de T par une série irréductible $g(T)$ première à T. On en déduit que T^2 ne divise pas $f(E/K, T)$, donc que $Ш(K)(\mathfrak{p})$ est fini. Un calcul de hauteur $\mathfrak{p}$-adique montre alors que $f(E/K, T)/T$ est égale en $T=0$ à $5\#(Ш(K)(\mathfrak{p}))$. On en déduit de nouveau la conjecture principale et le fait que $Ш(K)(5)$ est égal à 1.

Bibliographie

1. Bernardi, D.: Hauteurs p-adiques sur les courbes elliptiques. Séminaire de théorie des nombres. Progress in Mathematics, vol. 12, pp. 1-14. Paris: Birkhäuser 1979-80
2. Coates, J.: Elliptic curves with complex multiplication. Hermann Weyl Lectures 1979, Annals of Math. Studies, à paraître
3. Coates, J., Wiles, A.: On p-adic L-functions and elliptic Units. J. Austral. Math. Soc. (séries A) **26**, 1-25 (1978)
4. Coates, J., Goldstein, C.: Sur la conjecture principale pour les courbes elliptiques à multiplication complexe
5. Diaz y Diaz, F.: Tables minorant la racine n-ième du discriminant d'un corps de degré n. Publ. Math. Orsay 80-06 (1980)
6. Greenberg, R.: On the Structure of Certain Galois Groups. Invent. Math. **47**, 85-99 (1978)
7. Gross, B.H.: On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex Multiplication, à paraître
8. Neron, A.: Hauteurs et fonctions thêta. Rend. Sci. Math. Milano **46**, 111-135 (1976)
9. Oesterle, J.: Construction de hauteurs archimédiennes et p-adiques suivant la méthode de Bloch, Séminaire de théorie des nombres, Paris 1980-81, Progress in Mathematics, Birkhäuser
10. Perrin-Riou, B.: Groupe de Selmer d'une courbe elliptique à multiplication complexe, Compositio Mathematica. **43**, 387-417 (1981)
11. Schneider, P.: Iwasawa L-functions of varieties over algebraic number fields. A first approach. Invent. Math. (à paraître)
12. Weil, A.: L'arithmétique sur les courbes algébriques. Acta Math. **52**, 281-315 (1928)

Oblatum 4-III-1982