COMPOSITIO MATHEMATICA

BERNADETTE PERRIN-RIOU

Groupe de Selmer d'une courbe elliptique à multiplication complexe

Compositio Mathematica, tome 43, n° 3 (1981), p. 387-417

<http://www.numdam.org/item?id=CM_1981__43_3_387_0>

COMPOSITIO MATHEMATICA, Vol. 43, Fasc. 3, 1981, pag. 387–417

GROUPE DE SELMER D'UNE COURBE ELLIPTIQUE À MULTIPLICATION COMPLEXE

Bernadette Perrin-Riou

Soient K un corps quadratique imaginaire, F une extension finie de K et E une courbe elliptique définie sur F, à multiplication complexe par l'anneau des entiers $\mathcal{O}$ de K. Dans cet article, l'arithmétique des courbes elliptiques est étudiée avec le point de vue suivant. La conjecture de Birch et Swinnerton–Dyer relie les invariants arithmétiques fondamentaux de la courbe elliptique E sur F (en particulier le groupe de Mordell–Weil et le groupe de Tate-Shafarevitch) et le comportement de la fonction L de Hasse–Weil de E sur F au point $s = 1$. Une des raisons principales de la difficulté de cette conjecture est le manque de liens directs entre des deux aspects de la courbe elliptique. Cependant, en combinant la théorie classique de la descente de Mordell et de Weil avec certaines idées provenant de la théorie d'Iwasawa sur les $\mathbf{Z}_p$-extensions de corps de nombres, on est naturellement conduit à relier le groupe de Mordell–Weil et le groupe de Tate–Shafarevitch au comportement de certaines fonctions p-adiques holomorphes au voisinage de $s = 0$. Dans le langage de la théorie d'Iwasawa, ces fonctions p-adiques sont les séries caractéristiques de certains modules de descente attachés à la courbe elliptique E sur F. Cette idée est due à Mazur ([12]) et a été étudiée ultérieurement par plusieurs autres auteurs ([8], [10]). Le but de ce texte est de poursuivre dans cette direction et en particulier de faire le calcul du premier coefficient non nul du développement de ces fonctions p-adiques en 0. La formule obtenue est assez analogue à celle donnée par la conjecture de Birch et Swinnerton–Dyer pour la fonction L de Hasse–Weil de E sur F. Cependant, nous n'avons que des résultats très incomplets sur le lien entre un certain indice dans notre formule et la hauteur p-adique canonique sur la courbe. Nous ne

0010–437X/81/060387–31$00.20/0

faisons ici aucun essai de conjecture précise entre les fonctions p-adiques et les propriétés d'interpolation des fonctions L complexes. Cependant, la valeur de ce travail dépend de la solution de ce problème profond et difficile.

Nous allons maintenant donner un énoncé plus précis des résultats. On suppose désormais que p est un nombre premier vérifiant les

HYPOTHÈSES:

(i) $p \neq 2, 3$;

(ii) *E a bonne réduction en toute place de F au dessus de p*;

(iii) *p se décompose dans K en deux idéaux premiers distincts $\mathfrak{P}$ et $\mathfrak{P}^*$.*

Soit K_∞ l'unique extension galoisienne de K, non ramifiée au dehors de p et dont le groupe de Galois est topologiquement isomorphe à $\mathbf{Z}_p \times \mathbf{Z}_p$. Appelons F_∞ le composé de F et de K_∞ et Γ le groupe de Galois de F_∞ sur F. L'arithmétique de E sur F_∞ a de bonnes propriétés (par exemple, le groupe de Mordell–Weil $E(F_\infty)$ des points de E rationnels sur F_∞, modulo son groupe de torsion, est un groupe abélien libre, cf théorème 2.11). L'extension F_∞ peut s'interpréter à l'aide des points de p^n-torsion ($n \geq 1$) de la courbe elliptique. En effet, la théorie classique de la multiplication complexe permet de montrer que F_∞ est l'unique $\mathbf{Z}_p^2$-extension contenue dans $F(E_{p^\infty})$. D'autre part, grâce à l'hypothèse (iii), deux $\mathbf{Z}_p$-extensions de F contenues dans F_∞ jouent un rôle particulier fondamental: l'unique $\mathbf{Z}_p$-extension de F contenue dans F_∞ non ramifiée au dehors de $\mathfrak{P}$ que l'on notera N_∞ et l'unique $\mathbf{Z}_p$-extension de F contenue dans F_∞ non ramifiée au dehors de $\mathfrak{P}^*$ que l'on notera N_∞^*. Elles ont des interprétations analogues à l'aide des points de $\mathfrak{P}^n$-torsion et de $\mathfrak{P}^{*n}$-torsion ($n \geq 1$). On posera $\mathcal{F}_\infty = F_\infty(E_\mathfrak{P})$, $\mathcal{N}_\infty = N_\infty(E_\mathfrak{P})$.

Le groupe de Selmer $S(F_\infty)$ de E/F_∞ relatif à la descente pour $\mathfrak{P}^\infty$ peut être vu comme un module sur l'algèbre d'Iwasawa à deux variables $\Lambda = \mathbf{Z}_p[[\Gamma]]$. Son dual de Pontryagin $\widehat{S(F_\infty)}$ est un Λ-module compact de type fini. On conjecture que c'est un Λ-module de Λ-torsion, dont tout sous-Λ-module pseudo-nul est réduit à 0. Nous démontrons ici que cela est vrai si l'on suppose pour le corps $F(E_\mathfrak{P})$ des points de $\mathfrak{P}$-torsion une hypothèse $\mathfrak{P}$-adique de Leopoldt que l'on note Leop$(F(E_\mathfrak{P}), \mathfrak{P})$. Précisément, 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, congrues à 1 modulo v. Si $\mathfrak{Q}$ est une place de K et $\mathcal{E}_{L,\mathfrak{Q}}$ le groupe des unités globales de L, congrues à 1 modulo v pour toute place v de L au

dessus de $\mathfrak{Q}$, soit $i_{L,\mathfrak{Q}}$ l'injection diagonale

$$\mathscr{E}_{L,\mathfrak{Q}} \to \prod_{v/\mathfrak{Q}} U_{L,v}.$$

On notera Leop(L, $\mathfrak{Q}$) l'hypothèse suivante: *le* $\mathbf{Z}_p$*-rang de la clôture de* $i_{L,\mathfrak{Q}}(\mathscr{E}_{L,\mathfrak{Q}})$ *pour la topologie* $\mathfrak{Q}$*-adique est égal au* $\mathbf{Z}$*-rang de* $\mathscr{E}_{L,\mathfrak{Q}}$. Elle a été vérifiée par les méthodes de Baker dès que L est une extension abélienne de K.

Il ne semble pas qu'il y ait d'analogue p-adique de la conjecture de Birch et Swinnerton–Dyer pour la série caractéristique à deux variables du dual de Pontryagin du groupe de Selmer de E sur F_∞. Cependant, on utilise le fait que Γ est riche en quotients isomorphes à $\mathbf{Z}_p$ et on étudie l'arithmétique de E sur L_∞ où L_∞ désigne une $\mathbf{Z}_p$-extension arbitraire de F contenue dans F_∞. Nous calculons alors la multiplicité du zéro de la série caractéristique du dual de Pontryagin de $S(L_\infty)$ et la valeur p-adique du premier coefficient non nul de son développement, sous certaines hypothèses de finitude (théorème 3.2). Cependant comme cela a déjà été dit, il manque l'interprétation de certains indices grâce à une hauteur p-adique que nous décrivons ensuite.

Dans le paragraphe 1, on étudie la théorie de Galois du groupe de Selmer $S(F_\infty)$ et son lien avec un groupe de Galois. Dans le paragraphe 2, on démontre que, sous l'hypothèse Leop($F(E_\mathfrak{P})$, $\mathfrak{P}$), son dual de Pontryagin est un Λ-module de torsion et n'a pas de Λ-module pseudo-nul non nul, et on en déduit des conséquences sur les groupes de Selmer $S(L_\infty)$ et sur les groupes de Mordell–Weil $E(L_\infty)$. Le paragraphe 3 est consacré à l'étude des séries caractéristiques et le paragraphe 4 à la construction d'une forme quadratique p-adique analogue à celle construite dans [1], mais qui semble plus adaptée à notre situation.

Je tiens à remercier John Coates de l'aide qu'il m'a apportée au cours de nombreuses conversations.

1. Groupe de Selmer et descente

1.1. *Notations*

Si L est un corps, on note G_L le groupe de Galois sur L d'une clôture algébrique de L. 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 séparable 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.

Si A est un $\mathcal{O}$-module et α un élement de $\mathcal{O}$, on notera A_α le noyau de l'endomorphisme α dans A et $A(\alpha)$ la réunion des A_{α^n} pour $n \geq 1$. Pour chaque idéal entier $\mathfrak{h}$ de $\mathcal{O}$, on définit $E_\mathfrak{h}$ comme la réunion des E_α pour $\alpha \in \mathfrak{h}$. D'autre part, on choisit un élément π de $\mathcal{O}$ ayant une factorisation de la forme

$$(\pi) = \mathfrak{P}^k (\text{pour } k \geq 1).$$

Soit π^* son conjugué. On notera $A(\mathfrak{P}) = A(\pi)$, $A(\mathfrak{P}^*) = A(\pi^*)$. On pose aussi $E_{\mathfrak{P}^\infty} = E(\bar{F})(\mathfrak{P})$, $E_{\mathfrak{P}^{*\infty}} = E(\bar{F})(\mathfrak{P}^*)$ où $\bar{F}$ est une clôture algébrique de F.

1.2. *Descente*

Soit L une extension de F qui n'est pas forcément finie et $I(L)$ l'ensemble des places non archimédiennes de L. Pour tout $n \geq 1$, on a la suite exacte de G_L-modules

$$0 \longrightarrow E_{\pi^n} \longrightarrow E(\bar{F}) \xrightarrow{\pi^n} E(\bar{F}) \longrightarrow 0,$$

d'où la suite exacte de cohomologie

$$0 \to E(L)/\pi^n E(L) \to H^1(L, E_{\pi^n}) \to H^1(L, E)_{\pi^n} \to 0.$$

Le groupe de Tate–Shafarevitch $Ш(L)$ de E sur L est défini par l'exactitude de la suite

$$0 \to Ш(L) \to H^1(L, E) \to \prod_{v \in I(L)} H^1(L_v, E).$$

On définit alors le groupe de Selmer $S(L)^{(\pi^n)}$ relatif à E/L et à π^n comme l'image réciproque dans $H^1(L, E_{\pi^n})$ de $Ш(L)_{\pi^n}$ par l'application $H^1(L, E_{\pi^n}) \to H^1(L, E)_{\pi^n}$. On a donc la suite exacte

$$0 \to E(L)/\pi^n E(L) \to S(L)^{(\pi^n)} \to Ш(L)_{\pi^n} \to 0. \tag{1}$$

Ces suites exactes forment un système inductif pour $n \geq 1$. On définit alors le groupe de Selmer relatif à E/L et à $\mathfrak{P}^\infty$ par

$$S(L) = \varinjlim S(L)^{(\pi^n)}.$$

En prenant la limite inductive des suites exactes (1), on déduit la suite exacte

$$0 \to E(L) \otimes K_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}} \to S(L) \to Ш(L)(\mathfrak{P}) \to 0. \tag{2}$$

1.3. *Groupe de Selmer modifié*

Pour des raisons techniques, il est utile d'introduire un autre groupe de Selmer. On définit le groupe de Tate-Shafarevitch modifié $Ш'(L)$ par l'exacitude de la suite

$$0 \to Ш'(L) \to H^1(L, E) \to \prod_{v \nmid \mathfrak{P}} H^1(L_v, E),$$

où le produit est pris sur les places non archimédiennes v de L qui ne sont pas au dessus de $\mathfrak{P}$. On peut alors définir de la même manière que précédemment un sous-groupe $S'(L)$ de $H^1(L, E_{\mathfrak{P}^\infty})$ vérifiant la suite exacte

$$0 \to E(L) \otimes K_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}} \to S'(L) \to Ш'(L)(\mathfrak{P}) \to 0. \tag{3}$$

Pour certaines extensions infinies de F, il n'y a pas de différence entre $S(L)$ et $S'(L)$. Plus précisemment, on a:

LEMME 1.1: *On a* (*i*) $S(F_\infty) = S'(F_\infty)$, $Ш(F_\infty)(\mathfrak{P}) = Ш'(F_\infty)(\mathfrak{P})$; (*ii*) $S(L_\infty) = S'(L_\infty)$, $Ш(L_\infty)(\mathfrak{P}) = Ш'(L_\infty)(\mathfrak{P})$ *si* L_∞ *est différente de* N_∞^*. (cf. [5], lemme 3.1).

DÉMONSTRATION: Il suffit de démontrer que, si L est une $\mathbf{Z}_p$-extension de F contenue dans F_∞ et différente de N_∞ ou si L est égale à F_∞, le groupe $H^1(L_v, E)(\mathfrak{P})$ est nul pour toute place v de L au dessus de $\mathfrak{P}$. Soit L_n le sous-corps de L fixé par $G(L/F)^{p^n}$ et soit $L_{n,v}$ le complété de L_n pour la restriction de v à L_n. Comme, par définition, L_v est égal à $\bigcup_{n \geq 1} L_{n,v}$, on voit facilement que

$$H^1(L_v, E) = \varinjlim H^1(L_{n,v}, E).$$

où la limite inductive est prise relativement aux applications restriction. Par la dualité locale de Tate, le dual de Pontryagin de $H^1(L_{n,v}, E)(\mathfrak{P})$ est égal à

$$\bar{E}(L_{n,v}) = \varprojlim E(L_{n,v})/\pi^{*m} E(L_{n,v}),$$

et le dual de l'application restriction est l'application norme. Il suffit donc de montrer que

$$\lim_{\leftarrow} \bar{E}(L_{n,v}) \tag{4}$$

est nul, où la limite projective est prise relativement aux applications norme. Notons $\tilde{E}_v$ le réduction de E modulo v et $E_{1,v}$ le noyau de l'application réduction. Comme v est une place au dessus de $\mathfrak{P}$, π^* induit un automorphisme de $E_{1,v}(L_{n,v})$. D'où l'isomorphisme $\bar{E}(L_{n,v}) \simeq \tilde{E}_v(k_{n,v})(p)$ où $k_{n,v}$ désigne le corps résiduel de $L_{n,v}$. Vérifions que ce dernier groupe est isomorphe au groupe $E_{\mathfrak{P}^{*\infty}}(L_{n,v})$ des points de $\mathfrak{P}^{*\infty}$-torsion de $E(L_{n,v})$. En effet, comme v est une place au dessus de $\mathfrak{P}$, l'application de réduction induit une injection de $E_{\mathfrak{P}^{*\infty}}(L_{n,v})$ dans $\tilde{E}_v(k_{n,v})(p)$. Or, le grossencharakter Ψ_{E/L_n} de E sur L_n vérifie

$$\Psi_{E/L_n}(v)\rho = (v, L_n(E_{\mathfrak{P}^{*m}})/L_n)\rho$$

où $(v, L_n(E_{\mathfrak{P}^{*m}})/L_n)$ est le symbole d'Artin de v, pour tout point de $\mathfrak{P}^{*m}$-division ρ et toute place v première à $\mathfrak{P}^*$. Comme $E_{\mathfrak{P}^{*m}}$ est isomorphe en tant que $\mathcal{O}$-module à $\mathcal{O}/\mathfrak{P}^{*m}$, on en déduit que $E_{\mathfrak{P}^{*m}}$ appartient à $L_{n,v}$ si et seulement si $\Psi_{E/L_n}(v)$ est congru à 1 modulo $\mathfrak{P}^{*m}$, ce qui est encore équivalent à $\bar{\Psi}_{E/L_n}(v) \equiv 1 \bmod \mathfrak{P}^m$. Donc, le cardinal de $E_{\mathfrak{P}^{*\infty}}(L_{n,v})$ est exactement $|1 - \bar{\Psi}_{E/L_n}(v)|_{\mathfrak{P}}^{-1}$. Il en est de même du cardinal de $\tilde{E}_v(k_{n,v})(p)$ grâce à la relation

$$\begin{aligned} \# \tilde{E}_v(k_{n,v}) &= q_{n,v} + 1 - \Psi_{E/L_n}(v) - \bar{\Psi}_{E/L_n}(v) \\ &= (1 - \Psi_{E/L_n}(v))(1 - \bar{\Psi}_{E/L_n}(v)) \end{aligned}$$

où $q_{n,v}$ désigne le cardinal de $k_{n,v}$. On a donc les isomorphismes

$$\bar{E}(L_{n,v}) \simeq \tilde{E}_v(k_{n,v})(p) \simeq E_{\mathfrak{P}^{*\infty}}(L_{n,v}) \tag{5}$$

pour une place v au dessus de $\mathfrak{P}$. Supposons maintenant que $L(E_{\mathfrak{P}^*})$ ne contienne pas $E_{\mathfrak{P}^{*\infty}}$, ce qui est vérifié dans le cas (ii). Alors $\bar{E}(L_{n,v})$ est un groupe fini sur lequel le groupe de Galois de L_v sur $L_{n,v}$ agit trivialement pour n assez grand. Donc la limite projective (4) est nulle. Dans le cas où L est égale à F_∞, $\bar{E}(L_{n-1,v})$ est d'indice au plus p dans $\bar{E}(L_{n,v})$ et la norme de l'extension L_n/L_{n-1} agit par multiplication par p^2 sur $\bar{E}(L_{n,v})$ pour n assez grand. On en déduit facilement que (4) est encore nulle. Ce qui démontre le lemme.

Il reste le cas où L_∞ est égal à N_∞^*. Les groupes de cohomologie $H^1(N_{\infty,v}^*, E)(\mathfrak{P})$ ne sont alors pas toujours nuls. Nous allons les

calculer; cependant, je ne sais calculer le quotient $Ш'(N_\infty^*)(\mathfrak{P})/Ш(N_\infty^*)(\mathfrak{P})$ que sous des hypothèses supplémentaires de finitude sur certains groupes de Tate–Shafarevitch.

Introduisons quelques nouvelles notations. Si G est le groupe de Galois sur F d'une extension abélienne L de F et si v est une place de F, soit G_v le sous-groupe de décomposition de G relatif à un prolongement choisi de v à L, que l'on note encore v. Soit M un $\mathbf{Z}_p[[G_v]]$-module. On pose

$$\mathrm{Ind}_v^G(M) = M \underset{\mathbf{Z}_p[[G_v]]}{\otimes} \mathbf{Z}_p[[G]]$$

muni de sa structure naturelle de $\mathbf{Z}_p[[G]]$-module. D'autre part, on note $T_{\mathfrak{Q}}(F)$ (resp. $T_{\mathfrak{Q}}(F_v)$) le module de Tate associé à $E_{\mathfrak{Q}^\infty}(F_\infty)$ (resp. $E_{\mathfrak{Q}^\infty}(F_{\infty,v})$) et $T_{\mathfrak{Q}}$ le module de Tate associé à $E_{\mathfrak{Q}^\infty}$ (pour $\mathfrak{Q} = \mathfrak{P}$ ou $\mathfrak{P}^*$, les applications de transition étant les multiplications par π^n ou π^{*n}). Par exemple, $T_{\mathfrak{P}^*}(F_v)$ est aussi égal à $\varprojlim E_{\mathfrak{P}^{*\infty}}(N_{n,v}^*)$ où la limite projective peut être prise relativement aux applications norme et où N_n^* est le sous-corps de N_∞^* fixé par $G(N_\infty^*/F)^{p^n}$. C'est un $\mathbf{Z}_p[[G(N_\infty^*/F)]]$-module. Il est en particulier nul si F_v ne contient pas de point de $\mathfrak{P}^*$-torsion.

LEMME 1.2: (i) *Il existe un $G(N_\infty^*/F)$-module U_∞ dont le dual de Pontryagin est isomorphe à $\prod_{v|\mathfrak{P}} \mathrm{ind}_v^{G(N_\infty^*/F)} T_{\mathfrak{P}^*}(F_v)$ où le produit est pris sur les places de F au dessus de $\mathfrak{P}$ et qui vérifie la suite exacte de $G(N_\infty^*/F)$-modules*

$$0 \to S(N_\infty^*) \to S'(N_\infty^*) \to U_\infty; \tag{6}$$

(ii) *Si l'on suppose de plus que $Ш(N_n^*)(\mathfrak{P}^*)$ est fini pour tout $n \geq 1$ et que $E(N_\infty^*)$ modulo torsion est de type fini, le dual de Pontryagin du conoyau de $S'(N_\infty^*) \to U_\infty$ est isomorphe à $T_{\mathfrak{P}^*}(F)$.*

REMARQUE: L'hypothèse que $E(N_\infty^*)$ modulo torsion est de type fini est vérifiée dès que l'hypothèse Leop($F(E_{\mathfrak{P}^*})$, $\mathfrak{P}^*$) est vérifiée ([5], theorem 3.8).

DÉMONSTRATION: Prenons pour U_∞ le $G(N_\infty^*/F)$-module

$$\prod_{v/\mathfrak{P}} H^1(N_{\infty,v}^*, E)(\mathfrak{P})$$

où le produit est pris sur les places v de N_∞^* divisant $\mathfrak{P}$. Il vérifie la

suite exacte (6) et le dual de Pontryagin $\hat{U}_\infty$ de U_∞ est isomorphe à $\prod_{v|\mathfrak{P}} \mathrm{Ind}_v^{G(N_\infty^*/F)} M_v$ où le produit est ici pris sur les places v de F divisant $\mathfrak{P}$ et où M est le dual de Pontryagin de $H^1(N_{\infty,v}^*, E)(\mathfrak{P})$ (on a alors choisi un prolongement de v à N_∞^*). Le calcul fait dans la démonstration du lemme 1.1 montre que M_v est égal à la limite projective relativement aux applications norme de $\tilde{E}_v(k_{n,v})(p)$, donc de $E_{\mathfrak{P}^{*\infty}}(N_{n,v}^*)$. Donc, M_v est égal à $T_{\mathfrak{P}^*}(F_v)$, ce qui donne le résultat (i). Grâce à un théorème de Cassels ([3]), si $Ш(N_n^*)(\mathfrak{P}^*)$ est fini, on peut identifier le dual du conoyau de l'homomorphisme

$$Ш'(N_n^*)(\mathfrak{P}) \to \prod_{v/\mathfrak{P}} H^1(N_{n,v}^*, E)(\mathfrak{P})$$

avec l'image de $E(N_n^*) \otimes \mathcal{O}_{\mathfrak{P}^*} = \varprojlim E(N_n^*)/\pi^{*m} E(N_n^*)$ dans $\prod_{v|\mathfrak{P}} \tilde{E}_v(k_{n,v})(p)$ (pour les détails, voir [5], theorem 3.12). Comme on a supposé que $E(N_\infty^*)$ modulo torsion est un groupe abélien de type fini, les groupes $E(N_n^*)$ modulo torsion se stabilisent et l'image de $\varprojlim E(N_n^*) \otimes \mathcal{O}_{\mathfrak{P}^*}$ (où la limite est prise relativement aux applications norme) dans $\varprojlim \prod_{v|\mathfrak{P}} \tilde{E}_v(k_{n,v})(p)$ (c'est-à-dire dans le dual de U_∞) est égale à $\varprojlim E_{\mathfrak{P}^{*\infty}}(N_n^*)$, c'est-á-dire à $T_{\mathfrak{P}^*}(F)$, d'où le lemme.

1.4. *Théorie de Galois pour les groupes de Selmer modifiés*

On étudie maintenant le lien existant entre le groupe de Selmer de F et celui d'une $\mathbf{Z}_p$-extension L_∞ de F, contenue dans F_∞. Nous ne regarderons pour le moment que le cas où L_∞ est différente de N_∞ (voir 2.3 si $L_\infty = N_\infty$).

PROPOSITION 1.3: *Si L_∞ est différente de N_∞, l'application de restriction donne un isomorphisme*

$$S'(L_\infty) \xrightarrow{\sim} S(F_\infty)^{G(F_\infty/L_\infty)}.$$

DÉMONSTRATION: Remarquons que $S'(L_\infty)$ est le noyau de l'homomorphisme

$$H^1(L_\infty, E_{\mathfrak{P}^\infty}) \longrightarrow \prod_{v \nmid \mathfrak{P}} H^1(L_{\infty,v}, E)$$

et que $S(F_\infty)$ est le noyau de l'homomorphisme

$$H^1(F_\infty, E_{\mathfrak{P}^\infty}) \longrightarrow \prod_{v \nmid \mathfrak{P}} H^1(F_{\infty,v}, E).$$

Il est alors facile de voir que la proposition résulte des deux lemmes suivants.

LEMME 1.4: *Si L_∞ ne contient pas $E_{\mathfrak{P}^\infty}$, on a l'isomorphisme*

$$H^1(L_\infty, E_{\mathfrak{P}^\infty}) \xrightarrow{\sim} H^1(F_\infty, E_{\mathfrak{P}^\infty})^{G(F_\infty/L_\infty)}.$$

DÉMONSTRATION DU LEMME 1.4: On a la suite exacte de cohomologie

$$O \to H^1(F_\infty/L_\infty, E_{\mathfrak{P}^\infty}(F_\infty)) \to H^1(L_\infty, E_{\mathfrak{P}^\infty}) \to \mathrm{H}^1(F_\infty, E_{\mathfrak{P}^\infty})^{G(F_\infty/L_\infty)} \to$$
$$\cdots \to H^2(F_\infty/L_\infty, E_{\mathfrak{P}^\infty}(F_\infty)).$$

Il suffit donc de montrer que $H^i(F_\infty/L_\infty, E_{\mathfrak{P}^\infty}(F_\infty))$ est nul pour $i = 1, 2$. Or, $E_{\mathfrak{P}^\infty}(F_\infty)$ est soit nul, et le lemme est trivial, soit égal à $E_{\mathfrak{P}^\infty}$. Dans ce dernier cas, $G(F_\infty/L_\infty)$ agit non trivialement sur $T_\mathfrak{P}$, car L_∞ ne contient pas $E_{\mathfrak{P}^\infty}$. Soit $V_\mathfrak{P}$ le $K_\mathfrak{P}$-espace vectoriel $T_\mathfrak{P} \underset{\mathcal{O}_\mathfrak{P}}{\otimes} K_\mathfrak{P}$ de dimension 1. On a la suite exacte

$$0 \to T_\mathfrak{P} \to V_\mathfrak{P} \to E_{\mathfrak{P}^\infty} \to 0.$$

Si γ est un générateur topologique de $G(F_\infty/L_\infty)$ qui est isomorphe à $\mathbf{Z}_p$, $\gamma - 1$ est un endomorphisme non nul de $V_\mathfrak{P}$, donc surjectif; il est donc surjectif sur $E_{\mathfrak{P}^\infty}$, ce qui implique que $H^1(F_\infty/L_\infty, E_{\mathfrak{P}^\infty})$ est nul. Quant à $H^2(F_\infty/L_\infty, E_{\mathfrak{P}^\infty})$, il est nul car $G(F_\infty/L_\infty)$ est de dimension cohomologique égale à 1.

Enonçons maintenant le second lemme.

LEMME 1.5: *Si L_∞ est différente de N_∞ et si v est une place de F_∞ qui ne divise pas $\mathfrak{P}$, l'application de restriction*

$$H^1(L_{\infty,v}, E)(\mathfrak{P}) \to H^1(F_{\infty,v}, E)(\mathfrak{P})$$

est injective.

DÉMONSTRATION DU LEMME 1.5: Le noyau de l'application de restriction est $H^1(F_{\infty,v}/L_{\infty,v}, E(F_{\infty,v}))$. L'extension $F_{\infty,v}/L_{\infty,v}$ étant non ramifiée et la courbe E ayant bonne réduction en v, ce dernier groupe est nul ([11] pour le cas des extensions finies contenues dans $L_{\infty,v}$, puis passage à la limite inductive).

1.5. *Groupe de Selmer et groupe de Galois*

Pour toute extension L de K, notons M_L la p-extension abélienne non ramifiée au dehors de $\mathfrak{P}$ de L et X_L le groupe de Galois de M_L sur L. Le groupe de Galois $G_\infty = G(\mathcal{F}_\infty/F)$ opère sur $X_{\mathcal{F}_\infty}$ par automorphismes intérieurs (on rappelle que $\mathcal{F}_\infty = F_\infty(E_\mathfrak{P})$). En particulier, si $\Delta = G(\mathcal{F}_\infty/F_\infty)$, $X_{\mathcal{F}_\infty}$ est un $\mathbf{Z}_p[[\Delta]]$-module. Or, Δ est un groupe fini cyclique d'ordre premier à p. Soit κ le caractère de G_∞ donnant l'action de G_∞ sur $E_{\mathfrak{P}^\infty}$ et χ la restriction de κ à Δ. Alors, tout $\mathbf{Z}_p[[\Delta]]$-module se décompose en somme directe de sous-espaces propres correspondant aux caractères χ^i. On notera en particulier $X^{(1)}_{\mathcal{F}_\infty}$ le sous-espace propre de $X_{\mathcal{F}_\infty}$ sur lequel Δ agit comme χ. D'autre part, $X_{\mathcal{F}_\infty}$ et $X^{(1)}_{\mathcal{F}_\infty}$ sont des Γ-modules (on identifiera lorsque cela sera utile Γ avec $G(\mathcal{F}_\infty/F(E_\mathfrak{P}))$).

De plus, si A et B sont des Γ-modules, on munit comme d'habitude $\mathrm{Hom}(A, B)$ de la structure de Γ-modules donnée par $(\gamma f)(a) = \gamma f(\gamma^{-1}a)$ pour $\gamma \in \Gamma$ et $a \in A$.

THÉORÈME 1.6:

(i) *$S(N_\infty)$ est $G(N_\infty/F)$-isomorphe à* $\mathrm{Hom}(X^{(1)}_{\mathcal{N}_\infty}, E_{\mathfrak{P}^\infty})$ *où* $\mathcal{N}_\infty = N_\infty(E_\mathfrak{P})$;

(ii) *$S(F_\infty)$ est Γ-isomorphe à* $\mathrm{Hom}(X^{(1)}_{\mathcal{F}_\infty}, E_{\mathfrak{P}^\infty})$.

La démonstration de (i) est faite dans [5] et celle de (ii) est tout à fait analogue, compte tenu de l'égalité $S'(F_\infty) = S(F_\infty)$.

On pose $T_\mathfrak{P}^{(-1)} = \mathrm{Hom}(T_\mathfrak{P}, \mathbf{Z}_p)$ et $X_{\mathcal{F}_\infty}(-1) = X_{\mathcal{F}_\infty} \underset{\mathbf{Z}_p}{\otimes} T_\mathfrak{P}^{(-1)}$. Alors, on a

$$\mathrm{Hom}(X^{(1)}_{\mathcal{F}_\infty}, E_{\mathfrak{P}_\infty}) = \mathrm{Hom}(X^{(1)}_{\mathcal{F}_\infty}(-1), K_\mathfrak{P}/\mathcal{O}_\mathfrak{P}).$$

Le dual de Pontryagin de $S(F_\infty)$, que l'on notera $\widehat{S(F_\infty)}$, est donc extrêmement lié à $X_{\mathcal{F}_\infty}$ et l'étude de ce dernier G_∞-module par la théorie du corps de classes permet d'obtenir des renseignements sur le groupe de Selmer $S(F_\infty)$. C'est ce que nous allons faire dans le paragraphe 2.

2. Le Λ-module $S(F_\infty)$

2.1. *Premières propriétés*

Posons $\Lambda = \mathbf{Z}_p[[\Gamma]]$ et $\Lambda_{L_\infty} = \mathbf{Z}_p[[G(L_\infty/F)]]$ si L_∞ est comme d'habitude une $\mathbf{Z}_p$-extension de F, contenue dans F_∞. D'autre part, si H est un sous-groupe de Γ et M un Γ-module, on notera M_H (resp. M^H) le plus grand quotient (resp. sous-groupe) de M sur lequel H agit

trivialement. L'action de Γ sur le $\mathbf{Z}_p$-module $X_{\mathcal{F}_\infty}$ par automorphismes intérieurs permet de munir $X_{\mathcal{F}_\infty}$ d'une structure de Λ-module compact. Le premier résultat élémentaire est le suivant.

LEMME 2.1: *Le groupe de Galois $X_{\mathcal{F}_\infty}$ est un Λ-module de type fini.*

DÉMONSTRATION: Soit M_0' l'extension abélienne maximale de $\mathcal{F}_0 = F(E_{\mathfrak{P}})$ contenue dans $M_{\mathcal{F}_\infty}$. On a alors la suite exacte de Δ-modules

$$\mathbf{Z}_p \to (X_{\mathcal{F}_\infty})_\Gamma \to G(M_0'/\mathcal{F}_\infty) \to 0. \tag{7}$$

En effet, introduisons une $\mathbf{Z}_p$-extension $\mathcal{L}_\infty$ de $\mathcal{F}_0$ contenue dans $\mathcal{F}_\infty$. On a alors facilement l'isomorphisme

$$(X_{\mathcal{F}_\infty})_{G(\mathcal{F}_\infty/\mathcal{L}_\infty)} \xrightarrow{\sim} G(M'_{\mathcal{L}_\infty}/\mathcal{F}_\infty),$$

si $M'_{\mathcal{L}_\infty}$ est l'extension abélienne maximale de $\mathcal{L}_\infty$ contenue dans $M_{\mathcal{F}_\infty}$, ce qui peut s'écrire par la suite exacte

$$0 \to (X_{\mathcal{F}_\infty})_{G(\mathcal{F}_\infty/\mathcal{L}_\infty)} \to G(M'_{\mathcal{L}_\infty}/\mathcal{L}_\infty) \to G(\mathcal{F}_\infty/\mathcal{L}_\infty) \to 0.$$

On a de même l'isomorphisme

$$G(M'_{\mathcal{L}_\infty}/\mathcal{L}_\infty)_{G(\mathcal{L}_\infty/\mathcal{F}_0)} \simeq G(M_0'/\mathcal{L}_\infty).$$

D'où la suite exacte

$$\mathbf{Z}_p \to (X_{\mathcal{F}_\infty})_\Gamma \to G(M_0'/\mathcal{L}_\infty) \to G(\mathcal{F}_\infty/\mathcal{L}_\infty) \to 0,$$

ce qui est équivalent à (7). Soit maintenant $M_0 = M_{\mathcal{F}_0}$ la p-extension abélienne non ramifiée au dehors de $\mathfrak{P}$ maximale de $\mathcal{F}_0$. Par la théorie du corps de classes, $G(M_0/\mathcal{F}_0)$ est un $\mathbf{Z}_p$-module de type fini. D'autre part, le composé J des sous-groupes d'inertie des places de $\mathcal{F}_0$ au dessus de $\mathfrak{P}^*$ dans l'extension abélienne $M_0'/\mathcal{F}_0$ est un $\mathbf{Z}_p$-module de type fini, puisque l'ensemble des places de $\mathcal{F}_\infty$ au dessus de $\mathfrak{P}^*$ est fini et on a la suite exacte

$$0 \to J \to G(M_0'/\mathcal{F}_0) \to G(M_0/\mathcal{F}_0) \to 0. \tag{8}$$

De (7) et (8), on déduit que $(X_{\mathcal{F}_\infty})_\Gamma$ est un $\mathbf{Z}_p$-module de type fini et donc par un argument classique que $X_{\mathcal{F}_\infty}$ est un Λ-module de type fini.

PROPOSITION 2.2: *Sous l'hypothèse* Leop$(F(E_{\mathfrak{P}}), \mathfrak{P})$, $X^{(1)}_{\mathcal{F}_\infty}$ *est un* Λ*-module de type fini et de* Λ*-torsion.*

Avant de démontrer cette proposition, on énonce le lemme suivant.

LEMME 2.3: *Soit* H *un sous-groupe de* Γ *tel que* $\Gamma/H \simeq \mathbf{Z}_p$ *et soit* M *un* Λ*-module compact de type fini. Si* M_H *est un* $\mathbf{Z}_p[[\Gamma/H]]$*-module de torsion,* M *est un* Λ*-module de* Λ*-torsion.*

(Pour la démonstration, voir [6]).

DÉMONSTRATION DE LA PROPOSITION 2.2: D'après le lemme 2.3, il suffit de montrer que $(X^{(1)}_{\mathcal{F}_\infty})_{G(F_\infty/N_\infty)}$ est un Λ_{N_∞}-module de torsion ($H = G(F_\infty/N_\infty)$). Nous allons faire le lien entre les deux modules $(X^{(1)}_{\mathcal{F}_\infty})_{G(F_\infty/N_\infty)}$ et $X^{(1)}_{\mathcal{N}_\infty}$ et voir qu'ils sont simultanément de Λ_{N_∞}-torsion. Or, sous l'hypothèse Leop$(F(E_{\mathfrak{P}}), \mathfrak{P})$, $X^{(1)}_{\mathcal{N}_\infty}$ est de Λ_{N_∞}-torsion d'après [5], ce qui démontrera la proposition.

Soit $M'_{\mathcal{N}_\infty}$ l'extension abélienne de $\mathcal{N}_\infty$ contenue dans $M_{\mathcal{F}_\infty}$ maximale et soit le composé $\mathcal{S}$ des sous-groupes d'inertie aux places de $\mathcal{N}_\infty$ au dessus de $\mathfrak{P}^*$ dans l'extension abélienne $M'_{\mathcal{N}_\infty}/\mathcal{N}_\infty$. Comme chacun de ces sous-groupes est isomorphe à $\mathbf{Z}_p$ et qu'il n'y a qu'un nombre fini de places au dessus de $\mathfrak{P}$ dans $\mathcal{F}_\infty$, $\mathcal{S}^{(1)}$ est un Λ_{N_∞}-module de Λ_{N_∞}-torsion. Il est d'autre part facile d'établir les deux suites exactes de Δ-modules

$$0 \to \mathcal{S} \to G(M'_{\mathcal{N}_\infty}/\mathcal{N}_\infty) \to X_{\mathcal{N}_\infty} \to 0, \tag{9}$$

$$0 \to (X_{\mathcal{F}_\infty})_{G(\mathcal{F}_\infty/\mathcal{N}_\infty)} \to G(M'_{\mathcal{N}_\infty}/\mathcal{N}_\infty) \to \mathbf{Z}_p \to 0. \tag{10}$$

Donc, si $X^{(1)}_{\mathcal{N}_\infty}$ est un Λ_{N_∞}-module de Λ_{N_∞}-torsion, il en est de même de $(X^{(1)}_{\mathcal{F}_\infty})_{G(\mathcal{F}_\infty/\mathcal{N}_\infty)}$. On peut alors terminer la démonstration comme indiqué ci-dessus.

2.2. *Sur les modules pseudo-nuls de* $\widehat{S(F_\infty)}$.

Abordons maintenant le théorème principal.

THÉORÈME 2.4: *Sous l'hypothèse* Leop$(F(E_{\mathfrak{P}}), \mathfrak{P})$, *le dual de Pontryagin de* $S(F_\infty)$ *est un* Λ*-module de type fini de* Λ*-torsion, dont tout sous-*Λ*-module pseudo-nul est réduit à* 0.

DÉMONSTRATION: D'après le théorème 1.6, on a l'isomorphisme

$$\widehat{S(F_\infty)} \simeq X_{\mathfrak{P}_\infty}^{(1)}(-1).$$

Donc, d'après la proposition 2.2, $\widehat{S(F_\infty)}$ est un Λ-module de type fini et de Λ-torsion. On peut supposer pour simplifier les notations que $E_{\mathfrak{P}}$ est contenu dans F_∞ et il suffit alors de montrer que $X_\infty = X_{F_\infty}$ n'a pas de sous-Λ-module pseudo-nul non nul. Soit Y_∞ le groupe de Galois sur F_∞ de la p-extension abélienne non ramifiée au dehors de p, maximale de F_∞. Le lien entre X_∞ et Y_∞ est donné dans le lemme suivant.

LEMME 2.5: *Il existe un Λ-module Z_∞ vérifiant les propriétés suivantes*

(i) *on a la suite exacte de Λ-modules*

$$Z_\infty \to Y_\infty \to X_\infty \to 0; \tag{11}$$

(ii) *Z_∞ s'injecte dans un Λ-module libre de rang $r_2(F)$ avec un conoyau pseudo-nul isomorphe à*

$$T_\infty = \prod_{v/\mathfrak{P}^*} \mathrm{Ind}_v^{G(F_\infty/F)} T_p(F_v)$$

où le produit porte sur les places de F divisant $\mathfrak{P}^*$, où $T_p(F_v)$ est le module de Tate associé aux racines de l'unité de $F_{\infty,v}$, muni de sa structure naturelle de $\mathbf{Z}_p[[G(F_\infty/F)_v]]$-module et où $r_2(F)$ est le nombre de places imaginaires de F.

On en déduit donc en particulier que Z_∞ n'a pas de Λ-torsion. D'autre part, ce lemme n'utilise pas le fait que F contient $E_{\mathfrak{P}}$.

DÉMONSTRATION DU LEMME 2.5: Soit F_n le corps fixé par Γ^{p^n}. Appelons M_n (resp. N_n) la p-extension abélienne non ramifiée au dehors de $\mathfrak{P}$ (resp. de p) maximale de F_n, $U_{n,v}$ le groupe des unités locales congrues à 1 modulo v du complété de F_n en v. On pose $U_{n,p} = \prod_{v/p} U_{n,v}$, $U_{n,\mathfrak{P}} = \prod_{v/\mathfrak{P}} U_{n,v}$. Soit $\mathscr{E}_{n,p}$ (resp. $\mathscr{E}_{n,\mathfrak{P}}$) le groupe des unités globales de F_n, congrues à 1 modulo toutes les places v divisant p (resp. $\mathfrak{P}$). On a des injections naturelles

$$i_{n,p} : \mathscr{E}_{n,p} \to U_{n,p}$$

$$i_{n,\mathfrak{P}} : \mathscr{E}_{n,\mathfrak{P}} \to U_{n,\mathfrak{P}}.$$

Si A_n est la composante p-primaire du groupe des classes d'idéaux de F_n, par la théorie du corps de classes, on a les suites exactes et le diagramme commutatif exact suivants:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_{n,p}/\overline{i_{n,p}(\mathscr{E}_{n,p})} & \longrightarrow & G(N_n/F_n) & \longrightarrow & A_n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & U_{n,\mathfrak{P}}/\overline{i_{n,\mathfrak{P}}(\mathscr{E}_{n,\mathfrak{P}})} & \longrightarrow & G(M_n/F_n) & \longrightarrow & A_n & \longrightarrow & 0. \\ & & & & \downarrow & & & & \\ & & & & 0 & & & & \end{array}$$

où la première application verticale pr_n est induite par la projection naturelle. Le noyau K_n de $G(N_n/F_n) \to G(M_n/F_n)$ est donc égale au noyau de pr_n. D'autre part, comme $\mathscr{E}_{n,p}$ est sous-$\mathbf{Z}$-module de $\mathscr{E}_{n,\mathfrak{P}}$ d'indice premier à p, l'application

$$\overline{i_{n,p}(\mathscr{E}_{n,p})} \to \overline{i_{n,\mathfrak{P}}(\mathscr{E}_{n,\mathfrak{P}})}$$

est surjective et K_n est un quotient de $U_{n,\mathfrak{P}^*}$ (avec une notation évidente). Soit alors Z_∞ la limite projective des $U_{n,\mathfrak{P}^*}$ pour $n \geq 1$ relativement aux applications norme. Comme Y_∞ (resp. X_∞) est la limite projective des groupes $G(N_n/F_n)$ (resp. $G(M_n/F_n)$), on déduit de ce qui précède la suite exacte

$$Z_\infty \to Y_\infty \to X_\infty \to 0.$$

Il ne reste plus qu'à montrer que Z_∞ vérifie (ii). Or, il est immédiat que l'on a l'isomorphisme de Λ-modules

$$Z_\infty = \prod_{v/\mathfrak{P}^*} \mathrm{Ind}_v^{G(F_\infty/F)} Z_{\infty,v},$$

où le produit est pris sur les places v de F divisant $\mathfrak{P}^*$ et où $Z_{\infty,v}$ est égal à la limite projective des $U_{n,v}$ relativement aux normes des extensions locales $F_{n,v}$ pour un prolongement choisi de v à F_n. Or la structure de $\mathbf{Z}_p[[G(F_\infty/F)_v]]$-module de $Z_{\infty,v}$ est connue. Elle est étudiée par Wintenberger dans [14], ce qui permet de conclure.

Poursuivons la démonstration du théorème 2.4. Greenberg ([16]) a montré que, sous l'hypothèse Leop($F, \mathfrak{P}$), Y_∞ est un Λ-module de rang $r_2(F)$ sans Λ-module pseudo-nul non nul. Comme X_∞ est de Λ-torsion, le noyau de $Z_\infty \to Y_\infty$ est de torsion, donc nul. Soit B le sous-module pseudo-nul maximal de X_∞ et soit C son image réci-

proque dans Y_∞ par l'application $Y_\infty \to X_\infty$. Comme le sous-Λ-module de torsion de C s'injecte dans B et que Y_∞ n'a pas de Λ-module pseudo-nul non nul, C est sans torsion. Par la théorie générale des Λ-modules de type fini, il s'injecte dans un Λ-module réflexif R avec un conoyau D pseudo-nul et D est entièrement déterminé par C. Soit K le conoyau de l'application composée

$$Z_\infty \to C \to R.$$

On a la suite exacte par le lemme du serpent

$$0 \to B \to K \to D \to 0.$$

Comme B et D sont pseudo-nuls, K l'est aussi. Il est donc isomorphe à T_∞. Mais, pour presque tout sous-groupe H de tel que $\Gamma/H \simeq \mathbf{Z}_p$ (c'est-à-dire sauf pour un nombre fini), B, K et D sont des $\mathbf{Z}_p[[H]]$-modules de torsion et d'après la structure de T_∞ donnée dans le lemme 2.5, $(T_\infty)_H$ est fini. On en déduit que B_H est fini. On montre alors facilement que, B étant le sous-module pseudo-nul maximal de X_∞, B_H est un sous-module de $(X_\infty)_H$ pour presque tout H et donc de X_{L_∞} si L_∞ est le sous-corps de F_∞ fixé par H. Par une démonstration analogue à celle de Greenberg dans [6] (voir aussi [5]), on montre que, toujours sous l'hypothèse Leop$(F, \mathfrak{P})$, X_{L_∞} n'a pas de sous-$\mathbf{Z}_p[[\Gamma/H]]$-module fini non nul. Donc B_H est nul et B aussi, ce qui termine la démonstration du théorème 2.4.

2.3. *Conséquences sur le groupe de Selmer d'une* $\mathbf{Z}_p$*-extension*

THÉORÈME 2.6: *Pour toute* $\mathbf{Z}_p$*-extension* L_∞ *de* F *contenue dans* F_∞, *le dual de Pontryagin* $\widehat{S(L_\infty)}$ *de* $S(L_\infty)$ *est un* Λ_{L_∞}*-module de type fini. Sous l'hypothèse* Leop$(F(E_\mathfrak{P}), \mathfrak{P})$, *pour presque toute* $\mathbf{Z}_p$*-extension* L_∞, $\widehat{S(L_\infty)}$ *est de* Λ_{L_∞}*-torsion et* $[(\widehat{S(L_\infty)}_{G(F_\infty/L_\infty)}]^{G(L_\infty/F)}$ *n'a pas de* $\mathbf{Z}_p$*-torsion.*

DÉMONSTRATION: D'après la proposition 1.3, $\widehat{S(L_\infty)}$ est égal à $\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}$ pour L_∞ différent de N_∞ et de N_∞^*. On en déduit qu'il est de type fini et de Λ_{L_∞}-torsion pour presque toute $\mathbf{Z}_p$-extension L_∞, puisque $\widehat{S(F_\infty)}$ est un Λ-module de Λ-torsion. On désire ensuite montrer que $(\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)})^{G(L_\infty/F_\infty)}$ n'a alors pas de $\mathbf{Z}_p$-torsion. Grâce au lemme ci-dessous, il suffit de le démontrer dans le cas particulier $L_\infty = N_\infty$.

LEMME 2.7: *Soit* M *un* Λ*-module de type fini et de torsion, sans*

Λ-module pseudo-nul non nul. Soient H_1 et H_2 deux sous-groupes de Γ tels que $\Gamma/H_1 \simeq \mathbf{Z}_p$, $\Gamma/H_2 \xrightarrow{\sim} \mathbf{Z}_p$ et tels que M_{H_1} (resp. M_{H_2}) soit un $\mathbf{Z}_p[[\Gamma/H_1]]$ (resp. $\mathbf{Z}_p[[\Gamma/H_2]]$)-module de torsion. Alors $(M_{H_1})^{\Gamma/H_1}$ et $(M_{H_2})^{\Gamma/H_2}$ sont isomorphes en tant que $\mathbf{Z}_p$-modules.

On appliquera le lemme avec $M = \widehat{S(F_\infty)}$, $H_1 = G(F_\infty/N_\infty)$, $H_2 = G(F_\infty/L_\infty)$.

DÉMONSTRATION: On suppose d'abord que H_1 et H_2 engendrent topologiquement Γ. Les hypothèses faites impliquent que M^{H_1} et M^{H_2} sont pseudo-nuls donc nuls. On a alors le diagramme commutatif exact

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M & \longrightarrow & M & \longrightarrow & M_{H_1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M & \longrightarrow & M & \longrightarrow & M_{H_1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & M_{H_2} & \longrightarrow & M_{H_2} & \longrightarrow & M_\Gamma & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Par le lemme du serpent, on en déduit que le noyau de $M_{H_1} \to M_{H_1}$ est isomorphe au noyau de $M_{H_2} \to M_{H_2}$, d'où l'isomorphisme $(M_{H_1})^{\Gamma/H_1} \xrightarrow{\sim} (M_{H_2})^{\Gamma/H_2}$. Si H_1 et H_2 n'engendrent pas topologiquement Γ, il suffit d'introduire un troisième sous-groupe.

Montrons maintenant que $\widehat{S(F_\infty)}_{G(F_\infty/N_\infty)}$ n'a pas de sous-Λ_{N_∞}-module fini non nul, ce qui permettra de terminer la démonstration du théorème 2.6. Rappelons les suites exactes (9) et (10)

$$0 \to \widehat{S(F_\infty)}_{G(F_\infty/N_\infty)} \to G(M'_{\mathcal{N}_\infty}/\mathcal{N}_\infty)^{(1)}(-1) \to T_{\mathfrak{P}}(F) \to 0$$
$$0 \to \mathcal{P}^{(1)} \to G(M'_{\mathcal{N}_\infty}/\mathcal{N}_\infty)^{(1)} \to X^{(1)}_{\mathcal{N}_\infty} \to 0.$$

Comme $X_{\mathcal{N}_\infty}$ n'a pas de Λ_{N_∞}-module fini non nul d'après [5], il ne reste plus qu'à montrer qu'il en est de même de $\mathcal{P}^{(1)}$, ce qui se déduit du lemme de structure suivant.

LEMME 2.8: *Le Λ_{N_∞}-module $\mathcal{P}^{(1)}(-1)$ est isomorphe à*

$$\prod_{v/\mathfrak{P}^*} \mathrm{Ind}_v^{G(N_\infty/F)} \mathrm{Hom}_{\mathbf{Z}_p}(T_{\mathfrak{P}}(F_v), \mathbf{Z}_p).$$

DÉMONSTRATION: Si L est une extension de K, soit N_L la p-extension abélienne non ramifiée au dehors de p de L. Posons $Y_L = G(N_L/L)$ et $Z_L = \varprojlim U_{l,\mathfrak{P}^*}$ où l parcourt les sous-extensions finies de L et où la limite projective est prise relativement aux normes. On a l'isomorphisme

$$(Y_{\mathcal{F}_\infty})_{G(\mathcal{F}_\infty/\mathcal{N}_\infty)} \simeq G(N_{\mathcal{N}_\infty}/\mathcal{F}_\infty),$$

et les suites exactes

$$0 \to (Z_{\mathcal{F}_\infty})_{G(\mathcal{F}_\infty/\mathcal{N}_\infty)} \to Y_{\mathcal{N}_\infty} \to G(M'_{\mathcal{N}_\infty}/\mathcal{N}_\infty) \to 0$$

$$0 \to Z_{\mathcal{N}_\infty} \to Y_{\mathcal{N}_\infty} \to X_{\mathcal{N}_\infty} \to 0$$

se démontrent de la même manière que le lemme 2.5. Donc, le conoyau de $(Z_{\mathcal{F}_\infty})_{G(\mathcal{F}_\infty/\mathcal{N}_\infty)} \to Z_{\mathcal{N}_\infty}$ est isomorphe à $\mathcal{S}$. Or, d'après le lemme 5.2 (ii) de [14], il est aussi isomorphe à $\prod_{v/\mathfrak{P}^*} \mathrm{Ind}_v^{G(\mathcal{N}_\infty/F)} \mathbf{Z}_p$, où le produit est pris sur les places de F divisant $\mathfrak{P}^*$. On en déduit alors facilement l'isomorphisme de $\Lambda_{\mathcal{N}_\infty}$-modules

$$\mathcal{S}^{(1)}(-1) \simeq \prod_{v/\mathfrak{P}^*} \mathrm{Ind}_v^{G(N_\infty/F)} \mathrm{Hom}_{\mathbf{Z}_p}(T_{\mathfrak{P}}(F_v), \mathbf{Z}_p).$$

2.4. *Conséquences sur les groupes de Mordell–Weil*

Commençons par donner une propriété du groupe de Mordell–Weil sur F indépendante de ce qui a été fait auparavant et en particulier de la conjecture de Leopoldt. Nous montrons auparavant deux lemmes préliminaires.

LEMME 2.9: *Soit Y un Γ-module sans $\mathbf{Z}$-torsion. Si Γ' est un sous-groupe de Γ, le quotient $Y/Y^{\Gamma'}$ est sans torsion.*

DÉMONSTRATION: Supposons qu'il existe un élément y de Y et $m \in \mathbf{Z}$ tels que my appartienne à $Y^{\Gamma'}$. On a alors

$$m(\gamma y - y) = \gamma(my) - my = 0$$

pour tout $\gamma \in \Gamma'$. Donc $\gamma y - y$ est un élément de torsion de Y. Il est nécessairement nul. Donc y appartient à $Y^{\Gamma'}$, ce qui démontre le lemme.

LEMME 2.10: *Si* $\Gamma_n = \Gamma^{p^n}$ *et si* $\Omega(F_\infty)$ *est le sous-groupe de torsion de* F_∞, *le groupe de cohomologie* $H^1(\Gamma_n, \Omega(F_\infty))$ *est fini.*

DÉMONSTRATION: Il suffit de démontrer le lemme lorsque E_p est contenu dans F. La composante d'ordre premier à p de $\Omega(F_\infty)$ étant finie, on doit montrer que $H^1(F_\infty/F_n, E_{\mathfrak{P}^\infty})$ est fini si F_n est le corps fixé par Γ_n (la composante $\mathfrak{P}^*$-primaire se traitant de la même manière). Or, on a la suite exacte de cohomologie

$$0 \to H^1(F(E_{\mathfrak{P}^{*\infty}}, E_{\mathfrak{P}^m})/F(E_{\mathfrak{P}^m}), E_{\mathfrak{P}^m}) \to H^1(F_\infty/F_n, E_{\mathfrak{P}^\infty}) \to \cdots$$

$$\cdots \to H^1(F_\infty/F(E_{\mathfrak{P}^{*\infty}}, E_{\mathfrak{P}^m}), E_{\mathfrak{P}^\infty})$$

avec m tel que $E_{\mathfrak{P}^\infty}(F_n) = E_{\mathfrak{P}^m}$. Le dernier groupe est nul par un argument analogue à celui du lemme 1.4. Quand au premier groupe, il est fini d'ordre p^m.

Notons $\Omega(L)$ le sous-groupe de torsion de $E(L)$ pour toute extension L de F.

THÉORÈME 2.11: *Le groupe abélien* $E(F_\infty)/\Omega(F_\infty)$ *est libre. Il en est de même de* $E(L_\infty)/\Omega(L_\infty)$ *pour toute* $\mathbf{Z}_p$*-extension* L_∞ *de* F_∞ *contenue dans* F.

DÉMONSTRATION: La seconde affirmation se déduit de la première puisque un sous-groupe d'un groupe abélien libre est libre. Elle pourrait d'ailleurs se démontrer directement par des arguments analogues à ceux que l'on va donner pour $E(F_\infty)$.

Posons toujours $\Gamma_n = \Gamma^{p^n}$ et soit F_n le sous-corps de F fixé par Γ_n. Posons encore $Y_n = E(F_n)/\Omega(F_n)$ pour $n = 1, \infty$. De la suite exacte

$$0 \to \Omega(F_\infty) \to E(F_\infty) \to Y_\infty \to 0,$$

on déduit la suite exacte de cohomologie

$$0 \to Y_n \to Y_\infty^{\Gamma_n} \to H^1(\Gamma_n, \Omega(F_\infty)).$$

D'après le théorème de Mordell–Weil, Y_n est un groupe abélien de type fini. Donc, $Y_\infty^{\Gamma_n}$ est un groupe abélien de type fini d'après le lemme 2.10, sans torsion, donc libre de type fini. D'autre part, $Y_\infty^{\Gamma_m}/Y_\infty^{\Gamma_n}$ est sans torsion pour $m \geq n$ (lemme 2.9). Donc, $Y_\infty^{\Gamma_n}$ est facteur direct dans $Y_\infty^{\Gamma_m}$. Il existe des $\mathbf{Z}$-modules libres R_n tels que

$Y_\infty^{\Gamma_{n+1}} = Y_\infty^{\Gamma_n} \oplus R_n$. On a donc $Y_\infty^{\Gamma_n} = \bigoplus_{i=0}^{n-1} R_i$ et Y_∞ qui est la limite injective des $Y_\infty^{\Gamma_n}$ est libre.

On peut vérifier facilement que le lemme 2.10, donc le théorème 2.11, est vrai aussi dans le cas où p est inerte dans K.

THÉORÈME 2.12: *Sous l'hypothèse* $\mathrm{Leop}(F(E_{\mathfrak{P}}), \mathfrak{P})$ *ou* $\mathrm{Leop}(F(E_{\mathfrak{P}^*}), \mathfrak{P}^*)$, *pour presque toute* $\mathbf{Z}_p$*-extension* L_∞ *de* F *contenue dans* F_∞, $E(L_\infty)/\Omega(L_\infty)$ *est un groupe abélien libre de type fini.*

DÉMONSTRATION: Supposons par exemple $\mathrm{Leop}(F(E_{\mathfrak{P}}), \mathfrak{P})$. Grâce au théorème 2.11, $Y(L_\infty) = E(L_\infty)/\Omega(L_\infty)$ est de type fini si et seulement si $Y(L_\infty) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{P}}$ est un $\mathcal{O}_{\mathfrak{P}}$-module de type fini. Or, on a $\mathrm{Hom}_{\mathcal{O}_{\mathfrak{P}}}(Y(L_\infty) \otimes \mathcal{O}_{\mathfrak{P}}, \mathcal{O}_{\mathfrak{P}}) \tilde{\to} \mathrm{Hom}_{\mathcal{O}}(Y(L_\infty), \mathcal{O}_{\mathfrak{P}}) \tilde{\to} \widehat{E(L_\infty) \otimes K_{\mathfrak{P}}}/\mathcal{O}_{\mathfrak{P}}$ où $\hat{M}$ désigne le dual de Pontryagin de M. Ce dernier $\mathcal{O}_{\mathfrak{P}}$-module est de type fini dès que le dual de Pontryagin de $S(L_\infty)$ est un Λ_{L_∞}-module de torsion. On utilise alors le théorème 2.6.

Mazur et Kurchanov ont montré que, sous certaines hypothèses sur le corps F, il existe une $\mathbf{Z}_p$-extension L_∞ contenue dans F_∞ telle que $E(L_\infty)/\Omega(L_\infty)$ ne soit pas de type fini.

3. Séries caractéristiques

3.1. *Préliminaires*

Soit M un Λ-module compact de type fini de Λ-torsion, de série caractéristique f, celle-ci étant définie à une unité près. Soient H un sous-groupe de Γ tel que $\Gamma/H \simeq \mathbf{Z}_p$ et π_H la projection canonique

$$\Lambda \to \Lambda_H = \mathbf{Z}_p[[\Gamma/H]].$$

Alors, M_H est un Λ_H-module de torsion si et seulement si $\pi_H(f)$ est non nul, ce qui est vérifié sauf pour un nombre fini de sous-groupes H. Dans ce cas, M^H est un Λ-module pseudonul et un Λ_H-module de torsion; enfin, si f_{M_H} (resp. f_{M^H}) désigne la série caractéristique de M_H (resp. M^H) en tant que Λ_H-modules, on a $\pi_H(f) \sim f_{M_H}/f_{M^H}$, où $f \sim g$ signifie que f/g est une unité. En effet, on montre d'abord que, si M est pseudo-nul, on a bien $f_{M_H} \sim f_{M^H}$. Il existe un sous-groupe H' de Γ tel que $\Gamma/H' \simeq \mathbf{Z}_p$, $HH' = \Gamma$ et tel que M soit un $\mathbf{Z}_p[[H']]$-module de type fini et de torsion. On a alors la suite exacte de $\mathbf{Z}_p[[H']]$-modules

$$0 \to M^H \to M \to M \to M_H \to 0.$$

D'où l'égalité des séries caractéristiques de M_H et de M^H en tant que $\mathbf{Z}_p[[H']]$-modules et donc de f_{M_H} et de f_{M^H}, puisque H agit trivialement sur M_H et M^H. On montre ensuite que $\pi_H(f) \sim f_{M_H}/f_{M^H}$ dans le cas des Λ-modules du type $\Lambda/(f)$ puis dans le cas général en utilisant le théorème de classification des Λ-modules de type fini à modules pseudo-nuls près.

On peut d'autre part identifier l'algèbre d'Iwasawa Λ à l'algèbre des séries formelles à 2 variables $\mathbf{Z}_p[[T_1, T_2]]$ de la manière suivante. Soit M un Λ-module compact et soit γ_1 (resp. γ_2) un générateur topologique de $G(F_\infty/N_\infty^*)$ (resp. $G(F_\infty/N_\infty)$). On pose alors $T_1 x = (\gamma_1 - 1)x$, $T_2 x = (\gamma_2 - 1)x$ pour $x \in M$ et on prolonge cette action par continuité.

On appliquera ces remarques au dual de Pontryagin $\widehat{S(F_\infty)}$ de $S(F_\infty)$. Comme $\widehat{S(F_\infty)}$ n'a pas de sous- modules pseudo-nuls non nuls sous l'hypothèse Leop$(F(E_\mathfrak{P}), \mathfrak{P})$, $\widehat{S(F_\infty)}^{G(F_\infty/L_\infty)}$ est nul dès que $\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}$ est de Λ_{L_∞}-torsion. C'est la raison pour laquelle on étudie dans le paragraphe suivant la série caractéristique de $\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}$. Rappelons que, en général, c'est à-dire pour L_∞ différent de N_∞ et de N_∞^*, on a l'égalité

$$\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)} \simeq \widehat{S(L_\infty)}.$$

3.2. *Série caractéristique de* $\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}$

Commençons par donner l'indice de Ш$(F)(\mathfrak{P})$ dans Ш$'(F)(\mathfrak{P})$. On utilisera les notations suivantes: si a et b sont deux éléments de $K_\mathfrak{P}$, $a \sim b$ signifie que a/b est une unité de $K_\mathfrak{P}$; le cardinal d'un ensemble A est noté $\#A$; si B est un sous-module de A, $[A : B]$ désigne l'indice de B dans A. D'autre part, $\tilde{E}_v$ désignant toujours la réduction de E modulo v et k_v le corps résiduel de F en v, soit $\lambda_\mathfrak{P} : E(F) \to \prod_{v/\mathfrak{P}} \tilde{E}_v(k_v)$ l'homomorphisme donné par le produit des applications de réduction aux places de F divisant $\mathfrak{P}$ et soit $E_1(F)$ le noyau de $\lambda_\mathfrak{P}$.

PROPOSITION 3.1: ([5]). *L'indice de* Ш$(F)(\mathfrak{P})$ *dans* Ш$'(F)(\mathfrak{P})$ *est fini et divise le cardinal de* $\prod_{v/\mathfrak{P}} \tilde{E}_v(k_v)$. *De plus, si* Ш$(F)(\mathfrak{P}^*)$ *est fini, il est égal, à une unité près de* $K_\mathfrak{P}$, *à*

$$\frac{\prod_{v/\mathfrak{P}} \#\tilde{E}_v(k_v)}{\#E_{\mathfrak{P}^\infty}(F)[E(F)/\Omega(F) \otimes \mathcal{O}_{\mathfrak{P}^*} : E_1(F) \otimes \mathcal{O}_{\mathfrak{P}^*}]}$$

où $\Omega(F)$ *désigne le sous-groupe de torsion de* $E(F)$.

On suppose désormais qu'est vérifiée Leop$(F(E_\mathfrak{P}), \mathfrak{P})$ et que L_∞ est une $\mathbf{Z}_p$-extension telle que $\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}$ soit de Λ_{L_∞}-torsion.

On note $\tilde{g}(L_\infty, T)$ la série caractéristique (définie à une unité près) du Λ_{L_∞}-module $\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}$ où Λ_{L_∞} a été identifié à $\mathbf{Z}_p[[T]]$. On note d'autre part u_1 l'élément de $\mathbf{Z}_p$ donnant l'action du générateur γ_1 de $G(F_\infty/N_\infty^*)$ sur $E_{\mathfrak{P}^\infty}$(γ_1 étant prolongé à $F_\infty(E_\mathfrak{P})$ de manière à agir trivialement sur $E_\mathfrak{P}$).

THÉORÈME 3.2:

(i) *La multiplicité de T dans la série $\tilde{g}(L_\infty, T)$ est supérieure ou égale au rang $n_{E/F}$ de $E(F)$ sur $\mathcal{O}$.*

(ii) *Elle est égale à $n_{E/F}$ si et seulement si $Ш(F)(\mathfrak{P})$ est fini et l'image de $\widehat{S(L_\infty)}^{G(L_\infty/F)}$ dans $\mathrm{Hom}_{\mathbf{Z}_p}(E(F)\otimes_{\mathcal{O}}\mathcal{O}_\mathfrak{P}, \mathbf{Z}_p)$ est d'indice fini.*

Lorsque ces conditions sont vérifiées, l'application

$$\Phi_\mathfrak{P}(L_\infty) : [\widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}]^{G(L_\infty/F)} \to \mathrm{Hom}_{\mathbf{Z}_p}(E(F)\underset{\mathcal{O}}{\otimes}\mathcal{O}_\mathfrak{P}, \mathbf{Z}_p)$$

est injective car son noyau est alors à priori fini et donc nul d'après le théorème 2.6. On a alors:

THÉORÈME 3.3:

(i) *La valeur de $\tilde{g}(L_\infty, T)/T^{n_{E/F}}$ en $T=0$ est à une unité près, dans l'hypothèse du théorème* 3.2(ii),

$$\frac{\#Ш'(F)(\mathfrak{P})\prod_{v/\mathfrak{P}^*}\#\tilde{E}_v(k_v)}{\#E_{\mathfrak{P}^\infty}(F)}\cdot\frac{\#\mathrm{coker}\,\Phi_\mathfrak{P}(L_\infty)}{[\widehat{S(N_\infty)}^{G(N_\infty/F)} : \widehat{S(F_\infty)}^{G(N_\infty/F)}_{G(F_\infty/N_\infty)}]}$$

(ii) *Si $Ш(F)(\mathfrak{P})$ est fini et si l'image de $\widehat{S(N_\infty)}^{G(N_\infty/F)}$ dans $\mathrm{Hom}(E(F)\otimes_{\mathcal{O}}\mathcal{O}_\mathfrak{P}, \mathbf{Z}_p)$ est d'indice fini, pour presque toute $\mathbf{Z}_p$-extension L_∞, la multiplicité de T dans $\tilde{g}(L_\infty, T)$ est égale à $n_{E/F}$ et la valeur de $\tilde{g}(L_\infty, T)/T^{n_{E/F}}$ en $T=0$ est alors à une unité près*

$$\frac{\#Ш(F)(\mathfrak{P})\cdot\prod_{v/p}\#\tilde{E}_v(k_v)\cdot[\mathrm{Hom}(E(F)\otimes\mathcal{O}_\mathfrak{P}, \mathbf{Z}_p) : \widehat{S(N_\infty)}^{G(N_\infty/F)}]}{\#E_{\mathfrak{P}^\infty}(F)\#E_{\mathfrak{P}^{*\infty}}(\mathrm{F})\cdot[\mathrm{E(F)}/\Omega(\mathrm{F})\otimes\mathcal{O}_{\mathfrak{P}^*} : E_1(F)\otimes\mathcal{O}_{\mathfrak{P}^*}]}$$

$$\times\frac{\#\mathrm{coker}\,\Phi_\mathfrak{P}(L_\infty)}{\#\mathrm{coker}\,\Phi_\mathfrak{P}(N_\infty)}$$

si l'on suppose de plus que $Ш(F)(\mathfrak{P}^*)$ est fini.

Rappelons que l'on a $\#\tilde{E}_v(k_v)\sim\left(1-\dfrac{\Psi_{E/F}(v)}{Nv}\right)$ si Nv est le cardinal de k_v.

Avant de commencer la démonstration, démontrons les deux lemmes suivants.

LEMME 3.4: *L'homomorphisme* $\varphi : \widehat{S(F_\infty)}_\Gamma \to \widehat{S'(F)}$ *a un noyau et un conoyau finis.*

DÉMONSTRATION: Soient L_∞ une $\mathbf{Z}_p$-extension de F différente de N_∞, contenue dans F_∞ et ϵ l'homomorphisme

$$H^1(L_\infty/F, E_{\mathfrak{P}^\infty}(L_\infty)) \to \prod_{v/\mathfrak{P}^*} H^1(L_{\infty,v}/F_v, E)(\mathfrak{P}).$$

On vérifie facilement que, si $\hat{\varphi}$ est l'application transposée de φ dans la dualité de Pontryagin, le noyau de $\hat{\varphi}$ est égal à celui de ϵ et le conoyau de $\hat{\varphi}$ est un sous-groupe du conoyau de ϵ. Or, $E_{\mathfrak{P}^\infty}(L_\infty)$ est fini, donc $H^1(L_\infty/F, E_{\mathfrak{P}^\infty}(L_\infty))$ aussi (remarquons que l'on a aussi $H^1(N_\infty/F, E_{\mathfrak{P}^\infty}(N_\infty)) = 0$). Montrons que

$$H^1(L_{\infty,v}/F_v, E)(\mathfrak{P}) \tag{12}$$

est fini si v est une place au dessus de $\mathfrak{P}^*$. Par la dualité de Tate, le dual de (12) est égal à la limite projective des $E_{1,v}(F_v)/N_{\ell_v/F_v}(E_{1,v}(\ell_v))$ pour ℓ_v extension finie de F, contenue dans L_∞. D'après [12], ce dernier groupe est fini. Il en est donc de même de (12), ce qui démontre le lemme. Remarquons que de plus (12) est nul si $L_\infty = N_\infty$ car l'extension $N_{\infty,v}/F_v$ est alors non ramifiée pour v au dessus de $\mathfrak{P}^*$. On a donc démontré de plus que

$$\widehat{S'(F)} \simeq \widehat{S(N_\infty)}^{G(N_\infty/F)}. \tag{13}$$

LEMME 3.5: *L'injection naturelle* $[\widehat{S(F_\infty)}_{G(F_\infty/N_\infty)}]^{G(N_\infty/F)} \to \widehat{S(N_\infty)}^{G(N_\infty/F)}$ *a un conoyau fini C de cardinal*

$$\frac{\#\text{coker } \varphi}{\#\ker \varphi} \cdot \frac{\prod_{v/\mathfrak{P}^*} \#\tilde{E}_v(k_v)(p)}{\#E_{\mathfrak{P}^\infty}(F)}$$

où φ *est l'application du lemme* 3.4.

DÉMONSTRATION: Cette application s'étudie à l'aide des suites exactes (9) et (10). En posant $X = G(M'_{\mathcal{N}_\infty}/\mathcal{N}_\infty)^{(1)}(-1)_{G(N_\infty/F)}$, on en déduit facilement les suites exactes

$$0 \to C \to \mathcal{S}^{(1)}(-1)_{G(N_\infty/F)} \to X \to \widehat{S(N_\infty)}_{G(N_\infty/F)} \to 0$$

$$0 \to \widehat{S(F_\infty)}_\Gamma \to X \to (T_{\mathfrak{P}}(F))_\Gamma \to 0.$$

Comme d'après (13), $\widehat{S(N_\infty)}_{G(N_\infty/F)}$ est égal à $\widehat{S'(F)}$, on a la suite exacte

$$0 \to \ker \varphi \to \mathcal{S}^{(1)}(-1)_{G(N_\infty/F)}/C \to (T_{\mathfrak{P}}(F))_\Gamma \to \operatorname{coker} \varphi \to 0.$$

Il ne reste plus qu'à montrer l'égalité

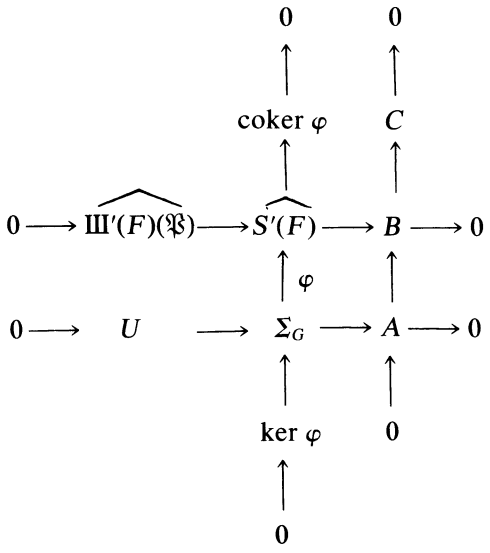
$$\#\mathcal{S}^{(1)}(-1)_{G(N_\infty/F)} = \prod_{v/\mathfrak{P}^*} \#\tilde{E}_v(k_v)(p) \tag{14}$$

Or, d'après le lemme 2.8, la série caractéristique de $\mathcal{S}^{(1)}(-1)$ est égale au produit sur les places v divisant $\mathfrak{P}^*$ telles que F_v contienne $E_{\mathfrak{P}}$ de $\omega_{n_v}(u_1(1+T)-1)$, où p^{n_v} est l'indice de $G(N_\infty/F)_v$ dans $G(N_\infty/F)$ et $\omega_n(T) = (1+T)^{p^n} - 1$; de plus, $\mathcal{S}^{(1)}(-1)^{G(N_\infty/F)}$ est fini donc nul. D'où

$$\begin{aligned}\#\mathcal{S}^{(1)}(-1)_{G(N_\infty/F)} &= \prod_{v/\mathfrak{P}^*} \omega_{n_v}(u_1 - 1) \\ &= \prod_{v/\mathfrak{P}^*} \#E_{\mathfrak{P}^\infty}(F_v),\end{aligned}$$

ce qui donne bien l'égalité (14) grâce à (5) et termine la démonstration du lemme 3.5.

DÉMONSTRATION DES THÉORÈMES 3.2 ET 3.3: Remarquons d'abord que le noyau de l'application $E(F) \otimes K_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}} \to E(F_\infty) \otimes K_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}$ est fini. Il est en effet inclus dans le noyau de l'application $S(F) \to S(F_\infty)$ qui est lui-même contenu dans $H^1(F_\infty/F, E_{\mathfrak{P}^\infty})$. Ce dernier groupe est fini (par exemple, il est isomorphe à $H^1(N_\infty^*/F, E_{\mathfrak{P}^\infty}(N_\infty^*))$. Posons $G = G(L_\infty/F)$, $\Sigma = \widehat{S(F_\infty)}_{G(F_\infty/L_\infty)}$ et $B = E(F)\widehat{\otimes} K_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}} = \operatorname{Hom}_{\mathbf{Z}_p}(E(F) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{P}}, \mathbf{Z}_p)$. La série caractéristique de B est égale à $T^{n_{E/F}}$. Or, d'après la remarque qui vient d'être faite, l'application naturelle de Σ dans B a un conoyau fini. Donc, $\tilde{g}(L_\infty, T)$ est divisible par $T^{n_{E/F}}$, ce qui démontre 3.2. (i). Soient R le noyau et C le conoyau de l'application $\Sigma \to B$. Notons encore A l'image de Σ dans B. Alors, si h est la série caractéristique du Λ_{L_∞}-module R, $\tilde{g}(L_\infty, T)$ a un zéro de multiplicité $n_{E/F}$ exactement en 0 si et seulement si $h(0)$ est non nul, ce qui est équivalent à R_G fini. On remarque d'autre part que si R_G est fini, R^G l'est aussi et donc est nul d'après le théorème 2.6. Soit U le noyau de l'application $\Sigma_G \to B$. On a alors le diagramme commutatif exact suivant:



où φ est l'application du lemme 3.4. On en déduit la suite exacte

$$0 \to \mathrm{Ker}\,\varphi \to U \to Ш'(F)(\mathfrak{P}) \to \mathrm{coker}\,\Phi \to C \to 0.$$

L'équivalence de 3.2 (ii) est alors immédiate. Pour calculer la valeur de $\tilde{g}(L_\infty, T)$, il suffit alors de calculer R_G (puisque R^G est nul), ce qui se fait facilement en reprenant les suites exactes et en comparant les cardinaux (par exemple, on a

$$[A : \Sigma^G] \cdot [B : A] = [B : \Sigma^G]).$$

Pour démontrer 3.3 (ii), introduisons la série caractéristique $g(F_\infty, T_1, T_2)$ du Λ-module $\widehat{S(F_\infty)}$ et le polynôme homogène $P(T_1, T_2)$ de plus bas degré de la série $g(F_\infty, T_1, T_2)$. Ce degré est supérieur ou égal à $n_{E/F}$. Les hypothèses de (ii) impliquent que ce degré est exactement $n_{E/F}$. D'autre part, le sous-groupe de Γ laissant fixe L est engendré par $\gamma_1^a \gamma_2^b$, où le couple (a, b) de $\mathbf{Z}_p \times \mathbf{Z}_p$ est déterminé par L_∞ à multiplication par une unité de $\mathbf{Q}_p^\times$ près et où a et b sont premiers entre eux. Pour un bon choix de l'identification de Λ_{L_∞} avec $\mathbf{Z}_p[[T]]$, le lien entre $g(F_\infty, T_1, T_2)$ et $\tilde{g}(L_\infty, T)$ est le suivant

$$\tilde{g}(L_\infty, T) \sim g(F_\infty, (1+T)^b - 1, (1+T)^a - 1).$$

La valeur de $\tilde{g}(L_\infty, T)/T^{n_{E/F}}$ en $T = 0$ est donc $P(b, a)$. En particulier, la multiplicité de T dans $\tilde{g}(L_\infty, T)$ est $n_{E/F}$ sauf pour un nombre fini de $\mathbf{Z}_p$-extensions (en fait au plus $2n_{E/F}$) correspondant aux zéros de

$P(T, 1)$ et de $P(1, T)$. On en déduit facilement, grâce à (ii) et à la proposition 3.1, la suite de (iv).

3.3. *Conséquences*

Remarquons d'abord que l'on retrouve la formule de [5] pour $\widehat{S(N_\infty)}$. En effet, en utilisant les suites exactes (9) et (10), on montre facilement que la série caractéristique $g(N_\infty, T)$ de $\widehat{S(N_\infty)}$ est égale à

$$(u_1(1+T)-1)\prod_{v/\mathfrak{P}^*}\omega_{n_v}(u_1(1+T)-1)^{-1}\tilde{g}(N_\infty, T)$$

où le produit est pris sur les places v de F au dessus de $\mathfrak{P}^*$, telles que F_v contienne $E_\mathfrak{P}$ et où p^{n_v} est l'indice de $G(N_\infty/F)_v$ dans $G(N_\infty/F)$.

Donnons maintenant un corollaire du théorème 3.3 et de sa démonstration.

COROLLAIRE 3.6: *On suppose toujours vérifiée l'hypothèse* Leop$(F(E_\mathfrak{P}), \mathfrak{P})$. *Si* Ш$(F)(\mathfrak{P})$ *est fini et si* $E(F)$ *est un groupe de torsion, alors pour toute* $\mathbf{Z}_p$*-extension* L_∞, $E(L_\infty)/\Omega(L_\infty)$ *est un* $\mathbf{Z}$*-module de type fini. Si de plus la valeur* $g(F_\infty, 0, 0)$ *de la série caractéristique du* Λ*-module* $\widehat{S(F_\infty)}$ *est une unité, alors* Ш$(F_\infty)(\mathfrak{P})$ *est nul et* $E(F_\infty)$ *est un groupe de torsion.*

EXEMPLE: Supposons de plus que E est défini sur $\mathbf{Q}$ et que Ш$(\mathbf{Q})(p)$ est fini. Le groupe de Tate–Shafarevitch Ш$(K)(p)$ de E sur K peut être alors décomposé selon les sous-espaces propres relatifs aux caractères de $G(K/\mathbf{Q})$

$$Ш(K)(p) = Ш(K)(p)^{G(K/\mathbf{Q})} \oplus Ш(K)(p)^{-}$$

notons Ψ le caractère non trivial de $G(K/\mathbf{Q})$. Le premier de ces sous-groupes Ш$(K)(p)^{G(K/\mathbf{Q})}$ est isomorphe à Ш$(\mathbf{Q})(p)$. On peut interpréter Ш$(K)(p)^{-}$ à l'aide de la courbe elliptique E tordue par le caractère Ψ que l'on note $E^{(\Psi)}$. En effet, Ш$(K)(p)^{-}$ est égal au groupe de Tate–Shafarevitch de $E^{(\Psi)}$ sur $\mathbf{Q}$ (si Φ est un isomorphisme de E sur $E^{(\Psi)}$ sur K, on a $\Phi^{-1}\circ {}^{\sigma}\Phi = \Psi(\sigma)$ pour $\sigma \in G(\bar{\mathbf{Q}}/\mathbf{Q})$). D'autre part, comme E et $E^{(\Psi)}$ sont a multiplication complexe par K, elles sont isogènes sur $\mathbf{Q}$ ([7]). Elles ont donc même rang sur $\mathbf{Q}$, qui est aussi égal au rang $n_{E/K}$ de $E(K)$ en tant que $\mathcal{O}$-module. De plus, d'après [3] (invariance de la conjecture de Birch et Swinnerton-Dyer par isogénie), si $E(\mathbf{Q})$ est fini, les composantes p-primaires des groupes de

Tate–Shafarevitch de E de $E^{(\Psi)}$ sur $\mathbf{Q}$ sont simultanément finies et de même cardinal (car p est non ramifié dans K, différent de 2 et 3, et E et $E^{(\Psi)}$ ont bonne réduction en p sur K, donc sur $\mathbf{Q}$). On en déduit donc que, si $Ш(\mathbf{Q})(p)$ est fini, il en est de même de $Ш(K)(p)$ et on a $\#Ш(K)(p) = \#Ш(\mathbf{Q})(p)^2$. D'autre part, par l'accouplement de Cassels, on a $\#Ш(K)(p) = \#Ш(K)(\mathfrak{P})^2 = \#Ш(K)(\mathfrak{P}^*)^2$.

Supposons toujours que E est défini sur $\mathbf{Q}$, que $E(\mathbf{Q})$ est fini, que $Ш(\mathbf{Q})(p)$ est réduit à 1 et que $\tilde{E}_p(\mathbf{F}_p)$ est d'ordre premier à p (p est dit non anormal). Alors, $g(F_\infty, 0, 0)$ est une unité et les hypothèses du corollaire sont vérifiées. Par exemple, soit E la courbe elliptique définie par $x^3 + y^3 = 1$. Le groupe $E(\mathbf{Q})$ est cyclique d'ordre 3 et la courbe admet des multiplications complexes par l'anneau des entiers de $K = \mathbf{Q}(\sqrt{-3})$. Conjecturalement, c'est-à-dire par la conjecture de Birch et Swinnerton–Dyer, le groupe $Ш(\mathbf{Q})$ est réduit à 1 ([2], [5]). Prenons pour p le nombre premier $p = 13$. Alors, toutes les conditions précédentes sont remplies. Donc, $Ш(F_\infty)(p)$ devrait être nul et $E(F_\infty)$ un groupe abélien de torsion.

4. Construction d'une forme bilinéaire sur $E(F)$

4.1. *Notations*

Soit L une extension finie de F. Si v est une place de L, on note $e_v(L/\mathbf{Q})$ l'indice de ramification de L sur $\mathbf{Q}$ en v. Si v divise q ou ∞, on considère la valeur absolue $|\ |_v$ prolongeant $|\ |_q$ ou $|\ |_\infty$ sur $\mathbf{Q}_q$ normalisée par $|q|_q = 1/q$, $|2|_\infty = 2$. On pose alors $\nu(x) = -\log|x|_v$ et $\nu'(x) = e_v(L/\mathbf{Q})\ \nu(x)/\log q$. Alors, si x est un élément de L, $\nu'(x)$ est un entier et on a

$$(x) = \prod_{v \in I(L)} \mathfrak{P}_v^{\nu'(x)} \tag{15}$$

où le produit porte sur les places v finies de L et où $\mathfrak{P}_v$ est l'idéal premier associé à v.

On fait désormais l'hypothèse que E a bonne réduction partout sur L (par exemple, on peut prendre ici $L = F(E_{\mathfrak{P}})$). Le grossencharakter $\Psi_{E/L}$ de E sur L est alors de conducteur 1. Il est défini sur le groupe des idéaux de L et vérifie sur les idéaux principaux de L la formule

$$\Psi_{E/L}((a)) = N_{L/K}(a) \text{ pour } a \in L. \tag{16}$$

4.2. *Facteurs locaux de la hauteur de Néron–Tate*

On choisit une équation de Weierstrass de E, 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 F. Soient Δ son discriminant et v une place de L.

THÉORÈME 4.1: (Néron–Tate): *Il existe une unique fonction* $\lambda_v : E(L_v) - \{0\} \to \mathbb{R}$, *continue pour la topologie v-adique et telle que* (i) $\lim_{p \to 0} \lambda_v(P) - \nu(t(P))$ *existe pour un, donc pour tout, paramètre uniformisant de la courbe à l'origine*; (ii) *pour tout couple* (P, Q) *de* $E(L_v)$ *tel que* $P \pm Q \neq 0$, *on a*

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) + \nu(x(P) - x(Q)) - \tfrac{1}{6}\nu(\Delta). \tag{17}$$

On connait des formules explicites pour λ_v. Dans le cas qui nous intéresse ici, si v est non archimédienne et si E a bonne réduction en v, on a

$$\lambda_v(P) = \tfrac{1}{2}\,\mathrm{Sup}(0, -\nu(x(P))) - \tfrac{1}{6}\,\nu(\Delta),$$

où $x(P)$ et $y(P)$ sont les coordonnées de P dans le modèle choisi. Posons $\lambda'_v(P) = e_v(L/\mathbf{Q})\ \lambda_v(P)/\log q$ (si v est au dessus du nombre premier q). Alors $6\lambda'_v(P)$ est un entier dès que P appartient à $E(L_v)$.

4.3. *Partie rationnelle de la forme quadratique*

Posons

$$\mu(P) = \prod_{v \in I(L)} \Psi_{E/L}(\mathfrak{P}_v)^{6\lambda'_v(P)}$$

pour $P \in E(L)$, où $\mathfrak{P}_v$ est toujours l'idéal premier associé à v (que l'on notera aussi v par abus de notation) et où le produit porte sur les places finies de L. C'est un élément de K et on a

$$\frac{\mu(P+Q)\mu(P-Q)}{\mu(P)^2\mu(Q)^2} = \frac{N_{L/K}(x(P) - x(Q))^6}{N_{L/K}(\Delta)} \tag{18}$$

si $P \pm Q \neq 0$. En effet, l'expression de gauche est égale, grâce à (15), à

$$\prod_{v \in I(L)} \Psi_{E/L}(\mathfrak{P}_v^{v'((x(P)-x(Q))^6/\Delta)})$$
$$= \Psi_{E/L}((x(P)-x(Q))^6/\Delta) = N_{L/K}(x(P)-x(Q))^6/N_{L/K}(\Delta).$$

4.4. *Partie transcendante de la forme quadratique*

On suppose désormais que l'équation de Weierstrass est minimale pour toute place v au dessus de $\mathfrak{P}$. Soient v une place au dessus de $\mathfrak{P}$, $t = -x/y$ un paramètre uniformisant de la courbe en 0 et $\mathscr{L}_v$ le logarithme du groupe formel $E_{1,v}$, noyau de la réduction modulo v. Notons φ_v la série entière récriproque de $\mathscr{L}_v$. On définit alors les séries

$$\mathfrak{P}_v(z) = x(\varphi_v(z)) + (a_1^2 + 4a_2)/12$$
$$= 1/z^2 + \sum_2^\infty \gamma_k z^{2k-2},$$
$$\sigma_v(z) = z \exp\left(-\sum_2^\infty \gamma_k \frac{z^{2k}}{2k(2k-1)}\right)$$
$$\Theta_v(z) = \Delta \exp(-6s_2 z^2)\, \sigma_v(z)^{12}$$

(pour la définition de s_2, cf [1]). La série $\Theta_v(z)$ converge dans $\bar{\mathbf{Q}}_p$ pour $v(z) > v(p)/(p-1)$. Soit $E_1'(L)$ le sous-groupe de $E(L)$ suivant

$$E_1'(L) = \left\{ \begin{array}{l} P \in E(L) \text{ tel que } v(x(P)) < 0 \\ \qquad\qquad\qquad\qquad \text{pour tout } v \mid \mathfrak{P} \\ v(t(P)) > \dfrac{v(p)}{p-1} \end{array} \right\}$$

On pose alors

$$\Phi(P) = \prod_{v/\mathfrak{P}} N_{L_v/\mathbf{Q}_p}(\Theta_v(\mathscr{L}_v(j_v(t(P))))) \in \mathbf{Q}_p$$

pour $P \in E_1'(L)$, où j_v est le plongement de L dans $\bar{\mathbf{Q}}_p$ correspondant à la place v (par abus de notation, on n'écrira plus j_v, il est aussi sous-entendu dans les injections $E(L) \to E(L_v)$). Alors, on a la formule

$$(19) \qquad \frac{\Phi(P+Q)\Phi(P-Q)}{\Phi(P)^2\Phi(Q)^2} = (-1)^{[L:K]} \frac{N_{L/K}(x(P)-x(Q))^{12}}{N_{L/K}(\Delta)^2}$$

lorsque P et Q appartiennent à $E'_1(L)$ et $P \pm Q \neq 0$ (démonstration analogue à celle de [1]).

4.5. *Définition et théorème*

Posons

$$\varphi(P) = \mu(P)^2 \Phi(P)^{-1} \in \mathbf{Q}_p$$
$$h(P) = \log_p \varphi(P)$$

pour P élément non nul de $E'_1(L)$ et

$$h(0) = 0,$$

où $\log_p$ est le logarithme sur $\bar{\mathbf{Q}}_p$ déterminé par $\log_p p = 0$ et où un élément de K est plongé dans $\mathbf{Q}_p$ par le plongement associé à la place $\mathfrak{P}$. *Alors, h est une fonction quadratique de $E'_1(L)$, c'est-à-dire qu'elle vérifie*

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

En effet, cela est vrai pour $P \pm Q \neq 0$, d'après (18) et (19), et donc pour tout couple (P, Q) d'éléments de $E'_1(L)$. Remarquons que comme $E'_1(L)$ est d'indice fini N dans $E(L)/\Omega(L)$ (où $\Omega(L)$ est le sous-groupe de torsion de $E(L)$), on peut prolonger h à $E(L)/\Omega(L)$ par

$$h(P) = h(NP)/N^2 \text{ si } P \in E(L).$$

On a donc construit ainsi une forme quadratique sur $E(L)/\Omega(L)$ à valeurs dans $\mathbf{Q}_p$. Nous allons maintenant en donner quelques propriétés élémentaires, en particulier une propriété d'intégralité.

4.6. *Quelques remarques et propriétés*

Remarquons d'abord que $\varphi(P)$ est une unité de $\mathbf{Q}_p$. On a en effet si P ne se réduit pas en un point singulier dans le modèle choisi

$$(20) \quad \varphi(P) = \Big(\prod_{v \in I(L)} \psi_{E/L}(v)^{6 \operatorname{Sup}(0, \nu'(x(P)))}, t^{-12} \Big) \prod_{v/\mathfrak{P}} N_{L_v/\mathbf{Q}_p}(\psi_v(t(P)))^{-1}$$

où l'on a posé $\psi_v(t) = \Theta_v(\mathscr{L}_v(t)) \cdot t^{-12} \cdot \Delta^{-1}$. Il suffit pour le voir d'utiliser l'expression explicite de λ_v et la formule (15) appliquée à Δ.

Comme $P \in E_1'(L)$, le premier facteur est une unité. Il en est de même de $\psi_v(t)$ dès que $v(t) > v(p)/p - 1$.

La forme quadratique h a d'autre part un bon comportement vis-à-vis des endomorphismes. On peut en effet montrer de la même manière que dans [1] que, si α est un élément de $\mathcal{O}$, on a $h(\alpha P) = \deg \alpha\, h(P)$. Ici, deg α désigne le degré de l'endomorphisme α, c'est-à-dire la norme sur $\mathbf{Q}$ de α.

Il serait intéressant de montrer que h est à valeurs dans $\mathbf{Z}_p$. A défaut de le faire, nous allons montrer le

LEMME 4.2: *Si P appartient à $E_1'(L)$, $h(P)$ appartient à $\#E_{\mathfrak{P}^\infty}(L(E_{\mathfrak{P}}))\mathbf{Z}_p$.*

DÉMONSTRATION: Posons $n = \#E_{\mathfrak{P}^\infty}(L(E_{\mathfrak{P}}))$. Soient ω le caractère de Teichmüller de $\mathbf{Z}_p$ et $\langle x \rangle = x\omega(x)^{-1}$. Si x appartient à $\mathbf{Z}_p$ et si x est congru à 1 modulo p^m, alors $\log_p x$ appartient à $p^m\mathbf{Z}_p$. Utilisons la formule (20) et étudions chacun des termes. Il y a d'abord un produit de $\psi_{E/L}(v)$ pour des places v premières à $\mathfrak{P}$. Or, pour une telle place, $E_{\mathfrak{P}^m}$ est contenu dans $L(E_{\mathfrak{P}})$ si et seulement si $\psi_{E/L}(v) \equiv 1 \bmod \mathfrak{P}^m$. Donc, en particulier, $\psi_{E/L}(v)$ est congru à 1 modulo $\mathfrak{P}^n$. D'autre part, l'unique $\mathbf{Z}_p$-extension K_∞ de K non ramifiée en dehors de $\mathfrak{P}$ est totalement ramifiée en $\mathfrak{P}$. En effet, choisissons une courbe elliptique auxiliaire $\mathcal{E}$ définie sur le corps de Hilbert H de K, à multiplication complexe par $\mathcal{O}$ et ayant bonne réduction aux places de H divisant $\mathfrak{P}$. Alors, l'extension $H(\mathcal{E}_{\mathfrak{P}^\infty})/H$ est totalement ramifiée aux places de H divisant $\mathfrak{P}$. On en déduit que $\mathcal{E}_{\mathfrak{P}^\infty}(H(\mathcal{E}_{\mathfrak{P}}))$ est égal à $\mathcal{E}_{\mathfrak{P}}$. Comme $H(\mathcal{E}_{\mathfrak{P}^\infty})$ est le composé de $H(\mathcal{E}_{\mathfrak{P}})$ et de K_∞, on en déduit que $H \cap K_\infty$ est réduit à K, ce qui implique que K_∞/K est totalement ramifiée en $\mathfrak{P}$. On peut alors appliquer le lemme 6 de [4] à $\psi_v(t(P))$ qui est une unité congrue à 1 modulo v.

EXEMPLE: Soit la courbe elliptique $E/\mathbf{Q}$ définie par $y^2 = x^3 - 49x$. Elle est à multiplication complexe par l'anneau des entiers de $K = \mathbf{Q}(\sqrt{-1})$ et a bonne réduction en tout nombre premier différent de 2 et de 7. Le groupe $E(\mathbf{Q})$ est de rang 1 et son groupe de torsion est le groupe des points d'ordre 2([2]). Choisissons comme nombre premier $p = 5$. On vérifie que $\tilde{E}_5(\mathbf{F}_5)$ est d'ordre 4 (5 est donc non anormal). Soit le point $P = 2(25, 120)$ de $E(\mathbf{Q})$. Il appartient à $E_1'(K)$. D'autre part, comme la valuation de $t = x/y$ en 5 est 1, l'indice de $\mathcal{O}P$ dans $E(K)$ est premier à 5. Calculons la valuation de $h(P)$. On a

$$\varphi(P) = (\Psi_{E/K}(\mathfrak{P}_5)\Psi_{E/K}(\mathfrak{P}_5^*))^{48} \times \Theta(\mathcal{L}_{\mathfrak{P}_5}(t))^{-4} \times \Delta^4$$

où $\mathfrak{P}_5$ et $\mathfrak{P}_5^*$ sont les deux idéaux de K au dessus de 5. Comme E est définie sur $\mathbf{Q}$, $\Psi_{E/K}(\mathfrak{P}_5^*)$ est égal au conjugué de $\Psi_{E/K}(\mathfrak{P}_5)$ et on a donc

$$\varphi(P) = \alpha^{48} \times (\Theta(\mathscr{L}_{\mathfrak{P}_5}(t)\Delta^{-1}\mathscr{L}_{\mathfrak{P}_5}(t)^{-12})^{-4} \times (\mathscr{L}_{\mathfrak{P}_5}(t)/t)^{-48}$$

avec $\alpha = 9179039\mathscr{L}$.

Or, si $\nu(z)$ et $\nu(t)$ sont supérieurs à 1, la valuation de $\log \Theta_v(z)/\Delta z^{12}$ et de $1 - \mathscr{L}_{\mathfrak{P}_5}(t)/t$ est supérieure à 4. En effet, la courbe E étant à multiplication complexe par l'anneau des entiers de $\mathbf{Q}(\sqrt{-1})$, s_2 est nul. Donc, le développement de $\log \Theta_v(z)/\Delta z^{12}$ est de la forme $\alpha_4 z^4 + \alpha_6 z^6 + \cdots$ (avec $n!\ \alpha_n \in \mathbf{Z}_5$). De même, le développement de $1 - \mathscr{L}_{\mathfrak{P}_5}(t)/t$ est de la forme $\frac{98}{5}t^4 + \beta_5 t^5 + \cdots$ avec $(n+1)\beta_n \in \mathbf{Z}_5$. Une étude de ces séries permet alors de conclure. Comme d'autre part α^{48} est non congru à 1 modulo 25, on en déduit que $h(P)$ est égale à une unité près de $\mathbf{Q}_5^\times$ à 5.

BIBLIOGRAPHIE

[1] D. BERNARDI: Hauteurs p-adiques sur les courbes elliptiques. *Séminaire Delange–Pisot–Poitou* (1980).

[2] B.J. BIRCH et H.P.F. SWINNERTON-DYER: Notes on elliptic curves I. *J. reine angew. Math., 212* (1963) 7–25.

[3] J.W.S. CASSELS: Arithmetic on curves of genus 1. *J. reine angew. Math. (IV) 207* (1962) 234–246, *(VIII) 217* (1965) 180–189.

[4] J.- COATES: Kummer's criterium for Hurwitz numbers. *Proceedings of the International Congress on Algebraic Number Theory, Japan: Kyoto* (1976).

[5] J. COATES: Elliptic curves with complex multiplication. Hermann Weyl lectures 1979, Annals of Math. Studies (à paraître).

[6] R. GREENBERG: On the structure of certains Galois groups. *Inventiones Math. 47* (1978) 85–99.

[7] B.H. GROSS: Arithmetic on elliptic curves with complex multiplication. *Lecture notes in Mathematics 776*, Berlin–Heidelberg–New York: Springer (1980).

[8] M. HARRIS: P-adic representation arising from descent on abelian varieties. *Compositio Mathematica, 39* (1979) 177–245.

[9] M. HARRIS: Systematic growth of Mordell–Weil groups of abelian varieties in towers of number fields. *Inventiones Math. 51* (1979) 123–141.

[10] P.F. KURCHANOV: Elliptic curves of infinite rank over Γ-extensions. *Mat. U.S.S.R. Sbornik. Vol 19, No.* 2 (1973).

[11] S. LANG et J. TATE: Principal homogeneous spaces over abelian varieties. *American J. of Math. 78* (1956) 659–684.

[12] B. MAZUR: Rational points on abelian varieties with values in towers of number fields. *Inventiones Math. 18* (1972) 183–266.

[13] B. MAZUR: Trees of rational points on elliptic curves. (Non publié).

[14] J.-P. WINTENBERGER: Structure galoisienne de limites projectives d'unités locales. *Compositio Mathematica, 42* (1980) 89–104.

(Oblatum 22-X-1980 & 11-XII-1980)

Université Pierre et Marie Curie
L.M.F. 46–45
2, Place Jussieu
75230 Paris Cedex 05