MÉMOIRES DE LA S. M. F.

BERNADETTE PERRIN-RIOU

Arithmétique des courbes elliptiques et théorie d'Iwasawa

Mémoires de la S. M. F. 2^e série, tome 17 (1984)

<http://www.numdam.org/item?id=MSMF_1984_2_17__1_0>

Mémoire de la Société Mathématique de France, n° 17
Supplément au Bulletin de la S.M.F.
Tome 112, 1984, fascicule 4

ARITHMÉTIQUE DES COURBES ELLIPTIQUES ET THÉORIE D'IWASAWA

Bernadette PERRIN-RIOU

RÉSUMÉ

On applique à l'arithmétique des courbes elliptiques à multiplication complexe les méthodes d'Iwasawa sur les $\mathbb{Z}_p$-extensions et l'on relie la série caractéristique du groupe de Selmer relatif à un nombre premier ordinaire sur une $\mathbb{Z}_p$-extension aux hauteurs p-adiques construites de manière analogue à la hauteur complexe de Néron-Tate.

ABSTRACT

We apply the methods of the theory of $\mathbb{Z}_p$-extensions of Iwasawa to study the arithmetic of elliptic curves with complex multiplication. We link the characteristic power series of the Selmer group of the elliptic curve, relative to an ordinary prime p, to a canonical p-adic height on the curve which is analogous to the archimedean canonical height of Néron-Tate.

Bernadette PERRIN-RIOU
U. E. R. 48
Tour 45-46, 3ème étage
Université Pierre et Marie Curie
4, place Jussieu
75230 PARIS CEDEX 05
FRANCE

Texte reçu le 19 décembre 1983, révisé le 13 décembre 1984

0037-9484/84 04/01.130/$ 130/

Je dois tout d'abord remercier J. Coates qui m'a initié aux courbes elliptiques. Mes remerciements vont également à G. Poitou qui m'a introduit à l'arithmétique, à D. Bertrand pour l'intérêt qu'il a bien voulu accorderà ce travail, à P. Cassou-Noguès pour avoir accepté de faire partie du jury et à J. Sjöstrand qui m'a donné un sujet de seconde thèse. Je remercie D. Bernardi pour de nombreuses discussions fructueuses, en particulier à propos des exemples numériques.

C'est Mme Le Bronnec qui a assuré la frappe de ce texte. Je la remercie pour le goût et la gentillesse avec lesquels elle l'a fait.

COURBES ELLIPTIQUES ET THÉORIE D'IWASAWA

Introduction

Le résultat fondamental dû à Mordell et Weil concernant une courbe elliptique E définie sur un corps de nombres F est que le groupe $E(F)$ de ses points rationnels sur F est un groupe abélien de type fini. En fait, trouver un algorithme pour calculer le groupe $E(F)$ et son rang est un problème remontant à Diophante qui n'est toujours pas résolu. Dans la recherche du rang de $E(F)$ par la méthode classique de la descente apparaissent naturellement d'autres invariants arithmétiques comme le groupe de Shafarevitch et Tate de E sur F et la hauteur canonique de Néron et Tate qui est une forme bilinéaire sur $E(F)$ modulo torsion à valeurs dans $\mathbb{R}$ non dégénérée sur $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Dans les années trente, Hasse et Weil ont associé à la courbe elliptique E/F une fonction $L(E,s)$ d'une variable complexe construite comme produit sur les places v de F des fonctions zêta de la courbe réduite en v et conjecturé que cette fonction admet un prolongement analytique et une équation fonctionnelle pour le changement de s en $2-s$. Inspirés par les travaux de Siegel, Birch et Swinnerton-Dyer ont ensuite conjecturé que le comportement de $L(E,s)$ au point critique $s=1$ est lié aux invariants arithmétiques précédents. Dans le cas des courbes elliptiques à multiplication complexe, l'existence d'un Grössencharakter associé à E/F montrée par Deuring et Weil permet de démontrer la conjecture de Hasse-Weil. Par contre, nous connaissons très peu de choses sur le moyen de démontrer la conjecture de Birch et Swinnerton-Dyer.

Nous prenons dans cette thèse le point de vue p-adique qui a été inspiré à la fois par les travaux de Artin et Tate sur l'analogue géométrique de la conjecture de Birch et Swinnerton-Dyer et par les idées d'Iwasawa sur les $\mathbb{Z}_p$-extensions de corps de nombres. Nous supposons que E est une courbe elliptique à multiplication complexe et que p est un nombre premier tel que E a bonne réduction ordinaire en toute place de F au dessus de p. Soit $F_\infty = F(E_{p^\infty})$ le corps obtenu en rajoutant à F les points de p^n-torsion de E $(n \geq 1)$. Appelons dans cette introduction module d'Iwasawa de E/F_∞ le dual de Pontryagin du groupe de Selmer de E sur F_∞ relatif à p^∞. C'est un $\mathbb{Z}_p[[G(F_\infty/F)]]$-module de type fini. L'objet de cette thèse est l'étude de ce module et de sa série caractéristique lorsqu'il est de torsion. Nous commençons donc par donner des conditions pour que le module d'Iwasawa de E/F_∞ soit de torsion. Ces conditions sont liées aux conjec-

tures de Leopoldt. Nous montrons aussi, toujours sous des hypothèses de Leopoldt, qu'il est de dimension projective inférieure à 1.

La série caractéristique de ce module est conjecturalement liée aux fonctions L p-adiques à deux variables construites par Katz. Nous montrons pour cette série caractéristique l'analogue p-adique de la conjecture de Birch et Swinnerton-Dyer (Théorème V.17). Remarquons qu'il est possible de formuler cette conjecture p-adique même si le groupe de Shafarevitch-Tate n'est pas fini. La démonstration consiste à construire une famille de formes bilinéaires algébriques sur $E(F)$, associées aux caractères de $G(F_\infty/F)$ à valeurs dans $\mathbb{Z}_p^*$. Elles se déduisent en fait d'un pseudo-isomorphisme canonique entre le module d'Iwasawa de E/F_∞ et une version tordue de son adjoint (remarquons que ce pseudo-isomorphisme permet aussi de montrer une équation fonctionnelle sur sa série caractéristique (Théorème V.6), version fidèle des équations fonctionnelles des fonctions L complexes et p-adiques). D'autre part, ont été construites des formes bilinéaires appellées hauteurs p-adiques, analogues de la hauteur complexe de Néron-Tate, de nature analytique et facilement calculables. Le coeur de la démonstration est de montrer l'égalité entre ces deux familles de formes bilinéaires.

Enfin, pour égayer cette introduction de quelques exemples numériques, remarquons que la connaissance des propriétés arithmétiques de E/F et de ces formes bilinaires donne des renseignements sur la croissance du rang de E le long d'une $\mathbb{Z}_p$-extension de F contenue dans F_∞. Les exemples sont choisis parmi les courbes elliptiques $E : y^2 = x^3 - dx$ ($d \in \mathbb{Z}$) à multiplication complexe par $K = \mathbb{Q}(i)$. On prend comme nombre premier $p = 5$. Une $\mathbb{Z}_5$-extension de K joue un rôle particulier : c'est l'unique $\mathbb{Z}_5$-extension de K galoisienne sur $\mathbb{Q}$ et non abélienne sur $\mathbb{Q}$; on la note K_∞^-.

$E : y^2 = x^3 - x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est nul. Pour toute $\mathbb{Z}_5$-extension L_∞ de K, $E(L_\infty)$ modulo torsion est nul.

$E : y^2 = x^3 - 36x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 1. Pour toute $\mathbb{Z}_5$-extension L_∞ de K sauf peut-être K_∞^-, $E(L_\infty)$ modulo torsion est de type fini.

$E : y^2 = x^3 - 2x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 1. Pour toute $\mathbb{Z}_5$-extension L_∞ de K sauf peut-être K_∞^-, $E(L_\infty)$ modulo torsion est de type fini. De plus si N_∞ est l'unique $\mathbb{Z}_5$-extension de K non ramifiée au dehors de $(2+i)$, $E(N_\infty)$ modulo torsion est de rang 2 sur $\mathbb{Z}$.

$E : y^2 = x^3 + 14x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 2. Pour toute $\mathbb{Z}_5$-extension L_∞ de K sauf peut-être pour deux d'entre elles, $E(L_\infty)$ modulo torsion est de rang fini. Les niveaux finis de ces deux $\mathbb{Z}_5$-extensions peuvent être calculés explicitement.

$E : y^2 = x^3 - 226x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 3. Pour toute $\mathbb{Z}_5$-extension L_∞ sauf peut-être K_∞^-, $E(L_\infty)$ modulo torsion est de type fini.

Finalement, donnons un résumé de chacun des chapitres. Dans le chapitre I, on rappelle les résultats sur les $\mathbb{Z}_p[[T_1,\ldots,T_r]]$-modules qui seront nécessaires par la suite[1]. Dans le chapitre II, après avoir introduit les objets qui seront utilisés (par exemple divers groupes de Selmer) et les avoir comparés, on étudie la structure de $G(F_\infty/F)$-module du groupe de Selmer de E/F_∞ et on montre que son dual de Pontryagin est de dimension projective sur $\mathbb{Z}_p[[G(F_\infty/F)]]$ inférieure ou égale à 1 sous certaines hypothèses reliées à la conjecture de Leopoldt que nous supposerons par la suite. Dans le chapitre III, on définit les hauteurs p-adiques attachées à une $\mathbb{Z}_p$-extension et on donne un moyen pratique de les calculer. Dans le chapitre IV, on construit une forme bilinéaire algébrique attachée à la $\mathbb{Z}_p$-extension particulière N_∞ et on la relie à la hauteur p-adique définie dans le chapitre III. Dans le chapitre V, on étudie le cas d'une $\mathbb{Z}_p$-extension quelconque de F contenue dans F_∞ et on démontre l'analogue p-adique de la conjecture de Birch et Swinnerton-Dyer pour la série caractéristique du module d'Iwasawa de E/F_∞ et l'équation fonctionnelle p-adique.

Certains des exemples numériques s'appuient sur les calculs faits dans [3]. D'autre part, précisons que, dans le but d'être complet, nous avons repris les démonstrations de résultats précédemment parus ([25], [26]), la partie réellement nouvelle étant le chapitre V.

(1) voir aussi la thèse de 3ème cycle de Patrick Billot (Orsay 1984).

Notations.

Si M est un ensemble fini, on note $\#(M)$ son cardinal.

Si L est un sous-$\mathbb{Z}_p$-module de L' d'indice fini, on note $[L' : L]$ cet indice.

Si F'/F est une extension finie, on note $N_{F'/F}$ la norme de F' sur F et $tr_{F'/F}$ la trace.

Si F'/F est une extension galoisienne, $G(F'/F)$ désigne le groupe de Galois de F' sur F.

Si M est un $\mathbb{Z}_p$-module, on note $\hat{M}$ son dual de Pontryagin : $\hat{M} = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

Si A est un anneau commutatif intègre unitaire et a et b deux éléments de A, le symbole $a \sim b$ signifie que $a = ub$ avec u unité de A; si M est un A-module, M_a désigne le noyau de la multiplication par a sur M et $M(a)$ est la réunion des M_{a^n} pour $n \in \mathbb{N}$; l'expression "M est un A-module de torsion" signifie que M est un A-module de A-torsion.

Si M est un $\mathbb{Z}_p$-module et G un groupe opérant sur M, M_G désigne le plus grand $\mathbb{Z}_p$-module quotient de M sur lequel G opère trivialement et M^G le plus grand sous $\mathbb{Z}_p$-module de M sur lequel G opère trivialement. Le dual de Pontryagin $\hat{M}$ est muni de l'action de G suivante

$$(g\phi)(m) = \phi(g^{-1}m)$$

pour $g \in G$, $\phi \in \hat{M}$, $m \in M$.

Chapitre I. Généralités sur les Λ-modules.

Soit Λ un anneau local régulier complet de dimension r et de corps résiduel fini de caractéristique p. Tous les Λ-modules considérés dans ce paragraphe sont supposés compacts et de type fini. Ils sont caractérisés de la manière suivante : si m est l'idéal maximal de Λ, un Λ-module compact M est de type fini si et seulement si M/mM est fini.

1. Généralités ([5]).

1.1. Définitions.

Si $\mathfrak{q}$ est un idéal premier, le localisé $\Lambda_{\mathfrak{q}}$ de Λ en $\mathfrak{q}$ est défini comme le sous-anneau du corps des fractions de Λ formé des éléments x/y avec x et y appartenant à Λ et y n'appartenant pas à $\mathfrak{q}$. Le localisé $M_{\mathfrak{q}}$ d'un Λ-module M est $M \otimes_{\Lambda} \Lambda_{\mathfrak{q}}$. On peut de même définir le localisé d'un homomorphisme de Λ-modules. Un Λ-module est dit pseudo-nul si son localisé en tout idéal premier de hauteur 1 est nul. Cela est équivalent à ce qu'il est annulé par deux éléments de Λ premiers entre eux. Un homomorphisme de Λ-modules est dit pseudo-isomorphisme si son localisé en tout idéal premier de hauteur 1 est un isomorphisme. Cela est équivalent à ce que son noyau et conoyau sont pseudo-nuls. Un Λ-module sans torsion est dit réflexif si il est égal à l'intersection de ses localisés en tout idéal premier de hauteur 1 (les localisés étant plongés dans l'espace vectoriel engendré par le Λ-module sur le corps de fractions de Λ).

Exemple 1. Si $r = 1$, les modules pseudo-nuls sont nuls; si r est égal à 1 ou 2, les Λ-modules réflexifs sont les Λ-modules libres.

1.2. Théorème de structure.

Les Λ-modules compacts de type fini sont caractérisés à pseudo-isomorphisme près par le théorème de structure bien connu suivant.

Théorème 1. (i) *Si M est un Λ-module compact de type fini sans torsion, il existe un homomorphisme injectif de M dans un Λ-module réflexif dont le conoyau est pseudo-nul et déterminé à isomorphisme près par M.*

(ii) *Si M est un Λ-module compact de type fini de Λ-torsion, il existe un unique Λ-module de la forme*

$$E(M) = \bigoplus_{i=1}^{s} \Lambda/\mathfrak{q}_i^{e_i}$$

(où les $\mathfrak{q}_i$ sont des idéaux premiers de hauteur 1 et où les e_i sont des entiers positifs) pseudo-isomorphe à M.

Les modules de la forme E(M) sont appelés élémentaires. Soit f_i un générateur de $\mathfrak{q}_i$. L'élément

$$f_M = \prod_{i=1}^{s} f_i^{e_i}$$

est appelé série caractéristique de M. Il est défini à une unité près de Λ. La notation $f \sim g$ pour f et g appartenant à Λ signifiera que f/g est une unité de Λ. Remarquons que, si M n'admet pas de sous-Λ-modules pseudo-nuls non nuls, f_M appartient à l'annulateur de M. La série caractéristique dépend multiplicativement de M, c'est-à-dire que si l'on a une suite exacte de Λ-modules de torsion

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0,$$

alors $f_M \cdot f_{M''} \sim f_{M'}$.

1.3. Modules de torsion.

Soit $\mathfrak{q}$ un idéal de hauteur 1. Si M est un Λ-module compact de type fini, $M/\mathfrak{q}M$ est un $\Lambda/\mathfrak{q}$-module de type fini. Si de plus M est de Λ-torsion et que $\mathfrak{q}$ est premier à la série caractéristique f_M de M, alors $M/\mathfrak{q}M$ est un $\Lambda/\mathfrak{q}$-module de torsion. Réciproquement, on a le lemme suivant.

Lemme 2. Si $M/\mathfrak{q}M$ est un $\Lambda/\mathfrak{q}$-module de torsion, alors M est un Λ-module de torsion.

Démonstration. On remarque d'abord que si X est un Λ-module sans Λ-torsion de rang d, il s'injecte dans un Λ-module libre de rang d et l'on peut choisir cette injection de manière à ce que le conoyau ait un annulateur premier à $\mathfrak{q}$:

$$0 \longrightarrow X \longrightarrow \Lambda^d \longrightarrow Y \longrightarrow 0$$

On en déduit la suite exacte

$$0 \longrightarrow X/\mathfrak{q}X \longrightarrow (\Lambda/\mathfrak{q})^d \longrightarrow Y/\mathfrak{q}Y \longrightarrow 0 .$$

Le Λ/q-module Y/qY est de Λ/q-torsion et le rang du Λ/q-module X/qX est donc égal à celui du Λ-module X. Revenons au Λ-module M du lemme. Si d est son rang sur Λ, on a la suite exacte

$$0 \longrightarrow T \longrightarrow M \longrightarrow X \longrightarrow 0$$

où X est un Λ-module sans torsion et de Λ-rang d et où T est le sous-module de torsion maximal de M. On en déduit de nouveau la suite exacte de Λ/q-modules

$$0 \longrightarrow T/qT \longrightarrow M/qM \longrightarrow X/qX \longrightarrow 0 .$$

Le rang du Λ/q-module M/qM est donc supérieur à celui du Λ-module M. D'où le lemme.

Donnons maintenant un exemple fondamental d'anneau Λ.

Soit Θ un $\mathbb{Z}_p$-module isomorphe à $\mathbb{Z}_p^{r-1}$. Définissons $\mathbb{Z}_p[[\Theta]]$ comme la limite projective des algèbres de groupe $\mathbb{Z}_p[\Theta/U]$ pour U sous-groupe ouvert de Θ (donc d'indice fini dans Θ). C'est un anneau local régulier de dimension r isomorphe non canoniquement à l'algèbre des séries formelles à $r-1$ variables à coefficients dans $\mathbb{Z}_p$. Un tel isomorphisme correspond à la donnée d'une base $\gamma = (\gamma_1,\ldots,\gamma_{r-1})$ du $\mathbb{Z}_p$-module libre Θ:

$$\gamma_i \longrightarrow 1 + T_i .$$

C'est dans ce cadre que le terme de "série caractéristique" prend sa signification. Nous n'utiliserons en fait cet anneau que pour $r = 1$, 2 ou 3. On posera quelquefois $\Lambda_\Theta = \mathbb{Z}_p[[\Theta]]$.

Lemme 3. Supposons $r = 2$ (c'est-à-dire Θ isomorphe à $\mathbb{Z}_p$). Posons $\omega_n = \gamma^{p^n} - 1$ si γ est un générateur topologique de Θ. Alors, M est un Λ-module de torsion si et seulement si $M/\omega_n M$ est de $\mathbb{Z}_p$-rang borné par rapport à n.

Pour la démonstration, voir [17] .

Supposons maintenant $r \geq 2$. Soit H un sous-groupe de Θ tel que Θ/H soit isomorphe à $\mathbb{Z}_p^{r-2}$ (si r est égal à 2, H est donc nécessairement égal à Θ). Notons $\Lambda_{\Theta/H}$ l'anneau $\mathbb{Z}_p[[\Theta/H]]$ et

$$\pi_H : \Lambda \longrightarrow \Lambda_{\Theta/H}$$

la projection canonique. Si M est un Λ-module, soit M_H (resp. M^H) le plus grand quotient (resp. sous-module) de M sur lequel H agit trivialement. Le $\Lambda_{\Theta/H}$-module M_H est aussi isomorphe canoniquement à $M \underset{\Lambda}{\otimes} \Lambda_{\Theta/H}$.

Lemme 4. Soient M un Λ-module de torsion et f sa série caractéristique.

1. Le $\Lambda_{\Theta/H}$-module M_H est de torsion si et seulement si $\pi_H(f)$ est non nul, ce qui est encore équivalent à f premier à $h-1$ où h est un générateur topologique de H.

2. Si M_H est de $\Lambda_{\Theta/H}$-torsion, M^H est un Λ-module pseudo-nul et un $\Lambda_{\Theta/H}$-module de torsion. Si f_{M^H} (resp. f_{M_H}) désigne alors la série caractéristique de M^H (resp. M_H) en tant que $\Lambda_{\Theta/H}$-module, on a

$$\pi_H(f) \sim f_{M_H}/f_{M^H} . \tag{1}$$

Remarque. Dans le cas où r est égal à 2, cela redonne un résultat classique : par exemple, si M_Θ est fini, alors

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

Démonstration. La partie 1 et le début de la partie 2 se vérifient facilement. Pour montrer (1), supposons d'abord que M est pseudo-nul. Alors, il existe un sous-groupe H' de Θ tel que $\Theta/H' \simeq \mathbb{Z}_p$ et $\Theta = H \oplus H'$ et tel que M soit un $\Lambda_{H'}$-module de type fini et de torsion. On a alors la suite exacte de $\Lambda_{H'}$-modules de torsion

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

D'où l'égalité des séries caractéristiques de M_H et de M^H en tant que $\Lambda_{H'}$-modules et donc de f_{M^H} et de f_{M_H} puisque H agit trivialement sur M_H et sur M^H. Comme $\pi_H(f)$ est une unité lorsque M est pseudo-nul, on en déduit que (1) est vérifié dans ce cas. On montre ensuite que (1) est vrai 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.

Remarque. Supposons $r = 3$ et soient $\gamma = (\gamma_1, \gamma_2)$ une base de Θ et $(\gamma) : \Lambda \longrightarrow \mathbb{Z}_p[[T_1, T_2]]$ l'isomorphisme associé. A un générateur h de H, on peut associer le générateur τ_h de Θ/H vérifiant

$$\tau_h^{-b} \equiv \gamma_1 \mod H$$

$$\tau_h^{a} \equiv \gamma_2 \mod H$$

si $h = \gamma_1^a \gamma_2^b$. Alors, l'homomorphisme

$$\psi_{\gamma,h} : \mathbb{Z}_p[[T_1,T_2]] \longrightarrow \mathbb{Z}_p[[T]]$$

$$T_1 \longmapsto (1+T)^{-b} - 1$$

$$T_2 \longmapsto (1+T)^{a} - 1$$

fait commuter le diagramme

$$\begin{array}{ccc} \Lambda & \xrightarrow{\pi_H} & \Lambda_{\Theta/H} \\ {\scriptstyle (\gamma)}\downarrow & & \downarrow{\scriptstyle (\tau_h)} \\ \mathbb{Z}_p[[T_1,T_2]] & \xrightarrow{\psi_{\gamma,h}} & \mathbb{Z}_p[[T]] \end{array} .$$

D'autre part, les éléments de Λ peuvent aussi s'interpréter comme fonctions du groupe des caractères de Θ dans $\mathbb{Z}_p^\times$. En effet, soit ρ un caractère de Θ dans $\mathbb{Z}_p^\times$. Il s'étend en une fonction de Λ dans $\mathbb{Z}_p$ que l'on notera de la même manière. A un élément f de Λ, on peut alors associer la fonction f' du groupe des caractères de Θ dans $\mathbb{Z}_p^\times$ définie de la manière suivante

$$f'(\rho) = \rho(f) = ((\gamma)f)(\rho(\gamma_1) - 1, \rho(\gamma_2) - 1).$$

Maintenant, si ρ est un caractère de Θ se factorisant par H, on a simplement

$$\pi_H(f)(\rho) = f'(\rho).$$

2. Adjoint.

2.1. Dimension projective ([33], [6]).

Rappelons que l'on appelle dimension projective (appelée dimension homologique dans [33] et notée $dh_\Lambda(M)$) d'un Λ-module M de type fini la borne supérieure $dp_\Lambda(M)$ des entiers p tels que $\mathrm{Ext}^p_\Lambda(M,N)$ est non nul pour au moins un Λ-module N de type fini. Par exemple, comme Λ est un anneau local, $dp_\Lambda(M)$ est nul si et seulement si M est libre.

Lemme 5. *Si M n'a pas de Λ-sous-module pseudo-nul non nul, alors $dp_\Lambda(M) = dp_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M)$ pour presque tout idéal premier $\mathfrak{q}$ de hauteur 1 tel que $\Lambda/\mathfrak{q}$ soit régulier.*

Avant de démontrer le lemme 5, rappelons les faits importants suivants. On appelle M-suite régulière toute suite $\{a_1,\dots,a_p\}$ d'éléments de l'idéal maximal de Λ telle que pour tout i, a_i n'est pas diviseur de 0 dans $M/(a_0,\dots,a_{i-1})M$ (on pose $a_0 = 0$). On montre que toutes les M-suites régulières maximales ont le même nombre d'éléments que l'on note $\mathrm{cod}\, h_\Lambda(M)$ et que l'on appelle codimension homologique de M. Ici, Λ est un anneau local régulier; on a donc la relation

$$dp_\Lambda(M) + \mathrm{cod}\, h_\Lambda(M) = r$$

([33], IV- A-4, IV- D-1).

Démonstration du lemme 5. Soit $\mathfrak{q} = (g)$ un idéal premier de hauteur 1 tel que $\Lambda/\mathfrak{q}$ soit régulier. Supposons-le premier à la série caractéristique de M. Alors, la multiplication par g est injective sur M. On en déduit en revenant à la définition de la codimension homologique que .

$$\mathrm{cod}\, h_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M) = \mathrm{cod}\, h_\Lambda(M) - 1 \ .$$

Comme la dimension de $\Lambda/\mathfrak{q}$ est $r-1$, on en déduit que $dp_\Lambda(M)$ est égal à $dp_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M)$.

Proposition 6 (Oesterlé). *Les conditions suivantes sont équivalentes :*

(i) $dp_\Lambda(M) \leq 1$;

(ii) *M n'a pas de sous-module pseudo-nul non nul et il existe une*

infinité d'idéaux premiers $\mathfrak{q}$ de hauteur 1 tels que $\Lambda/\mathfrak{q}$ soit régulier et qu'on ait $dp_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M) \leq 1$;

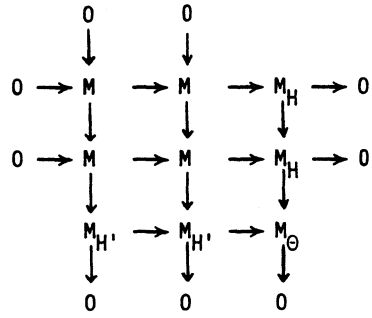
(iii) M n'a pas de sous-module pseudo-nul non nul et pour presque tout idéal premier $\mathfrak{q}$ de hauteur 1 tel que $\Lambda/\mathfrak{q}$ soit régulier, on a $dp_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M) \leq 1$.

Démonstration. La hauteur des idéaux premiers associés à M est majorée par $dp_\Lambda(M)$ ([33], p. 80). Donc, si $dp_\Lambda(M)$ est inférieure à 1, M n'a pas de sous-module pseudo-nul non nul. La proposition résulte alors du lemme 5.

Notons encore le lemme suivant dans le cas où Λ est de la forme $\mathbb{Z}_p[[\Theta]]$. Il sera utilisé dans la démonstration du théorème II.25.

Lemme 7. Supposons que $\Lambda = \mathbb{Z}_p[[\Theta]]$ et que M est un Λ-module de torsion, sans Λ-modules pseudo-nuls non nuls. Soient H et H' deux sous-groupes de Θ tels que $\Theta/H \simeq \Theta/H' \simeq \mathbb{Z}_p$ et tels que M_H (resp. $M_{H'}$) soit un $\Lambda_{\Theta/H}$-(resp. $\Lambda_{\Theta/H'}$-)module de torsion. Alors, $(M_H)^{\Theta/H}$ et $(M_{H'})^{\Theta/H'}$ sont des $\mathbb{Z}_p$-modules isomorphes.

Démonstration. On suppose d'abord que H et H' engendrent topologiquement Θ. Les hypothèses faites impliquent que M^H et $M^{H'}$ sont pseudo-nuls donc nuls. On a alors le diagramme commutatif exact suivant



Par le lemme du serpent, on en déduit que le noyau de $M_H \longrightarrow M_H$ est isomorphe au noyau de $M_{H'} \longrightarrow M_{H'}$, d'où l'isomorphisme $(M_H)^{\Theta/H} \simeq (M_{H'})^{\Theta/H'}$. Si H et H' n'engendrent pas topologiquement Θ, il suffit d'introduire un troisième sous-groupe.

2.2. Adjoint.

On suppose désormais que tous les Λ-modules considérés sont de Λ-torsion. On appelle adjoint de M le Λ-module compact de type fini et de torsion

$$a_\Lambda(M) = \mathrm{Ext}^1_\Lambda(M,\Lambda).$$

De manière générale, si A est un anneau et M un A-module, on pose

$$a_A(M) = \mathrm{Ext}^1_A(M,A).$$

L'importance de cette notion ici est que les équations fonctionnelles sur les fonctions L p-adiques algébriques que nous définirons plus loin proviennent d'un pseudo-isomorphisme entre un certain module d'Iwasawa et une forme tordue de son adjoint. Nous construirons au chapitre V un tel pseudo-isomorphisme canonique qui contiendra toutes les informations arithmétiques dont nous avons besoin ici.

Proposition 8. L'adjoint de M vérifie les propriétés suivantes :

(i) si M est pseudo-nul, $a_\Lambda(M)$ est nul;

(ii) l'adjoint $a_\Lambda(M)$ de M n'a pas de sous-Λ-modules pseudo-nuls non nuls;

(iii) il est pseudo-isomorphe à M.

Démonstration. (i) Si $a_\Lambda(M)$ est nul, il en est de même de $a_\Lambda(M')$ pour tout quotient M' de M. Comme tout module pseudo-nul est un quotient de sommes directes de modules du type $\Lambda/\mathfrak{a}$ où $\mathfrak{a}$ est un idéal de hauteur supérieure à 2, il suffit de montrer que $a_\Lambda(\Lambda/\mathfrak{a})$ est nul pour un tel idéal $\mathfrak{a}$. Mais $a_\Lambda(\Lambda/\mathfrak{a})$ peut se calculer grâce à la suite exacte suivante

$$0 \longrightarrow \mathrm{Hom}_\Lambda(\Lambda,\Lambda) \longrightarrow \mathrm{Hom}_\Lambda(\mathfrak{a},\Lambda) \longrightarrow a_\Lambda(\Lambda/\mathfrak{a}) \longrightarrow 0 .$$

Un Λ-homomorphisme de $\mathfrak{a}$ dans Λ est la multiplication par un élément f du corps de fractions de Λ vérifiant $f\mathfrak{a} \subset \Lambda$. Pour tout idéal premier $\mathfrak{q}$ de hauteur 1, le localisé de $\mathfrak{a}$ en $\mathfrak{q}$ est $\Lambda_\mathfrak{q}$. Donc f appartient à l'intersection des $\Lambda_\mathfrak{q}$ pour tout idéal premier $\mathfrak{q}$ de hauteur 1, il appartient donc à Λ et $a_\Lambda(\Lambda/\mathfrak{a})$ est nul.

(ii) et (iii) Considérons d'abord le cas où M est de la forme

$\Lambda/(f)$ avec f appartenant à Λ. De la suite exacte

$$0 \longrightarrow \Lambda \xrightarrow{f} \Lambda \longrightarrow \Lambda/(f) \longrightarrow 0 ,$$

on déduit la suite exacte

$$\mathrm{Hom}_\Lambda(\Lambda,\Lambda) \xrightarrow{f} \mathrm{Hom}_\Lambda(\Lambda,\Lambda) \longrightarrow \mathrm{Ext}^1_\Lambda(\Lambda/(f),\Lambda) \longrightarrow 0 .$$

En utilisant un isomorphisme entre Λ et $\mathrm{Hom}_\Lambda(\Lambda,\Lambda)$, on en déduit que $a_\Lambda(\Lambda/(f))$ est isomorphe à $\Lambda/(f)$.

Si maintenant M est quelconque, il existe un homomorphisme injectif de $E(M)$ dans M de conoyau pseudo-nul D. On a alors la suite exacte

$$0 \longrightarrow a_\Lambda(D) \longrightarrow a_\Lambda(M) \longrightarrow a_\Lambda(E(M)) \longrightarrow \mathrm{Ext}^2_\Lambda(D,\Lambda).$$

Comme $a_\Lambda(D)$ est nul d'après (i) et que $\mathrm{Ext}^2_\Lambda(D,\Lambda)$ est pseudo-nul, (ii) et (iii) s'en déduisent facilement.

Exemples. Si $\Lambda = \mathbb{Z}_p[G]$ où G est un groupe fini et si M est un $\mathbb{Z}_p[G]$-module fini, $a_\Lambda(M)$ est le dual de Pontryagin de M muni de la structure de Λ-module donnée par

$$(\lambda\phi)(m) = \phi(\lambda m)$$

comme on le voit en utilisant la suite exacte

$$0 \longrightarrow \mathbb{Z}_p[G] \longrightarrow \mathbb{Q}_p[G] \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p[G] \longrightarrow 0$$

et l'isomorphisme canonique

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(M, \mathbb{Q}_p/\mathbb{Z}_p[G]) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) .$$

2.3. Propriétés et calculs d'adjoint.

Nous allons ici donner quelques lemmes permettant de comparer des adjoints calculés pour divers anneaux.

Lemme 9. Soit Λ' un anneau contenant Λ et plat sur Λ. Si M est un Λ-module, on a l'isomorphisme canonique

$$a_\Lambda(M) \underset{\Lambda'}{\otimes} \Lambda \xrightarrow{\simeq} a_{\Lambda'}(M \underset{\Lambda}{\otimes} \Lambda') .$$

(démonstration dans [33], IV-31, proposition 18).

Par exemple, si R est un anneau qui est en même temps un $\mathbb{Z}_p$-module libre de dimension finie, $\Lambda' = R[[\Theta]]$ est plat sur $\Lambda_\Theta = \mathbb{Z}_p[[\Theta]]$. En particulier, l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$ convient.

Dans les lemmes qui suivent, on supposera toujours que $\mathfrak{q}$ est un idéal premier de hauteur 1 et que M est un Λ-module de torsion tel que $M/\mathfrak{q}M$ soit de $\Lambda/\mathfrak{q}$-torsion.

Lemme 10. On a l'isomorphisme

$$a_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M) \xrightarrow{\simeq} \mathrm{Ext}^1_\Lambda(M,\Lambda/\mathfrak{q}) .$$

Démonstration. Soit

$$0 \longrightarrow L' \longrightarrow L \longrightarrow M \longrightarrow 0$$

une présentation de M avec L module libre sur Λ. Soit L'' le noyau de

$$L/\mathfrak{q}L \longrightarrow M/\mathfrak{q}M .$$

Comme $M_\mathfrak{q}$ est de $\Lambda/\mathfrak{q}$-torsion, on a

$$\mathrm{Hom}_{\Lambda/\mathfrak{q}}(L'',\Lambda/\mathfrak{q}) = \mathrm{Hom}_{\Lambda/\mathfrak{q}}(L'/\mathfrak{q}L',\Lambda/\mathfrak{q}) .$$

D'autre part, pour tout Λ-module R, on a l'isomorphisme

$$\mathrm{Hom}_\Lambda(R,\Lambda/\mathfrak{q}) \xrightarrow{\simeq} \mathrm{Hom}_{\Lambda/\mathfrak{q}}(R/\mathfrak{q}R,\Lambda/\mathfrak{q}).$$

De plus, $L/\mathfrak{q}L$ est libre sur $\Lambda/\mathfrak{q}$. On en déduit le diagramme commutatif exact suivant et l'isomorphisme voulu :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_\Lambda(L,\Lambda/\mathfrak{q}) & \longrightarrow & \mathrm{Hom}_\Lambda(L',\Lambda/\mathfrak{q}) & \longrightarrow & \mathrm{Ext}^1_\Lambda(M,\Lambda/\mathfrak{q}) & \longrightarrow & 0 \\
 & & \downarrow \wr & & \downarrow \wr & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_{\Lambda/\mathfrak{q}}(L/\mathfrak{q}L,\Lambda/\mathfrak{q}) & \longrightarrow & \mathrm{Hom}_{\Lambda/\mathfrak{q}}(L'/\mathfrak{q}L',\Lambda/\mathfrak{q}) & \longrightarrow & a_{\Lambda/\mathfrak{q}}(M) & \longrightarrow & 0
\end{array}$$

Lemme 11. Si de plus M est un Λ-module pseudo-nul, il existe un isomorphisme

$$a_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M) \xrightarrow{\simeq} \mathrm{Ext}^2_\Lambda(M,\Lambda)_\mathfrak{q} ,$$

dépendant du choix d'un générateur de $\mathfrak{q}$.

Démonstration. Soit f un générateur de $\mathfrak{q}$. De la suite exacte

$$0 \longrightarrow \Lambda \xrightarrow{f} \Lambda \longrightarrow \Lambda/\mathfrak{q} \longrightarrow 0 ,$$

on déduit la suite exacte

$$\mathrm{Ext}^1_\Lambda(M,\Lambda) \longrightarrow \mathrm{Ext}^1_\Lambda(M,\Lambda/\mathfrak{q}) \longrightarrow \mathrm{Ext}^2_\Lambda(M,\Lambda)_{\mathfrak{q}} \longrightarrow 0$$

Comme M est pseudo-nul, le premier module est nul. Le lemme 11 se déduit alors du lemme 10.

Proposition 12. Soit M un Λ-module de torsion sans Λ-sous-modules pseudo-nuls non nuls. On suppose que $M/\mathfrak{q}M$ est de $\Lambda/\mathfrak{q}$-torsion. Alors $a_\Lambda(M)/\mathfrak{q}a_\Lambda(M)$ s'injecte dans $a_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M)$ avec un conoyau pseudo-nul. Si de plus $dp_\Lambda(M) \leq 1$, c'est un isomorphisme.

Démonstration. De la suite exacte

$$0 \longrightarrow \Lambda \longrightarrow \Lambda \longrightarrow \Lambda/\mathfrak{q} \longrightarrow 0 ,$$

on déduit la suite exacte

$$0 \longrightarrow a_\Lambda(M)/\mathfrak{q}a_\Lambda(M) \longrightarrow \mathrm{Ext}^1_\Lambda(M,\Lambda/\mathfrak{q}) \longrightarrow \mathrm{Ext}^2_\Lambda(M,\Lambda) .$$

Le second module est isomorphe à $a_{\Lambda/\mathfrak{q}}(M/\mathfrak{q})$ d'après le lemme 10. Si M n'a pas de sous Λ-modules pseudo-nuls non nuls, le calcul des séries caractéristiques montre que $a_\Lambda(M)/\mathfrak{q}a_\Lambda(M)$ et $a_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M)$ ont même série caractéristique en tant que $\Lambda/\mathfrak{q}$-modules. On en déduit que le conoyau de

$$a_\Lambda(M)/\mathfrak{q}a_\Lambda(M) \longrightarrow a_{\Lambda/\mathfrak{q}}(M/\mathfrak{q}M)$$

est pseudo-nul. Si de plus M est de dimension projective inférieure ou égale à 1, le Λ-module $\mathrm{Ext}^2_\Lambda(M,\Lambda)$ est nul. D'où la dernière affirmation de la proposition.

Corollaire 13. Soit M un Λ-module de torsion de dimension projective inférieure ou égale à 1. Soit $(\mathfrak{q}_i)$ une suite d'idéaux emboîtés premiers à la série caractéristique de M. Alors, on a l'isomorphisme

$$a_\Lambda(M) = \varprojlim a_{\Lambda/q_i}(M/q_iM).$$

Cela redonne un moyen de calcul de l'adjoint montré par Iwasawa dans le cas où $\Lambda = \Lambda_{\mathbb{Z}_p}$. Plus précisément, si M est un Λ_Θ-module, notons $\dot{M}$ le Λ_Θ-module dont le $\mathbb{Z}_p$-module sous-jacent est M et sur lequel Θ opère par

$$\theta \cdot m = \theta^{-1}m.$$

Alors, dans le cas particulier $\Lambda = \Lambda_{\mathbb{Z}_p}$, on a

$$\dot{a}_\Lambda(M) = \varprojlim \widehat{(M/q_iM)}.$$

Revenons d'autre part au lemme 11. Supposons $\Lambda = \Lambda_\Theta$ avec Θ isomorphe à $\mathbb{Z}_p^2$ et soit M un $\mathbb{Z}_p$-module de type fini sur lequel Θ agit trivialement. Il est donc pseudo-nul. Soit h un élément de Θ engendrant topologiquement un sous-groupe H de Θ tel que $\Theta/H \simeq \mathbb{Z}_p$ et τ un générateur topologique de Θ/H. On peut alors attacher au couple (h,τ) un isomorphisme

$$\mathrm{Hom}_{\mathbb{Z}_p}(M,\mathbb{Z}_p) \longrightarrow \mathrm{Ext}^2_\Lambda(M,\Lambda)$$

déduit des deux suites exactes

$$0 \longrightarrow \Lambda \xrightarrow{h-1} \Lambda \longrightarrow \Lambda_{\Theta/H} \longrightarrow 0$$

$$0 \longrightarrow \Lambda_{\Theta/H} \xrightarrow{\tau-1} \Lambda_{\Theta/H} \longrightarrow \mathbb{Z}_p \longrightarrow 0 .$$

Nous en aurons besoin dans le chapitre V.

2.4. Dualité.

Proposition 14. *Soit M un Λ-module compact de type fini et de Λ-torsion. Il existe un homomorphisme naturel de Λ-modules*

$$M \longrightarrow a_\Lambda(a_\Lambda(M))$$

qui est un isomorphisme dès que la dimension projective de M est inférieure ou égale à 1.

Démonstration. Si L est un Λ-module, on pose

$$\beta_\Lambda(L) = \mathrm{Hom}_\Lambda(\mathrm{Hom}_\Lambda(L,\Lambda),\Lambda).$$

L'homomorphisme cherché se déduit du Λ-homomorphisme canonique $L \longrightarrow \beta_\Lambda(L)$ (qui est un isomorphisme dès que L est libre sur Λ) de la manière suivante : soit

$$0 \longrightarrow L' \longrightarrow L \longrightarrow M \longrightarrow 0$$

une présentation de M avec L module libre. On en déduit les suites exactes

$$0 \longrightarrow \mathrm{Hom}_\Lambda(L,\Lambda) \longrightarrow \mathrm{Hom}_\Lambda(L',\Lambda) \longrightarrow a_\Lambda(M) \longrightarrow 0$$

puis

$$(2) \quad 0 \longrightarrow \beta_\Lambda(L') \longrightarrow \beta_\Lambda(L) \longrightarrow a_\Lambda(a_\Lambda(M)) \longrightarrow \mathrm{Ext}^1_\Lambda(\mathrm{Hom}_\Lambda(L;\Lambda),\Lambda).$$

Les Λ-homomorphismes $L \longrightarrow \beta_\Lambda(L)$ et $L' \longrightarrow \beta_\Lambda(L')$ induisent un Λ-homomorphisme

$$M \longrightarrow a_\Lambda(a_\Lambda(M)) \ .$$

Lorsque la dimension projective de M est inférieure à 1, celle de L' est nulle. Donc L' est libre et le dernier module de la suite exacte (2) est nul. Les Λ-homomorphismes $L \longrightarrow \beta_\Lambda(L)$ et $L' \longrightarrow \beta_\Lambda(L')$ sont des isomorphismes; il en est donc de même du Λ-homomorphisme

$$M \longrightarrow a_\Lambda(a_\Lambda(M)).$$

Chapitre II. Arithmétique des courbes elliptiques et théorie d'Iwasawa.

1. Généralités.

1.1. Notations.

Les notations introduites ici seront utilisées dans tout le reste du texte.

Soient K un corps quadratique imaginaire d'anneau des entiers $\mathcal{O}$ et F une extension finie de $\mathbb{Q}$. Fixons une clôture algébrique $\bar{F}$ de F. Considérons une courbe elliptique E définie sur F et ayant multiplication complexe par l'anneau des entiers $\mathcal{O}$ de K, ce qui veut dire que l'anneau $\mathrm{End}_F(E)$ des endomorphismes de E définis sur F est isomorphe à $\mathcal{O}$. Cet anneau est alors aussi égal à l'anneau des endomorphismes de E définis sur $\bar{F}$ et on l'identifie à $\mathcal{O}$. L'action de $\mathcal{O}$ sur l'espace des formes différentielles invariantes de E définies sur F fixe un plongement i de K dans F de la manière suivante : si α est un endomorphisme de E et ω une forme différentielle invariante de E définie sur F, $\alpha^*\omega = i(\alpha)\omega$. On supposera désormais K contenu dans F de cette manière.

Si L est une extension algébrique de F, le groupe des points de $E(\bar{F})$ rationnels sur L est noté $E(L)$. Si B est un $G(\bar{F}/L)$-module discret, $H^i(L,B)$ désigne le groupe de cohomologie de $G(\bar{F}/L)$ agissant sur B. De plus, si B est le groupe $E(\bar{F})$, on notera ce groupe $H^i(L,E)$. Si L est une extension de $\mathbb{Q}$ non nécessairement finie et si v est une place non archimédienne de L, on définit L_v comme la réunion des complétés en v des extensions finies de $\mathbb{Q}$ contenues dans L; on note $\tilde{L}_v$ le corps résiduel de L_v en v et Nv le cardinal de $\tilde{L}_v$ si celui-ci est fini. On désigne par v_L la valuation associée à v et vérifiant $v_L(L^\times) = \mathbb{Z}$ lorsque L est une extension finie de $\mathbb{Q}$. On note $\tilde{E}_v$ la courbe réduite en v et $E_{1,v}$ le noyau de l'homomorphisme de réduction modulo v.

Si α appartient à $\mathcal{O}$, on écrira E_α pour le groupe $E(\bar{F})_\alpha$ des points de $E(\bar{F})$ annulés par α. Pour tout idéal entier $\mathfrak{h}$ de $\mathcal{O}$, on notera $E_\mathfrak{h}$ l'intersection des E_α pour $\alpha \in \mathfrak{h}$. On pose

$$E_{\mathfrak{h}^\infty} = E(\bar{F})(\mathfrak{h}) = \bigcup_{n \in \mathbb{N}} E_{\mathfrak{h}^n}.$$

Si M est un $\mathcal{O}$-module, on note $T_\alpha(M)$ la limite projective des M_{α^n},

les applications de transition étant données par la multiplication par α. On posera

$$T_\alpha(E) = T_\alpha(E(\bar{F})) = T_\alpha(E_{\alpha^\infty}) .$$

On le notera même T_α lorsqu'il n'y a pas d'ambiguité.

Si M est un sous-ensemble de $E(\bar{F})$ et L une extension de F, $L(M)$ désigne le plus petit sous-corps de $\bar{F}$ tel que les éléments de M soient contenus dans $E(L(M))$.

On choisit désormais un nombre premier p impair se décomposant dans K en deux idéaux distincts $\mathfrak{p}$ et $\mathfrak{p}^*$ et tel que E a bonne réduction en toute place de F au dessus de p. La courbe E a donc bonne réduction ordinaire au dessus de p, c'est-à-dire que le noyau de réduction $E_{1,v}$ est un groupe formel de hauteur 1. On choisit un élément π de $\mathcal{O}$ divisible uniquement par $\mathfrak{p}$: $(\pi) = \mathfrak{p}^h$ $(h \geq 1)$. Si α est un élément de K, son conjugué sur $\mathbb{Q}$ est noté α^* et sa norme $N(\alpha)$. La norme $N(\alpha)$ est aussi le degré de l'endomorphisme α agissant sur la courbe elliptique E. On pose $q = \pi\pi^* = N(\pi)$. On note $i_\mathfrak{p}$ l'isomorphisme topologique du complété $K_\mathfrak{p}$ de K en $\mathfrak{p}$ avec $\mathbb{Q}_p$. Si M est un $\mathcal{O}$-module, on considère $M \underset{\mathcal{O}}{\bullet} \mathcal{O}_\mathfrak{p}$ comme un $\mathbb{Z}_p$-module à travers $i_\mathfrak{p}$. On considère de même l'isomorphisme $i_{\mathfrak{p}^*}$ de $K_{\mathfrak{p}^*}$ avec $\mathbb{Q}_p$. La conjugaison complexe $\alpha \longrightarrow \alpha^*$ sur K induit un isomorphisme de $K_\mathfrak{p}$ sur $K_{\mathfrak{p}^*}$ noté de la même manière et on a $i_{\mathfrak{p}^*}(x^*) = i_\mathfrak{p}(x)$ pour $x \in K_\mathfrak{p}$.

Notons F_∞ le corps obtenu en rajoutant à F la composante p-primaire E_{p^∞} de $E(\bar{F})$, N_∞ (resp. N_∞^*) le corps obtenu en rajoutant à F la composante $\mathfrak{p}$-primaire (resp. $\mathfrak{p}^*$-primaire) de $E(\bar{F})$:

$$F_\infty = F(E_{p^\infty}), \quad N_\infty = F(E_{\mathfrak{p}^\infty}), \quad N_\infty^* = F(E_{\mathfrak{p}^{*\infty}}) .$$

Nous verrons plus loin que la courbe E ayant bonne réduction partout sur $F(E_p)$, $F(E_\mathfrak{p})$ et $F(E_{\mathfrak{p}^*})$, l'extension $F_\infty/F(E_p)$ est non ramifiée en dehors de p, l'extension $N_\infty/F(E_\mathfrak{p})$ en dehors de $\mathfrak{p}$. On peut en fait montrer que F_∞ (resp. N_∞) est le composé de $F(E_p)$ (resp. $F(E_\mathfrak{p})$) avec l'unique extension de K non ramifiée en dehors de p (resp. de $\mathfrak{p}$) et de groupe de Galois topologiquement isomorphe à $\mathbb{Z}_p^2$ (resp. $\mathbb{Z}_p$). Toute place de F au dessus de $\mathfrak{p}$ (resp. de $\mathfrak{p}^*$) se ramifie donc dans

N_∞ (resp. N_∞^*). On note F_∞ l'unique $\mathbb{Z}_p^2$-extension de F contenue dans F_∞ et N_∞ (resp. N_∞^*) l'unique $\mathbb{Z}_p$-extension de F contenue dans N_∞ (resp. N_∞^*).

L'action de $G_\infty = G(F_\infty/F)$ sur $T_p(E)$ définit un homomorphisme ρ_p de G_∞ dans $\mathrm{Aut}_{\mathcal{O}}(T_p(E))$ de conoyau fini. Il admet comme directions propres $T_\pi(E)$ et $T_{\pi^*}(E)$. On note $\rho_\mathfrak{p}$ et $\rho_{\mathfrak{p}^*}$ les homomorphismes correspondants

$$\rho_\mathfrak{p} : G_\infty \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_\pi(E)) = \mathcal{O}_\mathfrak{p} \xrightarrow{i_\mathfrak{p}} \mathbb{Z}_p$$

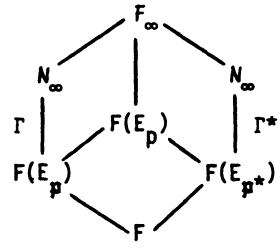
$$\rho_{\mathfrak{p}^*} : G_\infty \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_{\pi^*}(E)) = \mathcal{O}_{\mathfrak{p}^*} \xrightarrow{i_{\mathfrak{p}^*}} \mathbb{Z}_p .$$

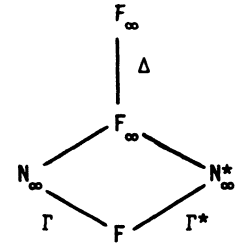
En particulier, le groupe de Galois $\Delta = G(F(E_p)/F)$ qui est canoniquement isomorphe à $G(F_\infty/F_\infty)$ est donc produit de deux sous-groupes cycliques, chacun d'ordre divisant $p-1$. Notons χ (resp. χ^*) la restriction de $\rho_\mathfrak{p}$ (resp. $\rho_{\mathfrak{p}^*}$) à Δ. Tout $\mathbb{Z}_p[\Delta]$-module M se décompose en somme directe de sous-espaces propres correspondant aux caractères $\chi^i\chi^{*j}$. Si ψ est un tel caractère, on note $M^{(\psi)}$ le sous-module maximal de M sur lequel Δ agit à travers ψ. Le caractère κ (resp. κ^*) défini par $\kappa = \rho_\mathfrak{p}\chi^{-1}$ (resp. $\kappa^* = \rho_{\mathfrak{p}^*}\chi^{*-1}$) se factorise par $G(N_\infty/F)$ (resp. par $G(N_\infty^*/F)$). On pose

$$\Theta = G(F_\infty/F(E_p)).$$

Ce groupe de Galois est produit direct de $\Gamma = G(N_\infty/F(E_\mathfrak{p}))$ et de $\Gamma^* = G(N_\infty^*/F(E_{\mathfrak{p}^*}))$. Le groupe Θ sera aussi considéré comme le groupe de Galois de F_∞/F. On convient de prolonger un élément γ de Γ à F_∞ par $\gamma(x) = x$ si $x \in F(E_{\mathfrak{p}^*})$ et de faire de manière identique pour les éléments de Γ^*.

Récapitulons les corps définis par les diagrammes suivants :





1.2. Théorie de la multiplication complexe.

Nous allons rappeler ici quelques résultats bien connus relatifs à la multiplication complexe. Soient L une extension finie de F et $R(L)$ l'ensemble des places de L de mauvaise réduction pour E.

a. Les résultats suivants portent sur les points de torsion de E et sur la division de points par un endomorphisme de E.

(1) Soit v une place de L de bonne réduction et α un élément de O premier à v; l'homomorphisme de réduction

$$E(L_v) \longrightarrow \tilde{E}_v(\tilde{L}_v)$$

est injectif sur $E(L_v)_\alpha$ et le noyau de la réduction $E_{1,v}(L_v)$ est uniquement divisible par α.

(2) Soit a un idéal de O; l'extension $L(E_a)/L$ est abélienne et non ramifiée au dehors de $R(L)$ et des places de L divisant a.

(3) Supposons que E_α est contenu dans $E(L)$; pour tout point P de $E(L)$, soit Q un élément de $E(\bar{F})$ tel que $\alpha Q = P$. Le corps $L(Q)$ ne dépend pas du choix de Q; c'est une extension abélienne de L non ramifiée au dehors de $R(L)$ et des places de L divisant α.

b. Faisons maintenant quelques rappels concernant le Grössencharakter ψ_L attaché à la courbe elliptique E sur L. Son existence a été montrée par Deuring. Soit v une place finie de L qui n'est pas dans $R(L)$. Alors, on montre qu'il existe un unique élément de O (que l'on note $\psi_L(v)$) dont la réduction modulo v en tant qu'endomorphisme est l'endomorphisme de Frobenius sur $\tilde{E}_v(\tilde{L}_v)$. Il vérifie

$$(4) \qquad (1 - \psi_L(v))(1 - \psi_L(v)^*) = \#(\tilde{E}_v(\tilde{L}_v)) \ .$$

On définit alors par multiplicativité un homomorphisme ψ_L du groupe des idéaux fractionnaires de L premiers à $R(L)$ dans $K^\times$. On montre de plus que l'idéal engendré par la norme sur K de v est principal et engendré par $\psi_L(v)$. En particulier, on en déduit que F contient le corps de Hilbert de K et que la norme de tout idéal de F sur K est principal.

En fait, ψ_L est un Grössencharakter de L au sens de Hecke c'est-à-dire qu'il existe un idéal f de L divisible uniquement par les pla-

ces de mauvaise réduction de $R(L)$ tel que, pour tout élément β de L vérifiant $\beta \equiv 1 \bmod^{\times} \mathfrak{f}$, on a

$$\psi_L((\beta)) = N_{L/K}(\beta).$$

Le plus petit idéal $\mathfrak{f}$ convenant est appelé conducteur de ψ_L.

On peut aussi interpréter ψ_L comme donnant l'action du symbole d'Artin de v sur les points d'ordre fini : précisemment, si $\mathfrak{a}$ est un idéal entier de K et $\mathfrak{h}$ un idéal de L premier aux places de $R(L)$ et à $\mathfrak{a}$, pour tout point P de $E_{\mathfrak{a}}$, on a

$$(\mathfrak{h},L(E_{\mathfrak{a}})/L)(P) = \psi_L(\mathfrak{h})P \tag{5}$$

où $(\mathfrak{h},L(E_{\mathfrak{a}})/L)$ désigne le symbole d'Artin de $\mathfrak{h}$ pour l'extension abélienne $L(E_{\mathfrak{a}})/L$.

Le comportement du Grössencharakter par extension des scalaires est le suivant : si L'/L est une extension finie,

$$\psi_L \circ N_{L'/L} = \psi_{L'}.$$

La courbe elliptique E ayant multiplication complexe a bonne réduction potentielle partout. On peut montrer qu'elle a en fait bonne réduction partout sur le corps $F(E_{\mathfrak{p}})$ en utilisant le critère de Néron-Ogg-Shafarevitch et le caractère de Serre-Tate ε_L dont nous allons maintenant expliquer le lien avec le Grössencharakter ψ_L ([34]). Soit I_L le groupe des idèles de L. Il existe un unique homomorphisme ε_L de I_L dans $K^{\times}$ vérifiant les trois conditions suivantes

1 - ε_L est continu, c'est-à-dire que son noyau est ouvert dans I_L;

2 - $\varepsilon_L(\alpha) = N_{L/K}(\alpha)$ pour tout $\alpha \in L^{\times}$;

3 - si x est un élément de I_L tel que $x_v = 1$ pour toute place v appartenant à $R(L)$ et pour toute place infinie, on a

$$\varepsilon_L(x) = \prod_{\substack{v \notin R(L) \\ v \text{ finie}}} \psi_L(v)^{v_L(x)}.$$

A partir de l'homomorphisme ε_L, on obtient les représentations p-adiques attachées à la courbe elliptique E/L de la manière suivante. Soit $\mathfrak{q}$ une place finie de K; on note $L_{\mathfrak{q}}$ le produit des complétés

de L aux places de L divisant $\mathfrak{q}$ c'est-à-dire $L_{\mathfrak{q}} = L \otimes_K K_{\mathfrak{q}}$ et $N_{\mathfrak{q}}$ la norme de $L_{\mathfrak{q}}$ dans $K_{\mathfrak{q}}$ induite par le produit des normes locales; si x appartient à I_L, $x_{\mathfrak{q}}$ désigne l'image de x dans $L_{\mathfrak{q}}$ par la projection naturelle. Posons alors

$$\varepsilon_{\mathfrak{q}}(x) = \varepsilon_L(x) N_{\mathfrak{q}}(x_{\mathfrak{q}})^{-1} .$$

Cela définit un homomorphisme de I_L dans $K_{\mathfrak{q}}^{\times}$ trivial sur $L^{\times}$. Composé avec l'homomorphisme d'Artin de la théorie du corps de classes global, il détermine l'action de $G(\bar{L}/L)$ sur $E_{\mathfrak{q}^{\infty}}$ et se factorise par $G(L(E_{\mathfrak{q}^{\infty}})/L)$. Par exemple, si L est F et si $\mathfrak{q}$ est égal à $\mathfrak{p}$, on retrouve l'homomorphisme $\rho_{\mathfrak{p}}$ de G_{∞} défini précédemment.

Exemples 1. Considérons la $\mathbb{Q}$-courbe $A(\ell)$ définie par Gross dans [15] pour un nombre premier ℓ différent de 2 et 3 et congru à 3 modulo 4. Elle est à multiplication complexe par $\mathbb{Q}(\sqrt{-\ell})$, est définie sur le corps de Hilbert H de $\mathbb{Q}(\sqrt{-\ell})$ et même sur son sous-corps totalement réel et est isogène à toutes ses conjuguées sur $\mathbb{Q}$. La courbe $A(\ell)$ a mauvaise réduction uniquement en ℓ. Par exemple, un modèle de $A(\ell)$ pour $\ell = 7$ et 11 est donné par :

$$A(7) : y^2 + xy = x^3 - x^2 - 2x - 1$$

$$A(11) : y^2 + xy = x^3 - x^2 - 7x + 10 .$$

Soit ε le caractère de $(O/\sqrt{-\ell}\,O)^{\times}$ dans $\{\pm 1\}$ composé de l'inverse de l'isomorphisme

$$(\mathbb{Z}/\ell\mathbb{Z})^{\times} \longrightarrow (O/\sqrt{-\ell}\,O)^{\times}$$

avec le caractère quadratique associé à l'extension $\mathbb{Q}(\sqrt{-\ell})/\mathbb{Q}$:

$$\varepsilon(a + b\sqrt{-\ell}) = \left(\frac{a}{\ell}\right)$$

où $\left(\frac{a}{\ell}\right)$ est le symbole de Legendre $(a \in \frac{1}{2}\mathbb{Z})$. Pour toute place v de H première à ℓ, $\psi_H(v)$ est le générateur de $N_{H/K}(v)$ qui est dans le noyau de ε. Le conducteur de ψ_H est l'idéal de H engendré par $\sqrt{-\ell}$.

Par exemple, calculons le nombre de points de la réduction de $A(59)$ en une place de H au dessus de 3 et 5. Ces deux nombres pre-

miers sont décomposés dans $\mathbb{Q}(\sqrt{-59})$. Le nombre de classes de $\mathbb{Q}(\sqrt{-59})$ est 3. Les idéaux de $\mathbb{Q}(\sqrt{-59})$ au dessus de 3 et 5 ne sont pas principaux car les équations $a^2+59b^2 = 12$ (ou 20) n'ont pas de solutions entières. Il n'y a donc qu'un seul idéal au dessus de chacun d'eux dans H. Des équations

$$27 = N_{K/\mathbb{Q}}\left(\frac{7+\sqrt{-59}}{2}\right)$$

$$125 = N_{K/\mathbb{Q}}\left(\frac{21+\sqrt{-59}}{2}\right),$$

on déduit que pour l'un des deux idéaux $\mathfrak{q}_3$ (resp. $\mathfrak{q}_5$) de H au dessus de 3 (resp. 5), on a

$$\psi_H(\mathfrak{q}_3) = \frac{7+\sqrt{-59}}{2}$$

$$\psi_H(\mathfrak{q}_5) = \frac{21+\sqrt{-59}}{2}$$

On en déduit que $\#(\widetilde{A(59)}(\mathbf{F}_{27})) = 21$

$$\#(\widetilde{A(59)}(\mathbf{F}_{125})) = 105$$

si $\mathbf{F}_q$ désigne le corps fini à q éléments.

Donnons ici trois lemmes qui nous seront utiles par la suite.

Lemme 1. Soit L une extension finie de F. Pour toute place v de L^* divisant $\mathfrak{p}$, l'homomorphisme de réduction induit un isomorphisme

$$E(L_v)(\mathfrak{p}^*) \xrightarrow{\simeq} \tilde{E}_v(\tilde{L}_v)(p),$$

et on a $$\#(\tilde{E}_v(\tilde{L}_v)) \sim i_{\mathfrak{p}}\left(1-\frac{\psi_L(v)}{Nv}\right).$$

Démonstration. Ce lemme précise (1) qui affirme que l'homomorphisme de réduction est injectif sur $E(L)(\mathfrak{p}^*)$. Il suffit donc de montrer l'égalité des cardinaux de $E(L)(\mathfrak{p}^*)$ et de $\tilde{E}_v(\tilde{L}_v)(p)$. Le groupe $E_{\mathfrak{p}^{*m}}$ est isomorphe en tant que O-module à $O/\mathfrak{p}^{*m}$. Donc la propriété (5) du Grössencharakter montre que $E_{\mathfrak{p}^{*m}}$ est contenu dans $E(L_v)$ si et seulement si $\psi_L(v)$ est congru à 1 modulo $\mathfrak{p}^{*m}$. Le cardinal de $E(L)(\mathfrak{p}^*)$ est donc égal (à une unité de $O_{\mathfrak{p}}$ près) à $1-\psi_L(v)^*$. Il en est de même de

celui de $\tilde{E}_v(\tilde{L}_v)(p)$ grâce à la relation (4) et au fait que $\psi_L(v)$ appartient à $\mathfrak{p}$. La dernière affirmation du lemme 1 se déduit alors simplement de

$$\psi_L(v)\psi_L(v)^* = Nv.$$

Lemme 2. Soit L une $\mathbb{Z}_p$-extension d'une extension finie L de F, ne contenant pas N_∞^*. Alors, si v est une place de L au dessus de $\mathfrak{p}$, $E(L_v)(\mathfrak{p}^*)$ est fini.

Démonstration. On peut supposer pour la démonstration que $E(L)$ contient E_p. Le corps L ne contient pas N_∞^*; donc v se ramifie dans L (sinon LN_∞^* serait non ramifié en v sur L). La place v est alors totalement ramifiée dans L/L_n pour n assez grand si L_n désigne le sous-corps de L fixé par $G(L/L)^{p^n}$. Le corps résiduel $\tilde{L}_v$ de L en v est donc fini et $E(L_v)(\mathfrak{p}^*)$ étant plongé dans $\tilde{E}_v(\tilde{L}_v)(p)$ est lui aussi fini.

Lemme 3. Il n'y a qu'un nombre fini de places au dessus de p dans F_∞.

Démonstration. Supposons qu'il y ait une infinité de places au dessus de $\mathfrak{p}$, par exemple, dans F_∞. Alors, il existerait une extension finie L de F et une place v de L se décomposant totalement dans F_∞. On en déduirait que $E(L_v)(\mathfrak{p}^*)$ serait infini, ce qui est impossible.

1.3. Groupes de Mordell-Weil.

Par le théorème de Mordell et Weil, le groupe de Mordell-Weil $E(L)$ des points de E rationnels sur un corps de nombres L contenant F est un $\mathbb{Z}$-module de type fini. Dans le cas où L est une $\mathbb{Z}_p$-extension de F, cela n'est plus toujours vrai ([18], [20], [16]). Cependant, des résultats de finitude du rang de $E(L)$ pour certaines $\mathbb{Z}_p$-extensions ont été donnés par Greenberg ([3]) et par Rubin et Wiles ([30]). Nous montrerons nous-mêmes quelques résultats dans cette direction au chapitre V. De toute façon, il ne peut y avoir de parties indéfiniment divisibles dans $E(L)$ à part la partie de torsion. On notera $\Omega(L)$ le sous-groupe de torsion de $E(L)$.

Théorème 4. Pour toute $\mathbb{Z}_p$-extension L_∞ de F, le groupe abélien $E(L_\infty)/\Omega(L_\infty)$ est libre. Il en est de même de $E(F_\infty)/\Omega(F_\infty)$.

Nous ne démontrerons le théorème que pour l'extension F_∞, le cas

d'une $\mathbb{Z}_p$-extension se faisant de même. Démontrons d'abord deux lemmes.

Lemme 5. *Soient Θ un $\mathbb{Z}_p$-module isomorphe à $\mathbb{Z}_p^r$ et Y un Θ-module sans $\mathbb{Z}$-torsion. Si Θ' est un sous-groupe de Θ, le quotient $Y/Y^{\Theta'}$ est sans torsion.*

Démonstration. Supposons qu'il existe un élément y de Y et $m \in \mathbb{Z}$ tels que my appartient à $Y^{\Theta'}$. On a alors

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

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

Rappelons que l'on a noté Θ le groupe de Galois de F_∞/F.

Lemme 6. *Le groupe de cohomologie $H^1(\Theta,\Omega(F_\infty))$ est fini.*

Démonstration. Montrons d'abord que la composante $\Omega(F_\infty)'(p)$ d'ordre premier à p de $\Omega(F_\infty)$ est finie. L'extension F_∞/F est non ramifiée au dehors de p. Mais, si ℓ est premier à p, l'extension $F(E_\ell)/F$ est non ramifiée en p car E/F a bonne réduction aux places divisant p. Donc $F(\Omega(F_\infty)'(p))$ est une extension abélienne non ramifiée de F. Elle est donc finie sur F et le groupe $\Omega(F_\infty)'(p)$ est nécessairement fini. Montrons maintenant que $H^1(\Theta,E(F_\infty)(\mathfrak{p}))$ est fini (la composante $\mathfrak{p}$*-primaire de $H^1(\Theta,\Omega(F_\infty))$ se traiterait de la même manière). Si F ne contient pas $E_\mathfrak{p}$, $E(F_\infty)(\mathfrak{p})$ est nul et la finitude est triviale; sinon $E(F_\infty)(\mathfrak{p})$ est égal à $E_{\mathfrak{p}^\infty}$. Soit m l'entier tel que $E_{\mathfrak{p}^\infty}^{\Theta} = E_{\mathfrak{p}^m}$. On a la suite exacte d'inflation-restriction :

$$0 \longrightarrow H^1(F(E_{\mathfrak{p}^{*\infty}})/F, E_{\mathfrak{p}^m}) \longrightarrow H^1(\Theta, E_{\mathfrak{p}^\infty}) \longrightarrow H^1(F_\infty/F(E_{\mathfrak{p}^{*\infty}}), E_{\mathfrak{p}^\infty}) .$$

Le dernier groupe est nul (voir par exemple le lemme 15 qui suit). Quant au premier groupe, il est fini d'ordre p^m. Cela termine la démonstration du lemme.

Passons à la démonstration du théorème 4. Posons $\Theta_n = \Theta^{p^n}$ et soit F_n le sous-corps de F_∞ fixé par Θ_n. Posons encore $Y_n = E(F_n)/\Omega(F_n)$ et $Y_\infty = E(F_\infty)/\Omega(F_\infty)$. De la suite exacte

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

on déduit la suite exacte de cohomologie

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

D'après le théorème de Mordell-Weil, Y_n est un groupe abélien de type fini. Comme $H^1(\Theta_n, \Omega(F_\infty))$ est fini d'après le lemme 6 appliqué au corps de base F_n, $Y_\infty^{\Theta_n}$ est un groupe abélien de type fini qui est de plus sans torsion donc libre. D'autre part, $Y_\infty^{\Theta_m}/Y_\infty^{\Theta_n}$ est sans torsion $(m \geq n)$. Donc $Y_\infty^{\Theta_n}$ est facteur direct dans $Y_\infty^{\Theta_m}$. Il existe des $\mathbb{Z}$-modules libres R_n tels que

$$Y_\infty^{\Theta_{n+1}} = Y_\infty^{\Theta_n} \oplus R_n .$$

On a donc

$$Y_\infty^{\Theta_n} = \bigoplus_{i=0}^{n-1} R_i$$

et Y_∞ qui est la limite inductive des $Y_\infty^{\Theta_n}$ est libre.

Remarque. Dans le cas où p est inerte dans K au lieu d'être décomposé, le théorème 4 reste vrai pour $E(F_\infty)/\Omega(F_\infty)$.

1.4. Descente et groupes de Selmer.

Soit L une extension de F, non nécessairement finie. Pour tout élément α de $\mathcal{O}$, la suite de $G(\bar{F}/L)$-modules

$$0 \longrightarrow E_\alpha \longrightarrow E(\bar{F}) \xrightarrow{\alpha} E(\bar{F}) \longrightarrow 0$$

est exacte de même que la suite de cohomologie qui s'en déduit

$$(6) \qquad 0 \longrightarrow E(L)/\alpha E(L) \longrightarrow H^1(L, E_\alpha) \longrightarrow H^1(L,E)_\alpha \longrightarrow 0.$$

Le groupe de Shafarevitch-Tate $Ш(L)$ de E sur L est défini comme l'intersection des noyaux des homomorphismes de restriction

$$H^1(L,E) \longrightarrow H^1(L_v, E)$$

pour toute place v finie c'est-à-dire qu'il vérifie la suite exacte

$$0 \longrightarrow Ш(L) \longrightarrow H^1(L,E) \longrightarrow \prod_v H^1(L_v, E).$$

Le groupe de Selmer $S(L)^{(\alpha)}$ relatif à E/L et à α est alors l'image réciproque de $Ш(L)_\alpha$ dans $H^1(L,E_\alpha)$. C'est donc le noyau de l'homomorphisme naturel

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

et on a la suite exacte

$$0 \longrightarrow E(L)/\alpha E(L) \longrightarrow S(L)^{(\alpha)} \longrightarrow Ш(L)_\alpha \longrightarrow 0 .$$

Deux autres types de groupes de Selmer joueront un rôle important. Soit d'abord $S'(L)^{(\alpha)}$ le noyau de

$$H^1(L,E_\alpha) \longrightarrow \prod_{v \nmid \alpha} H^1(L_v,E)$$

où le produit est pris sur les places v de L premières à α. Le groupe $S(L)^{(\alpha)}$ est un sous-groupe de $S'(L)^{(\alpha)}$. L'autre groupe que l'on notera $\Sigma(L)^{(\alpha)}$ est lui un sous-groupe de $S(L)^{(\alpha)}$. Par définition du groupe de Selmer $S(L)^{(\alpha)}$, l'image par restriction d'un élément de $S(L)^{(\alpha)}$ dans $H^1(L_v,E_\alpha)$ est en fait dans $E(L_v)/\alpha E(L_v)$ grâce à la suite exacte locale analogue à (6) :

$$(7) \qquad 0 \longrightarrow E(L_v)/\alpha E(L_v) \longrightarrow H^1(L_v,E_\alpha) \longrightarrow H^1(L_v,E)_\alpha \longrightarrow 0.$$

On note $\Sigma(L)^{(\alpha)}$ le noyau de l'homomorphisme

$$S(L)^{(\alpha)} \longrightarrow \prod_{v \mid \alpha^*} E(L_v)/\alpha E(L_v) .$$

On n'utilisera ici ces groupes que pour $\alpha = \pi^n$ ou π^{*n}. Les inclusions $E_{\alpha^n} \longrightarrow E_{\alpha^{n+1}}$ induisent des applications sur tous ces groupes. On note leur limite inductive $S(L)$, $S'(L)$, $\Sigma(L)$ pour $\alpha = \pi$ et $S^*(L)$, $S'^*(L)$, $\Sigma^*(L)$ pour $\alpha = \pi^*$. De même, la multiplication par $\alpha : E_{\alpha^{n+1}} \longrightarrow E_{\alpha^n}$ induit des applications sur les groupes de Selmer. On notera leur limite projective $\overset{\vee}{S}(L)$, $\overset{\vee}{S}'(L)$, $\overset{\vee}{\Sigma}(L)$ pour $\alpha = \pi$ et $\overset{\vee}{S}^*(L)$, $\overset{\vee}{S}'^*(L)$, $\overset{\vee}{\Sigma}^*(L)$ pour $\alpha = \pi^*$. On pose $D_\mathfrak{p} = K_\mathfrak{p}/O_\mathfrak{p}$. Les suites suivantes sont exactes :

$$0 \longrightarrow E(L) \bullet_{0} D_{\mathfrak{p}} \longrightarrow S(L) \longrightarrow Ш(L)(\mathfrak{p}) \longrightarrow 0$$

$$0 \longrightarrow E(L) \bullet_{0} O_{\mathfrak{p}^*} \longrightarrow \overset{\vee}{S}{}^*(L) \longrightarrow T_{\pi^*}(Ш(L)) \longrightarrow 0$$

(en général, on distingue une place $\mathfrak{p}$ et l'on n'écrit pas les suites exactes de manière symétrique en $\mathfrak{p}$ et $\mathfrak{p}^*$). On notera encore $Y(L)$ (resp. $Y^*(L)$) le dual de Pontryagin de $S(L)$ (resp. $S^*(L)$).

Enfin, notons $E_1(L)$ le noyau du produit des homomorphismes de réduction

$$E(L) \longrightarrow \tilde{E}_v(\tilde{L}_v)$$

sur les places v divisant $\mathfrak{p}$ (lorsqu'on voudra être plus précis, on le notera $E_{1,\mathfrak{p}}(L)$).

Pourquoi introduire ces différentes versions du groupe de Selmer ? Le groupe $S(L)^{(\pi^n)}$ est le groupe de Selmer classique. Cependant, le groupe $S'(L)^{(\pi^n)}$ obtenu en oubliant les places au dessus de $\mathfrak{p}$ est plus facile à calculer et s'interprète en termes de groupe de Galois lorsque E_{π^n} est contenu dans $E(L)$ car le groupe E_{π^n} est étale en toutes les places de L différentes de $\mathfrak{p}$. Le groupe $\Sigma(L)^{(\pi^{*n})}$ jouera un rôle très important pour nous et intervient naturellement dans la suite exacte fondamentale (chapitre IV). Par dualité de Cassels, il apparait lorsqu'on cherche à calculer l'indice de $S(L)^{(\pi^n)}$ dans $S'(L)^{(\pi^n)}$.

Dans le paragraphe suivant, on comparera les indices de $\overset{\vee}{\Sigma}{}^*(L)$ dans $\overset{\vee}{S}{}^*(L)$ et de $S(L)$ dans $S'(L)$ dans le cas où L est une extension <u>finie</u>. Dans le paragraphe 1.6, on étudie les rapports entre les trois groupes de Selmer dans le cas d'une extension <u>infinie</u>. Enfin dans le paragraphe 1.7, on comparera les groupes de Selmer relatifs à 2 corps différents.

1.5. <u>Comparaison des groupes de Selmer relatifs à une extension finie</u>.

On suppose donc dans ce paragraphe que L est une extension finie de F. Nous allons comparer $S(L)$ et $S'(L)$, $\overset{\vee}{\Sigma}{}^*(L)$ et $\overset{\vee}{S}{}^*(L)$.

Notons $Ш_1(L)^{(\pi^{*n})}$ l'image de $\Sigma(L)^{(\pi^{*n})}$ dans $Ш(L)$ et $\overset{\vee}{Ш}{}^*_1(L)$ la limite projective des $Ш_1(L)^{(\pi^{*n})}$. Alors, on a le lemme suivant.

Lemme 7. Le groupe $\overset{v}{\Sigma}{}^*(L)$ est d'indice fini dans $\overset{v}{S}{}^*(L)$. La suite

$$0 \longrightarrow E_1(L) \underset{O}{\otimes} O_{\mathfrak{p}^*} \longrightarrow \overset{v}{\Sigma}{}^*(L) \longrightarrow \overset{v}{Ш}{}^*_1(L) \longrightarrow 0$$

est exacte et on a l'égalité d'indices

$$[\overset{v}{S}{}^*(L) : \overset{v}{\Sigma}{}^*(L)] = [E(L) \underset{O}{\otimes} O_{\mathfrak{p}^*} : E_1(L) \underset{O}{\otimes} O_{\mathfrak{p}^*}][T_{\pi^*}(Ш(L)) : \overset{v}{Ш}{}^*_1(L)].$$

Démonstration. Si v est une place au dessus de $\mathfrak{p}$, π^* induit un automorphisme sur $E_{1,v}(L_v)$. On en déduit que $E(L_v)/\pi^{*n}E(L_v)$ est isomorphe à $\tilde{E}_v(\tilde{L}_v)/\pi^{*n}\tilde{E}_v(\tilde{L}_v)$ et que $E(L_v) \underset{O}{\otimes} O_{\mathfrak{p}^*}$ est isomorphe à la composante p-primaire de $\tilde{E}_v(\tilde{L}_v)$. On montre alors facilement les suites exactes

$$0 \longrightarrow \overset{v}{\Sigma}{}^*(L) \longrightarrow \overset{v}{S}{}^*(L) \longrightarrow \prod_{v|\mathfrak{p}} \tilde{E}_v(\tilde{L}_v)(p) ,$$

$$0 \longrightarrow E_1(L) \underset{O}{\otimes} O_{\mathfrak{p}^*} \longrightarrow E(L) \underset{O}{\otimes} O_{\mathfrak{p}^*} \longrightarrow \prod_{v|\mathfrak{p}} \tilde{E}_v(\tilde{L}_v)(p) ,$$

$$0 \longrightarrow \Sigma^*(L) \longrightarrow S^*(L) \longrightarrow \prod_{v|\mathfrak{p}} \tilde{E}_v(\tilde{L}_v)(p)$$

(la dernière suite exacte ne servira pas pour le lemme mais sera utile par la suite). Comme $\tilde{E}_v(\tilde{L}_v)$ est fini, $\overset{v}{\Sigma}{}^*(L)$ est d'indice fini dans $\overset{v}{S}{}^*(L)$ (et même d'indice divisant $\prod_{v|\mathfrak{p}} \#(\tilde{E}_v(\tilde{L}_v)(p))$). Par définition de $\overset{v}{Ш}{}^*_1(L)$, on a le diagramme commutatif suivant :

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \\
 & & \overset{v}{Ш}{}^*_1(L) & \longrightarrow & T_{\pi^*}(Ш(L)) & & \\
 & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \overset{v}{\Sigma}{}^*(L) & \longrightarrow & \overset{v}{S}{}^*(L) & \longrightarrow & \prod_{v|\mathfrak{p}} \tilde{E}_v(\tilde{L}_v)(p) \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & E_1(F) \underset{O}{\otimes} O_{\mathfrak{p}^*} & \longrightarrow & E(F) \underset{O}{\otimes} O_{\mathfrak{p}^*} & \longrightarrow & \prod_{v|\mathfrak{p}} \tilde{E}_v(\tilde{L}_v)(p) \\
 & & & & \uparrow & & \uparrow \\
 & & & & 0 & & 0
\end{array}$$

D'où la suite exacte du lemme 7 et l'égalité d'indices par application du lemme du serpent.

L'étude de la comparaison de $S(L)$ et de $S'(L)$ est très liée à celle de $\overset{\vee}{S}{}^*(L)$ et de $\overset{\vee}{\Sigma}{}^*(L)$ grâce à un théorème de Cassels. Afin de ne pas alourdir le texte, nous nous contenterons d'énoncer ici les résultats qui se déduisent de ce théorème et de démontrer celui-ci en annexe.

Soit $B(L)$ le conoyau de l'homomorphisme canonique

$$S'(L) \longrightarrow \prod_{v|\mathfrak{p}} H^1(L_v,E)(\mathfrak{p}).$$

On a donc la suite exacte

$$0 \longrightarrow S(L) \longrightarrow S'(L) \longrightarrow \prod_{v|\mathfrak{p}} H^1(L_v,E)(\mathfrak{p}) \longrightarrow B(L) \longrightarrow 0 .$$

Proposition 8. Le dual de Pontryagin de $B(L)$ est isomorphe canoniquement à l'image de $\overset{\vee}{S}{}^*(L)$ dans $\prod_{v|\mathfrak{p}} E(L_v) \otimes_{O} O_{\mathfrak{p}^*}$. On a donc l'égalité d'indices

$$[\overset{\vee}{S}{}^*(L) : \overset{\vee}{\Sigma}{}^*(L)][S'(L) : S(L)] = \prod_{v|\mathfrak{p}} \#(\tilde{E}_v(\tilde{L}_v)(p)) .$$

Remarquons que lorsque $\tilde{E}_v(\tilde{L}_v)$ est d'ordre premier à p pour toute place v divisant $\mathfrak{p}$, $S'(L)$ et $S(L)$ sont égaux (il en est en fait de même de $S(L)^{(\pi^n)}$ et $S'(L)^{(\pi^n)}$) et $\overset{\vee}{S}{}^*(L)$ et $\overset{\vee}{\Sigma}{}^*(L)$ sont égaux. Lorsque $\tilde{E}_v(\tilde{L}_v)$ est d'ordre divisible par p, les groupes $S(L)$ et $S'(L)$ peuvent aussi bien être égaux que différents.

Exemples 2. Considérons les courbes E définies sur $\mathbb{Q}$ et à multiplication complexe par $\mathbb{Q}(i)$ d'équation

$$y^2 = x^3 - dx$$

où d est un entier non divisible par une puissance quatrième. Prenons comme nombre premier $p = 5$ et pour π, $2+i$. Alors, $\pi = 2+i$ est non anormal (c'est-à-dire que $\tilde{E}_5(\mathbb{F}_5)$ est d'ordre premier à 5) si et seulement si d n'est pas congru à 2 modulo 8 (on suppose bien sûr que 5 ne divise pas d afin que E ait bonne réduction en 5).

Le point $P = (-1,1)$ appartient à la courbe $y^2 = x^3 - 2x$. Comme P n'appartient pas à $E_1(K) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}$, l'indice de $\check{\Sigma}^*(K)$ dans $\check{S}^*(K)$ est divisible par 5. Donc $S(K)$ et $S'(K)$ sont égaux. Par contre, considérons la courbe $y^2 = x^3 - 2662x$. Elle contient le point $P = (-50,90)$. Comme $2P$ appartient à $E_1(K)$, P appartient à $E_1(K) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}$. Mais le point P n'est pas divisible par 5 (ou par $\pi = 2+i$) dans $E(K)$ ou dans $E(\mathbb{Q})$: il suffit pour le voir d'écrire les formules de multiplication par $2+i$. On aurait

$$50 = -a\,\frac{(a^2 + 2662(2i-1))^2}{((2+i)a^2 - 2662i)^2} \quad \text{avec} \quad a \in \mathbb{Z}[i] \ ,$$

ce qui impliquerait que π divise a et que π^3 divise 50, ce qui est impossible. On en déduit que si $Ш(K)(5)$ est fini, $\check{S}^*(K)$ et $\check{\Sigma}^*(K)$ sont égaux et que l'indice de $S(K)$ dans $S'(K)$ est égal à 5.

1.6. Comparaison des groupes de Selmer relatifs à une extension infinie.

Lemme 9. *Si L_∞ est une $\mathbb{Z}_p$-extension de F différente de N_∞^* ou si L_∞ est égale à F_∞, $S(L_\infty)$ et $S'(L_\infty)$ sont égaux.*

Démonstration. Il suffit de démontrer que le groupe $H^1(L_{\infty,v},E)(\mathfrak{p})$ est nul pour toute place v de L_{∞_n} au dessus de $\mathfrak{p}$. Soit L_n le sous-corps de L_∞ fixé par $G(L_\infty/F)^{p^n}$ et soit $L_{n,v}$ le complété de L_n pour la restriction de v à L_n. Comme par définition $L_{\infty,v}$ est égal à la réunion des $L_{n,v}$ pour $n \geq 1$, $H^1(L_{\infty,v},E)$ est la limite inductive des $H^1(L_{n,v},E)$ relativement aux applications restriction. Par la dualité locale de Tate ([35]), 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'homomorphisme de restriction est l'homomorphisme de norme. Il suffit donc de montrer que

$$\varprojlim \bar{E}\,(L_{n,v}) \tag{8}$$

est nul, où la limite projective est prise relativement aux applications normes. Or, on a les isomorphismes

$$\bar{E}(L_{n,v}) \xrightarrow{\simeq} \tilde{E}_v(\tilde{L}_{n,v})(p) \xrightarrow{\simeq} E_{\mathfrak{p}^{*\infty}}(L_{n,v})$$

pour une place au dessus de $\mathfrak{p}$. Dans le cas où L_∞ est une $\mathbb{Z}_p$-extension différente de N_∞^*, $\tilde{E}(L_{n,v})$ est un groupe fini d'ordre borné sur lequel le groupe de Galois de $L_{\infty,v}$ sur $L_{n,v}$ agit donc trivialement pour n assez grand. La limite projective (8) est donc nulle. Dans le cas où L_∞ est égale à F_∞, $\tilde{E}(L_{n-1,v})$ est d'indice au plus p dans $\tilde{E}(L_{n,v})$ et la norme de l'extension L_n/L_{n-1} agit par multiplication par p^2 sur $\tilde{E}(L_{n,v})$ pour n assez grand. On en déduit facilement que (8) 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. C'est ce que nous allons étudier maintenant.

Introduisons d'abord 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 $\mathbb{Z}_p[[G_v]]$-module; on pose

$$\mathrm{Ind}_v^G(M) = M \otimes_{\mathbb{Z}_p[[G_v]]} \mathbb{Z}_p[[G]] ,$$

muni de sa structure naturelle de $\mathbb{Z}_p[[G]]$-module. On rappelle d'autre part que le dual de Pontryagin d'un $\mathbb{Z}_p$-module M est noté $\hat{M}$.

Lemme 10. 1. *Il existe un $G(N_\infty^*/F)$-module U_∞ dont le dual de Pontryagin est isomorphe à*

$$\prod_{v|\mathfrak{p}} \mathrm{Ind}_v^{G(N_\infty^*/F)} T_{\pi^*}(E(N_{\infty,v}^*))$$

(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

$$0 \longrightarrow S(N_\infty^*) \longrightarrow S'(N_\infty^*) \longrightarrow U_\infty \; ; \tag{9}$$

2. *Si l'on suppose de plus que le dual de Pontryagin de $S^*(N_\infty^*)$ est un $\mathbb{Z}_p[[G(N_\infty^*/F)]]$-module de torsion, le dual de Pontryagin du conoyau de $S'(N_\infty^*) \longrightarrow U_\infty$ est isomorphe à $T_{\pi^*}(E)$, c'est-à-dire que l'on a la suite exacte*

$$0 \to T_{\pi^*}(E(N_\infty^*)) \to \prod_{v|\mathfrak{p}} \mathrm{Ind}_v^{G(N_\infty^*/F)} T_{\pi^*}(E(N_{\infty,v}^*)) \to \widehat{S'(N_\infty^*)} \to \widehat{S(N_\infty^*)} \to 0 .$$

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 (9) et le dual de Pontryagin 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_v 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 9 montre à l'aide du lemme 1 que M_v est égal à $T_{\pi^*}(E(N_{\infty,v}^*))$, ce qui donne le résultat 1.

De plus, par la proposition 8, on peut identifier le dual du conoyau $B(N_n^*)$ de l'homomorphisme

$$S'(N_n^*) \longrightarrow \prod_{v|\mathfrak{p}} H^1(N_{n,v}^*,E)(\mathfrak{p})$$

avec l'image de $\overset{v}{S}{}^*(N_n^*)$ dans $\prod_{v|\mathfrak{p}} E(N_{n,v}^*) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*}$ (où N_n^* est ici le corps fixé par $G(N_\infty^*/F)^{p^n}$). L'hypothèse que $\widehat{S^*(N_\infty^*)}$ est un $\mathbb{Z}_p[[G(N_\infty^*/F)]]$-module de torsion implique que les $\mathbb{Z}_p$-rangs de $\widehat{E(N_n^*) \underset{\mathcal{O}}{\otimes} D_{\mathfrak{p}^*}}$ et de $T_{\pi^*}(Ш(N_n^*))$ sont bornés. Comme $E(N_\infty^*)$ modulo torsion est un groupe abélien libre, on en déduit qu'il est de type fini et que $\varprojlim E(N_n^*) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*}$ est égal à $T_{\pi^*}(E(N_\infty^*))$. D'un autre côté, $T_{\pi^*}(Ш(N_n^*))$ est un $\mathbb{Z}_p$-module libre de type fini. On montre facilement que la limite projective des $T_{\pi^*}(Ш(N_n^*))$ est nulle. Cela démontre que $\varprojlim \overset{v}{S}{}^*(N_n^*)$ est isomorphe à $T_{\pi^*}(E(N_\infty^*))$ et finit la démonstration.

Nous allons maintenant comparer les groupes Σ et S. Cependant, nous serons obligés d'utiliser des résultats énoncés dans la suite.

Lemme 11. Soit L_∞ une $\mathbb{Z}_p$-extension de F différente de N_∞^* et telle que $L_\infty(E_{\mathfrak{p}^*})$ vérifie l'hypothèse $\mathfrak{p}^*$-adique faible de Leopoldt (paragraphe 2.2). Alors $\Sigma^*(L_\infty)$ et $S^*(L_\infty)$ sont égaux.

Démonstration. On déduit de la suite exacte

$$0 \longrightarrow \Sigma^*(L_\infty) \longrightarrow S^*(L_\infty) \longrightarrow \prod_{v|\mathfrak{p}} \tilde{E}_v(\tilde{L}_{\infty,v})(p)$$

et du lemme 2 que le conoyau de $\Sigma^*(L_\infty) \longrightarrow S^*(L_\infty)$ est fini si L_∞ est différente de N^*_∞. Mais sous l'hypothèse $\mathfrak{p}^*$-adique faible de Leopoldt pour $L_\infty(E_{\mathfrak{p}^*})$, $S^*(L_\infty)$ n'a pas de $\mathbb{Z}_p[[G(L_\infty/F)]]$-modules finis non nuls. On en déduit donc que $\Sigma^*(L_\infty)$ et $S^*(L_\infty)$ sont égaux.

1.7. Théorie de Galois pour les groupes de Selmer.

Nous allons étudier dans ce paragraphe le lien existant entre le groupe de Selmer sur F_∞ et le groupe de Selmer sur une $\mathbb{Z}_p$-extension L_∞ de F contenue dans F_∞ ou sur F.

Proposition 12. *Si L_∞ est différente de N_∞, l'homomorphisme de restriction induit un isomorphisme*

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

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

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

grâce au lemme 9. Il est alors facile de voir que la proposition résulte des deux lemmes suivants.

Lemme 13. *Si L_∞ est différente de N_∞ et si v est une place de F_∞ ne divisant pas $\mathfrak{p}$, l'homomorphisme de restriction*

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

est injectif.

Démonstration. Le noyau de l'homomorphisme 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 ayant bonne réduction en v au moins sur $F(E_{\mathfrak{p}})$, la composante $\mathfrak{p}$-primaire de ce dernier groupe est nulle.

Enonçons maintenant le second lemme.

Lemme 14. *Si L_∞ ne contient pas $E_{\mathfrak{p}^\infty}$, l'homomorphisme de restriction induit un isomorphisme*

$$H^1(L_\infty, E_{p^\infty}) \xrightarrow{\simeq} H^1(F_\infty, E_{p^\infty})^{G(F_\infty/L_\infty)}.$$

Démonstration. Par la suite exacte d'inflation-restriction, il suffit de montrer que $H^i(F_\infty/L_\infty, E_{p^\infty}(F_\infty))$ est nul pour $i = 1$ et 2. Or $E_{p^\infty}(F_\infty)$ est soit nul et le lemme est trivial soit égal à E_{p^∞}. On peut alors conclure par passage à la limite à partir du lemme suivant (qui nous a d'ailleurs déjà servi).

Lemme 15. Soit 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 $i \geq 1$.

Démonstration. Si p^r est l'ordre de A, on peut déjà supposer que Δ est d'ordre $p^s (s < r)$. Soit δ un générateur de Δ. On a alors

$$\delta a = (1 + p^{r-s}u)a$$

avec u premier à p. On en déduit que

$$N_\Delta(a) = \sum_{\delta \in \Delta} \delta a = \frac{(1 + p^{r-s}u)^{p^s} - 1}{p^{r-s}u} a = p^s(1+u'p)a$$

avec u' premier à p et que $N_\Delta(A)$ est exactement le sous-groupe de A d'ordre p^{r-s}. D'autre part le sous-groupe des éléments de A invariants par Δ est contenu dans ce sous-groupe. On en déduit que $H^2(\Delta, A)$ qui est isomorphe à $A^\Delta/N_\Delta(A)$ et $H^i(\Delta, A)$ pour $i \geq 1$ sont nuls.

On montre de même la proposition suivante.

Proposition 16. L'homomorphisme de restriction induit l'isomorphisme

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

Lemme 17. L'homomorphisme de restriction

$$S'(F) \longrightarrow S(F_\infty)^{G(F_\infty/F)}$$

a un noyau et conoyau finis.

Démonstration. Nous n'aurons en fait besoin que de la finitude du noyau. Ce noyau est contenu dans $H^1(L_\infty/F, E_{p^\infty}(L_\infty))$ pour une $\mathbb{Z}_p$-extension L_∞

contenue dans F_∞ et différente de N_∞ et ce dernier groupe est évidemment fini. Quand à la finitude du conoyau, elle vient de la finitude du groupe $H^1(L_{\infty,v}/F_v,E)(\mathfrak{p})$ ([19]). Nous en verrons une autre démonstration au paragraphe 2.3.

2. Le Λ-module $S(F_\infty)$.

2.1. 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 $\mathfrak{p}$ maximale de L et $X(L)$ le groupe de Galois de M_L sur L. Le groupe de Galois $G(F_\infty/F)$ opère sur $X(F_\infty)$ par automorphismes intérieurs de la manière suivante : si γ appartient à $G_\infty = G(F_\infty/F)$ et si $\tilde{\gamma}$ est un prolongement de γ à M_{F_∞}, alors on pose

$$\gamma x = \tilde{\gamma} x \tilde{\gamma}^{-1} \quad \text{pour tout } x \in X(F_\infty) .$$

Rappelons d'autre part que χ est le caractère de $\Delta = G(F_\infty/F_\infty)$ identifié à $G(F(E_p)/F)$ donnant l'action de ce groupe sur $E_\mathfrak{p}$.

Théorème 18. 1- Le groupe de Selmer $S(N_\infty)$ est $G(N_\infty/F)$-isomorphe à $\mathrm{Hom}_{\mathbb{Z}_p}(X(N_\infty)^{(\chi)},E_{\mathfrak{p}^\infty})$.

2- Le groupe de Selmer $S(F_\infty)$ est $G(F_\infty/F)$-isomorphe à $\mathrm{Hom}_{\mathbb{Z}_p}(X(F_\infty)^{(\chi)},E_{\mathfrak{p}^\infty})$.

Démonstration. Les deux démonstrations sont tout à fait similaires. Démontrons par exemple la deuxième assertion. La démonstration repose sur le fait que si E a bonne réduction en une place v d'une extension L sur F, le groupe de cohomologie $H^1(L_v^{nr}/L_v,E(L_v^{nr}))$ est nul si L_v^{nr} désigne l'extension non ramifiée maximale de L_v.

Il est clair que l'on a les égalités

$$\mathrm{Hom}_{\mathbb{Z}_p}(X(F_\infty)^{(\chi)},E_{\mathfrak{p}^\infty}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}(X(F_\infty),E_{\mathfrak{p}^\infty})^\Delta$$

$$S(F_\infty) \xrightarrow{\sim} S(F_\infty)^\Delta ,$$

Δ étant d'ordre premier à p. On peut donc supposer pour la démonstration que E_p est contenu dans $E(F)$. Alors, $S(F_\infty)$ et $\mathrm{Hom}_{\mathbb{Z}_p}(X(F_\infty),E_{\mathfrak{p}^\infty})$

sont tous deux des sous-groupes de $\mathrm{Hom}_{\mathbb{Z}_p}(G(\bar{F}/F_\infty), E_{\mathfrak{p}^\infty})$. Soit x un élément du second groupe. Par définition de $X(F_\infty)$, pour toute place v de F ne divisant pas $\mathfrak{p}$, la restriction de x au sous-groupe de décomposition de v se factorise par le groupe de Galois de $F_{\infty,v}^{nr}/F_{\infty,v}$. L'image de x dans $H^1(F_{\infty,v},E)$ est donc nulle et x appartient à $S'(F_\infty)$ donc à $S(F_\infty)$ grâce au lemme 9. Réciproquement, tout élément x de $S(F_\infty)$ provient d'un élément x_n de $S(F_\infty)^{(\pi^n)}$ pour un certain n. La restriction $x_{n,v}$ de x_n au groupe de décomposition de v appartient à l'image de $E(F_{\infty,v})/\pi^n E(F_{\infty,v})$. Si v ne divise pas $\mathfrak{p}$, $x_{n,v}$ se factorise à travers $G(F_{\infty,v}^{nr}/F_{\infty,v})$ et x_n appartient à $\mathrm{Hom}_{\mathbb{Z}_p}(X(F_\infty),E_{\pi^n})$ et x à $\mathrm{Hom}_{\mathbb{Z}_p}(X(F_\infty),E_{\mathfrak{p}^\infty})$.

Exemples 3. La démonstration montre qu'une propriété analogue est vraie à un niveau fini, plus précisemment on a l'isomorphisme :

$$S'(N_n)^{(\pi^n)} \simeq \mathrm{Hom}_{\mathbb{Z}_p}(X(N_n)^{(\chi)},E_{\pi^n})$$

si N_n est le sous-corps de $N_n = F(E_{\pi^n})$ fixé par Δ. Par la théorie du corps de classes, $X(N_n)^{(\chi)}$ est lié au groupe des classes d'idéaux de N_n. En particulier, savoir que p ne divise pas le nombre de classes de $F(E_{\mathfrak{p}})$ permet souvent de calculer la composante $\mathfrak{p}$-primaire du groupe de Shafarevitch-Tate. C'est en fait le principe de la descente. Nous allons donner des exemples dans cette direction. Afin de montrer dans quelques cas particuliers que p ne divise pas le nombre de classes de $F(E_{\mathfrak{p}})$, nous allons utiliser les bornes sur le discriminant d'un corps de nombres démontrées par Odlyzko et Poitou (on utilisera les tables de Diaz-y-Diaz [11]). On suppose ici que F est le corps de Hilbert H de K et que p est différent de 2 et 3 (et toujours décomposé dans K). Si K est différent de $\mathbb{Q}(\sqrt{-1})$ et de $\mathbb{Q}(\sqrt{-3})$ et si $\mathfrak{f}$ est le conducteur du Grössencharakter ψ_H de E sur H, le discriminant de $H(E_{\mathfrak{p}})$ sur H est $\mathfrak{f}^{(p-1)/2}\mathfrak{p}^{p-2}$. On en déduit que si l'on note $d(L/M)$ le discriminant de L sur M on a

$$\frac{1}{[H(E_{\mathfrak{p}}):\mathbb{Q}]} \log d(H(E_{\mathfrak{p}})/\mathbb{Q}) = \frac{1}{2[H:\mathbb{Q}]} \log N_{H/\mathbb{Q}}(\mathfrak{f}) + \frac{p-2}{2(p-1)} \log p + \frac{1}{2} \log d(K/\mathbb{Q}).$$

En comparant ce nombre avec les bornes sur les discriminants des corps totalement imaginaires de degré $p(p-1)[H:\mathbb{Q}]$, on montre que p ne divise pas le nombre de classes de $H(E_{\mathfrak{p}})$ pour les courbes elliptiques et

nombres premiers suivants

A(7) $p = 11,\ p = 23$ $(H = \mathbb{Q}(\sqrt{-7}))$;

A(11) $p = 5$ $(H = \mathbb{Q}(\sqrt{-11}))$.

Le produit U des unités locales de $H(E_{\mathfrak{p}})$ congrues à 1 modulo v pour les places v divisant $\mathfrak{p}$ est un $\mathbb{Z}_p[G(H(E_{\mathfrak{p}})/H)]$-module de rang $[H : K]$. On en déduit que le $\mathbb{Z}_p$-rang de $U^{(X)}$ est égal au degré h de H sur K et que sous l'hypothèse que p ne divise pas le nombre de classes de $H(E_{\mathfrak{p}})$, on a

$$rg_{\mathcal{O}} E(H) + \dim_{\mathbf{F}_p} (Ш'(H)/\mathfrak{p}Ш'(H)) \leq h.$$

Le $\mathcal{O}$-rang de $A(7)(K)$ est nul; donc le rang de $Ш'(H)/\mathfrak{p}Ш'(H)$ sur $\mathbf{F}_p$ est inférieur à 1 pour $p = 11$ et 23. Le $\mathcal{O}$-rang de $A(11)(K)$ est égal à 1; donc $Ш'(K)(5)$ est nul.

Nous allons maintenant nous intéresser à $X(F_\infty)$ et nous en déduirons les propriétés correspondantes de $S(F_\infty)$ quitte à remplacer F par $F(E_{\mathfrak{p}})$.

2.2. Premières propriétés du Λ-module $X(F_\infty)$.

L'action de $\Theta = G(F_\infty/F)$ sur le $\mathbb{Z}_p$-module $X(F_\infty)$ par automorphismes intérieurs permet de munir $X(F_\infty)$ d'une structure de $\mathbb{Z}_p[[\Theta]]$-module compact. Si G est un $\mathbb{Z}_p$-groupe, on pose $\Lambda_G = \mathbb{Z}_p[[G]]$. En particulier, on pose $\Lambda = \Lambda_\Theta$ lorsqu'il n'y a pas de confusion possible. Le premier résultat élémentaire est le suivant.

Lemme 19. Le Λ-module $X(F_\infty)$ est de type fini.

Démonstration. Soit M_0' l'extension abélienne maximale de F contenue dans M_{F_∞}. Nous allons d'abord montrer la suite exacte

$$\mathbb{Z}_p \longrightarrow X(F_\infty)_\Theta \longrightarrow G(M_0'/F_0) \longrightarrow 0. \tag{10}$$

Pour cela, introduisons une $\mathbb{Z}_p$-extension L_∞ de F contenue dans F_∞. On a alors facilement l'isomorphisme

$$X(F_\infty)_{G(F_\infty/L_\infty)} \xrightarrow{\alpha} G(M_{L_\infty}'/F_\infty)$$

si M_{L_∞}' est l'extension abélienne maximale de L_∞ contenue dans M_{F_∞},

ce qui peut s'écrire par la suite exacte

$$0 \longrightarrow X(F_\infty)_{G(F_\infty/L_\infty)} \longrightarrow G(M'_{L_\infty}/L_\infty) \longrightarrow G(F_\infty/L_\infty) \longrightarrow 0.$$

On a de même l'isomorphisme

$$G(M'_{L_\infty}/L_\infty)_{G(L_\infty/F)} \xrightarrow{\simeq} G(M'_0/L_\infty) ,$$

d'où la suite exacte

$$\mathbb{Z}_p \longrightarrow X(F_\infty)_\Theta \longrightarrow G(M'_0/L_\infty) \longrightarrow G(F_\infty/L_\infty) \longrightarrow 0$$

et (10). Comme M'_0 est contenu dans la p-extension abélienne non ramifiée au dehors de p maximale, le groupe de Galois de M'_0 sur F est un $\mathbb{Z}_p$-module de type fini. Il en est donc de même de $X(F_\infty)_\Theta$ et $X(F_\infty)$ est un Λ-module de type fini.

On se demande maintenant si le Λ-module $X(F_\infty)$ est un Λ-module de Λ-torsion. Pour répondre, nous devons d'abord parler de la conjecture $\mathfrak{p}$-adique 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 $E_{L,\mathfrak{p}}$ le groupe des unités globales de L congrues à 1 modulo toute place v de L au dessus de $\mathfrak{p}$ et $i_{L,\mathfrak{p}}$ l'injection diagonale de $E_{L,\mathfrak{p}}$ dans $\prod_{v|\mathfrak{p}} U(L_v)$. On note $\delta_{\mathfrak{p}}(L)$ la différence entre le $\mathbb{Z}_p$-rang de la clôture de $i_{L,\mathfrak{p}}(E_{L,\mathfrak{p}})$ pour la topologie $\mathfrak{p}$-adique et le $\mathbb{Z}$-rang de $E_{L,\mathfrak{p}}$. La conjecture $\mathfrak{p}$-adique de Leopoldt pour l'extension finie L de F est que $\delta_{\mathfrak{p}}(L)$ est nulle. Elle a été montrée par Brumer dans le cas d'une extension abélienne de K par les méthodes de Baker.

On appellera ici

Hypothèse $\mathfrak{p}$-adique de Leopoldt pour une extension finie L : le nombre $\delta_{\mathfrak{p}}(L)$ est nul.

Si L_∞ est une $\mathbb{Z}_p$-extension, nous n'aurons besoin que d'une propriété plus faible des nombres $\delta_{\mathfrak{p}}(L)$ où L est une sous-extension finie de L_∞. Nous appellerons donc

Hypothèse $\mathfrak{p}$-adique de Leopoldt pour une $\mathbb{Z}_p$-extension L_∞ d'une extension finie de F : les nombres entiers $\delta_{\mathfrak{p}}(L)$ sont bornés lorsque L parcourt les extensions finies de F contenues dans L_∞.

Nous utiliserons aussi les versions p-adiques et $\mathfrak{p}^*$-adiques de ces hypothèses.

Proposition 20. *Soit L_∞/F une $\mathbb{Z}_p$-extension de groupe de Galois H. Alors le Λ_H-module $X(L_\infty)$ est de Λ_H-torsion si et seulement si l'hypothèse $\mathfrak{p}$-adique de Leopoldt pour L_∞ est vérifiée.*

Démonstration. Soit L_n le sous-corps de L_∞ fixé par $H_n = H^{p^n}$. Le module $X(L_\infty)$ est de Λ_H-torsion si et seulement si $X(L_\infty)_{H_n}$ est de $\mathbb{Z}_p$-rang borné. Or le nombre de places de L_∞ ramifiées dans L_∞/F étant fini, il est facile de voir que la différence du $\mathbb{Z}_p$-rang de $X(L_\infty)_{H_n}$ et de $X(L_n)$ est bornée. Mais la théorie du corps de classes donne une description de ce dernier module : on a la suite exacte de modules

$$0 \longrightarrow \prod_{v|\mathfrak{p}} U(L_{n,v})/\overline{i_{L_n,\mathfrak{p}}(E_{L_n,\mathfrak{p}})} \longrightarrow X(L_n) \longrightarrow A(L_n) \longrightarrow 0$$

où $A(L_n)$ désigne la composante p-primaire du groupe des classes d'idéaux de L_n et où la barre désigne la clôture pour la topologie $\mathfrak{p}$-adique. Le $\mathbb{Z}_p$-rang de $X(L_n)$ est donc $\delta_{\mathfrak{p}}(L_n)+1$, d'où la proposition.

Proposition 21. *Le Λ-module $X(F_\infty)$ est de Λ-torsion si l'hypothèse $\mathfrak{p}$-adique de Leopoldt pour N_∞ est vérifiée.*

Démonstration. D'après le lemme I.2, il suffit de montrer que $X(F_\infty)_{G(F_\infty/N_\infty)}$ est un Λ_Γ-module de torsion (on rappelle que Γ est le groupe de Galois de N_∞ sur F). Posons $H = G(F_\infty/N_\infty)$. Nous allons faire le lien entre $X(F_\infty)_H$ et $X(N_\infty)$ et voir qu'ils sont simultanément de Λ_Γ-torsion. On terminera alors la démonstration avec la proposition 20.

Soit M'_{N_∞} l'extension abélienne de N_∞ contenue dans M_{F_∞} maximale et soit J_{N_∞} le composé des sous-groupes d'inertie aux places de N_∞ au dessus de $\mathfrak{p}^*$ dans l'extension abélienne M'_{N_∞}/N_∞. Comme chacun de ces sous-groupes est isomorphe à $\mathbb{Z}_p$ et qu'il n'y a qu'un nombre fini de places au dessus de $\mathfrak{p}^*$ dans N_∞, J_{N_∞} est un Λ_Γ-module de torsion. On a d'autre part les deux suites exactes

$$(11) \qquad 0 \longrightarrow J_{N_\infty} \longrightarrow G(M'_{N_\infty}/N_\infty) \longrightarrow X(N_\infty) \longrightarrow 0$$

$$(12) \qquad 0 \longrightarrow X(F_\infty)_H \longrightarrow G(M'_{N_\infty}/N_\infty) \longrightarrow G(F_\infty/N_\infty) \longrightarrow 0 .$$

Donc si $X(N_\infty)$ est un Λ_Γ-module de torsion, il en est de même de $X(F_\infty)_H$.

Remarque. En remplaçant F par $F(E_\mathfrak{p})$, on a montré que le Λ-module $\widehat{S(F_\infty)}$ est de Λ-torsion si l'hypothèse $\mathfrak{p}$-adique de Leopoldt pour N_∞ est vérifiée.

2.3. Sur les Λ-modules pseudo-nuls de $X(F_\infty)$.

Notons $X(L)$ le groupe de Galois de la p-extension abélienne de L non ramifiée au dehors de p maximale sur L. Nous ramenons dans ce paragraphe l'étude des sous-Λ-modules pseudo-nuls de $X(F_\infty)$ à l'étude de ceux de $X(F_\infty)$. L'étude de ces derniers a été faite par Greenberg ([12]).

Commençons par relier les Λ-modules $X(F_\infty)$ et $X(F_\infty)$.

Lemme 22. *Il existe un Λ-module $U(F_\infty)$ vérifiant les propriétés suivantes :*

(i) on a la suite exacte de Λ-modules

$$(13) \qquad U(F_\infty) \longrightarrow X(F_\infty) \longrightarrow X(F_\infty) \longrightarrow 0 ,$$

(ii) $U(F_\infty)$ s'injecte dans un Λ-module libre de rang $r_2(F)$ (c'est-à-dire le nombre de places imaginaires de F) avec un conoyau pseudo-nul isomorphe à

$$T(F_\infty) = \prod_{v|\mathfrak{p}^*} \mathrm{Ind}_v^{G(F_\infty/F)} T_p(\mu_{p^\infty}(F_{\infty,v}))$$

où le produit porte sur les places v de F au dessus de $\mathfrak{p}^*$.

Démonstration. Soit F_n le corps fixé par Θ^{p^n}. Appelons M_n (resp. R_n) la p-extension abélienne non ramifiée en dehors de $\mathfrak{p}$ (resp. de p) maximale de F_n et $U_{n,v}$ le groupe des unités locales congrues à 1 modulo v de $F_{n,v}$. Posons

$$U_{n,p} = \prod_{v|p} U_{n,v} , U_{n,\mathfrak{q}} = \prod_{v|\mathfrak{q}} U_{n,v} \quad (\mathfrak{q} = \mathfrak{p} \text{ ou } \mathfrak{p}^*).$$

Soit $E_{n,p}$ (resp. $E_{n,\mathfrak{p}}$) le groupe des unités globales de F_n congrues à 1 modulo toutes les places v divisant p (resp. $\mathfrak{p}$). On a les injec-

tions naturelles

$$i_{n,p} : E_{n,p} \longrightarrow U_{n,p}$$

$$i_{n,\mathfrak{p}} : E_{n,\mathfrak{p}} \longrightarrow U_{n,\mathfrak{p}} .$$

Si A_n est la composante p-primaire du groupe des classes d'idéaux de F_n, grâce à la théorie du corps de classes, les suites et diagramme suivants sont exacts et commutatifs :

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

La première application verticale pr_n est induite par la projection naturelle. Le noyau K_n de l'application quotient

$$G(R_n/F_n) \longrightarrow G(M_n/F_n)$$

est égal au noyau de pr_n. D'autre part, comme $E_{n,p}$ est un sous-$\mathbb{Z}$-module de $E_{n,\mathfrak{p}}$ d'indice premier à p, l'homomorphisme

$$\overline{i_{n,p}(E_{n,p})} \longrightarrow \overline{i_{n,\mathfrak{p}}(E_{n,\mathfrak{p}})}$$

est surjectif et K_n est un quotient de $U_{n,\mathfrak{p}^*}$. Soit $U(F_\infty)$ la limite projective des $U_{n,\mathfrak{p}^*}$ pour $n \geq 1$ relativement aux homomorphismes de norme. Comme $X(F_\infty)$ (resp. $X(F_\infty)$) est la limite projective des groupes $G(R_n/F_n)$ (resp. $G(M_n/F_n)$), on déduit de ce qui précède la suite exacte

$$U(F_\infty) \longrightarrow X(F_\infty) \longrightarrow X(F_\infty) \longrightarrow 0 .$$

Il ne reste plus qu'à montrer que $U(F_\infty)$ vérifie (ii). Il est immédiat que l'on a l'isomorphisme de Λ-modules

$$U(F_\infty) \simeq \prod_{v|\mathfrak{p}^*} \mathrm{Ind}_{V}^{G(F_\infty/F)} U(F_{\infty,v}) ,$$

où le produit est pris sur les places v de F divisant $\mathfrak{p}^*$ et où

$U(F_{\infty,v})$ 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_∞. Elle est étudiée par Wintenberger qui généralise les résultats d'Iwasawa ([37], [17]) et cela donne tout de suite le résultat.

Remarquons que, dans le cas d'une $\mathbb{Z}_p$-extension L_∞, on peut de même montrer qu'il existe un $\Lambda_{G(L_\infty/F)}$-module $U(L_\infty)$ sans torsion de rang $r_2(F)$ sur $\Lambda_{G(L_\infty/F)}$ tel que la suite de $\Lambda_{G(L_\infty/F)}$-modules

$$U(L_\infty) \longrightarrow X(L_\infty) \longrightarrow X(L_\infty) \longrightarrow 0$$

soit exacte en utilisant les résultats d'Iwasawa concernant les $\mathbb{Z}_p$-extensions ([17]).

Enonçons maintenant les résultats obtenus par Greenberg dans [12]. Dans toute la fin de ce paragraphe, L_∞ sera une $\mathbb{Z}_p$-extension de F.

1- L'extension F_∞ contenant la $\mathbb{Z}_p$-extension cyclotomique, le Λ-module $X(F_\infty)$ est un Λ-module compact de type fini de Λ-rang $r_2(F)$ sans Λ-sous-modules finis.

2- Si L_∞ vérifie l'hypothèse p-adique de Leopoldt, le $\Lambda_{G(L_\infty/F)}$-module $X(L_\infty)$ est de rang $r_2(F)$ sans $\Lambda_{G(L_\infty/F)}$-sous-modules finis non nuls.

3- Si L_∞ vérifie l'hypothèse p-adique de Leopoldt, le $\Lambda_{G(L_\infty/F)}$-module $X(L_\infty)$ est un $\Lambda_{G(L_\infty/F)}$-module de torsion sans $\Lambda_{G(L_\infty/F)}$-sous-modules finis non nuls.

4- Si F vérifie la conjecture p-adique de Leopoldt, le Λ-module $X(F_\infty)$ n'a pas de Λ-sous-modules pseudo-nuls non nuls.

On déduit de ces résultats et de la proposition I.6 que la dimension projective de $X(F_\infty)$ est inférieure à 1 dès que la conjecture p-adique de Leopoldt est vraie pour F.

Théorème 23. Supposons que $X(F_\infty)$ est un Λ-module de torsion. Alors $X(F_\infty)$ n'a pas de Λ-modules pseudo-nuls non nuls si et seulement si $X(F_\infty)$ n'en a pas.

Démonstration. Comme le Λ-module $X(F_\infty)$ est de torsion, le noyau de l'homomorphisme $U(F_\infty) \longrightarrow X(F_\infty)$ l'est aussi. Mais $U(F_\infty)$ n'a pas de

torsion grâce au lemme 22. Donc ce noyau est nul et on a la suite exacte

$$0 \longrightarrow U(F_\infty) \longrightarrow X(F_\infty) \longrightarrow X(F_\infty) \longrightarrow 0 .$$

Il est alors clair que si $X(F_\infty)$ a un module pseudo-nul non nul, celui-ci s'injecte dans $X(F_\infty)$. Réciproquement, soit B le sous-module pseudo-nul maximal de $X(F_\infty)$ et soit C son image réciproque dans $X(F_\infty)$. Le Λ-sous-module de torsion de C s'injecte dans B; comme $X(F_\infty)$ n'a pas de Λ-sous-modules pseudo-nuls non nuls, C est sans torsion. Il est donc contenu dans un Λ-module réflexif R avec un conoyau D pseudo-nul. Si K est le conoyau de l'homomorphisme composé

$$U(F_\infty) \longrightarrow C \longrightarrow R ,$$

la suite $0 \longrightarrow B \longrightarrow K \longrightarrow D \longrightarrow 0$ est exacte. Comme B et D sont pseudo-nuls, K l'est aussi. Il est donc isomorphe à $T(F_\infty)$ (lemme 22). Mais pour presque tout sous-groupe H de Θ tel que $\Theta/H \simeq \mathbb{Z}_p$, B, K et D sont des Λ_H-modules de torsion et $T(F_\infty)_H$ est fini. On en déduit que B_H est fini. De plus, B étant le sous-module pseudo-nul maximal de $X(F_\infty)$, B_H est un sous-module de $X(F_\infty)_H$ pour presque tout H et donc de $X(L_\infty)$ si L_∞ est le sous-corps de F_∞ fixé par H. Pour un tel H, B_H est donc nul dès que $X(L_\infty)$ est de $\Lambda_{\Theta/H}$-torsion (c'est-à-dire dès que L_∞ vérifie l'hypothèse de Leopoldt) et un tel H existe car $X(F_\infty)$ est de Λ-torsion. Donc B est nul lui aussi, ce qui démontre le théorème.

Lemme 24. Supposons que N_∞ vérifie l'hypothèse $\mathfrak{p}$-adique de Leopoldt. Alors, le Λ_Γ-module J_{N_∞} défini dans la démonstration de la proposition 21 est isomorphe à

$$\prod_{v|\mathfrak{p}^*} \mathrm{Ind}_v^\Gamma \mathbb{Z}_p .$$

Démonstration. Si L est une extension de K, soit R_L la p-extension abélienne non ramifiée en dehors de p de L. On a l'isomorphisme

$$X(F_\infty)_{G(F_\infty/N_\infty)} \simeq G(R_{N_\infty}/F_\infty)$$

et les suites exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U(F_\infty)_{G(F_\infty/N_\infty)} & \longrightarrow & X(N_\infty) & \longrightarrow & G(M'_{N_\infty}/N_\infty) & \longrightarrow & 0 \\ 0 & \longrightarrow & U(N_\infty) & \longrightarrow & X(N_\infty) & \longrightarrow & X(N_\infty) & \longrightarrow & 0 . \end{array}$$

On en déduit que le conoyau de

$$U(F_\infty)_{G(F_\infty/N_\infty)} \longrightarrow U(N_\infty)$$

est isomorphe à J_{N_∞}. Mais la structure de ce conoyau est donnée dans le lemme 5.2 (ii) de [37]. On en déduit le lemme.

Nous allons maintenant traduire les résultats obtenus en termes du dual de Pontryagin $Y(F_\infty)$ de $S(F_\infty)$.

Théorème 25. On suppose que N_∞ vérifie l'hypothèse $\mathfrak{p}$-adique de Leopoldt et que $F(E_\mathfrak{p})$ vérifie l'hypothèse p-adique de Leopoldt. Alors, $Y(F_\infty)$ est un Λ-module de Λ-torsion et de dimension projective inférieure à 1.

Démonstration. Nous avons déjà vu que $Y(F_\infty)$ est de Λ-torsion. Par le théorème 23, il n'a pas de Λ-modules pseudo-nuls non nuls. Grâce à la proposition I.6, il suffit donc de montrer que pour une infinité de sous-groupes H de Θ tels que $\Theta/H \simeq \mathbb{Z}_p$, $Y(F_\infty)_H$ n'a pas de $\Lambda_{\Theta/H}$-sous-modules finis. Cela est vrai pour $H = G(F_\infty/N_\infty)$ grâce au lemme 24 et aux suites exactes suivantes :

$$(14) \quad 0 \longrightarrow Y(F_\infty)_{G(F_\infty/N_\infty)} \longrightarrow G(M'_{N_\infty}/N_\infty)^{(\chi)}(-1) \longrightarrow T_\pi(E) \longrightarrow 0$$

$$(15) \quad 0 \longrightarrow J_{N_\infty}^{(\chi)}(-1) \longrightarrow G(M'_{N_\infty}/N_\infty)^{(\chi)}(-1) \longrightarrow Y(N_\infty) \longrightarrow 0$$

où l'on pose $M(-1) = \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi(E), M)$. De plus, $Y(F_\infty)_H$ n'a pas de $\Lambda_{\Theta/H}$-modules finis si et seulement si $(Y(F_\infty)_H)^{\Theta/H}$ n'a pas de sous-modules finis. Le lemme I.7 permet alors de finir la démonstration.

Chapitre III. Hauteurs p-adiques.

Les premières constructions de hauteurs p-adiques ont été faites par D. Bernardi ([2]) dans le cas des courbes elliptiques en suivant une idée d'Abramov et Rosenblum et par Néron dans le cas des variétés abéliennes. Cependant, la canonicité de ces hauteurs n'apparaissait que dans le cas de multiplication complexe. La définition de ces hauteurs p-adiques repose sur la construction de fonctions σ p-adiques aux places divisant p. D'autres constructions s'inspirent de la méthode qu'utilise S. Bloch pour construire la hauteur quadratique complexe de Néron-Tate à partir des extensions de groupes algébriques de la variété abélienne par un tore. Elles ont été faites par B. Gross dans le cas des courbes elliptiques à multiplication complexe mais surtout par P. Schneider dans le cas général des variétés abéliennes à bonne réduction ordinaire en p. Enfin, Mazur et Tate ont défini les fonctions σ p-adiques canoniques aux places au dessus de p où la courbe elliptique a réduction ordinaire. Dans le cas des variétés abéliennes à réduction ordinaire en p, ils ont aussi défini des hauteurs canoniques en utilisant la théorie des bi-extensions de groupes (c'est-à-dire un point de vue analogue à celui de Bloch) et retrouvent les résultats de P. Schneider.

Nous allons ici nous borner au cas particulier où la courbe elliptique E a multiplication complexe et nous garderons la présentation des fonctions σ faite par D. Bernardi en allant un peu plus loin dans les propriétés d'intégralité. Par contre, nous adopterons le point de vue de Mazur et Tate d'associer à toute représentation continue du groupe des classes d'idèles de F dans $\mathbb{Z}_p$ une hauteur p-adique. Nous donnons ensuite un procédé de calcul de ces hauteurs qui fait apparaître une expression que l'on peut qualifier à postériori de hauteur naïve.

1. Définition des hauteurs p-adiques.

Soient L une extension finie de F et S un ensemble de places de L au dessus de p. On utilise un modèle de Weierstrass de E sur l'anneau des entiers de L ayant bonne réduction aux places de S, c'est-à-dire une équation de la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

(où les a_i appartiennent à l'anneau des entiers de L) et de discriminant Δ premier aux places de S. Si v est une place finie de L, on normalise la valuation associée par $v_L(L^x) = \mathbb{Z}$ et on note $\omega_{L,v}$ une uniformisante de L en v. 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.

1.1. Facteurs locaux de Néron-Tate.

Si v est une place finie de L, Néron et Tate ont démontré qu'il existe une unique fonction $\lambda_{L,v}$ de $E(L_v) - \{0\}$ 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 0 de $\lambda_{L,v}(P) - v_L(t(P))$ existe pour un, donc pour tout, paramètre uniformisant t de E à l'origine;

(ii) pour tout couple (P,Q) de points de $E(L_v) - \{0\}$ tel que $P \pm Q \neq 0$, on a

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

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

$$(3) \qquad \lambda_{L,v}(\alpha P) = N(\alpha)\lambda_{L,v}(P) + \frac{1}{12} v_L(\gamma_\alpha(P)\alpha^{12}).$$

Lemme 1. Soient v une place finie de L où E a bonne réduction et (x,y) les coordonnées des points de E dans un modèle ayant bonne réduction en v. Alors,

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

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

Si E n'a pas bonne réduction en v mais que P ne se réduit pas au point singulier en v dans le modèle considéré, on a la formule

$$\lambda_{L,v}(P) = \mathrm{Sup}(0, -\tfrac{1}{2} v_L(x(P))) + \tfrac{1}{12} v_L(\Delta).$$

1.2. Fonctions σ p-adiques.

Fixons une place v de S. Comme le modèle (1) de E a bonne réduction en v, $t = -x/y$ est un paramètre uniformisant de E à l'origine. Soient L_v le logarithme de $E_{1,v}$ et ϕ_v la série entière réciproque de L_v. Alors $z = L_v(t)$ est un paramètre uniformisant du groupe formel additif. On définit les séries formelles suivantes

$$\begin{aligned}
\wp_v(z) &= x(\phi_v(z)) + (a_1^2+4a_2)/12 \\
&= 1/z^2 + \sum_2^\infty \gamma_k z^{2k-2} \\
\sigma_v(z) &= z \exp\Big(-\frac{s_2}{2} z^2 - \sum_2^\infty \gamma_k z^{2k}/2k(2k-1)\Big) \\
\theta_v(z) &= \Delta\, \sigma_v(z)^{12}.
\end{aligned}$$

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 L. Soit alors

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

Comme E est à multiplication complexe, il est bien connu que $s_2(L)$ est un nombre algébrique, image par le plongement de L dans $\mathbb{C}$ 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 $E_{2k}(L)$. L'étude du comportement de s_2, γ_k, t par changement de modèle montre facilement que $\theta_v(L_v(t(P)))$ 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

$$(\alpha^2 - \alpha\alpha^*)s_2 = \sum_{\substack{r\in E_\alpha \\ r\neq 0}} (x(r) + (a_1^2 + 4a_2)/12).$$

Exemples 1. Si K est égal à $\mathbb{Q}(\sqrt{-1})$ et $\mathbb{Q}(\sqrt{-3})$, s_2 est nul : en effet, le réseau L étant invariant par multiplication par une racine de l'unité de K, on a $s_2(L) = s_2(\zeta L) = \zeta^2 s_2(L)$ pour $\zeta^{12} = 1$ et $\zeta \in K$. La réciproque a été montrée par Masser (Springer L.N. 437).

Donnons quelques autres valeurs de s_2 calculées dans [29] (table B II, E III).

$$y^2 = 4x^3 - 35x - 49 \qquad K = \mathbb{Q}(\sqrt{-7}) \qquad s_2 = 1/2$$

$$y^2 = 4x^3 - 152x - 361 \qquad K = \mathbb{Q}(\sqrt{-19}) \qquad s_2 = 2$$

$$y^2 = 4x^3 - 3\sqrt{5}(4+\sqrt{5})x - 7(3+2\sqrt{5}) \qquad K = \mathbb{Q}(\sqrt{-15}) \qquad s_2 = \frac{1}{2}\left(1 + 2\,\frac{\sqrt{5}}{5}\right).$$

La série $\sigma_v(z)$ converge dans L_v pour $v_L(z) > v_L(p)/(p-1)$. De plus, pour α impair, $\sigma_v(\alpha z)/\sigma_v(z)^{N(\alpha)}$ est égal à une fonction $g_\alpha(P)$ rationnelle sur la courbe et de diviseur $\sum_{r \in E_\alpha} ((r) - (0))$. Le lemme suivant se déduit des résultats de Mazur et Tate sur les fonctions σ p-adiques mais nous en donnons ici une démonstration indépendante.

Lemme 2. *La série $\sigma_v(L_v(t))$ comme série en t appartient à $t(1 + tR_v[[t]])$ où R_v est l'anneau des entiers de L_v.*

Démonstration. Supposons par exemple que v divise p. Comme la réduction modulo v est injective sur E_{π^*}, la fonction g_{π^*} s'écrit comme série en t sous la forme

$$g_{\pi^*}(t) = c\, t^{-(p-1)}\, u(t)$$

où $u(t)$ appartient à $1 + t R_v[[t]]$ et où c est une unité de R_v (en fait π^*). Donc si l'on pose $h(t) = \sigma_v(t)/t$, h vérifie l'équation

$$\frac{h([\pi^*](t))}{h(t)^p} = c\, u'(t)$$

(ici $[\pi^*]$ désigne la multiplication par π^* dans le groupe formel $E_{1,v}$). Remarquons que l'on peut écrire h de manière unique sous la forme

$$h(t) = \prod_1^\infty (1 - a_n t^n)$$

avec a_n appartenant à L_v et que si a_r appartient à R_v, le quotient

$$\frac{1 - a_r([\pi^*](t))^r}{(1 - a_r t^r)^p}$$

appartient à $1 + t R_v[[t]]$. Donc si m est le plus petit entier tel que a_m n'appartienne pas à R_v et si l'on pose

$$h_1(t) = \prod_m^{\infty} (1 - a_n t^n),$$

h_1 vérifie

$$\frac{h_1([\pi^*](t))}{h_1(t)^p} \in 1 + t R_v[[t]] .$$

Mais ce quotient commence par $1 - (\pi^{*m} - p)a_m t^m + \ldots$ car $[\pi^*](t) = \pi^* t + \ldots$. Comme π^* est une unité dans R_v, a_m appartient à R_v, ce qui finit la démonstration du lemme 2.

Lemme 3. Soit v une place au dessus de p appartenant à S. Il existe une fonction $\mathfrak{D}_{L,v}$ de $E_{1,v}(L_v)$ à valeurs dans R_v continue et vérifiant les deux propriétés suivantes pour P et Q non nuls

$$\text{(i)} \quad \left(\frac{\mathfrak{D}_{L,v}(P+Q)\mathfrak{D}_{L,v}(P-Q)}{\mathfrak{D}_{L,v}(P)^2 \mathfrak{D}_{L,v}(Q)^2} \right)^6 = \gamma(P,Q)$$

$$\text{(ii)} \quad (\mathfrak{D}_{L,v}(\alpha P)/\mathfrak{D}_{L,v}(P)^{N(\alpha)})^{12} = \gamma_\alpha(P)\alpha^{12}$$

pour tout α appartenant à O. Elle est unique à une racine douzième de l'unité près.

Démonstration. Les propriétés usuelles de la fonction θ permettent de montrer que la fonction

$$\mathfrak{D}_{L,v}(P) = \theta_v(L_v(t(P)))$$

convient. L'unicité se montre grâce au lemme suivant.

Lemme 4. Soient v une place de S et D une fonction sur $E_{1,v}(L_v) - \{0\}$ à valeurs dans R_v, continue et vérifiant $D(\alpha P) = D(P)^{N(\alpha)}$ pour tout α appartenant à $\mathcal{O}$. Alors, D est identiquement égale à 1.

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 $\mathcal{O}$ pour la topologie v-adique est α et telle que $k_n P$ est non nulle. Alors, αP est la limite de la suite $k_n P$ dans $E_{1,v}(L_v)$. Donc

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

D'autre part, $D(\alpha P)$ est égale à $D(P)^{N(\alpha)}$. Cela implique que $D(P)$ est égale à 1.

1.3. Hauteurs p-adiques.

Considérons un homomorphisme continu ρ du groupe d'idèles I_L de L dans $\mathbb{Z}_p$, trivial sur $L^\times$. L'ensemble S_ρ des places de ramification de ρ est un sous-ensemble non vide de l'ensemble des places de L divisant p. On suppose cet ensemble contenu dans S. On note ρ_v le composé de ρ avec l'injection canonique de $L_v^\times$ dans I_L et $\tilde{\rho}$ l'homomorphisme du groupe des idéaux de L premiers aux places de S_ρ à valeurs dans $\mathbb{Z}_p$ associé à ρ. Soit $E'_{1,S}(L)$ le sous-groupe de $E(L)$ formé des points qui sont dans le noyau de l'homomorphisme de réduction de la courbe elliptique modulo toute place de S et qui ne se réduisent pas en un point singulier de la courbe en toute place. A tout point P de $E'_{1,S}(L)$, on associe un idèle $i(P)$ de I_L vérifiant les conditions suivantes

$$i(P)_v = \begin{cases} 1 & (v \text{ archimédienne}) \\ \mathfrak{D}_{L,v}(P)^{12} & (v \in S) \end{cases}$$

$$v_L(i(P)_v) = 12\lambda_{L,v}(P) \quad (v \notin S,\ v \text{ non archimédienne}).$$

On pose alors

$$h_\rho(P) = \frac{1}{12}\,\rho(i(P))$$

pour P appartenant à $E'_{1,S}(L)$. C'est la hauteur p-adique associée à l'homomorphisme ρ. Elle est à valeurs dans $\frac{1}{3}\mathbb{Z}_p$ sur $E'_{1,S}(L)$.

Proposition 5. La fonction h_ρ est une fonction quadratique, c'est-à-dire qu'elle vérifie

$$h_\rho(P+Q) + h_\rho(P-Q) = 2\,h_\rho(P) + 2\,h_\rho(Q).$$

Elle vérifie aussi l'équation

$$h_\rho(\alpha P) = N(\alpha) h_\rho(P) \quad \text{pour} \quad \alpha \in \mathcal{O}.$$

De plus, si L' est une extension finie de L et ρ' la restriction de ρ à L', on a

$$h_{\rho'}(P) = [L' : L] h_\rho(P) \quad \text{pour} \quad P \in E'_{1,S}(L).$$

Démonstration. Les deux premières propriétés se déduisent de la propriété (2) et du lemme 3-(i) d'une part et de la propriété (3) et du lemme 3-(ii) d'autre part et de la nullité de ρ sur L^*. La dernière propriété se déduit de la définition.

La forme quadratique h_ρ se prolonge naturellement à $E(L)$ et prend alors ses valeurs dans $\mathbb{Q}_p$. Considérons maintenant la forme bilinéaire symétrique $(\ ,\ )_\rho$ sur $E(L) \times E(L)$ à valeurs dans $\mathbb{Q}_p$ associée à h_ρ :

$$(P,Q)_\rho = \frac{1}{2}\,[h_\rho(P+Q) - h_\rho(P) - h_\rho(Q)].$$

Elle se prolonge en une forme bilinéaire sur

$$E(L) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p \times E(L) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p.$$

De la décomposition $\mathcal{O} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p \simeq \mathcal{O}_\mathfrak{p} \times \mathcal{O}_{\mathfrak{p}^*}$, on déduit l'isomorphisme

$$E(L) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p \xrightarrow{\sim} E(L) \underset{\mathcal{O}}{\otimes} \mathcal{O}_\mathfrak{p} \times E(L) \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}^*}.$$

La forme bilinéaire $(\ ,\ )_\rho$ vérifiant

$$(\alpha x, \alpha y)_\rho = N(\alpha)(x,y)_\rho\ ,$$

on a aussi

$$(\alpha x,y)_\rho = (x,\alpha^* y)_\rho$$

et la restriction de $(\ ,\ )_\rho$ à $E(L) \underset{O}{\otimes} O_\mathfrak{p} \times E(L) \underset{O}{\otimes} O_\mathfrak{p}$ ou à $E(L) \underset{O}{\otimes} O_{\mathfrak{p}^*} \times E(L) \underset{O}{\otimes} O_{\mathfrak{p}^*}$ est nulle. On notera $<\ ,\ >_{\rho,\mathfrak{p}}$ la restriction de $(\ ,\ )_\rho$ à

$$E(L) \underset{O}{\otimes} O_\mathfrak{p} \times E(L) \underset{O}{\otimes} O_{\mathfrak{p}^*}$$

et $<\ ,\ >_{\rho,\mathfrak{p}^*}$ la restriction de $(\ ,\ )_\rho$ à

$$E(L) \underset{O}{\otimes} O_{\mathfrak{p}^*} \times E(L) \underset{O}{\otimes} O_\mathfrak{p} .$$

Si $i_\mathfrak{p}$ désigne l'isomorphisme de $K_\mathfrak{p}$ sur $\mathbb{Q}_p$ induit par le plongement $\mathfrak{p}$-adique de K dans $\mathbb{Q}_p$, on a donc l'équation

$$<\alpha x,y>_{\rho,\mathfrak{p}} = <x,\alpha^* y>_{\rho,\mathfrak{p}} = i_\mathfrak{p}(\alpha)<x,y>_{\rho,\mathfrak{p}}$$

pour tout α appartenant à O. De plus, $(\ ,\ )_\rho$ étant symétrique, $<\ ,\ >_{\rho,\mathfrak{p}}$ est égale à la transposée de $<\ ,\ >_{\rho,\mathfrak{p}^*}$. On montre en fait facilement le lemme suivant.

Lemme 6. Soit h une forme quadratique sur $E(L)$ à valeurs dans $\mathbb{Q}_p$ et vérifiant

$$h(\alpha P) = N(\alpha)h(P) \qquad \text{pour } \alpha \in O .$$

Il existe une unique forme bilinéaire B vérifiant

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

(ii) $B(\alpha P,Q) = B(P,\alpha^* Q) = i_\mathfrak{p}(\alpha)B(P,Q)$ pour P,Q appartenant à $E(L)$ et α appartenant à O.

Remarque. Le lien calculatoire entre $(P,Q)_\rho$ et $<P,Q>_{\rho,\mathfrak{p}}$ est le suivant

$$<P,Q>_{\rho,\mathfrak{p}} = \frac{2}{\beta-\beta^*}\,[i_\mathfrak{p}(\beta)(P,Q)_\rho - (P,\beta Q)_\rho]$$

où β est un élément de $O - \mathbb{Z}$. Enfin, si $\underset{i=1}{\overset{2r}{\oplus}} \mathbb{Z}Q_i$ est un sous O-

module libre de $E(F)$ d'indice fini dont une $\mathcal{O}$-base est $P_1,\ldots,P_r$, on a

$$\det(((Q_i,Q_j)_\rho)) \sim \det((\langle P_i,P_j\rangle_{\rho,\mathfrak{p}}))^2.$$

Donnons quelques exemples fondamentaux. Remarquons d'abord que si $L^{(p)}$ est le composé des $\mathbb{Z}_p$-extensions de L, un homomorphisme $\rho : I_L \longrightarrow \mathbb{Z}_p$ se factorise par $G(L^{(p)}/L)$. Son noyau détermine une $\mathbb{Z}_p$-extension L_ρ de L. Nous noterons de la même manière l'homomorphisme de $G(L_\rho/L)$ dans $\mathbb{Z}_p$ qui s'en déduit. D'autre part, si ρ' est un homomorphisme de $G(L_\rho/L)$ dans $\mathbb{Z}_p^*$ tel que $\log_p\rho' = \rho$, on notera par abus $(\ ,\ )_{\rho'} = (\ ,\ )_\rho, \langle\ ,\ \rangle_{\rho';\mathfrak{p}} = \langle\ ,\ \rangle_{\rho,\mathfrak{p}}$. Par exemple, si κ est le caractère de $G(F_\infty/F)$ déduit de l'action de $G(F_\infty/F)$ sur $E_{\mathfrak{p}^\infty}$, l'homomorphisme $\rho: I_F \longrightarrow \mathbb{Z}_p$ correspondant à $\log_p\kappa$ vérifie :

$$\widetilde{\rho} = \log_{\mathfrak{p}} N_{F/K}$$

$$\rho_v(x) = \begin{cases} v_F(x)\log_{\mathfrak{p}}N_{F/K}(v) & \text{si } v\neq\mathfrak{p} \\ v_F(x)\log_{\mathfrak{p}}N_{F/K}(v) - \log_{\mathfrak{p}}N_{F_v/K_{\mathfrak{p}}}(x) & \text{si } v\mid\mathfrak{p}, \end{cases}$$

où l'on a posé $\log_{\mathfrak{p}} = \log_p \circ i_{\mathfrak{p}}$ (on rappelle que F contenant le corps de Hilbert de K, $N_{F/K}(v)$ est un idéal principal de K).

Le problème fondamental qui se pose ici est celui de la non-dégénérescence des formes bilinéaires $(\ ,\ )_K$ et $(\ ,\ )_{K^*}$. Dans tous les exemples numériques calculés, ces deux formes bilinéaires sont non dégénérées. D'autre part, D. Bertrand ([4]) a montré le résultat suivant par des méthodes de transcendance p-adique : si E est définie sur K et si P est un point de $E(K)$ qui n'est pas de torsion, $(P,P)_K$ et $(P,P)_{K^*}$ sont non nuls. On conjecture que $(\ ,\ )_K$ et $(\ ,\ )_{K^*}$ sont non dégénérées sur $E(F) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p$ modulo torsion. Nous verrons au chapitre V qu'un tel résultat apporte des renseignements sur le comportement du rang de la courbe elliptique le long de certaines $\mathbb{Z}_p$-extensions.

2. Hauteur naïve et procédé de calcul des hauteurs p-adiques.

Nous allons maintenant exprimer les hauteurs h_ρ en termes d'une fonction hauteur naïve m_ρ sur la courbe elliptique. La fonction m_ρ est dite naïve au sens où elle s'exprime de manière élémentaire (et sans fonction de type transcendant comme la fonction σ) en fonction des co-

ordonnées du point.

Nous distinguerons deux cas : le premier (cas I) sera en fait le cas général, le second (cas II) sera celui où S_ρ est contenu dans l'ensemble des places divisant $\mathfrak{p}$ (le cas où S_ρ est contenu dans l'ensemble des places divisant $\mathfrak{p}^*$ se traiterait bien sûr de la même manière). Le calcul fait dans le cas (I) n'utilise pas la multiplication complexe et se généralise aux cas des courbes elliptiques sans multiplication complexe ([27]).

On garde les mêmes notations que dans le paragraphe précédent et on choisit toujours un modèle de Weierstrass généralisé (1) de E sur l'anneau des entiers de L, minimal aux places de S_ρ. On note $E''_{1,S_\rho}(L)$ le sous-groupe de $E(L)$ formé des points qui sont dans le noyau de l'homomorphisme de réduction en toute place de S_ρ et qui ne se réduisent pas en un point singulier pour toute place de mauvaise réduction du modèle (1). Le dénominateur de $x(P)$ est le carré d'un idéal $\mathfrak{h}(P)$ de L. Notons d'autre part $\mathfrak{p}(P)$ la fonction de Weierstrass usuelle

$$\mathfrak{p}(P) = x(P) + (a_1^2+4a_2)/12 ,$$

et posons $\mathfrak{a}(P) = \mathfrak{h}(P)^2(\mathfrak{p}(P))$. Lorsque P appartient à $E''_{1,S_\rho}(L)$, c'est un idéal premier aux places de S_ρ sauf peut-être pour $p = 3$, où cela est certainement vrai pour l'idéal $\mathfrak{a}(3^nP)$ avec n assez grand. Pour un point P de $E''_{1,S_\rho}(L)$ tel que $\mathfrak{a}(P)$ est premier aux places de S_ρ, on définit la hauteur naïve du point P relative au modèle (1) par

$$m_\rho(P) = \tfrac{1}{2}\,\tilde{\rho}(\mathfrak{a}(P)) \qquad \text{(cas I)}$$

$$m'_\rho(P) = \tfrac{1}{2}\,\tilde{\rho}(\mathfrak{h}(P)^2(x(P))) \qquad \text{(cas II)}$$

où $\tilde{\rho}$ désigne l'homomorphisme du groupe des idéaux fractionnaires de L premiers aux places de S à valeurs dans $\mathbb{Z}_p$ associé à ρ.

Introduisons une dernière notation technique : soit r_v l'unique homomorphisme de L_v dans $\mathbb{Q}_p$ prolongeant le composé de ρ avec l'exponentielle de L_v.

Théorème 7. Soit P un point de $E''_{1,S_\rho}(L)$ qui n'est pas de torsion; alors

$$h_\rho(P) = \lim_{n\to\infty} m_\rho(p^n P)/p^{2n} - \frac{1}{2}\sum_{v\in S_\rho} r_v(s_2 L_v(t(P))^2) \quad \text{(cas I)}$$

$$h_\rho(P) = \lim_{n\to\infty} m'_\rho(\pi^n P)/N(\pi)^n = \lim_{n\to\infty} m_\rho(\pi^n P)/N(\pi)^n \quad \text{(cas II)}.$$

Démonstration. On a les développements suivants en fonction de $t = -x/y$:

$$L_v(t) = t + a_1 t^2/2 + (a_1^2+a_2) t^3/3 + \dots$$

$$\sigma_v(L_v(t)) = t + \frac{a_1}{2} t^2 + (\frac{a_1^2+a_2}{3} - \frac{s_2}{2}) t^3 + \dots$$

$$x(t) = t^{-2}(1 - a_1 t - a_2 t^2 + \dots)$$

$$\sigma_v(L_v(t))^2 \mathfrak{p}(t) = 1 - s_2 t^2 + \dots$$

Notons que les coefficients de cette dernière série sont dans $\frac{1}{3} R_v$. Supposons $\mathfrak{a}(Q)$ premier aux places de S_ρ. Comme ρ est trivial sur L^x, on a

$$h_\rho(Q) = \frac{1}{2}\sum_{v\notin S_\rho} v_L(\mathfrak{a}(Q))\rho_v(\omega_{L,v}) + \frac{1}{2}\sum_{v\in S_\rho} \rho_v(\sigma_v(L_v(t(Q)))^2 \mathfrak{p}(Q))$$

$$= m_\rho(Q) + \frac{1}{2}\sum_{v\in S_\rho} \rho_v(\sigma_v(L_v(t(Q)))^2 \mathfrak{p}(Q)).$$

On a de plus

$$\sigma_v(L_v(t(Q)))^2 \mathfrak{p}(Q) \equiv 1 - s_2 t(Q)^2 \bmod t(Q)^3/3\, R_v[[t(Q)]].$$

Comme h_ρ est une fonction quadratique et vérifie $h_\rho(\pi P) = N(\pi) h_\rho(P)$, le théorème se déduit du lemme suivant

Lemme 8. Soit v une place de S.

1 - Si $f(t) \in 1 + t^3/3R_v[[t/3]]$, $\lim_{n\to\infty} \rho_v(f(t(p^n P)))/p^{2n} = 0$.

2 - Si $f(t) \in 1 + t^2/3R_v[[t/3]]$, $\lim_{n\to\infty} \rho_v(f(t(\pi^n P)))/N(\pi)^n = 0$.

3 - Si $d \in L_v^x$, $\lim_{n\to\infty} \rho_v(1 - dt(p^n P)^2)/p^{2n} = -r_v(dL_v(t(P))^2)$.

Démonstration. Pour n assez grand, l'unité $f(t(p^nP))$ (resp. $f(t(\pi^nP))$ dans le cas 2) est une unité de R_v congrue à 1 modulo v^{k_n} avec $k_n = 3\,v_L(p)n + c_o$ (resp. $2v_L(\pi)n + c_o$) et $c_o \in \mathbb{Z}$. Or l'homomorphisme ρ_v vérifie

$$\rho_v(U_v^{(v_L(p)k+c_o)}) \subset (p)^{k+c_1} \qquad \text{(pour } c_1 \in \mathbb{Z},\ k>>0),$$

si $U_v^{(m)}$ est comme d'habitude le groupe des unités de L_v congrues à 1 modulo v^m. On en déduit que

$$\rho_v(f(t(p^nP)))/p^{2n} \equiv 0 \bmod p^{n+c_1}$$

$$(\text{resp. } \rho_v(f(t(\pi^nP)))/N(\pi)^n \equiv 0 \bmod p^{v_L(\pi)/v_L(p)n+c_1}).$$

D'où les parties 1 et 2 du lemme 8. Pour démontrer 3, on remarque que

$$\rho_v(1 - dt(p^nP)^2) = r_v(\log_p(1 - dt(p^nP)^2))$$

pour n assez grand. Mais

$$\log_p(1 - dt(p^nP)^2) \equiv -dt(p^nP)^2 \bmod t(p^nP)^3\,\omega_{L,v}^c$$

(pour un $c \in \mathbb{Z}$). Comme d'autre part $L_v(t(P))$ est la limite de $t(p^nP)/p^n$ lorsque $n \longrightarrow \infty$, on en déduit le résultat.

Remarque. Dans le cas où p est inerte dans K (cas super-singulier), l'existence d'une fonction du type $\sigma_v(L_v(t))\exp(c_v L_v(t)^2)$ appartenant à $t(1 + tR_v[[t]])$ pour v divisant p n'a pas été montrée. Une telle fonction appartient en tout cas à $t(1 + tR_v\langle\langle t\rangle\rangle)$ où $R_v\langle\langle t\rangle\rangle$ désigne le sous-anneau de $L_v[[t]]$ formé des séries formelles $\Sigma\, a_n t^n$ avec $n!\, a_n \in R_v$. On peut construire une fonction h_ρ sur $E(L)$ à valeurs dans $\mathbb{Q}_p$ à partir de ces fonctions de la même manière qu'au paragraphe 1.3. Une telle fonction h_ρ est encore quadratique et vérifie

$$h_\rho(\alpha P) = N(\alpha)h_\rho(P) \qquad \text{pour } \alpha \in \mathcal{O}.$$

On peut alors montrer que

$$h_\rho(P) = \lim_{n\to\infty} m_\rho(p^nP)/p^{2n} + \sum_{v\in S_\rho} r_v(\alpha_v L_v(t(P))^2)$$

avec α_v défini par

$$\sigma_v(z)\exp(c_v z^2) = z\exp(\alpha_v z^2 + \dots)$$

c'est-à-dire $\alpha_v = -\frac{s_2}{2} + c_v$. La démonstration est identique lorsqu'on a remarqué que $v_L(\frac{t^n}{n!}) \geq v_L(\frac{t^3}{3!})$ pour $v_L(t)$ assez grand (indépendamment de n).

Revenons au cas décomposé. La démonstration du théorème 7 est tout à fait effective. Donnons un exemple. Supposons que E est défini sur K et prenons pour homomorphisme ρ l'homomorphisme $\log_p\kappa$. Si P est un point de $E_1(K)$ ne se réduisant pas en un point singulier du modèle, on a en choisissant π de valuation 1 sur K :

$$v_K(t(\pi P)) = v_K(t(P)) + 1 \qquad (v|p)\ ,$$

$$\sigma_v(L_v(t(P)))^2 x(P) \equiv 1 \bmod t(P)^h$$

avec $h=2$ en général, $h=3$ si $s_2 = a_1 = a_2 = 0$, $h=4$ si $s_2 = a_1 = a_2 = a_3 = 0$,

$$\log_{\mathfrak{p}}(1+z) \equiv z \bmod p^{v_K(z)+1} \qquad \text{si } v_K(z) > 0.$$

On en déduit que pour tout $n \geq 0$,

$$(4) \qquad h_K(P) \equiv \frac{1}{2p^n}\log_{\mathfrak{p}} a(\pi^n P) \text{ modulo } p^{(h-1)n+hv_K(t(P))}$$

où P est un point de $E_1(K)$ ne se réduisant pas en un point singulier de (1) et où $a(Q)$ désigne le numérateur de $x(Q)$ (défini à une racine de l'unité près de K).

La deuxième remarque qui facilite l'utilisation de cette formule pour calculer numériquement la hauteur d'un tel point est le fait classique que $a(\pi P)$ se calcule comme un polynôme en $a(P)$ et $b(P)^2 = a(P)x(P)^{-1}$ comme le montrera le lemme 9. Il est donc possible de calculer $a(\pi^n P)$ non pas en entier mais p-adiquement. Avant d'énoncer le lemme 9, faisons quelques rappels. Soit α un élément impair de O. La multiplication par α se décrit de la manière suivante. Il existe deux polynômes ψ_α et ϕ_α appartenant à $O[a_1,a_2,a_3,a_4,a_6,x]$ tels que

$$x(\alpha P) = \phi_\alpha(x(P))\psi_\alpha(x(P))^{-2}$$

et vérifiant les propriétés suivantes :

a) $\psi_\alpha(x)$ est de degré $\frac{N(\alpha)-1}{2}$ et $\phi_\alpha(x)$ est de degré $N(\alpha)$; ils sont homogènes en $a_1, \ldots a_6$ et x si l'on donne à a_i le poids i et à x le poids 2; le coefficient du terme de plus haut degré de ψ_α est α, celui de ϕ_α est 1;

b) ψ_α et ϕ_α sont premiers entre eux sur K et le restent sur tout corps résiduel de O où E a bonne réduction et dans lequel α est non nul.

Notons $\bar{\psi}_\alpha$ et $\bar{\phi}_\alpha$ les polynômes homogènes en deux variables (au sens ordinaire) associés à ψ_α et ϕ_α :

$$\bar{\psi}_\alpha(X,Z) = Z^{(N(\alpha)-1)/2}\,\psi_\alpha(X/Z)$$

$$\bar{\phi}_\alpha(X,Z) = Z^{N(\alpha)}\,\phi_\alpha(X/Z)$$

Lemme 9. Soit P un point de $E_1(K)$ ne se réduisant pas en un point singulier aux places de mauvaise réduction du modèle (1). Alors, on a

$$a(\pi P) = \bar{\phi}_\pi(a(P),b(P)^2) .$$

Démonstration. Posons $a = a(P)$, $b = b(P)$. Il suffit de montrer que les deux entiers $\bar{\phi}_\pi(a,b^2)$ et $b^2\bar{\psi}_\pi(a,b^2)$ de O sont premiers entre eux. Prenons d'abord $\mathfrak{q} = \mathfrak{p}$; comme il divise b et ne divise pas a, il ne peut diviser $\bar{\phi}_\pi(a,b^2)$. Supposons ensuite que $\mathfrak{q}$ est un idéal premier de O, premier à $\mathfrak{p}$ et pour lequel le modèle a bonne réduction. Les polynômes homogènes réduits de $Z\bar{\psi}_\pi(X,Z)^2$ et $\bar{\phi}_\pi(X,Z)$ étant premiers entre eux sur le corps résiduel $O/\mathfrak{q}$, $\mathfrak{q}$ ne divise pas le p.g.c.d. de $\bar{\phi}_\pi(a,b^2)$ et de $b^2\bar{\psi}_\pi(a,b^2)^2$.

Soit finalement $\mathfrak{q}$ un idéal premier de O où le modèle (1) de E a mauvaise réduction. On peut par un changement de modèle du type $x = x' + r$, $y = y' + sx' + t$ supposer que la réduction du modèle est $x^3 = y^2$, c'est-à-dire que $\mathfrak{q}$ divise a_i ($i = 1,2,3,4,6$). Si $\mathfrak{q}$ divise le p.g.c.d. de $\bar{\phi}_\pi(a,b^2)$ et de $b^2\bar{\psi}_\pi(a,b^2)$ dans l'ancien modèle, il le divise aussi dans le nouveau. Grâce à a), le p.g.c.d. de la réduction de $\bar{\phi}_\pi(X,Z)$ et de $Z\psi_\pi(X,Z)$ est X. Donc $\mathfrak{q}$ divise a et P se ré-

duit au point singulier qui est $(0,0)$.

Exemple 2. Montrons d'abord sur un exemple que l'hypothèse que P ne se réduit pas en point singulier est fondamentale pour la validité de la formule (4). Considérons la courbe $y^2 = x^3 - 49x$, $p = 5$ et les points

$$P_1 = \left(-\frac{49}{25}, \frac{24 \times 49}{125}\right), \quad P_2 = (25, 120), \quad P_3 = (0,0).$$

Le point P_3 est d'ordre 2 et on a les relations

$$P_2 + P_3 = P_1$$

$$x(2P_1) = x(2P_2) = \frac{337^2}{120^2}.$$

Le point P_1 est singulier et on a

$$\frac{1}{2} \log_5 a(P_1) \equiv 100 \bmod 125$$

$$\frac{1}{8} \log_5 a(2P_2) \equiv 60 \bmod 125,$$

donc $$h(P_1) = h(P_2) \equiv 60 \bmod 125$$

et $$h(P_1) \not\equiv \frac{1}{2} \log_5 a(P_1) \bmod 125.$$

Exemples 3. Donnons ici quelques valeurs de hauteurs de points pour des courbes elliptiques $y^2 = x^3 - dx$ à multiplication par $\mathbb{Z}[i]$ et de rang 1 sur $\mathbb{Q}$:

$y^2 = x^3 - 2x$	$P = (-1,1)$	$p = 5$	$h_K(P) \equiv 77 \bmod 625$	;
$y^2 = x^3 - 14x$,	$P = (8,20)$	$p = 5$	$h_K(P) \equiv 290 \bmod 625$	;
$y^2 = x^3 + 9x$,	$P = (4,10)$	$p = 5$	$h_K(P) \equiv 150 \bmod 625$	;
$y^2 = x^3 + 31x$,	$P = \left(\frac{25}{9}, \frac{280}{27}\right)$,	$p = 5$	$h_K(P) \equiv 250 \bmod 625$	;
$y^2 = x^3 - 54x$	$P = (27, 135)$,	$p = 5$	$\frac{1}{5} h_K(P) \equiv 5401 \bmod 15\,625$	

(rappelons que si $\pi = 2 + i$, on a

$$a(\pi P) = a(P)(a(P)^2 + (2i-1)db(P)^4)^2$$
$$b(\pi P) = ((2+i)a(P)^2 - idb(P)^4)b(P)^2) ;$$

$y^2 = x^3 - 2x$ $\quad P = (-1,1)$ $\quad 3P = \left(-\frac{1}{13^2}, \frac{239}{13^3}\right)$, $p = 13, h_K(P) \equiv 0 \bmod 13^4$;

$y^2 = x^3 - 2662x$ $\quad P = (-50,90)$ $\quad ,p = 5$ $\quad h_K(P) \equiv 220 \bmod 625$.

Exemples 4. Donnons quelques exemples choisis parmi les courbes $A(\ell)$; dans ce cas, l'entier h de la formule (4) est égal à 2 :

$$A(11) : P = (4,5), \quad x(9P) = \frac{4789}{100}, \quad p = 5, \quad h_K(P) \equiv 20 \bmod 25$$

$$x(5P) = -\frac{8}{9}, \quad p = 3, \quad h_K(P) \equiv 0 \bmod 9 .$$

Exemples 5. Donnons des exemples où le rang de $E(\mathbb{Q})$ est supérieur à 2.

$y^2 = x^3 + 14x$; $P_1 = (2,6)$, $P_2 = (\frac{1}{4}, \frac{15}{8})$; le rang de $E(\mathbb{Q})$ est 2; prenons toujours $p = 5$; alors la matrice

$$\langle P_i , P_j \rangle_{K,\mathfrak{p}}$$

est congrue modulo 625 à

$$\begin{pmatrix} 80 & 340 - 120i \\ 340 + 120i & 290 \end{pmatrix} ,$$

et son déterminant est congru à 25×103 modulo 5^5.

$y^2 = x^3 - 226x$: un système libre maximal de $E(\mathbb{Q})$ est $P_1 = (-1,15)$, $P_2 = (\frac{121}{4}, \frac{1155}{8})$, $P_3 = (-8,36)$; la matrice de $\langle , \rangle_{K,\mathfrak{p}}$ pour ce système est

$$\begin{pmatrix} 5 \times 38 & 5 \times 53 & 5 \times 5 \\ 5 \times 102 & 5 \times 80 & 5 \times 100 \\ 5 \times 53 & 5 \times 84 & 5 \times 113 \end{pmatrix} \quad \text{modulo } 625$$

pour $\mathfrak{p} = (2 - i)$ (calculs effectués par D. Bernardi); le déterminant est donc congru à $5^3 \times 107$ modulo 5^6.

Note. Une généralisation de ce paragraphe se trouve dans "Hauteurs p-adiques", Séminaire de Théorie des Nombres 1982-83, à paraître dans Birkhäuser.

Chapitre IV. Hauteurs algébrique et analytique associées à la $\mathbb{Z}_p$-extension N_∞.

Dans ce chapitre, nous construisons une forme bilinéaire algébrique canonique attachée à la $\mathbb{Z}_p$-extension N_∞ qui permet de calculer une partie de la série caractéristique du dual de Pontryagin $Y(N_\infty)$ de $S(N_\infty)$ et nous la lions à la hauteur p-adique analytique associée au caractère κ définie dans le chapitre précédent. Le point de départ de cette construction est la suite exacte (1) de la proposition 1, obtenue grâce à une exploitation de la théorie de Kummer sur la courbe elliptique et de la théorie multiplicative. Cette suite exacte permet de relier entre eux des groupes de Selmer relatifs à $\mathfrak{p}$ et à $\mathfrak{p}^*$. On l'utilisera de nouveau dans le chapitre V pour construire un pseudo-isomorphisme entre $Y(F_\infty)$ et l'adjoint de $Y^*(F_\infty)$ et pour attacher à chaque $\mathbb{Z}_p$-extension une forme bilinéaire. Le contenu de ce chapitre est dans [26].

1. Hauteurs algébriques.

1.1. Suite exacte fondamentale.

Nous utiliserons dans tout ce chapitre les notations suivantes : on pose

$$N_n = F(E_{\pi^n}), \quad F_n = F(E_{q^n}), \quad G_n = G(N_n/F), \quad \Gamma = G(N_\infty/F).$$

Soit I_n le groupe des idèles de N_n, V_n le sous-groupe des idèles de N_n dont les composantes sont égales à 1 en toute place divisant $\mathfrak{p}$ et une unité ailleurs. On pose

$$C_n = I_n / V_n N_n^\times, \quad \Omega_n = \prod_{v|\mathfrak{p}} \mu_{q^n}(N_{n,v}).$$

Ce dernier groupe est d'ordre borné. Le noyau de l'homomorphisme naturel

$$\mathrm{Hom}(E_{\pi^n}, \Omega_n) \longrightarrow \mathrm{Hom}(E_{\pi^n}, C_n)$$

est $\mathrm{Hom}(E_{\pi^n}, \mu_{q^n}(N_n))$.

Proposition 1. Il existe une suite exacte naturelle

$$(1) \quad 0 \to \mathrm{Hom}(E_{\pi^n}, \mu_{q^n}(N_n))^{G_n} \to \mathrm{Hom}(E_{\pi^n}, \Omega_n)^{G_n} \to \mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} \to \Sigma(F)^{(\pi^{*n})} \to 0.$$

On notera η_n l'homomorphisme $\mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} \longrightarrow \Sigma(F)^{(\pi^{*n})}$.

Le reste de ce paragraphe est consacré à la démonstration de la proposition et aux propriétés de fonctorialité par changement de corps. Les corollaires et la construction de la forme bilinéaire algébrique annoncée seront donnés dans le paragraphe 1.2.

On définit d'abord l'accouplement de Weil

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

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 N_n de diviseur

$$q^n((u) - (0))$$

(resp.

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

On a évidemment la relation

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

donc quitte à changer $f_{n,u}$ par une constante, on peut supposer que

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

On pose alors

$$W_n(u,v) = g_{n,u}(P+v) \,/\, g_{n,u}(P). \tag{2}$$

Propriétés 2. 1 - L'accouplement W_n définit un isomorphisme de $G(\bar{F}/F)$-modules

$$E_{\pi^{*n}} \longrightarrow \mathrm{Hom}(E_{\pi^n}, \mu_{q^n})$$

$$v \longmapsto (u \longmapsto W_n(u,v)) \; .$$

2 - Si α appartient à O, $W_n(\alpha u, v) = W_n(u, \alpha^* v)$.

3 - Si u appartient à E_{π^n} et v à $E_{\pi^{*n}}$,

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

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

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

On analyse maintenant les propriétés des éléments de $\Sigma(N_n)^{(\pi^{*n})}$ et de $\Sigma(F)^{(\pi^{*n})}$.

Lemme 3. On a un isomorphisme de $G(N_n/F)$-modules

$$H^1(N_n, E_{\pi^{*n}}) \longrightarrow \mathrm{Hom}(E_{\pi^n}, N_n^\times / N_n^{\times q^n})$$

que l'on notera $f \longmapsto \tilde{f}$.

Démonstration. Le lemme II.15 montre la nullité de

$$H^i(F_n/N_n, E_{\pi^{*n}})$$

pour $i \geq 1$. On en déduit que l'homomorphisme de restriction

$$H^1(N_n, E_{\pi^{*n}}) \longrightarrow H^1(F_n, E_{\pi^{*n}})^{G(F_n/N_n)}$$

est un isomorphisme. Mais l'on a

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

L'accouplement de Weil W_n induit alors un isomorphisme

$$H^1(F_n, E_{\pi^{*n}}) \longrightarrow \mathrm{Hom}(E_{\pi^n}, H^1(F_n, \mu_{q^n})).$$

Toujours grâce au lemme II.15, les groupes $H^1(F_n, \mu_{q^n})^{G(F_n/N_n)}$ et $H^1(N_n, \mu_{q^n})$ sont isomorphes car $F_n = N_n(\mu_{q^n})$. La théorie de Kummer multiplicative donne alors un isomorphisme de $H^1(N_n, \mu_{q^n})$ dans $N_n^x/N_n^{xq^n}$. D'où le lemme 3.

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

Lemme 4. Pour toute place v de N_n, on a un isomorphisme canonique

$$H^1(N_{n,v}, E_{\pi^{*n}}) \longrightarrow \mathrm{Hom}(E_{\pi^n}, N_{n,v}^x/N_{n,v}^{xq^n}).$$

Par définition, un élément h de $H^1(N_n, E_{\pi^{*n}})$ appartient à $\Sigma(N_n)^{(\pi^{*n})}$ si et seulement si ses images par localisation appartiennent à $E(N_{n,v})/\pi^{*n}E(N_{n,v})$ 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 $N_{n,v}^{xq^n}$ pour $u \in E_{\pi^n}$. 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^x/k^{xq^n}.

Lemme 5. Soit v une place de N_n ne divisant pas $\mathfrak{p}$. On a l'isomorphisme

$$E(N_{n,v})/\pi^{*n}E(N_{n,v}) \longrightarrow \mathrm{Hom}(E_{\pi^n}, U(N_{n,v})/U(N_{n,v})^{q^n}).$$

Démonstration. Considérons les deux suites exactes :

$$0 \longrightarrow E(N_{n,v})/\pi^n E(N_{n,v}) \longrightarrow H^1(N_{n,v}, E_{\pi^n}) \longrightarrow H^1(N_{n,v}, E)_{\pi^n} \longrightarrow 0$$

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

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

$$E(N_{n,v})/\pi^{*n}E(N_{n,v})$$

est exactement

$$E(N_{n,v})/\pi^n E(N_{n,v})$$

(dualité de Tate, [35]). Soit $N_{n,v}^{nr}$ l'extension non ramifiée maximale de $N_{n,v}$. Comme v ne divise pas $\mathfrak{p}$, la suite

$$0 \longrightarrow E_{\pi^n} \longrightarrow E(N_{n,v}^{nr}) \longrightarrow E(N_{n,v}^{nr}) \longrightarrow 0$$

est exacte. On déduit alors de la nullité de

$$H^1(N_{n,v}^{nr}/N_{n,v},\ E(N_{n,v}^{nr}))$$

l'isomorphisme

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

L'orthogonal de ce dernier groupe dans

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

est alors exactement par la théorie du corps de classe local

$$\mathrm{Hom}(E_{\pi^n}, U(N_{n,v})/U(N_{n,v})^{q^n}),$$

ce qui démontre le lemme.

Rappelons que si h est un élément de $H^1(N_n, E_{\pi^{*n}})$, $\tilde{h}$ est son image dans $\mathrm{Hom}(E_{\pi^n}, N_n^{\times}/N_n^{\times q^n})$. Le lemme 5 admet comme corollaire le lemme suivant.

Lemme 6. *Un élément h de $H^1(N_n, E_{\pi^{*n}})$ appartient à $\Sigma(N_n)^{(\pi^{*n})}$ si et seulement si $\tilde{h}(u)$ appartient à $N_{n,v}^{\times q^n}$ pour toute place v divisant $\mathfrak{p}$ et si $v_{N_n}(h(u))$ est divisible par q^n pour toute place v (pour u quelconque dans E_{π^n}).*

Nous allons donner maintenant la description de l'homomorphisme η_n. Remarquons que dans le cas où $E(F)$ contient E_{π^n} c'est-à-dire dans le cas où F est égal à N_n, elle se fait facilement de la manière suivante. Notons d_n la projection sur $\bar{F}^{\times}$ du produit direct $\bar{F}^{\times}V_n$ considéré comme un sous-groupe de la réunion des groupes d'idèles des exten-

sions finies de F contenues dans $\bar{F}$. Soit f un élément de $\mathrm{Hom}(E_{\pi^n}, C_n)^{G_n}$. Si u appartient à E_{π^n}, soit f'_u un représentant de $f(u)$ dans I_n. Alors,

$$d_n(f'^{q^n}_u) = a_u \quad \text{avec} \quad a_u \in N_n^{\times} ;$$

a_u est défini modulo $N_n^{\times q^n}$ et vérifie les propriétés du lemme 6. Il existe donc un élément h de $\Sigma(N_n)^{(\pi^{*n})}$ tel que

$$\tilde{h}(u) \equiv a_u \mod N_n^{\times q^n}.$$

On vérifie alors facilement que l'application $f \longmapsto h$ vérifie les propriétés demandées pour η_n. Dans le cas général, nous démontrerons la proposition 1 de deux manières différentes. La première est simplement un raffinement algébrique de l'argument précédent; la seconde qui nous a été indiquée par P. Billot est plus dans la ligne des théorèmes de dualité globale (voir par exemple [28]) mais utilise la théorie du corps de classe globale. Remarquons que la démonstration de P. Schneider dans le le cas sans multiplication complexe utilise les théorèmes de dualité plate de Artin et Mazur et semble être une généralisation de cette seconde méthode.

Considérons le composé des homomorphismes

$$\mathrm{Hom}(E_{\pi^n}, C_n) \longrightarrow \mathrm{Ext}^1(E_{\pi^n}, N_n^{\times} V_n) \xrightarrow{d_n} \mathrm{Ext}^1(E_{\pi^n}, N_n^{\times})$$

et soit g l'image d'un élément f de $\mathrm{Hom}(E_{\pi^n}, C_n)^{G_n}$. Si f'_u est un représentant de $f(u)$ dans I_n, c'est par définition la classe de

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

D'autre part, comme $\bar{F}^{\times}$ est p-divisible, l'homomorphisme de connection

$$\mathrm{Hom}(E_{\pi^n}, \bar{F}^{\times}/N_n^{\times}) \longrightarrow \mathrm{Ext}^1(E_{\pi^n}, N_n^{\times})$$

est surjectif. Donc il existe un élément β de $\mathrm{Hom}(E_{\pi^n}, \bar{F}^{\times}/N_n^{\times})$ 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 que l'application $u \longrightarrow f'_u \beta'^{-1}_u$ soit un homo-

morphisme de E_{π^n} à valeurs dans $I_n\bar{F}^x/V_n$. De plus, deux tels choix de β'_u diffèrent d'un homomorphisme de E_{π^n} dans $\bar{F}^x$. 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 $\bar{F}^x V_n$ pour $\sigma \in G(\bar{F}/F)$. Notons $t_u(\sigma)$ sa projection sur $\bar{F}^x$. Alors $u \longrightarrow t_u(\sigma)$ est un homomorphisme de E_{π^n} dans $\bar{F}^x$ (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 $E_{\pi^{*n}}$. Sa classe $\bar{s}$ dans $H^1(F,E_{\pi^{*n}})$ ne dépend que de f. On vérifie facilement que la restriction de $\bar{s}$ à $H^1(N_n,E_{\pi^{*n}})$ est exactement l'élément h construit précédemment et que $\bar{s}$ appartient en fait à $\Sigma(F)^{(\pi^{*n})}$. En posant $\eta_n(f) = \bar{s}$, on définit ainsi un homomorphisme η_n

$$\eta_n : \mathrm{Hom}(E_{\pi^n},C_n)^{G_n} \longrightarrow \Sigma(F)^{(\pi^{*n})}.$$

Le calcul du noyau se fait aisément. Nous allons plutôt détailler 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 $\beta'_u \in \bar{F}^x$ tel que $t_u(\sigma) = \sigma\beta'_u/\beta'_u$ pour $\sigma \in G(\bar{F}/N_n)$. De plus,

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

appartient à $N_{n,v}^{\times q^n}$ pour toute place divisant $\mathfrak{p}$ et est de valuation divisible par q^n pour les autres places par le lemme 6. D'autre part, la restriction de s à $G(\bar{F}_v/F_v)$ étant un cobord pour v divisant $\mathfrak{p}$,

on a

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

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_o de v à $\bar{F}$, on a

$$(3) \qquad c_{\sigma,u} = \sigma(\beta'_{\sigma^{-1}u}\,\zeta_v(\sigma^{-1}u)^{-1})/(\beta'_u\,\zeta_v(u)^{-1}) \quad \text{pour} \quad \sigma \in G(\bar{F}_{v_o}/F_v)\ .$$

On définit maintenant un idèle f'_u de N_n par

$$(f'_u)_w = 1 \qquad \text{si} \quad w|\infty$$

$$w_{N_n}((f'_u)_w) = w_{N_n}(a_u)/q^n \qquad \text{si} \quad w\nmid\mathfrak{p}\,,\ w\neq\infty$$

$$(f'_u)_{v_o} = \zeta_v(u)^{-1}\,\beta'_u \qquad \text{si} \quad v|\mathfrak{p}$$

$$(f'_u)_w = \sigma(f'_{\sigma^{-1}u})_{v_o}\, c^{-1}_{\sigma,u} \qquad \text{si} \quad w|\mathfrak{p}\ \ w = \sigma v_o$$

La relation (3) assure que f'_u appartient à I_n, que sa classe $f(u)$ dans C_n ne dépend pas des choix de v_o et de σ et que $u \longrightarrow f(u)$ est un élément de

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

tel que $\eta_n(f) = \bar{s}$, ce qui termine la première démonstration de la proposition 1.

Comme annoncé, nous allons maintenant en donner une seconde.

Soit M_∞ la p-extension non ramifiée au dehors de p de F maximale. De manière analogue au théorème II-18, on montre que $S(F)^{(\pi^{*n})}$ est contenu dans $H'(M_\infty/F, E_{\pi^{*n}})$. D'autre part, le groupe $U(N_{n,v})/U(N_{n,v})^{q^n}$ fait partie d'une suite exacte analogue à (II,7). En effet la suite

$$(4)\quad 0 \longrightarrow U(N_{n,v})/U(N_{n,v})^{q^n} \longrightarrow N_{n,v}^{\times}/N_{n,v}^{\times q^n} \longrightarrow H^1(N_{n,v},U(\bar{N}_{n,v}))_{q^n} \longrightarrow 0$$

est exacte (elle se déduit de la suite exacte de cohomologie de la suite exacte

$$0 \longrightarrow \mu_{q^n} \longrightarrow U(\bar{N}_{n,v}) \longrightarrow U(\bar{N}_{n,v}) \longrightarrow 0).$$

Les lemmes 4 et 5 et la suite exacte (4) donnent alors l'idée d'introduire l'homomorphisme naturel

$$(5)\qquad H^1(M_\infty/F,E_{\pi^{*n}}) \longrightarrow \prod_{v|\mathfrak{p}^*} \mathrm{Hom}(E_{\pi^n},H^1(N_{n,v},U(\bar{N}_{n,v}))) .$$

Il est en fait facile de voir que $\Sigma(F)^{(\pi^{*n})}$ est égal à l'intersection du noyau de l'homomorphisme (5) et du noyau de l'homomorphisme

$$(6)\qquad H^1(M_\infty/F,E_{\pi^{*n}}) \longrightarrow \prod_{v|\mathfrak{p}} H^1(F_v,E_{\pi^{*n}})$$

Nous allons maintenant mettre (6) dans une suite exacte. Introduisons d'abord quelques notations complémentaires. Si L est une extension de F contenue dans M_∞, notons $E_{\mathfrak{p}}(L)$ le groupe des $\mathfrak{p}$-unités de L (c'est-à-dire des éléments de L qui sont des unités au dehors des places divisant $\mathfrak{p}$), $I_{L,\mathfrak{p}}$ le groupe des $\mathfrak{p}$-idèles de L (c'est-à-dire des idèles dont les composantes sont 1 aux places non divisibles par $\mathfrak{p}$) et V_L le sous-groupe des idèles de L dont les composantes sont égales à 1 en toute place divisant $\mathfrak{p}$ et une unité ailleurs.

Lemme 7. La suite

$$(7)\quad 0 \longrightarrow \mathrm{Hom}(E_{\pi^n},E_{\mathfrak{p}}(M_\infty)) \longrightarrow \mathrm{Hom}(E_{\pi^n},I_{M_\infty,\mathfrak{p}}) \longrightarrow \mathrm{Hom}(E_{\pi^n},C_{M_\infty}) \longrightarrow 0$$

est exacte (avec $C_{M_\infty} = I_{M_\infty}/M_\infty^{\times} V_{M_\infty}$).

Démonstration. On montre d'abord que la suite

$$0 \longrightarrow E_{\mathfrak{p}}(M_\infty) \longrightarrow I_{M_\infty,\mathfrak{p}} \longrightarrow C_{M_\infty} \longrightarrow 0$$

est exacte. Le seul point délicat est la surjectivité. Soit $\bar{x}$ un élément de C_{M_∞} et (x_v) un représentant de x dans le groupe des idèles I_L d'une extension finie de F. Quitte à passer au corps de Hilbert de

L, on peut supposer que x_v est une unité pour toute place v et $\bar{x}$ est donc représenté par un élément de $I_{L,\mathfrak{p}}$ modulo V_L. On en déduit alors le lemme 7 en remarquant que $E_{\mathfrak{p}}(M_\infty)$ est un groupe divisible par p.

En prenant les invariants de la suite exacte (7) par $G(M_\infty/F)$, on obtient la suite exacte

$$\mathrm{Hom}(E_{\pi^n}, I_{M_\infty,\mathfrak{p}})^{G(M_\infty/F)} \longrightarrow \mathrm{Hom}(E_{\pi^n}, C_{M_\infty})^{G(M_\infty/F)} \longrightarrow H^1(M_\infty/F, E_{\pi^{*n}}) \downarrow \prod_{v|\mathfrak{p}} H^1(F_v, E_{\pi^{*n}})$$

De la nullité du groupe de cohomologie $H^1(M_\infty/N_n, I_{M_\infty}/M_\infty^\times)$ par la théorie du corps de classes, on déduit la suite exacte

$$(8) \qquad 0 \longrightarrow C_n \longrightarrow C_{M_\infty}^{G(M_\infty/N_n)} \longrightarrow H^1(M_\infty/N_n, V_{M_\infty}) \longrightarrow 0.$$

On voit alors que $H^1(M_\infty/N_n, V_{M_\infty}) = \prod_{v|\mathfrak{p}^*} H^1(M_{\infty,v}/N_{n,v}, U(M_{\infty,v}))$,

l'extension M_∞/N_n étant non ramifiée au dehors de p. On a alors le diagramme commutatif exact suivant

$$\begin{array}{ccccc} 0 & & & & \\ \downarrow & & & & \\ \mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} & & & & \\ \downarrow & & & & \\ \mathrm{Hom}(E_{\pi^n}, C_{M_\infty})^{G(M_\infty/F)} & \longrightarrow & H^1(M_\infty/F, E_{\pi^{*n}}) & \longrightarrow & \prod_{v|\mathfrak{p}} H^1(F_v, E_{\pi^{*n}}) \\ \downarrow & & \downarrow & & \\ \mathrm{Hom}(E_{\pi^n}, \prod_{v|\mathfrak{p}^*} H^1(N_{n,v}, U(\bar{N}_{n,v}))) & \longrightarrow & \prod_{v|\mathfrak{p}^*} \mathrm{Hom}(E_{\pi^n}, H^1(N_{n,v}, U(\bar{N}_{n,v}))) & & \end{array}$$

et la suite exacte (1) se déduit de ce diagramme et de la suite exacte (8).

Nous allons maintenant comparer les homomorphismes η_n lorsque n varie ou lorsque le corps de base change. Notons $N_{n,n-1}$ la norme de N_n à N_{n-1} (sur C_n ou sur $N_n^\times$).

Lemme 8. Pour n assez grand, il existe un unique homomorphisme t_n

$$t_n : \mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} \longrightarrow \mathrm{Hom}(E_{\pi^{n-1}}, C_{n-1})^{G_{n-1}}$$

vérifiant

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

On a pour cela besoin du lemme.

Lemme 9. Soit i_n l'homomorphisme de C_{n-1} dans C_n induit par l'inclusion $I_{n-1} \longrightarrow I_n$. Pour n assez grand, i_n est injectif sur $(C_{n-1})_{q^n}$.

Démonstration. Soit x un élément de I_{n-1} tel que

$$x^{q^n} = ay \quad \text{avec} \quad a \in N_{n-1}^{\times}, \ y \in V_{n-1}$$

$$x = bz \quad \text{avec} \quad b \in N_n^{\times}, \ z \in V_n .$$

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

$$H^1(N_n/N_{n-1}, \mu_{q^n}(N_n)) \longrightarrow \prod_{v|\mathfrak{p}} H^1(N_{n,v}/N_{n-1,v}, \mu_{q^n}(N_{n,v}))$$

est nul pour n assez grand. Cela implique que a appartient à $N_{n-1}^{\times q^n}$ et que x appartient à $N_{n-1}^{\times} V_n$.

Démonstration du lemme 8. 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 9, il suffit de montrer que

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

Mais cela est égal à

$$\prod_{\sigma \in G(N_n/N_{n-1})} \sigma h(u) = h(u)^q = 1.$$

On montre facilement les trois lemmes suivants.

Lemme 10. Si r_n est l'homomorphisme

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

induit par la multiplication par π^*, on a

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

Lemme 11. L'homomorphisme $\Sigma(F)^{(\pi^{*n})} \longrightarrow \Sigma(F)^{(\pi^{*n+1})}$ induit par l'inclusion $E_{\pi^{*n}} \longrightarrow E_{\pi^{*n+1}}$ et l'homomorphisme

$$\mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} \longrightarrow \mathrm{Hom}(E_{\pi^{n+1}}, C_{n+1})^{G_{n+1}}$$

$$\phi \longmapsto (u \longmapsto i_n(\phi(\pi u)))$$

font commuter le diagramme

$$\begin{array}{ccc} \mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} & \xrightarrow{\eta_n} & \Sigma(F)^{(\pi^{*n})} \\ \downarrow & & \downarrow \\ \mathrm{Hom}(E_{\pi^{n+1}}, C_{n+1})^{G_{n+1}} & \xrightarrow{\eta_{n+1}} & \Sigma(F)^{(\pi^{*n+1})} \end{array} .$$

Lemme 12. (changement de corps de base). Soit L une extension finie de F. L'homomorphisme restriction

$$\Sigma(F)^{(\pi^{*n})} \longrightarrow \Sigma(L)^{(\pi^{*n})}$$

et l'homomorphisme

$$\mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} \longrightarrow \mathrm{Hom}(E_{\pi^n}, C(LN_n))^{G(N_nL/L)}$$

induit par l'inclusion du groupe des idèles de N_n dans celui de LN_n font commuter le diagramme

$$\begin{array}{ccc} \mathrm{Hom}(E_{\pi^n}, C_n)^{G_n} & \xrightarrow{\eta_n} & \Sigma(F)^{(\pi^{*n})} \\ \downarrow & & \downarrow \\ \mathrm{Hom}(E_{\pi^n}, C(N_n L)^{G(N_n/L)} & \xrightarrow{\eta_n(L)} & \Sigma(L)^{(\pi^{*n})} \end{array}$$

(avec des notations évidentes).

1.2. Corollaires et hauteurs algébriques.

Soit η_n' l'homomorphisme déduit de η_n par passage au quotient par le noyau de η_n et posons

$$\Xi_n = \delta^{-1}\pi^{*-n}\eta_n'^{-1}$$

où δ est le degré de l'extension $F(E_\mathfrak{p})/F$. Rappelons que l'on a noté $\overset{\vee}{\Sigma}{}^*(F)$ la limite projective de $\Sigma(F)^{(\pi^{*n})}$.

Proposition 13. Les homomorphismes Ξ_n forment un système compatible d'homomorphismes qui induisent un isomorphisme Ξ_F

$$\Xi_F : \overset{\vee}{\Sigma}{}^*(F) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \varprojlim C_n(p))^{G(N_\infty/F)}$$

où la limite projective des $C_n(p)$ est prise relativement à la norme.

Démonstration. La première partie de la proposition se déduit du lemme 10. 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

$$\varprojlim \mathrm{Hom}(E_{\pi^n}, C_n)^{G(N_\infty/F)}.$$

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

$$\varprojlim \mathrm{Hom}(T_\pi, (C_n)_{q^n})^{G(N_\infty/F)} = \varprojlim \mathrm{Hom}(T_\pi, C_n(p))^{G(N_\infty/F)}.$$

En effet, si (f_n) est un élément de ce dernier groupe, l'image de f_n dans C_n est nécessairement d'ordre divisant q^n car f_n est invariant par $G(N_\infty/N_n)$:

$$\gamma f_n = f_n = f_n^{\kappa(\gamma)} \qquad \text{pour} \quad \gamma \in G(N_\infty/N_n)$$

et $\kappa(\gamma)$ est exactement congru à 1 modulo q^n pour γ générateur de $G(N_\infty/N_n)$. D'où la proposition.

Rappelons que l'on a noté M_n la p-extension abélienne non ramifiée au dehors de $\mathfrak{p}$ maximale de N_n et X_n le groupe de Galois de M_n sur N_n. L'homomorphisme d'Artin $(\ ,M_n/N_n)$ induit un homomorphisme surjectif de $I_n/\overline{V_n N_n^\times}$ sur X_n de noyau fini d'ordre premier à p. On en déduit un homomorphisme surjectif

$$A : \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \varprojlim C_n(p)) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \varprojlim X_n(p)) .$$

Remarquons que l'on a l'égalité

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \varprojlim X_n(p))^{G(N_\infty/F)} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, X(N_\infty))^{G(N_\infty/F)}$$

où $X(N_\infty)$ est la limite projective des X_n : un élément de ce dernier groupe est en effet toujours d'ordre fini. Le composé $\Phi_F = A \circ \Xi_F$ est donc un homomorphisme surjectif de $\overset{v}{\Sigma}{}^*(F)$ sur $\mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, X(N_\infty))^{G(N_\infty/F)}$. Rappelons que, d'après le théorème II.18, $\mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, X(N_\infty))$ est le dual de Pontryagin $Y(N_\infty)$ de $S(N_\infty)$.

Théorème 14. <u>L'homomorphisme</u> Φ_F

$$\Phi_F : \overset{v}{\Sigma}{}^*(F) \longrightarrow Y(N_\infty)^\Gamma$$

<u>est un isomorphisme si et seulement si</u> N_∞ <u>vérifie l'hypothèse</u> $\mathfrak{p}$-<u>adique de Leopoldt</u>.

<u>Démonstration</u>. Notons E_n le groupe des unités globales de N_n congrues à 1 modulo toute place v au dessus de $\mathfrak{p}$ et $\bar{E}_n$ son adhérence dans $\prod_{v|\mathfrak{p}} U(N_{n,v})$. Le $\mathbb{Z}$-module $\bar{E}_n/E_n$ est p-divisible car $\bar{E}_n = E_n \bar{E}_n^{p^r}$ pour tout entier r. On a donc la suite exacte

(9) $$0 \longrightarrow \bar{E}_n/E_n(p) \longrightarrow C_n(p) \longrightarrow (I_n/\overline{V_n N_n^\times})(p) \longrightarrow 0 .$$

De plus, si l'on pose $M(-1) = \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, M)$ pour un Λ_Γ-module M, $\bar{E}_n/E_n(p)(-1)_\Gamma$ est nul. En effet, si γ appartient à G_n, $\kappa(\gamma)^{-1}\gamma - 1$ agit sur $\bar{E}_n/E_n$ comme une puissance de p à un automorphisme près et $\bar{E}_n/E_n$ est p-divisible. On a donc la suite exacte (à l'aide de l'homomorphisme d'Artin) :

$$0 \longrightarrow \bar{E}_n/E_n(p)(-1)^\Gamma \longrightarrow C_n(p)(-1)^\Gamma \longrightarrow X_n(p)(-1)^\Gamma \longrightarrow 0 .$$

Le théorème 14 est alors équivalent au lemme suivant.

Lemme 15. Le groupe $\varprojlim \bar{E}_n/E_n(p)(-1)^\Gamma$ est nul si et seulement si N_∞ vérifie l'hypothèse $\mathfrak{p}$-adique de Leopoldt.

Démonstration. Supposons d'abord l'hypothèse de Leopoldt vérifiée pour N_∞. Si E_n' est le quotient de E_n par son sous-groupe de torsion, on a

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

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

(10) $$(\bar{E}_n'/E_n')_{q^n} = (\bar{E}_r'/E_r')_{q^n}$$

Soit $(e_1,\ldots,e_{h_n})$ une base du $\mathbb{Z}$-module E_n' telle que $e_1' = e_1^{a_1},\ldots,$ $e_h' = e_h^{a_h}$ soit une $\mathbb{Z}$-base de 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 $\overline{E_n'}$.

Soit x un élément de $\overline{E_n'}$ tel que x^{q^n} appartient à 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 $y^S \in \widetilde{E_r'}$, $\beta_i' \in \mathbb{Z}$. Comme $\widetilde{E_r'}/E_r'$ est un $\mathbb{Z}$-module p-divisible, x est donc congru à un élément de $\widetilde{E_r'}$ modulo E_n'. D'où l'égalité (10). On en déduit que $\widetilde{E_n'}/E_n'(-1)^\Gamma$ est fini d'ordre borné par rapport à n et que la limite projective des $\widetilde{E_n'}/E_n'(-1)^\Gamma$ est nulle.

Réciproquement, supposons que $\varprojlim \widetilde{E_n'}/E_n'(-1)^\Gamma$ n'est pas réduit à 1. Nous allons montrer que pour tout $r\geq 0$, il existe $n\geq r$ et un élément de $(\widetilde{E_n'}/E_n')_{q^n}$ n'appartenant pas à $(\widetilde{E_r'}/E_r)_{q^n}$, ce qui contredira (10) et finira la démonstration du lemme 15. Soit $x=(x_n)$ un élément de $\varprojlim \widetilde{E_n'}/E_n'(-1)^\Gamma$ différent de 1; supposons que x_n appartient à $\widetilde{E_r'}/E_r'$ pour tout $n\geq r$. L'équation

$$\gamma x_n = x_n^{\kappa(\gamma)} \qquad \text{pour } \gamma \in G(N_\infty/N_r)$$

implique que $x_n^{q^r} = 1$. On a d'autre part

$$N_{n,n-1}(x_n) = x_n^{qu} \qquad \text{avec } u \in \mathbb{Z}_p^\times .$$

On en déduit que $x_r = 1$ ce qui est absurde.

Les trois corollaires suivants du théorème 14 sont donnés sous l'hypothèse $\mathfrak{p}$-adique de Leopoldt pour N_∞.

Corollaire 16. 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

$$(11) \qquad 0 \longrightarrow E_1(F) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*} \longrightarrow \overset{\vee}{\Sigma}{}^*(F) \longrightarrow T_{\pi^*}(Ш(F))$$

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

$$E(F) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*} \longrightarrow \prod_{v|\mathfrak{p}} E(F_v) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}.$$

Comme $E(F_v) \otimes_{\mathcal{O}_v} \mathcal{O}_{\mathfrak{p}^*}$ est fini pour toute place v divisant $\mathfrak{p}$, le rang sur $\mathbb{Z}_p$ de $\Sigma^*(F)$ est égal à la somme du $\mathcal{O}$-rang n_F de $E(F)$ et du rang sur $\mathbb{Z}_p$ de $\widehat{Ш(F)(\mathfrak{p}^*)}$. D'autre part, comme $Y(N_\infty)$ est un Λ_Γ-module de torsion, les $\mathbb{Z}_p$-rangs de $Y(N_\infty)_\Gamma$ et de $Y(N_\infty)^\Gamma$ sont égaux, et égaux à la somme du rang sur $\mathbb{Z}_p$ de $\widehat{Ш(F)(\mathfrak{p})}$ et de n_F. L'isomorphisme Φ_F entre $\overset{\vee}{\Sigma}{}^*(F)$ et $Y(N_\infty)^\Gamma$ permet alors de terminer la démonstration.

Corollaire 17. Le Λ_Γ-module $Y^*(N_\infty)$ est un Λ_Γ-module de type fini et de Λ_Γ-torsion.

Démonstration. Grâce au corollaire 16, 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. D'autre part, l'homomorphisme de restriction

$$S^*(L) \longrightarrow S^*(N_\infty)^{G(N_\infty/L)}$$

a un noyau et conoyau finis. On en déduit que le $\mathbb{Z}_p$-rang de $Y^*(N_\infty)_{G(N_\infty/L)}$ est borné lorsque L parcourt les extensions finies de F contenues dans N_∞ et donc que $Y^*(N_\infty)$ est de Λ_Γ-torsion.

Corollaire 18. Si $Ш(F)(\mathfrak{p})$ est fini, les $\mathbb{Z}_p$-modules $E_1(F) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}$ et $Y(N_\infty)^\Gamma$ sont canoniquement isomorphes.

Démonstration. L'hypothèse implique que $T_\pi(Ш(F))$ et $T_{\pi^*}(Ш(F))$ sont nuls. On utilise alors la suite exacte (11) et le théorème 14.

On construit maintenant à partir de l'homomorphisme Φ_F une forme bilinéaire

$$B_{F,\mathfrak{p}} : \overset{\vee}{S}(F) \times \overset{\vee}{S}{}^*(F) \longrightarrow \mathbb{Q}_p$$

que nous noterons B_F lorsqu'il n'y aura pas de confusion possible.

Si M est un $\mathbb{Z}_p$-module, on note $\mathrm{div}(M)$ le sous-groupe p-divisible maximal de M et M/div le quotient de M par $\mathrm{div}(M)$. Rappelons que nous avons montré (proposition II.16) l'existence d'un homomorphisme surjectif de $Y(N_\infty)$ sur $\widehat{S'(F)}$. En le composant avec l'homomorphisme surjectif évident

$$\widehat{S'(F)} \longrightarrow \widehat{\mathrm{div}(S'(F))}$$

et en prenant les invariants par Γ, on construit l'homomorphisme α_F

$$\alpha_F : Y(N_\infty)^\Gamma \longrightarrow \widehat{\mathrm{div}(S'(F))} .$$

D'autre part, $\mathrm{div}(S'(F))$ est égal à $\mathrm{div}(S(F))$ et son dual de Pontryagin est canoniquement isomorphe à

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_\pi(S(F)), \mathbb{Z}_p) .$$

En partant des suites exactes

$$0 \longrightarrow E_{\pi^n} \longrightarrow E_{\pi^\infty} \xrightarrow{\pi^n} E_{\pi^\infty} \longrightarrow 0 ,$$

on montre facilement que les homomorphismes

$$S(F)^{(\pi^n)} \longrightarrow S(F)_{\pi^n}$$

qui s'en déduisent sont surjectifs et de noyau $E_{\pi^\infty}(F)/\pi^n E_{\pi^\infty}(F)$. Ils induisent par passage à la limite projective un homomorphisme surjectif de noyau fini $E(F)(p)$

$$\overset{\vee}{S}(F) \longrightarrow T_\pi(S(F)) .$$

Donc α_F peut être considéré comme un homomorphisme

$$Y(N_\infty)^\Gamma \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\overset{\vee}{S}(F), \mathbb{Z}_p) .$$

On déduit alors du composé $\alpha_F \circ \Phi_F$:

$$\alpha_F \circ \Phi_F : \overset{\vee}{\Sigma}{}^*(F) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\overset{\vee}{S}(F), \mathbb{Z}_p)$$

une forme bilinéaire $B_{F,\mathfrak{p}} = B_F$

$$\overset{\vee}{S}(F) \times \overset{\vee}{\Sigma}{}^*(F) \longrightarrow \mathbb{Z}_p$$

$$(x,y) \longmapsto B_F(x,y) = \alpha_F \circ \Phi_F(y)(x)$$

que l'on peut prolonger à $\overset{\vee}{S}(F) \times \overset{\vee}{S}{}^*(F)$ (à valeurs dans $\mathbb{Q}_p$), $\overset{\vee}{\Sigma}{}^*(F)$ étant d'indice fini dans $\overset{\vee}{S}{}^*(F)$. Remarquons que $E(F) \underset{O}{\otimes} O_{\mathfrak{p}}$ et $E(F) \underset{O}{\otimes} O_{\mathfrak{p}^*}$ étant des sous-groupes de $\overset{\vee}{S}(F)$ et de $\overset{\vee}{S}{}^*(F)$ respectivement, $B_{F,\mathfrak{p}}$ induit une forme bilinéaire $\{\ ,\ \}_{F,\mathfrak{p}}$

$$\{\ ,\ \}_{F,\mathfrak{p}} : E(F) \underset{O}{\otimes} O_{\mathfrak{p}} \times E(F) \underset{O}{\otimes} O_{\mathfrak{p}^*} \longrightarrow \mathbb{Q}_p.$$

Si P et Q sont deux points de E(F), on posera

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

La construction faite permet de donner des formules "explicites" pour $B_{F,\mathfrak{p}}(x,y)$ et en particulier pour $\{P,Q\}_{F,\mathfrak{p}}$ lorsque P appartient à $E(F)$ et Q appartient à $E_1(F)$. Soit ρ_n le composé de Φ_F avec la projection

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_\pi\ ,\ \varprojlim C_n(p))^\Gamma \longrightarrow \mathrm{Hom}(E_{\pi^n}, I_n/\overline{N_n^\times V_n})^\Gamma$$

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

Lemme 19. 1 - <u>Pour tout</u> $u \in E_{\pi^n}$, <u>on a</u>

$$\{P,Q\}_{F,\mathfrak{p}} u = (\rho_n(Q)(u), M_n/N_n)(P_n) - P_n \tag{12}$$

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

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

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

<u>pour tout</u> $u \in E_{\pi^n}$. <u>Alors</u>,

$$(13) \qquad \delta\, \pi^{*n}\{P,Q\}_{F,\mathfrak{p}} \equiv \sum_{v} \{P,Q\}_{n,v}^{(u)} \quad \text{modulo } \pi^{n(u)}$$

où v parcourt les places finies de 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 $Q \longrightarrow S_{n,u}(Q)_v$ soit continue sur $E_1(F)$ pour la topologie v-adique $(v|\mathfrak{p})$.

Démonstration. 1 - La formule (12) provient immédiatement du diagramme commutatif exact suivant

$$\begin{array}{ccccc} E_1(F) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*} & \xrightarrow{\Phi_F} & Y(N_\infty)^\Gamma & \xrightarrow{\alpha_F} & \mathrm{Hom}_{\mathbb{Z}_p}(E(F) \otimes_{\mathcal{O}} D_{\mathfrak{p}}, D_{\mathfrak{p}}) \\ \downarrow & & \downarrow & & \downarrow \\ E_1(F)/\pi^{*n}E_1(F) & \longrightarrow & \mathrm{Hom}(E_{\pi^n}, I_n/\overline{V_n N_n^x})^\Gamma & \longrightarrow & \mathrm{Hom}(E(F)/\pi^n E(F), \mathcal{O}/\pi^n\mathcal{O}). \end{array}$$

La seconde application de la ligne inférieure est

$$f \longmapsto (P \bmod \pi^n E(F) \longmapsto (u \mapsto (f(u), M_n/N_n)(P_n) - P_n))$$

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

2 - La formule (13) provient de la décomposition du symbole d'Artin par la théorie du corps de classes

$$(y, M_n/N_n) = \prod_{v} (y_v, M_{n,v}/N_{n,v}) \qquad \text{si } y \in I_n.$$

Propriétés 20. Si α appartient à $\mathcal{O}$, on a

$$i_{\mathfrak{p}}(\alpha)\, B_{F,\mathfrak{p}}(x,y) = B_{F,\mathfrak{p}}(\alpha x, y)$$

$$B_{F,\mathfrak{p}}(\alpha x, y) = B_{F,\mathfrak{p}}(x, \alpha^* y) .$$

Démonstration. La première formule se voit immédiatement. La deuxième se déduit du fait que

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

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

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

Donnons maintenant une propriété des formes bilinéaires $B_{L,\mathfrak{p}}$ vraie sans aucune hypothèse de Leopoldt.

Proposition 21. Les rangs des formes bilinéaires $B_{L,\mathfrak{p}}$ sont bornés lorsque L parcourt les extensions finies de N_∞/F.

Démonstration. Le rang de $B_{L,\mathfrak{p}}$ est majoré par le $\mathbb{Z}_p$-rang de $Y(N_\infty)^{G(N_\infty/L)}$. Celui-ci est borné lorsque L parcourt les sous-extensions finies de N_∞/F : on rappelle en effet que si M est un Λ_Γ-module compact de type fini et t(M) son Λ_Γ-module de torsion, le $\mathbb{Z}_p$-rang de $M^{G(N_\infty/L)}$ est égal au $\mathbb{Z}_p$-rang de $t(M)_{G(N_\infty/L)}$, qui est borné pour L contenu dans N_∞.

1.3. Hauteur algébrique et série caractéristique.

On suppose dans ce paragraphe que N_∞ vérifie l'hypothèse $\mathfrak{p}$-adique de Leopoldt. Le Λ_Γ-module $Y(N_\infty)$ est donc de Λ_Γ-torsion. Soit $f(N_\infty,T)$ sa série caractéristique (définie comme toujours à une unité de Λ_Γ près). Notons n_F le O-rang de E(F) et r_F le $\mathbb{Z}_p$-rang de $T_\pi(Ш(F))$; c'est aussi le $\mathbb{Z}_p$-rang de $T_{\pi^*}(Ш(F))$ d'après le corollaire 16.

Si M et N sont deux $\mathbb{Z}_p$-modules de type fini de même rang et si B est une forme bilinéaire de $M \times N$ à valeurs dans $\mathbb{Q}_p$, on dira par abus de langage que B est non dégénérée si sa restriction à des sous-modules libres M' et N' de rang maximal l'est. On pose alors

$$\text{disc } B(M,N) = \frac{\det(B(m'_i,n'_j))_{i,j}}{[M:M'][N:N']}$$

où m'_i (resp. n'_j) est une $\mathbb{Z}_p$-base de M' (resp. N'). Ce nombre n'est en fait défini qu'à une unité près. Par contre, si $P_1,\ldots,P_n$ est une O-base d'un O-module libre E' contenu dans E(F) et de rang maximal, le nombre

$$\text{disc } \{,\}_{F,\mathfrak{p}} = \frac{\det(\{P_i,P_j\}_{F,\mathfrak{p}})_{i,j}}{[E(F):E']}$$

a la même valuation que $\mathrm{disc}\{E(F)\otimes_{\mathcal{O}}\mathcal{O}_{\mathfrak{p}}, E(F)\otimes_{\mathcal{O}}\mathcal{O}_{\mathfrak{p}^*}\}_{F,\mathfrak{p}}$ mais ne dépend pas du choix de E' et de sa base.

Théorème 22. 1- *La série* $f(N_\infty,T)$ *est divisible par* $T^{n_F+r_F}$.

2- *Elle est exactement divisible par* $T^{n_F+r_F}$ *si et seulement si la forme bilinéaire* $B_{F,\mathfrak{p}}$ *est non dégénérée.*

3- *On a la formule*

$$(14)\quad f(N_\infty,T)/T^{n_F+r_F}\Big|_{T=0} \sim \#(E(F)(\mathfrak{p}))\prod_{v|\mathfrak{p}} i_{\mathfrak{p}}\Big(1-\frac{\psi_F(v)}{Nv}\Big)\mathrm{disc}\, B_{F,\mathfrak{p}}(S(F),S^*(F)) \cdot \#(Ш(F)(\mathfrak{p})/\mathrm{div}).$$

Si $Ш(F)(\mathfrak{p})$ *est fini, la formule devient*

$$f(N_\infty,T)/T^{n_F}\Big|_{T=0} \sim \#(E(F)(\mathfrak{p}))\prod_{v|\mathfrak{p}} i_{\mathfrak{p}}\Big(1-\frac{\psi_F(v)}{Nv}\Big)\mathrm{disc}\{\ ,\ \}_{F,\mathfrak{p}} \cdot \#(Ш(F)(\mathfrak{p})).$$

Démonstration. L'homomorphisme $Y(N_\infty) \longrightarrow \widehat{\mathrm{div}(S(F))}$ étant surjectif et $\widehat{\mathrm{div}(S(F))}$ étant de $\mathbb{Z}_p$-rang n_F+r_F, $f(N_\infty,T)$ est toujours divisible par $T^{n_F+r_F}$. Soit Z_∞ le noyau de cet homomorphisme. La suite suivante est exacte

$$0 \to (Z_\infty)^\Gamma \to Y(N_\infty)^\Gamma \to \widehat{\mathrm{div}(S(F))} \to (Z_\infty)_\Gamma \to Y(N_\infty)_\Gamma \to \widehat{\mathrm{div}(S(F))} \to 0\ .$$

Mais par la proposition II.16, le noyau de la dernière flèche est $\widehat{S'(F)/\mathrm{div}}$ qui est fini. D'autre part, la multiplicité de T dans $f(N_\infty,T)$ est n_F+r_F si et seulement si $(Z_\infty)_\Gamma$ est fini, ce qui est le cas si et seulement si l'indice de $Y(N_\infty)^\Gamma$ dans $\widehat{\mathrm{div}(S(F))}$ est fini. Cette dernière condition est équivalente à la non-dégénérescence de $B_{F,\mathfrak{p}}$. Lorsqu'elle est réalisée, comme $Y(N_\infty)$ n'a pas de Λ_Γ-sous-module fini non nul, $(Z_\infty)^\Gamma$ est nul et on a

$$f(N_\infty,T)/T^{n_F+r_F}\Big|_{T=0} \sim \#(Z_\infty)_\Gamma \sim \#(S'(F)/\mathrm{div})[\widehat{\mathrm{div}(S(F))} : Y(N_\infty)^\Gamma].$$

Mais, d'après la proposition II.8 et le lemme II.1, on a

$$\begin{aligned}\#(S'(F)/\mathrm{div}) &= \#(S(F)/\mathrm{div})[S'(F) : S(F)] \\ &\sim \#(Ш(F)(\mathfrak{p})/\mathrm{div})\prod_{v|\mathfrak{p}} i_{\mathfrak{p}}\Big(1-\frac{\psi_F(v)}{Nv}\Big)[S^*(F) : \Sigma^*(F)]^{-1}.\end{aligned}$$

D'autre part,

$$[\widehat{\mathrm{div}(S(F))} : Y(N_\infty)^\Gamma] = [T_\pi(S(F)) : \Phi_F(\overset{\vee}{\Sigma}{}^*(F))]$$

$$\sim \mathrm{disc}\, B_{F,\mathfrak{p}}(\overset{\vee}{S}(F),\overset{\vee}{S}{}^*(F)) \cdot [\overset{\vee}{S}{}^*(F) : \overset{\vee}{\Sigma}{}^*(F)]\#(E(F)(\mathfrak{p}))$$

(on rappelle que le noyau de $\overset{\vee}{S}(F) \longrightarrow T_\pi(S(F))$ est isomorphe à $E(F)(\mathfrak{p})$). En mettant ensemble les trois formules précédentes, on obtient (14) et le théorème 22.

Il nous reste maintenant à comparer la forme bilinéaire algébrique $\{\,,\,\}_{F,\mathfrak{p}}$ que nous venons de construire et la forme bilinéaire analytique p-adique $\langle\,,\,\rangle_{K,\mathfrak{p}}$ construite au chapitre III et associée à l'homomorphisme $\log_p \kappa$. C'est ce que nous allons faire dans le paragraphe suivant. Auparavant, donnons quelques exemples en supposant déjà démontré le lien entre les deux formes bilinéaires, c'est-à-dire

$$\{\,,\,\}_{F,\mathfrak{p}} = \#(E(F(E_\mathfrak{p}))(\mathfrak{p}))^{-1}\langle\,,\,\rangle_{K,\mathfrak{p}}\,.$$

Exemples. Il est fondamental de comparer la fonction $f(N_\infty,T)$ et la série d'Iwasawa G_1 associée à la fonction L p-adique analytique ([3]). Nous allons donner des exemples où il est possible d'en montrer l'égalité. Les trois premières courbes citées ont un $\mathcal{O}$-rang sur K égal à 1.

$y^2 = x^3 - 2x$. Il est montré dans [3] que la composante 5-primaire de $Ш(\mathbb{Q})$ est nulle. On a alors

$$f(N_\infty,T) \sim T \qquad (\text{pour } \mathfrak{p} = (2+i)).$$

Il en est de même de $G_1(\kappa(\gamma)(1+T) - 1)$. On a donc

$$f(N_\infty,T) \sim G_1(\kappa(\gamma)(1+T)-1)$$

De plus, $Ш(N_n)(5)$ est nul pour toute extension N_n contenue dans N_∞ et le rang de $E(N_n)$ est égal à 1.

$y^2 = x^3 + 31x$. On ne sait pas ici si $Ш(K)(5)$ est fini. Donc, soit T^2 divise $f(N_\infty,T)$, soit

$$f(T) = T\,g(T)$$

avec $g(T)$ une série telle que 5^2 divise $g(0)$. Il est démontré dans [3] que $G_1(\kappa(\gamma)(1+T)-1)$ est de même égal à $T(T+\beta)$ avec β divisi-

ble par 5^2. Mais, on ne peut prouver l'égalité de f et de $G_1(\kappa(\gamma)(1+T)-1)$.

$y^2 = x^3 - 36x$. De nouveau, le calcul du second membre de (14) montre que soit T^2 divise $f(N_\infty,T)$, soit $f(T)$ est égal au produit de T par une série $g(T)$ telle que $g(0)$ est divisible par 5. De plus il est montré dans [3] que $G_1(\kappa(\gamma)(1+T)-1)$ est égal à $T(T+\beta)$ avec $\beta \sim 5$. On est donc dans la même situation que pour l'exemple précédent. Cependant, dans ce cas un élément nouveau permet de conclure. Il est facile de voir que 2 divise le nombre de classes de $K(E_\mathfrak{p})$ et que grâce aux minorations d'Odlyzko 5 ne le divise pas. Grâce au théorème de Coates et Wiles démontré dans [10], on en déduit que $f(T)$ divise $G_1(\kappa(\gamma)(1+T)-1)$. Donc $f(T)$ est exactement divisible par T et égal à une unité près à $G_1(\kappa(\gamma)(1+T)-1)$. De plus, $Ш(K)(\mathfrak{p})$ est fini et de cardinal égal à 1.

$y^2 = x^3 + 14x$. Ici, n_K est égal à 2, $Ш(K)(\mathfrak{p})$ est trivial pour $\mathfrak{p} = (2+i)$ toujours d'après [3] et $f(N_\infty,T)$ est égal à T^2 à une unité près.

2. Comparaison des deux formes bilinéaires.

Théorème 23. *Les deux formes bilinéaires* $\{\,,\}_{F,\mathfrak{p}}$ *et* $\langle\,,\rangle_{\kappa,\mathfrak{p}}$ *sur* $E(F)$ *sont proportionnelles :*

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

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

Démonstration. Les deux formes bilinéaires vérifiant les propriétés (i) et (ii) du lemme II.6, 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 égal à $h_\kappa(P) = \langle P,P\rangle_\kappa$. 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. On montre ensuite que l'on peut éviter de le calculer pour les places au dessus de $\mathfrak{p}^*$ puis par un argument différent pour les places au dessus de $\mathfrak{p}$.

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

$$q^n((u)-(0)),$$

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

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

et que les deux fonctions sont reliées par

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

Lemme 24. 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 $\mathrm{Hom}(E_{\pi^n}, N_n^x/N_n^{xq^n})$ est donné par

$$\tilde{h}_{n,P}(u) \equiv f_{n,u}(P) \text{ modulo } N_n^{xq^n}.$$

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 N_n^x tel que si

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

on ait pour $\sigma \in G(\bar{F}/N_n)$

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

Mais, par définition de W_n, on a

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

$$= \sigma g_{n,u}(P_n^*)/g_{n,u}(P_n^*)$$

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 $E_{\pi^{*n}} - \{0\}$ 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

$$\mathrm{div}(g_{n,u}) = \mathrm{div}(F_{n,u}) + q^n((u') - (0)) \ .$$

On pose

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

On a donc

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

Lemme 25. Supposons que v ne divise pas p. Alors

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

Démonstration. Soit $\Omega_n = F_n(P_n^*)$. L'extension Ω_n/N_n est non ramifiée en v d'où

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

D'après (III.3), on a

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

D'autre part, on a

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

et l'extension $N_n(P^*_{2n})/N_n$ est 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 $\{\ ,\ \}^{(u)}_{n,v}$ (lemme 19) calculées à partir de l'idèle $S_{n,u}(P)$ vérifiant

$$(15)\qquad S_{n,u}(P)_v = \begin{cases} 1 & \text{si } v|\infty \\ t_{n,u}(P^*_{n,v}) & \text{si } v|\mathfrak{p} \end{cases}$$

$$v_{N_n}(S_{n,u}(P)_v) = v_{N_n}(a_{n,u}(P))/q^n \quad \text{sinon}$$

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

Proposition 26. Supposons que v ne divise pas p. Alors, pour P appartenant à $E_1(F)$ et qui n'est pas de torsion, on a

$$(16)\qquad \{P,P\}^{(u)}_{n,v}u = [\pi^{-n}\lambda_{N_n,v}(P-u)\log_{\mathfrak{p}}\psi_{N_n}(v)]u$$

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

Démonstration. Pour simplifier les notations, on pose $\psi = \psi_{N_n}$. Par définition, si ω_v est une uniformisante de N_n en v, on a

$$\{P,P\}^{(u)}_{n,v}u = v_{N_n}(a_{n,u}(P)/q^n)[(\omega_v,M_{n,v}/N_{n,v})(P_n) - P_n]$$

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

$$(\omega_v,M_{n,v}/N_{n,v})(\tilde{P}_n) = \psi(v)\tilde{P}_n.$$

Comme $E(N_n)$ contient $E_{\pi^n},\psi(v)$ est congru à 1 modulo π^n et $\log_{\mathfrak{p}}\psi(v)$

est congru à $i_{\mathfrak{p}}(\psi(v)-1)$ modulo q^{2n}. D'où

$$\{P,P\}^{(u)}_{n,v}\tilde{u} = q^{-n}v_{N_n}(a_{n,u}(P))\pi^{-n}(\psi(v)-1)\tilde{P}$$

$$= [\lambda_{N_n,v}(P-u) - \lambda_{N_n,v}(P)]\pi^{-n}\log_{\mathfrak{p}}\psi(v)\tilde{P}$$

(la première ligne est en fait vraie dès que v ne divise pas $\mathfrak{p}$). D'autre part, par le lemme III.1, $\lambda_{N_n,v}(P)\tilde{P}$ est toujours nul de même que $\lambda_{N_n,v}(P-u)(\tilde{P}-\tilde{u})$. D'où

$$\{P,P\}^{(u)}_{n,v}\tilde{u} = \lambda_{N_n,v}(P-u)\pi^{-n}\log_{\mathfrak{p}}\psi(v)\ \tilde{u}$$

et la proposition.

Lemme 27. *Choisissons un entier* m *tel que* π^m *annule* $E(F_\omega)(\mathfrak{p})$ *pour toute place* ω *de* F *au dessus de* $\mathfrak{p}^*$. *Alors, pour tout* $n>m$ *et pour toute place* v *de* N_n *au dessus de* $\mathfrak{p}^*$, *on a*

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

(ii) $\quad \lambda_{N_n,v}(P-u) = 0$ *pour tout* $u \in E_{\pi^n} - E_{\pi^m}$.

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 $E(\tilde{F}_\omega)(p)$. On en déduit (i). Quant à (ii), il se déduit du lemme III.1.

On peut réécrire (ii) de la manière suivante

$$\pi^m\lambda_{N_n,v}(P-u)\,u = 0 \quad \text{pour tout} \quad u \in E_{\pi^n}\ .$$

Effectuons maintenant le calcul de $\{P,P\}_{F,\mathfrak{p}}$ en utilisant la formule (13). Posons κ_n pour la restriction de κ à $G(N_\infty/N_n)$. On a alors pour un point P de $E_1(F)$:

$$h_{\kappa_n}(P-u) = h_{\kappa_n}(P) = [N_n : F]\ h_\kappa(P)$$

$$= \delta q^n t_{\mathfrak{p}}(F)^{-1}\ h_\kappa(P).$$

On déduit alors de la définition h_{κ_n}, de la proposition 26 et du lemme

27 la formule

$$\delta\pi^m\pi^{*n}\{P,P\}_{F,\mathfrak{p}}u$$

$$= \pi^m \sum_{v|\mathfrak{p}} [\{P,P\}^{(u)}_{n,v} - \pi^{-n}(\log_p \mathfrak{D}_{N_n,v}(P-u) - \lambda_{N_n,v}(P-u)\log_{\mathfrak{p}}\psi(v))]u$$

$$+ \pi^{m-n} h_{K_n}(P-u)\, u\,.$$

D'où une égalité du type

$$\{P,P\}_{F,\mathfrak{p}} - t_{\mathfrak{p}}(F)^{-1}h_K(P) \equiv D_n(P) \bmod q^{n-m}\mathbb{Z}_p.$$

où $D_n(P)$ est une fonction quadratique sur $E_1(F)$ à valeurs dans $\mathbb{Z}_p/p^{n-m}\mathbb{Z}_p$ vérifiant

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

pour α appartenant à $\mathcal{O}$ et continue pour la topologie induite par l'inclusion

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

On en déduit que D_n est nulle et que

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

et le théorème 23.

Chapitre V. Hauteurs algébrique et analytique associées à une $\mathbb{Z}_p$-extension contenue dans F_∞ et série caractéristique à 2 variables.

Dans ce chapitre, nous démontrons les théorèmes IV.22 et IV.23 pour une $\mathbb{Z}_p$-extension L_∞ contenue dans F_∞ et donnons une formule analogue à 2 variables pour la série caractéristique de $\widehat{S(F_\infty)}$ (paragraphe 5). Les formes bilinéaires algébriques utilisées sont construites à partir d'un pseudo-isomorphisme $\Phi_{\mathfrak{p}}(F_\infty)$ entre $\widehat{S^*(F_\infty)}$ et l'adjoint à $(\widehat{S(F_\infty)})$ de $\widehat{S(F_\infty)}$ (le . signifiant que l'action de Θ a été changée par $\theta \longrightarrow \theta^{-1}$). Ce dernier se démontre à partir de la suite exacte (IV.1). Il peut être considéré comme une dualité entre $\widehat{S(F_\infty)}$ et $\widehat{S^*(F_\infty)}$ et l'on en déduit une équation fonctionnelle entre les séries caractéristiques. De plus, afin de montrer l'égalité entre ces formes bilinéaires algébriques et les hauteurs p-adiques définies au chapitre III, nous montrons que les Λ-homomorphismes

$$\Phi_{\mathfrak{p}}(F_\infty) : \widehat{S^*(F_\infty)} \longrightarrow \dot{a}_\Lambda(\widehat{S(F_\infty)})$$

$$\Phi_{\mathfrak{p}^*}(F_\infty) : \widehat{S(F_\infty)} \longrightarrow \dot{a}_\Lambda(\widehat{S^*(F_\infty)})$$

sont adjoints l'un de l'autre.

Cependant, nous n'irons au bout de ce programme qu'<u>en supposant que les conjectures $\mathfrak{p}$-adique et $\mathfrak{p}^*$-adique de Leopoldt sont vraies pour toute extension finie de F contenue dans F_∞</u>, ce qui est par exemple vérifié dès que $F(E_p)$ est abélien sur K.

1. Equation fonctionnelle.

1.1. Rappels et notations.

On reprend les notations utilisées dans le chapitre IV. On pose donc en particulier

$$F_n = F(E_{\mathfrak{q}^n}),\ N_n = F(E_{\pi^n}),\ N_n^* = F(E_{\pi^{*n}}).$$

Si L est une extension abélienne de F et M un $\mathbb{Z}_p[[G(L/F)]]$-module compact et de type fini, on pose

$$a_L(M) = a_{\mathbb{Z}_p[[G(L/F)]]}(M) .$$

De plus si L est une $\mathbb{Z}_p$-extension d'une extension finie F' de F, M est pseudo-nul s'il est pseudo-nul en tant que $\Lambda_{G(L/F')}$-module.

Dans le cas où L est une extension finie de F contenant N_n, la suite exacte (1) de IV devient

$$(1)_{L,n} \quad 0 \longrightarrow \mathrm{Hom}(T_\pi, \mu_{q^n}(L)) \longrightarrow \prod_{v|\mathfrak{p}} \mathrm{Hom}(T_\pi, \mu_{q^n}(L_v)) \longrightarrow$$
$$\longrightarrow \mathrm{Hom}(T_\pi, X(L)_{q^n}) \longrightarrow \Sigma(L)^{(\pi^{*n})} \longrightarrow 0 .$$

En effet, l'hypothèse $\mathfrak{p}$-adique de Leopoldt pour L implique que $\bar{E}_{L,\mathfrak{p}}/E_{L,\mathfrak{p}}(p)$ est nul et donc, grâce à la suite exacte (IV.9), que $X(L)_{q^n}$ est isomorphe à $C(L)_{q^n}$ par l'homomorphisme d'Artin. Le dernier homomorphisme de $(1)_{L,n}$ est noté $\eta_n(L)$.

1.2. Equation fonctionnelle pour N_∞.

Proposition 1. Soit L une extension finie de F. Les homomorphismes $\eta_n(LN_n)$ permettent de construire un $\Lambda_{G(LN_\infty/L)}$ pseudo-isomorphisme $\phi_{\mathfrak{p}}(LN_\infty)$ injectif

$$\phi_{\mathfrak{p}}(LN_\infty) : Y^*(LN_\infty) \hookrightarrow \dot{a}_{LN_\infty}(Y(LN_\infty)) .$$

Le dual de Pontryagin de son conoyau $T^*(LN_\infty)$ vérifie la suite exacte

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \mu_{p^\infty}(LN_\infty)) \longrightarrow \prod_{v|\mathfrak{p}} \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \mu_{p^\infty}((LN_\infty)_v)) \longrightarrow \widehat{T^*(LN_\infty)} \longrightarrow 0.$$

Démonstration. Pour simplifier les notations, on supposera que L est égale à F dans la démonstration. La limite inductive des $\Sigma(N_n)^{(\pi^{*n})}$ relativement aux homomorphismes induits par les inclusions $E_{\pi^{*n}} \longrightarrow E_{\pi^{*n+1}}$ et $N_n \hookrightarrow N_{n+1}$ est égale à $\Sigma^*(N_\infty)$ qui grâce au lemme II.11 est encore égale au dual de Pontryagin de $Y^*(N_\infty)$. D'autre part, la limite inductive des $X(N_n)_{q^n}$ relativement aux homomorphismes de norme est égale à $\varinjlim X(N_n)(p)$. Mais, $X(N_n)(p)$ est exactement $X(N_\infty)_{G(N_\infty/N_n)}$ qui est fini puisque nous avons supposé que N_n vérifie l'hypothèse $\mathfrak{p}$-adique de Leopoldt. Donc d'après le corollaire I.13, $\varinjlim X(N_n)(p)$ est égal au dual de Pontryagin de $\dot{a}_{N_\infty}(X(N_\infty))$. Grâce aux lemmes IV.11 et IV.12, les suites exactes $(1)_{N_n,n}$ entraînent alors par

passage à la limite inductive la proposition.

1.3. Equation fonctionnelle pour F_∞.

Proposition 2. Les homomorphismes $\phi_{\mathfrak{p}}(LN_\infty)$ permettent de construire un Λ-pseudo-isomorphisme $\Phi_{\mathfrak{p}}(F_\infty)$ injectif

$$\Phi_{\mathfrak{p}}(F_\infty) : Y^*(F_\infty) \hookrightarrow \dot{a}_{F_\infty}(Y(F_\infty)).$$

Remarque. La structure du conoyau de $\Phi_{\mathfrak{p}}(F_\infty)$ sera donnée au cours de la démonstration. D'autre part, l'existence d'un tel Λ-pseudo-isomorphisme a été démontrée indépendamment par Greenberg ([13]).

Démonstration. On fait maintenant varier L le long d'une $\mathbb{Z}_p$-extension L_∞ de $F(E_p)$ différente de $N_\infty(E_{\mathfrak{p}^*})$. On note L_n les corps intermédiaires. De l'étude des homomorphismes de transition faite au lemme IV.12, on déduit la suite exacte

$$(2) \qquad 0 \longrightarrow Y^*(F_\infty) \longrightarrow \varprojlim \dot{a}_{L_nN_\infty}(Y(L_nN_\infty)) \longrightarrow T^*(F_\infty) \longrightarrow 0$$

où le dual de Pontryagin de $T^*(F_\infty)$ vérifie la suite exacte

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \mu_{p^\infty}) \longrightarrow \prod_{v|\mathfrak{p}} \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \mu_{p^\infty}(F_{\infty,v})) \longrightarrow \widehat{T^*(F_\infty)} \longrightarrow 0.$$

Il reste à comparer le module du milieu de la suite exacte (2) avec l'adjoint de $Y(F_\infty)$. D'après le corollaire I.13, l'adjoint de $Y(F_\infty)$ peut se calculer par la formule

$$a_\Lambda(Y(F_\infty)) = \varprojlim a_{L_nN_\infty}(Y(F_\infty)^{G(F_\infty/L_nN_\infty)}).$$

Soit $M'_{L_nN_\infty}$ l'extension abélienne maximale de L_nN_∞ contenue dans M_{F_∞} et J_n le composé des sous-groupes d'inertie aux places de L_nN_∞ divisant $\mathfrak{p}^*$. Pour n assez grand ($n \geq n_0$), l'homomorphisme de projection

$$J_n \longrightarrow G(F_\infty/L_nN_\infty)$$

est surjectif. Soit J'_n son noyau. On a alors la suite exacte

$$0 \longrightarrow J'_n \longrightarrow X(F_\infty)^{G(F_\infty/L_nN_\infty)} \longrightarrow X(N_\infty L_n) \longrightarrow 0.$$

Le groupe $G(M_{N_\infty L_n}/N_\infty L_n)$ est produit direct de $G(M_{N_\infty L_n}/F_\infty)$ et de $G(F_\infty/N_\infty L_n)$. L'homomorphisme de transition sur $X(N_\infty L_n)$ est induit par la multiplication par la somme des éléments de $G(L_{n+1}N_\infty/L_nN_\infty)$ sur $X(F_\infty)_{G(F_\infty/N_\infty L_n)}$ et induit la multiplication par q sur $G(F_\infty/N_\infty L_n)$. Supposons $n \geq n_o$ et notons $v_{i,n}$ les places de L_nN_∞ au dessus de $\mathfrak{p}^*$ et τ_{i,n_o} un générateur du groupe d'inertie de v_{i,n_o} se projetant sur un générateur γ_{n_o} fixé de $G(F_\infty/L_{n_o}N_\infty)$. On vérifie que

$$\tau_{i,n_o}^{q^{n-n_o}} = \Big(\sum_{\gamma \in G(L_nN_\infty/L_{n_o}N_\infty)} \gamma\Big) y_i \, \tau_{i,n_o}^{q^{n-n_o}}$$

avec $y_i \in X(F_\infty)$ et que $\tau_{i,n} = \tau_{i,n_o}^{q^{n-n_o}}$ est un générateur du groupe d'inertie de $v_{i,n}$. Donc l'image de $\tau_{i,n}$ par l'homomorphisme de transition est $\tau_{i,n+1}$ et l'homomorphisme de transition

$$J'_n \longrightarrow J'_{n+1}$$

est un isomorphisme pour $n \gg 0$. Posons alors

$$T(F_\infty) = \mathrm{Hom}_{\mathbb{Z}_p}\left(T_\pi, \varprojlim \dot{a}_{L_nN_\infty}(J'_n)\right).$$

C'est un Λ-module pseudo-nul et on a la suite exacte de $\Lambda_{G(F_\infty/F)}$-modules

$$(3) \qquad 0 \longrightarrow \varprojlim \dot{a}_{L_nN_\infty}(Y(N_\infty L_n)) \longrightarrow \dot{a}_{F_\infty}(Y(F_\infty)) \longrightarrow T(F_\infty) \longrightarrow 0.$$

On déduit de (2) et (3) la proposition 2.

Remarque. Le premier module de (3) peut aussi être décrit comme le dual de Pontryagin de

$$\mathrm{Hom}_{\mathbb{Z}_p}\left(T_\pi, \varprojlim X(F_n)(p)\right).$$

On déduit de $\Phi_{\mathfrak{p}}(F_\infty)$ un Λ-homomorphisme injectif et à conoyau pseudo-nul

$$\Phi_{\mathfrak{p}}(F_\infty) : Y^*(F_\infty) \longrightarrow \dot{a}_\Lambda(Y(F_\infty)).$$

Corollaire 3. Pour toute $\mathbb{Z}_p$-extension L_∞ de F contenue dans F_∞, il existe un pseudo-isomorphisme injectif $\phi'_{\mathfrak{P}}(L_\infty)$ de $\Lambda_{G(L_\infty/F)}$-modules

$$\phi'_{\mathfrak{P}}(L_\infty) : Y^*(F_\infty)_{G(F_\infty/L_\infty)} \longrightarrow \dot{a}_{L_\infty}(Y(F_\infty)_{G(F_\infty/L_\infty)})$$

dès que $Y(F_\infty)_{G(F_\infty/L_\infty)}$ est un $\Lambda_{G(L_\infty/F)}$-module de torsion.

Rappelons que si L_∞ est différent de N_∞ et de N_∞^*, on a

$$Y^*(F_\infty)_{G(F_\infty/L_\infty)} \simeq Y^*(L_\infty)$$

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

Pour la démonstration du corollaire 3, on applique la proposition I.12 et le théorème II.25.

Remarque. La construction de la proposition 2 aurait pu être faite à partir de n'importe quelle $\mathbb{Z}_p$-extension L_∞ de F contenue ou non dans F_∞. En particulier pour toute $\mathbb{Z}_p$-extension L_∞ de F, il existe un $\Lambda_{G(L_\infty/F)}$-homomorphisme injectif de $Y^*(L_\infty)$ dans $\dot{a}_{L_\infty}(Y(L_\infty))$ à conoyau pseudo-nul dès que $Y(L_\infty)$ est de $\Lambda_{G(L_\infty/F)}$-torsion. De même, la construction des hauteurs algébriques qui suit est valable pour n'importe quelle $\mathbb{Z}_p$-extension de F. Cependant, dans ce cadre général, nous ne savons pas pour l'instant lier ces hauteurs algébriques aux hauteurs analytiques définies dans le chapitre III. Aussi, nous limitons-nous dans l'exposition aux $\mathbb{Z}_p$-extensions contenues dans F_∞.

2. Hauteurs algébriques.

Nous allons d'abord montrer comment l'on retrouve à partir de $\phi_{\mathfrak{P}}(N_\infty)$ la forme bilinéaire $B_{F,\mathfrak{P}}$ du chapitre IV. Rappelons que, d'après la proposition I.14 et le théorème II.25, $\dot{a}_{N_\infty} \circ \dot{a}_{N_\infty}(Y(N_\infty))$ est canoniquement isomorphe à $Y(N_\infty)$. En prenant l'adjoint $\dot{a}(\phi_{\mathfrak{P}}(N_\infty))$ de l'homomorphisme $\phi_{\mathfrak{P}}(N_\infty)$, on obtient la suite exacte

$$0 \longrightarrow Y(N_\infty) \longrightarrow \dot{a}_{N_\infty}(Y^*(N_\infty)) \longrightarrow \widehat{T^*(N_\infty)} \longrightarrow 0 .$$

Ce dernier module étant fini, l'image de $Y(N_\infty)^\Gamma$ dans $\dot{a}_{N_\infty}(Y^*(N_\infty))^\Gamma$ est d'indice fini. D'autre part, notons $Z^*(N_\infty)$ le noyau de l'homomorphisme

canonique

$$Y(N_\infty) \longrightarrow \widehat{div(S^*(F))}$$

et U^* son image. Grâce au lemme II.17, U^* est d'indice fini dans $\widehat{div(S^*(F))}$. Par passage à l'adjoint, on obtient un homomorphisme injectif

$$\dot{a}_{N_\infty}(U^*) \longrightarrow \dot{a}_{N_\infty}(Y^*(N_\infty))^\Gamma .$$

Ce premier module est isomorphe à $\mathrm{Hom}_{\mathbb{Z}_p}(U^*,\mathbb{Z}_p)$. Plus précisemment, comme U^* est un $\mathbb{Z}_p$-module de type fini sur lequel Γ agit trivialement, à chaque générateur γ de Γ est associé un isomorphisme

$$\mathrm{Hom}_{\mathbb{Z}_p}(U^*,\mathbb{Z}_p) \longrightarrow \dot{a}_{N_\infty}(U^*)$$

déduit de la suite exacte $0 \longrightarrow \Lambda_\Gamma \xrightarrow{\gamma-1} \Lambda_\Gamma \longrightarrow \mathbb{Z}_p \longrightarrow 0$. Considérons alors le diagramme suivant

$$\begin{array}{ccccc}
(4)\ \mathrm{Hom}_{\mathbb{Z}_p}(U^*,\mathbb{Z}_p) & \xrightarrow{\simeq} & \dot{a}_{N_\infty}(U^*) & \longrightarrow & \dot{a}_{N_\infty}(Y^*(N_\infty))^\Gamma \\
\uparrow & & & & \uparrow \sim \\
T_{\pi^*}(S^*(F)) & & & & Y(N_\infty)^\Gamma \\
\uparrow \sim & & & & \downarrow \\
\overset{\vee}{S^*}(F) & & \mathrm{Hom}_{\mathbb{Z}_p}(\overset{\vee}{S}(F),\mathbb{Z}_p) & \xleftarrow{\sim} & \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi(S(F)),\mathbb{Z}_p),
\end{array}$$

le symbole $\sim$ indiquant que l'homomorphisme est à noyau et conoyau finis. On en déduit une forme bilinéaire sur $\overset{\vee}{S}(F) \times \overset{\vee}{S^*}(F)$ à valeurs dans $\mathbb{Q}_p$ que l'on note pour l'instant B_γ.

Lemme 4. *Les deux formes bilinéaires $B_{F,\mathfrak{p}}$ et B_γ sont proportionnelles* :

$$B_{F,\mathfrak{p}} = -\frac{\log_p \kappa(\gamma)}{t_{\mathfrak{p}}(F)}\, B_\gamma .$$

Démonstration. La forme bilinéaire $B_{F,\mathfrak{p}}$ se calcule à partir de l'homomorphisme

$$Y(N_\infty)^\Gamma \longrightarrow \overset{\vee}{\Sigma}{}^*(F)$$

qui se décompose ainsi

$$Y(N_\infty)^\Gamma \xrightarrow{\psi_1} \mathrm{Hom}_{\mathbb{Z}_p}\left(\widehat{\varprojlim X(N_n)(-1)}^{\Gamma}, \mathbb{Z}_p\right) \longrightarrow \mathrm{Hom}(\widehat{\Sigma^*(F)}, \mathbb{Z}_p)$$

$$\mathrm{Hom}(\widehat{\Sigma^*(F)}, \mathbb{Z}_p) \xrightarrow{h} \overset{\vee}{\Sigma}{}^*(F)$$

L'homomorphisme ψ_1 se calcule de la manière suivante : soit un élément $x = (x_n)$ de $\varprojlim \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, X(N_n)_{q^n})^\Gamma$ et ϕ un élément de $\widehat{\varprojlim X(N_n)(-1)}^{\Gamma}$. Alors

$$\psi_1(x)(\phi) \equiv q^n \phi(x_n) \bmod q^n \mathbb{Z}_p .$$

La forme bilinéaire B_γ se calcule à partir de l'homomorphisme

$$Y(N_\infty)^\Gamma \longrightarrow \overset{\vee}{S}{}^*(F)$$

(diagramme (4)) décomposé ainsi

$$Y(N_\infty)^\Gamma \longrightarrow \dot{a}_{\Lambda_\Gamma} \circ \dot{a}_{\Lambda_\Gamma}(Y(N_\infty))^\Gamma \longrightarrow \mathrm{Hom}\left(\widehat{\varprojlim X(N_n)(-1)}^{\Gamma}, \mathbb{Z}_p\right) \xrightarrow{h} \overset{\vee}{\Sigma}{}^*(F) .$$

$$\psi_2$$

L'homomorphisme ψ_2 se calcule de la manière suivante :

$$\psi_2(x_n)(\phi) \equiv \phi(x_n) \sum_{a \bmod p^m} \kappa(\gamma)^{-a} \gamma^a (\kappa(\gamma)^{-1}\gamma - 1)\Big|_{\gamma=1} \bmod q^n \mathbb{Z}_p$$

si p^m est le degré de N_n sur $F(E_\mathfrak{p})$ (on a donc $p^m = q^n t_\mathfrak{p}(F)^{-1}$). La comparaison entre ψ_1 et ψ_2 montre alors que

$$\psi_2 = -\log_p \kappa(\gamma) t_\mathfrak{p}(F)^{-1} \psi_1 ,$$

d'où le lemme.

On peut de la même manière qu'au début de ce paragraphe associer à un générateur τ d'une $\mathbb{Z}_p$-extension L_∞ de F une forme bilinéaire B_τ dépendant de τ sur $\overset{\vee}{S}(F) \times \overset{\vee}{S}{}^*(F)$ en utilisant l'homomorphisme

$\phi'_{\mathfrak{p}}(L_\infty)$. Nous allons plutôt faire une construction légérement différente de ces formes bilinéaires algébriques (donnant le même résultat) qui permet de comprendre comment elles varient avec la $\mathbb{Z}_p$-extension.

On fixe une paramétrisation du groupe Θ c'est-à-dire une $\mathbb{Z}_p$-base $\theta = (\gamma,\gamma^*)$. Il sera commode de supposer que γ est un générateur topologique de $G(F_\infty/N_\infty^*)$ et γ^* un générateur topologique de $G(F_\infty/N_\infty)$. On a vu (I.1.3) qu'un tel choix permet d'associer à tout élément h de Θ tel que le quotient de Θ par le sous-groupe H topologiquement engendré par h soit isomorphe à $\mathbb{Z}_p$ un générateur $\tau_{(\theta)}(h)$ de Θ/H vérifiant

$$\tau_{(\theta)}(h)^{-b} \equiv \gamma \text{ modulo } H$$

$$\tau_{(\theta)}(h)^{a} \equiv \gamma^* \text{ modulo } H$$

si $h = \gamma^a\gamma^{*b}$. Remarquons que si ${}^t\theta = (\gamma^*,\gamma)$, on a

$$\tau_{({}^t\theta)}(h) = \tau_{(\theta)}(h)^{-1}.$$

Soit de nouveau U^* l'image de $Y^*(F_\infty)$ dans $\widehat{\mathrm{div}(S^*(F))}$. D'après la remarque de la fin du paragraphe I.2.3, on peut associer à (θ) un isomorphisme que l'on notera $H_{(\theta)}$

$$H_{(\theta)} : \mathrm{Hom}_{\mathbb{Z}_p}(U^*,\mathbb{Z}_p) \longrightarrow \mathrm{Ext}^2_\Lambda(U^*,\Lambda).$$

Notons $Z^*(F_\infty)$ le noyau de $Y^*(F_\infty) \longrightarrow U^*$. On a donc la suite exacte

$$0 \longrightarrow Z^*(F_\infty) \longrightarrow Y^*(F_\infty) \longrightarrow U^* \longrightarrow 0 .$$

Comme U^* est pseudo-nul et que la dimension projective de $Y^*(F_\infty)$ en tant que Λ-module est égale à 1, la suite

$$0 \longrightarrow a_\Lambda(Y^*(F_\infty)) \longrightarrow a_\Lambda(Z^*(F_\infty)) \longrightarrow \mathrm{Ext}^2_\Lambda(U^*,\Lambda) \longrightarrow 0$$

est exacte. Soit H un sous-groupe de Θ et h un générateur topologique. On déduit (par exemple du lemme du serpent) la suite exacte

$$(5)\quad a_\Lambda(Z^*(F_\infty))^H \to \mathrm{Ext}^2_\Lambda(U^*,\Lambda) \to a_\Lambda(Y^*(F_\infty))_H \to a_\Lambda(Z^*(F_\infty))_H \to \mathrm{Ext}^2_\Lambda(U^*,\Lambda) \to 0 .$$

La seconde flèche dépend du choix de h dans H; on la note r_h. D'autre part, l'homomorphisme $\hat{a}(\Phi_{\mathfrak{P}}(F_\infty))$ induit un homomorphisme de $\mathbb{Z}_p$-modules

$$(6) \qquad (Y(F_\infty)_H)^{\Theta/H} \longrightarrow (\hat{a}_\Lambda(Y^*(F_\infty))_H)^{\Theta/H}$$

dont on voit facilement que le conoyau et le noyau sont finis d'ordre borné indépendamment de H. On a le diagramme suivant

$$(7) \qquad \begin{array}{ccccc} \mathrm{Hom}_{\mathbb{Z}_p}(U^*,\mathbb{Z}_p) & \xrightarrow[\simeq]{H(\theta)} & \mathrm{Ext}^2_\Lambda(U^*,\Lambda) & \xrightarrow{r_h} & (\hat{a}_\Lambda(Y^*(F_\infty))_H)^{\Theta/H} \\ \uparrow \sim & & & & \uparrow \sim \\ T_{\pi^*}(S^*(F)) & & & & (Y(F_\infty)_H)^{\Theta/H} \\ \uparrow \sim & & & & \downarrow \\ \overset{\vee}{S}{}^*(F) & & \mathrm{Hom}_{\mathbb{Z}_p}(\overset{\vee}{S}(F),\mathbb{Z}_p) & \xleftarrow{\sim} & \mathrm{Hom}_{\mathbb{Z}_p}(T_\pi(S(F)),\mathbb{Z}_p)\,. \end{array}$$

On construit alors à partir de (7) une forme bilinéaire

$$\overset{\vee}{S}(F) \times \overset{\vee}{S}{}^*(F) \longrightarrow \mathbb{Q}_p$$

que l'on note pour l'instant $B_{(\theta),h}$.

Lemme 5. La forme bilinéaire $B_{(\theta),h}$ dépend linéairement de h et on a

$$B_{(\theta),h} = B_{\tau(\theta)(h)}\,.$$

Démonstration. Soit x un élément de $\mathrm{Ext}^2_\Lambda(U^*,\Lambda)$ tel que $r_h(x)$ appartienne à l'image de $(Y(F_\infty)_H)^{\Theta/H}$ par $\hat{a}(\Phi_{\mathfrak{P}}(F_\infty))$ pour tout h (le sous-groupe des éléments de $\mathrm{Ext}^2_\Lambda(U^*,\Lambda)$ vérifiant cette propriété est d'indice fini) et soient h_1 et h_2 deux éléments de Θ. Il existe $z \in \hat{a}_\Lambda(Z^*(F_\infty))$ dont l'image est x. On a alors

$$r_h(x) = hz - z \quad \text{dans} \quad \hat{a}_\Lambda(Y^*(F_\infty))_H.$$

De l'égalité

$$h_1h_2z - z = h_1(h_2z - z) + h_1z - z,$$

on déduit alors le premier résultat. Pour montrer l'égalité de $B_{(\theta),h}$ et de $B_{\tau_{(\theta)}(h)}$, on remarque d'abord que $H_{(\theta)}$ peut se calculer en utilisant les homomorphismes et suites exactes suivants

$$0 \longrightarrow \Lambda \xrightarrow{h-1} \Lambda \longrightarrow \Lambda_{\Theta/H} \longrightarrow 0$$

$$0 \longrightarrow \Lambda_{\Theta/H} \xrightarrow{\tau_{(\theta)}(h)-1} \Lambda_{\Theta/H} \longrightarrow \mathbb{Z}_p \longrightarrow 0 .$$

L'égalité se déduit alors de la comparaison de (7) et du diagramme définissant $B_{\tau_{(\theta)}(h)}$ (analogue à (4)).

3. Hauteurs algébriques et séries caractéristiques.

Nous montrerons dans le paragraphe 4 le lien entre $B_{(\theta),h}$ et les hauteurs analytiques définies dans le chapitre III. Auparavant, nous allons lier ces formes bilinéaires et les séries caractéristiques.

3.1. Notations.

Considérons une série caractéristique de $Y(F_\infty)$. On peut la voir soit comme une série de deux variables à coefficients dans $\mathbb{Z}_p$ grâce à l'identification de Λ avec $\mathbb{Z}_p[[T_1,T_2]]$ associée au choix d'une base (γ_1,γ_2) de Θ et on la notera alors $f(F_\infty;T_1,T_2)$, soit comme fonction sur le groupe des caractères de Θ à valeurs dans $\mathbb{Z}_p^*$ (en fait dans $1+p\mathbb{Z}_p$) et on la notera alors $H_{\mathfrak{p}}$

$$H_{\mathfrak{p}}(\rho) = f(F_\infty ; \rho(\gamma_1) - 1 , \rho(\gamma_2) - 1) .$$

De plus, on appelle fonction d'Iwasawa une fonction analytique g sur $\mathbb{Z}_p^2$ telle qu'il existe une série f appartenant à $\mathbb{Z}_p[[T_1,T_2]]$ telle que

$$g(s_1,s_2) = f(u^{s_1} - 1 , u^{s_2} - 1)$$

pour un générateur u de $1+p\mathbb{Z}_p$. La série caractéristique peut donc aussi être vue comme une fonction d'Iwasawa :

$$(s,s^*) \longrightarrow H_{\mathfrak{p}}(\kappa^s \kappa^{*s^*}) .$$

Nous utiliserons l'une ou l'autre de ces formulations.

Posons $L_{\mathfrak{p}}(\rho) = H_{\mathfrak{p}}(\rho\kappa^{-1})$. La fonction $L_{\mathfrak{p}}$ appartient à Λ et est une série caractéristique du Λ-module $X(F_\infty)^{(\chi)}$. Rappelons d'autre part que si L_∞ est une $\mathbb{Z}_p$-extension de F contenue dans F_∞, la fonction $H_{\mathfrak{p}}$ restreinte aux caractères de Θ triviaux sur $G(F_\infty/L_\infty)$ est une série caractéristique de $Y(F_\infty)_{G(F_\infty/L_\infty)}$. On introduit de même la fonction $H_{\mathfrak{p}^*}(\rho)$, série caractéristique de $Y^*(F_\infty)$ et $L_{\mathfrak{p}^*}(\rho) = H_{\mathfrak{p}^*}(\rho\kappa^{*-1})$.

Si ρ est un caractère de Θ à valeurs dans $\mathbb{Z}_p^\times$ trivial sur un sous-groupe H de Θ tel que $\Theta/H \simeq \mathbb{Z}_p$ et engendré topologiquement par h, on pose avec $\tau_h = \tau_{(\theta)}(h)$

$$B_{\rho,\mathfrak{p}} = -\log_p \rho(\tau_h) B_{\tau_h} = -\log_p \rho(\tau_h) B_{(\theta),h} .$$

Cette forme bilinéaire sur $\overset{v}{S}(F) \times \overset{v}{S}^*(F)$ ne dépend plus que de ρ.

3.2. Résultats.

Théorème 6. *Les fonctions $H_{\mathfrak{p}}$ et $H_{\mathfrak{p}^*}$ vérifient l'équation fonctionnelle*

$$H_{\mathfrak{p}}(\rho^{-s}) = u(s) H_{\mathfrak{p}^*}(\rho^s)$$

où u est une unité de l'algèbre des fonctions d'Iwasawa à une variable.

Corollaire 7. *Posons $N = \kappa\kappa^*$; alors*

$$L_{\mathfrak{p}}(\rho) = u_\rho L_{\mathfrak{p}^*}(\rho^{-1} N)$$

avec u_ρ unité de $\mathbb{Z}_p$.

Démonstration. C'est une conséquence simple de l'existence d'un pseudo-isomorphisme entre $Y(F_\infty)$ et $\dot{a}_\Lambda(Y^*(F_\infty))$ et de la proposition I.8.

Rappelons que n_F désigne le $\mathcal{O}$-rang de $E(F)$ modulo torsion et r_F le $\mathbb{Z}_p$-rang de $T_\pi(Ш(F))$.

Théorème 8. 1. *La fonction $H_{\mathfrak{p}}(\rho^s)$ a un zéro en $s = 0$ de multiplicité supérieure ou égale à $n_F + r_F$.*

2. *Ce zéro est de multiplicité exactement $n_F + r_F$ si et seulement si la forme bilinéaire $B_{\rho,\mathfrak{p}}$ est non dégénérée.*

3. On a la formule

$$\lim_{s\to 0} H_{\mathfrak{p}}(\rho^s)/s^{n_F+r_F} \sim$$

$$i_{\mathfrak{p}}\Big(\prod_{v|\mathfrak{p}}\Big(1-\frac{\psi_F(v)}{Nv}\Big)\prod_{v|\mathfrak{p}^*}\Big(1-\frac{\psi_F(v)^*}{Nv}\Big)\Big)\ \mathrm{disc}\ B_{\rho,\mathfrak{p}}(\check{S}(F),\check{S}^*(F))\,\#(Ш(F)(\mathfrak{p})/\mathrm{div}).$$

Démonstration. Soit H le noyau de ρ, L_∞ la $\mathbb{Z}_p$-extension fixée par H et h un générateur topologique de H. Si $Y(F_\infty)_H$ n'est pas de $\Lambda_{\Theta/H}$-torsion, $H_{\mathfrak{p}}(\rho^s)$ est nulle et la forme bilinéaire $B_{\rho,\mathfrak{p}}$ est dégénérée. Nous reviendrons sur ce fait dans le paragraphe 5. Supposons maintenant que $Y(F_\infty)_H$ est un $\Lambda_{\Theta/H}$-module de torsion.

Soit U l'image de $Y(F_\infty)$ dans $\mathrm{Hom}_{\mathbb{Z}_p}(\check{S}(F),\mathbb{Z}_p)$ et $Z(F_\infty)$ le noyau de cet homomorphisme. On vérifie facilement que $T^{r_F+n_F}$ divise exactement la série caractéristique f_H de $Y(F_\infty)_H$ si et seulement si l'indice de $(Y(F_\infty)_H)^{\Theta/H}$ dans $\mathrm{Hom}_{\mathbb{Z}_p}(\check{S}(F),\mathbb{Z}_p)$ est fini et on a alors

$$f_H(T)/T^{n_F+r_F}\Big|_{T=0} \sim \#(\ker((Y_\infty)_\Theta \longrightarrow U))[U : (Y(F_\infty)_H)^{\Theta/H}]$$

$$\sim c\,[\mathrm{Hom}_{\mathbb{Z}_p}(\check{S}(F),\mathbb{Z}_p) : (Y(F_\infty)_H)^{\Theta/H}]$$

où c est une constante indépendante de H. Calculons maintenant ce dernier indice.

Lemme 9. Si $B_{\rho,\mathfrak{p}}$ est non dégénérée, on a

$$\mathrm{disc}\ B_{(\theta),h}(\check{S}(F),\check{S}^*(F)) \sim c'[\mathrm{Hom}_{\mathbb{Z}_p}(\check{S}(F),\mathbb{Z}_p) : (Y(F_\infty)_H)^{\Theta/H}]$$

où $$c' = \frac{[\check{S}^*(F) : \mathrm{Ext}^2_\Lambda(U^*,\Lambda)]\,\#[(T(F_\infty)_H)^{\Theta/H}]\,\#[(T(F_\infty)^H)_{\Theta/H}]}{\#(\ker(Y(F_\infty)_\Gamma \longrightarrow \dot{a}_\Lambda(Y^*(F_\infty)_\Gamma))}$$

est une constante indépendante de H et $T(F_\infty)$ est le conoyau du Λ-homomorphisme $\dot{a}(\Phi_{\mathfrak{p}}(F_\infty))$.

On déduira du lemme 9 que l'on a

$$f_H(T)/T^{n_F+r_F}\Big|_{T=0} \sim cc'^{-1}\ \mathrm{disc}\ B_{(\theta),h}(\check{S}(F),\check{S}^*(F)).$$

Démonstration. La structure de $T(F_\infty)$ est donnée dans la démonstration de la proposition 2. Il est facile de voir qu'il vérifie les propriétés suivantes :

$T(F_\infty)^\Theta = 0$, $(T(F_\infty)_H)^{\Theta/H}$ fini;

$T(F_\infty)^H = 0$ si H est différent de $G(F_\infty/N_\infty)$ et de $G(F_\infty/N_\infty^*)$;

$\#((T(F_\infty)_H)^{\Theta/H}) \cdot \#((T(F_\infty)^H)_{\Theta/H})$ indépendant de H.

D'autre part, de la suite exacte

$$0 \longrightarrow Y(F_\infty) \longrightarrow \mathring{a}_\Lambda(Y^*(F_\infty)) \longrightarrow T(F_\infty) \longrightarrow 0 ,$$

on déduit la suite exacte de $\Lambda_{\Theta/H}$-modules

$$0 \longrightarrow T(F_\infty)^H \longrightarrow Y(F_\infty)_H \longrightarrow \mathring{a}_\Lambda(Y^*(F_\infty))_H \longrightarrow T(F_\infty)_H \longrightarrow 0 .$$

Un calcul facile d'indices montre que

$$(8)\quad [(\mathring{a}_\Lambda(Y^*(F_\infty))_H)^{\Theta/H} : (Y(F_\infty)_H)^{\Theta/H}] = \frac{\#((T(F_\infty)_H)^{\Theta/H}) \cdot \#((T(F_\infty)^H)_{\Theta/H})}{\#(\ker(Y(F_\infty)_\Theta \longrightarrow \mathring{a}_\Lambda(Y^*(F_\infty))_\Theta))} .$$

D'autre part de la suite exacte (5) et du fait que $a_\Lambda(Z^*(F_\infty))_H$ n'a pas de sous-$\Lambda_{\Theta/H}$-modules finis non nuls (prop. I.12), on déduit que l'homomorphisme r_h

$$\mathrm{Ext}^2_\Lambda(U^*,\Lambda) \longrightarrow (\mathring{a}_\Lambda(Y^*(F_\infty))_H)^{\Theta/H}$$

est un isomorphisme si et seulement si la série caractéristique de $Z^*(F_\infty)_H$ n'est pas divisible par $\tau_{(\theta)}(h) - 1$ ce qui est vrai si et seulement si la série caractéristique de $Y^*(F_\infty)_H$ (et de $Y(F_\infty)_H$) est exactement divisible par

$$(\tau_{(\theta)}(h) - 1)^{n_F + r_F}$$

et donc si et seulement si $B_{(\theta),h}$ est non dégénérée. On en déduit donc que

(9) $$\operatorname{disc} B_{(\theta),h}(\check{S}(F), \check{S}^*(F)) \sim$$

$$\#(\check{S}(F)/T_\pi(S(F))) \cdot [\operatorname{Hom}_{\mathbb{Z}_p}(T_\pi(\check{S}(F)), \mathbb{Z}_p) : (Y(F_\infty)_H)^{\Theta/H}]$$

$$\times [\check{S}^*(F) : \operatorname{Ext}^2_\Lambda(U^*,\Lambda)][(\dot{a}_\Lambda(Y^*(F_\infty))_H)^{\Theta/H} : (Y(F_\infty)_H)^{\Theta/H}].$$

Les formules (8) et (9) donnent le lemme.

On déduit du lemme II.24 et des suites exactes (II.14) et (II.15) le lemme suivant.

Lemme 10. Soit p^{n_v} l'indice du sous-groupe de décomposition de $G(N_\infty/F)$ en v dans $G(N_\infty/F)$ et S' l'ensemble des places v de F au dessus de $\mathfrak{p}^*$ tel que F_v contienne $E_\mathfrak{p}$. On pose $r_n(T) = (\kappa(\gamma)(1+T))^{p^n} - 1$. Alors, si $f(N_\infty,T)$ est une série caractéristique de $Y(F_\infty)$, une série caractéristique de $Y(F_\infty)_{G(F_\infty/N_\infty)}$ est donnée par

$$g(N_\infty,T) = \Big(\prod_{v\in S'} r_{n_v}(T)\Big) r(T)^{-1} f(N_\infty,T)$$

avec $r(T) = \begin{cases} r_0(T) & \text{si } E_\mathfrak{p} \subset E(F) \\ 1 & \text{sinon} \end{cases}$.

Corollaire 11. $$\frac{g(N_\infty,T)}{T^{n_F+r_F}}\Big|_{T=0} = \frac{\prod_{v|\mathfrak{p}^*} \#(\tilde{E}_v(\tilde{F}_v)(p))}{\#(E(F)(\mathfrak{p}))} \frac{f(N_\infty,T)}{T^{n_F+r_F}}\Big|_{T=0}.$$

On déduit maintenant du théorème IV.22 et du corollaire 11 que le théorème 8 est vrai pour la $\mathbb{Z}_p$-extension N_∞ et que de plus la constante c/c' vaut

$$i_\mathfrak{p}\Big(\prod_{v|\mathfrak{p}} \Big(1-\frac{\psi_F(v)}{Nv}\Big) \prod_{v|\mathfrak{p}^*} \Big(1-\frac{\psi_F(v)^*}{Nv}\Big)\Big) \#(Ш(F)(\mathfrak{p})/\mathrm{div}),$$

ce qui démontre le théorème 8 en remarquant que

$$\frac{d}{ds}(\rho(\tau)^s - 1)\Big|_{s=0} = \log_p \rho(\tau).$$

4. Symétrie et comparaison des hauteurs algébriques et analytiques.

Notons C et C' les restrictions des formes bilinéaires B et B'

à $E(F) \underset{O}{\bullet} O_{\mathfrak{P}} \times E(F) \underset{O}{\bullet} O_{\mathfrak{P}^*}$. Nous avons déjà comparé les formes bilinéaires $C_{\kappa,\mathfrak{P}}$ et $<,>_{\kappa,\mathfrak{P}}$. On a en effet

$$\begin{aligned} C_{\kappa,\mathfrak{P}} &= -\log_p \kappa(\gamma) C_\gamma \qquad (\gamma \in G(N_\infty/F)) \\ &= t_{\mathfrak{P}}(F)\{\,,\}_{F,\mathfrak{P}} \qquad \text{(lemme 4)} \\ &= <,>_{\kappa,\mathfrak{P}} \qquad \text{(théorème IV.23).} \end{aligned}$$

On désire de même montrer que l'on a

$$C_{\rho,\mathfrak{P}} = <,>_{\rho,\mathfrak{P}} \tag{10}$$

pour tout homomorphisme ρ se factorisant par $\Theta = G(F_\infty/F)$. Remarquons d'abord qu'il suffit de le faire pour κ^*. En effet, on voit facilement que

$$C_{\rho^\lambda,\mathfrak{P}} = \lambda C_{\rho,\mathfrak{P}} .$$

Il suffit donc de montrer (10) pour tout homomorphisme ρ_h vérifiant $\rho_h(h) = 1$ et telle que $\log_p \rho_h(\tau_{(\theta)}(h)) = 1$, c'est-à-dire

$$\log_p \rho_h = a(\log_p \kappa^*(\gamma^*))^{-1} \log_p \kappa^* - b(\log_p \kappa(\gamma))^{-1} \log_p \kappa$$

si $h = \gamma^a \gamma^{*b}$. On a alors

$$\begin{aligned} C_{\rho_h,\mathfrak{P}} &= C_{\tau_{(\theta)}(h)} = C_{(\theta),h} \\ &= aC_{(\theta),\gamma} + bC_{(\theta),\gamma^*} \\ &= -aC_{\gamma^*} + bC_\gamma \\ &= a(\log_p \kappa^*(\gamma^*))^{-1} <,>_{\kappa^*,\mathfrak{P}} - b(\log_p \kappa(\gamma))^{-1} <,>_{\kappa,\mathfrak{P}} \\ &= <,>_{\rho_h,\mathfrak{P}} . \end{aligned}$$

Ceci montre d'ailleurs que $C_{\rho,\mathfrak{P}}$ est linéaire en ρ.

Nous devons donc montrer que

$$C_{\kappa^*,\mathfrak{P}} = <,>_{\kappa^*,\mathfrak{P}} .$$

Mais la théorie analogue relative à $\mathfrak{p}^*$ et à l'accouplement de Weil

$$ {}^tW_n(\ ,\ )^{-1} : E_{\pi^{*n}} \times E_{\pi^n} \longrightarrow \mu_{q^n} $$

donne une forme bilinéaire $C_{K^*,\mathfrak{p}^*}$

$$ E(F) \underset{O}{\bullet} O_{\mathfrak{p}^*} \times E(F) \underset{O}{\bullet} O_{\mathfrak{p}} \longrightarrow \mathbb{Q}_p $$

qui est égale à $\langle\ ,\ \rangle_{K^*,\mathfrak{p}^*} = {}^t\langle\ ,\ \rangle_{K^*,\mathfrak{p}}$ d'après l'analogue du théorème IV.23 (la transposée d'une forme bilinéaire f est notée ${}^tf$). Ce qui conduit à penser qu'il y a un lien entre $\dot{a}(\Phi_{\mathfrak{p}}(F_\infty))$ et $\Phi_{\mathfrak{p}^*}(F_\infty)$. Nous allons en effet montrer un tel lien. On rappelle que, $Y(F_\infty)$ étant de dimension projective inférieure ou égale à 1, $Y(F_\infty)$ est canoniquement isomorphe à $\dot{a}_\Lambda \circ \dot{a}_\Lambda(Y(F_\infty))$.

Théorème 12. Les deux Λ-homomorphismes $\dot{a}(\Phi_{\mathfrak{p}}(F_\infty))$ et $\Phi_{\mathfrak{p}^*}(F_\infty)$

$$ Y(F_\infty) \longrightarrow \dot{a}_\Lambda(Y^*(F_\infty)) $$

sont égaux.

Corollaire 13. Les deux formes bilinéaires ${}^tB_{\rho,\mathfrak{p}^*}$ et $B_{\rho,\mathfrak{p}}$

$$ \overset{\vee}{S}(F) \times \overset{\vee}{S}^*(F) \longrightarrow \mathbb{Q}_p $$

sont égales.

Démonstration du corollaire. Il suffit de comparer les deux diagrammes de définition des formes bilinéaires ${}^tB_{\tau,\mathfrak{p}^*}$ et $B_{\tau,\mathfrak{p}}$ (où τ est un générateur de $\Theta/\mathrm{Ker}\,\rho$). Le passage de l'un à l'autre se fait par les homomorphismes du type suivant pour un $\Lambda_{\Theta/H}$-module M

$$ \dot{a}_{\Lambda_{\Theta/H}}(M)^{\Theta/H} \longrightarrow \dot{a}_{\Lambda_{\Theta/H}}(M^{\Theta/H}) $$

induit par

$$ M^{\Theta/H} \longrightarrow M\ . $$

Passons à la démonstration du théorème. Le noeud de la démonstration est la loi de réciprocité. Nous allons d'abord nous ramener à un niveau fini. Si z est un élément de $\varprojlim H_n$, on note z_n un élément de H_n dont il provient pour n assez grand.

Lemme 14. Pour démontrer le théorème, il suffit de montrer que, si z (resp z^*) appartient à

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_\pi, \varprojlim X(F_n)_{q^n})$$

(resp.

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_{\pi^*}, \varprojlim X(F_n)_{q^n})),$$

on a pour n assez grand

$$(11) \qquad W_n(u, \eta_n(z_n)(z_n^*(u^*))) = W_n(\eta_n^*(z_n^*)(z_n(u)), u^*)$$

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

On a noté η_n^* l'analogue de η_n relatif à la théorie pour $\mathfrak{p}^*$.

Ecrivons l'égalité (11) d'une autre manière. Soit $a_u(z_n)$ un représentant de l'image de z_n dans

$$\mathrm{Hom}(E_{\pi^n}, F_n^\times / F_n^{\times q^n})$$

et idem pour z_n^* (voir paragraphe IV.1.1). On a alors

$$W_n(u, \eta_n(z_n)(z_n^*(u^*))) = z_n^*(u^*)(\sqrt[q^n]{a_u(z_n)}) / \sqrt[q^n]{a_u(z_n)},$$

$$W_n(\eta_n^*(z_n^*)(z_n(u)), u^*) = z_n(u)(\sqrt[q^n]{a_{u^*}(z_n^*)}) / \sqrt[q^n]{a_{u^*}(z_n^*)}.$$

D'autre part, si L est un corps de nombres contenant les racines q^m-ièmes de l'unité, on note

$$(\ ,\ )_{L,v}^{(m)} : L_v^\times \times L_v^\times \longrightarrow \mu_{q^m}$$

le symbole de Hilbert de L_v relatif à q^m et

$$(a,b)_L^{(m)} = \sum_v (a_v,b)_L^{(m)} \quad \text{pour} \quad a \in I_L , b \in L^\times .$$

La loi de réciprocité affirme que

$$(a,b)_L^{(m)} = 1 \quad \text{si} \quad a , b \in L^\times .$$

Pour simplifier les notations, on pose

$$\gamma_n = a_u(z_n) , \gamma_n^* = a_{u^*}(z_n^*) ,$$

$$(,)_{F_{n,v}} = (,)_{n,v} , v_{F_n} = v_n , \omega_{n,v} \text{ uniformisante de } F_n .$$

La formule (11) peut s'écrire alors

$$(12) \qquad \prod_{v \nmid \mathfrak{p}} (\omega_{n,v}^{v_n(\gamma_n^*)/q^n} , \gamma_n)_{n,v}^{(n)} \prod_{v \mid \mathfrak{p}} (\gamma_n^* , \gamma_n)_{n,v}^{(n)}$$

$$\times \prod_{v \nmid \mathfrak{p}^*} (\omega_{n,v}^{v_n(\gamma_n)/q^n} , \gamma_n^*)_{n,v}^{(n)} \prod_{v \mid \mathfrak{p}^*} (\gamma_n , \gamma_n^*)_{n,v}^{(n)} = 1 .$$

Lemme 15. 1 - Si v ne divise pas $\mathfrak{p}^*$, on a

$$(\gamma_n,\zeta)_{n,v}^{(n)} = 1 \quad \text{pour tout} \quad \zeta \in \mu_{q^n} .$$

2 - Si v divise $\mathfrak{p}^*$ et si n est assez grand (pour que le groupe de décomposition de $G(F_m/F_n)$ en v soit égal à $G(F_m/F_n)$ pour $m \geq n$), on a

$$(13) \qquad (\gamma_m,\zeta)_{m,v}^{(m)} = [(\gamma_n,\zeta')_{n,v}^{(n)}]^{q^{m-n}}$$

avec $\zeta' = N_{F_n(\mu_{q^m})/F_n}(\zeta)$ pour $\zeta \in \mu_{q^m}$.

Démonstration. La première propriété vient de ce que la valuation de γ_n est divisible par q^n et que si v divise $\mathfrak{p}$, γ_n est une puissance q^n-ième dans $F_{n,v}$. Si v divise $\mathfrak{p}^*$, on remarque que γ_m est congru ·

à $\gamma_n^{q^{m-n}}$ modulo $F_{m,v}^{\times q^m}$. L'égalité (13) se déduit alors des propriétés classiques du symbole de Hilbert.

Corollaire 15. Pour n assez grand, γ_n et γ_n^* sont des normes dans l'extension $F_n(\mu_{q^{2n}})/F_n$.

Démonstration. Il suffit de montrer que pour $n \gg 0$,

$$(\gamma_n,\zeta)_{n,v} = 1$$

pour toute place v de F_n et pour toute racine de l'unité ζ de μ_{q^n} (l'extension $F_n(\mu_{q^{2n}}) = F_n(\sqrt[q^n]{\zeta})$ pour ζ d'ordre q^n étant cyclique sur F_n), ce qui se déduit du lemme 1.

Notons δ (resp. δ^*) un élément de $F_n(\mu_{q^{2n}})$ de norme γ_n (resp. γ_n^*) sur F_n et posons pour simplifier encore $\gamma = \gamma_n$, $\gamma^* = \gamma_n^*$. Alors par la loi de réciprocité,

$$(\delta,\gamma^*)_{F_n(\mu_{q^{2n}})}^{(2n)} = 1 .$$

Pour démontrer le théorème, il suffit donc de montrer le lemme suivant.

Lemme 16. L'expression de gauche de (11) est égale à $(\delta,\gamma^*)_{F_n(\mu_{q^{2n}})}^{(2n)}$.

Démonstration. Posons $L = F_n(\mu_{q^{2n}})$. Si v est une place de F_n, on pose

$$(a,b)_{L,v}^{(2n)} = \prod_{w|v} (a_w,b)_{L,w}^{(2n)}$$

où le produit est pris sur les places de L au dessus de v et où a appartient à $\prod_{w|v} L_w$ (de composante a_w).

La démonstration du lemme 16 se fait par calcul de chacun des composants de $(\delta,\delta^*)_L^{(2n)}$.

Soit v une place de F_n. Montrons d'abord que $(\delta,\gamma^*)_{L,v}^{(2n)}$ est une racine q^n-ième de l'unité. On a en effet

$$((\delta,\gamma^*)_{L,v}^{(2n)})^{q^n} = (\delta,\gamma^*)_{L,v}^{(n)} = (\gamma,\gamma^*)_{n,v}^{(n)} ,$$

et ceci vaut 1 parce que $v_n(\gamma) \equiv v_n(\gamma^*) \equiv 0 \bmod q^n\mathbb{Z}$ et que γ ou γ^* appartiennent à $F_{n,v}^{\times q^n}$ si v divise p. On a alors

$$(\delta,\gamma^*)_{L,v}^{(2n)} = \prod_{\tau\in G(L/F_n)} \tau(\tau^{-1}\delta\,,\,\delta^*)_{L,v}^{(2n)}$$

$$= \prod_{\tau\in G(L/F_n)} (\tau^{-1}\delta\,,\,\delta^*)_{L,v}^{(2n)} = (\gamma,\delta^*)_{L,v}^{(2n)}\,.$$

D'où

$$(\delta,\gamma^*)_{L,v}^{(2n)} = (\gamma,\delta^*)_{L,v}^{(2n)}\,. \tag{14}$$

Supposons maintenant que v ne divise pas p. On a alors

$$(\delta,\gamma^*)_{L,v}^{(2n)} = (\delta,\omega_{n,v}^{v_n(\gamma^*)}\mu^*)_{L,v}^{(2n)} = (\delta,\omega_{n,v}^{v_n(\gamma^*)/q^n})_{L,v}^{(n)}(\delta,\mu^*)_{L,v}^{(2n)}$$

$$= (\gamma,\omega_{n,v}^{v_n(\gamma^*)/q^n})_{n,v}^{(n)}\,(\delta,\mu^*)_{L,v}^{(2n)}$$

avec $\gamma^* = \omega_{n,v}^{v_n(\gamma^*)}\mu^*$.

Mais μ^* est une norme dans $\prod_{w|v} L_w$, par exemple de μ'^*. D'où

$$(\delta,\mu^*)_{L,v}^{(2n)} = (\gamma,\mu'^*)_{L,v}^{(2n)} = (\omega_{n,v}^{v_n(\gamma)/q^n},\mu'^*)_{L,v}^{(n)}$$

$$= (\omega_{n,v}^{v_n(\gamma)/q^n},\mu^*)_{n,v}^{(n)}$$

$$= (\omega_{n,v}^{v_n(\gamma)/q^n},\gamma^*)_{n,v}^{(n)}$$

car $v_n(\gamma^*) \equiv 0 \bmod q^n\mathbb{Z}$. Donc

$$(\delta,\gamma^*)_{L,v}^{(2n)} = (\omega_{n,v}^{v_n(\gamma)/q^n},\gamma^*)_{n,v}^{(n)}\,(\gamma,\omega_{n,v}^{v_n(\gamma^*)/q^n})_{n,v}^{(n)} \qquad (v\nmid p). \tag{15}$$

Si maintenant v divise $\mathfrak{p}^*$, on a

$$(\delta,\gamma^*)_{L,v}^{(2n)} = (\delta,\sqrt[q^n]{\gamma^*})_{L,v}^{(n)} = (\gamma,\sqrt[q^n]{\gamma^*})_{n,v}^{(n)} \qquad (v|\mathfrak{p}^*) \tag{16}$$

et si v divise $\mathfrak{p}$, on fait de même en utilisant (14) :

$$(17) \qquad (\delta,\gamma^*)_{L,v}^{(2n)} = (q^n\sqrt{\gamma},\gamma^*)_{n,v}^{(n)} \qquad (v|\mathfrak{p}).$$

Des égalités (15), (16) et (17), on déduit le lemme 16 et donc le théorème 12.

5. Conclusion.

Nous allons d'abord réécrire une partie des résultats obtenus sous une forme qui se prête à une conjecture p-adique à deux variables de Birch et Swinnerton-Dyer des fonctions L p-adiques de Katz. Nous donnerons ensuite quelques conséqences sur la croissance du $\mathcal{O}$-rang du groupe des points rationnels de E le long d'une $\mathbb{Z}_p$-extension.

Soit toujours ρ un homomorphisme continu de Θ dans $\mathbb{Z}_p$. Au chapitre III, nous avons construit une forme bilinéaire p-adique analytique sur $E(F) \bullet_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} \times E(F) \bullet_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}$ à valeurs dans $\mathbb{Q}_p$ que nous avons noté $\langle , \rangle_{\rho,\mathfrak{p}}$. Dans ce chapitre, nous l'avons prolongé à $\overset{v}{S}(F) \times \overset{v}{S}^*(F)$. On note maintenant $<,>_{\rho,\mathfrak{p}}$ ce prolongement (au lieu de $B_{\rho,\mathfrak{p}}$). Rappelons d'autre part que n_F est le $\mathcal{O}$-rang de $E(F)$, t_F le $\mathbb{Z}_p$-rang de $T_\pi(Ш(F))$ (ou qui revient au même de $T_{\pi^*}(Ш(F))$) et que $H_{\mathfrak{p}}$ (resp. $H_{\mathfrak{p}^*}$) est une série caractéristique de $Y(F_\infty)$ (resp. $Y^*(F_\infty)$). On a de plus posé

$$L_{\mathfrak{p}}(\rho) = H_{\mathfrak{p}}(\rho\kappa^{-1}) \, , \, L_{\mathfrak{p}^*}(\rho) = H_{\mathfrak{p}^*}(\rho\kappa^{*-1}) \, .$$

Rappelons d'abord l'équation fonctionnelle vérifiée par ces fonctions d'Iwasawa.

Equation fonctionnelle. Il existe des unités u et u' de l'algèbre des fonctions d'Iwasawa tels que

$$H_{\mathfrak{p}}(\kappa^s\kappa^{*s^*}) = u(s,s^*)H_{\mathfrak{p}^*}(\kappa^{-s}\kappa^{*-s^*}) \, ,$$

$$L_{\mathfrak{p}}(\kappa^s\kappa^{*s^*}) = u'(s,s^*)L_{\mathfrak{p}^*}(\kappa^{1-s}\kappa^{*1-s^*}).$$

Rappelons maintenant une partie du théorème 8 , c'est-à-dire la formule :

$$(18)\qquad \lim_{s\to 0} \frac{H_{\mathfrak{p}}(\rho^s)}{s^{n_F+r_F}} =$$

$$u_\rho\, i_{\mathfrak{p}}\Big(\prod_{v|\mathfrak{p}}\Big(1-\frac{\psi_F(v)}{Nv}\Big)\prod_{v|\mathfrak{p}^*}\Big(1-\frac{\psi_F(v)^*}{Nv}\Big)\Big)\,\#(Ш(F)(\mathfrak{p})/\mathrm{div})\,\mathrm{disc}\,\langle\,,\rangle_{\rho,\mathfrak{p}}$$

où $\mathrm{disc}\,\langle\,,\rangle_{\rho,\mathfrak{p}} = \mathrm{disc}\langle \overset{v}{S}(F), \overset{v}{S}{}^*(F)\rangle_{\rho,\mathfrak{p}}$.

Théorème 17. La fonction d'Iwasawa $H_{\mathfrak{p}}(\kappa^s\kappa^{*s^*})$ admet le développement en s et s^* suivant

$$(19)\qquad H_{\mathfrak{p}}(\kappa^s\kappa^{*s^*}) = u\, i_{\mathfrak{p}}\Big(\prod_{v|\mathfrak{p}}\Big(1-\frac{\psi_F(v)}{Nv}\Big)\prod_{v|\mathfrak{p}^*}\Big(1-\frac{\psi_F(v)^*}{Nv}\Big)\Big)\times$$

$$\times\,\#(Ш(F)(\mathfrak{p})/\mathrm{div})\,\mathrm{disc}(\langle\,,\rangle_{\kappa,\mathfrak{p}}s+\langle\,,\rangle_{\kappa^*,\mathfrak{p}}s^*)$$

$$\text{modulo } (s,s^*)^{n_F+r_F+1},$$

avec u appartenant à $\mathbb{Z}_p^\times$.

Démonstration. Soit $P(s,s^*)$ le polynôme homogène de degré n_F+r_F tel que $H_{\mathfrak{p}}(s,s^*)$ soit congru à $P(s,s^*)$ modulo $(s,s^*)^{n_F+r_F+1}$ et notons $Q(s,s^*)$ le second membre de la formule (19). On a pour le moment montré que $P(s,s^*)$ et $Q(s,s^*)$ ont même valuation p-adique pour tout couple (s,s^*) d'éléments de $\mathbb{Z}_p$. Mais les constructions faites s'étendent par extension des scalaires. Soit R_p l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$. On pose $\Lambda' = R_p[[\Theta]] = \Lambda \underset{\mathbb{Z}_p}{\bullet} R_p$. Si M est un Λ-module, $M' = M \underset{\mathbb{Z}_p}{\bullet} R_p$ est un Λ'-module et par le lemme I.9, on a

$$a_{\Lambda'}(M') = a_\Lambda(M) \underset{\mathbb{Z}_p}{\bullet} R_p.$$

L'étude de $H_{\mathfrak{p}}(\rho^s)$ pour un homomorphisme continu ρ de $\Theta' = \Theta \underset{\mathbb{Z}_p}{\bullet} R_p$ montre alors que $P(s,s^*)$ et $Q(s,s^*)$ ont même valuation p-adique pour (s,s^*) appartenant à R_p^2. On en déduit que les deux polynômes homogènes $P(s,s^*)$ et $Q(s,s^*)$ ont même factorisation dans une clôture algébrique de $\mathbb{Q}_p$ et donc diffèrent d'une unité de $\mathbb{Z}_p$, ce qui termine la démonstration.

Notons L_∞ la $\mathbb{Z}_p$-extension de F telle que le noyau de ρ soit égal à $G(F_\infty/L_\infty)$. La construction de la forme bilinéaire $B_{\rho,\sharp}$ a été faite indépendamment de toute hypothèse sur le $\Lambda_{G(L_\infty/F)}$-rang du module $Y(L_\infty)$.

Proposition 18. *Si $<,>_{\rho,\sharp}$ est non dégénérée sur $\overset{\vee}{S}(F) \times \overset{\vee}{S}^*(F)$, le $\Lambda_{G(L_\infty/F)}$-module $Y(L_\infty)$ est de torsion et $E(L_\infty)$ modulo torsion est un $\mathbb{Z}$-module de type fini.*

Démonstration. Posons $H = G(L_\infty/F)$. Si $<,>_{\rho,\sharp}$ est non dégénérée sur $\overset{\vee}{S}(F) \times \overset{\vee}{S}^*(F)$, il existe un homomorphisme à noyau fini de $\overset{\vee}{S}(F)$ dans $Y(L_\infty)^H$. Donc $Y(L_\infty)^H$ est de rang supérieur à $n_F + r_F$ sur $\mathbb{Z}_p$. Mais il est de manière générale inférieur au $\mathbb{Z}_p$-rang de $Y(L_\infty)_H$ qui est égal à $n_F + r_F$. On en déduit que les $\mathbb{Z}_p$-rangs de $Y(L_\infty)^H$ et de $Y(L_\infty)_H$ sont égaux et donc que $Y(L_\infty)$ est un Λ_H-module de Λ_H-torsion. La dernière affirmation se déduit alors du fait que le $\mathbb{Z}_p$-rang de $E(L) \underset{O}{\otimes} O_\sharp$ est alors borné lorsque L parcourt les extensions finies de F contenues dans L_∞ et que d'autre part $E(L_\infty)$ modulo torsion est un groupe abélien libre (théorème II.4).

Dans le cas où E est une courbe définie sur $\mathbb{Q}$, une des $\mathbb{Z}_p$-extensions de K contenue dans $K_\infty = F_\infty$ joue un rôle particulier. C'est l'unique $\mathbb{Z}_p$-extension de K galoisienne sur $\mathbb{Q}$ et non abélienne sur $\mathbb{Q}$, appelé anticyclotomique dans [20]. Notons-la K_∞^-. Le groupe de Galois de K_∞^- sur $\mathbb{Q}$ est un groupe diédral. L'extension K_∞^- est aussi caractérisée par la propriété arithmétique suivante : c'est l'unique $\mathbb{Z}_p$-extension contenue dans la réunion des extensions abéliennes de K associées par la théorie du corps de classes à l'ordre de K de conducteur p^n pour $n \geq 1$ (ring class field). C'est principalement cette propriété et le fait que E est une courbe modulaire qui permet de montrer que pour une extension finie convenable F de K, $E(FK_\infty^-)$ est de rang infini ([18], [20], [16]). Greenberg a récemment obtenu des résultats fondamentaux sur $E(K_\infty^-)$ par des méthodes différentes. Nous allons nous contenter de donner des exemples d'application de la proposition 18.

Supposons que E est définie sur $\mathbb{Q}$. Notons $\overset{\vee}{S}_p(\mathbb{Q})$ la limite projective des groupes de Selmer $S(\mathbb{Q})^{(p^n)}$ pour $n \geq 1$ relativement à la multiplication par p. Les isomorphismes suivants sont canoniques

$$\overset{\vee}{S}_p(\mathbb{Q}) \underset{\mathbb{Z}}{\otimes} O \xrightarrow{\sim} \overset{\vee}{S}_p(K) \xrightarrow{\sim} \overset{\vee}{S}(K) \otimes \overset{\vee}{S}^*(K).$$

Notons t(resp. t^*) la projection de $\overset{v}{S}_p(K)$ sur $\overset{v}{S}(K)$ (resp. $\overset{v}{S}^*(K)$) et choisissons un système libre maximal $(x_1,\dots,x_n)$ du $\mathbb{Z}_p$-module $\overset{v}{S}_p(\mathbb{Q})$ (avec $n = n_K$). Le discriminant de $<\ ,\ >_{\rho,\mu}$ peut être calculé à l'aide des systèmes libres $t(x_1),\dots,t(x_n)$ et $t^*(x_1),\dots,t^*(x_n)$. Posons donc

$$D_{\rho,\mu} = \det((<t(x_i)\ ,\ t^*(x_j)>_{\rho,\mu}))_{i,j}\ .$$

Comme E est définie sur $\mathbb{Q}$, on a la propriété fonctorielle

$$<z\ ,\ z'>_{\kappa,\mu} = <\tau z\ ,\ \tau z'>_{\kappa^*,\mu^*} = <\tau z'\ ,\ \tau z>_{\kappa^*,\mu}$$

où τ est l'automorphisme non trivial de $G(K/\mathbb{Q})$. Si $\rho = \kappa^{\lambda}\kappa^{*\mu}$, on a donc

$$D(\lambda,\mu) = D_{\rho,\mu} = \det(\lambda M + \mu\,{}^tM)$$

où M est la matrice $((<t(x_i),t^*(x_j)>_{\kappa,\mu}))$ (c'est une matrice carrée d'ordre $r_K + n_K$). Posons $D_0 = D(0,1) = D(1,0)$. On peut faire les remarques suivantes (essentiellement triviales) sur la dégénérescence éventuelle de $<\ ,\ >_{\rho,\mu}$.

a) Si $r_K + n_K$ est égal à 1, la seule $\mathbb{Z}_p$-extension dégénérée (c'est-à-dire correspondant à une forme bilinéaire $<\ ,\ >_{\rho,\mu}$ dégénérée) est la $\mathbb{Z}_p$-extension anticyclotomique K_∞^- dès que la $\mathbb{Z}_p$-extension N_∞ est non dégénérée. Ainsi, dans ce cas, pour toute $\mathbb{Z}_p$-extension L_∞ de K différente de K_∞^-, $E(L_\infty)$ modulo torsion est de type fini.

Exemples.
$$y^2 = x^3 - 2x,\quad p = 5$$
$$y^2 = x^3 + 9x,\quad p = 5$$
$$y^2 = x^3 - 49x,\quad p = 5,\ 13,\ 17.$$

b) De manière générale, si $r_K + n_K$ est impair, la $\mathbb{Z}_p$-extension anticyclotomique K_∞^- est toujours dégénérée.

c) Etudions le cas particulier où $r_K + n_K$ est égal à 2. Si M est la matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, on a

$$D(\lambda,\mu) = (ad - bc)\lambda^2 + 2\lambda\mu\left(ad - bc - \frac{(b-c)^2}{2}\right) + (ad - bc)\mu^2\ .$$

Le discriminant de cette équation étant

$$(b-c)^2((b-c)^2-4D_0)$$

(avec $D_0 = ad-bc$), on en déduit que

i) si $b=c$, la seule $\mathbb{Z}_p$-extension dégénérée est l'extension K_∞^-;

ii) si $(b-c)^2 = 4D_0$, la seule $\mathbb{Z}_p$-extension dégénérée est la $\mathbb{Z}_p$-extension cyclotomique;

iii) si $(b-c)^2-4D_0$ n'est pas un carré et si b est différent de c, aucune $\mathbb{Z}_p$-extension de K n'est dégénérée;

iv) si $(b-c)^2-4D_0$ est un carré non nul et si b est différent de c, il y a exactement deux $\mathbb{Z}_p$-extensions dégénérées (distinctes).

Les deux exemples que nous avons calculés donnent le cas iv) :

$$y^2 = x^3+14x \ , \ p=5$$
$$y^2 = x^3-17x \ , \ p=5.$$

d) Nous avons encore étudié un cas où le rang de $E(\mathbb{Q})$ est 3 :

$$y^2 = x^3-226x \ , \ p=5.$$

On a ici trouvé que

$$D(\lambda,\mu) \equiv (\lambda+\mu)(107\lambda^2+53\lambda\mu+107\mu^2) \bmod 125 \ .$$

On en déduit que la seule $\mathbb{Z}_p$-extension dégénérée est K_∞^- et que pour toute $\mathbb{Z}_p$-extension L_∞ différente de K_∞^-, $E(L_\infty)$ modulo torsion est de type fini.

APPENDICE : THÉORÈME DE CASSELS

Appendice

Nous allons ici démontrer le théorème de Cassels énoncé dans le chapitre II.1.5 en nous bornant au cas de multiplication complexe utilisé ici et en nous inspirant d'une démonstration donnée par Bashmakov ([1]).

1. Accouplement de Weil.

Rappelons la définition de l'accouplement de Weil utilisé ici

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

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. $g_{n,u}$) de diviseur

$$q^n((u) - (0))$$

(resp.

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

et telles que

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

On pose alors

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

2. Accouplement local de Tate ([35])

Soit k une extension finie de F ou le complété en une place d'un tel corps. L'accouplement de Weil induit grâce au cup-produit un accouplement

$$(,)_{n,k} : H^1(k , E_{\pi^n}) \times H^1(k , E_{\pi^{*n}}) \longrightarrow H^2(k , \mu_{q^n}) .$$

Lorsque k est un corps local, le dernier groupe est isomorphe à $\mathbb{Z}/q^n\mathbb{Z}$ et l'accouplement est non dégénéré. D'autre part, notons i_n l'injection canonique

$$i_n : E(k)/\pi^{*n}E(k) \longrightarrow H^1(k,E_{\pi^{*n}})$$

et p_n la projection

$$p_n : H^1(k,E_{\pi^n}) \longrightarrow H^1(k,E)_{\pi^n} .$$

Si k est un corps local, l'orthogonal de $E(k)/\pi^{*n}E(k)$ pour $(\ ,\ )_{n,k}$ est $E(k)/\pi^nE(k)$ et l'accouplement qui s'en déduit est l'accouplement de Tate $T_{n,k}$

$$T_{n,k} : H^1(k,E)_{\pi^n} \times E(k)/\pi^{*n}E(k) \longrightarrow \mathbb{Z}/q^n\mathbb{Z} .$$

On a donc

$$T_{n,k}(x\ ,\ i_n(y)) = (x'\ ,\ y)_{n,k}$$

avec $p_n(x') = x$.

Fixons une extension finie L de F. Si v est une place finie de L, on pose $(\ ,\ )_{n,L_v} = (\ ,\ )_{n,v}, \ldots$. La théorie du groupe de Brauer montre que si f appartient à $H^1(L,E_{\pi^n})$ et g à $H^1(L,E_{\pi^{*n}})$, on a

$$\sum_v (f\ ,\ g)_{n,v} = 0$$

où la somme est prise sur toutes les places de L.

Remarquons d'autre part que si k est un corps local contenant E_{π^n}, on a

$$H^1(k,E_{\pi^n}) \xrightarrow[\sim]{\phi} \mathrm{Hom}(G(k^{ab}/k),E_{\pi^n})$$

$$H^1(k,E_{\pi^{*n}}) \xrightarrow[\sim]{\psi} \mathrm{Hom}(E_{\pi^n},k^x/k^{xq^n})$$

et que si l'on identifie $\mathrm{Hom}(E_{\pi^n},E_{\pi^n})$ avec $\mathbb{Z}/q^n\mathbb{Z}$, on a

$$(x,y)_{n,k} \cdot u = \phi(x)(\psi(y)(u)\ ,\ k^{ab}/k) \quad \text{pour } u \in E_{\pi^n}$$

($(\ ,k^{ab}/k)$ désigne le symbole d'Artin de k^x dans le groupe de Galois de l'extension abélienne de k maximale k^{ab} sur k).

3. Théorème de Cassels.

Soit T un ensemble de places de L que l'on suppose pour l'instant fini. On note $R_T^{(\pi^n)}$ le noyau de l'homomorphisme

$$H^1(L,E_{\pi^n}) \longrightarrow \prod_{v\notin T} H^1(L_v,E)$$

et $\beta_{n,T}$ l'homomorphisme

$$R_T^{(\pi^n)} \longrightarrow \prod_{v\in T} H^1(L_v,E)_{\pi^n}.$$

On définit de la même manière $R_T^{(\pi^{*n})}$ et $\beta^*_{n,T}$. Soient maintenant $Ш_T$ le noyau des homomorphismes de restriction

$$H^1(L,E) \longrightarrow \prod_{v\notin T} H^1(L_v,E)$$

et $\gamma_{n,T}$ l'homomorphisme

$$(Ш_T)_{\pi^n} \longrightarrow \prod_{v\in T} H^1(L_v,E)_{\pi^n}.$$

Soit enfin l'homomorphisme

$$\delta^*_{n,T} : S^{(\pi^{*n})} \longrightarrow \prod_{v\in T} E(L_v)/\pi^{*n}E(L_v)$$

où l'on a posé pour simplifier $S^{(\pi^{*n})} = S(L)^{(\pi^{*n})}$.

L'accouplement somme des accouplements $T_{n,v}$ pour $v\in T$ est exact et induit par la somme des $(\ ,\ )_{n,v}$ pour $v\in T$. On notera le premier $T_{n,T}$ et le second $(\ ,\ )_{n,T}$. On identifie à l'aide de $(\ ,\ )_{n,T}$ le dual de $\prod_{v\in T} H^1(L_v,E_{\pi^n})$ avec $\prod_{v\in T} H^1(L_v,E_{\pi^{*n}})$. De la suite exacte

$$0 \longrightarrow S^{(\pi^{*n})} \longrightarrow R_T^{(\pi^{*n})} \longrightarrow \prod_{v\in T} H^1(L_v,E)_{\pi^{*n}},$$

on déduit que le dual de $S^{(\pi^{*n})}$ est isomorphe au quotient du dual de $R^{(\pi^{*n})}$ par $\widehat{\beta}_{n,T}(\prod_{v\in T} E(L_v)/\pi^nE(L_v))$ où $\widehat{\beta}_{n,T}$ est l'application transposée de $\beta_{n,T}$.

Lemme 1. Soit z un élément de $\prod_{v\in T} H^1(L_v,E_{\pi^n})$. Il est orthogonal à l'image de $S^{(\pi^{*n})}$ dans $\prod_{v\in T} H^1(L_v,E_{\pi^{*n}})$ si et seulement si il est la somme d'un élément de l'image de $R_T^{(\pi^n)}$ et d'un élément de $\prod_{v\in T} E(L_v)/\pi^n E(L_v)$.

Démonstration. Soit T' la réunion de T et de l'ensemble des places de L au dessus de p. Soit $L_{T'}$ l'extension de L non ramifiée au dehors de T' maximale. Les théorèmes de dualité globale de Poitou et Tate affirment que la suite

$$H^1(L_{T'}/L,E_{\pi^n}) \longrightarrow \prod_{v\in T'} H^1(L_v,E_{\pi^n}) \longrightarrow \widehat{H^1(L_{T'}/L,E_{\pi^{*n}})}$$

est exacte (si l'on identifie $E_{\pi^{*n}}$ avec $\mathrm{Hom}(E_{\pi^n},\mu_{q^n})$ par l'accouplement de Weil). On en déduit facilement que la suite

$$R_T^{(\pi^n)} \longrightarrow \prod_{v\in T} H^1(L_v,E_{\pi^n}) \longrightarrow \widehat{R_T^{(\pi^{*n})}}$$

est exacte. Le noyau de

$$\prod_{v\in T} H^1(L_v,E_{\pi^n}) \longrightarrow \widehat{S^{(\pi^{*n})}}$$

est donc égal à la somme de l'image de $R_T^{(\pi^n)}$ et de $\prod_{v\in T} E(L_v)/\pi^n E(L_v)$. Ce noyau est aussi l'orthogonal de l'image de $S^{(\pi^{*n})}$ dans $\prod_{v\in T} H^1(L_v,E_{\pi^{*n}})$, ce qui démontre le lemme 1.

Théorème 2 (Cassels). L'image de $\gamma_{n,T}$

$$\gamma_{n,T} : (Ш_T)_{\pi^n} \longrightarrow \prod_{v\in T} H^1(L_v,E)_{\pi^n}$$

est orthogonal à l'image de $\delta_{n,T}$

$$\delta_{n,T} : S^{(\pi^{*n})} \longrightarrow \prod_{v\in T} E(L_v)/\pi^{*n}E(L_v),$$

ce qui peut encore s'exprimer par : le dual du conoyau de $\gamma_{n,T}$ est isomorphe à l'image de $\delta_{n,T}$.

Démonstration. Soit f un élément de $(Ш_T)_{\pi^n}$ et $x=(x_v)$ un élément

de l'image de $\delta_{n,T}$. Nous devons d'abord montrer que

$$T_{n,T}(\gamma_{n,T}(f),x) = 0 .$$

Soient F un élément de $R_T^{(\pi^n)}$ dont l'image dans $H^1(L,E)$ est f et G un élément de $S^{(\pi^{*n})}$ dont les composantes locales sont x_v pour $v \in T$. On note F_v (resp. G_v) la composante locale de F (resp. G) dans $H^1(L_v,E_{\pi^n})$ (resp. $H^1(L_v,E_{\pi^{*n}})$). Comme F_v (resp. G_v) appartient à $E(L_v)/\pi^n E(L_v)$ (resp. $E(L_v)/\pi^{*n}E(L_v)$) le symbole

$$(F_v , G_v)_{n,v}$$

est nul pour toute place v n'appartenant pas à T. On a donc

$$T_{n,T}(\gamma_{n,T}(f),x) = \sum_{v\in T} (F_v,x_v)_{n,v} = \sum_{v} (F_v,G_v)_{n,v}$$

et cette dernière expression est nulle car F et G sont des éléments globaux. Donc, l'image de $\gamma_{n,T}$ annule l'image de $\delta_{n,T}$. Réciproquement, soit $f = (f_v)$ un élément de $\prod_{v\in T} H^1(L_v,E)_{\pi^{*n}}$ annulant l'image de $\delta_{n,T}$ et soit F un relèvement de f dans $\prod_{v\in T} H^1(L_v,E_{\pi^{*n}})$. Il est orthogonal à l'image de $S^{(\pi^{*n})}$ dans $\prod_{v\in T} H^1(L_v,E_{\pi^{*n}})$ pour l'accouplement $(\ ,\ )_{n,T}$. On en déduit par le lemme 1 qu'il est égal à la somme d'un élément de $\prod_{v\in T} E(L_v)/\pi^n E(L_v)$ et d'un élément de l'image de $R_T^{(\pi^n)}$ dans $\prod_{v\in T} H^1(L_v,E_{\pi^n})$. Donc f appartient lui à l'image de $(Ш_T)_{\pi^n}$ par $\gamma_{n,T}$, ce qui démontre le théorème.

Donnons maintenant deux corollaires.

Corollaire 3. Soit $C_n(L)$ le groupe défini par la suite exacte

$$0 \longrightarrow Ш(L)_{\pi^n} \longrightarrow H^1(L,E)_{\pi^n} \longrightarrow \sum_v H^1(L_v,E)_{\pi^n} \longrightarrow C_n(L) \longrightarrow 0.$$

Alors, le dual de $C_n(L)$ est isomorphe à $S(L)^{(\pi^{*n})}$.

Démonstration. Le corollaire s'obtient par passage à la limite sur les ensembles finis T. Si $T(L)$ est l'ensemble de toutes les places de L, l'homomorphisme $\delta_{n,T(L)}$ est alors injectif et $Ш(L)_{T(L)}$ est égal à

$H^1(L,E)$.

Corollaire 4. Soit $B_n(L)$ le groupe défini par la suite exacte

$$0 \longrightarrow S(L)^{(\pi^n)} \longrightarrow S'(L)^{(\pi^n)} \longrightarrow \prod_{v|\mathfrak{p}} H^1(L_v,E)_{\pi^n} \longrightarrow B_n(L) \longrightarrow 0.$$

Alors le dual de $B_n(L)$ est isomorphe à l'image de $S(L)^{(\pi^{*n})}$ dans $\prod_{v|\mathfrak{p}} E(L_v)/\pi^{*n}E(L_v)$.

Démonstration. On prend ici pour T l'ensemble des places au dessus de $\mathfrak{p}$. Il est facile de voir que $B_n(L)$ est aussi le conoyau de $\gamma_{n,T}$.

La proposition II.8 s'en déduit, les homomorphismes de transition

$$B_n(L) \longrightarrow B_{n+1}(L)$$

induites par les inclusions

$$E_{\pi^n} \longrightarrow E_{\pi^{n+1}}$$

correspondant par les accouplements $T_{n,T}$ aux homomorphismes de transition

$$S(L)^{(\pi^{*n+1})} \longrightarrow S(L)^{(\pi^{*n})}$$

induites par les multiplications par π^*

$$E_{\pi^{*n+1}} \longrightarrow E_{\pi^{*n}}.$$

BIBLIOGRAPHIE

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

[2] D. BERNARDI : Hauteurs p-adiques sur les courbes elliptiques. Séminaire de théorie des nombres. Progress in Mathematics, vol. 12, p. 1-14. Paris : Birkhäuser 1979-80.

[3] D. BERNARDI, C. GOLDSTEIN et N. STEPHENS : Notes p-adiques sur les courbes elliptiques, à paraître.

[4] D. BERTRAND : Valeurs de fonctions thêta et hauteurs p-adiques. Séminaire de théorie des nombres. Progress in Mathematics, vol. 22, p. 1-11. Paris : Birkhäuser (1982).

[5] N. BOURBAKI : Algèbre commutative. Paris : Hermann.

[6] N. BOURBAKI : Algèbre homologique, chapitre 10, Paris : Masson 1980.

[7] J.W.S. CASSELS : Arithmetic on curves of genus 1. J. Reine angew. Math. (IV) 207, p. 234-246 (1962), (VIII) 217, p. 180-189 (1965).

[8] J. COATES : Elliptic curves with complex multiplication. Hermann Weyl Lectures 1979, Annals of Math. Studies, à paraître.

[9] J. COATES et C. GOLDSTEIN : Some remarks on the main conjecture for elliptic curves with complex multiplication. Am. Journal of Math. 103, p. 411-435 (1983).

[10] J. COATES et A. WILES : On p-adic L functions and elliptic units. J. Austral. Math. Soc. (series A) 26, p. 1-25 (1978).

[11] F. DIAZ Y DIAZ : Tables minorant la racine n-ième du discriminant d'un corps de degré n. Publ. Math. Orsay 80-06 (1980).

[12] R. GREENBERG : On the structure of certain galois groups. Invent. Math. 47, p. 85-99 (1978).

[13] R. GREENBERG : Iwasawa's theory and p-adic L functions for imaginary quadratic fields. Number theory related to Fermat's last theorem. Progress in Mathematics, vol. 26, p. 275-285. Birkhäuser (1982).

[14] R. GREENBERG : On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication. Invent. Math. (à paraître).

[15] B.H. GROSS : Arithmetic on elliptic curves with complex multiplication. Lecture Notes in Mathematics 776, Berlin-Heidelberg-New York : Springer (1980).

[16] M. HARRIS : Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields. Invent. Math. 51, p. 123-141 (1979).

[17] K. IWASAWA : On $\mathbb{Z}_p$-extensions of algebraic numbers. Annals of Math. 98, p. 246-326 (1973).

[18] P.F. KURČANOV : Elliptic curves of infinite rank over Γ-extensions. Mat. U.S.S.R. Sbornik. vol. 19 (1973).

[19] B. MAZUR : Rational points on abelian varieties with values in towers of number fields. Invent. Math. 18, p. 183-266 (1972).

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

[21] B. MAZUR et J. TATE : Canonical height pairings via biextensions. Vol. dédié à Shafarevič. Progress in Mathematics. Birkhäuser (à paraître).

[22] A. NERON : Hauteurs et fonctions thêta. Rend. Sci. Math. Milano 46, p. 111-135 (1976).

[23] A. NERON : Fonctions thêta p-adiques et hauteurs p-adiques. Séminaire de théorie des nombres. Progress in Mathematics, vol. 22. Paris : Birkhäuser (1982).

[24] T. NGUYEN-QUANG-DO : Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa. Thèse d'Etat (Orsay) 1982.

[25] B. PERRIN-RIOU : Groupe de Selmer d'une courbe elliptique à multiplication complexe. Comp. Math. 43, p. 387-417 (1981).

[26] B. PERRIN-RIOU : Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe. Invent. Math. 70, p. 369-398 (1983).

[27] B. PERRIN-RIOU : Sur les hauteurs p-adiques. C.R. Acad. Sc. Paris Paris, t. 296, p. 291-294 (1983).

[28] G. POITOU : Théorèmes de dualité globale (cours à Grenoble non publié).

[29] G. ROBERT : Nombres de Hurvitz et unités elliptiques : un critère de régularité pour les extensions abéliennes d'un corps quadratique imaginaire. Thèse d'Etat (Orsay) 1977.

[30] K. RUBIN et A. WILES : Mordell-Weil groups of elliptic curves over cyclotomic fields. Number Theory related to Fermat's last theorem. Progress in Mathematics, vol. 26, p. 237-254. Birkhäuser (1982).

[31] P. SCHNEIDER : p-adic heights. Invent. Math. 69, p. 401-409 (1982).

[32] P. SCHNEIDER : Iwasawa L functions of varieties over a number field. A first approach. Invent. Math. 71, p. 251-293 (1983).

[33] J.-P. SERRE : Algèbre locale. Multiplicités. Lecture Notes in Mathematics 11, Berlin-Heidelberg-New York : Springer (1975).

[34] J.-P. SERRE et J. TATE : Good reduction of abelian varieties. Annals of Math. 88, p. 492-517 (1968).

[35] J. TATE : WC-groups over p-adic fields. Séminaire Bourbaki, n° 156 (décembre 1957).

[36] J. TATE : The arithmetic of elliptic curves. Invent. Math. 23, p. 179-206 (1974).

[37] J.-P. WINTENBERGER : Structure galoisienne de limites projectives d'unités locales. Comp. Math. 42, p. 89-104 (1980).