COMPOSITIO MATHEMATICA

PATRICK BILLOT

Quelques aspects de la descente sur une courbe elliptique dans le cas de réduction supersingulière

Compositio Mathematica, tome 58, n° 3 (1986), p. 341-369

<http://www.numdam.org/item?id=CM_1986__58_3_341_0>

[1] Compositio Mathematica 58 (1986) 341–369

QUELQUES ASPECTS DE LA DESCENTE SUR UNE COURBE ELLIPTIQUE DANS LE CAS DE RÉDUCTION SUPERSINGULIÈRE

Patrick Billot

Introduction

Soit E une courbe elliptique définie sur un corps de nombres F, à multiplication complexe par un corps quadratique imaginaire K que nous supposerons inclus dans F. Si p est un nombre premier, le corps $F(E_{p^\infty})$ engendré sur F par les coordonnées des points de p^∞-torsion de E contient une unique $\mathbb{Z}_p^2$-extension F_∞ de F. Pour chaque corps N avec $F \subset N \subset F_\infty$, on définit le groupe de Selmer:

$$S(N) = \mathrm{Ker}\left(H^1(N,\ E_{p^\infty}) \to \prod_v H^1(N_v,\ E) \right).$$

Si N est le corps F_∞, ou une $\mathbb{Z}_p$-extension de F contenue dans F_∞, le dual de Pontryagin $\widehat{S(N)}$ de $S(N)$ est un module de type fini sur l'algèbre d'Iwasawa du groupe $\mathrm{Gal}(N/F)$. Dans le cas où p est un nombre premier de bonne réduction ordinaire $\widehat{S(F_\infty)}$ est conjecturalement un module de torsion et la structure des modules $\widehat{S(N)}$ ainsi que leur interprétation arithmétique ont été largement éclaircies.

Le cas où p est un nombre premier de bonne réduction supersingulière, que nous considérons ici, reste encore très obscur; le module $\widehat{S(N)}$ n'est plus de torsion sur l'algèbre d'Iwasawa ce qui en rend l'examen plus délicat. L'objet de cet article est de montrer que l'étude du sous-module de torsion de $\widehat{S(N)}$ est étroitement liée à celle du dual de Pontryagin d'un sous-module $\Sigma(N)$ de $S(N)$ naturellement introduit dans la théorie de la descente:

$$\Sigma(N) = \mathrm{Ker}\left(S(N) \to \prod_{v \mid p} H^1(N_v,\ E_{p^\infty}) \right).$$

Les deux principaux résultats, énoncés ci-dessous, sont obtenus dans le paragraphe 3 en faisant l'hypothèse de Léopoldt sur tous les corps

intermédiaires de la $\mathbb{Z}_p^2$-extension F_∞, signalons toutefois que pour le premier cette hypothèse est superflue ([1]).

Cas a: $N = F_\infty$
On montre (Théorème 3.24) l'existence d'un pseudo-isomorphisme entre le sous-module de torsion de $\widetilde{S(F_\infty)}$ et $\widetilde{\Sigma(F_\infty)}$, avec l'action inversée du groupe de Galois sur ce dernier module (voir 3.4).

Cas b: N est une $\mathbb{Z}_p$-extension de F.
On suppose ici que $\widetilde{\Sigma(N)}$ est un module de torsion sur l'algèbre d'Iwasawa identifiée à $\mathbb{Z}_p[[T]]$, on pense que cette condition est toujours satisfaite mais on ne la vérifiera que pour presque toute $\mathbb{Z}_p$-extension de F contenue dans F_∞. Si $f(T)$ est la série caractéristique de sous-module de torsion de $\widetilde{S(N)}$ et $g(T)$ celle de $\widetilde{\Sigma(N)}$, on établit l'égalité à un élément inversible près (Théorème 3.25):

$$g(T) = f\left(\frac{1}{1+T} - 1\right).$$

Ce dernier résultat permet de donner, pour certaines courbes, des exemples de $\mathbb{Z}_p$-extensions N telles que le sous-module de torsion de $\widetilde{S(N)}$ ne soit pas pseudo-nul. Notons enfin que les deux premiers paragraphes sont de nature purement algébrique et consacrés à la définition et aux méthodes de calcul de l'adjoint d'un module de torsion sur l'algèbre d'Iwasawa d'un groupe topologique isomorphe à $\mathbb{Z}_p^2$.

§1. Résultats préliminaires

(A) Quelques résultats de cohomologie locale

Les démonstrations des résultats rappelés ci-dessous se trouvent dans le livre de A. Grothendieck cité [L.C].

Soient A un anneau local noetherien, m son idéal maximal, k son corps résiduel.

On note H_m^i les foncteurs dérivés du foncteur sur Mod(A):

$$M \to H_m^0(M)$$

$$= \{\text{sections de } M \text{ à support dans le fermé défini par } m\}.$$

Propriétés des foncteurs H_m^i.

C1. La suite exact longue de cohomologie associée à toute suite exacte:

$$0 \to M' \to M \to M'' \to 0.$$

C2. Pour tout A-module M et tout $i \geqslant 0$, $H^i_m(M)$ est une A-module à support dans le fermé défini par m.
C3. La suite:

$$(*) \quad 0 \to H^0_m(M) \to M \to H^0(\mathrm{Spec}(A) - \{m\}, M)$$

$$\to H^1_m(M) \to 0$$

est exacte ([L.C] Proposition 2.2).
C4. Changement de base:

Si $A \to A'$ est un homomorphisme local tel que mA' soit un idéal m' primaire et si M' est un A'-module:

$$H^i_{m'}(M') = H^i_m(M') \quad ([\text{L.C}] \text{ Corollaire 5.7}).$$

THÉORÈME DE DUALITÉ LOCALE ([L.C] Théorème 6.3):
Soit A un anneau de Gorenstein complet de dimension n:

(1) *$H^n_m(A)$ est une enveloppe injective de k.*

(2) *Pour tout A-module M de type fini on a un isomorphisme fonctoriel:*

$$\mathrm{Ext}^i_A(M, A) \tilde{\to} \mathrm{Hom}_A\big(H^{n-i}_m(M), H^n_m(A)\big).$$

REMARQUE: On appliquera ce théorème dans le cas où A est un anneau régulier complet ou le quotient d'un tel anneau par un élément non nul de m.

Dans la suite nous rencontrerons la situation suivante: A est un anneau vérifiant les hypothèses du théorème de dualité, contenant $\mathbb{Z}_p$ et de corps résiduel $\mathbb{F}_p$. L'enveloppe injective $\mathbb{Q}_p/\mathbb{Z}_p$ de $\mathbb{F}_p$ sur $\mathbb{Z}_p$ est alors facteur direct de $H^n_m(A)$ comme $\mathbb{Z}_p$-module, notons ϕ la projection de $H^n_m(A)$ sur $\mathbb{Q}_p/\mathbb{Z}_p$; si M est un A-module l'application ϕ induit un homomorphisme naturel de A-modules:

$$\phi_* : \mathrm{Hom}_A\big(M, H^n_m(A)\big) \to \mathrm{Hom}_{\mathbb{Z}_p}\big(M, \mathbb{Q}_p/\mathbb{Z}_p\big).$$

(le second module est un A-module par l'action de A sur M).

PROPOSITION 1.1: *Soit M un A-module dont le support est le fermé défini par m, alors l'application ϕ_* est un isomorphisme.*

DÉMONSTRATION: On suppose tout d'abord $M = k$, le résultat est alors conséquence des isomorphismes suivants:

$$\mathrm{Hom}_A\big(\mathbb{F}_p, H^n_m(A)\big) \tilde{\to} \mathrm{Hom}_{\mathbb{F}_p}\big(\mathbb{F}_p, \mathbb{F}_p\big) \tilde{\to} \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathbb{F}_p, \mathbb{Q}_p/\mathbb{Z}_p\big).$$

Ces isomorphismes résultent du fait que $H_m^n(A)$. (resp.: $\mathbb{Q}_p/\mathbb{Z}_p$) est l'enveloppe injective sur A (resp. sur $\mathbb{Z}_p$) de $\mathbb{F}_p$.

Supposons maintenant que M est de type fini, il admet alors une suite de composition dont les quotients successifs sont isomorphes à $\mathbb{F}_p$. Les deux foncteurs $\mathrm{Hom}_A(\cdot, H_m^n(A))$ et $\mathrm{Hom}_{\mathbb{Z}_p}(\cdot, \mathbb{Q}_p/\mathbb{Z}_p)$ sont exacts sur $\mathrm{Mod}(A)$, le résultat est alors conséquence du cas particulier déja traité.

Dans le cas général, on écrit M comme limite inductive de ses sous-modules M_j de type fini:

$$\begin{aligned}\mathrm{Hom}_A(M, H_m^n(A)) &= \mathrm{Hom}_A\Big(\varinjlim M_j, H_m^n(A)\Big)\\ &= \varprojlim \mathrm{Hom}_A(M_j, H_m^n(A))\\ &\xrightarrow{\sim} \varprojlim \mathrm{Hom}_{\mathbb{Z}_p}(M_j, \mathbb{Q}_p/\mathbb{Z}_p)\\ &= \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p).\end{aligned}$$

COROLLAIRE 1.2: *Les hypothèses sur A étant les mêmes que précédemment, si M est un A-module de type fini on a un isomorphisme*:

$$\mathrm{Ext}_A^i(M, A) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}\big(H_m^{n-i}(M), \mathbb{Q}_p/\mathbb{Z}_p\big).$$

REMARQUE: Lorsque $A = \mathbb{Z}_p[[T]]$ ce résultat et la suite exacte $(*)$ permettent de montrer immédiatement que l'adjoint d'un A-module de torsion M tel qu'il est défini par Iwasawa [4] est isomorphe à $\mathrm{Ext}_A^1(M, A)$.

(B) Comportement des invariants λ et μ dans une $(\mathbb{Z}_p)^2$-extension

Notations:

Θ = un groupe topologique isomorphe à $(\mathbb{Z}_p)^2$

$$\Lambda = \Lambda_\Theta = \varprojlim \mathbb{Z}_p[\Theta/\Theta^{p^n}]$$

A tout choix γ, γ' de deux générateurs topologiques de Θ est associé, par la méthode classique, un isomorphisme $\mathbb{Z}_p[[T, T']] \xrightarrow{\sim} \Lambda$ qui à T (resp. T') associe $\gamma - 1$ (resp. $\gamma' - 1$). Ce choix étant fait, si n_0 et m_0 sont deux

entiers, on pose pour $n \geqslant n_0$ et $m \geqslant m_0$ n et m positifs:

$$v_n = \frac{\gamma^{p^n} - 1}{\gamma^{p^{n_0}} - 1} = \frac{(1+T)^{p^n} - 1}{(1+T)^{p^{n_0}} - 1}$$

$$v'_m = \frac{\gamma'^{p^m} - 1}{\gamma'^{p^{m_0}} - 1} = \frac{(1+T)^{p^m} - 1}{(1+T)^{p^{m_0}} - 1}$$

Nous conviendrons que si $n_0 < 0$ (resp. $m_0 < 0$), $v_n = \gamma^{p^n} - 1$ (resp. $v'_m = \gamma'^{p^m} - 1$), enfin on notera $\Lambda_2 = \mathbb{Z}_p[[T']]$.

LEMME 1.3: *Soient M un Λ-module de type fini et de torsion, f sa série caractéristique et $n \geqslant n_0$. Le Λ_2-module M/v_nM est de torsion si et seulement si $(v_n, f) = 1$.*

DÉMONSTRATION:

$$M/_{v_nM} \text{ de } \Lambda_2\text{-torsion} \Leftrightarrow \dim_{\Lambda_2}\left(M/_{v_nM}\right) \leqslant 1$$

$$\Leftrightarrow \dim_{\Lambda/v_n\Lambda}\left(M/_{v_nM}\right) \leqslant 1 \Leftrightarrow \dim_{\Lambda}\left(M/_{v_nM}\right) \leqslant 1.$$

Le dernière condition est vérifiée si et seulement si les localisés de $M/_{v_nM}$ en les idéaux premiers de hauteur 1 de Λ sont nuls, c'est-à-dire si et seulement si $(v_n, f) = 1$.

LEMME 1.4: *Soient M vérifiant les conditions du Lemme* 1.3, *$n \geqslant n_0$, $m \geqslant m_0$. $M/_{v_nM + v'_mM}$ est fini si et seulement si $(v_n, f) = 1$ dans Λ et $(v'_m, f_n) = 1$ dans Λ_2 où f_n désigne la série caractéristique de $M/_{v_nM}$ comme Λ_2-module.*

DÉMONSTRATION: On utilise le lemme 1.3 et le fait que, pour un Λ_2-module N de type fini $N/_{v'_mN}$ est fini si et seulement si N est de torsion et v'_m est premier à la série caractéristique de N.

Dans la suite si M est un Λ-module de torsion tel que, pour tout $n \geqslant n_0$, $M/_{v_nM}$ soit un Λ_2-module de torsion, on notera $\lambda_n(M)$ et $\mu_n(M)$ les invariants d'Iwasawa du Λ_2-module $M/_{v_nM}$.

PROPOSITION 1.5: *Soit M un Λ-module pseudo-nul (i.e.: $M_{\mathfrak{p}} = 0$ pour tout idéal $\mathfrak{p}$ de Λ de hauteur* 1), *les invariants λ_n et μ_n sont constants pour n assez grand.*

DÉMONSTRATION:

$$0 \to {}_{v_n}(M) \to M \xrightarrow{v_n} M \to M/_{v_n M} \to 0.$$

On sait ([2] Proposition A) que, pour presque tout choix de γ'' générateur topologique d'un facteur direct de Θ, le module M est de type fini et de torsion sur $\mathbb{Z}_p[[T'']]$ avec $T'' = \gamma'' - 1$. En particulier ce résultat est vrai pour $\gamma'' = \gamma^{p^n}\gamma'$ avec n assez grand. Si l'on constate maintenant que les structures de ${}_{v_n}(M)$ et $M/_{v_n M}$ comme $\mathbb{Z}_p[[T']]$ et $\mathbb{Z}_p[[T'']]$-modules sont les mêmes puisque γ^{p^n} opère trivialement sur ces 2 modules, on peut affirmer que les invariants de ${}_{v_n}(M)$ et $M/_{v_n M}$ sur $\mathbb{Z}_p[[T']]$ sont égaux à ceux relatifs à $\mathbb{Z}_p[[T'']]$. La suite exacte précédente, regardée comme suite de $\mathbb{Z}_p[[T'']]$-modules permet de conclure à l'égalité des invariants de ${}_{v_n}(M)$ et $M/_{v_n M}$. Il ne reste plus qu'à vérifier que la suite croissante des sous-modules ${}_{v_n}(M)$ de M est stationnaire, ce qui est clair puisque M est noetherien.

Signalons le résultat plus général dû à Cuoco [2] que nous n'utiliserons pas dans la suite.

PROPOSITION 1.6: *Soit M un Λ-module de torsion tel que $M/_{v_n M}$ soit de Λ_2-torsion pour tout $n \geqslant n_0$. Les invariants $\lambda_n(M)$ et $\mu_n(M)$ pour n assez grand ne dépendent, à une constante près, que de la série caractéristique de M et ils ne sont tous deux constants que si M est pseudo-nul.*

§2. Adjoints: Définition et Calcul

Dans la suite, le groupe Θ et les anneaux Λ, Λ_2 sont ceux définis dans le paragraphe 1.(B).

Soit M un Λ-module de type fini et de torsion, B. Perrin-Riou a défini dans sa thèse l'adjoint de M par $a_\Lambda(M) = \mathrm{Ext}^1_\Lambda(M, \Lambda)$. Nous montrons que, sous des hypothèses assez larges, cet adjoint peut se calculer par des techniques analogues à celles utilisées par Iwasawa dans le cas d'une variable.

Rappelons ici que dans la situation analogue à une variable, c'est-à-dire $\Theta \simeq \mathbb{Z}_p$, Iwasawa [4] a montré, dans notre terminologie, que si M est de torsion et les v_n premiers à la série caractéristique de M, $H^1_m(M) = \varinjlim(M/_{v_n M})$, la limite étant prise sur la multiplication par $\dfrac{v_p}{v_n}$ pour $p \geqslant n$.

Revenons maintenant à notre cas. Si M est un Λ-module de type fini, pour tout couple (n, m) d'entiers tels que $n \geqslant n_0$ et $m \geqslant m_0$ soit $M_{(n,m)} = M/_{v_n M + v'_m M}$. Si $p \geqslant n$ et $q \geqslant m$ on définit un Λ-homomorphisme

$$\phi^{(p,q)}_{(n,m)} : M_{(n,m)} \to M_{(p,q)}$$

en faisant correspondre à la classe de x modulo $(v_n M + v'_m M)$ celle de $\frac{v_p}{v_n} \cdot \frac{v'_q}{v'_m} \cdot x$ modulo $(v_p M + v'_q M)$. On forme ainsi un système inductif indexé par les couples (m, n).

LEMME 2.1: *Soit M un Λ-module de type fini, pseudo-nul, tel que $M/_{v_n M + v'_m M}$ soit fini pour $n \geqslant n_0$, $m \geqslant m_0$ alors* $\varinjlim M_{(n,m)} = 0$.

DÉMONSTRATION: L'hypothèse faite sur $M/_{v_n M + v'_m M}$ montre que v'_m est premier à la série caractéristique de $M/v_n M$ sur Λ_2. En utilisant les résultats d'Iwasawa on sait que:

$$\mathrm{Hom}_{\mathbf{Z}_p}\left(\varinjlim_{m}\left(M/_{v_n M + v'_m M}\right), \mathbb{Q}_p/\mathbf{Z}_p\right) \simeq a_{\Lambda_2}\left(M/_{v_n M}\right).$$

D'après la Proposition 1.5, il existe un entier n_1 $(\geqslant n_0)$ tel que, pour $n \geqslant n_1$, les invariants de $M/_{v_n M}$ soient tous égaux. La projection naturelle de $M/_{v_{n+1} M}$ sur $M/_{v_n M}$ est alors un pseudo-isomorphisme dont l'adjoint donne un isomorphisme $a_{\Lambda_2}(M/_{v_n M}) \xrightarrow{\sim} a_{\Lambda_2}(M/_{v_{n+1} M})$. Enfin par passage au dual on obtient: $\varinjlim_{m}(M/_{v_{n+1} M + v'_m M}) \xrightarrow{\sim} \varinjlim_{m}(M/_{v_n M + v'_m M})$ induit par les projections naturelles. Ce dernier isomorphisme permet d'identifier $\varinjlim_{m}(M/_{v_n M + v'_m M})$ à $\varinjlim_{m}(M/_{v_{n_1} M + v'_m M})$ et par conséquent:

$$\begin{aligned}
\varinjlim_{(n,m)} M_{(n,m)} &= \varinjlim_{n}\left(\varinjlim_{m}\left(M/_{v_n M + v'_m M}\right)\right) \\
&= \varinjlim_{n}\left(\varinjlim_{m}\left(M/_{v_{n_1} M + v'_m M}\right)\right) \\
&= \varinjlim_{m}\left(\varinjlim_{n}\left(M/_{v_{n_1} M + v'_m M}\right)\right).
\end{aligned}$$

Le système inductif $\varinjlim_{n}(M/_{v_{n_1} M + v'_m M})$ est pris selon les multiplications par v_p/v_n pour $p \geqslant n$. Il est alors clair, puisque $M/_{v_{n_1} M + v'_m M}$ est fini et que v_p/v_n tend vers 0 pour la topologie m-adique que $\varinjlim_{n}(M/_{v_{n_1} M + v'_m M}) = 0$ et donc $\varinjlim_{(n,m)} M_{(n,m)} = 0$.

LEMME 2.2: *Soit M un Λ-module de type fini, supposons que pour $n \geqslant n_0$ v_n n'est pas diviseur de zéro dans M, alors*

$$H^2_m(M) = \varinjlim_{n} H^1_{m_2}\left(M/_{v_n M}\right)$$

où m_2 est l'idéal maximal de Λ_2 et $M/_{v_nM}$ est considéré comme Λ_2-module.

DÉMONSTRATION: Considérons le diagramme commutatif suivant pour $p \geqslant n$:

$$\begin{array}{ccccccc} 0 \to M & \xrightarrow{\cdot v_n} & M & \to & M/_{v_nM} & \to 0 \\ \| & & \downarrow \cdot \frac{v_p}{v_n} & & \downarrow \cdot \frac{v_p}{v_n} & & \\ 0 \to M & \xrightarrow{\cdot v_p} & M & \to & M/_{v_pM} & \to 0 \end{array}$$

Par passage à la cohomologie locale on obtient:

$$\begin{array}{ccccccccc} \to H^1_m(M) & \xrightarrow{\cdot v_n} & H^1_m(M) & \to H^1_m(M/_{v_nM}) & \to H^2_m(M) & \xrightarrow{\cdot v_n} & H^2_m(M) & \to \\ \| & & \downarrow \cdot \frac{v_p}{v_n} & \downarrow \cdot \frac{v_p}{v_n} & \| & & \downarrow \cdot \frac{v_p}{v_n} & \\ \to H^1_m(M) & \xrightarrow{\cdot v_p} & H^1_m(M) & \to H^1_m(M/_{v_pM}) & \to H^2_m(M) & \xrightarrow{\cdot v_p} & H^2_m(M) & \to \end{array}$$

Les modules $H^2_m(M)$ et $H^2_m(M)$ sont à support dans le fermé défini par l'idéal m et la suite $\frac{v_p}{v_n}$ tend vers 0 pour la topologie m-adique (lorsque $p \to \infty$), par conséquent $\lim\limits_{\overrightarrow{n}} H^1_m(M) = \lim\limits_{\overrightarrow{n}} H^2_m(M) = 0$ les limites inductives étant prises sur les multiplications par $\frac{v_p}{v_n}$ pour $p \geqslant n$. Le passage à la limite inductive dans le diagramme précédent donne donc un isomorphisme:

$$H^2_m(M) \xrightarrow{\sim} \lim_{\overrightarrow{n}} H^1_m\left(M/_{v_nM}\right).$$

En utilisant la Propriété C_4 du Paragraphe 1 on voit que $H^1_m(M/_{v_nM}) \simeq H^1_{m_2}(M/_{v_nM})$.

PROPOSITION 2.3: *Soit M un Λ-module de type fini, supposons que pour $n \geqslant n_0$ et $m \geqslant m_0$ v_n n'est pas diviseur de zéro dans M et v'_m n'est pas diviseur de zéro dans M/v_nM, on a un isomorphisme*:

$$\mathrm{Ext}^1_\Lambda(M, \Lambda) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}\left(\lim_{\overrightarrow{(n,m)}} \left(M_{(n,m)}(p)\right), \mathbf{Q}_p/\mathbf{Z}_p\right)$$

où $M_{(n,m)}(p)$ est la p-torsion de $M_{(n,m)}$.

DÉMONSTRATION: La méthode utilisée dans le Lemme précédent, appliquée au Λ_2-module M/v_nM, nous donne les isomorphismes:

$$H^1_{m_2}\left(M/_{v_nM}\right) \tilde{\to} \varinjlim_n H^0_{m_2}\left(M/_{v_nM+v'_mM}\right)$$

$$\tilde{\to} \varinjlim_n H^0_{(p)}\left(M/_{v_nM+v'_mM}\right)$$

où (p) est l'idéal maximal de $\mathbb{Z}_p$. Si l'on remarque que $H^0_{(p)}(M/_{v_nM+v'_mM}) = M/_{v_nM+v'_mM}(p)$ on obtient $H^2_{(m)}(X) \simeq \varinjlim_{(n,m)} M_{(n,m)}(p)$. Le résultat s'en déduit en appliquant le théorème de dualité locale (§1).

LEMME 2.4: *Soit M un Λ-module de type fini et de torsion sans sous-Λ-module pseudonul non nul tel que, pour $n \geqslant n_0$ et $m \geqslant m_0$ $M/_{v_nM+v'_mM}$ soit fini. On a un isomorphisme*:

$$a_\Lambda(M) \tilde{\to} \mathrm{Hom}_{\mathbb{Z}_p}\left(\varinjlim_{(n,m)} M_{(n,m)}, \mathbb{Q}_p/\mathbb{Z}_p\right).$$

DÉMONSTRATION: D'après le Lemme 2.2, $H^2_m(M) = \varinjlim_n H^1_{m_2}(M/_{v_nM})$, puisque $M/_{v_nM+v'_mM}$ est fini, nous savons que v'_m est premier à la série caractéristique du Λ_2-module M/v_nM, le résultat d'Iwasawa rappelé au début de ce paragraphe nous donne

$$H^1_{m_2}\left(M/_{v_nM}\right) = \varinjlim_m M/_{v_nM+v'_mM}.$$

Le théorème de dualité locale achève la démonstration.

THÉORÈME 2.5: *Soit M un Λ-module de type fini et de torsion tel que pour $n \geqslant n_0$ et $m \geqslant m_0$ $M/v_nM + v'_mM$ soit fini, alors*:

$$a_\Lambda(M) \tilde{\to} \mathrm{Hom}_{\mathbb{Z}_p}\left(\varinjlim_{(n,m)} M_{(n,m)}, \mathbb{Q}_p/\mathbb{Z}_p\right).$$

DÉMONSTRATION: Soit M^0 le sous-module pseudo-nul maximal de M et M_0 le module défini par l'exactitude de la suite:

$$0 \to M^0 \to M \to M_0 \to 0$$

D'après le Lemme 2.1, $\varinjlim_{(n,m)} M/_{v_n M + v'_m M} = \varinjlim_{(n,m)} M_0/_{v_n M_0 + v'_m M_0}$, il nous faut donc, compte-tenu du Lemme 2.4, montrer que $a_\Lambda(M) \simeq a_\Lambda(M_0)$.

Les modules $\mathrm{Hom}_\Lambda(M^0, \Lambda)$ et $\mathrm{Ext}^1_\Lambda(M^0, \Lambda)$ sont nuls, c'est évident pour le premier car M^0 est de torsion, pour le second c'est une conséquence de [6] Chapitre 1, Proposition 8 puisque M^0 est pseudo-nul. L'isomorphisme cherché s'obtient alors en utilisant la suite exacte des Ext.

REMARQUE: Cette méthode de calcul de l'adjoint permet de généraliser certains résultats d'Iwasawa sur la structure du groupe de Galois de la p-extension abélienne maximale non ramifiée hors de p d'une $\mathbb{Z}_p$-extension d'un corps de nombres au cas d'une $(\mathbb{Z}_p)^2$-extension ([1]).

§3. Torsion de groupe du Selmer

Dans tout ce paragraphe E est une courbe elliptique définie sur un corps de nombres F, à multiplication complexe par l'anneau des entiers $\mathcal{O}$ d'un corps quadratique imaginaire K, p est un nombre premier $\neq 2$.

On suppose: (1) $K \subset F$ (2) p est inerte dans K
(3) E a bonne réduction en p (4) $E_p \subset E(F)$.

Remarquons que, sous les conditions 3) et 4) la courbe E a bonne réduction en toute place de F.

Notations:

- $F_\infty = F(E_{p^\infty})$, c'est une $\mathbb{Z}_p^2$-extension de F dans laquelle toutes les places de F divisant p sont presque totalement ramifiées.
- $\Theta = \mathrm{Gal}(F_\infty/F) = \langle \gamma, \gamma' \rangle$, $\Lambda = \Lambda_\Theta \simeq \mathbb{Z}_p[[T, T']]$
  $\Lambda' = \Lambda_{\mathbb{Z}_p} \otimes \mathcal{O}_p = \mathcal{O}_p[[T, T']]$.
- $F_n = F(E_{p^n})$
- M_∞ est la p-extension abélienne maximale de F_∞ non ramifiée hors de p, $X = \mathrm{Gal}(M_\infty/_{F_\infty})$ est de façon canonique un Λ-module dont le sous-module de torsion sera noté Z.
  Pour $0 \leqslant n \leqslant \infty$ et $1 \leqslant r \leqslant \infty$
- $H^i_p(F_n, E_{p^r}) = H^i(P_\infty/F_n, E_{p^r})$ où P_∞ est l'extension galoisienne de F non ramifiée en dehors de p maximale.
- $S'^{(p^r)}(F_n) = H^1_p(F_n, E_{p^r})$, $S'(F_n) = S'^{(p^\infty)}(F_n)$.
- $S^{(p^r)}(F_n) = \mathrm{Ker}(H^1_p(F_n, E_{p^r}) \to \bigoplus_{v \mid p} H^1(F_{n,v}, E))$, $S(F_n) = S^{(p^\infty)}(F_n)$.
- $\Sigma^{(p^r)}(F_n) = \mathrm{Ker}(S^{(p^r)}(F_n) \to \bigoplus_{v \mid p} H^1(F_{n,v}, E_{p^r}))$, $\Sigma(F_n) = \Sigma^{(p^\infty)}(F_n)$.

On peut considérer S, S' et Σ comme les trois variantes possibles du groupe de Selmer dans la théorie de la descente.

LEMME 3.1. (voir aussi [7]): *Pour toute place v de F_∞ divisant p, $H^1(F_{\infty,v}, E)(p)=0$*

DÉMONSTRATION:

$$H^1(F_{\infty,v}, E) = \varinjlim_{n} H^1(F_{n,v}, E).$$

Par la dualité de Tate ([8]): $H^1(F_{n,v}, E) \tilde{\to} E(F_{n,v})^*$ et par conséquent $H^1(F_{\infty,v}, E) \tilde{\to} (\varprojlim E(F_{n,v}))^*$, la limite projective étant prise sur les normes. Le corps résiduel de $F_{\infty,v}$ est fini et donc, en négligeant éventuellement un groupe fini d'ordre premier à p, $\varprojlim E(F_{n,v}) \simeq \varprojlim E_{1,v}(F_{n,v})$ où $E_{1,v}$ est le groupe formel de la courbe en v. D'après [5], le groupe formel $E_{1,v}$ étant de hauteur 2, il n'y a pas de normes universelles non nulles relatives à une $\mathbb{Z}_p$-extension dans $E_{1,v}(F_{n,v})$, par suite $\varprojlim E_{1,v}(F_{n,v})=0$.

COROLLAIRE 3.2:

$$S'(F_\infty) = S(F_\infty) = \mathrm{Hom}(X, E_{p^\infty}).$$

La deuxième égalité est conséquence de l'isomorphisme entre

$$\mathrm{Hom}\left(\mathrm{Gal}\left(P_\infty/_{F_\infty}\right), E_{p^\infty}\right) \quad \textit{et} \quad \mathrm{Hom}(X, E_{p\infty}).$$

REMARQUE 3.3: Si N_∞ est une $\mathbb{Z}_p$-extension de F contenue dans F_∞, le même argument donne $S'(N_\infty)=S(N_\infty)$.

Dans la suite, si M et N sont deux Θ-modules, on munit $\mathrm{Hom}(M, N)$ de la structure de Θ-module définie par:

$$(\alpha f)(m) = \alpha \cdot f(\alpha^{-1} m), \quad \alpha \in \Theta \quad \text{et } f \in \mathrm{Hom}(M, N).$$

Le dual de Pontryagin $\widehat{S(F_\infty)} = \mathrm{Hom}_{\mathbb{Z}_p}(S(F_\infty), \mathbb{Q}_p/_{\mathbb{Z}_p})$ de $S(F_\infty)$ sera muni de la structure précédente.

REMARQUE 3.4: Si M est un Λ-module de type fini, pour $0 \leqslant i \leqslant 3$ $\mathrm{Hom}_{\mathbb{Z}_p}(H^i_m(M), \mathbb{Q}_p/_{\mathbb{Z}_p})$ est, avec la convention précédente, un Θ-module compact. Le Λ-module qui lui est associé est isomorphe à $\mathrm{Ext}^{3-i}_\Lambda(M, \Lambda)^\cdot$ où, pour tout Λ-module T, on note $T^\cdot$ le Λ-module

obtenu par restriction des scalaires selon $\phi : \Lambda \xrightarrow{\sim} \Lambda$ définie par $\phi(T) = \dfrac{1}{1+T} - 1$, $\phi(T') = \dfrac{1}{1+T'} - 1$ (i.e.: $\phi(\gamma) = \gamma^{-1}$, $\phi(\gamma') = \gamma'^{-1}$).

LEMME 3.5:
(1) *Si T_p est le module de Tate de E_{p^∞}, $\widehat{S(F_\infty)} \simeq \mathrm{Hom}_{\mathbf{Z}_p}(T_p, X)$*
(2) $\widehat{S(F_\infty)} \underset{\Lambda}{\otimes} \Lambda' \simeq \mathrm{Hom}_{\mathcal{O}_p}(T_p \underset{\mathbf{Z}_p}{\otimes} \mathcal{O}_p, X \underset{\Lambda}{\otimes} \Lambda')$.

DÉMONSTRATION:

$$(1)\quad S(F_\infty) = \mathrm{Hom}_{\mathbf{Z}_p}\left(\mathrm{Hom}_{\mathbf{Z}_p}(X, E_{p^\infty}), \mathbb{Q}_p/\mathbf{Z}_p\right)$$

$$\simeq \mathrm{Hom}_{\mathbf{Z}_p}\left(\mathrm{Hom}_{\mathbf{Z}_p}(X, \mathbb{Q}_p/\mathbf{Z}_p) \otimes T_p, \mathbb{Q}_p/\mathbf{Z}_p\right)$$

$$\simeq \mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, \mathrm{Hom}_{\mathbf{Z}_p}\left(\mathrm{Hom}_{\mathbf{Z}_p}(X, \mathbb{Q}_p/\mathbf{Z}_p), \mathbb{Q}_p/\mathbf{Z}_p\right)\right)$$

$$\simeq \mathrm{Hom}_{\mathbf{Z}_p}(T_p, X).$$

$$(2)\quad \widehat{S(F_\infty)} \underset{\Lambda}{\otimes} \Lambda' \simeq \mathrm{Hom}_{\mathbf{Z}_p}(T_p, X) \underset{\Lambda}{\otimes} \Lambda' \simeq \mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, X \underset{\Lambda}{\otimes} \Lambda'\right)$$

puisque $\Lambda' = \Lambda \underset{\mathbf{Z}_p}{\otimes} \mathcal{O}_p$, enfin

$$\mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, X \underset{\Lambda}{\otimes} \Lambda'\right) \simeq \mathrm{Hom}_{\mathcal{O}_p}\left(T_p \underset{\mathbf{Z}_p}{\otimes} \mathcal{O}_p, X \underset{\Lambda}{\otimes} \Lambda'\right).$$

Le $\mathbb{Z}_p$-module T_p est muni d'une structure naturelle de $\mathcal{O}_p$-module (libre de rang 1), si c désigne l'unique automorphisme non trivial de K_p sur $\mathbb{Q}_p$, on a un isomorphisme de $\mathcal{O}_p$-module: $T_p \underset{\mathbf{Z}_p}{\otimes} \mathcal{O}_p \xrightarrow{\sim} T_p \oplus \overline{T_p}$ où $\overline{T_p}$ est le $\mathcal{O}_p$-module obtenu à partir de T_p par l'extension des scalaires $\mathcal{O}_p \xrightarrow{c} \mathcal{O}_p$.

Résumons la discussion précédente:

LEMME 3.6:
(1) $\widehat{S(F_\infty)} \underset{\Lambda}{\otimes} \Lambda' \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_p}(T_p, X \underset{\Lambda}{\otimes} \Lambda') \oplus \mathrm{Hom}_{\mathcal{O}_p}(\overline{T_p}, X \underset{\Lambda}{\otimes} \Lambda')$.
(2) *Si $\epsilon : \Theta \to 1 + p\,\mathcal{O}_p$ est le caractère donnant l'action de Θ sur T_p, le groupe Θ agit sur $\overline{T_p}$ par le caractère $\bar{\epsilon} = c \circ \epsilon$.*

PROPOSITION 3.7: *Le sous Λ-module de Λ-torsion de $\widehat{S(F_\infty)}$ est égal à* $\mathrm{Hom}_{\mathbf{Z}_p}(T_p, Z)$.

DÉMONSTRATION: Puisque Λ' est libre de rang 2 sur Λ, il suffit de vérifier l'égalité après extension des scalaires à Λ', compte-tenu du Lemme précédent on est amené à montrer que le sous-Λ'-module de torsion de $\mathrm{Hom}_{\mathcal{O}_p}(T_p,\ X \underset{\Lambda}{\otimes} \Lambda')$ (resp. $\mathrm{Hom}_{\mathcal{O}_p}(\overline{T_p},\ X \underset{\Lambda}{\otimes} \Lambda')$) est $\mathrm{Hom}_{\mathcal{O}_p}(T_p,\ Z \underset{\Lambda}{\otimes} \Lambda')$ (resp. $\mathrm{Hom}_{\mathcal{O}_p}(\overline{T_p},\ Z \underset{\Lambda}{\otimes} \Lambda')$).

Soit $\phi = \Lambda' \xrightarrow{\sim} \Lambda'$ l'isomorphisme défini par:

$$\phi(\gamma) = \epsilon(\gamma)^{-1}\gamma, \quad \phi(\gamma') = \epsilon(\gamma')^{-1}\gamma'.$$

Le Λ'-module $\mathrm{Hom}_{\mathcal{O}_p}(T_p,\ X \underset{\Lambda}{\otimes} \Lambda')$ est isomorphe au Λ'-module déduit de $X \underset{\Lambda}{\otimes} \Lambda'$ par restriction des scalaires selon ϕ soit $(X \underset{\Lambda}{\otimes} \Lambda')_\phi$. Puisque $Z \underset{\Lambda}{\otimes} \Lambda'$ est la torsion de $X \underset{\Lambda}{\otimes} \Lambda'$, $(Z \underset{\Lambda}{\otimes} \Lambda')_\phi$ est celle de $(X \underset{\Lambda}{\otimes} \Lambda')_\phi$ car ϕ est un isomorphisme, on en déduit le résultat pour $\mathrm{Hom}_{\mathcal{O}_p}(T_p,\ X \underset{\Lambda}{\otimes} \Lambda')$. Le même raisonnement s'applique au module $\mathrm{Hom}_{\mathcal{O}_p}(\overline{T_p},\ X \underset{\Lambda}{\otimes} \Lambda')$, l'application ψ définie par $\psi(\gamma) = \bar{\epsilon}(\gamma)^{-1}\gamma$, $\psi(\gamma') = \bar{\epsilon}(\gamma')^{-1}\gamma'$ remplaçant l'application ϕ.

PROPOSITION 3.8: *Le Λ-module $\widehat{\Sigma(F_\infty)}$ est de torsion.*

DÉMONSTRATION: Les conditions définissant $\Sigma(F_\infty)$ dans $S(F_\infty) = \mathrm{Hom}(X,\ E_{p^\infty})$ permettent d'identifier ce dernier à $\mathrm{Hom}(X',\ E_{p^\infty})$ où X' est le groupe de Galois de la p-extension abélienne maximale non ramifiée de F_∞ totalement décomposée en p. Par un raisonnement analogue à celui utilisé dans la démonstration du Lemme 3.5, on montre que $\widehat{\Sigma(F_\infty)} \simeq \mathrm{Hom}_{\mathbb{Z}_p}(T_p,\ X')$ il suffit alors de noter que le Λ-module X' est de torsion pour conclure comme dans la Proposition précédente.

Le reste de ce paragraphe est consacré à la comparaison des séries caractéristiques de $\widehat{\Sigma(F_\infty)}$ (qui est un quotient de $S(F_\infty)$) et du sous-module de torsion de $S(F_\infty)$ ainsi qu'au problème analogue lorsque l'on remplace F_∞ par une $\mathbb{Z}_p$-extension L_∞ de F contenue dans F_∞. Nous n'obtiendrons cependant nos résultats qu'en supposant vérifier la condition suivante:

L'hypothèse de Léopoldt est satisfaite pour tous les corps intermédiaires de la $\mathbb{Z}_p^2$-extension F_∞

LEMME 3.9: (voir aussi [6], IV Proposition 11):

Soient $J_n = J(F_n)$ *les idèles de* F_n,
$V_n = \{(x_v) \in J_n,\ x_v = 1$ *si* $v \mid p$ *et* x_v *unité* $\forall v\}$
$C_n = J_n / F_n^* V_n$.

Il existe une suite exacte:

$$0 \to E_{p^n} \to \bigoplus_{v \mid p} E_{p^n}(F_{n,v}) \to \mathrm{Hom}(E_{p^n}, C_n)$$

$$\to H_p^1(F_n, E_{p^n}) \to \bigoplus_{v \mid p} H^1(F_{n,v}, E_{p^n}).$$

DÉMONSTRATION: Pour toute extension finie L de F_n contenue dans P_∞ on note $J(L)$ les idèles de L, $J_p(L) = \{(x_v) \in J(L);\ x_v = 1 \text{ si } v \nmid p\}$, $V_p(L) = \{(x_v) \in J(L);\ x_v = 1 \text{ si } v \mid p \text{ et } x_v \text{ unité } \forall v\}$, $U_p(L)$ les p-unités de L; J_∞ ($J_{p,\infty}$, $V_{p,\infty}$, $U_{p,\infty}$) la réunion, pour $L \subset P_\infty$, des $J(L)$ ($J_p(L)$, $V_p(L)$, $U_p(L)$).

On montre tout d'abord l'exactitude de la suite:

$$0 \to U_{p,\infty} \to J_{p,\infty} \to J_\infty / P_\infty^* V_{p,\infty} \to 0.$$

Le seul point délicat est la surjectivité, pour le montrer on constate que tout idèle (x_v) de $J(L)$ est, quitte à passer au corps de Hilbert $H(L)$ de L, équivalent modulo $H(L)^*$ à un idèle (y_v) de $J(H(L))$ où y_v est une unité pour tout v; modifiant (y_v) par un élément de $V_p(H(L))$ on obtient un idèle de $J_p(H(L))$. Le groupe $U_{p,\infty}$ étant divisible par p, la suite

$$(1) \quad 0 \to \mathrm{Hom}(E_{p^n}, U_{p,\infty}) \to \mathrm{Hom}(E_{p^n}, J_{p,\infty})$$

$$\to \mathrm{Hom}(E_{p^n}, J_\infty / P_\infty^* V_{p,\infty}) \to 0$$

est exacte. Si $G = \mathrm{Gal}(P_\infty / F_n)$ on obtient par passage à la cohomologie:

$$0 \to \mathrm{Hom}(E_{p^n}, U_p(F_n)) \to \mathrm{Hom}(E_{p^n}, J_p(F_n))$$

$$\to \mathrm{Hom}\left(E_{p^n}, \left(J_\infty / P_\infty^* V_{p,\infty}\right)^G\right) \to H^1(G, \mathrm{Hom}(E_{p^n}, U_{p,\infty}))$$

$$\to H^1(G, \mathrm{Hom}(E_{p^n}, J_{p,\infty})).$$

La théorie du corps de classe et la cohomologie de la suite exacte:

$$0 \to V_{p,\infty} \to J_\infty / P_\infty^* \to J_\infty / P_\infty^* V_{p,\infty} \to 0$$

nous donnent un isomorphisme: $C_n \xrightarrow{\sim} (J_\infty / P_\infty^* V_{p,\infty})^G (H^1(G, V_{p,\infty}) = 0$ car l'extension P_∞ / F_n est non ramifiée hors de p). En utilisant l'identifica-

tion de E_{p^n} avec son dual par l'accouplement de Weil et nos notations, la suite (1) s'écrit:

$$0 \to E_{p^n} \to \bigoplus_{v \mid p} E_{p^n}(F_{n,v}) \to \mathrm{Hom}(E_{p^n}, C_n)$$

$$\to H^1_p(F_n, E_{p^n}) \to \bigoplus_{v \mid p} H^1(F_{n,v}, E_{p^n}).$$

COROLLAIRE 3.10: *La suite*:

$$(2) \quad 0 \to E_{p^n} \to \bigoplus_{v \mid p} E_{p^n}(F_{n,v}) \to \mathrm{Hom}(E_{p^n}, C_n) \to \Sigma^{(p^n)}(F_n) \to 0$$

est exacte.

Nous faisons le choix des générateurs topologiques γ et γ' de Θ de telle façon que, pour n assez grand, le groupe $\mathrm{Gal}(F_\infty/F_n)$ soit engendré par $\gamma^{p^{n-r}}$, $\gamma'^{p^{n-s}}$ où r et s sont des entiers indépendants de n. Si $\omega_n = \gamma^{p^n} - 1$, $\omega'_m = \gamma'^{p^m} - 1$, nous noterons $X_{n,m}$ le Λ-module $X/_{\omega_n X + \omega'_m X}$.

L'hypothèse de Léopoldt sur F_n nous assure l'égalité entre la p-torsion de $C_n = J_n/_{F_n^* V_n}$ et celle de $J_n/_{\overline{F_n^* V_n}}$, la p-torsion de ce dernier groupe s'identifie par la loi de réciprocité d'Artin à celle de $\mathrm{Gal}(M(F_n)/F_n)$, où $M(F_n)$ est la p-extension abélienne maximale de F_n non ramifiée en dehors de p. Le groupe de Galois de F_∞ sur F_n est libre sur $\mathbb{Z}_p$, la p-torsion de $\mathrm{Gal}(M(F_n)/F_n)$ est donc celle de $G_n = \mathrm{Gal}(M(F_n)/F_\infty)$. L'application d'Artin induit par conséquent un isomorphisme:

$$\mathrm{Hom}(E_{p^n}, C_n) \simeq \mathrm{Hom}(E_{p^n}, G_n(p)).$$

Nous cherchons à passer à la limite inductive sur n dans la suite exacte (2), les applications de transition étant induites par la restriction sur la cohomologie et les inclusions $E_{p^n} \hookrightarrow E_{p^{n+1}}$.

LEMME 3.11: *Il existe une suite exacte de Λ-modules*:

$$0 \to E_{p^\infty} \to \bigoplus_{v \mid p} E_{p^\infty}(F_{\infty,v}) \to \mathrm{Hom}_{\mathbb{Z}_p}\Big(T_p, \varinjlim_n G_n(p)\Big)$$

$$\to \Sigma(F_\infty) \to 0.$$

DÉMONSTRATION: On obtient le résultat en passant à la limite sur n dans la suite exacte (2), compte tenu des identités:

$$\lim_{\overrightarrow{n}} \Sigma^{(p^n)}(F_n) = \Sigma(F_\infty).$$

$$\lim_{\overrightarrow{n}} \Big(\bigoplus_{v \mid p} E_{p^n}(F_{n,v}) \Big) = \bigoplus_{v \mid p} E_{p^\infty}(F_{\infty,v}).$$

$$\lim_{\overrightarrow{n}} \operatorname{Hom}\big(E_{p^n}, C_n\big) = \lim_{\overrightarrow{n}} \operatorname{Hom}\big(E_{p^n}, G_n(p)\big)$$

$$= \operatorname{Hom}_{\mathbf{Z}_p}\Big(T_p, \lim_{\overrightarrow{n}} G_n(p)\Big).$$

Il nous reste à préciser les applications $j_{n,n+1} : G_n(p) \to G_{n+1}(p)$ définissant la limite inductive des $G_n(p)$. L'image par l'application de transition de $f \in \operatorname{Hom}(E_{p^n}, C_n)$ dans $\operatorname{Hom}(E_{p^{n+1}}, C_{n+1})$ est l'application $\tilde{f}$ définie par le diagramme commutatif suivant

$$\begin{array}{ccccc} E_{p^{n+1}} & \xrightarrow{\tilde{f}} & C_{n+1}(p) & \overset{\text{Artin}}{\underset{\sim}{\to}} & G_{n+1}(p) \\ \downarrow \times p & & \uparrow i_{n,n+1} & & \uparrow j_{n,n+1} \\ E_{p^n} & \xrightarrow{f} & C_n(p) & \overset{\text{Artin}}{\underset{\sim}{\to}} & G_n(p) \end{array}$$

où $i_{n,n+1}$ est induite par l'inclusion de J_n dans J_{n+1}.

REMARQUE: Dans la suite (2) E_{p^n} a été identifié à son dual, ce qui a pour effet de transformer $E_{p^n} \hookrightarrow E_{p^{n+1}}$ en $E_{p^{n+1}} \xrightarrow{\times p} E_{p^n}$.

LEMME 3.12: *Les groupes G_n et G_{n+1} étant munis de leur structure naturelle de Λ-module, si $\bar{\sigma} \in G_n(p)$ est la restriction de $\sigma \in G_{n+1}$ à $M(F_n)$:*

$$j_{n,n+1}(\bar{\sigma}) = \frac{\omega_{n+1-r}}{\omega_{n-r}} \cdot \frac{\omega'_{n+1-s}}{\omega'_{n-s}} \cdot \sigma.$$

DÉMONSTRATION: Le sous-groupe de Θ engendré topologiquement par γ^{p^n} et γ'^{p^m} sera noté $\Theta_{n,m}$. La théorie du corps de classe nous assure la

commutativité du diagramme suivant:

$$\begin{array}{ccc} C_n & \overset{\text{Artin}}{\to} & \mathrm{Gal}(M(F_{n+1})/F_n)^{ab} = \mathrm{Gal}(M(F_n)/_{F_n}) \\ {\scriptstyle i_{n,n+1}}\downarrow & & \mathrm{Ver}\downarrow \\ C_{n+1} & \overset{\text{Artin}}{\to} & \mathrm{Gal}(M(F_{n+1})/F_{n+1})^{ab} = \mathrm{Gal}(M(F_{n+1})/_{F_{n+1}}) \end{array}$$

où Ver est l'application de transfert.

Calculons $\mathrm{Ver}(\bar{\sigma})$ lorsque $\bar{\sigma} \in \mathrm{Gal}(M(F_n)/_{F_n})$ est la classe de $\sigma \in \mathrm{Gal}(M(F_{n+1}/_{F_n})$.

$$\mathrm{Gal}(F_{n+1}/_{F_n}) = \Theta_{n+1-r,n+1-s}/_{\Theta_{n-r,n-s}}$$

$$= \{\alpha^a\beta^b;\ 0 \leqslant a,\ b \leqslant p-1\}$$

où α est la restriction de $\gamma^{p^{n-r}}$ à F_{n+1} et β celle $\gamma'^{p^{n-s}}$. Choisissons des relèvements $\tilde{\alpha}$, $\tilde{\beta}$ de α, β dans $\mathrm{Gal}(M(F_{n+1}/_{F_n})$ et définissons $\delta_{a,b} \in \mathrm{Gal}(M(F_{n+1})/F_{n+1})$ par l'égalité $\tilde{\alpha}^a\tilde{\beta}^b\sigma = \delta_{a,b}\tilde{\mu}_{a,b}$ avec $\mu_{a,b} \in \mathrm{Gal}(F_{n+1}/F_n)$. Par définition du transfert, $\mathrm{Ver}(\bar{\sigma}) = \prod_{a,b}\delta_{a,b}$. Si maintenant $\bar{\sigma} \in \mathrm{Gal}(M(F_n)/_{F_n})(p) = G_n(p)$, $\sigma \in G_{n+1}$ et fixe F_∞ par conséquent $\mu_{a,b} = \alpha^a\beta^b$, $\delta_{a,b} = (\tilde{\alpha}^a\tilde{\beta}^b)\sigma(\tilde{\alpha}^a\tilde{\beta}^b)^{-1}$ et $\mathrm{Ver}(\bar{\sigma}) = \prod_{a,b}(\tilde{\alpha}^a\tilde{\beta}^b)\sigma(\tilde{\alpha}^a\tilde{\beta}^b)^{-1}$. Compte-tenu de la structure de Θ-module de G_{n+1} la dernière identité s'écrit:

$$\mathrm{Ver}(\bar{\sigma}) = \left(1 + \gamma^{p^{n-r}} + \ldots + \gamma^{p^{n-r}(p-1)}\right)$$

$$\times\left(1 + \gamma'^{p^{n-s}} + \ldots + \gamma'^{p^{n-s}(p-1)}\right)\sigma$$

$$= \frac{\omega_{n+1-r}}{\omega_{n-r}} \cdot \frac{\omega'_{n+1-s}}{\omega'_{n-s}} \cdot \sigma$$

PROPOSITION 3.13:

(1) *ω_n n'est pas diviseur de zéro dans X et ω'_m n'est pas diviseur de zéro dans $X/\omega_n X$.*

(2) *Soit $\tilde{\gamma}$ (resp. $\tilde{\gamma}'$) un élément de $Gal(M_\infty/F)$ dont la restriction à F_∞ est égale à γ (resp. γ'). Si $\alpha_{n,m} \in X$ est le commutateur de $\tilde{\gamma}^{p^n}$ et $\tilde{\gamma}'^{p^m}$, il existe une suite exacte*:

$$0 \to \mathbb{Z}_p \overset{\mu_n}{\to} X_{n-r,n-s} \to G_n \to 0$$

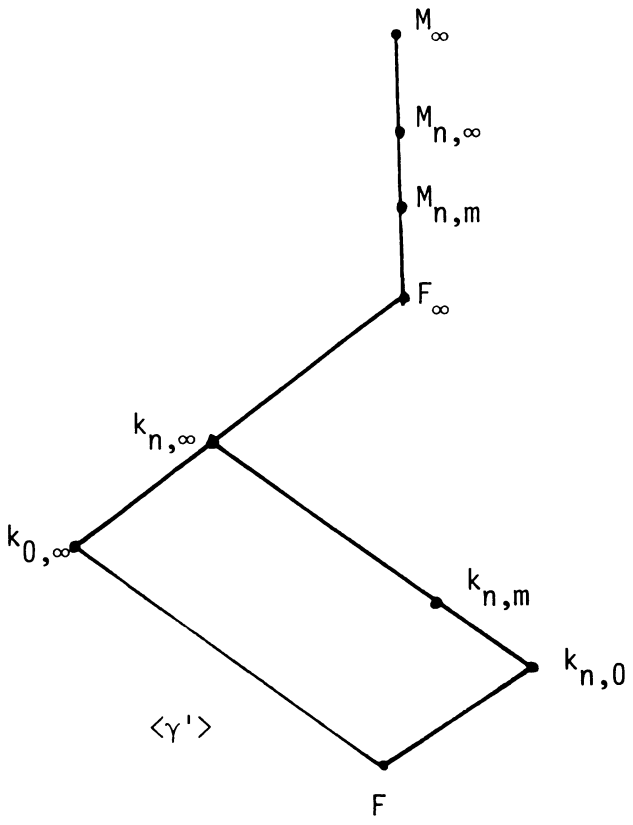

Figure 1

où l'image de μ_n *est engendré par la classe de* $\alpha_{n-r,n-s}$ *dans* $X_{n-r,n-s} = X/\omega_{n-r}X + \omega'_{n-s}X$.

DÉMONSTRATION:
1°/ a) ω_n n'est pas diviseur de zéro dans X.
Notons $k_{n,\infty}$ le sous-corps de F_∞ fixé par le groupe $\Theta_{n,\infty} = \langle \gamma^{p^n} \rangle$ et $k_{n,0}$ celui fixé par $\Theta_{n,0} = \langle \gamma^{p^n}, \gamma' \rangle$, $k_{n,0}$ est une extension finie de F de degré p^n et $k_{n,\infty}$ est une $\mathbb{Z}_p$-extension de $k_{n,0}$. Si $M_{n,\infty}$ est la p-extension abélienne maximale de $k_{n,\infty}$ non ramifiée hors de p et $Y_{n,\infty} = \mathrm{Gal}(M_{n,\infty}/k_{n,\infty})$ la suite:

$$(3) \quad 0 \to X/\omega_n X \to Y_{n,\infty} \to \mathrm{Gal}(F_\infty/k_{n,\infty}) \to 0$$

est exacte. Le rang sur Λ_2 de $Y_{n,\infty}$ est égal, sous l'hypothèse de Léopoldt sur $k_{n,0}$ à $r_2 p^n$ avec $r_2 = \frac{1}{2}[F:\mathbb{Q}]$ ([3] Proposition 2); il en est de même du rang sur Λ_2 de $X/\omega_n X$ puisque $\mathrm{Gal}(F_\infty/k_{n,\infty}) \simeq \mathbb{Z}_p$. Si Z est le

sous-module de Λ-torsion de X et X_0 le quotient de X par Z, la suite:

$$0 \to Z/\omega_n Z \to X/\omega_n X \to X_0/\omega_n X_0 \to 0$$

est exacte. Le Λ-module X étant de rang r_2 ([3] Proposition 2), on peut plonger X_0 dans un Λ-module libre de rang r_2 avec un quotient de torsion et de série caractéristique première à ω_n, on obtient alors par réduction:

$$\operatorname{rang}_{\Lambda_2}(X_0/\omega_n X_0) = \operatorname{rang}_{\Lambda_2}(\Lambda^{r_2}/\omega_n \Lambda^{r_2}) = r_2 p^n.$$

De l'égalité entre $\operatorname{rang}_{\Lambda_2}(X/\omega_n X)$ et $\operatorname{rang}_{\Lambda_2}(X_0/\omega_n X_0)$ on déduit $\operatorname{rang}_{\Lambda_2}(Z/\omega_n Z) = 0$, c'est-à-dire ω_n premier à la série caractéristique de Z; X étant sans sous-module pseudo-nul non nul ([3] Proposition 5) ω_n n'est pas diviseur de zéro dans X.
1°/ b) ω'_m n'est pas diviseur de zéro dans $X/\omega_n X$.
Il suffit de montrer que ω'_m n'est pas diviseur de zéro dans $Y_{n,\infty}$. Si $k_{n,m}$ est le corps fixé par $\Theta_{n,m}$ et $M_{n,m}$ la p-extension abélienne maximale de $k_{n,m}$ non ramifiée hors de p, on a une suite exacte:

$$0 \to Y_{n,\infty}/\omega'_m Y_{n,\infty} \to \operatorname{Gal}(M_{n,m}/k_{n,m}) \to \operatorname{Gal}(k_{n,\infty}/k_{n,m}) \to 0.$$

Puisque $\operatorname{Gal}(k_{n,\infty}/k_{n,m}) \simeq \mathbb{Z}_p$ on obtient $\operatorname{rang}_{\mathbf{Z}_p}(Y_{n,\infty}/\omega'_m Y_{n,\infty}) = \operatorname{rang}_{\mathbf{Z}_p}(\operatorname{Gal}(M_{n,m}/k_{n,m})) - 1$, l'hypothèse de Léopoldt sur $k_{n,m}$ nous donne alors $\operatorname{rang}_{\mathbf{Z}_p}(Y_{n,\infty}/\omega'_m Y_{n,\infty}) = r_2 p^n p^m$. Sachant que $\operatorname{rang}_{\Lambda_2}(Y_{n,\infty}) = r_2 p^n$ et que $Y_{n,\infty}$ est sans sous-module pseudo-nul non nul on termine comme précédemment.
2°/ Notons que $F_n = k_{n-r,n-s}$ et réécrivons la suite (3):

$$0 \to X/\omega_{n-r} X \to Y_{n-r,\infty} \to \mathbb{Z}_p \to 0.$$

En tensorisant par $\Lambda_2/\omega'_{n-s}\Lambda_2$ après avoir noté que ω'_{n-s} n'est pas diviseur de zéro dans $Y_{n-r,\infty}$, on obtient la suite exacte:

$$0 \to \mathbb{Z}_p \to X_{n-r,n-s} \to \operatorname{Gal}(M_n/k_{n-r,\infty}) \to \mathbb{Z}_p \to 0.$$

Le groupe G_n s'identifie au noyau de l'application de $\operatorname{Gal}(M_n/k_{n-r,\infty})$ dans $\mathbb{Z}_p$ ($\simeq \operatorname{Gal}(F_\infty(k_{n-r,\infty}))$ et l'assertion 2°/ en résulte.

LEMME 3.14: *Pour tout $n \geqslant 0$ il existe une suite exacte*:

$$0 \to X_{n-r,n-s}(p) \to G_n(p) \xrightarrow{\delta_n} \mathbb{Q}_p/\mathbb{Z}_p$$

et le diagramme suivant est commutatif

$$\begin{array}{ccccc} 0 \to & X_{n-r,n-s}(p) & \to G_n(p) \to & \mathbb{Q}_p/\mathbb{Z}_p \\ & \downarrow \tilde{j_{n,n+1}} & \downarrow j_{n,n+1} & \| \\ 0 \to & X_{n+1-r,n+1-s}(p) & \to G_{n+1}(p) \to & \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

où $\tilde{j_{n,n+1}} : X/\omega_{n-r}X + \omega'_{n-s}X \to X/\omega_{n+1-r}X + \omega'_{n+1-s}X$ *est déduit de la multiplication par* $\dfrac{\omega_{n+1-r}}{\omega_{n-r}} \cdot \dfrac{\omega'_{n+1-s}}{\omega'_{n-s}}$ *dans X par passage au quotient.*

DÉMONSTRATION: D'après la Proposition 3.13 la suite:

$$0 \to \mathbb{Z}_p \xrightarrow{\mu_n} X_{n-r,n-s} \to G_n \to 0$$

est exacte, en appliquant le foncteur $\mathrm{Hom}_{\mathbf{Z}_p}(\mathbb{Z}/p^t\mathbb{Z}, \cdot)$ on obtient l'exactitude de la suite:

$$0 \to X_{n-r,n-s}(p^t) \to G_n(p^t) \to \mathrm{Ext}^1_{\mathbf{Z}_p}(\mathbb{Z}/_{p^t\mathbf{Z}}, \mathbb{Z}_p) \simeq \mathbb{Z}/_{p^t\mathbf{Z}}.$$

Il suffit de passer à la limite sur t pour obtenir la première partie du lemme. La seconde partie du lemme est alors conséquence de la commutativité du diagramme suivant:

$$\begin{array}{ccccccc} 0 \to & \mathbb{Z}_p & \to & X_{n-r,n-s} & \to & G_n & \to 0 \\ & \| & & \downarrow \tilde{j_{n,n+1}} & & \downarrow j_{n,n+1} & \\ 0 \to & \mathbb{Z}_p & \to & X_{n+1-r,n+1-s} & \to & G_{n+1} & \to 0. \end{array}$$

Pour le carré de droite ceci résulte du Lemme 3.12. Pour celui de gauche il suffit de remarquer que:

$$\alpha_{n+1-r,n+1-s} = \frac{\omega_{n+1-r}}{\omega_{n-r}} \cdot \frac{\omega'_{n+1-s}}{\omega'_{n-s}} \cdot \alpha_{n-r,n-s}.$$

PROPOSITION 3.15:

(1) $\varinjlim_n X_{n-r,n-s}(p) \simeq H^2_m(X)$.

La limite inductive étant prise selon les applications $\tilde{j_{n,n+1}}$.

(2) *Il existe une suite exacte de* Λ*-modules*:

$$0 \to \mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, H^2_m(X)\right) \to \mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, \varinjlim_n G_n(p)\right)$$

$$\to \mathrm{Hom}_{\mathbf{Z}_p}(T_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

le module $\mathbb{Q}_p/\mathbb{Z}_p$ *étant muni de l'action triviale de* Θ.

DÉMONSTRATION: La première assertion est une conséquence de la Proposition 2.3 et de la première partie de la Proposition 3.13. Pour la seconde assertion il suffit d'appliquer le foncteur $\mathrm{Hom}_{\mathbf{Z}_p}(T_p, \cdot)$ à la suite exacte obtenue dans le lemme précédent puis de passer à la limite sur n.

LEMME 3.16:

$$\widehat{\mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, H_m^2(X)\right)} \simeq \mathrm{Ext}^1_\Lambda\left(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, X), \Lambda\right)^\cdot.$$

DÉMONSTRATION: Pour tout Λ-module de type fini M on a un isomorphisme fonctoriel $\mathrm{Hom}_{\mathbf{Z}_p}(T_p, H_m^0(M)) \simeq H_m^0(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, M))$, la suite spectrale des foncteurs composés nous donne alors un isomorphisme $\mathrm{Hom}_{\mathbf{Z}_p}(T_p, H_m^2(M)) \simeq H_m^2(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, M))$, en particulier $\mathrm{Hom}_{\mathbf{Z}_p}(T_p, H_m^2(X)) \simeq H_m^2(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, X))$. En utilisant le théorème de dualité locale et la Remarque 3.4 on obtient: $\widehat{\mathrm{Hom}_{\mathbf{Z}_p}(T_p, H_m^2(X))} \simeq \mathrm{Ext}^1_\Lambda(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, X), \Lambda)^\cdot$.

La proposition suivante résume les propriétés obtenues.

PROPOSITION 3.17: *Il existe des suites exactes de Λ-modules*:

$$0 \to \widehat{\Sigma(F_\infty)} \xrightarrow{\eta} \widehat{\mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, \varinjlim_n G_n(p)\right)}$$

$$\to \bigoplus_{v \mid p} \widehat{E_{p^\infty}(F_{\infty,v})} \to \widehat{E_{p^\infty}} \to 0.$$

$$T_p \to \mathrm{Hom}_{\mathbf{Z}_p}\left(T_p, \varinjlim_n G_n(p)\right)^\wedge \xrightarrow{\nu} \mathrm{Ext}^1_\Lambda\left(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, X), \Lambda\right)^\cdot \to 0.$$

Ces suites s'obtiennent en dualisant respectivement les suites exactes obtenues dans le Lemme 3.11 et la Proposition 3.15. Dans la suite on cherche à étudier les propriétés de la série caractéristique du module $\mathrm{Ext}^1_\Lambda(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, X), \Lambda)$, pour cela on considère la situation plus générale suivante: Soient M un Λ-module de type fini sans sous-modules pseudo-nuls non nuls et P son sous-module de torsion, on supposera que $(\gamma - 1)$ est premier à la série cractéristique de P et donc non diviseur de zéro dans P. Si R est un Λ-module de torsion (resp. un $\Lambda_2 = \Lambda/(\gamma - 1)\Lambda$-module de torsion) sa série caractéristique sera notée $f_\Lambda(R)$ (resp. $f_{\Lambda_2}(R)$). Nous utiliserons les deux suites exactes suivantes:

(1) $0 \to P \to M \to L \to 0$

où L est sans torsion

$$(2) \quad 0 \to L \to \Lambda^s \to N \to 0$$

où N est de torsion et de série caractéristique première à $(\gamma - 1)$ (il est facile de montrer qu'une telle suite existe). En utilisant (1) on peut écrire la suite exacte:

$$(3) \quad 0 \to \mathrm{Ext}^1_\Lambda(L, \Lambda) \to \mathrm{Ext}^1_\Lambda(M, \Lambda) \to \mathrm{Ext}^1_\Lambda(P, \Lambda) \to \mathrm{Ext}^2_\Lambda(L, \Lambda).$$

LEMME 3.18: $\mathrm{Ext}^1_\Lambda(L, \Lambda)$ *est pseudo-nul et* $\mathrm{Ext}^2_\Lambda(L, \Lambda)$ *est fini.*

DÉMONSTRATION: De la suite (2) on déduit les isomorphismes:

$$\mathrm{Ext}^1_\Lambda(L, \Lambda) \simeq \mathrm{Ext}^2_\Lambda(N, \Lambda)$$

$$\mathrm{Ext}^2_\Lambda(L, \Lambda) \simeq \mathrm{Ext}^3_\Lambda(N, \Lambda).$$

Il suffit alors de remarquer que $\mathrm{Ext}^2_\Lambda(N, \Lambda)$ est pseudo-nul et $\mathrm{Ext}^3_\Lambda(N, \Lambda)$ est à support dans l'idéal maximal donc fini.

L'exactitude de la suite

$$0 \to P/_{(\gamma-1)P} \to \left(M/_{(\gamma-1)M}\right)_{\mathrm{tors}} \to \left(L/_{(\gamma-1)L}\right)_{\mathrm{tors}} \to 0$$

(tors $= \Lambda_2$-torsion) et l'isomorphisme entre $\left(L/_{(\gamma-1)L}\right)_{\mathrm{tors}}$ et $N_{(\gamma-1)} = \{n \in N, (\gamma - 1)n = 0\}$ obtenu à partir de (2) conduisent à l'égalité:

$$(*) \quad f_{\Lambda_2}\left(\left(M/_{(\gamma-1)M}\right)_{\mathrm{tors}}\right) = f_{\Lambda_2}\left(P/_{(\gamma-1)P}\right) \cdot f_{\Lambda_2}\left(N_{(\gamma-1)}\right)$$

à un élément inversible près. Les hypothèses faites sur N montrent que $N_{(\gamma-1)} = \mathrm{N}^0_{(\gamma-1)}$ où N^0 désigne le sousmodule pseudo-nul maximal de N, on peut par conséquent remplacer $f_{\Lambda_2}(N_{(\gamma-1)})$ par $f_{\Lambda_2}(N^0_{(\gamma-1)})$ dans l'égalité précédente. Nous utiliserons les deux lemmes suivants démontrés dans [6].

LEMME 3.19 [6, Chapitre 1 Lemme 4]: *Si R est un Λ-module de torsion tel que $R/_{(\gamma-1)R}$ soit de Λ_2-torsion, on a l'égalité à un élément inversible près:*

$$f_{\Lambda_2}\left(R/_{(\gamma-1)R}\right) = \pi\left(f_\Lambda(R)\right) \cdot f_{\Lambda_2}\left(R_{(\gamma-1)}\right)$$

où π est la projection naturelle de Λ sur Λ_2.

LEMME 3.20 [6, Chapitre 1 Lemme 11]: *Si R est un Λ-module pseudo-nul alors*:

$$a_{\Lambda_2}\left(R/_{(\gamma-1)R}\right) \simeq \mathrm{Ext}^2_\Lambda(R, \Lambda)_{(\gamma-1)}.$$

Le Lemme 3.19 nous donne l'égalité des séries $f_{\Lambda_2}(N^0_{(\gamma-1)})$ et $f_{\Lambda_2}(N^0/_{(\gamma-1)N^0})$ puisque $f_\Lambda(N^0) = 1$ ainsi que celle des séries $f_{\Lambda_2}(P/_{(\gamma-1)P})$ et $\pi(f_\Lambda(P))$ puisque $P_{(\gamma-1)} = 0$. Du pseudo-isomorphisme entre $\mathrm{Ext}^1_\Lambda(M, \Lambda)$ et $\mathrm{Ext}^1_\Lambda(P, \Lambda)$ on déduit $f_\Lambda(\mathrm{Ext}^1_\Lambda(M, \Lambda)) = f_\Lambda(\mathrm{Ext}^1_\Lambda(P, \Lambda)) = f_\Lambda(P)$. L'égalité $(*)$ devient alors:

$$(**) \quad f_{\Lambda_2}\left(\left(M/_{(\gamma-1)M}\right)_{\mathrm{tors}}\right)$$

$$= \pi\left(f_\Lambda\left(\mathrm{Ext}^1_\Lambda(M, \Lambda)\right) \cdot f_{\Lambda_2}\left(N^0/_{(\gamma-1)N^0}\right)\right)$$

$$= \pi\left(f_\Lambda\left(\mathrm{Ext}^1_\Lambda(M, \Lambda)\right) \cdot f_{\Lambda_2}\left(\mathrm{Ext}^2_\Lambda(N^0, \Lambda)_{(\gamma-1)}\right)\right).$$

La dernière égalité s'obtenant du Lemme 3.20.

LEMME 3.21:

(1) *L'application* $\mathrm{Ext}^2_\Lambda(N, \Lambda) \to \mathrm{Ext}^2_\Lambda(N^0, \Lambda)$ *est surjective à noyau fini.*

(2) $\mathrm{Ext}^1_\Lambda(M, \Lambda)_{(\gamma-1)}$ *est pseudo-isomorphe sur* Λ_2 *à* $\mathrm{Ext}^2_\Lambda(N^0, \Lambda)_{(\gamma-1)}$.

DÉMONSTRATION:

(1) Il suffit de montrer que, si $N_0 = N/_{N^0}$, $\mathrm{Ext}^3_\Lambda(N_0, \Lambda) = 0$ et $\mathrm{Ext}^2_\Lambda(N_0, \Lambda)$ est fini. Ces deux résultats s'obtiennent en plongeant N_0 dans un modèle W sur Λ et en utilisant le fait que $\mathrm{Ext}^2_\Lambda(W, \Lambda) = \mathrm{Ext}^3_\Lambda(W, \Lambda) = 0$.

(2) Le Λ-module $\mathrm{Ext}^1_\Lambda(P, \Lambda)$ étant sans $(\gamma - 1)$-torsion,la suite (3) nous donne l'égalité $\mathrm{Ext}^1_\Lambda(M, \Lambda)_{(\gamma-1)} = \mathrm{Ext}^1_\Lambda(L, \Lambda)_{(\gamma-1)}$, ce dernier module est, d'après le Lemme 3.18 isomorphe à $\mathrm{Ext}^2_\Lambda(N, \Lambda)_{(\gamma-1)}$. La conclusion résulte alors de la première partie du lemme.

THÉORÈME 3.22:

$$f_{\Lambda_2}\left(\left(M/_{(\gamma-1)M}\right)_{\mathrm{tors}}\right) = f_{\Lambda_2}\left(\mathrm{Ext}^1_\Lambda(M, \Lambda)/_{(\gamma-1)\,\mathrm{Ext}^1_\Lambda(M, \Lambda)}\right).$$

DÉMONSTRATION: En utilisant le lemme précédent l'égalité $(**)$ s'écrit:

$$f_{\Lambda_2}\left(\left(M/_{(\gamma-1)M}\right)_{\mathrm{tors}}\right)$$

$$= \pi\left(f_\Lambda\left(\mathrm{Ext}^1_\Lambda(M, \Lambda)\right)\right) \cdot f_{\Lambda_2}\left(\mathrm{Ext}^1_\Lambda(M, \Lambda)_{(\gamma-1)}\right).$$

Il suffit alors d'appliquer le Lemme 3.19 pour obtenir l'identité cherchée. Précisons ces résultats lorsque $M = \mathrm{Hom}_{\mathbf{Z}_p}(T_p, X) = \widehat{S(F_\infty)}$ et $P = \mathrm{Hom}_{\mathbf{Z}_p}(T_p, Z) = (\widehat{S(F_\infty)})_{\mathrm{tors}}$.

THÉORÈME 3.23: *Les Λ-modules $\widehat{\Sigma(F_\infty)}$ et $(\widehat{S(F_\infty)})^{\cdot}_{\mathrm{tors}}$ sont pseudo-isomorphes.*

DÉMONSTRATION: La Proposition 3.17 nous donne un pseudo-isomorphisme:

$$\nu \circ \eta : \widehat{\Sigma(F_\infty)} \to \mathrm{Ext}^1_\Lambda\left(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, X), \Lambda\right)^{\cdot}.$$

Il suffit donc de noter que $\mathrm{Ext}^1_\Lambda(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, X), \Lambda)$ est pseudo-isomorphe à $\mathrm{Ext}^1_\Lambda(\mathrm{Hom}_{\mathbf{Z}_p}(T_p, Z), \Lambda) = a_\Lambda((\widehat{S(F_\infty)})_{\mathrm{tors}})$ et the remarquer que pour un Λ-module M de torsion, $a_\Lambda(M)$ est pseudo-isomorphe à M ([6], chapitre 1, §2.2).

THÉORÈME 3.24: *On suppose $(\gamma - 1)$ premier à la série caractéristique de $(\widehat{S(F_\infty)})_{\mathrm{tors}}$ et on note L_∞ la $\mathbf{Z}_p$-extension fixée par γ.*

Les deux séries $f_{\Lambda_2}(\widehat{\Sigma(L_\infty)})$ et $f^{\cdot}_{\Lambda_2}((\widehat{S(L_\infty)})_{\mathrm{tors}})$ sont égales (si $\Lambda_2 = \mathbf{Z}_p[[T]]$, $f^{\cdot}_{\Lambda_2}(T) = f_{\Lambda_2}(\frac{1}{1+T} - 1)$).

DÉMONSTRATION: Le nombre premier p étant inerte dans K, les modules $\widehat{E_{p^\infty}(F_{\infty,v})}/(\gamma - 1)\widehat{E_{p^\infty}(F_{\infty,v})}$, $T_p/(\gamma - 1)T_p$ sont finis et $(E_{p^\infty}(F_{\infty,v}))_{(\gamma-1)} = 0$, l'application $\nu \circ \eta$ obtenue dans la Proposition 3.17 donne par réduction modulo $(\gamma - 1)$ un pseudo-isomorphisme sur Λ_2 entre $\widehat{\Sigma(F_\infty)}/(\gamma - 1)\widehat{\Sigma(F_\infty)}$ et $(\mathrm{Ext}^1_\Lambda(\widehat{S(F_\infty)}, \Lambda)/(\gamma - 1)\mathrm{Ext}^1_\Lambda(\widehat{S(F_\infty)}, \Lambda))^{\cdot}$. La série caractéristique du dernier module est égale d'après le Théorème 3.22 à $f^{\cdot}_{\Lambda_2}((\widehat{S(F_\infty)}/(\gamma - 1)\widehat{S(F_\infty)})_{\mathrm{tors}})$, pour obtenir le résultat il suffit donc de montrer que:

$$\widehat{\Sigma(f_\infty)}/(\gamma - 1)\widehat{\Sigma(F_\infty)} = \widehat{\Sigma(L_\infty)} \quad \text{et}$$

$$\widehat{S(F_\infty)}/(\gamma - 1)\widehat{S(F_\infty)} = \widehat{S(L_\infty)}.$$

Pour cela considérons le diagramme suivant:

$$\begin{array}{ccccc}
0 \to (\Sigma(F_\infty))_{(\gamma-1)} & \to & (H^1_p(F_\infty, E_{p^\infty}))_{(\gamma-1)} & \to & (\bigoplus_{v \mid p} H^1(F_{\infty,v}, E_{p^\infty}))_{(\gamma-1)} \\
\uparrow & & \uparrow r_1 & & \uparrow r_2 \\
0 \to \Sigma(L_\infty) & \to & H^1_p(L_\infty, E_{p^\infty}) & \to & \bigoplus_{v \mid p} H^1(L_{\infty,v}, E_{p^\infty})
\end{array}$$

Les groupes $H^1(F_\infty/L_\infty, E_{p^\infty})$ et $H^1(F_{\infty,v}/L_{\infty,v}, E_{p^\infty})$ étant nuls, les applications r_1 et r_2 sont des isomorphismes. D'après le Corollaire 3.2, $H^1_p(F_\infty, E_{p^\infty}) = S(F_\infty)$ et $H^1_p(L_\infty, E_{p^\infty}) = S(L_\infty)$, les égalités précédentes s'en déduisent par passage au dual.

REMARQUE: Les Théorèmes 3.23 et 3.24 restent valables sans l'hypothèse $E_p \subset E(F)$ comme on le voit en faisant agir le groupe $\Delta = \mathrm{Gal}(F(E_p)/F))$ d'ordre premier à p sur les divers modules intervenant.

Nous savons que le Λ-module $\widehat{S(F_\infty)}$ est sans sous-module pseudo-nul non nul, nous terminerons ce paragraphe en montrant que si L_∞ est une $\mathbb{Z}_p$-extension de F contenue dans F_∞, vérifiant les hypothèses du Théorème précédent, le Λ_2-module $\widehat{S(L_\infty)}$ est lui aussi sans sous-module pseudo-nul non nul.

LEMME 3.25: *Soient M un $\Lambda' = \mathcal{O}_p[[T, T']]$-module de type fini sans sous-modue pseudonul non nul, α et β deux éléments de l'idéal maximal de Λ' premiers à la série caractéristique de $(M)_{\mathrm{tors}}$. Le module $M/_{\alpha M}$ est alors sans sous-module fini non nul si et seulement si il en est de même de $M/_{\beta M}$.*

DÉMONSTRATION: Considérons le diagramme exact:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & M & \xrightarrow{\alpha} & M & \to & M/_{\alpha M} & \to & 0 \\
 & & \downarrow \beta & & \downarrow \beta & & \downarrow \beta & & \\
0 & \to & M & \xrightarrow{\alpha} & M & \to & M/_{\alpha M} & \to & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & M/_{\beta M} & \xrightarrow{\alpha} & M/_{\beta M} & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Le lemme du serpent nous fornit un isomorphisme:

$$_\beta(M/_{\alpha M}) =_\alpha (M/_{\beta M}).$$

Puisque $M/\alpha M$ a un sous-module fini non nul si et seulement si il en est de même de $_\beta(M/\alpha M)$, le résultat est clair.

PROPOSITION 3.26: *Soit L_∞ une $\mathbb{Z}_p$-extension contenue dans F_∞. On suppose, en reprenant les notations du Théorème* 3.24, *que le rang sur Λ_2*

de $\widehat{S(L_\infty)}$ *est égal à celui de* $\widehat{S(F_\infty)}$ *sur* Λ (*i.e.*: $(\gamma-1)$ *est premier à la série caractéristique de* $(\widehat{S(F_\infty)})_{\text{tors}}$).

Le Λ_2*-module* $\widehat{S(L_\infty)}$ *est alors sans sous-module pseudo-nul non nul.*

DÉMONSTRATION: D'après le Lemme 3.6 on dispose d'un isomorphisme:

$$\widehat{S(F_\infty)} \underset{\Lambda}{\otimes} \Lambda' \simeq \mathrm{Hom}_{\mathcal{O}_p}\Big(T_p,\ X \underset{\Lambda}{\otimes} \Lambda'\Big) \oplus \mathrm{Hom}_{\mathcal{O}_p}\Big(\overline{T_p},\ X \underset{\Lambda}{\otimes} \Lambda'\Big).$$

Puisque $\widehat{S(L_\infty)} \simeq \widehat{S(F_\infty)}/_{(\gamma-1)\widehat{S(F_\infty)}}$, il suffit donc de montrer que chacun des Λ'-modules $\mathrm{Hom}_{\mathcal{O}_p}(T_p,\ X \underset{\Lambda}{\otimes} \Lambda')$ et $\mathrm{Hom}_{\mathcal{O}_p}(\overline{T_p},\ X \underset{\Lambda}{\otimes} \Lambda')$ réduits modulo $(\gamma-1)$ ne possède pas de sous-module fini non nul, nous le montrerons pour le premier.

Rappelons (Démonstration de 3.7) que $\mathrm{Hom}_{\mathcal{O}_p}(T_p,\ X \underset{\Lambda}{\otimes} \Lambda')$ est isomorphe au Λ-module $(X \underset{\Lambda}{\otimes} \Lambda')_\phi$ obtenu à partir de $X \underset{\Lambda}{\otimes} \Lambda'$ par restriction des scalaires selon l'isomorphisme $\phi\colon \Lambda' \xrightarrow{\sim} \Lambda'$ défini par $\phi(\gamma) = \epsilon(\gamma)^{-1}\gamma$, $\phi(\gamma') = \epsilon(\gamma')^{-1}\gamma'$. On obtient donc les isomorphismes:

$$\begin{aligned}
&\mathrm{Hom}_{\mathcal{O}_p}\Big(T_p,\ X \underset{\Lambda}{\otimes} \Lambda'\Big)/(\gamma-1)\mathrm{Hom}_{\mathcal{O}_p}\Big(T_p,\ X \underset{\Lambda}{\otimes} \Lambda'\Big)\\
&\quad\simeq \Big(X \underset{\Lambda}{\otimes} \Lambda'\Big)_\phi/(\gamma-1)\Big(X \underset{\Lambda}{\otimes} \Lambda'\Big)_\phi\\
&\quad\simeq \Big(X \underset{\Lambda}{\otimes} \Lambda'/\big(\epsilon(\gamma)^{-1}\gamma-1\big)X \underset{\Lambda}{\otimes} \Lambda'\Big)_\phi.
\end{aligned}$$

Ce dernier module est sans sous-module fini non nul si et seulement si il en est de même de $X \underset{\Lambda}{\otimes} \Lambda'/(\epsilon(\gamma)^{-1}\gamma-1)X \underset{\Lambda}{\otimes} \Lambda'$. Il nous suffit alors d'appliquer le lemme précédent avec $M = X \underset{\Lambda}{\otimes} \Lambda'$, $\alpha = \gamma-1$ et $\beta = \epsilon(\gamma)^{-1}\gamma-1$. D'après les résultats de Greenberg ([3]), nous savons que $X \underset{\Lambda}{\otimes} \Lambda'$ est sans sous Λ'-module pseudo-nul non nul, que $(\gamma-1)$ est premier à la série caractéristique de la torsion de $X \underset{\Lambda}{\otimes} \Lambda'$ et enfin que $X \underset{\Lambda}{\otimes} \Lambda'/(\gamma-1)X \underset{\Lambda}{\otimes} \Lambda'$ est sans sous-module fini non nul, l'hypothèse faite implique d'autre part que $\epsilon(\gamma)^{-1}\gamma-1$ est premier à la série caractéristique de la torsion de $X \underset{\Lambda}{\otimes} \Lambda'$.

APPLICATION 1: Nous donnons des exemples de $\mathbb{Z}_p$-extensions sur lesquelles la torsion du dual du groupe de Selmer n'est pas pseudo-nul.

Nous considérons pour cela une courbe elliptique définie sur le corps de multiplication complexe K telle que le rang sur $\mathbb{Z}$ de $E(K)$ soit supérieur ou égal à 4 et une $\mathbb{Z}_p$-extension L_∞ de K telle que $\widehat{\Sigma(L_\infty)}$ soit de torsion, notons que cette dernière condition est réalisée pour presque toute $\mathbb{Z}_p$-extension de K. En utilisant le Théorème 3.24 il nous suffit de montrer que le module $\widehat{\Sigma(L_\infty)}$ n'est pas pseudo-nul.

Si $\Gamma = \mathrm{Gal}(L_\infty/K)$, on vérifie (voir Application 2) l'égalité:

$$\Sigma(K) = \Sigma(L_\infty)^\Gamma.$$

En considérant le diagramme exact suivant:

$$\begin{array}{ccccc} & & E(K)\otimes Q_p/\mathbb{Z}_p & \xrightarrow{\phi} & E(K_p)\otimes \mathbb{Q}_p/\mathbb{Z}_p \\ & & \downarrow & & \downarrow \\ 0 \to \Sigma(K) \to & & S(K) & \to & H^1(K_p,\, E_{p^\infty}) \end{array}$$

On note que $\mathrm{Ker}(\phi) \subset \Sigma(K)$; le rang sur $\mathbb{Z}_p$ du dual de $E(K_p)\otimes \mathbb{Q}_p/\mathbb{Z}_p$ est égal à 2 alors que celui du dual de $E(K)\otimes \mathbb{Q}_p/\mathbb{Z}_p$ est, compte-tenu des hypothèses faites, supérieur à 4. Il résulte alors que $\widehat{\Sigma(K)}$ est de rang sur $\mathbb{Z}_p$ strictement positif et que par conséquent $\widehat{\Sigma(L_\infty)}$ n'est pas pseudo-nul.

Application 2: Soient E une courbe elliptique définie sur un corps quadratique imaginaire K à multiplication complexe par les entiers de K, $F = K(E_p)$, $\Delta = \mathrm{Gal}(F/K)$, L_∞ une $\mathbb{Z}_p$-extension de K. Si P est la pro-p-extension maximale non ramifiée hors de p de F on vérifie les identités suivantes:

$$S'(L_\infty) = S'(L'_\infty)^\Delta = H^1(P/_{L'_\infty},\, E_{p^\infty})^\Delta = H^1(P/_{L_\infty},\, E_{p^\infty})$$

$$S'(K) = S'(F)^\Delta = H^1(P/_F,\, E_{p^\infty})^\Delta = H^1(P/_K,\, E_{p^\infty})$$

$$S'^{(p)}(K) = H^1(P/_K,\, E_p)$$

$$\Sigma^{(p)}(K) = \Sigma^{(p)}(F)^\Delta$$

Lemme 3.26: *Si* $G = \mathrm{Gal}(L_\infty/K)$ *on a*:

$$S'(K) = S'(L_\infty)^G$$

$$\Sigma(K) = \Sigma(L_\infty)^G$$

DÉMONSTRATION: En utilisant le fait que $E_{p^\infty}(L_\infty) = E_{p^\infty}(L_{\infty,p}) = 0$ on obtient le diagramme exact:

$$\begin{array}{ccccccc} 0 \to \Sigma(L_\infty)^G & \to & H^1(P/L_\infty,\ E_{p^\infty})^G & \to & H^1(L_{\infty,p},\ E_{p^\infty})^G \\ \uparrow & & \uparrow & & \uparrow \\ 0 \to \Sigma(K) & \to & H^1(P/K,\ E_{p^\infty}) & \to & H^1(K_p,\ E_{p^\infty}) \end{array}$$

Le lemme s'en déduit immédiatement.

LEMME 3.27:

$$S'^{(p)}(K) = S'(K)(p)$$

$$\Sigma^{(p)}(K) = \Sigma(K)(p).$$

DÉMONSTRATION: Le groupe $E_{p^\infty}(K)$ étant nul, la cohomologie de la suite

$$0 \to E_p \to E_{p^\infty} \xrightarrow{p} E_{p^\infty} \to 0$$

nous donne la suite exacte:

$$0 \to H^1(P/K,\ E_p) \to H^1(P/K,\ E_{p^\infty}) \xrightarrow{p} H^1(P/K,\ E_{p^\infty})$$

d'où $S'^{(p)}(K) = S'(K)(p)$.

Puisque $E_{p^\infty}(K_p) = 0$, le diagramme suivant est exact:

$$\begin{array}{ccccc} 0 \to \Sigma(K) & \to & S'(K) & \to & H^1(K_p,\ E_{p^\infty}) \\ \uparrow & & \uparrow & & \uparrow \\ 0 \to \Sigma^{(p)}(K) & \to & S'^{(p)}(K) & \to & H^1(K_p,\ E_p) \end{array}$$

On en déduit $\Sigma^{(p)}(K) = \Sigma(K) \cap S'^{(p)}(K) = \Sigma(K)(p)$.
Dans la suite nous faisons l'hypothèse que p ne divise pas le nombre de classes h(F) du corps F

LEMME 3.28:

$$\Sigma(K) = 0.$$

DÉMONSTRATION:

$$\Sigma^{(p)}(F) = \mathrm{Ker}\Big(H^1(P/F,\ E_p) \to H^1(F_p,\ E_p)\Big) \subset \mathrm{Hom}\big(\mathrm{Gal}(H(F)/F),\ E_p\big)$$

où H est le corps de Hilbert de F.

Sous notre hypothèse le dernier groupe est nul donc $\Sigma^{(p)}(F) = 0$ et par conséquent $\Sigma(K)(p) = \Sigma^{(p)}(K) = (\Sigma^{(p)}(F))^{\Delta} = 0$. Le groupe $\Sigma(K)$ étant de p-torsion le lemme est démontré.

COROLLAIRE 3.29:

(1) $\widehat{S(L_\infty)} = 0$

(2) $\widehat{S(L_\infty)}$ *se plonge dans un* $\mathbb{Z}_p[[\mathrm{Gal}(L_\infty/K)]]$*-module libre de rang* 2 *avec un conoyau fini.*

D'après les résultats précédents il suffit de vérifier la première assertion:

$$\left(\widehat{\Sigma(L_\infty)}\right)_G = \left(\widehat{\Sigma(L_\infty)}^G\right) = \widehat{\Sigma(K)} = 0.$$

EXEMPLE: Si E est la courbe d'équation $y^2 = x^3 - x$ à multiplication complexe par $K = \mathbb{Q}(i)$, on vérifie en calculant le discriminant du corps $K(E_7)$ et en utilisant les bornes sur les discriminants des corps totalement imaginaires [9] que 7 ne divise pas le nombre de classe de $K(E_7)$.

Il serait intéressant d'aller plus loin dans l'analyse du module $\widehat{S(L_\infty)}$ et de savoir sous quelles conditions il est libre, on montre sans difficulté que c'est le cas si et seulement si $S'^{(p)}(K)$ est de rang 2 sur le corps $\mathbb{F}_p$; cette dernière condition est elle-même liée à la structure, sous l'action de Δ, du groupe des unités locales en p de F quotienté par l'adhérence de l'image des unités globales.

Bibliographie

[L.C] A. GROTHENDIECK: Local cohomology, *Lectures notes in Math.* 41, Springer Verlag, Berlin (1967).

[1] P. BILLOT: Thèse 3ème cycle, Orsay. Groupe de Selmer et Théorie d'Iwasawa.

[2] A. CUOCO: The growth of Iwasawa invariants in a family, *Compositio Math.*, Vol. 41, fasc 3 (1980) 415–437.

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

[4] K. IWASAWA: $\mathbb{Z}_\ell$-extensions of number fields, Notes d'un cours à Princeton rédigées par R. Greenberg.

[5] KONOVALOV: The universal G-norms of formal groups over a local field, *Vkranian Math. J.* 28 (1976) 310–311.

[6] B. PERRIN-RIOU: Thèse d'Etat, Orsay, Arithmétique des courbes elliptiques, (1983).

[7] K. RUBIN: Elliptic curves and $\mathbb{Z}_p$-extensions, à paraître.

[8] J. TATE: W.C. groups over p-adic fields, Séminaire Bourbaki, No. 156 (1957).

[9] F. DIAZ et DIAZ: Tables minorant la racine n-ième du disriminant d'un corps de degré n, Publications Math. Orsay (1980).

(Oblatum 17-I-1985 & 24-VI-1985)

Patrick Billot
Université Paris-Sud, Centre d'Orsay
Mathematique, Pâtiment 425
F-91405 Orsay Cedex
France