Journal de Théorie des Nombres
de Bordeaux **7** *(1995), 307–331*

Structures Galoisiennes et Courbes Elliptiques

par Philippe Cassou-Nogues et Martin J. Taylor

Introduction

Soit N/K une extension galoisienne de corps de nombres, de groupe de Galois G. L'anneau des entiers O_N de N possède une structure naturelle de G-module. C'est un problème fondamental d'arithmétique que de classifier cette structure. Lorsque l'extension est modérément ramifiée, on sait par le célèbre théorème de E. Noether que O_N est localement libre en tant que $\mathbb{Z}[G]$-module. Après le résultat qu'il avait obtenu lorsque le groupe G est le groupe quaternionien d'ordre 8, Fröhlich avait conjecturé le résultat suivant qui a été démontré par le second auteur dans [T1].

Théorème 1. *Soit N/K une extension modérément ramifiée et soit (O_N) (resp. $(O_K[G])$) la classe de O_N (resp. $O_K[G]$) dans $K_0(\mathbb{Z}[G])$, le groupe de Grothendieck des $\mathbb{Z}[G]$-modules localement libres. Alors $2(O_N) = 2(O_K[G])$. En outre $(O_N) = (O_K[G])$, si les constantes d'Artin des caractères irréductibles et symplectiques de G sont égales à 1.*

Par contre, lorsque N/K est sauvagement ramifiée, la situation est moins claire. Si $K = Q$ et si G est abélien, Leopoldt a complètement déterminé la structure de O_N comme G-module, [Le]. Dans le cas d'une extension Kummerienne N/K, on peut utiliser le théorème de Stickelberger pour décrire la sructure galoisienne d'un sous-ordre naturel de O_N, qu'on appelle ordre de Kummer. Le lecteur peut se reporter à [T2] pour cette étude. Le but de cet article est de décrire une théorie analogue lorsqu'on remplace le groupe multiplicatif de la théorie de Kummer par une courbe elliptique. Plus précisément, on se propose de décrire l'anneau des entiers d'extensions engendrées par les points de division d'un point rationnel sur K d'une courbe elliptique définie sur K.

Manuscrit reçu le 9 Avril 1994, version corrigée le 17 Décembre 1995.

La première partie de cet article est entièrement algébrique : nous y introduisons la théorie des ordres de Hopf et de leurs espaces homogènes principaux, qu'on désigne par e.h.p. Nous définissons l'invariant de classe ou invariant de Picard d'un tel espace ; cet invariant nous permet d'étudier notre problème initial de structure galoisienne en termes géométriques. Dans la seconde partie, nous appliquons cette théorie aux ordres de Hopf, provenant des schémas en groupe associés à une courbe elliptique. Il est alors naturel de considérer séparément les invariants de Picard associés d'une part à un point de torsion de E et d'autre part à un point d'ordre infini. Pour les points de torsion, on trouve que l'invariant de Picard est en général trivial.

Les parties suivantes consistent en une étude détaillée des points d'ordre infini à invariant de Picard trivial. Nous commençons par rappeler les résultats de [A-T] : la théorie d'Iwasawa permet de montrer que les classes de e.h.p., libres sur l'ordre maximal, proviennent du sous-groupe de Greenberg du groupe de Mordell-Weil complété. Puis nous indiquons les résultats obtenus dans un travail commun, [CN-T], sur la construction de générateurs explicites pour ces modules libres. Le résultat principal est ici le rôle surprenant joué par la fonction L-p-adique de la courbe elliptique et les unités elliptiques dans cette construction.

1. Généralités algébriques

1.1. Structure de Hopf

Nous notons $\overline{K}$ une clôture algébrique d'un corps de nombres K et $\Omega_K = Gal(\overline{K}/K)$ le groupe de Galois absolu de K. Dorénavant G est un groupe abélien fini sur lequel opère Ω_K. L'action de Ω_K sur l'algèbre $\overline{K}[G]$ est définie par $(kg)^\omega = k^\omega g^\omega$, A_K est l'algèbre $(\overline{K}[G])^{\Omega_K}$ des points fixes et $B_K = Map(G, \overline{K})^{\Omega_K}$ est la K-algèbre des applications $b : G \to \overline{K}$ qui commutent avec l'action de Ω_K. En fait, A_K et B_K sont toutes les deux des K-algèbres de Hopf : les homomorphismes d'algèbres (que l'on appelle comultiplications)

$$\Delta_A : A_K \to A_K \otimes_K A_K, \Delta_B : B_K \to B_K \otimes_K B_K = Map(G \times G; \overline{K})^{\Omega_K}$$

sont induits par les applications $g \mapsto g \otimes g$ (resp. $\Delta_B(b)(g,h) = b(g \cdot h)$) sur $\overline{K}[G]$ (resp. $Map(G, \overline{K})$) ; l'homomorphisme d'augmentation (resp. d'évaluation sur 1_G) induit un homomorphisme

$$\varepsilon_A : A_K \to K (\text{resp. } \varepsilon_B : B_K \to K).$$

L'accouplement

$$<,>: A_K \times B_K \to K$$
$$< \sum_{g \in G} a_g g, b >= \sum_{g \in G} a_g b(g)$$

est non dégénéré, il nous permet donc d'identifier A_K avec B_K^D (Le K-dual de B_K) et B_K avec A_K^D. Avec ces identifications, on note que Δ_A^D (resp. Δ_B^D) est la multiplication de B_K (resp. de A_K).

Soit $\mathfrak{a}$ un O_K-ordre de A_K. On dit que $\mathfrak{a}$ est un ordre de Hopf s'il est stable par la comultiplication Δ_A, c'est-à-dire $\Delta_A(\mathfrak{a}) \subset \mathfrak{a} \otimes_{O_K} \mathfrak{a}$. (Puisque $\mathfrak{a}$ est O_K-projectif $\mathfrak{a} \otimes_{O_K} \mathfrak{a} \subset A_K \otimes_K A_K$). On définit un ordre de Hopf $\mathfrak{b}$ de B_K de la même mamière. Pour un tel ordre de Hopf $\mathfrak{b}$ on définit le O_K-dual

$$\mathfrak{b}^D = \{a \in A_K | < a, \mathfrak{b} >\subset O_K\}.$$

Il est facile de voir que $\mathfrak{b}^D$ est un ordre de Hopf de A_K : en effet, il est stable par multiplication (resp. comultiplication), parce que $\mathfrak{b}$ est stable par comultiplication (resp. multiplication).

Dans la suite $\mathfrak{b}$ sera construit géométriquement et, par raison de simplicité nous noterons toujours

$$\mathfrak{a} \stackrel{def}{=} \mathfrak{b}^D$$

Remarque. Dans le langage des schémas Spec $(\mathfrak{a})$ et Spec $(\mathfrak{b})$ sont tous les deux des schémas en groupe finis et plats sur Spec(O_K) ; ils sont duaux au sens de Cartier.

1.2. Structure de module

G opère par translation sur Map$(G, \overline{K})$. Cette action induit une structure de A_K-module sur B_K ; en fait $B_K \otimes_K \overline{K}$ est visiblement libre de rang un comme $A_K \otimes_K \overline{K}$ module ; et donc, par le théorème 90 de Hilbert, B_K est libre de rang un comme A_K-module.

Il découle directement de la définition de $\mathfrak{a}$ que $\mathfrak{b}$ est un $\mathfrak{a}$-module ; en fait, on peut faire beaucoup mieux. On a le théorème suivant dû à Larsen.

Théorème 2. *$\mathfrak{b}$ est un $\mathfrak{a}$-module localement libre.*

On peut se reporter à [SW] pour la démonstration. Un des principaux avantages des ordres de Hopf est l'existence d'un critère de Noether généralisé pour reconnaître ses modules projectifs. Posons $\Sigma = \sum_{g\in G} g \in A_K$ et définissons l'idéal $\mathfrak{c}$ de O_K par l'égalité $K\Sigma \cap \mathfrak{a} = \mathfrak{c}^{-1}\Sigma$.

Théorème 3 (Childs et Hurley). *Soit M un $\mathfrak{a}$-module de type fini, sans torsion sur O_K, tel que $M \otimes_{O_K} K$ soit libre de rang un sur A_K. Soit M^G le sous-module des points fixes par $\mathfrak{a}$, i.e.*

$$M^G = \{m \in M | ma = m\varepsilon_A(a), \forall a \in \mathfrak{a}\}$$

Alors M est un $\mathfrak{a}$-module projectif si et seulement si $M\Sigma = M^G\mathfrak{c}$.

1.3. Espaces homogènes principaux

Soit C une K-algèbre. On dit que C est une A_K-algèbre si C est un A_K-module et si pour tout $a \in A_K, c_1, c_2 \in C$

$$(c_1c_2)a = \sum_i (c_1a_{1i})(c_2a_{2i})$$

où

$$\Delta_A(a) = \sum_i a_{1i} \otimes a_{2i}.$$

On dit qu'une telle algèbre C est un espace homogène principal pour B_K, e.h.p., s'il existe une extension finie L/K telle que

$$C \otimes_K L \simeq B_K \otimes_K L$$

en tant que $A_K \otimes_K L$-algèbres. Un tel isomorphisme est appelé isomorphisme de décomposition. L'ensemble des classes d'isomorphismes de e.h.p. pour B_K est un groupe noté $PH(B_K)$ qui s'identifie avec $H^1(K, G)$.

Un espace homogène principal pour $\mathfrak{b}$ est une O_K-algèbre $\mathfrak{c}$ sur laquelle $\mathfrak{a}$ opère. C'est un ordre d'un e.h.p. pour $B_K, C = \mathfrak{c}K$ tel que l'isomorphisme de décomposition pour C induise un isomorphisme

$$\mathfrak{c} \otimes_{O_K} O_L \simeq \mathfrak{b} \otimes_{O_K} O_L$$

de $\mathfrak{a} \otimes O_L$-algèbres. Ceci revient à dire que les e.h.p. pour $\mathfrak{b}$ sont les torseurs de $\mathfrak{b}$ dans la catégorie des $\mathfrak{a}$-algèbres.

Nous notons $PH(\mathfrak{b})$ l'ensemble de classes d'isomorphismes d'e.h.p. de $\mathfrak{b}$. C'est un groupe : en effet, il s'identifie avec H^1_{flat} (Spec($\mathcal{O}_\mathcal{K}$), Spec ($\mathfrak{b}$)), (voir Milne Ch. III, §4).

1.4. L'invariant de classe

Nous gardons les notations et hypothèses du paragraphe précédent. Alors C est un A_K-module et $C \otimes_K L \simeq B_K \otimes_K L$ comme $A_K \otimes_K L$ algèbres ; donc C est un A_K module libre de rang un. Grâce au théorème 2, nous savons que $\mathfrak{b} \otimes_{O_K} O_L$ est localement libre sur $\mathfrak{a}$, de rang $[L : K]$; ceci implique que $\mathfrak{c}$ est un $\mathfrak{a}$-module projectif tel que $\mathfrak{c} \otimes_{O_K} K \simeq A_K$; d'où nous concluons que $\mathfrak{c}$ est nécessairement localement libre sur $\mathfrak{a}$ de rang un. (Voir [F1] par exemple). Ainsi nous avons construit une application

$$\psi_1 : PH(\mathfrak{b}) \to Cl(\mathfrak{a})$$
$$\psi_1(\mathfrak{c}) = (\mathfrak{c}) - (\mathfrak{b}).$$

où $Cl(\mathfrak{a})$ est le groupe des classes des $\mathfrak{a}$-modules localement libres. On appelle $\psi_1(\mathfrak{c})$ l'invariant de classes de $\mathfrak{c}$ (ou parfois l'invariant de Picard de $\mathfrak{c}$). Il est bien connu que ψ_1 est un homomorphisme : le lecteur peut trouver les détails dans [W] ou [B-T].

1.5. Un exemple

Supposons que Ω_K opère trivialement sur G. On vérifie aisément que $\mathfrak{b} = Map(G, O_K)$ est un ordre de Hopf et que $\mathfrak{a} = O_K[G]$ est son dual.

Soit N/K une extension galoisienne non ramifiée munie d'une injection $\mathfrak{i} : Gal(N/K) \hookrightarrow G$. Posons $H = Imi$ et $C = Map_H(G, N)$, c'est-à-dire la K-algèbre des applications $f : G \to N$ telles que

$$f(g)^\gamma = f(g.i(\gamma)), \forall \gamma \in Gal(N/K), g \in G.$$

Alors $\mathfrak{c} = Map_H(G, O_N)$ est l'ordre maximal de C et l'on a l'isomorphisme de $\mathfrak{a} \otimes O_N$ algèbres

$$\xi : \mathfrak{c} \otimes_{O_K} \xrightarrow{\simeq} Map(G, O_N) = \mathfrak{b} \otimes_{O_K} O_N.$$

$$\xi(c \otimes \lambda)(g) = c(g).\lambda.$$

Ainsi $\mathfrak{c}$ est e.h.p. pour $\mathfrak{b}$. Réciproquement, on vérifie que chaque e.h.p. de $\mathfrak{b}$ est de cette forme. En conclusion, on a montré que $PH(\mathfrak{b})$ est constitué dans ce cas des classes d'isomorphismes des anneaux d'entiers des algèbres galoisiennes non ramifiées de K, de groupe de Galois isomorphe à G.

2. Courbes elliptiques

2.1 Notations

Soit F un corps quadratique imaginaire. Désormais E est une courbe elliptique définie sur F, avec multiplication complexe par O_F. On sait que E a potentiellement bonne réduction ([Se-T]) ; nous supposons dans la suite que $K \supset F$ et que E/K a partout bonne réduction.

Une fois pour toutes, nous choisissons un endomorphisme non nul $\pi \in O_F$ et l'on note G le groupe des points de π-division de E

$$G = Ker(\pi : E(\overline{K}) \to E(\overline{K})).$$

En outre G est muni de sa structure naturelle de Ω_K module.

Soit $\mathcal{E}/Spec(\mathcal{O}_K)$ le modèle de Néron de E/K. Par la propriété universelle de ce modèle, π induit un endomorphisme $\tilde{\pi} : \mathcal{E} \to \mathcal{E}$; nous écrivons $\mathcal{G} = Ker(\tilde{\pi})$. Puisque E/K a partout bonne réduction, on sait que $\mathcal{G}/Spec(\mathcal{O}_K)$ est fini et plat ; il est donc localement libre et sa fibre générique $\mathcal{G} \underset{Spec(O_K)}{\times} Spec(K)$ peut être identifiée avec $Spec(B_K)$; donc il existe un unique ordre de Hopf dans B_K tel que $\mathcal{G} = Spec(\mathfrak{b})$.

Dans ce qui suit nous allons appliquer la théorie du §1 à ces ordres de Hopf $\mathfrak{b}$ et aux e.h.p. provenant du groupe de Mordell-Weil.

2.2. L'invariant de classe d'un point rationnel

Considérons la suite exacte Kummérienne associée à l'endomorphisme $\tilde{\pi}$ de $\mathcal{E}$:

$$\{0\} \to \mathcal{G} \to \mathcal{E} \xrightarrow{\tilde{\pi}} \mathcal{E} \to \{0\}.$$

Le foncteur de sections globales sur $Spec(O_K)$ permet de définir une suite exacte de cohomologie

$$\{0\} \to \mathcal{G} \to \mathcal{E}(O_K) \xrightarrow{\tilde{\pi}} \mathcal{E}(O_K) \to H^1(Spec(O_K), \mathcal{G}).$$

On a déjà vu que

$$PH(\mathfrak{b}) = H^1(Spec(O_K), \mathcal{G}).$$

De plus, par la propriété universelle du modèle de Néron, on sait que

$$\frac{E(K)}{\pi E(K)} \cong \frac{\mathcal{E}(O_K)}{\tilde{\pi}\mathcal{E}(O_K)}.$$

Ainsi nous avons construit un homomorphisme $E(K) \to PH(\mathfrak{b})$. Le but essentiel de cet article est l'étude de l'homomorphisme ψ

$$\begin{array}{ccc} E(K) & \longrightarrow & PH(\mathfrak{b}) \\ & \psi \searrow & \downarrow \psi_1 \\ & & cl(\mathfrak{a}) \end{array}$$

Il est évident que le comportement de ψ sur $E(K)_{torsion}$ est particulièrement intéressant pour deux raisons :

(1) Par la théorie de la multiplication complexe les points de torsion de $E(\overline{F})$ engendrent un système cofinal d'extensions abéliennes de F ;

(2) En se servant des groupes formels, on trouve que l'e.h.p. associé à un point de torsion est souvent intégralement clos.

Par conséquent le résultat suivant est très important pour l'étude des anneaux d'entiers des extensions abéliennes de F :

Théorème 4 (Srivastav-Taylor, [ST]). *Soit w_F le nombre de racines de l'unité de F. Si $(\pi, w_F) = 1$, alors $E(K)_{torsion} \subset Ker\ \psi$.*

Remarque. Le cas où l'idéal πO_F est un produit d'idéaux premiers pairs (i.e. au dessus de 2) semble être difficile, voir [CN-S] par exemple.

L'existence, pour les extensions modérément ramifiées, d'un lien entre la structure galoisienne des anneaux d'entiers et le comportement de certaines fonctions L d'Artin, mis en évidence par le théorème 1, est le résultat central de cette théorie. Dans le cas elliptique, que nous considérons dans ce paragraphe, le Théorème 4 nous incite à croire, via la conjecture de Birch-Swinnerton-Dyer, à l'existence d'un lien entre la structure galoisienne des e.h.p. associés aux points K-rationnels de E et le comportement de la fonction de Hasse-Weil de E/F. Il est donc intéressant de montrer dès maintenant qu'on peut construire des points d'ordre infini de $E(K)$ qui n'appartiennent pas à $Ker\ \psi$. Néanmoins comme le montre l'exemple qui suit il est difficile d'obtenir une description de $Ker\ \psi$ à "niveau fini". Ce problème peut se résoudre en "passant à la limite".

2.3. Exemple

On pose $F = \mathbb{Q}(\sqrt{-7}$ et $K = F(\sqrt[4]{63})$. On considère la courbe elliptique E/K d'équation.

$$y^2 + \sqrt[4]{63}xy = x^3 + x.$$

Cette courbe a multiplication complexe par O_F et possède partout bonne réduction sur K. Soit $\pi = \frac{1+i\sqrt{7}}{2}$. C'est un générateur d'un relèvement premier de 2 dans O_F et donc un diviseur de $2 = w_F$. On désigne par P le point de $E(K)$ de coordonnées affines $(i, 0)$.

Théorème 5 [CN-S].

1. $E(K)_{torsion} \subset Ker\ \psi$

2. $P \notin Ker\ \psi$.

Remarques.

1. Si l'on désigne par $\mathfrak{m}$ l'ordre maximal de $K[G]$ et par Φ l'homomorphisme obtenu en composant ψ par l'extension des scalaires $cl(\mathfrak{a}) \to cl(\mathfrak{m})$, on montre que $P \notin Ker\ \Phi$.

2. Si l'on remplace K par le corps $L = K(\sqrt{3u})$ où $u = (1-i)(1+\pi) + \sqrt[4]{63}$, et qu'on note Φ_L l'analogue de Φ dans cette nouvelle situation, on peut montrer que P appartient dans ce cas à $Ker\ \Phi_L$. C'est donc un élément d'ordre infini de $E(L)$ qui n'appartient pas à $\pi E(L)$ et dont l'image par Φ_L est triviale.

3. Passage à la limite

3.1. Notations et Hypothèses

Les notations sont celles du paragraphe 2. On suppose que l'extension (K/F) est abélienne, de groupe de Galois Δ.

On fixe jusqu'à la fin de cet article un nombre premier p. On suppose satisfaites les hypothèses suivantes :

a) p n'est pas anormal. Il est décomposé dans F et l'on a $\mathfrak{p}\ 0_F = \mathfrak{p}\mathfrak{p}^*$ où $\mathfrak{p}$ et $\mathfrak{p}^*$ sont des idéaux premiers distincts de F.

b) La courbe E/F a bonne réduction au-dessus de $\mathfrak{p}$ et $\mathfrak{p}^*$ et E/K a bonne réduction en toute place de K.

c) $p \geq 5$ et $p \nmid |\Delta|$.

Les premiers $\mathfrak{p}$ et $\mathfrak{p}^*$ sont principaux. On pose $\mathfrak{p} = \pi O_F$ et $\mathfrak{p}^* = \pi^* O_F$. On peut choisir pour π(resp.π^*) la valeur en $\mathfrak{p}$ (resp. $\mathfrak{p}^*$) du Grössencharakter attaché à la courbe E/F. On rappelle que p est dit anormal pour E si $\pi + \overline{\pi} = 1$, ou de façon équivalente si la trace de l'endomorphisme de Frobenius de E modulo $\mathfrak{p}$ est égale à 1.

Soit un entier, $n \geq 1$. On note $E_{\mathfrak{p}^n}$ (resp. $E_{\mathfrak{p}^{*n}}$) le groupe des points de $\mathfrak{p}^n$ (resp. $\mathfrak{p}^{*n}$) division de E. Si L/F est une extension de F on définit

$$L_n = L(E_{\mathfrak{p}^n}) \quad (\text{resp. } L_n^* = L(E_{\mathfrak{p}^{*n}}))$$

$$L_\infty = L(E_{\mathfrak{p}^\infty}) \quad (\text{resp. } L_\infty^* = L(E_{\mathfrak{p}^{*\infty}})).$$

On fait l'hypothèse que p est non ramifié dans K et même que $\mathfrak{p}^*$ est totalement décomposé dans K. On en déduit les égalités :

$$K \cap F_n = K \cap F_n^* = F$$

On désigne par X_n (resp. X_n^*) le groupe $Gal(K_n/K)$ (resp. $Gal(K_n^*/K)$). On obtient par restriction des isomorphismes qui permettent d'identifier les groupes

$$X_n \xrightarrow{\sim} Gal(F_n/F)$$

$$X_n^* \xrightarrow{\sim} Gal(F_n^*/F).$$

On pose $G_n = E_{\mathfrak{p}^n}$ (resp. $G_n^* = E_{\mathfrak{p}^{*n}}$) et on désigne par A_n (resp. B_n) les K-algèbres de Hopf introduites en (1-1), on note $\mathfrak{a}_n$ (resp. $\mathfrak{b}_n$) les ordres de Hopf de A_n (resp. B_n) définis en (2-1) pour l'endomorphisme π^n. On sait donc associer à toute classe d'isomorphisme de e.h.p. de $\mathfrak{b}_n$ un invariant dans $cl(\mathfrak{a}_n)$, c'est-à-dire définir un homomorphisme de groupe

$$\psi_n : PH(\mathfrak{b}_n) \to cl(\mathfrak{a}_n).$$

Si $\mathfrak{m}_n$ désigne l'ordre maximal de A_n, en composant ψ_n avec l'extension des scalaires $e_n : cl(\mathfrak{a}_n) \to cl(\mathfrak{m}_n)$, on obtient l'homomorphisme :

$$\phi_n : PH(\mathfrak{b}_n) \to cl(\mathfrak{m}_n).$$

3.2. Groupes de Selmer

Si M est un O_F-module et α un élément non nul de O_F, on note M_α le sous-module des éléments de M annulés par α et $T_\alpha(M)$ la limite projective des M_{α^n} où les applications de transition $M_{\alpha^{n+1}} \to M_{\alpha^n}$ sont induites par la multiplication par α.

On déduit de la suite exacte de Ω_K-modules

$$\{0\} \to E_{\pi^n} \to E(\overline{K}) \xrightarrow{\pi^n} E(\overline{K}) \to \{0\}$$

une suite exacte de cohomologie

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

On définit le groupe de Tate-Shafarevitch $Ш(K)$ de E/K comme le noyau de l'homomorphisme naturel

$$H^1(K, E) \to \prod_v H^1(K_v, E)$$

où v parcourt les places finies de K.

On définit le groupe de Selmer $S_n(K)$ de E/K, relatif à π^n, comme le noyau de l'homomorphisme naturel

$$H^1(K, E_{\pi^n}) \to \prod_v H^1(K_v, E).$$

On a la suite exacte

$$\{0\} \to \frac{E(K)}{\pi^n E(K)} \to S_n(K) \to Ш(K)_{\pi^n} \to \{0\}.$$

Soit $\mathfrak{c}$ un e.h.p. pour $\mathfrak{b}_n$ et C le K-algèbre $\mathfrak{c}.K$. On sait associer à une telle algèbre, par la théorie de la descente galoisienne, une classe de cohomologie de $H^1(K, E_{\pi^n})$. On en déduit un homomorphisme de groupe injectif

$$PH(\mathfrak{b}_n) \hookrightarrow PH(B_n) \simeq H^1(K, E_{\pi^n})$$

et l'on identifie $PH(\mathfrak{b}_n)$ et son image. On peut alors vérifier l'inclusion

$$S_n(K) \subset PH(\mathfrak{b}_n).$$

On va s'intéresser dorénavant aux restrictions de ψ_n et ϕ_n au groupe $S_n(K)$. Le principal intérêt de cela est de nous permettre d'utiliser des descriptions de $S_n(K)$ données par B. Perrin-Riou, [P-R].

La multiplication par π induit d'une part un homomorphisme

$$S_{n+1}(K) \to S_n(K),$$

d'autre part, un homomorphisme naturel de $G_{n+1} \to G_n$ et par conséquent, de $A_{n+1} \to A_n$ et par restriction de $\mathfrak{m}_{n+1} \to \mathfrak{m}_n$ et de $\mathfrak{a}_{n+1} \to \mathfrak{a}_n$. On en déduit un diagramme commutatif

$$\begin{array}{ccccc}
S_{n+1}(K) & \xrightarrow{\psi_{n+1}} & cl(\mathfrak{a}_{n+1}) & \xrightarrow{e_{n+1}} & cl(\mathfrak{m}_{n+1}) \\
\downarrow & & \downarrow & & \downarrow \\
S_n(K) & \xrightarrow{\psi_n} & cl(\mathfrak{a}_n) & \xrightarrow{e_n} & cl(\mathfrak{m}_n)
\end{array}$$

Ceci nous permet de considérer les limites projectives

$$\overset{\vee}{S}(K) = \varprojlim S_n(K), \overset{\vee}{cl}(\mathfrak{a}) = \varprojlim cl(\mathfrak{a}_n) \text{ et } \overset{\vee}{cl}(\mathfrak{m}) = \varprojlim cl(\mathfrak{m}_n)$$

et les homomorphismes

$$\psi = \varprojlim \psi_n \text{ et } \phi = \varprojlim \phi_n.$$

Soit v une place de K au-dessus de $\mathfrak{p}^*$, $\tilde{K}_v$ le corps résiduel de K_v et $\tilde{E}_v$ la réduction modulo v de la courbe E/K. On vérifie que nos hypothèses impliquent que $(|\tilde{E}_v(\tilde{K}_v)|, p) = 1$. On en déduit facilement que pour tout entier n le groupe $S_n(K)$ est égal à son sous-groupe $\Sigma_n(K)$ défini comme le noyau de l'homomorphisme

$$S_n(K) \to \prod_{v|\pi^*} (E(K_v)/\pi^n E(K_v)).$$

On pose $\text{Ш}(K)(p) = \bigcup_{n\geq 0} \text{Ш}(K)_{p^n}$ et l'on suppose dorénavant que $\text{Ш}(K)(p)$ est un groupe fini. On en déduit que $T_\pi(\text{Ш}(K)) = \{1\}$ et que par conséquent

$$E(K) \otimes_{O_F} O_{F_\mathfrak{p}} = \overset{\vee}{S}(K).$$

3.3. Résultats à la limite

Nous pouvons maintenant énoncer les principaux théorèmes de [A-T]. Ils décrivent le noyau des homomorphismes

$$\psi : \overset{\vee}{S}(K) \to \overset{\vee}{cl}(\mathfrak{a})$$
$$\phi : \overset{\vee}{S}(K) \to \overset{\vee}{cl}(\mathfrak{m})$$

THÉORÈME 6. *L'homomorphisme ψ est injectif.*

Remarque. Comme nous avons supposé que $K \cap F(E_{p\infty}) = F$ le résultat équivaut aux égalités

$$\left(E(K) \otimes_{O_F} O_{F_\mathfrak{p}}\right)_{torsion} = Ker\ \psi.$$

Soit $\overset{\wedge}{\Delta}$ le groupe $Hom\ (\Delta, \overline{\mathbb{Q}}_p^\times)$. Le groupe Δ opère sur $E(K) \otimes_{O_F} O_{F_\mathfrak{p}}$ et par restriction sur le groupe $Ker \phi$. Soit R l'anneau des entiers d'une extension de $F_\mathfrak{p}$ qui contient toutes les valeurs des éléments de $\overset{\wedge}{\Delta}$.

Pour tout $\chi \in \overset{\wedge}{\Delta}$ on désigne par $(E(K) \otimes_{O_F} R)^\chi$ le sous-module de $E(K) \otimes_{O_F} R$ sur lequel Δ opère via χ et on note

$$r_\chi = rang_R (E(K) \otimes_{O_F} R)^\chi .$$

On introduit également $\{,\}_{K,\mathfrak{p}^*}$ l'accouplement p-adique global

$$E(K) \otimes_{O_F} O_{F_\mathfrak{p}} \times E(K) \otimes_{O_F} O_{F_{\mathfrak{p}^*}} \to \mathbb{Q}_p$$

décrit dans [P-R].

THÉORÈME 7. *On suppose l'accouplement $\{,\}_{K,\mathfrak{p}^*}$ non dégénéré modulo la torsion. Si $r_\chi \geq 1$, alors*

$$rang_R (Ker \phi \otimes_{O_F} R)^\chi = 1.$$

Soit ε le caractère trivial de Δ. On a les inclusions et les égalités immédiates suivantes :

$$(Ker \phi)^\varepsilon = (Ker \phi)^\Delta \subset E(F) \otimes_{O_F} O_{F_\mathfrak{p}} = \overset{\vee}{S}(F) = \overset{\vee}{S}(K)^\Delta.$$

On pose :

$$r = rang_{O_F} E(F) = rang_{\mathbb{Z}_p} \overset{\vee}{S}(F).$$

On obtient grâce au Théorème 7 et aux égalités précédentes :

Si $r = 0$ alors $(Ker \phi)^\Delta = E(F) \otimes_{O_F} O_{F_\mathfrak{p}} = \{1\}$.

Si $r \geq 1$, alors

$$rang_{\mathbb{Z}_p} (Ker \phi)^\Delta = 1.$$

Les paragraphes suivants traitent de la construction explicite de ce sous-module de rang 1 de $Ker\phi$.

4. Constructions de générateurs

Si C est un anneau, on note $C^\times$ son groupe d'unités. Soit n un entier, $n \geq 1$. On considère l'homomorphisme

$$\phi_n : S_n(K) \to cl(\mathfrak{m}_n).$$

On pose :

$$\mathcal{A}_n(K) = Ker\phi_n \text{ et } \mathcal{A}_n(F) = \mathcal{A}_n(K)^\Delta$$

4.1. E.H.P. et Théorie de Kummer

On utilise la théorie de Kummer classique pour donner une description en "terme d'unités" des groupes $\mathcal{A}_n(K)$ et $\mathcal{A}_n(F)$.

On note N le compositum $K_n.K_n^*$ et on pose $q = p^n$. Le corps N contient le groupe μ_q des racines q-ièmes de l'unité. Le choix d'un point primitif de $\mathfrak{p}^{*n}$-division de E, qu'on note g_n^*, permet de définir un caractère

$$\chi : G_n \to \mu_q$$

en posant $\chi(g) = w_n(g, g_n^*)$, où w_n désigne l'accouplement de Weil sur les points de q-division de E.

On utilise les constructions d'algèbres et d'ordres du §2 avec maintenant N pour corps de base. On note

$$B_N = Map(G_n, N),\ A_N = N[G_n].$$

On désigne par $\mathfrak{b}_N$ (resp. $\mathfrak{a}_N$) l'ordre $\mathfrak{b}$ (resp. $\mathfrak{a}$) dans ce cas. On obtient par composition un isomorphisme

$$\varphi_N : PH(B_N) \xrightarrow{\sim} Hom(\Omega_N, G_n) \to Hom(\Omega_N, \mu_q) \xrightarrow{\sim} N^\times/N^{\times q}.$$

Le premier isomorphisme est obtenu par un procédé de descente galoisienne, [B-T], le second est obtenu via le caractère χ et le troisième est l'isomorphisme classique de la théorie de Kummer. On peut donner de φ_N et de l'isomorphisme réciproque φ_N^{-1} les descriptions explicites suivantes.

Soient C/N un e.h.p. pour B_N et c une base de C en tant que A_N-module. On considère la résolvande de c, c'est-à-dire l'élément de $C[G_n]$

$$r_C(c) = \sum_{g \in G_n} c^g g^{-1}.$$

On vérifie que $r_C(c)^q$ appartient à $N[G_n]^\times$ et l'on pose :

$$\varphi_N(C) = \chi(r_C(c)^q) N^{\times q}.$$

L'isomorphisme φ_N^{-1} est défini par :

$$\varphi_N^{-1}(a.N^{\times q}) = \left(N[x] = \frac{N[X]}{(X^q - a)} \right) \text{ avec } x^g = x\chi(g), \forall g.$$

On introduit les homomorphismes de groupes

$$\begin{aligned} i_n : PH(B_n) &\longrightarrow PH(B_N) \\ j_n : K_n^{*\times}/K_n^{*\times q} &\longrightarrow N^\times / N^{\times q} \end{aligned}$$

où i_n est induit par l'extension des scalaires et j_n par l'injection canonique $K_n^{*\times} \hookrightarrow N^\times$. On peut montrer, [A-T], que i_n et j_n sont injectifs et que φ_N induit par restriction à $PH(B_n)$ un homomorphisme injectif φ_K tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} PH(B_n) & \xrightarrow{\varphi_K} & K_n^{*\times}/K_n^{*\times q} \\ \big\downarrow{\scriptstyle i_n} & & \big\downarrow{\scriptstyle j_n} \\ PH(B_N) & \xrightarrow{\varphi_N} & N^\times/N^{\times q} \end{array}$$

On veut décrire l'image par φ_K des groupes $\mathcal{A}_n(K)$ et $\mathcal{A}_n(F)$. Pour cela on introduit quelques notations. Si L/F est une extension finie de F, on pose :

$U_n(L) = \{$ unités de $L_n \otimes_F F_{\mathfrak{p}}$, congrues à 1 modulo les relèvements de $\mathfrak{p}\}$

$\varepsilon_n(L) = \{$ le groupe des unités de $O_{L_n}\}$

$\overline{\varepsilon}_n(L) =$ l'adhérence de la projection de $\varepsilon_n(L)$ dans $U_n(L)$.

On définit de même les groupes $U_n^*(L), \varepsilon_n^*(L)$ et $\overline{\varepsilon}_n^*(L)$ en remplaçant L_n par L_n^* et $\mathfrak{p}$ par $\mathfrak{p}^*$.

Le groupe Ω_F opère sur $E_{\mathfrak{p}^\infty}$ et $E_{\mathfrak{p}^{*\infty}}$. On en déduit des caractères p-adiques de Ω_F

$$\kappa : \Omega_F \longrightarrow Aut(E_{\mathfrak{p}^\infty}) \xrightarrow{\sim} O_{F_{\mathfrak{p}}}^\times \xrightarrow{\sim} \mathbb{Z}_p^\times$$

$$\kappa^* : \Omega_F \longrightarrow Aut(E_{\mathfrak{p}^{*\infty}}) \xrightarrow{\sim} O_{F_{\mathfrak{p}^*}}^\times \xrightarrow{\sim} \mathbb{Z}_p^\times.$$

Par restriction de l'action de Ω_F à $E_{\mathfrak{p}^n}$ et $E_{\mathfrak{p}^{*n}}$ on déduit de κ et κ^* des homomorphismes κ_n et κ_n^* de Ω_F sur $Aut(E_{\mathfrak{p}^n})$ et $Aut(E_{\mathfrak{p}^{*n}})$. On confond dans les notations κ, κ^*, κ_n et κ_n^* et leurs restrictions à Ω_K. On rappelle que l'on a supposé

$$K \cap F(E_{p\infty}) = F.$$

En outre nos hypothèses impliquent que pour toute place v au dessus de $\mathfrak{p}^*, K_{n,v}^*$ ne contient pas de racine p-ième de l'unité.

Théorème 8 [CN-T]. *L'homomorphisme φ_K induit par restriction aux groupes $\mathcal{A}_n(K)$ et $\mathcal{A}_n(F)$ les isomorphismes*

$$(1) \qquad \mathcal{A}_n(K) \xrightarrow{\sim} \left(\frac{\varepsilon_n^*(K) \cap U_n^*(K)^q}{(\varepsilon_n^*(K) \cap U_n^*(K))^q}\right)^{(\kappa_n^*)}$$

$$(2) \qquad \mathcal{A}_n(F) \xrightarrow{\sim} \left(\frac{\varepsilon_n^*(F) \cap U_n^*(F)^q}{(\varepsilon_n^*(F) \cap U_n^*(F))^q}\right)^{(\kappa_n^*)}.$$

On note dorénavant φ_n les isomorphismes du Théorème 8.

Remarque. Puisque la conjecture de Leopoldt est démontrée pour les corps K_n^* et F_n^*, on a des isomorphismes de groupe

$$\tau_n : \frac{\varepsilon_n^*(L) \cap U_n^*(L)^q}{(\varepsilon_n^*(L) \cap U_n^*(L))^q} \xrightarrow{\sim} \frac{\overline{\varepsilon}_n^*(L) \cap U_n^*(L)^q}{(\overline{\varepsilon}_n^*(L))^q}$$

pour $L = F$ et K. On note $\overline{\varphi}_n$ l'isomorphisme $\varphi_n \circ \tau_n$.

4.2. Construction de générateurs dans le cas global

On commence par introduire "l'opérateur norme" ([A-T], §8). Puisque K et $F(E_{p^n})$ sont linéairement disjoints sur F on obtient un isomorphisme de K-algèbre

$$A_n \to \prod_{i=0}^{n} K_i^*$$

$$x \to (y_i)$$

en posant, si $x = \sum_{g \in G_n} x_g g, y_i = \sum_{g \in G_n} x_g w_n(g, p^{n-i} g_n^*), 0 \leq i \leq n$. On identifie ces deux algèbres par cet isomorphisme. Pour tout entier i, $0 \leq i \leq n$, on note $N_{n/i}$ (resp. $T_{n/i}$) la norme (resp. la trace) de K_n^*/K_i^*. On définit maintenant l'opérateur norme comme l'homomorphisme de groupe

$$\sigma : K_n^{*\times} \longrightarrow A_n^\times$$

$$x \longrightarrow (N_{n/i}(x)).$$

Soit C/K une K-algèbre commutative. le groupe Ω_K opère sur $\overline{K} \otimes_K C$ via le facteur de gauche. On note encore $N_{n/i}$ la norme (resp. la trace) de $K_n^* \otimes_K C \longrightarrow K_i^* \otimes_K C$. On en déduit un opérateur norme

$$\sigma_c : (K_n^* \otimes_K C)^\times \longrightarrow (A_n \otimes_K C)^\times.$$

L'utilisation de cet opérateur joue un rôle fondamental dans la démonstration du théorème suivant

THÉORÈME 9 ([CN-T]). *Soit $\mathfrak{c}$ un e.h.p. pour $\mathfrak{b}_n$. On pose $C = \mathfrak{c}K$. On suppose que $\mathfrak{c}$ définit un élément de $\mathcal{A}_n(K)$ et que l'on a :*

$$\varphi_n(\mathfrak{c}) = \alpha(\varepsilon_n^*(K) \cap U_n^*(K))^q \quad \text{où} \quad \alpha \in \varepsilon_n^*(K) \cap U_n^*(K)^q.$$

Alors

1) Il existe un unique élément y de $K_n^* \underset{F}{\otimes} C$ tel que

i) $y^q = \alpha$,

ii) $y^g = y\chi(g), \forall g \in G_n$.

On note $\alpha^{1/q}$ cet élément.

2) Soit $c(\alpha) = \frac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}(N_{n/i}(\alpha^{1/q}))$. L'élément $c(\alpha)$ appartient à C. En outre c'est une base de $\mathfrak{c}\mathfrak{m}_n$ sur $\mathfrak{m}_n$.

5. Formules locales

5.1. Approximation

Comme on va le constater dans le paragraphe suivant, on peut utiliser une construction de Rubin [R] pour obtenir un élément non trivial du groupe

$$\left(\frac{\overline{\varepsilon}_n^*(K) \cap U_n^*(K)^q}{\overline{\varepsilon}_n^*(K)^q}\right)^{(\kappa_n^*)}$$

et par conséquent, via $\overline{\varphi}_n$, un élément $(\mathfrak{c}) \neq (1)$ de $\mathcal{A}_n(K)$. Nous voulons maintenant relier le générateur galoisien de $\mathfrak{c}$ que nous avons construit et l'unité locale de $\overline{\varepsilon}_n^*(K)$ qui permet de le définir.

Soit C un e.h.p. pour B_n, qui définit un élément de $\mathcal{A}_n(K)$. puisque les hypothèses impliquent l'égalité des groupes $\Sigma_n(K)$ et $S_n(K)$ on en déduit que l'algèbre C est totalement décomposée au-dessus de $\mathfrak{p}^*$ et qu'ainsi il existe un isomorphisme d'algèbre

$$C_{\mathfrak{p}^*} \xrightarrow{\sim} B_{n,\mathfrak{p}^*}$$

Cet isomorphisme est unique puisque $Aut_{K_{\mathfrak{p}^*}}(B_{n,\mathfrak{p}^*})$ s'identifie avec les $K_{\mathfrak{p}^*}$-points de G_n. En le composant avec l'isomorphisme d'augmentation de $B_{n,\mathfrak{p}^*}$ on obtient un homomorphisme de $K_{\mathfrak{p}^*}$-algèbre

$$\rho_{\mathfrak{p}^*} = C_{\mathfrak{p}^*} \longrightarrow K_{\mathfrak{p}^*}$$

et plus généralement de $K^*_{n,\mathfrak{p}^*}$-algèbre

$$K^*_{n,\mathfrak{p}^*} \otimes_{K_{\mathfrak{p}^*}} C_{\mathfrak{p}^*} \longrightarrow K^*_{n,\mathfrak{p}^*}.$$

Puisque Ω_K opère sur $K_{*_{n,\mathfrak{p}^*}} \otimes_{K_{\mathfrak{p}^*}} C_{\mathfrak{p}^*}$ via le membre de gauche, $\rho_{\mathfrak{p}^*}$ commute avec l'action de Ω_K.

On conserve les notations du Théorème 9. Soit $\beta \in U_n^*(K)$ tel que $\alpha = \beta^q$. On obtient

$$\rho_{\mathfrak{p}^*}(c(\alpha)) = \frac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}(N_{n/i}(\rho_{\mathfrak{p}^*}(\alpha^{1/q})))$$

Dans $K^*_{n,\mathfrak{p}^*}$ on a l'égalité

$$\rho_{\mathfrak{p}^*}(\alpha^{1/q})^q = \rho_{\mathfrak{p}^*}(\beta)^q = \beta^q$$

Puisque $K^*_{n,\mathfrak{p}^*}$ ne contient pas de racine de l'unité d'ordre p, on en déduit que $\rho_{\mathfrak{p}^*}(\alpha^{1/q}) = \beta$. On obtient ainsi à partir du Théorème 9, la formule suivante :

$$\rho_{\mathfrak{p}^*}(c(\alpha)) = \frac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}(N_{n/i}(\beta)).$$

Supposons maintenant que

$$\overline{\varphi}_n(\mathfrak{c}) = \alpha' \overline{\varepsilon}^*_n(K)^q \text{ avec } \alpha' = \gamma^q, \gamma \in U^*_n(K)$$

On déduit de la définition même de φ_n et $\overline{\varphi}_n$ l'existence de $u \in \overline{\varepsilon}^*_n(K)$ tel que l'on ait

$$\alpha = \alpha' u^q$$

d'où l'égalité

$$\alpha = \beta^q = (\gamma u)^q$$

On utilise une nouvelle fois que $K^*_{n,\mathfrak{p}^*}$ ne contient pas de racine de l'unité pour en déduire que $\beta = \gamma u$. Puisque u est limite d'une suite de $\varepsilon^*_n(K) \cap U^*_n(K)$, pour tout entier $m, m \geq 1$, il existe $u_m \in \varepsilon^*_n(K) \cap U^*_n(K)$ et une unité locale $v_m, v_m \equiv 1 \mod p^{m+n}$, telle que

$$\beta u_m = \gamma v_m.$$

On pose $\alpha_m = (\beta u_m)^q$. C'est un nouveau représentant de $\overline{\varphi}_n(\mathfrak{c})$. On vérifie la congruence

$$\rho_{\mathfrak{p}^*}(c(\alpha_m)) \equiv \frac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}(N_{n/i}(\gamma)) \mod p^m.$$

On obtient ainsi la formule locale suivante :

Théorème 10 ([CN-T]). *Les notations sont celles du Théorème 9. On suppose que*

$$\overline{\varphi}(\mathfrak{c}) = \alpha' \overline{\varepsilon}^*_n(K)^q \text{ avec } \alpha' = \gamma^g, \gamma \in U^*_n(K)$$

Alors pour tout entier $m, m \geq 1$, il existe une base c_m de $\mathfrak{c}\mathfrak{m}_n$ sur $\mathfrak{m}_n$ telle que l'on ait

$$\rho_{\mathfrak{p}^*}(c_m) \equiv \frac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}(N_{n/i}(\gamma)) \mod p^m.$$

5.2. Mesures p-adiques

On se propose d'une part d'indiquer comment construire des éléments non triviaux du groupe $\mathcal{A}_n(K)$ et d'autre part d'interpréter en termes de mesures la somme $\sum_{i=0}^{n} T_{i/0}(N_{n/i}(\gamma))$.

On conserve les notations introduites en (3-1). On pose

$$X_\infty^* = Gal(F_\infty^*/F)$$

et l'on introduit les groupes

$$U_\infty^*(F) = \varprojlim U_n^*(F), \overline{\varepsilon}_\infty^*(F) = \varprojlim \overline{\varepsilon}_n^*(F)$$

et le module de Tate $T_{\pi *} = \varprojlim E_{\mathfrak{p}^{*n}}$. Les homomorphismes de transition sont respectivement induits par la norme et la multiplication par π^*. Tout élément x d'une limite projective $\varprojlim A_n$ est noté $x = ([x_n])$. On vérifie le lemme suivant :

Lemme 11. *Soient h un élément non trivial du groupe*

$$Hom(T_{\pi^*}, U_\infty^*(F)/\overline{\varepsilon}_\infty^*(F))^{X_\infty^*}$$

et $w^* = ([w_n^*])$ un générateur de T_π^*. On pose

$$h(w^*) = \gamma \overline{\varepsilon}_\infty^*(F) \text{ où } \gamma = ([\gamma_n]) \in U_\infty^*(F).$$

Alors il existe un entier n_0 tel que pour tout entier $n, n \geq n_0, \gamma_n^{p^n} \overline{\varepsilon}_n^*(F)^{p^n}$ définit via $\overline{\varphi}_n$ un élément non trivial de $\mathcal{A}_n(F)$.

Soit $\hat{E}$ (resp. G_m) le groupe formel défini sur $O_{F_{\mathfrak{p}^*}}$ associé au noyau de la réduction $\mod \mathfrak{p}^*$ de la courbe (resp. le groupe formel multiplicatif). Il s'agit de groupes formels de Lubin-Tate définis par des séries de Frobenius associées à des uniformisantes distinctes de $F_{\mathfrak{p}^*}$. Soit L le complété de l'extension abélienne maximale non ramifié de $F_{\mathfrak{p}^*}$. On sait qu'il existe un isomorphisme η défini sur O_L

$$\eta : G_m \to \hat{E}$$

qui commute avec l'action de $O_{F_{\mathfrak{p}^*}}$, ([L], VIII).

Soit $\gamma = ([\gamma_n])$ un élément de $U_\infty^*(K)$ et soit $v = ([v_n])$ un générateur du module de Tate associé à G_m. On vérifie que $w^* = ([w_n^*])$, où $w_n^* = \pi^n(\eta(v_n))$, est un générateur du module de Tate T_{π^*}. On sait par la théorie de Coleman qu'il existe une unique série formelle $g_\gamma(X) \in O_{F_{\mathfrak{p}^*}}[[X]]$ telle que

$$g_\gamma(w_n^*) = \gamma_n, \ \forall n \geq 1.$$

On note $\hat{g}_\gamma$ la série formelle de $O_L[[X]]$, définie par $g_\gamma \circ \eta$. On sait qu'à une telle série est associée une mesure p-adique sur $\mathbb{Z}_p$ à valeurs dans O_L qu'on note $\hat{\mu}_\gamma$.

Théorème 12. *Pour tout entier $n, n \geq 1$, on a l'égalité*

$$\frac{1}{p^n}\sum_{i=0}^{n} T_{i/0}(N_{n/i}(\gamma_n)) = \hat{\mu}_\gamma(p^n\mathbb{Z}_p) + \frac{1}{p^n}(1 - g_\gamma(0)).$$

Remarque. Le groupe X_∞^* se décompose en un produit direct de groupe $U \times V$ où $U \simeq \mathbb{Z}_p$ et $V \simeq Gal(F(E_{\mathfrak{p}^*})/F)$. Soit χ^* la restriction de κ^* à V. Si M est un $\mathbb{Z}_p[X_\infty^*]$-module, considéré comme $\mathbb{Z}_p[V]$-module, il se décompose en une somme directe

$$M = \bigoplus_{k=1}^{p-1} M^{(k)}$$

où $M^{(k)}$ désigne le sous-module de M sur lequel V opère via χ^{*k}. Si $\gamma \in M$ on désigne par $\gamma^{(k)}$ sa composante dans $M^{(k)}$. Avec les notations du lemme 11, l'élément γ de $U_\infty^*(F)$ satisfait pour tout v de V la congruence $\gamma^v \equiv \gamma^{\chi^*(v)} \mod \overline{\varepsilon}_\infty^*(F)$. On en déduit que $\gamma \equiv \gamma^{(1)} \mod \overline{\varepsilon}_\infty^*(F)$, or on peut montrer que pour un tel élément $g_{\gamma^{(1)}}(0) = 1$. On peut donc toujours se ramener à ce cas.

Avec les notations précédentes et en en supposant $g_\gamma(0) = 1$, on énonce le corollaire suivant :

Corollaire 12. *S'il existe un élément h non trivial de*

$$Hom(T_{\pi^*}, U_\infty^*(F)/\overline{\varepsilon}_\infty^*(F))^{X_\infty^*},$$

alors il existe un entier n_0 tel que pour tout entier $n \geq n_0$ il existe un e.h.p. $\mathfrak{c}_n$ qui satisfait les propriétés suivantes :

1) $\mathfrak{c}_n$ n'est pas isomorphe à $\mathfrak{b}_n$ comme $\mathfrak{a}_n$-module mais $\mathfrak{c}_n\mathfrak{m}_n$ est libre sur $\mathfrak{m}_n$.

2) Pour tout entier $m, m \geq 1$, il existe une base c_m de $\mathfrak{c}_n\mathfrak{m}_n$ sur $\mathfrak{m}_n$ telle que

$$\rho_{\mathfrak{p}^*}(c_m) \equiv \pi^n \hat{\mu}_\gamma(p^n\mathbb{Z}_p) \mod p^m.$$

6. Une construction de Rubin, [R]

On indique dans ce dernier paragraphe comment construire une fonction qui satisfait les hypothèses du lemme 11.

6.1. La fonction f_r

Pour tout entier $n, n \geq 1$, on note $C_n^*(F)$ le groupe des unités elliptiques de F_n^* et $\overline{C}_n^*(F)$ l'adhérence de la projection de $C_n^*(F)$ dans $U_n^*(F)$. On pose

$$\overline{C}_\infty^*(F) = \varprojlim \overline{C}_n^*(F).$$

Soit f le conducteur du Grössencharacter attaché à la courbe E/F. Le groupe Ω_F opère sur l'ensemble E_f' des points primitifs de f-division de E. A chaque orbite B de E_f'/Ω_F et à chaque générateur w^* de T_{π^*}, Rubin [R], §3, associe $\theta_B(w^*) = ([\theta_B(w_n^*)])$ de $\overline{C}_\infty^*(F)$. On choisit une fois pour toutes l'une des 2 orbites de E_f'/Ω_F et par raison de simplicité on écrit $\theta(w^*)$ pour $\theta_B(w^*)$.

Soit $\mathbb{Z}_p[[X_\infty^*]] = \varprojlim \mathbb{Z}_p[X_n^*]$. Le caractère κ^* induit un homomorphisme de $\mathbb{Z}_p$-algèbre

$$\kappa^* : \mathbb{Z}_p[[X_\infty^*]] \longrightarrow \mathbb{Z}_p.$$

On pose $J^* = Ker\kappa^*$. Pour tout entier $r, r \geq 1, , J^{*r}/J^{*r+1}$ est un $\mathbb{Z}_p$-module libre de rang 1. On définit un générateur de J^{*r}/J^{*r+1} suivant la méthode donnée dans [R] §6. C'est l'image dans J^{*r}/J^{*r+1} d'un élément v_r^* de J^{*r} dont on donne la construction. On peut montrer que $U_\infty^*(F) \otimes \mathbb{Q}$ n'a pas de v_r^*-torsion et qu'ainsi dans $U_\infty^*(F) \otimes \mathbb{Q}$ l'équation $x^{v_r^*} = \gamma$ a au plus une solution.

THÉORÈME 13. *([R], Théorème 4-2 et Proposition 4-4)*

1) Soit r un entier, $r \geq 1$, tel que

$$(*) \qquad \overline{C}_\infty^*(F) \subset J^{*r-1}\overline{\varepsilon}_\infty^*(F) \text{ et } \overline{C}_\infty^*(F) \subset J^{*r}(U_\infty^*(F) \otimes \mathbb{Q})$$

Alors il existe un unique homomorphisme

$$\xi_r \in Hom\,(T_{\pi^*}, U^*_\infty(F) \otimes \mathbb{Q} \;/\; \overline{\varepsilon}^*_\infty(F))^{X^*_\infty}$$

qui satisfait pour tout générateur w^* de T_{π^*}

$$\xi_r(w^*) = (\theta(w^*))^{1/\nu^*_r}\overline{\varepsilon}^*_\infty(F).$$

2) On suppose $E(F)$ infini et $\{,\}_{F,\mathfrak{p}^*}$ non dégénéré. Soit r le rang sur $\mathbb{Z}_p$ de $\overset{\vee}{S}(F)$. Alors la relation (*) est satisfaite et l'élément ξ_r est non trivial.

On déduit des travaux de [P-R] un homomorphisme injectif.

$$\Phi : Hom(T_{\pi^*}, U^*_\infty(F) \otimes \mathbb{Q}/\overline{\varepsilon}^*_\infty(F))^{X^*_\infty} \hookrightarrow \overset{\vee}{S}(F)$$

et l'on montre pour le choix de r du Théorème 13, 2), que $x_r = \Phi(\xi_r) \neq 1$.

Si l'on est sous les hypothèses du Théorème 13, 2), il existe un entier $m, m \geq 1$, tel que

$$\xi_r^{p^m} \in Hom(T_{\pi^*}, U^*_\infty(F)/\overline{\varepsilon}^*_\infty(F))^{X^*_\infty}$$

Puisque $\overset{\vee}{S}(F)$ est dans $\mathbb{Z}_p$-torsion, on en déduit que $x_r^{p^m} \neq 1$ et donc que $\xi_r^{p^n}$ n'est pas trivial.

Soit N le plus petit entier, $N \geq 1$, tel que $\xi_r^{p^N}$ ait la propriété précédente. On obtient ainsi

Corollaire 14. *Sous les hypothèses du Théorème 13, 2), il existe un homomorphisme non trivial*

$$f_r \in Hom(T_{\pi^*}, U^*_\infty(F)/\overline{\varepsilon}^*_\infty(F))^{X^*_\infty}$$

qui satisfait pour tout générateur w^* de T_{π^*}

$$f_r(w^*) = (\theta(w^*))^{p^N/\nu^*_r}).\overline{\varepsilon}^*_\infty(F).$$

On peut donc appliquer à cette fonction les constructions des paragraphes précédents. Ainsi pour n assez grand, les unités elliptiques permettent la construction d'un élément non trivial de $PH(\mathfrak{b}_n)$, "libre sur l'ordre maximal" de A_n et d'en déterminer une base.

6.2. La fonction L-$\mathfrak{p}$-adique

Les notations et définitions sont celles de Rubin, [R], §7. Soit R le complété de l'anneau des entiers de $F_\infty^* \otimes F_{\mathfrak{p}}$. On pose $\Lambda^*(R) = R[[X_\infty^*]]$. Si l'on fixe un choix w^* de générateur de T_{π^*} on définit la fonction $\mathfrak{L} - \mathfrak{p}$-adique de Katz-Manin et Vishik comme un élément de $R[[Gal(F_\infty F_\infty^*/F]]$. Par restriction à F_∞^* on obtient ainsi un élément $\mathfrak{L}_{\mathfrak{p}}$ de $\Lambda^*(R)$. Pour tout entier $n, n \geq 1$, on définit

$$V_n(F) = \{ \text{ unités de } F_n^* \otimes F_{\mathfrak{p}}, \text{ congrues à 1 au-dessus de } \mathfrak{p}\}$$

Soit $V_\infty(F) = \varprojlim V_n(F)$.

Puisque la conjecture de Leopoldt est vrai pour F_n^* on a pour tout entier $n, n \geq 1$, un isomorphisme

$$\varepsilon_n^*(F) \otimes \mathbb{Z}_p \simeq \overline{\varepsilon}_n^*(F).$$

En outre, on a un isomorphisme naturel

$$\varepsilon_n^*(F) \otimes \mathbb{Z}_p \hookrightarrow V_n(F)$$

On en déduit un plongement de $\overline{\varepsilon}_n^*(F) \hookrightarrow V_n(F))$ et par passage à la limite un plongement

$$j^* : \overline{\varepsilon}_\infty^*(F) \hookrightarrow V_\infty(F).$$

On note $N(f)$ la norme absolue du conducteur f du Grössencharacter attaché à E/F.

Théorème 15 ([R], Théorème 7.2). *Il existe un homomorphisme injectif*

$$i^* : V_\infty(F) \hookrightarrow \Lambda^*(R)$$

tel que $i^* \circ j^*(\theta(-N(f)w^*) = \mathfrak{L}_{\mathfrak{p}}$.

Remarque. Puisque $(f, p) = 1$ la multiplication par $-N(f)$ est un automorphisme de T_{π^*}.

On pose $k^* = i^* \circ j^*$. On définit $ord_\kappa(\mathfrak{L}_{\mathfrak{p}})$ comme l'ordre du zéro en $s = 0$, d'une fonction analytique sur $\mathbb{Z}_p$ associée à $\mathfrak{L}_{\mathfrak{p}}$, (voir [R], §7).

On peut conclure notre étude de la manière suivante :

COROLLAIRE 16. *Les propriétés suivantes sont équivalentes*

i) $(Ker\phi)^{\Delta} \neq \{1\}$

ii) $ord_{\kappa}(\mathfrak{L}_{\mathfrak{p}}) \geq 1$

En outre lorsque $r = ord_{\kappa}(\mathfrak{L}_{\mathfrak{p}})$ *est supérieur à 1, il existe un entier* n_0 *et, pour tout entier* $n, n \geq n_0$*, un e.h.p.* $\mathfrak{c}_n$ *pour* $\mathfrak{b}_n$ *satisfaisant les propriétés suivantes :*

1) $\mathfrak{c}_n$ *n'est pas isomorphe à* $\mathfrak{b}_n$ *comme* $\mathfrak{a}_n$*-module mais* $\mathfrak{c}_n\mathfrak{m}_n$ *est libre sur* $\mathfrak{m}_n$.

2)Pour tout entier $m, m \geq 1$*,il existe une bases de* c_m *de* $\mathfrak{c}_n\mathfrak{m}_n$ *sur* $\mathfrak{m}_n$ *telle que*

$$\rho_{\mathfrak{p}^*}(c_m) \equiv \pi^n \overset{\wedge}{\mu}_{\gamma(1)}(p^n\mathbb{Z}_p) \mod p^m$$

où $\gamma = k^{*-1}(\mathfrak{L}_{\mathfrak{p}})^{p^N/\nu_r^*)}$ *et* N *un entier précisé dans le §6.*

Il est clair que dans cette situation, le comportement de la fonction $L_{\mathfrak{p}}$ domine le problème de structure galoisienne.

REFERENCES

[A-T] S. A. Agboola et M.J. Taylor, *Class invariants of Mordell-Weil groups*, à paraître.

[B-T] S. N. Byott et M.J. Taylor, *Hopf structure and Galois modules, Group rings and class groups*, DMV seminar **18** (1992), Birkhaüser.

[CN-S] Ph. Cassou-Noguès et A. Srivastav, *Galois module structure of Kummer 2-extensions and elliptic curves of rank* ≥ 1, à paraître.

[CN-T] Ph. Cassou-Noguès et M.J. Taylor, *Espaces homogènes principaux, unités elliptiques et fonctions L*, Ann. Inst. **44** (1994), 631–661.

[F1] A. Fröhlich, *Invariants for modules over commutative separable orders*, Quart J. Math. Oxford 2 **16** (1965), 193–232.

[F2] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Invent. Math. **17** (1972), 143–166.

[Le] H.W. Leopoldt, *Uber die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew Math. **201** (1959), 119–149.

[F2] S. Lang, *Cyclotomic fields*, Graduate texts in Mathematics **59**, Springer-Verlag.

[M] J. Milne, *Etale cohomology*, Princeton Univ. Press, New Jersey (1980).

[PR] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mémoire de la S.M.F. **17** (1984).

[R] K. Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Invent. Math. **107** (1992), 323–350.

[Se-T] J.P. Serre et J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **68** (1968), 492–517.

[S-T] A. Srivastav et M.J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. **99** (1990), 165–184.

[SW] M.E. Sweedler, *Hopf algebras*, W.A. Benjamin, New York (1969).

[T1] M.J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41–79.

[T2] M.J. Taylor, *Galois module structure of rings of integers in Kummer extensions*, Bull. L.M.S. **12** (1980), 96–98.

[W] W.C. Waterhouse, *Principal homogeneous spaces and Group scheme extensions*, Trans. A.M.S. **153** (1971), 181–189.

Philippe Cassou-Nogues
UFR de Mathématiques et Informatique
Université Bordeaux I
33405 TALENCE CEDEX
FRANCE

Martin J. Taylor
U.M.I.S.T.
Department of Mathematics
P.O. Box 88 MANCHESTER
M.60 1QD ENGLAND