ANNALES DE L'INSTITUT FOURIER

PHILIPPE CASSOU-NOGUÈS
MARTIN J. TAYLOR

Espaces homogènes principaux, unités elliptiques et fonctions *L*

Annales de l'institut Fourier, tome 44, n° 3 (1994), p. 631-661
<http://www.numdam.org/item?id=AIF_1994__44_3_631_0>

Ann. Inst. Fourier, Grenoble
44, 3 (1994), 631–661

ESPACES HOMOGÈNES PRINCIPAUX, UNITÉS ELLIPTIQUES ET FONCTIONS L

par Ph. CASSOU-NOGUÈS (*) **et M.J. TAYLOR**

1. Introduction.

Dans cet article si C/F est une algèbre commutative sur un corps de nombres ou un corps local, nous notons O_C son anneau d'entiers. Si R est un anneau nous désignons par $R^\times$ le groupe multiplicatif de ses éléments inversibles.

Soit N/F une extension galoisienne et finie de corps de nombres de groupe de Galois G. L'anneau des entiers O_N possède une structure naturelle de module sur l'algèbre de groupe $O_F[G]$. Beaucoup de questions se posent alors dans cette situation : O_N est-il libre sur $O_F[G]$ ou sur un ordre convenable de l'algèbre $F[G]$? O_N, après extension des scalaires, est-il libre sur un ordre maximal de $F[G]$? Ces questions anciennes, étudiées notamment par Hilbert, puis par Leopoldt, sont devenues plus récemment, grâce aux travaux de Fröhlich, le centre d'actives recherches. Lorsque $F = Q$, un des résultats les plus intéressants de ce sujet est le lien mystérieux, deviné par Fröhlich et démontré par le deuxième auteur, entre ces problèmes de structure et le comportement des fonctions L-d'Artin associées aux caractères de G, [T1].

(*) La plus grande partie de ce travail s'est effectuée alors que le premier auteur bénéficiait d'une bourse du S.E.R.C. à UMIST.
Mots-clés : Espaces homogènes principaux – Ordres de Hopf – Courbes elliptiques – Fonctions L.
Classification A.M.S. : 11G16 – 11G40 – 11R33 – 11R65.

Beaucoup de travaux ont montré la difficulté à obtenir, dans le cas relatif, où $F \neq \mathbb{Q}$, une théorie générale. On sait grâce à E. Noether que la ramification de l'extension N/F joue un rôle fondamental dans la structure de O_N. On cherche donc à étudier des familles d'extensions N/F à ramification donnée. On souhaite aussi traiter des situations qui imposent le choix d'un ordre naturel de $F[G]$ sur lequel étudier nos modules. Ces considérations ont conduit le second auteur à introduire l'étude de la structure galoisienne des espaces homogènes principaux, e.h.p., comme modules sur les ordres de Hopf. De nombreux résultats ont déjà été obtenus dans ce cadre [ST], [AT].

Nous étudions ici une situation relative dont le cadre est défini par la géométrie. Plus précisément, les ordres de Hopf qui interviennent sont ceux qui définissent les schémas en groupe affines associés à des sous-groupes des points de torsion du groupe de Mordell-Weil d'une courbe elliptique E/F à multiplication complexe qui possède partout bonne réduction. Les résultats de cet article complètent ceux de [AT]. Nous montrons notamment en utilisant les travaux de Rubin [R], comment la fonction L-$\mathfrak{p}$-adique de Katz, Manin et Vishik, lorsqu'elle possède un zéro en $s = 0$, permet la construction explicite de classes de e.h.p. non triviaux, libres, après extension des scalaires, sur l'ordre maximal. L'existence de telles classes était démontrée dans [AT]. Nous utilisons cette fonction L et les unités elliptiques qui permettent de la définir pour construire une base de nos espaces sur l'ordre maximal. Encore une fois nous sommes dans une situation où le comportement d'une fonction L domine le problème de structure galoisienne.

Le plan de cet article est le suivant. Les notations et les principaux résultats sont rassemblés dans le paragraphe 2. Nous énonçons les théorèmes 1, 2 et 3. Puis nous utilisons ces théorèmes et les méthodes de Rubin pour démontrer le théorème 4. Les paragraphes 3, 4 et 5 sont respectivement consacrés aux démonstrations des théorèmes 1, 2 et 3.

2. Notations et résultats.

On considère une courbe elliptique E définie sur un corps quadratique imaginaire K, à multiplication complexe par O_K. Soit F une extension finie et abélienne de K, de groupe de Galois Δ telle que E/F possède partout bonne réduction.

On fixe un nombre premier p, $p \geq 5$, qui ne divise pas l'ordre de Δ et tel que $pO_K = \mathfrak{p} \cdot \mathfrak{p}^*$ où $\mathfrak{p}$ et $\mathfrak{p}^*$ sont des idéaux premiers distincts de K. On suppose en outre :

1) E/K a bonne réduction en $\mathfrak{p}$ et $\mathfrak{p}^*$.

2) p (resp. $\mathfrak{p}^*$) est non ramifié (resp. totalement décomposé) dans F.

Puisque le nombre de classes de K est égal à 1, les idéaux $\mathfrak{p}$ et $\mathfrak{p}^*$ sont principaux. On choisit π(resp. π^*) appartenant à O_K tel que $\mathfrak{p} = \pi O_K$ (resp. $\mathfrak{p}^* = \pi^* O_K$) et $p = \pi\pi^*$.

Suivant la terminologie de [CW] on suppose dorénavant que $\mathfrak{p}$ est anormal, c'est-à-dire que $\pi + \bar{\pi} = 1$ ou de manière équivalente que la trace de l'endomorphisme de Frobenius de E modulo $\mathfrak{p}$ est égale à 1.

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

$$L_n = L\big(E_{\mathfrak{p}^n}\big) \ \big(\text{resp. } L_n^* = L\big(E_{\mathfrak{p}^{*n}}\big)\big) \tag{2.1}$$
$$L_\infty = L\big(E_{\mathfrak{p}^\infty}\big) \ \big(\text{resp. } L_\infty^* = L\big(E_{\mathfrak{p}^{*\infty}}\big)\big)$$

et l'on pose :

$U_n(L) = \{$unités de $L_n \underset{K}{\otimes} K_{\mathfrak{p}}$, congrues à 1 modulo les idéaux premiers au-dessus de $\mathfrak{p}\}$

$$\begin{aligned} \mathcal{E}_n(L) &= \text{ le groupe des unités de } O_{L_n} \\ \mathcal{E}'_n(L) &= \mathcal{E}_n(L) \cap U_n(L) \\ \overline{\mathcal{E}}_n(L) &= \text{ l'adhérence de la projection de } \mathcal{E}_n(L) \text{ dans } U_n(L) \\ U_\infty(L) &= \varprojlim U_n(L), \quad \overline{\mathcal{E}}_\infty(L) = \varprojlim \overline{\mathcal{E}}_n(L) \end{aligned} \tag{2.2}$$

où les homomorphismes de transition sont donnés par la norme. On définit les groupes $U_n^*(L)$, $U_\infty^*(L)$, $\mathcal{E}_n^*(L)$, $\mathcal{E}_n^{*\prime}(L)$, et $\overline{\mathcal{E}}_n^*(L)$ en remplaçant L_n par L_n^* et $\mathfrak{p}$ par $\mathfrak{p}^*$.

Soit X_n (resp. X_n^*) le groupe $\mathrm{Gal}(F_n/F)$ (resp. $\mathrm{Gal}(F_n^*/F)$). Puisque p est non ramifié dans F on a les égalités

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

On obtient, par restriction, des isomorphismes qui permettent d'identifier les groupes

$$\begin{aligned} X_n &\xrightarrow{\sim} \mathrm{Gal}(K_n/K) \\ X_n^* &\xrightarrow{\sim} \mathrm{Gal}(K_n^*/K). \end{aligned} \tag{2.3}$$

On fixe une clôture algébrique F^c de F. Si L est une extension de K contenue dans F^c on note $\Omega_L = \mathrm{Gal}(F^c/L)$. Le groupe Ω_K opère sur $E_{\mathfrak{p}^\infty}$ et $E_{\mathfrak{p}^{*\infty}}$. On en déduit des caractères p-adiques naturels

$$\kappa : \Omega_K \longrightarrow \mathrm{Aut}\left(E_{\mathfrak{p}^\infty}\right) \xrightarrow{\sim} O_{K_\mathfrak{p}}^\times \xrightarrow{\sim} \mathbb{Z}_p^\times \tag{2.4}$$

$$\kappa^* : \Omega_K \longrightarrow \mathrm{Aut}\left(E_{\mathfrak{p}^{*\infty}}\right) \xrightarrow{\sim} O_{K_{\mathfrak{p}^*}}^\times \xrightarrow{\sim} \mathbb{Z}_p^\times.$$

Par restriction de l'action de Ω_K aux groupes $E_{\mathfrak{p}^n}$ et $E_{\mathfrak{p}^{*n}}$, κ et κ^* induisent respectivement des homomorphismes de Ω_K sur $(\mathbb{Z}/p^n\mathbb{Z})^\times$ et par passage au quotient des isomorphismes κ_n et κ_n^* de X_n et X_n^* sur $(\mathbb{Z}/p^n\mathbb{Z})^\times$. On confond dans nos notations $\kappa, \kappa^*, \kappa_n$ et κ_n^* et leurs restrictions à Ω_F.

Nous introduisons maintenant le groupe d'espaces homogènes principaux naturellement associés à cette situation. On peut se reporter à [BT], [CNT] Journées arithmétiques 1993 (à paraître J. de Théorie des Nombres de Bordeaux) ou [AT].

On note G_n (resp. G_n^*) le groupe $E_{\mathfrak{p}^n}$ (resp. $E_{\mathfrak{p}^{*n}}$) et l'on considère l'algèbre de groupe $F^c[G_n]$. Le groupe Ω_F opère à la fois sur G_n et sur F^c. On note A_n la F-algèbre des points fixes $(F^c[G_n])^{\Omega_F}$. Le groupe Ω_F opère également sur la F-algèbre des applications de G_n dans F^c. On désigne par B_n la sous-algèbre des éléments fixes par Ω_F. Il s'agit là de F-algèbres de Hopf, duales par la dualité de Cartier :

$$\begin{aligned} &A_n \times B_n \longrightarrow F \\ &a = \sum_{g \in G_n} a_g g, f \longrightarrow (a,f) = \sum_{g \in G_n} a_g f(g). \end{aligned} \tag{2.5}$$

Soit $\mathcal{E}/\mathrm{Spec}(O_F)$ le modèle de Néron de E/F. On sait, grâce à la propriété universelle de ce modèle, que la multiplication par π^n induit un endomorphisme. $\tilde{\pi}^n : \mathcal{E} \to \mathcal{E}$. On pose $\mathfrak{S}_n = \mathrm{Ker}(\tilde{\pi}^n)$. Puisque E/F a partout bonne réduction $\mathfrak{S}_n/\mathrm{Spec}(O_F)$ est un schéma en groupe affine, fini et plat, dont la fibre générique peut être identifiée à $\mathrm{Spec}(B_n)$. Il existe donc un unique ordre de Hopf $\mathfrak{B}_n$ de B_n tel que $\mathfrak{S}_n = \mathrm{Spec}(\mathfrak{B}_n)$. On associe à $\mathfrak{B}_n$ son O_F-dual

$$\mathcal{A}_n = \left\{a \in A_n | (a,f) \in O_F,\ \forall f \in \mathfrak{B}_n\right\}. \tag{2.6}$$

On obtient ainsi un ordre de Hopf de A_n. En remplaçant G_n par G_n^* on définit les F-algèbres A_n^* et B_n^* et les O_F-ordres $\mathcal{A}_n^*$ et $\mathfrak{B}_n^*$.

Une A_n-algèbre C est une F-algèbre commutative sur laquelle A_n agit à droite et qui satisfait

$$(xy)a = \sum_i (xa_{1i})(ya_{2i}) \quad \forall x, y \in C,\ \forall a \in A_n \tag{2.7}$$

où, si Δ_n désigne la comultiplication de A_n, on a

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

DÉFINITION 2.8. — *Un espace homogène principal pour B_n, e.h.p., est une A_n-algèbre telle qu'il existe une extension finie L/F et un isomorphisme*

$$\xi : C \underset{F}{\otimes} L \xrightarrow{\sim} B_n \underset{F}{\otimes} L$$

de $A_n \otimes L$ algèbre.

Remarque. — Lorsque les points de $\mathfrak{p}^n$-division sont rationnels sur F, l'algèbre A_n est l'algèbre de groupe $F[G_n]$ et la notion de e.h.p. coïncide alors avec celle de G_n-algèbre galoisienne.

DÉFINITION 2.9. — *Un espace homogène principal pour $\mathfrak{B}_n$ est un ordre $\mathcal{O}$ dans un e.h.p. (C/F) pour B_n, stable par l'action de $\mathcal{A}_n$ et tel que ξ induise par restriction*

$$\xi : \mathcal{O} \underset{O_F}{\otimes} O_L \xrightarrow{\sim} \mathfrak{B}_n \underset{O_F}{\otimes} O_L$$

un isomorphisme de O_L-algèbre qui respecte l'action de $\mathcal{A}_n$.

L'ensemble $PH(B_n)$ des classes d'isomorphisme d'e.h.p. pour B_n peut être muni d'une structure de groupe commutatif. Les méthodes de descente galoisienne permettent d'établir un isomorphisme

$$PH(B_n) \xrightarrow{\sim} H^1(F, G_n).$$

L'application $\mathcal{O} \to \mathcal{O}F$ induit un homomorphisme injectif $PH(\mathfrak{B}_n) \to PH(B_n)$. Ainsi, via l'isomorphisme précédent, on peut considérer $PH(\mathfrak{B}_n)$ comme un sous-groupe de $H^1(F, G_n)$. On montre, [BT], que tout e.h.p. pour $\mathfrak{B}_n$ est localement libre sur $\mathcal{A}_n$. Ceci nous permet d'associer à un tel espace sa classe dans le groupe des classes $C\ell(\mathcal{A}_n)$. On construit ainsi un homomorphisme de groupe

$$\begin{aligned} \Psi_n : PH(\mathfrak{B}_n) &\longrightarrow C\ell(\mathcal{A}_n) \\ (\mathfrak{C}) &\longrightarrow [\mathfrak{C}] - [\mathcal{A}_n]. \end{aligned} \tag{2.10}$$

Si $\mathfrak{M}_n$ désigne l'ordre maximal de A_n, en composant Ψ_n avec l'extension des scalaires, on définit

$$\varphi_n : PH(\mathfrak{B}_n) \longrightarrow C\ell(\mathfrak{M}_n). \tag{2.11}$$

On appelle invariant de Picard de $\mathfrak{C}$ dans $C\ell(\mathcal{A}_n)$ (resp. $C\ell(\mathfrak{M}_n)$) l'élément $[\mathfrak{C}] - [\mathcal{A}_n]$ (resp. $[\mathfrak{C}\mathfrak{M}_n] - [\mathfrak{M}_n]$). Par abus de language on dit qu'un e.h.p. $\mathfrak{C}$ pour $\mathfrak{B}_n$ est libre sur $\mathfrak{M}_n$ lorsque $\mathfrak{C}\mathfrak{M}_n$ est libre sur $\mathfrak{M}_n$ et l'on appelle base de $\mathfrak{C}$ sur $\mathfrak{M}_n$ toute base de $\mathfrak{C}\mathfrak{M}_n$ sur $\mathfrak{M}_n$.

Si L/K est une extension de corps, on définit le groupe de Tate-Schafarevitch $Ш(L)$ de E/L comme le noyau de l'homomorphisme naturel

$$H^1(L,E) \longrightarrow \prod_v H^1(L_v,E) \tag{2.12}$$

où v parcourt l'ensemble des places finies de L.

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

$$H^1(L,G_n) \longrightarrow \prod_v H^1(L_v,E). \tag{2.13}$$

On a une suite exacte

$$\{0\} \longrightarrow \frac{E(L)}{\pi^n E(L)} \longrightarrow S_n(L) \longrightarrow Ш(L)_{\pi^n} \longrightarrow \{0\} \tag{2.14}$$

où $Ш(L)_{\pi^n}$ désigne le sous-groupe des éléments de $Ш(L)$ annulés par π^n.

Remarque. — Si la définition de $S_n(L)$ est intrinsèque, l'application de $\dfrac{E(L)}{\pi^n E(L)} \to S_n(L)$ dépend du choix de π.

On peut montrer que $S_n(F)$ est un sous-groupe de $PH(\mathfrak{B}_n)$. On s'intéresse aux invariants de Picard des éléments de $S_n(F)$.

DÉFINITION 2.15. — *On définit*

$$\mathcal{D}_n(F) = S_n(F) \cap \operatorname{Ker} \varphi_n$$
$$\mathcal{D}_n(K) = S_n(F)^{\Delta} \cap \operatorname{Ker} \varphi_n.$$

Si M est un $(\mathbb{Z}/p^n\mathbb{Z})[X_n^*]$-module et θ un caractère de $X_n^* \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ on pose $M^{(\theta)}$ le sous-module de M sur lequel X_n^* opère via θ.

Notre premier résultat est de donner une description en terme d'unités des groupes $\mathcal{D}_n(F)$ et $\mathcal{D}_n(K)$. On pose $q = p^n$. Si M est un $\mathbb{Z}_p$-module on pose

$$M_q = \{m \in M \text{ tels que } qm = 0\}.$$

THÉORÈME 1. — *Pour tout entier n, $n \geq 1$, il existe des isomorphismes de groupes*

1) $\Phi_{n,K} : \mathcal{D}_n(F) \simeq ((\mathcal{E}_n^{*\prime}(F) \cap U_n^*(F)^q)/\mathcal{E}_n^{*\prime}(F)^q)^{(\kappa_n^*)}$

2) $\Phi_{n,K} : \mathcal{D}_n(K) \simeq ((\mathcal{E}_n^{*\prime}(K) \cap U_n^*(K)^q)/\mathcal{E}_n^{*\prime}(K)^q)^{(\kappa_n^*)}$.

Remarques (2.16). — 1. Puisque la conjecture de Leopoldt est démontrée pour les corps K_n^* et F_n^*, on a des isomorphismes de groupes :

$$c_n : (\mathcal{E}_n^{*\prime}(L) \cap U_n^*(L)^q)/\mathcal{E}_n^{*\prime}(L)^q) \simeq (\overline{\mathcal{E}}_n^{*\prime}(L) \cap U_n^*(L)^q)/\overline{\mathcal{E}}_n^*(L)^q)$$

pour $L = K$ ou F. Par raison de simplicité on note Φ_n les homomorphismes $\Phi_{n,K}$ et $\Phi_{n,F}$ et $\overline{\Phi}_n$ les homomorphismes $\Phi_n \circ c_n$.

2. Nos hypothèses impliquent que $L_n^* \underset{K}{\otimes} K_{\mathfrak{p}^*}$ ne contient pas de racine p-ième de l'unité si $L = K$ ou F. On en déduit que $x \to x^q$ induit un isomorphisme de groupe

$$\big(U_n^*(L)/\overline{\mathcal{E}}_n^*(L)\big)_q^{(\kappa_n^*)} \simeq \big((\overline{\mathcal{E}}_n^*(L) \cap U_n^*(L))^q)/\overline{\mathcal{E}}_n^*(L)^q)^{(\kappa_n^*)}.$$

Comme on le voit dans la démonstration de ce théorème, §3, la définition de Φ_n dépend du choix d'un point primitif de $\mathfrak{p}^{*n}$ division.

Si $M = \varprojlim M_n$, notons $m = [m_n]$ avec $m_n \in M_n$ tout élément de M. On considère le module de Tate $T_{\pi^*} = \varprojlim E_{\mathfrak{p}^{*n}}$ où les homomorphismes de transition sont donnés par la multiplication par π^*. C'est un $\mathbb{Z}_p$-module libre de rang 1 dont nous fixons une base $g^* = [g_n^*]$. Les applications Φ_n sont pour tout entier n associées à ce choix de g_n^*. On désigne par χ_n le caractère de G_n

$$\begin{aligned} \chi_n : G_n &\longrightarrow \mu_q \\ g &\longrightarrow w_n(g, g_n^*) \end{aligned} \tag{2.17}$$

où w_n désigne l'accouplement de Weil sur les points de q division de E.

Pour tout entier i, $0 \leq i \leq n$, on note $N_{n/i}$ (resp. $T_{n/i}$) la norme (resp. la trace) de F_n^* sur F_i^*. Plus généralement pour toute algèbre commutative C/F on note encore $N_{n/i}$ (resp. $T_{n/i}$) les applications induites par la norme (resp. la trace) de $F_n^* \underset{F}{\otimes} C \to F_i^* \underset{F}{\otimes} C$. Le théorème 2 fournit une méthode de construction d'une base sur l'ordre maximal d'un e.h.p. dont on connaît l'image par Φ_n.

THÉORÈME 2. — *Soit $\mathfrak{C}$ un e.h.p. pour $\mathfrak{B}_n$ dont la classe appartient à $\mathcal{D}_n(F)$. On suppose que l'on a :*

$$\Phi_n(\mathfrak{C}) = \alpha_n \mathcal{E}_n^{*\prime}(F)^q \quad \textit{avec} \quad \alpha_n \in \mathcal{E}_n^{*\prime}(F) \cap U_n^*(F)^q.$$

Alors

1) *Si* $C = \mathfrak{C}F$, *il existe un unique élément* y *de* $C \underset{F}{\otimes} F_n^*$ *tel que*

$$y^q = \alpha_n \quad \text{et} \quad y^g = y\chi_n(g), \quad \forall g \in G_n.$$

On note $\alpha_n^{1/q}$ *cet élément.*

2) *L'élément de* C, $c(\alpha_n) = \dfrac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}\big(N_{n/i}(\alpha_n^{1/q})$ *est une base de* $\mathfrak{C}\mathfrak{M}_n$ *sur* $\mathfrak{M}_n$.

Soit X_∞ (resp. X_∞^*) le groupe de Galois

$$\mathrm{Gal}(K_\infty/K) \quad (\text{resp. } \mathrm{Gal}(K_\infty^*/K)).$$

On considère le groupe

$$\mathrm{Hom}(T_{\pi^*}, U_\infty^*(K)/\overline{\mathcal{E}}^*{}_\infty(K))^{X_\infty^*}.$$

Les travaux de B. Perrin-Riou montrent que ce groupe est isomorphe à un sous-groupe de $\check{S}(K) = \varprojlim S_n(K)$, [R] Proposition 2.4. Il n'est donc pas surprenant que le théorème 1 nous permette, pour tout entier n, $n \geq 1$, d'associer à tout élément f de ce groupe une classe $(\mathfrak{C}_n(f))$ de $\mathcal{D}_n(K)$. Plus précisément si $f(g^*) = \gamma\overline{\mathcal{E}}^*{}_\infty(K)$, où $\gamma = [\gamma_n]$, on définit $(\mathfrak{C}_n(f))$ par

$$\overline{\Phi}_n(\mathfrak{C}_n(f)) = \gamma_n^{p^n}\, \overline{\mathcal{E}}^*{}_n(F)^{p^n}.$$

Nos hypothèses impliquent que tout e.h.p. pour B_n est totalement décomposé (c'est-à-dire est localement trivial) au-dessus de $\mathfrak{p}^*$. On pose $C_n(f) = \mathfrak{C}_n(f)F$ et $C_n(f)_{\mathfrak{p}^*}$ (resp. $B_{n,\mathfrak{p}^*}$) l'algèbre $C_n(f) \underset{F}{\otimes} F_{\mathfrak{p}^*}$ (resp. $B_n \underset{F}{\otimes} F_{\mathfrak{p}^*}$). Il existe donc un isomorphisme d'algèbre :

$$C_n(f)_{\mathfrak{p}^*} \xrightarrow{\sim} B_{n,\mathfrak{p}^*}.$$

Cet isomorphisme est unique puisque $\mathrm{Aut}_{F_{\mathfrak{p}^*}}(B_{n,\mathfrak{p}^*})$ s'identifie au groupe des $F_{\mathfrak{p}^*}$ points de G_n, ici réduit à $\{1\}$. En composant l'isomorphisme précédent avec l'homomorphisme d'augmentation de $B_{n,\mathfrak{p}^*}$ on obtient un homomorphisme de $F_{\mathfrak{p}^*}$-algèbre

$$\rho_{\mathfrak{p}^*} : C_n(f)_{\mathfrak{p}^*} \longrightarrow F_{\mathfrak{p}^*}. \tag{2.18}$$

Soit $\widehat{E}$ (resp. G_m) le groupe formel de Lubin-Tate défini sur $O_{K_{\mathfrak{p}^*}}$ associé à la réduction modulo $\mathfrak{p}^*$ de la courbe E/K (resp. le groupe formel multiplicatif). Si L désigne le complété de l'extension abélienne maximale non ramifiée de $K_{\mathfrak{p}^*}$, on sait qu'il existe un isomorphisme de groupe formel η, défini sur O_L, de G_m sur $\widehat{E}$, [L] VIII. La théorie développée par Coleman,

[C], affirme l'existence pour tout élément $\gamma = [\gamma_n]$ de $U_\infty^*(K)$ d'une unique série formelle h_γ de $O_{K_{\mathfrak{p}^*}}[[X]]$ telle que

$$h_\gamma(g_n^*) = \gamma_n\,, \quad \forall n \geq 1.$$

On note $\hat{h}_\gamma$ la série formelle $h_\gamma \circ \eta$ de $O_L[[X]]$ et $\hat{\mu}_\gamma$ la mesure de $\mathbb{Z}_p$ à valeurs dans O_L qui lui est associée lorsque l'on choisit 1 pour générateur topologique de $\mathbb{Z}_p$.

Le groupe X_∞^* se décompose en un produit direct d'un sous-groupe isomorphe à $\mathbb{Z}_p$ et d'un sous-groupe canoniquement isomorphe à X_1^*. On peut voir les valeurs de κ_1^* comme appartenant à $\mathbb{Z}_p$. Si A est un $\mathbb{Z}_p[X_\infty^*]$-module, considéré par restriction des scalaires comme un $\mathbb{Z}_p[X_1^*]$-module, il se décompose en somme directe.

$$A = \bigoplus_{k=1}^{p-1} A^{(k)} \tag{2.19}$$

où $A^{(k)}$ est le sous-module de A sur lequel X_1^* opère via κ_1^{*k}.

THÉORÈME 3. — *On suppose qu'il existe un élément non trivial*

$$f \in \mathrm{Hom}(T_{\pi^*}, U_\infty^*(K)/\overline{\mathcal{E}}^*_\infty(K))^{X_\infty^*}$$

tel que $f(g^*) = \gamma\overline{\mathcal{E}}^*_\infty(K)$ *où* $\gamma \in U_\infty^{*(1)}(K)$. *Alors*

1) *Il existe un entier* n_0 *tel que pour tout entier* n, $n \geq n_0$, $\mathfrak{C}_n(f)$ *n'est pas isomorphe à* $\mathfrak{B}_n$, *mais* $\mathfrak{C}_n(f)$ *est libre sur* $\mathfrak{M}_n$.

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

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

Nous terminons ce paragraphe en montrant comment, via les travaux de Rubin, [R], la fonction L-$\mathfrak{p}$-adique nous permet de construire grâce au théorème 3 des e.h.p. pour $\mathfrak{B}_n$, non triviaux, libres sur l'ordre maximal de A_n.

Nous adoptons dorénavant les notations de [R], notamment celles des paragraphes 5 et 6. Si n est un entier, $n \geq 1$, on note $\mathcal{C}_n^*(K)$ le groupe des unités elliptiques de K_n^*, [R], §3, et l'on pose

$$\overline{\mathcal{C}}^*_n(K) = \text{ l'adhérence de la projection de } \mathcal{C}_n^*(K) \text{ dans } U_n^*(K)$$
$$\overline{\mathcal{C}}^*_\infty(K) = \varprojlim \overline{\mathcal{C}}^*_n(K)$$

où les homomorphismes de transition sont définis par la norme.

Soit R le complété de l'anneau des entiers de $K_\infty^* \underset{K}{\otimes} K_\mathfrak{p}$, $\mathfrak{X}_\infty = \mathrm{Gal}(K_\infty K_\infty^*/K)$. On désigne par $\mathfrak{L}_\mathfrak{p}$ la fonction L-$\mathfrak{p}$-adique à 2 variables de Katz, Manin et Vishik. C'est la fonction L-p-adique de module $f\mathfrak{p}^{*\infty}$ considérée dans [dS], II, 4.16, où f est le conducteur du caractère de Hecke associé à E/K. On sait que $\mathfrak{L}_\mathfrak{p}$ est une mesure de $\mathfrak{X}_\infty$ à valeurs dans R. On note $R[[\mathfrak{X}_\infty]]$ la R-algèbre de ces mesures. La définition de $\mathfrak{L}_\mathfrak{p}$ sous-entend un certain nombre de choix précisés dans [R], §6, et notamment celui d'un générateur W^* de T_{π^*}. Le générateur g^* de T_{π^*} considéré dans le théorème 3 est choisi tel que

$$g^* = -N(f)W^*.$$

Nous commençons par traiter le cas où $n = 1$. Le lecteur peut se reporter à [T3] pour des résultats plus complets dans ce cas.

En considérant κ_1^* comme un caractère de $\mathfrak{X}_\infty$ à valeurs dans $\mathbb{Z}_p$ on définit $\mathfrak{L}_\mathfrak{p}(\kappa_1^{*^{-1}})$. On note $h_{K_1^*,1}$ l'ordre de la composante $A^{(1)}$ du p-sous-groupe de Sylow A du groupe des classes de K_1^*. On note $\mathfrak{F}$ le groupe formel de Lubin-Tate de paramètre π^*, défini sur $O_{K_{\mathfrak{p}^*}}$, qui possède $\pi^* X + X^p$ pour endomorphisme.

Si x et y sont des entiers p-adiques on note $x \sim y$ lorsque xy^{-1} est une unité p-adique.

COROLLAIRE. — *On a les propriétés suivantes :*

1) $\mathcal{D}_1(K)$ *est d'ordre 1 ou* p

2) $\mathcal{D}_1(K) = \{1\}$ *si et seulement si* $\mathfrak{L}_\mathfrak{p}(\kappa_1^{*^{-1}})h_{K_1^*,1}^{-1}$ *est une unité* p-*adique.*

3) *On suppose* $\mathfrak{L}_\mathfrak{p}(\kappa_1^{*^{-1}})h_{K_1^*,1}^{-1} \sim p^m$ *avec* $m \geq 1$, *alors* $\mathcal{D}_1(K)$ *est engendré par* $\alpha^{p^{m-1}\theta_1}\overline{\mathcal{E}}_1^*(K)$ *où* α *est un point primitif de* π^* *division de* $\mathfrak{F}$ *et* $\theta_1 = -\sum_{\sigma \in X_1^*} \kappa_1^{*^{-1}}(\sigma)\sigma$.

Puisque X_1^* est d'ordre premier à p on sait que $(U_1^*(K)/\overline{\mathcal{E}}_1^*(K))^{(1)}$ est isomorphe au quotient de groupes

$$(U_1^*(K)^{(1)}/\overline{\mathcal{C}}_1^*(K)^{(1)})/(\overline{\mathcal{E}}_1^*(K)^{(1)}/\overline{\mathcal{C}}_1^*(K)^{(1)}).$$

Le lemme 9 de [CW] affirme que le groupe $(U_1^*(K)^{(1)}/(U_1^*(K)^{(1)})^p$ est d'ordre p. On en déduit que $(U_1^*(K)^{(1)}/\overline{\mathcal{C}}_1^*(K)^{(1)})$, qui est un p-groupe abélien est cyclique. En outre par [T3], (14) on a l'équivalence :

$$\left(U_1^*(K)^{(1)} : \overline{\mathcal{C}}_1^*(K)^{(1)}\right) \sim \mathfrak{L}_\mathfrak{p}\left(\kappa_1^{*^{-1}}\right).$$

On sait par un résultat de Kolyvagin que $(\overline{\mathcal{E}}^*_1(K)^{(1)} : \overline{\mathcal{C}}^*_1(K)^{(1)})$ est équivalent à $h_{K^*_1,1}$. Puisque grâce au théorème 1 on a l'isomorphisme $\mathcal{D}_1(K) \simeq (U^*_1(K)^{(1)}/\overline{\mathcal{E}}^*_1(K)^{(1)p})$, on déduit 1) et 2) des équivalences précédentes. Posons $\alpha' = \alpha^{\theta_1}$. On sait par [CW] lemma 9 que α' définit un générateur de $(U^*_1(K)^{(1)}/U^*_1(K)^{(1)p})$. Puisque $K^*_{1,\mathfrak{p}^*}$ ne contient pas de racine p-ième de l'unité on en déduit que α' définit un générateur de $U^*_1(K)^{(1)}/(U^*_1(K)^{(1)})^{p^m}$ et donc de $U^*_1(K)^{(1)}/\overline{\mathcal{E}}^*_1(K)^{(1)}$ qui en est un quotient. On conclut que $\alpha'^{p^{m-1}}\overline{\mathcal{E}}^*_1(K)$ est un générateur de $\mathcal{D}_1(K)$ identifié avec son image par $\overline{\Phi}_1$.

□

Remarque. — Si $\mathfrak{L}_{\mathfrak{p}}(\kappa_1^{*^{-1}}) \sim 1$ alors $U^*_1(K)^{(1)}/\overline{\mathcal{E}}^*_1(K)^{(1)} = \{1\}$. On sait qu'alors $(U^*_n(K)/(\overline{\mathcal{E}}^*_n(K))^{(1)} = \{1\}$ pour tout entier n, [CW], Corollary 32, et que par conséquent $\mathcal{D}_n(K) = \{1\}$.

Nous revenons maintenant à la construction d'e.h.p. à partir de $\mathfrak{L}_{\mathfrak{p}}$.

On considère le plongement

$$i^* : \overline{\mathcal{C}}^*_\infty(K) \hookrightarrow R[[X^*_\infty]] \tag{2.20}$$

décrit dans [R], Théorème 7.2.

Nous montrons maintenant comment associer à tout ε de $\overline{\mathcal{C}}^*_\infty(K)$ un élément du groupe $\mathrm{Hom}(T_{\pi^*}, (U^*_n(K)\otimes\mathbb{Q})/\overline{\mathcal{E}}^*_n(K))^{X^*_\infty}$.

Le caractère p-adique κ^* induit un homomorphisme d'algèbre

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

On pose $J^* = \ker\kappa^*$. On fixe un générateur θ de J^* sur $\mathbb{Z}_p[[X^*_\infty]]$ en posant $\theta = x\kappa^*(x^{-1}) - 1$, où x est un générateur topologique de X^*_∞ qu'on peut choisir tel que $\log_p \kappa^*(x) = p$.

Soit r un entier, tel que

$$\overline{\mathcal{C}}^*_\infty(K) \subset J^{*^{r-1}}\overline{\mathcal{E}}^*_n(K) \quad \text{et} \quad \overline{\mathcal{C}}^*_\infty(K) \subset J^{*^r}(U^*_n(K)\otimes\mathbb{Q}). \tag{2.21}$$

Puisque $U^*_n(K)$ n'a pas de θ^r-torsion, [dS], III, (1.3), l'élément $\theta^{-r}\varepsilon$ est bien défini dans $U^*_n(K)\otimes\mathbb{Q}$. On pose

$$f^{(r)}_\varepsilon(g^*) = (\theta^{-r}\varepsilon)\overline{\mathcal{E}}^*_\infty(K) \tag{2.22}$$

et l'on prolonge $f^{(r)}_\varepsilon$ par $\mathbb{Z}_p$ linéarité à T_{π^*}. On a construit ainsi $f^{(r)}_\varepsilon$ appartenant à $\mathrm{Hom}(T_{\pi^*}, (U^*_\infty(K)\otimes\mathbb{Q})/\overline{\mathcal{E}}^*_\infty(K))^{X^*_\infty}$.

On déduit de (2.20) et de (2.22) une application $\lambda \to \tilde{\lambda}_r$ de $\mathrm{Im}\ i^*$ dans $\mathrm{Hom}(T_{\pi^*}, (U^*_\infty(K)\otimes\mathbb{Q})/\overline{\mathcal{E}}^*_\infty(K))^{X^*_\infty}$ en posant

$$\tilde{\lambda}_r = f^{(r)}_{i^{*^{-1}}(\lambda)}. \tag{2.23}$$

La restriction de $\mathfrak{L}_\mathfrak{p}$ à K_∞^* définit un élément de $R[[X_\infty^*]]$. Le théorème 7.2 (i) de [R] affirme que $\mathfrak{L}_{\mathfrak{p}|_{K_\infty^*}}$ appartient à Im i^*. Ainsi, en suivant la construction précédemment décrite, pour tout entier r satisfaisant (2.21), on construit à partir de $\mathfrak{L}_\mathfrak{p}$ un élément de

$$\mathrm{Hom}(T_{\pi^*}, (U_\infty^*(K) \otimes \mathbb{Q})/\overline{\mathcal{E}}^*_\infty(K))^{X_\infty^*}$$

qu'on note $\tilde{\mathfrak{L}}_{\mathfrak{p},r}$.

On désigne par $\langle\ ,\ \rangle_\mathfrak{p}$ l'accouplement défini par la hauteur $\mathfrak{p}$-adique et décrit dans [PR1]

$$\langle\ ,\ \rangle_\mathfrak{p} : \check{S}(K) \times \check{S}^*(K) \longrightarrow \mathbb{Q}_p$$

où $\check{S}(K) = \varprojlim S_n(K)$ (resp. $\check{S}^*(K) = \varprojlim S_n^*(K)$). Enfin, nous notons $\mathrm{ord}_\kappa(\mathfrak{L}_\mathfrak{p})$ l'ordre du zéro en $s = 0$ de la fonction analytique de la variable s associée à $\mathfrak{L}_\mathfrak{p}$ et au caractère p-adique κ, [R], §7. Avec les notations du théorème 3 on obtient :

THÉORÈME 4. — *On suppose le groupe* $Ш(K)_p$ *fini, l'accouplement* $\langle\ ,\ \rangle_\mathfrak{p}$ *non dégénéré et l'entier* $r = \mathrm{ord}_K(\mathfrak{L}_\mathfrak{p}) \geq 1$. *Alors*

1) *Il existe des entiers* N *et* $n_0 = n_0(N)$ *tels que pour tout entier* $n \geq n_0$, $\mathfrak{C}_n\left(\tilde{\mathfrak{L}}_{\mathfrak{p},r}^{p^N}\right)$ *est un e.h.p. pour* $\mathfrak{B}_n$, *non isomorphe à* $\mathfrak{B}_n$, *libre sur* $\mathfrak{M}_n$.

2) *On pose* $\tilde{\mathfrak{L}}_{\mathfrak{p},r}^{p^N}(g^*) = \gamma\overline{\mathcal{E}}^*_\infty(K))$ *où* $\gamma \in U_\infty^{*(1)}(K)$. *Pour tout entier* m *il existe une base* c_m *de* $\mathfrak{C}_n\left(\tilde{\mathfrak{L}}_{\mathfrak{p},r}^{p^N}\right)$ *sur* $\mathfrak{M}_n$ *telle que :*

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

Sous les hypothèses considérées, Rubin démontre [R], Proposition 4.4, que $\tilde{\mathfrak{L}}_{\mathfrak{p},r}$ est un élément non trivial de $\mathrm{Hom}(T_{\pi^*}, (U_\infty^*(K)\otimes\mathbb{Q})/\overline{\mathcal{E}}^*_\infty(K))^{X_\infty^*}$. Il existe donc un entier p^N tel que

$$\tilde{\mathfrak{L}}_{\mathfrak{p},r}^{p^N} \in \mathrm{Hom}\left(T_{\pi^*}, U_\infty^*(K)/\overline{\mathcal{E}}^*_\infty(K)\right)^{X_\infty^*}.$$

Puisque le groupe $\mathrm{Hom}\left(T_{\pi^*}, (U_\infty^*(K) \otimes \mathbb{Q})/\overline{\mathcal{E}}^*_\infty(K)\right)^{X_\infty^*}$ se plonge dans le groupe $\check{S}(K)$ qui ne contient pas d'élément d'ordre fini, on en déduit que $\tilde{\mathfrak{L}}_{\mathfrak{p},r}^{p^N}$ est non trivial. On achève la démonstration du théorème en appliquant à la fonction $f = \tilde{\mathfrak{L}}_{\mathfrak{p},r}^{p^N}$ les résultats du théorème 3. □

Remarque. — On note que l'image de $\tilde{\mathfrak{L}}_{\mathfrak{p},r}$ dans $\check{S}(K)$ est l'élément noté $x_\mathfrak{p}^{(r)}$ par Rubin [R]. Il est remarquable de constater qu'alors que le rang

r de $\check{S}(K)$ est quelconque, l'élément $x_{\mathfrak{p}}^{(r)}$ de $\check{S}(K)$ construit à partir de $\mathfrak{L}_{\mathfrak{p}}$ définit, précisément à une puissance de p près, un élément de $\varprojlim \mathcal{D}_n(K)$. On remarque également que les bases de nos e.h.p. sont construites à partir d'unités elliptiques.

3. Description des groupes $\mathcal{D}_n(F)$ et $\mathcal{D}_n(K)$.

On suppose l'entier n, $n \geq 1$, fixé dans ce paragraphe.

On considère les algèbres et les ordres de Hopf $A_n, B_n, A_n^*, B_n^*, \mathcal{A}_n, \mathfrak{B}_n$ introduits dans le §2. On désigne par $\mathfrak{M}_n$ (resp. $\mathfrak{M}_n^*$) l'ordre maximal de A_n (resp. B_n^*). On s'intéresse à l'homomorphisme

$$\varphi_n : PH(\mathfrak{B}_n) \longrightarrow C\ell(\mathfrak{M}_n). \tag{3.1}$$

On rappelle la description de Fröhlich, [F], du groupe $C\ell(\mathfrak{M}_n)$ ainsi que celle de φ_n.

Si A/F est une F-algèbre commutative et $\mathcal{U}$ un ordre de A on note $J(A)$ le groupe des idèles finies de A et $U(\mathcal{U})$ le groupe des idèles unités de $\mathcal{U}$. Si l'on pose

$$\widetilde{\mathcal{U}} = \prod_v \mathcal{U}_v$$

où v parcourt l'ensemble des places finies de F, $U(\mathcal{U})$ est le groupe des unités de $\widetilde{\mathcal{U}}$. On a un isomorphisme de groupe

$$C\ell(\mathfrak{M}_n) \simeq J(A_n)/(U(\mathfrak{M}_n)A_n^{\times}). \tag{3.2}$$

Soit $\mathfrak{C}$ un e.h.p. pour $\mathfrak{B}_n$. On pose $C = \mathfrak{C}F$ (resp. $\widetilde{\mathfrak{C}} = \mathfrak{C} \underset{o_F}{\otimes} \widetilde{\mathcal{A}}_n$). Puisque C (resp. $\widetilde{\mathfrak{C}}$) est libre sur A_n (resp. $\widetilde{\mathcal{A}}_n$) il existe $c \in C$ (resp. $\tilde{c} \in \widetilde{\mathfrak{C}}$) tel que

$$C = cA_n\ , \quad \widetilde{\mathfrak{C}} = \tilde{c}\widetilde{\mathcal{A}}_n. \tag{3.3}$$

On en déduit l'existence d'un élément λ de $J(A_n)$ tel que $c = \tilde{c} \cdot \lambda$. L'application φ_n est définie par

$$\varphi_n(\widetilde{\mathfrak{C}}) = \lambda U(\mathfrak{M}_n)A_n^{\times}. \tag{3.4}$$

Puisque les points de π^n division de E/F ne sont pas rationnels sur F, G_n n'est pas contenu dans A_n et de ce fait l'algèbre C, stable par A_n, ne l'est par G_n. Néanmoins si l'on étend les scalaires à F_n, $C \underset{F}{\otimes} F_n/F_n$

devient une G_n-algèbre galoisienne. Notons exponentiellement l'action de X_n sur G_n et considérons le groupe V_n produit semi-direct

$$V_n = G_n \ltimes X_n \tag{3.5}$$

où $x^{-1}gx = g^x$, $\forall x \in X_n$, $g \in G_n$.

L'algèbre $C \underset{F}{\otimes} F_n$ devient une V_n-algèbre galoisienne sur F. Plus généralement on définit l'action de V_n sur $(C \underset{F}{\otimes} F_n)[G_n]$ par la relation

$$\Big(\sum_{g\in G_n} a_g g\Big)^\sigma = \sum_{g\in G_n} a_g^\sigma g^x \quad \text{si } \sigma = h.x \tag{3.6}$$

où h (resp. x) appartient à G_n (resp. X_n). L'algèbre A_n est alors l'algèbre des éléments invariants par V_n, *i.e.*

$$A_n = \big((C \underset{F}{\otimes} F_n)\big)[G_n]\big)^{V_n}. \tag{3.7}$$

Si B/F est une F-algèbre commutative, on prolonge l'action de V_n à $(C \underset{F}{\otimes} F_n) \otimes B$ en posant

$$(a \otimes b)^\sigma = a^\sigma \otimes b\,, \quad \forall a \in C \underset{F}{\otimes} F_n\,,\ b \in B.$$

On considère notamment le cas où $B = F_v$ où v est une place finie de F et $B = \mathrm{Ad}(F)$ l'anneau des adèles de F.

On rappelle maintenant la notion de résolvande.

Soit C/F un e.h.p. pour B_n. On définit l'application résolvande introduite dans [T4]

$$r_C : C \longrightarrow (C \otimes F_n)[G_n]$$

par $r_C(c) = \sum_{g\in G_n} c^g g^{-1}$. Si B/F est une algèbre commutative, on prolonge naturellement r_c en une application de $C \otimes B$ dans $(C \otimes F_n \otimes B)[G_n]$. On déduit immédiatement de la définition que r_C est un homomorphisme de $A_n \otimes B$ module.

Lorsque C est fixé, on note r la résolvante r_C.

On associe à c et $\tilde{c}$ considérés en (3.3) des éléments $r(c)$ et $r(\tilde{c})$ de $(C \otimes \mathrm{Ad}(F_n))[G_n]$. On déduit de la relation $c = \tilde{c}\lambda$ l'égalité $r(c) = r(\tilde{c})\lambda$ dans cette algèbre. Par un résultat standard de théorie de Galois, on sait que $r(\tilde{c}) \in (C \otimes \mathrm{Ad}(F_n))[G_n]^\times$. On en déduit que

$$r(c)r(\tilde{c})^{-1} = \lambda. \tag{3.8}$$

On considère l'homomorphisme d'algèbre

$$F^c[G_n] \longrightarrow \mathrm{Map}(G_n^*, F^c)$$

$$x \longrightarrow \hat{x} \tag{3.9}$$

Si $x = \sum_g x_g g$ on vérifie que l'application qui, à x, associe $\hat{x}$ définie par

$$\hat{x}(g^*) = \sum_g x_g w_n(g, g^*), \quad \forall g^* \in G_n^*$$

induit un isomorphisme de F-algèbre de A_n sur B_n^* et par conséquent des isomorphismes de groupes

$$A_n^\times \simeq B_n^{*\times} = \mathrm{Map}\left(G_n^*, F_n^{*\times}\right)^{X_n^*}$$

$$\begin{aligned} U(\mathfrak{M}_n) \simeq U(\mathfrak{M}_n^*) &= \mathrm{Map}\left(G_n^*, U(O_{F_n^*})\right)^{X_n^*} \\ J(A_n) \simeq J(B_n^*) &= \mathrm{Map}\left(G_n^*, J(F_n^*)\right)^{X_n^*}. \end{aligned} \tag{3.10}$$

L'homomorphisme de groupe

$$J(F_n^*) \longrightarrow J(F_n^*)/\left(U\left(O_{F_n^*}\right)F_n^{*\times}\right)$$

induit un homomorphisme

$$J(B_n^*)/U(\mathfrak{M}_n^*)B_n^{*\times} \longrightarrow \mathrm{Map}\left(G_n^*, J(F_n^*)/\left(U\left(O_{F_n^*}\right)F_n^{*\times}\right)\right)^{X_n^*}. \tag{3.11}$$

On déduit de (3.2), de (3.10) et de (3.11) un homomorphisme

$$\lambda_n : C\ell(\mathfrak{M}_n) \longrightarrow \mathrm{Map}\left(G_n^*, J(F_n^*)/\left(U\left(O_{F_n^*}\right)F_n^{*\times}\right)\right)^{X_n^*}. \tag{3.12}$$

On pose $\theta_n = \lambda_n \circ \varphi_n$. On sait par (3.4), (3.6) et (3.7) que

$$\theta_n(\mathfrak{C}) = f \tag{3.13}$$

où $f(g^*)$ est représenté dans $J(F_n^*)$ par $\hat{r}(c)(g^*)\hat{r}(\tilde{c})^{-1}(g^*)$.

THÉORÈME 3.14.

1) *θ_n induit un homomorphisme de groupe de $PH(\mathfrak{B}_n)$ dans*

$$\mathrm{Hom}\left(G_n^*, J(F_n^*)/\left(U\left(O_{F_n^*}\right)F_n^{*\times}\right)\right)^{X_n^*}.$$

2) $\mathrm{Ker}\,\theta_n = \mathrm{Ker}\,\varphi_n$.

Soient B/F une algèbre commutative, $x = \sum_{g \in G_n} x_g g$ un élément de $B[G_n]$ et m un élément de $\mathbb{Z}$, on pose

$$[m]x = \sum_{g \in G_n} x_g g^m.$$

On note $c' = c\pi^{-n}$ et $\tilde{c}' = \tilde{c}\pi^{-n}$ et l'on considère l'élément $r(c')r(\tilde{c}')^{-1} = r(c)r(\tilde{c})^{-1}$ de $J(A_n)$. Soit $m \in \mathbb{Z}$. On pose

$$a_m = \big([m]r(c')\big)r(c')^{-m}, \quad b_m = \big([m]r(\tilde{c}')\big)r(\tilde{c}')^{-m}.$$

Par définition a_m (resp. b_m) appartient à $(C \otimes F_n)[G_n]^\times$ (resp. $(C \otimes \mathrm{Ad}(F_n))[G_n]^\times$). On sait en outre par [AT], Lemma 4.6, que b_m est une unité de l'ordre maximal de $(C \otimes \mathrm{Ad}(F_n))[G_n]$. En utilisant le lemme 4.25 de [AT] on montre que a_m (resp. b_m) est invariant par l'action de V_n. Grâce à (3.7), on en déduit que a_m (resp. b_m) appartient à $A_n^\times$ (resp. $U(\mathfrak{M}_n)$). Ainsi, pour tout $m \in \mathbb{Z}$

$$[m](r(c)r(\tilde{c})^{-1}) \equiv (r(c)r(\tilde{c})^{-1})^m \bmod A_n^\times U(\mathfrak{M}_n) \tag{3.15}$$

et par conséquent $(\hat{r}(c)\hat{r}(\tilde{c})^{-1})(g^{*^m}) \equiv (\hat{r}(c)\hat{r}(\tilde{c})^{-1}(g^*))^m \bmod U\big(O_{F_n^*}\big)F_n^{*\times}$, ce qui démontre 1).

Pour démontrer 2), il suffit de démontrer que $\ker\theta_n$ est contenu dans $\ker\varphi_n$. Soit $(\mathfrak{C})$ un élément de $\ker\theta_n$. On sait que $\varphi_n(\mathfrak{C})$ est représenté dans $J(B_n^*)$ par $f = \hat{r}(c')\hat{r}(\tilde{c}')^{-1}$. On veut montrer l'existence de u (resp. v) appartenant à $B_n^{*\times}$ (resp. $U(\mathfrak{M}_n^*)$) tel que $f = u.v$. On remarque qu'il suffit de définir u et v pour un élément de chaque orbite de G_n^*/X_n^*. Puisque $K_n^* \cap F = K$ on peut choisir $\{g_0^*, g_1^*, \ldots, g_n^*\}$ avec $g_i^* = p^{n-i}g_n^*$ et g_n^* primitif de $\mathfrak{p}^{*^n}$-division comme système de représentants de G_n^*/X_n^*. Puisque $\theta_n(\mathfrak{C}) = 1$ on sait que

$$f(g^*) \in U\big(O_{F_n^*}\big)F_n^{*\times}, \quad \forall g^* \in G_n^*.$$

Il suffit donc de montrer que

$$f(g_m^*) \in U\big(O_{F_m^*}\big)F_m^{*\times}, \quad 0 \le m \le n.$$

La démonstration se fait en deux parties suivant que $m \ge 1$ ou $m = 0$.

On suppose $m \ge 1$. On décompose $f(g_m^*)$ en produit

$$f(g_m^*) = N_{n/m}\big(f(g_n^*)\big)f(g_m^*)N_{n/m}\big(f(g_n^*)\big)^{-1}.$$

Il suffit donc de démontrer que

$$f(g_m^*)N_{n/m}\big(f(g_n^*)\big)^{-1} \in U\big(O_{F_m^*}\big)F_m^{*\times}. \tag{3.16}$$

Puisque p est décomposé dans K, on identifie X_n^* et $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Si $X_{n,m}^*$ désigne $\mathrm{Gal}(F_n^*/F_m^*)$, puisque $m \ge 1$, $\{1 + jp^m,\ 0 \le j \le p^{n-m} - 1\}$ est un système de représentants des éléments de $X_{n,m}^*$. Puisque f commute avec l'action de X_n^* on obtient

$$N_{n/m}\big(f(g_n^*)\big) = \prod_{0 \le j \le p^{n-m}-1} f\big((1 + jp^m)g_n^*\big).$$

Compte tenu de la définition de f on décompose $f(g_m^*)N_{n/m}\big(f(g_n^*)\big)^{-1}$ en un produit $u_m(g_n^*)v_m(g_n^*)$ avec

$$u_m(g_n^*) = \hat{r}(c')\big(p^{n-m}g_n^*\big) \prod_{0\le j\le p^{n-m}-1} \big(\hat{r}(c')\big((1+jp^m)g_n^*\big)\big)^{-1}$$

$$v_m^{-1}(g_n^*) = \hat{r}(\tilde{c}')\big(p^{n-m}g_n^*\big) \prod_{0\le j\le p^{n-m}-1} \big(\hat{r}(\tilde{c}')\big((1+jp^m)g_n^*\big)\big)^{-1}.$$

On pose maintenant

$$x_m = [p^{n-m}]r(c') \prod_{0\le j\le p^{n-m}-1} \big([1+jp^m]r(c')\big)^{-1}$$

$$\tilde{y}_m^{-1} = [p^{n-m}]r(\tilde{c}') \prod_{0\le j\le p^{n-m}-1} \big([1+jp^m]r(\tilde{c}')\big)^{-1}.$$

Par définition $x_m \in (C\otimes F_n)[G_n]$, tandis que y_m est une unité de l'ordre maximal de $(C\otimes \mathrm{Ad}(F_n))[G_n]$. Montrons que x_m et y_m sont invariants par l'action de V_n. Les démonstrations pour x_m et y_m sont semblables et nous nous contentons de vérifier cette propriété pour x_m. Soit $\sigma \in V_n$. On sait, [AT], Lemma 4.25, qu'il existe $g_o \in G_n$ tel que pour tout $q \in \mathbb{Z}$

$$([q]r(c'))^\sigma = [q]r(c')g_0^q.$$

On en déduit

$$[p^{n-m}]r(c')^\sigma = [p^{n-m}]r(c')g_0^{p^{n-m}}$$

$$\prod_{0\le j\le p^{n-m}-1} [1+jp^m]r(c')^\sigma = \Big(\prod_{0\le j\le p^{n-m}-1} [1+jp^m]r(c')\Big)g_0^\alpha$$

où $\alpha = p^{n-m} + p^n\dfrac{(p^{n-m}-1)}{2}$.

On conclut que x_m (resp. y_m) appartient à $A_n^\times$ (resp. $U(\mathfrak{M}_n)$). Or, on a les égalités

$$u_m(g_n^*) = \hat{x}_m(g_n^*)\,,\quad v_m(g_n^*) = \hat{y}_m(g_n^*).$$

C'est donc que $u_m(g_n^*) \in F_n^*$ $\big($resp. $v_m(g_n^*) \in U\big(O_{F_n^*}\big)\big)$. Puisque pour tout $\omega \in X_{n,m}^*$ on a : $\hat{x}_m(g_n^*)^\omega = \hat{x}_m(g_n^{*\omega}) = u_m(g_n^{*\omega}) = u_m(g_n^*) = \hat{x}_m(g_n^*)$ on conclut que $u_m(g_n^*) \in F_m^*$ et de même que $v_m(g_n^*) \in U\big(O_{F_m^*}\big)$ ce qui démontre (3.16).

On suppose pour terminer que $m = 0$. On sait par l'étude du cas précédent que $f(g_1^*) \in U\big(O_{F_1^*}\big)F_1^{*\times}$. On sait en outre, grâce à (3.15), que $[p]f \equiv f^p \bmod B_n^{*\times}U(\mathfrak{M}_n^*)$.

On en déduit que

$$f(g_0) \in U\big(O_{F_1^*}\big)F_1^{*\times}.$$

Puisque $f(g_0)$ est invariant par X_n^*, on obtient que $N_{1/0}f(g_0) = f(g_0)^{p-1} \in U(O_F)F^\times$.

En conclusion, on a montré que $\varphi_n(\mathfrak{C})^{p-1} = 1$. Or, puisque $PH(\mathfrak{B}_n)$ est contenu dans $H^1(F, E_{\pi^n})$, tout élément de ce groupe est d'ordre une puissance de p. On conclut que $\varphi_n(\mathfrak{C}) = 1$, ce qui achève la démonstration du théorème. □

On déduit de la définition même de $S_n(F)$ que l'image par restriction d'un élément de $S_n(F)$ dans $H^1(F_v, E_{\pi^n})$ appartient à $E(F_v)/\pi^n E(F_v)$. On définit le sous-groupe $\Sigma_n(F)$ de $S_n(F)$ comme le noyau de l'homomorphisme

$$S_n(F) \longrightarrow \prod_{v|\pi^*} \big(E(F_v)/\pi^n E(F_v)\big).$$

Si L est un corps de nombres et v une place finie de L on note $\tilde{L}_v$ le corps résiduel de L_v en v. Si E/L_v est une courbe elliptique définie sur L_v on note $\tilde{E}_v$ la courbe réduite en v. Si n est un entier, $n \geq 1$, on note $\mu_n(L_v)$ le groupe des racines n-ièmes de l'unité contenues dans L_v. Sous nos hypothèses on a le lemme suivant :

LEMME 3.17.

1) *Si v est une place de F au-dessus de $\mathfrak{p}^*$ l'ordre du groupe $\widetilde{E}_v(\widetilde{F}_v)$ est premier à p.*

2) *Pour tout entier n et toute place w de F_n^* au-dessus de $\mathfrak{p}^*$ alors $\mu_p(F_{n,w}^*) = \{1\}$.*

3) *Pour tout entier n on a l'égalité*

$$\Sigma_n(F) = S_n(F).$$

Les démonstrations sont standard.

Puisque $\mathfrak{p}^*$ est totalement décomposé dans F, on a l'égalité $\widetilde{E}_v(\widetilde{F}_v) = \widetilde{E}_{v_0}\big(\widetilde{K}_{v_0}\big)$ si v_0 désigne la restriction de v à K. Supposons π choisi comme la valeur en v_0 du Grössencharakter associé à E/K. On a l'égalité

$$(1-\pi)(1-\bar{\pi}) = \big|\widetilde{E}_{v_0}\big(\widetilde{K}_{v_0}\big)\big|$$

où $|H|$ désigne l'ordre du groupe H.

Puisque $\pi\bar{\pi} = p$ on en déduit que p divise $\left|\widetilde{E}_{v_0}\left(\widetilde{K}_{v_0}\right)\right|$ si et seulement si $\pi + \bar{\pi} \equiv 1 \bmod p$, c'est-à-dire, puisque $|\pi| = \sqrt{p}$, $\pi + \bar{\pi} = 1$. Or, ceci est impossible, car p n'est pas anormal.

Supposons que $F^*_{n,w}$ contienne ζ, une racine primitive p-ième de l'unité. Il existe $g \in E_\pi$ (resp. $g^* \in E_{\pi^*}$) tel que $\langle g, g^* \rangle = \zeta$ où $\langle\ ,\ \rangle$ désigne le pairing de Weil sur les points de p division. Puisque $g^* \in E(F^*_{n,w})$

$$\langle g^\omega, g^* \rangle = \langle g^\omega, g^{*^\omega} \rangle = \langle g, g^* \rangle^\omega = \langle g, g^* \rangle$$

pour tout $\omega \in \mathrm{Gal}\left(F^{*^c}_{n,w}/F^*_{n,w}\right)$. C'est donc que $g \in E(F^*_{n,w})$. Puisque la réduction en w est injective sur le groupe des points de π division, on en déduit que $\widetilde{E}_w(\widetilde{F}^*_{n,w})$ contient un point d'ordre p. Puisque (F^*_n/F) est totalement ramifiée au-dessus de $\mathfrak{p}^*$ on a l'égalité $\widetilde{E}_w(\widetilde{F}^*_{n,w}) = E_v(\widetilde{F}^*_v)$ si $w_{|F} = v$ et par conséquent, on sait par 1) que ce groupe ne contient pas d'élément d'ordre p. On conclut que $\mu_p(\widetilde{F}^*_{n,v}) = \{1\}$. Pour démontrer que $\Sigma_n(F) = S_n(F)$ il suffit de vérifier que $E(F_v) = \pi^n E(F_v)$ pour toute place v au-dessus de $\mathfrak{p}^*$. Soit $E_1(F_v)$ le noyau de la réduction en v. Grâce à 1) on sait que l'indice de $E_1(F_v)$ dans $E(F_v)$ est premier à p. Il suffit donc de montrer que la multiplication par π induit un automorphisme de $E_1(F_v)$, ce qui est bien connu puisque π et v sont premiers entre eux. □

On utilise maintenant un théorème de B. Perrin-Riou, [PR1], III, Proposition 1 ou [PR2].

On pose

$$V(F^*_n) = \{x = (x_v)\,,\ x \in U(F^*_n) \text{ tels que } x_v = 1\,,\ \forall v,\ v|\mathfrak{p}^*\}.$$

THÉORÈME 3.18. — *Il existe un isomorphisme de groupe*

$$\mu^*_n : S_n(F) \xrightarrow{\sim} \mathrm{Hom}\left(G^*_n, J(F^*_n)/V(F^*_n)F^{*\times}_n)\right)^{X^*_n}.$$

On note que cet isomorphisme est l'isomorphisme $\eta^{*^{-1}}_n$ de [PR1] puisque sous nos hypothèses $S_n(F) = \Sigma_n(F)$ et $\mu_{p^n}(F^*_n) = \{1\}$.

Démonstration du théorème 1. — Le théorème 1 se déduit facilement des théorèmes 3.14 et 3.18. On obtient immédiatement l'isomorphisme

$$\mathcal{D}_n(F) \simeq \mathrm{Hom}\left(G^*_n, U(O_{F^*})F^{*\times}_n/\left(V(F^*_n)F^{*\times}_n\right)\right)^{X^*_n}. \tag{3.19}$$

Des isomorphismes classiques de groupes, on déduit que

$$\left(U(O_{F^*})F^{*\times}_n\right)/\left(V(F^*_n)F^{*\times}_n\right) \simeq \left(U(O_{F^*_n})\right)/\left(V(F^*_n)\mathcal{E}^*_n(F)\right)$$

et par définition de $V(F_n^*)$

$$(U(O_{F^*})/(V(F_n^*)\mathcal{E}_n^*(F)) \simeq O^{\times}_{F_n^*,\mathfrak{p}^*}/\mathcal{E}_n^*(F). \tag{3.20}$$

Posons $q = p^n$. Le groupe $O^{\times}_{F_n^*,\mathfrak{p}^*}$ se décompose en un produit direct de $U_n^*(F)$ par un sous-groupe d'ordre premier à p. L'injection $U_n^*(F) \hookrightarrow O^{\times}_{F_n^*,\mathfrak{p}^*}$ induit donc un isomorphisme

$$U_n^*(F)/\mathcal{E}_n^{*\prime}(F))_q \simeq (O^{\times}_{F_n^*,\mathfrak{p}^*}/\mathcal{E}_n^*(F))_q. \tag{3.21}$$

Puisque $\mu_p(F_{n,w}^*) = \{1\}$, c'est immédiat que $x \to x^q$ induit un isomorphisme

$$(U_n^*(F)/\mathcal{E}_n^{*\prime}(F))_q \simeq (\mathcal{E}_n^{*\prime}(F) \cap U_n^*(F)^q)/(\mathcal{E}_n^{*\prime}(F))^q. \tag{3.22}$$

L'application $f \to f(g_n^*)$ est un isomorphisme de

$$\mathrm{Hom}\,(G_n^*, U(O_{F_n^*})F_n^{*\times}/(V(F_n^*)F_n^{*\times}))^{(X_n^*)}$$

dans $(U(O_{F_n^*})F_n^{*\times}/(V(F_n^*)F_n^{*\times}))_q^{(\kappa_n^*)}$. En composant cet isomorphisme avec les isomorphismes (3.20), (3.21) et (3.22) on obtient l'isomorphisme du théorème 1 (1). Pour démontrer (2), il suffit de montrer que l'homomorphisme naturel

$$t : \mathcal{E}_n^{*\prime}(K) \cap U_n^*(K)^q/\mathcal{E}_n^{*\prime}(K)^q \longrightarrow (\mathcal{E}_n^{*\prime}(F) \cap U_n^*(F)^q/\mathcal{E}_n^{*\prime}(F)^q)^{\Delta}$$

est un isomorphisme lorsqu'on a identifié les groupes Δ et $\mathrm{Gal}(F_n^*/K_n^*)$. On note N la norme de F_n^*/K_n^*, on pose $m = [F : K] = [F_n^* : K_n^*]$ et l'on rappelle que $(m, p) = 1$. En composant t avec l'homomorphisme induit par N on vérifie facilement que $N \circ t$ et $t \circ N$ sont l'élévation à la puissance m. Le résultat est alors immédiat. □

4. Construction de générateurs de e.h.p.

Le but de ce paragraphe est de démontrer le théorème 2. Nous commençons par rappeler les résultats de la théorie de Kummer pour les e.h.p. Notre référence est [AT], §7 et 8.

On fixe l'entier n, $n \geq 1$, on pose $q = p^n$. On considère l'extension $N = F_n^* F_n$ de F. Cette extension contient le groupe des racines q-ièmes de l'unité. On rappelle qu'au choix d'un point primitif de $\mathfrak{p}^{*^n}$ division, noté g_n^*, est associé le caractère χ_n de G_n introduit en (2.17).

Pour se trouver dans une situation kummérienne habituelle on étend les scalaires à N. On introduit les algèbres de Hopf $B_{n,N} = \mathrm{Map}(G_n, N)$

et $A_{n,N} = N[G_n]$, duales l'une de l'autre par la dualité de Cartier et l'on désigne par $\mathfrak{B}_{n,N}$(resp. $\mathcal{A}_{n,N}$) l'ordre de Hopf qui définit G_n considéré comme schéma en groupe sur $\mathrm{Spec}(O_N)$ (resp. le O_N-dual de $\mathfrak{B}_{n,N}$). On obtient alors un isomorphisme $\theta_{n,N}$:

$$PH(B_{n,N}) \simeq \mathrm{Hom}(\Omega_N, G_n) \xrightarrow{\sim} \mathrm{Hom}(\Omega_N, \mu_q) \xrightarrow{\sim} N^\times/N^{\times q}. \tag{4.1}$$

Le premier isomorphisme est décrit dans [BT], II, le second est obtenu via χ_n et le troisième est celui de la théorie de Kummer.

Si C est un e.h.p. pour $B_{n,N}$ et c une base de C comme $A_{n,N}$ module, on a

$$\theta_{n,N}(C) = \chi_n(r(c))^q N^{\times q}. \tag{4.2}$$

L'isomorphisme réciproque $\theta_{n,N}^{-1}$ est définie par

$$\theta_{n,N}^{-1}(aN^{\times q}) = N[X]/(X^q - a) = N[x]$$

avec $x^g = x\chi_n(g)$, $\forall g \in G_n$.

Si C est un e.h.p. pour B_n et c une base de C sur A_n on vérifie que $\chi_n(r(c))^q \in F_n^{*\times q}$ et l'on définit

$$\begin{aligned} \theta_{n,F} : PH(B_n) &\longrightarrow F_n^{*\times}/F_n^{*\times q} \\ (C) &\longrightarrow \chi_n(r(c))^q F_n^{*\times q}. \end{aligned}$$

L'extension des scalaires d'une part et l'injection canonique d'autre part permettent de définir

$$\begin{aligned} i_n &: PH(B_n) \longrightarrow PH(B_{n,N}) \\ d_n &: F_n^{*\times}/F_n^{*\times q} \longrightarrow N^\times/N^{\times q}. \end{aligned} \tag{4.3}$$

On déduit de [AT], §6 et Proposition 7.5.

PROPOSITION 4.4.

1) *i_n et d_n sont des homomorphismes injectifs.*

2) *Le diagramme suivant est commutatif*

$$\begin{array}{ccc} PH(B_{n,N}) & \xrightarrow{\theta_{n,N}} & N^\times/N^{\times q} \\ {\scriptstyle i_n}\uparrow & & {\scriptstyle d_n}\uparrow \\ PH(B_n) & \xrightarrow{\theta_{n,F}} & F_n^{*\times}/F_n^{*\times q} \end{array}$$

3) *i_n induit un homomorphisme*

$$PH(\mathfrak{B}_n) \longrightarrow PH(\mathfrak{B}_{n,N})$$

4) *$\theta_{n,F}$ induit par restriction à $\mathcal{D}_n(F)$ l'isomorphisme $\Phi_{n,F}$.*

Démonstration du théorème 2. — Nous commençons à montrer 1) sous forme d'un lemme :

LEMME 4.5. — *Soit* $(\mathfrak{C}) \in PH(\mathfrak{B}_n)$ *tel que* $\Phi_n(\mathfrak{C}) = \alpha_n \mathcal{E}_n^{*\prime}(F)^q$ *où* $\alpha_n \in \mathcal{E}_n^{*\prime}(F) \cap U_n^*(F)^q$. *On pose* $C = \mathfrak{C}F$. *Alors il existe un unique élément* y_n *de* $C \otimes F_n^*$ *tel que*

$$y_n^q = \alpha_n \quad \text{et} \quad y_n^g = y_n \chi_n(g), \quad \forall g \in G_n.$$

Démonstration. — On a l'égalité

$$\alpha_n F_n^{*\times q} = \chi_n(r(c))^q F_n^{*\times q}.$$

Il existe donc $\lambda_n \in F_n^{*\times}$ tel que

$$\alpha_n = \Big(\lambda_n \sum_{g \in G_n} c^g \chi_n^{-1}(g)\Big)^q.$$

On pose

$$y_n = \lambda_n \sum_g c^g \chi_n^{-1}(g) = \lambda_n \sum_g c^g w_n(-g, g_n^*). \tag{4.5}$$

Par définition y_n appartient à $C \otimes N$. Pour démontrer qu'il appartient à $C \otimes F_n^*$ il suffit de montrer qu'il est invariant par $\mathrm{Gal}(N/F_n^*)$. Comme dans le §3, on sait que $C \otimes N/F$ est une T_n-algèbre galoisienne en posant

$$T_n = G_n \ltimes Y_n \quad \text{avec} \quad Y_n = \mathrm{Gal}(N/F)$$

où $\sigma^{-1} g \sigma = g^\sigma$, $\forall g \in G_n$, $\sigma \in Y_n$.

Puisque $F_n \cap F_n^* = F$, le groupe $\mathrm{Gal}(N/F_n^*)$ s'identifie par restriction à X_n. Pour tout $\omega \in X_n$ on obtient

$$y_n^\omega = \lambda_n \sum_g c^{g^\omega} w_n(-g^\omega, g_n^{*\omega}) = \lambda_n \sum_g c^{g^\omega} w_n(-g^\omega, g_n^*).$$

Or g^ω décrit G_n lorsque g décrit G_n. C'est donc que $y_n^\omega = y_n$, $\forall \omega \in X_n$. Si $h \in G_n$ on a

$$y_n^h = \sum_g c^{gh} w_n(-g, g_n^*).$$

On conclut que $y_n^h = y_n w_n(h, g_n^*) = y_n \chi_n(h)$.

Montrons maintenant l'unicité de y_n. Soient y et z des éléments de $C \otimes F_n^*$ satisfaisant les propriétés du lemme. On pose $u = yz^{-1}$. Puisque u est invariant par G_n c'est un élément de N ; puisqu'il est invariant par X_n il appartient à F_n^*. Or $u^q = 1$. Comme $\mu_q(F_n^*) = \{1\}$, $u = 1$ et donc $y = z$. □

On déduit de (3.9) l'isomorphisme de F-algèbre

$$A_n \simeq \bigoplus_{k=0}^{n} F_k^*$$

$$\sum_g x_g g \longrightarrow \bigoplus_{k=0}^{n} \Big(\sum_g x_g w_n\big(g, p^{n-k} g_n^*\big)\Big). \tag{4.6}$$

On identifie dorénavant, via cet isomorphisme A_n et $\bigoplus_{k=0}^{n} F_k^*$. Pour toute algèbre commutative R/F on définit l'opérateur norme

$$\sigma_R = \big(F_n^* \underset{F}{\otimes} R\big)^\times \longrightarrow \big(A_n \underset{F}{\otimes} R\big)^\times \tag{4.7}$$

par $\sigma_R(x) = \bigoplus_{k=0}^{n} N_{n/k}(x)$ où $N_{n/k}$ sont les homomorphismes de norme introduits §2. On désigne par ℓ l'application R-linéaire

$$R[G_n] \longrightarrow R$$

définie par $\ell(g) = \begin{cases} 1 & \text{si } g = 1 \\ 0 & \text{sinon.} \end{cases}$

Puisque $\mathfrak{C}$ définit un élément de $\mathcal{D}_n(F)$ on peut considérer pour base de C sur A_n une base c de $\mathfrak{CM}_n$ sur $\mathfrak{M}_n$. On pose $y_n = \alpha_n^{1/q}$. On sait par (4.5) que

$$\alpha_n^{1/q} = \lambda_n \chi_n(r(c)) \quad \text{avec} \quad \lambda_n \in F_n^{*\times}. \tag{4.8}$$

On pose $\sigma = \sigma_C$. En appliquant σ aux deux membres de l'égalité (4.8) on obtient dans $(C \otimes N)[G_n]$

$$\sigma\big(\alpha_n^{1/q}\big) r(c)^{-1} = \sigma(\lambda_n)\sigma\big(\chi_n(r(c))\big) r(c)^{-1}. \tag{4.9}$$

Par définition $\sigma(\lambda_n) \in A_n^\times$. En outre [AT], Proposition 8.4, affirme que $\sigma\big(\chi_n(r(c))\big) r(c)^{-1} \in A_n^*$. On obtient ainsi que $\sigma(\alpha_n^{1/q}) r(c)^{-1} \in A_n^*$. On pose $x_n = \sigma(\alpha_n^{1/q})(\pi^n r(c)^{-1})$. On vient de démontrer que $x_n \in A_n^*$. Montrons que $x_n \in \mathfrak{M}_n^\times$. Puisque c désigne une base de $\mathfrak{CM}_n$ sur $\mathfrak{M}_n$, [T2], Théorème 3 ou [AT], Lemma 4.6, implique que $\pi^n r(c)^{-1}$ est une unité de l'ordre maximal de $(C \otimes F_n)[G_n]$. De même puisque $\alpha_n \in \mathcal{E}_n^{*\prime}(F), \sigma(\alpha_n^{1/q})$ est une unité de l'ordre maximal de $(C \otimes A_n)$. C'est donc que x_n est une unité de l'ordre maximal de $(C \otimes F_n)[G_n]$. On conclut que $x_n \in \mathfrak{M}_n^\times$. Ainsi

$$\pi^n \sigma(\alpha_n^{1/q}) = r(c) x_n \quad \text{avec} \quad x_n \in \mathfrak{M}_n^\times. \tag{4.10}$$

Posons $c' = c x_n$. C'est une base de $\mathfrak{CM}_n$ sur $\mathfrak{M}_n$ telle que $r(c') = \pi^n \sigma(\alpha_n^{1/q})$. Puisque $\ell(r(c')) = \ell(\Sigma c' g g^{-1}) = c'$, on obtient l'égalité .

$$c' = \pi^n \ell\big(\sigma(\alpha_n^{1/q})\big). \tag{4.11}$$

Pour achever la démonstration du théorème 2, il reste à vérifier le lemme suivant :

LEMME 4.12.

$$\ell\big(\sigma(\alpha_n^{1/q})\big) = \frac{1}{q}\sum_{i=0}^{n} T_{i/0}\big(N_{n/i}(\alpha_n^{1/q})\big).$$

Par définition de σ, on sait que $\sigma(\alpha_n^{1/q})$ est un élément de $(A_n \underset{F}{\otimes} C)^\times$, qu'on écrit

$$\sigma(\alpha_n^{1/q}) = \sum_{g\in G_n} a_g g.$$

Par la formule d'inversion de Fourier, on a l'égalité

$$q\ell\big(\sigma(\alpha_n^{1/q})\big) = qa_0 = \sum_{\chi} \chi\big(\sigma(\alpha_n^{1/q})\big)$$

où χ parcourt les caractères de G_n.

On traduit cette égalité par

$$qa_0 = \sum_{\substack{g\in G_n \\ g^*\in G_n^*}} a_g w_n(g,g^*).$$

Puisque $\sum_{g\in G_n} a_g g$ est invariant par l'action de Ω_F, cette égalité s'écrit

$$qa_0 = \sum_{i=0}^{n} T_{i/0}\Big(\sum_{g\in G_n} a_g w_n(g, p^{n-i}g_n^*)\Big). \tag{4.13}$$

Or, grâce à (4.6) et (4.7)

$$\sum_{g\in G_n} a_g w_n(g, p^{n-i}g_n^*) = N_{n/i}(\alpha_n^{1/q}). \tag{4.14}$$

L'égalité souhaitée se déduit de (4.13) et (4.14). □

5. Formules locales et mesures p-adiques.

Le but de ce paragraphe est essentiellement de démontrer le théorème 3. Le théorème se déduit de propositions que nous allons démontrer.

PROPOSITION 5.1. — *Soit $\mathfrak{C}$ un e.h.p. pour $\mathfrak{B}_n$ tel que $(\mathfrak{C}) \in \mathcal{D}_n(F)$. On suppose qu'on a*

$$\overline{\Phi}_n(\mathfrak{C}) = \alpha'_n \overline{\mathcal{E}}_n^*(F)^q \quad \text{où} \quad \alpha'_n = \gamma_n^q, \quad \gamma_n \in U_n^*(F).$$

Alors pour tout entier m, $m \geq 1$, il existe une base c_m de $\mathfrak{CM}_n$ sur $\mathfrak{M}_n$ telle que

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

On pose dans cette démonstration $\rho = \rho_{\mathfrak{p}^*}$. Par abus de notation c désigne à la fois un élément de $C = \mathfrak{C}F$ et son image dans $C_{\mathfrak{p}^*}$.

On suppose que

$$\Phi_n(\mathfrak{C}) = \alpha_n \mathcal{E}_n^*(F)^q \quad \text{avec} \quad \alpha_n = \beta_n^q \text{ et } \beta_n \in U_n^*(F).$$

On déduit du théorème 2 l'existence d'une base $c(\alpha_n)$ de $\mathfrak{CM}_n$ sur $\mathfrak{M}_n$ telle que

$$\rho(c(\alpha_n)) = \frac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}\big(N_{n/i}(\rho(\alpha_n^{1/q}))\big). \tag{5.2}$$

Puisque ρ est un homomorphisme d'algèbre, dans $F^*_{n,\mathfrak{p}^*}$ on a les égalités

$$\rho(\alpha_n^{1/q})^q = \rho(\alpha_n) = \rho(\beta_n)^q,$$

d'où

$$\rho(\alpha_n^{1/q}) = \rho(\beta_n), \quad \text{puisque } \mu_p(F^*_{n,\mathfrak{p}^*}) = \{1\}. \tag{5.3}$$

Par définition de α_n et α'_n, il existe $u_n \in \overline{\mathcal{E}}^*_n(F)$ tel que $\alpha_n = \alpha'_n u_n^q$. On en déduit que $\beta_n^q = (\gamma_n u_n)^q$ et comme précédemment que $\beta_n = \gamma_n u_n$.

Puisque u_n est limite d'une suite de $\mathcal{E}_n^{*\prime}(F)$, pour tout entier m, $m \geq 1$, il existe $v_m \in \mathcal{E}_n^{*\prime}(F)$ et $w_m \in U_n^*(F)$, $w_m \equiv 1 \bmod p^{m+n}$, tel que

$$\beta_n v_m = \gamma_n w_m.$$

Posons $\alpha''_n = (\beta_n v_m)^q$. Puisque l'on a $\Phi_n(\mathfrak{C}) = \alpha''_n \mathcal{E}_n^{*\prime}(F)^q$, de (5.2) et (5.3) on déduit l'existence d'une base c_m de $\mathfrak{CM}_n$ sur $\mathfrak{M}_n$ telle que

$$\rho(c_m) = \frac{1}{\pi^{*n}} \sum_{i=0}^{n} T_{i/0}\big(N_{n/i}(\gamma_n w_m)\big). \tag{5.4}$$

On en déduit immédiatement la congruence souhaitée. □

Soit f un élément non trivial du groupe

$$\mathrm{Hom}(T_{\pi^*}, U_\infty^*(K)/\overline{\mathcal{E}}^*_\infty(K))^{X^*_\infty}.$$

Pour tout entier n, $n \geq 1$, notons s_n la projection de $U_\infty^*(K)/\overline{\mathcal{E}}^*_\infty(K)$ dans $U_n^*(K)/\overline{\mathcal{E}}^*_n(K)$. On rappelle que g^* est un générateur fixé de T_{π^*}.

Il existe un entier n_0 tel que pour tout entier n, $n \geq n_0$, $s_n(f(g^*))$ est un élément non trivial de $U_n^*(K)/\overline{\mathcal{E}}_n^*(K)$. Soit ω un générateur de $\mathrm{Gal}(K_\infty^*/K_n^*)$. Alors

$$s_n(f(g^*)) = s_n(f(g^*))^\omega = s_n(f(g^{*^\omega})).$$

C'est donc que $s_n \circ f$ induit un homomorphisme de groupe de

$$T_{\pi^*}/(\omega - 1)T_{\pi^*} \to U_n^*(K)/\mathcal{E}_n^*(K).$$

Puisque l'on sait que la projection de $T_{\pi^*}/(\omega - 1)T_{\pi^*}$ sur $E_{\pi^{*n}}$ est un isomorphisme, on conclut que $s_n(f(g^*))$ est un élément non trivial de $(U_n^*(K)/\overline{\mathcal{E}}_n^*(K))_{p^n}^{(\kappa_n^*)}$. Ainsi, si $f(g^*) = \gamma\overline{\mathcal{E}}_\infty^*(K)$ où $\gamma = [\gamma_n]$, pour tout entier n, $n \geq n_0$, $\gamma_n\overline{\mathcal{E}}_n^*(K)$ est un élément non trivial du groupe $(U_n^*(K)/\overline{\mathcal{E}}_n^*(K))_{p^n}^{(\kappa_n^*)}$. On définit $(\mathfrak{C}_n(f))$ comme l'élément de $\mathcal{D}_n(K)$ tel que

$$\overline{\Phi}_n(\mathfrak{C}_n(f)) = \gamma_n^{p^n}\,\overline{\mathcal{E}}_n^*(K)^{p^n} \tag{5.4}$$

dans le groupe $\left((\overline{\mathcal{E}}_n^*(K) \cap U_n^*(K)^{p^n})/(\overline{\mathcal{E}}_n^*(K)^{p^n})\right)^{(\kappa_n^*)}$. Il vérifie les propriétés exigées par le théorème 3.

Remarque. — Puisque $f(g^*)^\sigma = f(g^*)^\sigma$, $\forall\sigma \in X_\infty^*$ on vérifie que $\gamma \equiv \gamma^{(1)} \bmod \overline{\mathcal{E}}_\infty^*(K)$. On suppose dorénavant que l'on a choisi $\gamma \in U_\infty^{*^{(1)}}(K)$.

Compte tenu de la proposition 5.1, il suffit, pour achever la démonstration du théorème 3, de montrer

PROPOSITION 5.5. — *Soit n un entier $n \geq 1$ et $q = p^n$. Soit $\gamma = [\gamma_n]$, $\gamma \in U_\infty^{*^{(1)}}$. Alors*

$$\frac{1}{q}\sum_{i=0}^{n} T_{i/0}(\gamma_i) = \hat{\mu}_\gamma(q\mathbb{Z}_p).$$

On utilise les notations du §2. Si $\mathfrak{F}/O_{K_{\mathfrak{p}^*}}$ est le groupe formel de Lubin-Tate associé à la série de Frobenius f et si $a \in O_{K_{\mathfrak{p}^*}}$ on note $[a]_f$ l'endomorphisme de $\mathfrak{F}$ défini par a. Soit $K_{p^*}^{nr}$ l'extension maximale non ramifiée de $K_{\mathfrak{p}^*}$, on note Φ le Frobenius de $K_{\mathfrak{p}^*}^{nr}/K_{\mathfrak{p}^*}$ prolongé par continuité à L. Grâce à [L], VIII, Théorème 3.1, il existe un homomorphisme de groupe formel $\eta : G_m \to \widehat{E}$, défini sur O_L tel que

$$\eta \circ [a]_f = [a]_{f'} \circ \eta\,, \quad \forall a \in O_{K_{\mathfrak{p}^*}} \tag{5.6}$$

$\eta(x) \equiv \varepsilon x \bmod \deg 2$ où ε est une unité de O_L telle que $\varepsilon^\Phi/\varepsilon = \pi^*/p = \pi^{-1}$.

On note ici $f = (1+X)^p - 1$ (resp. f' la série de Frobenius pour π^*) à laquelle G_m (resp. $\widehat{E}$) est associée. En outre η satisfait l'égalité

$$\eta^\Phi = \theta \circ [\pi^{-1}]_f. \tag{5.7}$$

Soit $v = [v_n]$ un générateur du module de Tate associé à G_m. Pour tout entier n, $n \geq 1$, on pose

$$g_n^* = [\pi^n]_{f'}(\eta(v_n)). \tag{5.8}$$

On a les relations :

$$\begin{aligned} [\pi^{*^n}]_{f'}(g_n^*) &= [p^n]_{f'}(\eta(v_n)) = \eta([p^n]_f(v_n)) = 0 \\ [\pi^*]_{f'}(g_n^*) &= [\pi^{n-1}]_{f'} \circ [p]_{f'}(\eta(v_n)) = [\pi^{n-1}]_{f'}(\eta(v_{n-1})) \end{aligned} \tag{5.9}$$

et donc $[\pi^*]_{f'}(g_n^*) = g_{n-1}^*$. C'est donc que $g^* = [g_n^*]$ est un générateur de T_{π^*}. On suppose que le générateur de T_{π^*} qu'on a fixé a été obtenu de cette manière.

On rappelle maintenant brièvement comment associer à tout élément de $O_L[[X]]$ une mesure sur $\mathbb{Z}_p$ à valeurs dans O_L. On sait que L et $\mathbb{Q}_p(\zeta_{p^\infty})$ sont linéairement disjoints sur $\mathbb{Q}_p$.

On considère l'isomorphisme de O_L-algèbre

$$O_L[[X]] \longrightarrow \varprojlim \left(O_L[X]/((X+1)^{p^n} - 1)\right),$$

[L], V, §1, défini par

$$h \longrightarrow [h_n] \tag{5.10}$$

où h_n est le reste de la "division euclidienne" de h par $(X+1)^{p^n} - 1$. On sait en effet, [L], V, Théorème 2.1, qu'il existe un couple unique (t_n, h_n), $t_n \in O_L[[X]]$, $h_n \in O_L[X]$ et $\deg(h_n) < p^n$, tel que

$$h = ((X+1)^{p^n} - 1)t_n + h_n. \tag{5.11}$$

On considère alors les isomorphismes

$$O_L[X]/((X+1)^{p^n} - 1) \longrightarrow O_L[X]/(X^{p^n} - 1) \qquad X \to (X-1) \tag{5.12}$$

$$O_L[X]/(X^{p^n} - 1) \longrightarrow O_L[\mathbb{Z}_p/p^n\mathbb{Z}_p] \qquad X \to \overline{1}. \tag{5.13}$$

Par passage à la limite, on déduit de (5.10), (5.12) et (5.13) l'isomorphisme

$$\begin{aligned} O_L[[X]] &\longrightarrow O_L[[\mathbb{Z}_p]] \\ h &\longrightarrow \mu_h. \end{aligned}$$

Avec ces notations, on vérifie facilement que pour tout entier n et tout entier k, $0 \leq k < p^n$, alors

$$\mu_h(k + p^n\mathbb{Z}p) = a_{k,n} \tag{5.14}$$

où $a_{k,n}$ est le coefficient de X^k dans $h_n(X-1)$.

On peut désormais démontrer la proposition 5.5. Soit h_γ la série de Coleman associée à γ. C'est un élément de $O_{K_{\mathfrak{p}^*}}[[X]]$ tel que

$$h_\gamma(g_n^*) = \gamma_n\,, \quad \forall n \geq 1.$$

Compte tenu de (5.8), on a :

$$h_\gamma \circ [\pi^n]_{f'} \circ \eta(v_n) = \gamma_n \quad \forall n \geq 1. \tag{5.15}$$

On fixe dorénavant n, $n \geq 1$. La théorie du corps de classe local associe à π un élément σ_π de $\mathrm{Gal}(K_{n,\mathfrak{p}^*}^*/K_{\mathfrak{p}^*})$ et l'on a :

$$(g^*)^{\sigma_\pi^{-1}} = [\pi]_{f'}(g^*)\,, \quad \forall g^* \in E_{\pi^{*n}} \tag{5.16}$$

([dS], I, Proposition 1.8).

Puisque $\eta(v_n) \in E_{\pi^{*n}}$ et que $h_\gamma \in O_{K_{\mathfrak{p}^*}}[[X]]$ on obtient grâce à (5.15) et (5.16)

$$h_\gamma \circ \eta(v_i) = \gamma_i^{\sigma_{\pi^i}}\,, \quad 1 \leq i \leq n. \tag{5.17}$$

C'est-à-dire, en posant $\hat{h}_\gamma = h_\gamma \circ \eta$,

$$\hat{h}_\gamma(v_i) = \gamma_i^{\sigma_{\pi^i}}\,, \quad 1 \leq i \leq n. \tag{5.18}$$

On associe à $\hat{h}_\gamma$, via (5.11) le polynôme $\hat{h}_{\gamma,n}$ et l'on écrit

$$\hat{h}_{\gamma,n}(X-1) = a_0 + a_1 X + \cdots + a_{q-1}X^{q-1}\,, \quad a_i \in O_L \quad 0 \leq i \leq q-1.$$

On évalue maintenant a_0 de deux manières différentes. De (5.14), on déduit que

$$\hat{\mu}_\gamma(q\mathbb{Z}_p) = a_0. \tag{5.19}$$

Notons c_n l'image de 1 dans $\mathbb{Z}/q\mathbb{Z}$. C'est un générateur de ce groupe cyclique. Notons dorénavant C_q ce groupe et multiplicativement sa loi. On considère l'élément

$$x = a_0 + a_1 c_n + \cdots + a_{q-1}c_n^{q-1}$$

de $O_L[C_q]$. En utilisant une nouvelle fois la formule d'inversion de Fourier, on obtient

$$a_0 = (1/q)\sum_\chi \chi(x) \tag{5.20}$$

où χ parcourt les caractères de C_q.

Pour tout entier i, $0 \leq i \leq q$, $1 + v_i$ est une racine primitive p^i-ième de l'unité qu'on note $\zeta_p i$. On désigne par χ_i le caractère de C_q défini par

$$\chi_i(c_n) = \zeta_p i.$$

On a alors les égalités

$$\chi_i(x) = \hat{h}_{\gamma,n}(v_i) = \hat{h}_\gamma(v_i) = \gamma_i^{\sigma_{\pi^i}}, \quad 1 \leq i \leq n. \tag{5.21}$$

Puisque $L \supset K_{\mathfrak{p}^*}(E_{\mathfrak{p}^\infty})$ alors $L(\zeta_p i) = L(E_{\mathfrak{p}^{*i}})$, $1 \leq i \leq n$. En outre $\omega \to \omega|_{K^*_{i,\mathfrak{p}^*}}$ induit un isomorphisme de $\mathrm{Gal}(L(\zeta_p i)/L)$ sur $\mathrm{Gal}(K^*_{i,\mathfrak{p}^*}/K_{\mathfrak{p}^*})$. On a donc pour tout entier i, $1 \leq i \leq n$.

$$\chi_i^\omega(x) = (\chi_i(x))^\omega = \left(\gamma_i^{\sigma_{\pi^i}}\right)^\omega, \quad \forall \omega \in \mathrm{Gal}(L(\zeta_{p^i})/L). \tag{5.22}$$

De (5.20), (5.21) et (5.22) on obtient

$$a_0 = (1/q)\Big(\varepsilon(x) + \sum_{i=1}^{n} T_{i/0}(\gamma_i)\Big) \tag{5.23}$$

où ε est le caractère trivial de C_q.

Puisque $\varepsilon(x) = \hat{h}_{\gamma,n}(0) = \hat{h}_\gamma(0) = h_\gamma(0)$, en comparant (5.19) et (5.23) on obtient l'égalité

$$\hat{\mu}_\gamma(q\mathbb{Z}_p) = (1/q)(h_\gamma(0) - \gamma_0) + (1/q)\sum_{i=0}^{n} T_{i/0}(\gamma_i). \tag{5.24}$$

On sait que $\gamma_0 \in U_0^*(K)$, en outre c'est une norme de $K^*_{n,\mathfrak{p}^*}$ pour tout entier n, $n \geq 1$. Ainsi $\gamma_0 \equiv 1 \bmod \mathfrak{p}^{*^n}$, pour tout entier n. On conclut que $\gamma_0 = 1$.

Pour achever la démonstration de la proposition 5.5 et donc du théorème 3, il nous suffit de montrer que $h_\gamma(0) = 1$.

On reprend les notations du §2, (2.19).

LEMME 5.25. — *Soient $\gamma \in U_\infty^{*(1)}(K)$ et h_γ la série de Coleman associée. Alors :*

1) $h_{\gamma^\sigma}(X) = h_\gamma\big([\kappa^*(\sigma)](X)\big)$, $\forall \sigma \in X^*_\infty$;

2) $h_{\gamma\gamma'}(X) = h_\gamma(X)h_{\gamma'}(X)$, $\forall \gamma, \gamma'$;

3) $h_\gamma(0) \equiv 1 \bmod p$.

Démonstration. — Il suffit d'utiliser l'unicité de la série de Coleman. Puisque pour tout entier n, $n \geq 1$, on a

$$(h_\gamma(g_n^*))^\sigma = \gamma_n^\sigma = h_\gamma(g_n^{*^\sigma}) = h_\gamma([\kappa^*(\sigma)](g_n^*)),$$

on en déduit 1). L'égalité 2) se déduit du fait que

$$h_\gamma(g_n^*)h_{\gamma'}(g_n^*) = \gamma_n\gamma'_n, \quad \forall n \geq 1.$$

Enfin si $\bar{\mathfrak{p}}^*$ est l'idéal maximal de K_∞^*, on a la congruence $h_\gamma(0) \equiv h_\gamma(g_n^*) \equiv \gamma_n \equiv 1 \bmod \bar{\mathfrak{p}}^*$. Puisque $h_\gamma(0) \in K_{\mathfrak{p}^*}$, on en déduit 3). □

Soit $\gamma \in U_\infty^{*(1)}(K)$, alors on a :

$$\gamma^{p-1} = \prod_{\sigma \in X_1^*} \gamma^{\kappa_1^*(\sigma)^{-1}\sigma}$$

lorsqu'on identifie X_1^* à un sous-groupe de X_∞^*.

On déduit du lemme

$$h_\gamma^{p-1}(X) = \prod_\sigma h_{\gamma^{\kappa_1^*(\sigma)^{-1}}}([\kappa_1^*(\sigma)](X)),$$

d'où l'égalité

$$h_\gamma^{p-1}(0) = \prod_\sigma h_{\gamma^{\kappa_1^*(\sigma)^{-1}}}(0).$$

Puisque $\sum_\sigma \kappa_1^*(\sigma) = 0$, on obtient, grâce à 2) que $\prod_\sigma h_{\gamma^{\kappa_1^*(\sigma)^{-1}}}(X) = h_1(X) = 1$. Il en découle que $h_\gamma^{p-1}(0) = 1$ et grâce à 3) que $h_\gamma(0) = 1$. □

BIBLIOGRAPHIE

[AT] A. AGBOOLA et M.J. TAYLOR, Class invariants of Mordell-Weil groups, to appear.

[BT] N. BYOTT et M.J. TAYLOR, Hopf structures and Galois modules, Group rings and class groups, D.M.V. Seminar 18 (1992), Birkhaüser.

[C] R. COLEMAN, Division values in local fields, Invent. Math., 116 (1979), 91–116.

[CNT] Ph. CASSOU-NOGUÈS et M.J. TAYLOR, Structure galoisienne et courbes elliptiques, à paraître.

[CW] J. COATES et A. WILES, On the conjecture of Birch and Swinnerton-Dyer, Invent. Math., 39 (1977), 223–251.

[dS] E. de SHALIT, Iwasawa theory of elliptic curves with complex multiplication, Perspectives in Mathematics, 3 (1987), Academic Press.

[F] A. FRÖHLICH, Galois module structure of algebraic integers, Ergebnisse 3 Folge, Band 1, Springer Verlag (1983).

[L] S. LANG, Cyclotomic fields, Graduate Texts in Mathematics 59, Springer Verlag (1978).

[PR1] B. PERRIN-RIOU, Arithmétique des courbes elliptiques et théorie d'Iwasawa, Mémoire de la S.M.F., 17 (1984).

[PR2] B. PERRIN-RIOU, Descente infinie et hauteur p-adique sur les courbes à multiplication complexe, Invent. Math., 70 (1983), 369–398.

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

[ST] A. SRIVASTAV et M.J. TAYLOR, Elliptic curves with complex multiplication and Galois module structure, Invent. Math., 99 (1990), 165–184.

[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, Mordell-Weil groups and the Galois module structure of rings of integers, Illinois J. Math., 32 (1988), 428–452.

[T3] M.J. TAYLOR, Galois module structure of arithmetic principal homogeneous spaces, Journal of Algebra, Vol. 153 (1992), 203–214.

[T4] M.J. TAYLOR, Résolvandes et espaces homogènes principaux de schémas en groupe, Séminaire de Théorie des Nombres, Bordeaux 2 (1990), 255–271.

Manuscrit reçu le 15 juin 1993,
révisé le 22 mars 1994.

Ph. CASSOU-NOGUÈS,
U.F.R. de Mathématiques
et Informatique
351, cours de la Libération
33405 Talence Cedex (France)
&
M.J. TAYLOR,
Department of Mathematics
UMIST
P.O. Box 88
Manchester M60 1QD (U.K.).