COMPOSITIO MATHEMATICA

ROLAND GILLARD

Unités elliptiques et fonctions L P-adiques

Compositio Mathematica, tome 42, n° 1 (1980), p. 57-88

<http://www.numdam.org/item?id=CM_1980__42_1_57_0>

COMPOSITIO MATHEMATICA, Vol. 42, Fasc. 1, 1981, pag. 57–88

UNITÉS ELLIPTIQUES ET FONCTIONS *L P*-ADIQUES

Roland Gillard

§0. Introduction

Soient K un corps quadratique imaginaire et p un nombre premier $\neq 2$ ou 3 *se décomposant en deux facteurs premiers distincts* $\mathfrak{p}$ *et* $\mathfrak{p}'$ *dans* K; désignons par K_∞ l'unique $\mathbb{Z}_p$-extension de K qui est non ramifiée en dehors de $\mathfrak{p}$. Si F est une extension finie quelconque de K, on note F_∞ l'extension composée de K_∞ et F. Ainsi F_∞/F est encore une $\mathbb{Z}_p$-extension et est non ramifiée en dehors des diviseurs premiers de $\mathfrak{p}$ dans F. Supposons maintenant que F est une extension *abélienne* finie de K. Le but de la première partie de cet article est d'associer, pour tout caractère du groupe de Galois de F sur K, une fonction L $\mathfrak{p}$-adique relative à l'extension F_∞/F; nous utilisons une méthode voisine de celle de [16]. Cependant nous n'avons pas réussi à mener à bien cette entreprise dans le cas le plus général: nous devons supposer dans toute la suite que F/K et $\mathfrak{p}$ satisfont aux hypothèses suivantes. Notons que pour F fixé, il n'y a qu'un nombre fini d'idéaux de K, premiers de degré 1, exclus par ces hypothèses. On désigne par e le nombre de racines de 1 dans K.

HYPOTHÈSES: (i) p *est premier au nombre de classes de* K *et au degré de l'extension* F/K.

(ii) *l'indice de ramification de* $\mathfrak{p}$ *dans* F/K *divise* $(p-1)/e$.

Notre motivation pour construire ces fonctions L est le rôle qu'elles jouent dans l'étude de la $\mathbb{Z}_p$-extension F_∞/F. Pour commencer cette étude, nous établissons une formule analogue, pour nos fonctions L $\mathfrak{p}$-adiques, à celle de Leopoldt sur le *résidu de la fonction zéta p-adique* d'une extension abélienne réelle de $\mathbb{Q}$ (cf. Théorème 3). Nous donnons ensuite une condition nécessaire, en termes de *nom-*

0010-437X/81/01057-32$00.20/0

bres de Hurwitz généralisés, pour que *p divise le quotient du nombre de classes de F par celui de* $F \cap H$, où H est le corps de classes de Hilbert de K. Cependant, notre résultat arithmétique le plus profond est le théorème 4 qui interprète les fonctions L $\mathfrak{p}$-adiques construites précédemment comme *séries caractéristiques de modules d'Iwasawa associés à la* $\mathbb{Z}_p$*-extension* F_∞/F. Pour tout n entier ≥ 0, soit F_n l'unique extension de F contenue dans F_∞ et de degré p^n. Désignons par U_n le p-sous-groupe de Sylow du produit des groupes des unités pour les complétés de F_n aux diviseurs premiers de $\mathfrak{p}$. Notons C_n le sous-groupe du groupe des unités elliptiques de G. Robert, formé de celles qui sont congrues à 1 modulo les diviseurs premiers de $\mathfrak{p}$. Posons

$$Y_\infty = \varprojlim U_n/\bar{C}_n,$$

où $\bar{C}_n$ désigne la clôture de C_n dans U_n pour la topologie produit; la limite projective est définie en utilisant les normes relatives comme applications de transition. Soit Φ un caractère de $\mathrm{Gal}(F/K)$ défini et irréductible sur $\mathbb{Q}_p$. En généralisant la méthode de [6] on explicite alors la *structure de* Γ*-module* ($\Gamma = \mathrm{Gal}(F_\infty/F)$) *de la* Φ*-composante de* Y_∞ *au moyen de la fonction* L $\mathfrak{p}$*-adique associée à* Φ. L'intérêt de l'introduction et de l'étude de Y_∞ est qu'elles apportent quelques informations sur le Γ-module X_∞ suivant, module qui joue un rôle fondamental dans l'arithmétique de F_∞/F. Désignons par M_∞ la p-extension abélienne non ramifiée en dehors de $\mathfrak{p}$ maximale de F_∞: alors $X_\infty = \mathrm{Gal}(M_\infty/F_\infty)$, Γ agissant par automorphismes intérieurs dans $\mathrm{Gal}(M_\infty/F)$. La conjecture principale sur le sujet, dont semble-t-il on est encore loin de la démonstration, affirme que les Φ-composantes de X_∞ et de Y_∞, considérés comme Γ-modules ont mêmes séries caractéristiques. Le corollaire 2 du théorème 3 donne un résultat nouveau mais très partiel dans cette direction.

Pour finir cette introduction, rappelons certains résultats déjà connus. Des fonctions L $\mathfrak{p}$-adiques ont déjà été construites dans [2], [12], [13], [16], [18] sous des hypothèses variées mais nous n'y avons pas trouvé de références commodes pour les formules du théorème 2 ci-dessous, formules essentielles pour nos applications arithmétiques. Robert [21], a prouvé un critère de divisibilité (cf. aussi [5]) pour le nombre de classes du corps de rayon modulo $\mathfrak{p}$ de K (contenant même le cas où p est inerte dans K). Enfin, Coates et Wiles [6], ont étudié la structure de Y_∞ pour K principal et F engendré sur K par les coordonnées des points de $\mathfrak{p}$-torsion sur une courbe elliptique

admettant l'anneau des entiers de K comme anneau d'endomorphismes.

Il est clair que cet article doit beaucoup aux exposés et publications de J. Coates. Je tiens aussi à remercier P. Cassou-Noguès: une version préliminaire de [2] m'a été utile en plusieurs endroits.[1] Enfin la théorie des unités locales repose sur une généralisation du résultat de [7] due à J.-P. Wintenberger, cf. §2.2 ci dessous.

§1. Généralités

Si $\mathfrak{f}$ est un idéal entier de K, on note $H_{\mathfrak{f}}$ (resp. $\mathrm{Cl}(\mathfrak{f})$) le corps (resp. le groupe) de classes de rayon modulo $\mathfrak{f}$ de K. On pose $H = H_{(1)}$. On choisit un prolongement v de la valuation $\mathfrak{p}$-adique à K^{ab}, l'extension abélienne maximale de K. Pour toute extension abélienne L de K, on note $h(L)$ le nombre de classes, $\mathcal{O}(L)$ l'anneau des entiers de L. On désigne par L^v le complété de L correspondant à v et $\mathcal{O}^v(L)$ son anneau d'entiers. On identifie K^v à $\mathbb{Q}_p$ et on note A' l'anneau des entiers du complété $\hat{\mathbb{Q}}_p^{nr}$ de l'extension non ramifiée maximale de $\mathbb{Q}_p$. Notons Ω_p (resp. $\bar{\mathbb{Q}}$) une clôture algébrique de $\mathbb{Q}_p$ (resp. de $\mathbb{Q}$); soit $\mathbb{C}_p$ le complété de Ω_p: on suppose que $\mathcal{O}(\mathbb{C}_p)$, l'anneau des entiers de $\mathbb{C}_p$ contient A'. On choisit deux plongements i_∞ et $i_\mathfrak{p}$ de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$ et $\mathbb{C}_p$, $i_\mathfrak{p}$ étant compatible avec le plongement de K^{ab} dans $\mathbb{C}_p$ défini par v. Pour tout groupe fini X, on note $[X]$ son ordre.

Soit E une courbe elliptique définie sur $\mathcal{O}(H)$, d'invariant égal à celui du réseau $\mathcal{O}(K)$ de $\mathbb{C}$, cf. [23] théorème 5.7. On choisit un modèle d'équation $y^2 = 4x^3 - g_2 \cdot x - g_3$ avec g_2 et g_3 dans $\mathcal{O}(H)$; le nombre complexe z correspond au point $\xi(z) = (\wp(z, \mathcal{L}), \wp'(z, \mathcal{L})) = (x, y)$ par le paramétrage de Weierstrass, le réseau $\mathcal{L}$ étant de la forme $\Omega_\infty \cdot \mathcal{O}(K)$ avec $\Omega_\infty \in \mathbb{C}$. Si $\alpha \in \mathcal{O}(K)$, on lui fait correspondre l'endomorphisme de E défini par $\xi(z) \to \xi(\alpha z)$. On désigne par ψ le "Grössencharacter" de E sur H et par $\mathcal{F}$ son conducteur, cf. [23] §7.8. D'après [22] §6 th.9 cor.1, on peut supposer que E a bonne réduction pour les diviseurs premiers de p dans H, et même, pour un choix convenable du modèle, que p est premier au discriminant $g_2^3 - 27g_3^2$; p est alors premier à $\mathcal{F}$. Si $\mathfrak{B}$ est un idéal entier de K, $E_\mathfrak{B}$ désigne le groupe des points de $\mathfrak{B}$-torsion de E, i.e. les $\xi(u)$ avec $u\mathfrak{B} \subset \Omega_\infty \cdot \mathcal{O}(K)$. L'extension $H(E_\mathfrak{B})$ engendrée sur H par les coordonnées de ces points est incluse dans H^{ab}, l'extension abélienne maximale de H; $H(E_\mathfrak{B})$ contient $H_\mathfrak{B}$, cf. [23] théorème 5.5. Pour $\mathfrak{U}$

[1] Notamment pour le rôle des sommes de Gauss au §3.4.

idéal de H, notons $[\mathfrak{U}, H(E_{\mathfrak{B}})/H]$ l'automorphisme d'Artin pour l'extension $H(E_{\mathfrak{B}})/H$ associé à $\mathfrak{U}$; on adopte une notation analogue pour les extensions abéliennes de K ou de H. En agissant sur les coordonnées, l'automorphisme ci-dessus opère sur un point de $E_{\mathfrak{B}}$ par:

$$[\mathfrak{U}, H(E_{\mathfrak{B}})/H] \cdot \xi(\rho) = \xi(\psi(\mathfrak{U})\rho), \text{ pour } \mathfrak{U} \text{ premier à } \mathfrak{B} \text{ et } \mathfrak{F}, \tag{1}$$

cf. [23] prop. 7.40. On sait que si $\mathfrak{U}$ est un idéal de H, sa norme dans K est l'idéal principal engendré par $\psi(\mathfrak{U})$, cf. [23] prop. 7.40 et 7.41. Ainsi, si $\mathfrak{P}_H$ est l'idéal de H au dessus de $\mathfrak{p}$ correspondant à v, posons $t = \psi(\mathfrak{P}_H)$: c'est un générateur de l'idéal $\mathfrak{p}^f$, où f désigne le degré résiduel en $\mathfrak{p}$ de H/K.

Si a est un élément inversible de $\mathcal{O}^v(K) \simeq \mathbb{Z}_p$, on le décompose en un produit $a = \omega(a).\langle a\rangle$, avec $\omega(a)$ racine de 1 d'ordre divisant $p-1$ et $\langle a\rangle$ dans $1+p\mathbb{Z}_p$. On voit, cf. (1) que $\omega_H = \omega \circ i_{\mathfrak{p}} \circ \psi$ définit un caractère sur $\mathrm{Gal}(H(E_{\mathfrak{p}})/H)$. Comme $H(E_{\mathfrak{p}})$ est une extension de $H_{\mathfrak{p}}$ de degré e, on déduit que ω_H^e provient d'un élément, en fait générateur, du groupe des caractères de $\mathrm{Gal}(H_{\mathfrak{p}}/H)$. On en choisit une fois pour toutes[1] un prolongement à $\mathrm{Gal}(H_{\mathfrak{p}}/K)$ qu'on note ω^e et on définit par multiplicativité ω^k pour $k \in e\mathbb{Z}$.

Notons Δ le groupe de Galois de F/K. Soient $\Phi \neq 1$, un caractère de Δ défini et irréductible sur $\mathbb{Q}_p$ et e_Φ l'idempotent correspondant dans $\mathbb{Z}_p[\Delta]$. Choisissons un facteur φ de la décomposition de Φ sur Ω_p et désignons par A le sous-anneau de A' engendré par les valeurs de φ. En prolongeant φ à $\mathbb{Z}_p[\Delta]$, on obtient un isomorphisme

$$e_\Phi \mathbb{Z}_p[\Delta] \xrightarrow{\sim} A. \tag{2}$$

D'après §0 hypothèse (i) le conducteur de φ est de la forme $\mathfrak{g}$ ou $\mathfrak{g}\mathfrak{p}$, avec $\mathfrak{g}$ idéal de K premier à $\mathfrak{p}$. Si F^φ désigne la sous-extension de F/K correspondant au noyau de φ, l'ordre du groupe d'inertie de $\mathfrak{p}$ dans $H_{\mathfrak{q}} \cdot F^\varphi/H_{\mathfrak{q}}$ divise $(p-1)/e$, cf. §0 hypothèse (ii). Comme l'extension $H_{\mathfrak{q}\mathfrak{p}}/H_{\mathfrak{q}}$ est cyclique et que $[H_{\mathfrak{q}} \cdot H_{\mathfrak{p}} : H_{\mathfrak{q}}] = [H_{\mathfrak{p}} : H] = (p-1)/e$, on en déduit l'inclusion $F^\varphi \subset H_{\mathfrak{q}} \cdot H_{\mathfrak{p}}$. Ainsi φ considéré comme caractère de $\mathrm{Gal}(H_{\mathfrak{g}} \cdot H_{\mathfrak{p}}/K)$ peut s'écrire comme produit d'un caractère provenant de $\mathrm{Gal}(H_{\mathfrak{p}}/K)$ et d'un caractère provenant de $\mathrm{Gal}(H_{\mathfrak{q}}/K)$. En posant

$$\varphi_k = \varphi \cdot \omega^{-k} \text{ pour } k \in e\mathbb{Z},$$

[1] Ce prolongement ne joue qu'un rôle très secondaire dans la suite, cf. §3.4 Remarque 3.

on obtient qu'il existe un unique i, $0 < i < p$ tel que le conducteur de φ_i soit premier à $\mathfrak{p}$: il vaut $\mathfrak{g}$. Dans la suite, on identifie caractères de Dirichlet et caractères de groupes de Galois: par exemple φ_i est aussi considéré comme un caractère sur $Cl(\mathfrak{g})$.

En raisonnant comme plus haut, on montre que le conducteur de F/K est de la forme $\mathfrak{f}$ ou $\mathfrak{f}\mathfrak{p}$, avec $\mathfrak{f}$ premier à $\mathfrak{p}$ et que F est contenue dans $H_{\mathfrak{f}} \cdot H_{\mathfrak{p}}$.

En utilisant le fait que p ne divise pas $h(K)$ pour extraire des racines d'ordre $h(K)$ dans $1 + p\mathbb{Z}_p$, on pose pour $k \in e\mathbb{Z}$ et $\mathfrak{B}$ idéal de K premier à $\mathfrak{F}$

$$\psi^k(\mathfrak{B}) = \langle i_{\mathfrak{p}} \circ \boldsymbol{\psi}(\mathfrak{B} \cdot \mathcal{O}(H)\rangle^{k/h(K)} \cdot \boldsymbol{\omega}^k(\mathfrak{B})$$
$$\langle \psi(\mathfrak{B})\rangle = \langle i_{\mathfrak{p}} \circ \boldsymbol{\psi}(\mathfrak{B} \cdot \mathcal{O}(H)\rangle^{1/h(K)}.$$

Cette formule définit ψ^k comme grössencharacter sur K à valeurs dans une extension finie non ramifiée de K^v (cf. valeurs de $\boldsymbol{\omega}^k$). De plus si $\mathfrak{B}$ est principal engendré par $b \in K$, c'est la norme d'un idéal $\mathfrak{U}$ de H: les éléments $\boldsymbol{\psi}(\mathfrak{B} \cdot \mathcal{O}(H))$ et $\boldsymbol{\psi}(\mathfrak{U})^{h(K)}$ (resp. $\boldsymbol{\psi}(\mathfrak{U})$ et b) de K engendrent le même idéal $\mathfrak{B}^{h(K)}$ (resp. $\mathfrak{B}$) de K; leurs puissances d'ordre e sont égales et on a

$$i_{\mathfrak{p}}^{-1}\psi^k(\mathfrak{B}) = \boldsymbol{\psi}^k(\mathfrak{U}) = b^k, \tag{3}$$

si bien que ψ^k $(k \in e \cdot \mathbb{Z})$ a pour conducteur l'idéal $\mathcal{O}(K)$; on peut aussi vérifier que ses valeurs sont algébriques: leurs images par $i_{\mathfrak{p}}^{-1}$ sont dans une extension finie de K puisque d'exposant borné et non ramifiée en dehors des diviseurs premiers de $h(K)$. Le grössencharacter ψ^e permet d'obtenir les caractères du groupe $\mathrm{Gal}(K_n/K)$:

LEMME 1: *Soient n un entier et π un caractère de $\mathbb{Z}_p^*$ d'ordre p^n; alors $\pi \circ \psi^e$ est un générateur du groupe des caractères de* $\mathrm{Gal}(K_n/K)$.

DÉMONSTRATION: Si a est un élément de $\mathcal{O}(K)$ premier à $\mathfrak{F}$, on a

$$\pi \circ \psi^e((a)) = \pi \circ i_{\mathfrak{p}}(a)^e,$$

ce qui prouve que $\pi \circ \psi^e$ est un caractère de Dirichlet de conducteur $\mathfrak{p}^{n+1}$ et d'ordre p^n. Le lemme résulte alors du fait que K_n/K est l'unique sous-extension de degré p^n de $H_{\mathfrak{p}^{n+1}}/K$.

§2. Unités locales et semi-locales

2.1. *Unités semi-locales*

Soit S l'ensemble fini des places de F_∞ au dessus de $\mathfrak{p}$: S contient la restriction de v, encore notée v. Pour $w \in S$ désignons par F_n^w le complété de F_n correspondant, $\mathcal{O}^w(F_n)$ l'anneau des entiers de F_n^w et U_n^w le p-groupe de Sylow du groupe des unités de F_n^w. En utilisant les normes relatives comme applications de transition, on considère

$$U^v = \varprojlim U_n^v \text{ et } U = \varprojlim U_n \text{ avec } U_n = \prod_{w \in S} U_n^w.$$

Soient c un générateur du groupe multiplicatif $1 + p\mathbb{Z}_p$ et γ le générateur de $\mathrm{Gal}(F_\infty/F)$ qui est la restriction à F_∞ de l'automorphisme de $\mathrm{Gal}(H(E_\mathfrak{p}) \cdot F_\infty/H(E_\mathfrak{p}) \cdot F)$ défini par $\xi(\rho) \to \xi(c\rho)$, pour tout point de $\mathfrak{p}^n$-torsion $\xi(\rho)$, n quelconque dans $\mathbb{N}$, de E. Comme U est un $\mathrm{Gal}(F_\infty/K)$-module compact, on peut le considérer comme un $\mathbb{Z}_p[\Delta][[T]]$-module de type fini: Δ opère via l'isomorphisme $\Delta \simeq \mathrm{Gal}(F_\infty/K_\infty)$ et l'action de γ se prolonge aux séries formelles en identifiant γ et $1 + T$; on adopte des notations additives pour U et les modules qui lui sont liés. Ce qui précède permet de considérer la Φ-partie $e_\Phi U$ de U comme un $A[[T]]$-module cf. (2). La proposition suivante est démontrée un peu plus loin.

PROPOSITION 1: *Le $A[[T]]$-module $e_\Phi U$ est libre de rang* 1.

Soient D le groupe de décomposition de $\mathfrak{p}$ dans F/K, φ_D la restriction de φ à D, Φ_D la somme de ses conjugués sur $\mathbb{Q}_p$ et A_D le sous-anneau de A engendré par les images de φ_D. On a un isomorphisme de $\mathbb{Z}_p[\mathrm{Gal}(F_n/K)]$-modules,

$$U_n \simeq U_n^v \otimes_{\mathbb{Z}_p[D]} \mathbb{Z}_p[\Delta],$$

d'où en utilisant (2) et un isomorphisme analogue avec D et Φ_D

$$e_\Phi U_n \simeq (e_{\Phi_D} U_n^v) \otimes_{A_D} A;$$

soit encore en passant à la limite projective,

$$e_\Phi U \simeq (e_{\Phi_D} U^v) \otimes_{A_D} A \tag{4}$$

puisque A est un A_D-module libre de type fini. Ceci ramène l'étude de $e_\Phi U$ à celle de $e_{\Phi_D} U^v$.

Soient $X_n = (F_n^v)^*$ et $X_n = \varprojlim X_n/p^m X_n$ (avec des notations additives!) son complété p-adique. La valuation fournit une suite exacte

$$0 \to U_n^v \to \hat{X}_n \to \mathbb{Z}_p \to 0. \tag{5}$$

D'où à la limite projective en posant $\hat{X} = \varprojlim \hat{X}_n$ (avec des applications de transition déduites des normes relatives):

$$0 \to U^v \to \hat{X} \to \mathbb{Z}_p \to 0. \tag{6}$$

Notons maintenant le résultat suivant:

LEMME 2: *Le $\mathbb{Z}_p$-module $e_{\Phi_D}\hat{X}$ est sans torsion.*

DÉMONSTRATION: Supposons le contraire et soit F_φ la sous-extension de F/K correspondant au noyau de φ. Alors F_φ^v contient les racines de l'unité d'ordre p, donc $p-1$ divise l'indice de ramification de $\mathfrak{p}$ dans F/K, contrairement à l'hypothèse (ii) du §0.

On voit alors en raisonnant comme dans [11]th.25, que $e_{\Phi_D}\hat{X}$ est un $A_D[[T]]$-module libre de rang 1; on déduit alors, cf. (6)

$$e_{\Phi_D}U^v = \begin{cases} e_{\Phi_D}\hat{X} & \text{si } \varphi_D \neq 1 \\ T \cdot e_{\Phi_D}\hat{X} & \text{si } \varphi_D = 1. \end{cases} \tag{7}$$

Ainsi $e_{\Phi_D}U^v$ est un $A_D[[T]]$-module libre de rang 1, et la proposition résulte alors de (4).

Soit V_n (resp. V_n^v, resp. $\hat{X}_n'$) l'intersection des images des U_m (resp. U_m^v, resp. $\hat{X}_m$) avec $m \geq n$ pour les applications de normes relatives. Notons ω_n la série $(1+T)^{p^n} - 1$.

PROPOSITION 2: *Pour n dans $\mathbb{N}$, on a $e_\Phi V_n \simeq e_\Phi(U/(\omega_n/T)\cdot U)$ si $\varphi(\mathfrak{p}) = 1$ et $e_\Phi U_n = e_\Phi V_n \simeq e_\Phi(U/\omega_n \cdot U)$ sinon.*

DÉMONSTRATION: La condition $\varphi(\mathfrak{p}) = 1$ signifie simplement que φ_D est trivial. On vérifie à l'aide du théorème 90 de Hilbert que $\hat{X}_n'$ est isomorphe à $\hat{X}/\omega_n\hat{X}$. A l'aide de (5) et (6), on en déduit l'isomorphisme entre V_n^v et $U^v/\omega_n\hat{X}$, d'où la proposition d'après (4) et (7).

2.2. *Unités locales et séries formelles* (d'après J.-P. Wintenberger)

Soit $L/\mathbb{Q}_p$ une extension finie: on note $\mathcal{O}(L)$ et $\mathfrak{M}_L$ l'anneau des

entiers et l'idéal maximal de L; on emploie des notations analogues pour tout corps local. Soit G une loi de groupe formel définie sur $\mathcal{O}(L')$, avec L' sous-extension de $L/\mathbb{Q}_p$. On note $X +_G Y$ la série formelle à deux variables donnant la loi de groupe sur G.

Il s'agit ici de généraliser les résultats de R. Coleman [7] à une situation incluant le complété formel $\hat{E}$ à l'origine de la courbe elliptique E: Coleman supposait que G est de type Lubin–Tate.[1] Ainsi, on suppose

(i) qu'il existe un plongement $a \to [a]$ de $\mathcal{O}(L'')$, avec L'' sous-extension de $L'/\mathbb{Q}_p$, dans l'anneau des endomorphismes de G sur $\mathcal{O}(L')$;

(ii) que la hauteur de G est égale à $[L'':\mathbb{Q}_p]$;

(iii) qu'il existe $t \in \mathfrak{M}_{L''}$ tel que la série $[t](X)$ soit congrue à $X^{p^f} \bmod \mathfrak{M}_{L'}$, où f est le degré résiduel de L'; on pose $q = p^f$;

(iv) que l'extension L/L'' est non ramifiée.

On choisit alors une suite d'éléments de $\mathfrak{M}_{\Omega_p}$ vérifiant $[t]\pi_n = \pi_{n-1}$, avec $\pi_0 \neq 0$ point de torsion de G, et on pose $L_n = L[\pi_n]$. On désigne par U_n le groupe des unités de L_n et on considère $u = (u_n)_{n\in\mathbb{N}}$ un élément de $U = \varprojlim U_n$, les applications de transition étant les normes relatives. Soit Frob le Frobenius de $\widehat{Q_p^{nr}}/L'$; il agit sur toute série $f(T)$ dans $\mathcal{O}(L)[[T]]$ par action sur les coefficients; on note $f^{\mathrm{Frob}^{-n}}(T)$ l'image de $f(T)$ par Frob^{-n}.

THÉORÈME 1: *Il existe une série entière unique $f_u(T)$ à coefficients dans $\mathcal{O}(L)$* avec

$$u_n = f_u^{\mathrm{Frob}^{-n}}(\pi_n) \quad \text{pour tout } n \in \mathbb{N}.$$

La démonstration de J.-P. Wintenberger reprend les grandes lignes de celle de [7]; énonçons d'abord les lemmes suivants; soient G_t le groupe des points de t-torsion de G et L_t l'extension de L engendrée par les b dans G_t. Notons $\mathcal{A}$ (resp. $\mathcal{A}_t$) l'anneau $\mathcal{O}(L)[[X]]$ (resp. $\mathcal{O}(L_t)[[X]]$) et $\mathfrak{M}_{\mathcal{A}}$ son idéal maximal.

LEMME 3: *Soient $e_j \in \mathbb{Z}[X_0, \ldots, X_{q-1}], 0 \leq j < q$, les polynômes symétriques élémentaires définis par l'identité*

$$\prod_{j=0}^{q-1} (T - X_j) = T^q + \sum_{j=0}^{q-1} e_j \cdot T^j;$$

[1] En fait $\hat{E}$ est de type Lubin–Tate sur $\mathcal{O}^v(H)$ si et seulement si $\mathfrak{p}$ est un idéal principal de K.

alors pour tout $f(X) \in \mathcal{A}$, il existe une série formelle H_f dans $\mathcal{O}(L)$ $[[X_0, \ldots, X_{q-1}]]$ telle que la série $\Pi_{j=0}^{q-1} f(X_j)$ soit égale à la série composée $H_f(e_0, \ldots, e_{q-1})$.

DÉMONSTRATION: On se ramène au cas classique où $f(X)$ est un polynôme en utilisant le fait que e_j est de poids $q-j>0$. Le lemme suivant est la clef de la démonstration du théorème.

LEMME 4: *Il existe une application $\mathcal{N}$ de $\mathcal{A}$ dans $\mathcal{A}$, induisant un homomorphisme sur le groupe multiplicatif des unités de $\mathcal{A}$, et telle que pour tout $f \in \mathcal{A}$, on ait l'identité*

$$\mathcal{N}(f)([t]X) = \prod_{b \in G_t} f(X +_G b)$$

DÉMONSTRATION: Appliquons le lemme de préparation de Weierstrass à la série formelle $[t]T - X \in \mathcal{A}[[T]]$; le premier coefficient non dans $\mathfrak{M}_{\mathcal{A}}$ est celui de T^q, si bien que l'on peut écrire

$$[t]T - X = P(X, T) \cdot U(T),$$

avec $P(X, T) \in \mathcal{A}[T]$, polynôme de degré q et $U(T)$ unité dans $\mathcal{A}[[T]]$. On déduit de l'identité précédente que

$$P([t]X, T) = \prod_{b \in G_t} [T - (X +_G b)].$$

On pose

$$\mathcal{N}(f)(X) = H_f(e_0(X), \ldots, e_{q-1}(X)),$$

avec $e_j(X)$ coefficient de T^j dans $P(X, T)$; la série $\mathcal{N}(f)(X)$ est bien définie car $e_j(X)$ est dans $\mathfrak{M}_{\mathcal{A}}$. La formule du lemme 4 résulte alors du lemme 3 en spécialisant les X_j en les $X +_G b \in \mathcal{A}_t$, où b parcourt G_t.

Soient $f(X) = \Sigma\, a_i \cdot X^i$ et $f'(X) = \Sigma\, a'_i \cdot X^i$ deux éléments de $\mathcal{A}$. On note $f \equiv f' \bmod \mathfrak{M}_L^k (k \in \mathbf{N})$ pour $a_i \equiv a'_i \bmod \mathfrak{M}_L^k$ pour tout i.

DÉMONSTRATION DU THÉORÈME 1: En remplaçant t par une puissance convenable de l'uniformisante de L'', on vérifie que π_n est une uniformisante de L_n. Ceci permet d'introduire des séries f_n, telles que

$$u_n = f_n^{\mathrm{Frob}^{-n}}(\pi_n).$$

Comme u_n est la norme entre L_{n+1} et L_n de u_{n+1}, on obtient

$$f_n(\pi_n) = \mathcal{N}(f_{n+1}^{\mathrm{Frob}^{-1}})(\pi_n).$$

En posant $g_n = \mathcal{N}^n(f_{2n})^{\mathrm{Frob}^{-n}}$, on trouve

$$u_n = \mathcal{N}^{m-n}(g_m^{\mathrm{Frob}^{-m}})(\pi_n).$$

La suite des g_n admet un point d'accumulation $f \in \mathcal{A}^*$. En utilisant les implications (cf. [7] lemme 13) pour $h \in \mathcal{A}$

(i) $h \in \mathcal{A}^* \Rightarrow \mathcal{N}(h)/h^{\mathrm{Frob}} \equiv 1 \bmod \mathfrak{M}_L$

(ii) $h \equiv 1 \bmod \mathfrak{M}_L^k \Rightarrow \mathcal{N}(h) \equiv 1 \bmod \mathfrak{M}_L^{k+1}$,

on déduit $\mathcal{N}^{m-n}(g_m^{\mathrm{Frob}^{-m}}) \equiv g_m^{\mathrm{Frob}^{-n}} \bmod \mathfrak{M}_L^m$. Ceci prouve, pour n fixé, qu'une sous-suite de $(\mathcal{N}^{m-n}(g_m^{\mathrm{Frob}^{-m}})(\pi_n))_{m\in\mathbb{N}}$ admet $f^{\mathrm{Frob}^{-n}}(\pi_n)$ comme limite. On a donc bien

$$u_n = f^{\mathrm{Frob}^{-n}}(\pi_n),$$

ce qui prouve le théorème en prenant $f_u = f$; l'unicité signalée provient immédiatement du théorème de préparation de Weierstrass.

2.3. *Mesures associées aux éléments de* U^v

Pour construire les fonctions L $\mathfrak{p}$-adiques, nous allons utiliser la transformation Γ de Leopoldt, exprimée suivant N. Katz en termes de mesures sur $\mathbb{Z}_p$, cf. [15] chap. 4 et [19]. Regroupons quelques propriétés et définitions.

Si X est un espace topologique compact, on note $\mathrm{Cont}(X, \mathcal{O}(C_p))$ le $\mathcal{O}(C_p)$-module des applications continues de X dans $\mathcal{O}(C_p)$.

M.0. Une mesure sur X à valeurs dans $\mathcal{O}(C_p)$ est une forme linéaire bornée sur $\mathrm{Cont}(X, \mathcal{O}(C_p))$: si $f \in \mathrm{Cont}(X, \mathcal{O}(C_p))$ et si μ est une mesure on note $\int_X f(x)\mu(x)$ l'image de f par μ.

M.1. Pour toute série formelle $F(T) \in \mathcal{O}(C_p)[[T]]$ il existe une unique mesure μ^F sur $\mathbb{Z}_p$ à valeurs dans $\mathcal{O}(C_p)$, telle que

$$\int_{\mathbb{Z}_p} x^k \mu^F(x) = (D^k F)(0) \quad \text{pour tout } k \in \mathbb{N},$$

où D est la dérivation sur $\mathcal{O}(C_p)$ définie par $(DF)(T) = (1+T)\cdot F'(T)$. Toute mesure sur $\mathbb{Z}_p$ est de la forme μ^F pour une unique série F.

M.2. Pour tout z dans l'idéal maximal de $\mathcal{O}(C_p)$, on a

$$\int_{Z_p} (1+z)^x \mu^F(x) = F(z).$$

M.3. Soit $\epsilon \in \mathrm{Cont}(Z_p, \mathcal{O}(C_p))$ périodique; si p^n est une période de ϵ, posons

$$G(T) = \sum \hat{\epsilon}(\zeta) F(\zeta(1+T)-1),$$

somme prise sur les racines p^n-ièmes de 1, avec

$$\hat{\epsilon}(\zeta) = \frac{1}{p^n} \sum \epsilon(j)\zeta^{-j}$$

On a alors $\int_{Z_p} x^k \epsilon(x) \mu^F(x) = \int_{Z_p} x^k \mu^G(x)$.

M.4. Pour $f \in \mathrm{Cont}(Z_p^*, \mathcal{O}(C_p))$, on note $\tilde{f} \in \mathrm{Cont}(Z_p, \mathcal{O}(C_p))$ son prolongement qui vaut 0 sur pZ_p. En posant

$$\int_{Z_p^*} f(x)\mu(x) = \int_{Z_p} \tilde{f}(x)\mu(x),$$

on associe à toute mesure sur Z_p une mesure sur Z_p^*; on a alors, en notant encore f la restriction de $f \in \mathrm{Cont}(Z_p, \mathcal{O}(C_p))$,

$$\int_{Z_p^*} f(x)\mu^F(x) = \int_{Z_p} f(x)\mu^{\tilde{F}}(x) \quad \text{avec}$$

$$\tilde{F}(T) = F(T) - \frac{1}{p} \sum F(\zeta(1+T)-1),$$

où la somme est prise sur les racines p-ièmes de 1.

M.5. (i) Soit $F(T) \in \mathcal{O}(C_p)[[T]]$, il existe une unique série $G \in \mathcal{O}(C_p)[[T]]$ vérifiant $DG = \tilde{F}$ et $\tilde{G} = G$.

(ii) on a alors $\int_{Z_p^*} x^{-1} \mu^F(x) = G(0)$.

On peut remplacer $\mathcal{O}(C_p)$ par A' (ou par l'anneau des entiers d'un corps local) dans ce qui précède.

Soit G le groupe formel défini sur $\mathcal{O}^v(H)$, complété formel de E à l'origine. On paramètre G grâce à $W = -2x/y$, ainsi $x(W) = W^{-2} \cdot a(W)$, $y(W) = -2W^{-3} \cdot a(W)$, où $a(W) = 1 + \cdots$ désigne une série formelle à coefficients dans $\mathcal{O}^v(H)$. Désignons par $\exp_G$(resp. λ) l'exponentielle (resp. le logarithme) de G, par $W_1 +_G W_2$ la série donnant l'addition sur G et par $[a](W)$ celle donnant la multiplication par $a \in Z_p$. On a donc les égalités de séries formelles

$$x(\exp_G z) = \wp(z) \text{ et } y(\exp_G z) = \wp'(z).$$

Pour $n \in \mathbf{N}$, choisissons $\rho_n \in \mathbf{C}$ tel que $\xi(\rho_n)$ soit dans $E_{\mathfrak{p}^n}$ et non dans $E_{\mathfrak{p}^{n-1}}$, pour $n \geq 1$. Soit $w_n \in \Omega_p$ le nombre tel que

$$i_\infty^{-1}(\xi(\rho_n)) = i_\mathfrak{p}^{-1}(x(w_n), y(w_n)).$$

On suppose vérifiée la relation de compatibilité *t.* $\rho_{n+f} = \rho_n$ (*t* comme après (1)) d'où $[t]w_{n+f} = w_n$. Soit $u = (u_n)_{n\in\mathbf{N}}$, un élément de U^v: on peut lui appliquer le théorème 1 pour trouver une série $F_u(W)$ à coefficients dans $\mathcal{O}^v(H_\mathfrak{f})$, $\mathfrak{f}$ comme au milieu du §1, telle que

$$u_{nf+1} = F_u^{\mathrm{Frob}^{-n}}(w_{nf+1}),$$

Frob désignant le Frobenius de $\hat{Q}_p^{nr}/H^v$.

Comme G est de hauteur 1, on sait, cf. [17] cor 4.3.3, qu'il existe un isomorphisme η défini sur A', avec le groupe multiplicatif G_m muni du paramètre usuel noté V. En posant $\Omega_\mathfrak{p} = \eta'(0)^{-1}$, unité de A', on a une égalité de séries formelles

$$\exp_G(z) = \eta(e^{\Omega_\mathfrak{p} \cdot z} - 1).$$

Introduisons alors les séries

$$f_u(W) = \left(\frac{d}{dz}\right) \log F_u(W) = \frac{F_u'(W)}{F_u(W) \cdot \lambda'(W)} \in \mathcal{O}^v(H_\mathfrak{f})[[W]]$$
$$g_u(V) = f_u \circ \eta(V) \in A'[[V]].$$

Notons μ_u la mesure μ^F de **M.1** avec $F = \Omega_\mathfrak{p}^{-1} \cdot g_u$; de **M.1** et **M.4**, on déduit

$$\int_{Z_p^*} x^{k-1} \mu_u(x) = \Omega_\mathfrak{p}^{-1} \left(\frac{d}{dz}\right)_{z=0}^{k-1} \tilde{g}_u(e^z - 1) \quad (k \geq 1).$$

Par ailleurs, on a

$$\tilde{g}_u(e^{\Omega_\mathfrak{p} \cdot z} - 1) = f_u(\exp_G z) - \frac{1}{p} \sum f_u(\exp_G z +_G b)$$

où b parcourt le groupe G_p des points de p-torsion de G. On vérifie, cf. [15] p. 214

$$\frac{d}{dz}(\log F_u(\exp_G z +_G b)) = f_u(\exp_G z +_G b) \quad \text{si } b \in G_p.$$

LEMME 5: *Pour k entier ≥ 0, on a*

$$\int_{Z_p^*} x^{k-1}\mu_u(x) = \Omega_{\mathfrak{p}}^{-k}\left(\frac{d}{dz}\right)^k_{z=0}\left[\log F_u(\exp_G z) - \frac{1}{p}\sum_{b\in G_p}\log F_u(\exp_G z +_G b)\right]$$

DÉMONSTRATION: La formule résulte de **M.1** et **M.4** si $k>0$. Si $k=0$, on doit considérer la série $h_u(V) = \log \circ F \circ \eta(V)$, série à coefficients dans $\widehat{Q_p^{nr}}$, définie à l'aide du logarithme p-adique et convergente sur l'idéal maximal de Ω_p: $\tilde{h}_u$, définie à partir de h_u par la formule de **M.4** est solution du système $DG = \Omega_{\mathfrak{p}}^{-1} g_u$, $\tilde{G} = G$. D'après le résultat d'unicité de [19] lemme 8.15 et d'après **M.5**(i) on a $\tilde{h}_u(V) \in A'[[V]]$. La formule du lemme 5 pour $k=0$ est exactement celle de **M.5**(ii).

Notons $\Delta_k^v(u)$ le deuxième membre de l'égalité du lemme 5.

LEMME 6: *Soit i un entier, $0<i<p$, il existe une série unique $G_u^i(T) \in A'[[T]]$ telle que pour tout $k \geq 0$, $k \equiv i \bmod(p-1)$ on ait*

$$G_u^i(c^k - 1) = \Delta_k^v(u).$$

DÉMONSTRATION: Reprenons les arguments de [19]: définissons pour $x \in Z_p^*$, $l(x) \in Z_p$ par $\langle x\rangle = c^{l(x)}$. On peut alors définir une mesure sur Z_p, μ_u^i, à valeurs dans A' en posant pour $f \in \mathrm{Cont}(Z_p, A')$

$$\int_{Z_p} f(x)\cdot\mu_u^i(x) = \int_{Z_p^*} f(l(x))\cdot\omega^i(x)\cdot x^{-1}\cdot\mu_u(x).$$

D'après **M.2**, la série $G_u^i(T) \in A'[[T]]$ associée par **M.1** à μ_u^i vérifie

$$G_u^i(c^s - 1) = \int_{Z_p} c^{xs}\mu_u^i(x) = \int_{Z_p^*}\langle x\rangle^s\cdot\omega^i(x)\cdot x^{-1}\cdot\mu_u(x),$$

pour tout $s \in Z_p$, d'où le résultat.

LEMME 7: *Si π est un caractère de Z_p^*, d'ordre une puissance de p, on a pour tout $k \in \mathbf{N}$:*

$$G_u^i(\pi(c)\cdot c^k-1)=\int_{Z_p^*} x^{k-1}\cdot\pi(x)\cdot\omega^{i-k}(x)\cdot\mu_u(x).$$

DÉMONSTRATION: On peut écrire $\pi(x)=\pi(c)^{l(x)}$, d'où d'après la définition de μ_u^i:

$$\int_{Z_p^*} x^{k-1}\cdot\pi(x)\cdot\omega^{i-k}(x)\mu_u(x)=\int_{Z_p}(\pi(c)\cdot c^k)^x\mu_u^i(x),$$

et le lemme résulte de **M.3.**

Soit ϵ un homomorphisme de $(Z/p^nZ)^*$, n entier >0, dans Ω_p^*; ϵ définit une application périodique de $\mathbb{Z}_p$ dans Ω_p, nulle sur $p\mathbb{Z}_p$. Notons ζ_n, la racine primitive $\eta^{-1}(w_n)$ d'ordre p^n de 1.

LEMME 8: *Pour tout k dans* $\mathbb{N}$,

$$\int_{Z_p^*} x^{k-1}\cdot\epsilon(x)\cdot\mu_u(x)=\Omega_{\mathfrak{p}}^{-k}\cdot\hat{\epsilon}(\zeta_n)\cdot\left(\frac{d}{dz}\right)_{z=0}^k \times\left[\sum_{j=1}^{p^n}\epsilon(j)^{-1}\log F_u([j]w_n+_G\exp_G z)\right]$$

si n est minimal.

DÉMONSTRATION: Il suffit d'appliquer **M.3** à la mesure associée par **M.1** à $\tilde{h}_u$.

REMARQUE 1: Soit $\mathfrak{q}$ un idéal premier à $\mathfrak{p}$. Définissons $U_n^v(H(E_{\mathfrak{q}\mathfrak{p}}))$ et $U^v(H(E_{\mathfrak{q}\mathfrak{p}}))$ comme U_n^v et U^v, i.e. en remplaçant $F_n=F\cdot K_n$ par $H(E_{\mathfrak{q}\mathfrak{p}^{n+1}})=H(E_{\mathfrak{q}\mathfrak{p}})\cdot K_n$. En s'inspirant de [4] Lemme 3, on vérifie que $H(E_{\mathfrak{q}})^v$ est une extension non ramifiée de $\mathbb{Q}_p$, ce qui permet de transposer les raisonnements précédents: à un élément $u\in U^v(H(E_{\mathfrak{q}\mathfrak{p}}))$ correspond une série F_u à coefficients dans $\mathcal{O}^v(H(E_{\mathfrak{q}}))$ et une mesure à valeurs dans A'. On définit $\Delta_k^v(u)$ comme plus haut. A cause du résultat d'unicité du théorème 1, les définitions de Δ_k^v sur U^v, $U^v(H(E_{\mathfrak{q}\mathfrak{p}}))$ pour $\mathfrak{q}$ divisant $\mathfrak{f}$ et $U^v(H(E_{\mathfrak{f}\mathfrak{p}}))$ sont compatibles entre elles.

§3. Fonctions L $\mathfrak{p}$-adiques

3.1. *Calculs dans* $\mathbb{C}$

G. Robert a introduit des unités elliptiques comme valeurs particulières de certaines fonctions θ, cf. [20]. En modifiant légèrement les

définitions de [20] §1, comme dans [21] introduisons pour $\mathscr{L}$ réseau quelconque dans $\mathbb{C}$ la fonction[1]

$$\theta(z, \mathscr{L}) = \Delta(\mathscr{L}) \cdot \exp(-6s_2(\mathscr{L})z^2) \cdot \sigma(z, \mathscr{L})^{12},$$

où $\Delta(\mathscr{L})$ est le discriminant, $\sigma(z, \mathscr{L})$ la fonction sigma

$$\sigma(z, \mathscr{L}) = z \cdot \prod (1 - z/\omega) \cdot e^{z/\omega + 1/2(z/\omega)^2},$$

et $s_2(\mathscr{L})$ est la limite pour $s \in \mathbb{R}$ tendant vers 0^+ de $\Sigma\, \omega^{-2} \cdot |\omega|^{-2s}$, la somme et le produit étant pris sur les éléments $\omega \neq 0$ de $\mathscr{L}$.

Soient $\mathfrak{g}$ un idéal entier de K (par exemple celui introduit au §1), et $I_\mathfrak{g}$ le monoïde unitaire des idéaux entiers de K premiers à 6, $\mathscr{F}$ et $\mathfrak{g}$. Pour $\mathfrak{U}$ dans $I_\mathfrak{g}$ de norme notée $N(\mathfrak{U})$, considérons l'élément $\mathfrak{U} - N(\mathfrak{U}) \cdot \mathcal{O}(K)$ de $Z[I_\mathfrak{g}]$, encore écrit $\mathfrak{U} - N(\mathfrak{U})$, et associons lui

$$\theta(z, \mathfrak{U} - N(\mathfrak{U})) = \theta(z, \Omega_\infty \cdot \mathfrak{U}^{-1})/\theta(z, \Omega_\infty \cdot \mathcal{O}(K))^{N(\mathfrak{U})}. \tag{8}$$

Soit $J_\mathfrak{g}$ l'idéal de $\mathbb{Z}[I_\mathfrak{g}]$ formé des $\alpha = \Sigma\, n(\mathfrak{U}) \cdot \mathfrak{U}$ vérifiant $\Sigma\, n(\mathfrak{U}) \cdot N(\mathfrak{U}) = 0$ et $\Sigma\, n(\mathfrak{U}) = 0$. Si α est un tel élément, il s'écrit $\alpha = \Sigma\, n(\mathfrak{U}) \cdot [\mathfrak{U} - N(\mathfrak{U})]$, ce qui permet de poser

$$\theta(z, \alpha) = \prod_{\mathfrak{U} \in I_\mathfrak{g}} \theta(z, \mathfrak{U} - N(\mathfrak{U}))^{n(\mathfrak{U})}. \tag{9}$$

Si b est un élément de K avec $(b) \in I_\mathfrak{g}$, on a alors

$$\theta(z, \alpha b) = \theta(bz, \alpha). \tag{10}$$

Choisissons ρ un point du réseau $\Omega_\infty \cdot \mathfrak{g}^{-1}$ primitif premier à $6\mathscr{F}$, i.e. tel que l'élément ρ/Ω_∞ de K engendre un idéal fractionnaire de la forme $\mathfrak{g}^{-1} \cdot \mathfrak{h}$, avec $\mathfrak{h} \in I_\mathfrak{g}$. Convenons de ne pas faire figurer le réseau $\mathscr{L}$ dans les notations lorsque $\mathscr{L} = \Omega_\infty \cdot \mathcal{O}(K)$.

LEMME 9: *La fonction $z \to \theta(z + \rho, \alpha)$ est une fraction rationnelle en $\mathfrak{p}(z)$ et $\mathfrak{p}'(z)$ dont les coefficients sont dans $H(E_\mathfrak{g})$.*

DÉMONSTRATION: On a en effet, si $\mathfrak{U} \in I_\mathfrak{g}$,

$$\theta(z, \mathfrak{U} - N(\mathfrak{U})) = \frac{\Delta(\Omega_\infty \cdot \mathfrak{U}^{-1})}{\Delta^{N(\mathfrak{U})}} \prod [\mathfrak{p}(z) - \mathfrak{p}(\lambda)]^6, \tag{11}$$

[1] Notée $\theta^{(12)}(z, \mathscr{L})$ dans [20].

où dans le produit λ parcourt un système de représentants de $(\Omega_\infty \mathfrak{U}^{-1}/\Omega_\infty \mathcal{O}(K)) - \{0\}$, cf. [21]; ceci montre que $\theta(z+\rho, \alpha)$ est une fraction rationnelle en $\mathfrak{p}$ et $\mathfrak{p}'$ si $\mathfrak{g} = 1$. Sinon on utilise

$$\theta(z+\rho, \mathfrak{U} - N(\mathfrak{U})) = \frac{\Delta(\Omega_\infty \mathfrak{U}^{-1})}{\Delta^{N(\mathfrak{U})}} \prod \left[\frac{1}{4}\left(\frac{\mathfrak{p}'(z)-\mathfrak{p}'(\rho)}{\mathfrak{p}(z)-\mathfrak{p}(\rho)}\right)^2 - \mathfrak{p}(z) - \mathfrak{p}(\rho) - \mathfrak{p}(\lambda)\right]^6. \tag{12}$$

L'assertion sur les coefficients provient de [20] prop. 8 et 9.

3.2. *Unités elliptiques*

On désigne par g le plus petit entier rationnel >0 contenu dans $\mathfrak{g}$ et par $e(\mathfrak{g})$ le nombre de racines de 1 dans K congrues à 1 modulo $\mathfrak{g}$. Le lemme suivant, théorème 8 de [20] §4.3, peut servir de définition du sous-groupe $\Omega_\mathfrak{g}$ d'unités de $H_\mathfrak{g}$.

LEMME 10: *Le groupe des unités elliptiques propres $\Omega_\mathfrak{g}$ de $H_\mathfrak{g}$ est engendré, si $\mathfrak{g} \neq 1$, par des racines de l'unité et par des racines d'ordre $e(\mathfrak{g})$ des éléments $\mathfrak{i}_\infty^{-1}\theta(\rho, \alpha)$ où α parcourt $J_\mathfrak{g}$ ou $J_{\mathfrak{g}\mathfrak{p}}$.*

Dans [20], intervient la fonction $\varphi^{(12)}(z, \mathscr{L}) = \theta(z, \mathscr{L}) \cdot \exp\left(\frac{-6\pi z\bar{z}}{a(\mathscr{L})}\right)$, où $a(\mathscr{L})$ désigne l'aire du réseau $\mathscr{L}$. On sait que $\varphi^{(12)g}(\rho, \Omega_\infty \cdot \mathfrak{U}^{-1})$ ne dépend que de la classe $C(\mathfrak{U}\mathfrak{h})$ de $\rho\Omega_\infty^{-1}\mathfrak{U}\mathfrak{g} = \mathfrak{U}\mathfrak{h}$ dans $Cl(\mathfrak{g})$: suivant [20], on le note $\varphi_\mathfrak{g}(C(\mathfrak{U}\mathfrak{h}))$. Puisque α est dans $J_\mathfrak{g}$, on a $\Sigma\, n(\mathfrak{U}) \cdot [N(\mathfrak{U}) - 1] = 0$ si bien que les facteurs exponentiels se simplifient dans l'expression de $\theta(\rho, \alpha)^g$ à l'aide de $\varphi^{(12)}$:

$$\theta(\rho, \alpha)^g = \prod_{\mathfrak{U}} \varphi^{(12)g}(\rho, \Omega_\infty \cdot \mathfrak{U}^{-1}) = \prod_{\mathfrak{U}} \varphi_\mathfrak{g}(C(\mathfrak{U}\mathfrak{h}))^{n(\mathfrak{U})}. \tag{13}$$

Ceci donne la partie de l'énoncé suivant relative à $k = 0$.

PROPOSITION 3: *Soit $\alpha = \Sigma\, n(\mathfrak{U}) \cdot \mathfrak{U}$ un élément de $J_\mathfrak{g}$, on a si $\mathfrak{g} \neq 1$,*

$$\left(\frac{d}{dz}\right)_{z=0}^k \log \theta(\rho + z, \alpha)$$

$$= \begin{cases} (1/g) & \Sigma\, n(\mathfrak{U}) \log \varphi_\mathfrak{g}(C(\mathfrak{U}\mathfrak{h})) \quad \text{si } k = 0 \\ -12 & \Sigma\, n(\mathfrak{U}) \mathfrak{p}^{(k-2)}(\rho, \Omega_\infty \cdot \mathfrak{U}^{-1}) \quad \text{si } k \geq 2. \end{cases}$$

DÉMONSTRATION: Pour $k \geq 2$, il suffit d'utiliser (8), (9) et la définition de $\theta(z, \mathscr{L})$.

Si $\mathscr{K}/K$ est une extension abélienne ramifiée de conducteur $\mathfrak{g}$, on appelle groupe des *unités elliptiques propres* $\Omega_{\mathscr{K}}$ de $\mathscr{K}$ le groupe des normes entre $H_{\mathfrak{g}}$ et $\mathscr{K}$ des éléments de $\Omega_{\mathfrak{g}}$. On appelle groupe des *unités elliptiques* $C_{\mathscr{K}}$ de $\mathscr{K}$ le produit

$$C_{\mathscr{K}} = \mu_{\mathscr{K}} \cdot \mathcal{O}(\mathscr{K} \cap H)^* \cdot \prod_{\mathscr{K}'} \Omega_{\mathscr{K}'},$$

où $\mathscr{K}'$ parcourt l'ensemble des sous-extensions *cycliques*[1] de $\mathscr{K}/\mathscr{K} \cap H$, $\mu_{\mathscr{K}}$ est le groupe des racines de 1 dans $\mathscr{K}$ et $\mathcal{O}(\mathscr{K} \cap H)^*$ est le groupe des unités de $\mathcal{O}(\mathscr{K} \cap H)$. Ainsi $C_{\mathscr{K}}$ est relié au groupe Ω^1 (relatif à $\mathscr{K}$) introduit dans [8] §6 par $C_{\mathscr{K}} = \mu_{\mathscr{K}} \cdot \mathcal{O}(\mathscr{K} \cap H)^* \cdot (\Omega^1)^{12}$. Supposons que le p-sous-groupe de Sylow de $\mathrm{Gal}(\mathscr{K}/\mathscr{K} \cap H)$ soit cyclique, alors d'après [8] th. 5

$$[\mathcal{O}(\mathscr{K})^* : C_{\mathscr{K}}] \sim \left(\prod_{\mathscr{K}'} l(\mathscr{K}')\right) \cdot h(\mathscr{K})/h(\mathscr{K} \cap H),$$

où $\sim$ signifie que les deux membres ne diffèrent que par une unité de Ω_p et où $l(\mathscr{K}')$ vaut 1 ou p. En raisonnant comme pour le lemme 2, on déduit de [8] §7.3 rq. 2 que pour $\mathscr{K} = F_n$, tous les $l(\mathscr{K}')$ valent 1. En abrégeant C_{F_n} en C_n comme au §0, on obtient donc

$$[\mathcal{O}(F_n)^* : C_n] \sim h(F_n)/h(F \cap H). \tag{14}$$

3.3. *Séries associées aux unités elliptiques*

Avec les notations introduites précédemment, on a en utilisant $i_{\mathfrak{p}}$ et i_∞ pour identifier des séries à coefficients dans $\mathbf{C}$ ou $\mathbf{C}_p$:

LEMME 11: *Soient $\mathfrak{g}$ un idéal entier de K premier à $\mathfrak{p}$, et α un élément de $J_{\mathfrak{g}\mathfrak{p}}$; il existe une série formelle $F(W, \alpha)$, à coefficients dans $\mathcal{O}^v(H(E_{\mathfrak{g}}))$, vérifiant pour tout $n \in \mathbf{N}$ et $j \in \mathbf{Z}$ l'égalité de séries formelles*:

$$\theta(z + j\rho_n + \rho, \alpha) = F(\exp_G z + {}_G[j]w_n, \alpha).$$

DÉMONSTRATION: Si par exemple $\mathfrak{g}$ est non trivial, on utilise (12) pour trouver l'égalité dans le corps de fractions de $H(E_{\mathfrak{g}})^v[[W]]$

[1] Si $\mathscr{K} = F_n$, on peut prendre *toutes* les sous-extensions ramifiées de F_n/K, sans changer les résultats qui suivent.

$$(15)\qquad \theta(z+\rho, \mathfrak{U}-N(\mathfrak{U})) = \frac{\Delta(\Omega_\infty \cdot \mathfrak{U}^{-1})}{\Delta^{N(\mathfrak{U})}} \cdot \prod \left[\frac{1}{4W^2}\left(\frac{2+W^3\mathfrak{p}'(\rho)/a(W)}{1-W^2\mathfrak{p}(\rho)/a(W)}\right)^2 - \frac{a(W)}{W^2} - \mathfrak{p}(\rho) - \mathfrak{p}(\lambda)\right]^6;$$

et on vérifie, comme dans [4] lemme 23, que le deuxième membre est une série dans $\mathcal{O}^v(H(E_\mathfrak{q}))[[W]]$.
On construit alors $F(W, \alpha)$ à l'aide de (9). Si $\mathfrak{q} = 1$, on procède de même en utilisant l'égalité (11). La formule du lemme 11 résulte alors du fait que les formules d'addition sont les mêmes pour E et G.

LEMME 12: *Pour tout α dans $J_{\mathfrak{q}\mathfrak{p}}$, on a, pour $n \in \mathbb{N}$*

$$\prod_{j=1}^{p^n} \theta(z + j\rho_n, \alpha) = \theta(z, \mathfrak{p}^n \cdot \alpha).$$

DÉMONSTRATION: La fonction de z obtenue en faisant le quotient du premier membre par le second est constante et est une racine de l'unité, cf. [20] §1 prop. 1: sa valeur se calcule en faisant tendre z vers 0; c'est:

$$\zeta = \prod_{\mathfrak{U}} \left(\frac{\Delta(\Omega_\infty \cdot \mathfrak{U}^{-1})}{\Delta(\Omega_\infty \cdot \mathfrak{U}^{-1} \cdot \mathfrak{p}^{-n})}\right)^{n(\mathfrak{U})} \cdot \prod_{j=1}^{p^n-1} \theta(j\rho_n, \alpha)$$

si $\alpha = \Sigma\, n(\mathfrak{U}) \cdot \mathfrak{U}$. On conclut que $\zeta = 1$ puisque d'après [10] prop. A-2, et [21] cor A-2, le deuxième membre est une puissance $12^{ième}$ dans $H_{\mathfrak{p}^n}$.

Rappelons que $\theta(\rho + \rho_n, \alpha)$ est l'image par i_∞ d'une unité de $H_{\mathfrak{q}\mathfrak{p}^n}$ si $\alpha \in J_{\mathfrak{q}\mathfrak{p}}$ et qu'un automorphisme d'Artin opère dessus par (cf. [20] §4.2 prop. 9 cor.)

$$(16)\qquad [\mathfrak{B}, H_{\mathfrak{q}\mathfrak{p}^n}/K] i_\infty^{-1}\theta(\rho + \rho_n, \alpha) = i_\infty^{-1}\theta(\rho + \rho_n, \alpha\mathfrak{B}).$$

Si $\alpha \in (p^{[H(E_\mathfrak{q})^v : \mathbf{Q}_p]} - 1) \cdot J_{\mathfrak{q}\mathfrak{p}}$, on définit un élément de $\mathcal{O}(H_{\mathfrak{q}\mathfrak{p}^{nf+1}})^*$ donc de $\mathcal{O}(H(E_{\mathfrak{q}\mathfrak{p}^{nf+1}}))^*$ en posant:

$$u_{nf+1}(\alpha) = i_\infty^{-1}\theta(t^{-n}\rho + \rho_{nf+1}, \alpha).$$

Ainsi, $i_\mathfrak{p}(u_{nf+1}(\alpha))$ est dans $U^v_{nf}(H(E_{\mathfrak{q}\mathfrak{p}}))$; le facteur dans α sert à assurer la congruence modulo l'idéal maximal de $H(E_{\mathfrak{q}\mathfrak{p}^{nf+1}})^v$.

PROPOSITION 4: *La suite des $(u_{nf+1}(\alpha))$ définit un élément $u_v(\alpha)$ dans $U^v(H(E_{\mathfrak{q}\mathfrak{p}}))$ et avec les notations de* 2.3, *on a*

$$F_{u_v}(\alpha)(W) = F(W, \alpha).$$

DÉMONSTRATION: A l'aide de (16), on vérifie en utilisant (10) et le lemme 12 que la norme de u_{nf+1} dans $H(E_{\mathfrak{a}\mathfrak{p}^{nf+1}})/H(E_{\mathfrak{a}\mathfrak{p}^{(n-1)f+1}})$ (ou encore dans $H_{\mathfrak{a}\mathfrak{p}^{nf+1}}/H_{\mathfrak{a}\mathfrak{p}^{(n-1)f+1}}$) est égale à

$$\prod_{j=1}^{p^f} i_\infty^{-1}\theta(t^{-n}\rho + \rho_{nf+1} + j\rho_f, \alpha) = i_\infty^{-1}\theta(t^{-n}\rho + \rho_{nf+1}, \alpha\mathfrak{p}^f)$$

donc aussi à $u_{(n-1)f+1}(\alpha)$ d'après l'égalité $\mathfrak{p}^f = (t)$, cf. (10). Ceci permet bien de définir[1] $u_v(\alpha)$. Si Frob désigne comme plus haut le Frobenius relatif à $\hat{\mathbb{Q}}_p^{nr}/H^v$, en utilisant (15) et (1), on voit que

$$i_\mathfrak{p}^{-1}(F^{\mathrm{Frob}^{-n}}(w_{nf+1}, \alpha)) = i_\infty^{-1}\theta(t^{-n}\rho + \rho_{nf+1}, \alpha).$$

Ceci prouve l'égalité des séries de la proposition 4 d'après le résultat d'unicité du théorème 1 appliqué avec $L = H(E_\mathfrak{a})^v$, $L' = H^v$.

3.4. *Fonctions L $\mathfrak{p}$-adiques*

DÉFINITIONS: Soit $\mathfrak{g}$ un idéal entier non trivial de K, avec ρ et $\mathfrak{h}$ comme en 3.1, et φ un caractère primitif de $Cl(\mathfrak{g})$, on pose

$$S(\varphi) = \sum \varphi^{-1}(C) \log i_\mathfrak{p} i_\infty^{-1} \varphi_g(C)$$

$$\tau(\varphi) = \varphi^{-1}(\mathfrak{h}) \sum \varphi^{-1}((c)) i_\mathfrak{p} i_\infty^{-1} \exp\left(2\pi i \,\mathrm{Tr}\left(\frac{c\rho}{\Omega_\infty\sqrt{d}}\right)\right)$$

$$b_k(\varphi) = \sum \varphi(\mathfrak{B}\mathfrak{h})^{-1}\psi(\mathfrak{B})^{-k} i_\mathfrak{p} i_\infty^{-1} \mathfrak{p}^{(k-2)}(\rho, \Omega_\infty \cdot \mathfrak{B}^{-1})$$

$$\text{si } k \in e \cdot \mathbb{Z}, \text{ et } k \geq 2.$$

Dans la première somme, C décrit $Cl(\mathfrak{g})$, et log est la fonction logarithme dans Ω_p (avec $\log p = 0$); dans la deuxième, c décrit un système de représentants de $(\mathcal{O}(K)/\mathfrak{g})^*$, $\sqrt{\mathrm{d}}$ désigne une racine carrée du discriminant de K et Tr la trace entre K et $\mathbb{Q}$. Dans le troisième somme, $\mathfrak{B}$ décrit un système de représentants de $Cl(\mathfrak{g})$: on vérifie, cf. (3), que $b_k(\varphi)$ ne dépend pas du choix des idéaux $\mathfrak{B}$. De même, $\tau(\varphi)$ et $b_k(\varphi)$ ne dépendent pas du choix de ρ grâce à la présence du facteur $\varphi(\mathfrak{h})^{-1}$.

Soient $\mathfrak{B}$ un idéal, b un générateur de $\mathfrak{B}^{h(K)}$, l'élément

[1] Avec des notations évidentes, on définit aussi $u(\alpha) \in U(H(E_{\mathfrak{a}\mathfrak{p}}))$.

$(b)^{-12} \cdot \Delta(\mathfrak{B}^{-1})^{h(K)}$ ne dépend que de l'image $C(\mathfrak{B})$ de $\mathfrak{B}$ dans $Cl((1))$, on le note $\delta(C(\mathfrak{B}))$, comparer à [20] §3.1.

DÉFINITIONS : Pour φ caractère non ramifié de F/K, on pose $\rho = 0$, $\mathfrak{h} = 1$ et

$$S(\varphi) = \frac{1}{h(K)} \sum \varphi^{-1}(\mathfrak{B}) \log i_{\mathfrak{p}} i_{\infty}^{-1} \delta(C(\mathfrak{B}))$$

$$\tau(\varphi) = 1$$

$$b_k(\varphi) = \sum \varphi(\mathfrak{B})^{-1} \psi(\mathfrak{B})^{-k} i_{\mathfrak{p}} i_{\infty}^{-1} \left(\frac{d}{dz}\right)_{z=0}^{(k-2)} \left(\mathfrak{p}(z, \Omega_{\infty}\mathfrak{B}^{-1}) - \frac{1}{z^2}\right),$$

si $k \in e\mathbb{Z}, k \geq 2$. Dans les sommes $\mathfrak{B}$ parcourt un système de représentants de $Cl((1))$, log désignant toujours le logarithme dans Ω_p; changer le système des $\mathfrak{B}$ n'affecte pas les valeurs de $S(\varphi)$, $\tau(\varphi)$ et $b_k(\varphi)$.

On reprend les notations et hypothèses introduites après (2) sur φ, i et $\mathfrak{g}$. Pour π comme dans le lemme 1, soit $\boldsymbol{\pi}$ le caractère d'ordre p^n de $Cl(\mathfrak{p}^{n+1})$ dont la puissance d'ordre e est $\pi \circ \psi^e$. Posons $\epsilon = \pi \cdot \omega^i$ et définissons $\hat{\epsilon}$ comme dans **M.3**. Le conducteur de $\varphi\boldsymbol{\pi}$ est de la forme $\mathfrak{g}\mathfrak{p}^m$; si $n > 0$, $m = n + 1$; si $n = 0$, $m = 0$ si $i \equiv 0 \bmod(p-1)$ et $m = 1$ sinon. Si $m \neq 0$, on pose $\rho'_m = \rho + \rho_m$ et on note $\mathfrak{h}'_m$ l'idéal $(\rho'_m/\Omega_\infty)\mathfrak{g}\mathfrak{p}^m$ de K. Soit c_m l'entier défini (modulo p^m) par

$$\exp 2\pi i \operatorname{Tr}\left(\frac{\rho_m}{\Omega_\infty \sqrt{d}}\right) = \zeta_m^{c_m},$$

où ζ_m est défini comme à la fin de 2.3. On peut relier $\tau(\rho\boldsymbol{\pi})$ et $\tau(\varphi_i)$:

LEMME 13: *Avec les notations précédentes, on a*:

$$\tau(\varphi\boldsymbol{\pi})\varphi(\mathfrak{h}'_m)\boldsymbol{\pi}(\mathfrak{h}'_m) = \tau(\varphi_i)\varphi_i(\mathfrak{h})\epsilon(c_m)/\hat{\epsilon}(\zeta_m).$$

DÉMONSTRATION: Pour expliciter $\tau(\varphi\boldsymbol{\pi})$, on utilise un système de représentants de $(\mathcal{O}(K)/\mathfrak{p}^m \cdot \mathfrak{g})^*$ de la forme $\lambda = bc$ avec $b \equiv 1 \bmod \mathfrak{p}^m$ et $c \equiv 1 \bmod \mathfrak{g}$, $c \in \mathbb{Z}$. Dans ces conditions,

$$i_{\mathfrak{p}} i_{\infty}^{-1} \exp 2\pi i \operatorname{Tr}\left(\frac{\lambda \rho'_m}{\Omega_\infty \sqrt{d}}\right) = \left[i_{\mathfrak{p}} i_{\infty}^{-1} \exp 2\pi i \operatorname{Tr}\left(\frac{b\rho}{\Omega_\infty \sqrt{d}}\right)\right] \cdot \zeta_m^{c \cdot c_m}$$

$$\varphi((\lambda)) = \varphi_i((b)) \cdot \epsilon(c).$$

Le premier membre du lemme 13 se décompose en un produit et pour obtenir la formule, il suffit d'utiliser l'égalité

$$\hat{\epsilon}(\zeta_m) \sum_{c=1}^{p^m} \epsilon(c)^{-1} \zeta_m^c = 1.$$

Pour $\mathfrak{U}$ dans $I_{\mathfrak{q}\mathfrak{p}}$, introduisons l'entier p-adique $l(\mathfrak{U}) = l(\psi(\mathfrak{U})^{h(K)})/h(K)$. Choisissons un élément $\alpha = \Sigma\, n(\mathfrak{U}) \cdot \mathfrak{U}$ dans $(p^{[H(E_{\mathfrak{q}})^v : \mathbf{Q}_p]} - 1) \cdot J_{\mathfrak{q}\mathfrak{p}}$.

DÉFINITIONS: On introduit la série

$$H_\alpha(T, \varphi) = \sum n(\mathfrak{U}) \cdot \varphi(\mathfrak{U}) \cdot (1+T)^{l(\mathfrak{U})},$$

le quotient de séries

$$f(T, \varphi) = \frac{\sum \varphi^{-1}(\mathfrak{B}) \cdot (1+T)^{-l(\mathfrak{B})} \cdot G^i_{u_v(\mathfrak{B}\alpha)}(T)}{12\sqrt{d}\, \varphi_i(\mathfrak{h}) \tau(\varphi_i) e(\mathfrak{g}) H_\alpha(T, \varphi)}$$

où $\mathfrak{B}$ parcourt un système de représentants de $Cl(\mathfrak{g})$, et la fonction de $s \in \mathbf{Z}_p$

$$L_{\mathfrak{p}}(s, \varphi\pi) = f(\pi(c) \cdot c^{1-s} - 1, \varphi).$$

Avec g et $e(\mathfrak{g})$ comme au début du §3.2, on peut énoncer pour $\nu = \varphi \cdot \pi$ et $\nu_k = \varphi_k \cdot \pi$.

THÉORÈME 2: *Le quotient $f(T, \varphi)$ est en fait dans $A'[[T]]$ et ne dépend pas de α. La fonction $L_{\mathfrak{p}}(s, \nu)$ vérifie*

$$L_{\mathfrak{p}}(1, \nu) = (12\sqrt{d}\, \tau(\nu) e(\mathfrak{g}\mathfrak{p}^m) g p^m)^{-1} \cdot \left(1 - \frac{\nu(\mathfrak{p})}{N\mathfrak{p}}\right) \cdot S(\nu) \cdot \epsilon(c_m) \text{ et si } k \in e\mathbf{Z},\ k \geq 2,$$

$$L_{\mathfrak{p}}(1-k, \nu) = -(\sqrt{d}\, \tau(\nu_k) e(\mathfrak{g}\mathfrak{p}^{m_k}))^{-1} \cdot \left(1 - \frac{\nu_k(\mathfrak{p}) \psi(\mathfrak{p})^k}{N\mathfrak{p}}\right) \cdot \Omega_{\mathfrak{p}}^{-k} \cdot b_k(\nu_k) \cdot \epsilon_k(c_{m_k}),$$

où ϵ_k et m_k sont définis à partir de $\varphi_k \pi = \nu_k$ comme ϵ et m à partir de $\varphi\pi = \nu$.

REMARQUE 2: L'indépendance de α provient de la formule donnant $L_{\mathfrak{p}}(1, \varphi\pi) = f(\pi(c) - 1, \varphi)$; on peut d'ailleurs aussi voir que le changement de η (ou de E) modifie f par multiplication par un facteur de la forme $\omega^i(a) \cdot (1+T)^{l(a)}$ avec $a \in \mathbb{Z}_p^*$.

REMARQUE 3: Le choix de $\boldsymbol{\omega}^e$ (cf. §1) a des conséquences sur φ_k, ν_k, ψ^k et $b_k(\varphi)$ mais $\tau(\nu_k)$ n'en dépend pas, ainsi que $b_k(\nu_k)$ (en vertu de l'égalité $\nu_k\psi^k = \nu \cdot \langle\psi\rangle^k$). On en déduit que $L_{\mathfrak{p}}(1-k, \nu)$ *et* $f(T, \varphi)$ *sont indépendants du choix de* $\boldsymbol{\omega}^e$.

La première assertion du théorème provient du lemme suivant. Observons d'abord que si $k \in e\mathbb{Z}$, on a

$$H_\alpha(\pi(c)c^k - 1, \varphi) = \sum n(\mathfrak{U}) \cdot \varphi_k(\mathfrak{U}) \cdot \boldsymbol{\pi}(\mathfrak{U}) \cdot \psi(\mathfrak{U})^k.$$

LEMME 14: *On peut trouver* $\alpha \in (p^{[H(E_\mathfrak{q})^\nu : \mathbf{Q}_p]} - 1) \cdot J_{\mathfrak{q}\mathfrak{p}}$, *tel que* $H_\alpha(T, \varphi)$ *soit inversible dans* $A'[[T]]$.

DÉMONSTRATION: Soient $\mu(\mathfrak{q}\mathfrak{p})$ le groupe des racines de 1 dans $H_{\mathfrak{q}\mathfrak{p}}$ et ζ un de ses générateurs. L'application $\mathbb{Z}$-linéaire de $\mathbb{Z}[I_{\mathfrak{q}\mathfrak{p}}]$ dans $\mathbb{Z} \oplus \mu(\mathfrak{q}\mathfrak{p})$ envoyant $\mathfrak{U}$ sur $1 \oplus \zeta^{\sigma(\mathfrak{U})}$ ($\sigma(\mathfrak{U})$ automorphisme d'Artin dans $H_{\mathfrak{q}\mathfrak{p}}/K$) a pour noyau $J_{\mathfrak{q}\mathfrak{p}}$ (cf. [3] lemme 12, cas $n = 1$). On a donc une suite exacte

$$0 \to J_{\mathfrak{q}\mathfrak{p}} \to \mathbb{Z}[I_{\mathfrak{q}\mathfrak{p}}] \to \mathbb{Z} \oplus \mu(\mathfrak{q}\mathfrak{p}) \to 0.$$

En composant l'application de réciprocité avec (2), on obtient la suite exacte

$$0 \to J_{\mathfrak{q}\mathfrak{p}}^{\varphi} \to A \to e_\Phi[\mathbb{Z}_p \oplus \mu(\mathfrak{q}\mathfrak{p}) \otimes \mathbb{Z}_p] \to 0,$$

où $J_{\mathfrak{q}\mathfrak{p}}^{\varphi}$ désigne l'idéal de A engendré par les sommes $\Sigma\, n(\mathfrak{U}) \cdot \varphi(\mathfrak{U})$ telles que $\Sigma\, n(\mathfrak{U}) \cdot \mathfrak{U} \in J_{\mathfrak{q}\varphi}$. Comme d'après les hypothèses Φ est non trivial et $e_\Phi[\mu(\mathfrak{q}\mathfrak{p}) \otimes \mathbb{Z}_p] = 0$ (cf. démonstration du lemme 2) on trouve que $A = J_{\mathfrak{q}\mathfrak{p}}^{\varphi}$, ce qui prouve que $H_\alpha(0, \varphi)$ et $H_\alpha(T, \varphi)$ et $H_\alpha(T, \varphi)$ sont inversibles respectivement dans A' et $A'[[T]]$ pour α convenablement choisi.

FIN DE LA DÉMONSTRATION DU THÉORÈME 2: Soit $N_\alpha(T, \varphi)$ le numérateur dans la définition de $f(T, \varphi)$, on a (cf. lemme 7):

$$N_\alpha(\pi(c)\cdot c^k-1,\varphi)=\sum \nu_k(\mathfrak{B})^{-1}\cdot\psi(\mathfrak{B})^{-k}$$
$$\cdot\int_{Z_p^*}x^{k-1}\cdot\epsilon_k(x)\cdot\mu_{u_v(\mathfrak{B}\alpha)}(x).$$

Puisque $F_{u_v(\alpha)}([j]w_{m_k}+_G\exp_G z)=F([j]w_{m_k}+_G\exp_G z,\alpha)=\theta(z+\rho+j\rho_{m_k},\alpha)$, d'après le lemme 11 et la proposition 4, on tire du lemme 8 si $m_k>0$,

$$N_\alpha(\pi(c)c^k-1,\varphi)=\Omega_{\mathfrak{p}}^{-k}\cdot\hat{\epsilon}_k(\zeta_m)\cdot i_{\mathfrak{p}}i_\infty^{-1}\left(\frac{d}{dz}\right)^k_{z=0}\sum_{\mathfrak{B},c}\nu_k(\mathfrak{B})^{-1}\cdot\psi(\mathfrak{B})^{-k}$$
$$\cdot\epsilon_k^{-1}(c)\log i_{\mathfrak{p}}i_\infty^{-1}\theta(z+\rho+c\rho_{m_k},\alpha\mathfrak{B}).$$

Ici c parcourt un système de représentants de $(\mathbb{Z}/p^{m_k}\cdot\mathbb{Z})^*$ congrus à 1 mod $\mathfrak{g}$, ce qui permet d'avoir les égalités

$$\nu_k(\mathfrak{B})\cdot\epsilon_k(c)=\nu_k(\mathfrak{B}c),$$
$$\psi(\mathfrak{B})^{-k}\left(\frac{d}{dz}\right)^k_{z=0}\log i_{\mathfrak{p}}i_\infty^{-1}\theta(z+\rho+c\rho_{m_k},\alpha\mathfrak{B})$$
$$=\psi(\mathfrak{B}_C)^{-k}\left(\frac{d}{dz}\right)^k_{z=0}\log i_{\mathfrak{p}}i_\infty^{-1}\theta(z+\rho'_{m_k},\alpha\mathfrak{B}c),$$

cf. (3) et (10). Dans la double somme la classe de $\mathfrak{B}c$ décrit $e(\mathfrak{g})/e(\mathfrak{g}\mathfrak{p}^{m_k})$ fois le groupe $Cl(\mathfrak{g}\mathfrak{p}^{m_k})$. En utilisant que $b_k(\nu_k)$ et $S(\nu)$ ne dépendent pas des systèmes de représentants utilisés, on peut faire des changements de sommations qui permettent de mettre

$$\sum n(\mathfrak{U})\nu_k(\mathfrak{U})\psi(\mathfrak{U})^k=H_\alpha(\pi(c)c^k-1,\varphi)$$

en facteur. Les formules du théorème 2 résultent alors si $m_k>0$ (d'où $\nu_k(\mathfrak{p})=0$) du lemme 13 et de la proposition 3 si $k\geq 2$ (ou de son analogue p-adique si $k=0$). Si $m_k=0$, d'où $\pi=1$ et $\epsilon_k=1$, on utilise le lemme 5 au lieu du lemme 8, ainsi que le lemme 12 (avec $n=1$) ce qui fait apparaitre le facteur $(1-(\nu_k(\mathfrak{p})\psi^k(\mathfrak{p})/\mathrm{N}(\mathfrak{p})))$. Si en plus $\mathfrak{g}=1$, on se sert de la formule avec $\mathfrak{U}^{h(k)}=(a)$

$$\theta(0,\alpha\mathfrak{B})^{h(K)}=\prod_{\mathfrak{U}}(a^{12}\delta(C(\mathfrak{U}\mathfrak{B})))^{n(\mathfrak{U})},$$

qui permet de faire apparaitre $S(\varphi)$ dans l'expression de $N_\alpha(0,\varphi)$.

§4. Applications des fonctions L $\mathfrak{p}$-adiques

4.1. *Formules $\mathfrak{p}$-adiques du nombre de classes*

On reprend des notations introduites précédemment, notamment aux §1, 2.1 et 3.2. Soit C_n' le sous-groupe de C_n relatif à F_n noté $\Theta_{I(\mathfrak{G})}$ dans [10]. Considérons l'intersection de l'image diagonale de C_n dans $\Pi_{w\in S} F_n^w$ avec U_n, et notons $\bar{C}_n$ sa fermeture dans U_n; définissons $\bar{C}_n'$ et $\mathcal{O}(F_n)^*$ par le même procédé. D'après [5] lemme 9, on a

$$(17)\qquad [U_n : \overline{\mathcal{O}(F_n)^*}\cdot(1+p\mathbb{Z}_p)] \sim p^n \frac{R(\mathcal{O}(F_n)^*)}{\sqrt{\Delta(F_n)}} \prod_{\lambda\neq 1}\left(1-\frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right)$$

où R désigne le régulateur p-adique (défini, cf. [5], comme le régulateur usuel mais en remplaçant la fonction logarithme par son équivalent dans F_n^v) et $\sqrt{\Delta(F_n)}$ une racine carrée du discriminant relatif de F_n/K; λ parcourt l'ensemble des caractères $\neq 1$ définis et irréductibles sur Ω_p de $\mathrm{Gal}(F_n/K)$. Pour un tel caractère on note $\mathfrak{g}_\lambda$ son conducteur et on définit g_λ et $e(\mathfrak{g}_\lambda)$ comme au §3.2, et $S(\lambda)$ comme l'analogue p-adique de la somme de [20] §2.3; $S(\lambda)$ a déjà été défini au §3.4. Avec la même démonstration que pour (17), on a

$$(18)\qquad [U_n : \bar{C}_n'\cdot(1+p\mathbb{Z}_p)] \sim p^n \frac{R(C_n')}{\sqrt{\Delta(F_n)}} \prod_{\lambda\neq 1}\left(1-\frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right).$$

Mais en reprenant les calculs menant à [10] (2), on trouve

$$(19)\qquad R(C_n') \sim h(K)^{[F_n:F\cap H]-1}\cdot A_n \cdot \prod_{\lambda\neq 1} S(\lambda),$$

où A_n (comme plus loin B_n) est la quantité A (resp. B) de [10] §2 relative à F_n. Mais d'après [10] (3):

$$(20)\qquad [\mathcal{O}(F_n)^* : C_n'] \sim \frac{h(F_n)}{h(K)}\cdot h(K)^{[F_n:F\cap H]-1}\cdot A_n \cdot \prod_{\lambda\neq 1}(g_\lambda e(\mathfrak{g}_\lambda)).$$

En multipliant (17) par (20) et en comparant à (18) et (19), on obtient

$$\frac{R(\mathcal{O}(F_n)^*)}{\sqrt{\Delta(F_n)}}\frac{h(F_n)}{h(K)}\prod_{\lambda\neq 1}\left(1-\frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right) \sim \frac{1}{\sqrt{\Delta(F_n)}}\prod_{\lambda\neq 1}\frac{\left(1-\frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right)S(\lambda)}{(g_\lambda\cdot e(\mathfrak{g}_\lambda))}$$

$$\sim \prod_{\lambda\neq 1}\frac{\left(1-\frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right)S(\lambda)}{12\sqrt{d}\, g_\lambda e(\mathfrak{g}_\lambda)\tau(\lambda)},$$

en utilisant la formule $\Delta(F_n) = \Pi_\lambda (d \cdot N(\mathfrak{g}_\lambda))$; d'autre part $(\Pi \tau(\lambda))/\sqrt{\Pi N(\mathfrak{g}_\lambda)}$ est un nombre complexe de module 1, et c'est de plus un nombre rationnel puisque la démonstration de [10] (3) pour F_n consiste en fait à prouver l'égalité

$$[\mathcal{O}(F_n)^* : C_n'] = \pm h(F_n) \cdot B_n \cdot \prod_{\lambda \neq 1} \left(\frac{\tau(\lambda)}{\sqrt{N(\mathfrak{g}_\lambda)}}\right).$$

D'autre part avec (14) et (17), on obtient aussi

$$[U_n : \bar{C}_n(1 + p\mathbb{Z}_p)] \sim p^n \frac{h(F_n)}{h(F \cap H)} \frac{R(\mathcal{O}(F_n)^*)}{\sqrt{\Delta(F_n)}} \prod_{\lambda \neq 1} \left(1 - \frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right)$$

$$\sim p^n \frac{h(K)}{h(F \cap H)} \prod_{\lambda \neq 1} \frac{\left(1 - \frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right) S(\lambda)}{12\sqrt{d}\, g_\lambda e(\mathfrak{g}_\lambda) \tau(\lambda)}.$$

A l'aide des formules du théorème 2, on peut donc énoncer:

THÉORÈME 3: *On a les relations*

$$[U_n : \bar{C}_n(1 + p\mathbb{Z}_p)] \sim \frac{p^n}{h(F \cap H)} \cdot \left[\frac{h(F_n) \cdot R(\mathcal{O}(F_n)^*)}{\sqrt{\Delta(F_n)}}\right] \cdot \prod \left[1 - \frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right]$$

$$\sim \frac{h(K)}{h(F \cap H)} \cdot \prod L_\mathfrak{p}(1, \lambda),$$

où les produits sont pris sur les caractères de F_n/K, $\neq 1$ sur F_n/K_n.

Soient Λ un caractère de $\Delta = \mathrm{Gal}(F/K)$ défini et irréductible sur $\mathbb{Q}$ et $e_\Lambda \in \mathbb{Z}_p[\Delta]$ l'idempotent associé. En remplaçant F_n par les sous-extensions de $F_n/(F \cap H)$, et en comparant les formules obtenues, on déduit:

COROLLAIRE 1: *On a* $[e_\Lambda(U_n/\bar{C}_n(1 + p\mathbb{Z}_p)] \sim [e_\Lambda(U_0/\bar{C}_0(1 + p\mathbb{Z}_p)] \cdot \Pi L_\mathfrak{p}(1, \lambda)$, *où λ parcourt l'ensemble des caractères de* $\mathrm{Gal}(F_n/K)$ *définis et irréductibles sur Ω_p dont la restriction à* $\mathrm{Gal}(F_n/K_n)$ *(resp. à* $\mathrm{Gal}(F_n/F)$*) est un facteur de Λ (resp. est $\neq 1$). Si Λ est ramifié, on a aussi*

$$[e_\Lambda(U_0/\bar{C}_0)] \sim \prod L_\mathfrak{p}(1, \lambda)$$

où λ parcourt l'ensemble des caractères de Δ, définis et irréductibles sur Ω_p qui sont facteurs de la décomposition de Λ sur Ω_p.

REMARQUE 4: Si $\Lambda \neq 1$, $e_\Lambda(U_n/\bar{C}_n \cdot (1+p\mathbb{Z}_p)) = e_\Lambda(U_n/\bar{C}_n)$. Désignons par M_n (resp. M_∞, cf. §0) la p-extension non ramifiée en dehors de $\mathfrak{p}$ abélienne maximale de F_n (resp. F_∞): en comparant la première relation du théorème 3 avec celle de [5] théorème 11, ainsi que les relations analogues obtenues en remplaçant F par les sous-extensions de $F/F \cap H$, on tire:

COROLLAIRE 2: *Soit Λ un caractère ramifié de Δ, défini et irréductible sur $\mathbb{Q}$, on a* $[e_\Lambda \operatorname{Gal}(M_n/K_n)] = [e_\Lambda(U_n/\bar{C}_n)]$.

REMARQUE 5: Avec les hypothèses du corollaire, le premier membre est encore égal à $e_\Lambda(\operatorname{Gal}(M_\infty/K_\infty)/\omega_n \cdot \operatorname{Gal}(M_\infty/K_\infty))$, cf. [11]. La formule (22) ci-dessous montre que le deuxième membre vaut $e_\Lambda(Y_\infty/\omega_n \cdot Y_\infty)$ si $\varphi(\mathfrak{p}) \neq 1$ (φ facteur irreductible de la décomposition de Λ sur Ω_p); si $\varphi(\mathfrak{p}) = 1$, on obtient seulement une égalité $[e_\Lambda(\operatorname{Gal}(M_\infty/K_\infty)/\omega_n \cdot \operatorname{Gal}(M_\infty/K_\infty))] = C(\Lambda) \cdot [e_\Lambda(Y_\infty/\omega_n \cdot Y_\infty)]$, où $C(\Lambda) \in \mathbb{Q}$ est indépendant de n (cf. théorèmes 4 et 5 ci-dessous).

REMARQUE 6: Par analogie, il est naturel de conjecturer que l'énoncé du corollaire 2 est encore vrai pour les caractères de Δ définis et irréductibles sur $\mathbb{Q}_p$: c'est un des problèmes fondamentaux sur la $\mathbb{Z}_l$-extension F_∞/F et sa solution aurait des conséquences importantes pour l'arithmétique des courbes elliptiques.

4.2. *Structure de Y_∞ et critère de Kummer*

On reprend les notations introduites précédemment, notamment au §1, pour énoncer les trois théorèmes suivants:

THÉORÈME 4: *Il existe une série $g(T,\varphi) \in A[[T]]$ telle que $Y_\infty = e_\Phi \varprojlim(U_n/\bar{C}_n)$ soit isomorphe à $A[[T]]/(g(T,\varphi))$, $g(T,\varphi)$ étant égale au produit de $f(T,\varphi)$ par une série inversible de $A'[[T]]$.*

On a donc un isomorphisme $e_\Phi Y_\infty \otimes_A A' \cong A'[[T]]/(f(T,\varphi))$.

THÉORÈME 5: *Soit $g(T,\varphi)$ comme dans le théorème précédent. Le $A[[T]]$-module $e_\Phi(U_n/\bar{C}_n)$ est isomorphe à $A[[T]]/(g(T,\varphi), \omega_n)$ si $\varphi(\mathfrak{p}) \neq 1$; il figure dans une suite exacte*

$$0 \to A[[T]]/(g(T,\varphi), \omega_n/T) \to e_\Phi(U_n/\bar{C}_n) \to e_\Phi(U_0/\bar{C}_0) \to 0,$$

où la surjection est induite par la norme, si $\varphi(\mathfrak{p}) = 1$.

THÉORÈME 6: (i) *Soit* Φ *un caractère de* $\mathrm{Gal}(F/K)$, cf. §1, *alors si* $\varphi(\mathfrak{p}) \neq 1$ $[e_\Phi(U_n/\bar{C}_n)]$ (*ou si* $\varphi(\mathfrak{p}) = 1$, $[e_\Phi(U_n/\bar{C}_n)]/[e_\Phi(U_0/\bar{C}_0)]$ *avec* $n \geq 1$) *vaut* 1 *si et seulement si* $b_i(\varphi_i)$ *est inversible dans* A'.

(ii) *Pour que* p *divise* $h(F)/h(F \cap H)$ (*resp.* $h(F_n)/h(F \cap H)$ *avec* $n \geq 1$) *il faut que l'un au moins des nombres* $b_i(\varphi_i)$, *où* φ *parcourt l'ensemble des caractères ramifiés* (*resp. l'ensemble des caractères* $\neq 1$) *de* Δ *définis et irréductibles sur* Ω_p, *soit dans* $p \cdot A'$.

REMARQUE 7: La condition $b_i(\varphi_i) \in p \cdot A'$ ne dépend donc pas du choix du facteur φ de Φ.

REMARQUE 8: Sans doute, n'y a-t-il pas lieu de distinguer le cas $\varphi(\mathfrak{p}) = 1$ dans (i) comme le donne à penser les formules du théorème 3.

DÉMONSTRATION DU THÉORÈME 6 À PARTIR DU THÉORÈME 5:

(i) D'après le théorème 5, il s'agit de discuter si $f(T,\varphi)$ est inversible dans $A'[[T]]$. Pour cela, on utilise le théorème 2: $b_i(\varphi_i)$ ne diffère de $L_\mathfrak{p}(1-i,\varphi) = f(c^i - 1, \varphi)$ que par une unité de A'; en effet, on a ici $\pi = 1$, $m_i = 0$, ce qui entraîne l'inversibilité de $\tau(\varphi_i)$, cf. [14] chap. 22 §1 **G3**.

(ii) On utilise la formule (14) et on distingue deux cas.

cas $n = 0$: si p divise $[\mathcal{O}(F_0)^* : C_0]$, il divise $[e_\Lambda(\mathcal{O}(F_0)^*/C_0)]$ pour un caractère Λ de Δ au moins qui est alors ramifié. Alors p divise $[e_\Lambda(U_0/\bar{C}_0)]$ d'où le résultat d'après les formules du théorème 2 et du corollaire 1 du théorème 3.

cas $n \geq 1$: on sait, d'après la formule des classes invariantes appliquée à l'extension K_n/K où seul $\mathfrak{p}$ est ramifié, que p ne divisant pas $h(K)$ ne divise pas $h(K_n)$. On peut donc supposer que p divise $[e_\Phi(\mathcal{O}(F_n)^*/C_n)]$ et non $[e_\Phi(\mathcal{O}(F_0)^*/C_0)]$ pour un caractère $\Phi \neq 1$ au moins. On déduit que le noyau de l'application $e_\Phi(U_n/\bar{C}_n) \to e_\Phi(U_0/\bar{C}_0)$ induite par la norme est non trivial et on conclut comme pour la partie (i).

Appelons théorèmes 4′ et 5′ les versions affaiblies des théorèmes 4 et 5 où on suppose seulement que $g(T,\varphi)$ est un diviseur de $f(T,\varphi)$ dans $A'[[T]]$: le théorème 4′ est démontré au §4.3.

DÉMONSTRATION DU THÉORÈME 5′ À PARTIR DU THÉORÈME

4′: Définissons $\bar{\Omega}_n$ par le même procédé que $\bar{C}_n$, cf. §4.1; mais en partant du groupe $\Omega_{F_n^\varphi}$, cf. §3.2, où F_n^φ est la sous-extension de F_n/K_n correspondant au noyau de φ. A l'aide de [20] théorèmes 1 et 2, on montre que $e_\Phi \bar{C}_n = e_\Phi(\bar{\Omega}_n \cdot \bar{\Omega}_0)$, et que la norme induit des surjections de A-modules, cf. (2):

$$(21) \qquad \left.\begin{array}{ll} e_\Phi \bar{\Omega}_m \to e_\Phi \bar{\Omega}_n & \text{si } m > n > 0 \\ e_\Phi \bar{\Omega}_m \to (1-\varphi(\mathfrak{p}))\cdot e_\Phi \bar{\Omega}_0 & \text{si } m > 0. \end{array}\right\}$$

On en déduit que $\bar{C} = \varprojlim e_\Phi \bar{C}_n$ s'identifie à $\varprojlim e_\Phi \bar{\Omega}_n$. Considérons la norme dans F_n de $i_\infty^{-1}\theta(\rho_n', \alpha)$, avec α choisi comme dans le lemme 14: son image dans $\bar{C}_n$, multipliée par e_Φ, engendre le A-module $e_\Phi \bar{\Omega}_n$, cf. lemme 10 et (16). On trouve alors, en utilisant (21) ainsi que des considérations de rang, les isomorphismes, pour $n > 0$

$$e_\Phi \bar{\Omega}_n \simeq \begin{cases} A[[T]]/(\omega_n) & \text{si } \varphi(\mathfrak{p}) \neq 1 \\ A[[T]]/(\omega_n/T) & \text{si } \varphi(\mathfrak{p}) = 1. \end{cases}$$

qui montrent que pour $n > 0$

$$(22) \qquad e_\Phi \bar{C} \simeq A[[T]] \text{ et } e_\Phi \bar{\Omega}_n \simeq \begin{cases} e_\Phi \bar{C}/\omega_n(e_\Phi \bar{C}) & \text{si } \varphi(\mathfrak{p}) \neq 1 \\ e_\Phi \bar{C}/(\omega_n/T)(e_\Phi \bar{C}) & \text{si } \varphi(\mathfrak{p}) = 1. \end{cases}$$

On déduit alors de la proposition 2 que $e_\Phi(U_n/\bar{C}_n)$ est isomorphe à $e_\Phi Y_\infty/\omega_n \cdot e_\Phi Y_\infty$ si $\varphi(\mathfrak{p}) \neq 1$. Si $\varphi(\mathfrak{p}) = 1$, il figure dans la suite exacte

$$0 \to e_\Phi Y_\infty/(\omega_n/T)(e_\Phi Y_\infty) \to e_\Phi(U_n/\bar{C}_n) \to e_\Phi(U_n/V_n\bar{C}_n) \to 0$$

et on sait, comparer à [5] lemme 5, que $e_\Phi V_n$ est le noyau de la norme $e_\Phi U_n \to e_\Phi U_0$; ceci montre que $e_\Phi(U_n/V_n\bar{C}_n)$ est isomorphe par la norme à $e_\Phi(U_0^{p^n}/\Omega_0^{p^n}) \simeq e_\Phi(U_0/\bar{C}_0)$.

DÉMONSTRATION DES THÉORÈMES 4 ET 5 À PARTIR DES THÉORÈMES 4′ ET 5′:

D'après le corollaire 1 du théorème 3, on a

$$[e_\Lambda(U_n/\bar{C}_n)] \sim \left(\prod L_\mathfrak{p}(1, \varphi\pi)\right) \cdot [e_\Lambda(U_0/\bar{C}_0)]$$

où π parcourt l'ensemble des caractères $\neq 1$ de K_n/K et φ l'ensemble

des facteurs irréductibles de la décomposition de Λ sur Ω_p. En utilisant l'égalité $L_{\mathfrak{p}}(1, \varphi\pi) = f(\pi(c) - 1, \varphi)$, on obtient

$$[e_\Lambda(U_n/\bar{C}_n)] \sim [e_\Lambda(U_0/\bar{C}_0)] \cdot \prod_{\varphi} \prod_{\substack{\zeta^{p^n}=1 \\ \zeta \neq 1}} f(\zeta - 1, \varphi).$$

En comparant avec une évaluation analogue tirée du théorème 5', on montre que les produits $\Pi f(T, \varphi)$ et $\Pi g(T, \varphi)$ (où Φ parcourt l'ensemble des facteurs irréductibles de la décomposition de Λ sur $\mathbb{Q}_p$ et φ est *un* facteur de celle de Φ sur Ω_p) ne diffèrent que par un élément inversible de $A'[[T]]$. Il en est donc de même pour chaque Φ pour $f(T, \varphi)$ et $g(T, \varphi)$, d'où les théorèmes 4 et 5, à partir des théorèmes 4' et 5'.

4.3. *Démonstration du théorème* 4'

Pour Φ, φ et $\mathfrak{g}$ comme au §1, on pose si $u \in U$

$$\Delta_k(u) = \sum \varphi^{-1}(\sigma)\Delta_k^v((\sigma u)_v),$$

où σ parcourt Δ; σu est l'image de u par l'action de σ, cf. §2.1, et $(\sigma u)_v$ est sa composante sur U^v; Δ_k^v a été défini juste avant le lemme 6.

LEMME 15: *Soient $f(T) \in A[[T]]$ et u un élément du $A[[T]]$-module $e_\Phi U$; pour tout $k \geq 0$, on a $\Delta_k(f(T) \cdot u) = f(c^k - 1) \cdot \Delta_k(u)$.*

DÉMONSTRATION: La formule résulte de la définition de l'isomorphisme (2) si la série $f(T)$ est constante. Si $f(T) = 1 + T$, $(\sigma u)_v$ est remplacé par $\gamma(\sigma u)_v$, donc $F_{(\sigma u)_v}(W)$ est remplacé par $F_{(\sigma u)_v}([c]W)$, cf. §2.3. La définition de Δ_k^v donne alors la relation $\Delta_k((1 + T) \cdot u) = c^k \cdot \Delta_k(u) \cdot$ et le lemme s'obtient par linéarité et continuité.

REMARQUE 9: On déduit immédiatement de la définition de Δ_k et du lemme l'existence d'une série dans $A'[[T]]$, dont la valeur en $c^k - 1$ est précisément $\Delta_k(u)$, pour k entier ≥ 0 et $k \equiv i \bmod(p - 1)$.

Rappelons que pour $\alpha \in (p^{[H(E_{\mathfrak{g}})^v : \mathbb{Q}_p]} - 1) \cdot J_{\mathfrak{g}\mathfrak{p}}$, on a introduit l'unité de $H_{\mathfrak{g}\mathfrak{p}^{nf+1}}$,

$$u_{nf+1}(\alpha) = i_\infty^{-1}\theta(t^{-n}\rho + \rho_{nf+1}, \alpha);$$

En notant $\bar{u}_{nf+1}(\alpha)$ sa norme dans F_{nf}^{φ}, la sous-extension de F_{nf}/K_{nf} correspondant au noyau de φ, on peut énoncer:

PROPOSITION 5: *La suite des $\bar{u}_{nf+1}(\alpha)$ définit un élément $\bar{u}(\alpha)$ de U, et on a*

$$\Delta_k(\bar{u}(\alpha)) = C \cdot \sum_{\mathfrak{B} \in Cl(\mathfrak{g})} \varphi_i^{-1}(\mathfrak{B}) \cdot \psi(\mathfrak{B})^{-k} \cdot G^i_{u_v(\mathfrak{B}\alpha)}(c^k - 1),$$

pour tout $k \geq 0$ et $k \equiv i \bmod(p-1)$, avec $C \in \mathbb{Z}_p^*$, indépendant de k.

DÉMONSTRATION: La possibilité de définir $\bar{u}(\alpha)$ provient de celle de définir $u(\alpha)$ et $u_v(\alpha)$, cf. prop. 4 et sa démonstration. Pour $\mathfrak{B}$ parcourant un système de représentants de $Cl(\mathfrak{g}\mathfrak{p}^m)$ ($\mathfrak{g}\mathfrak{p}^m$, avec $m = 0$ ou 1, désignant le conducteur de φ), notons $\sigma_{\mathfrak{B}}$ (resp. $\sigma_{n,\mathfrak{B}}$) l'image de $[\mathfrak{B}, H_{\mathfrak{g}\mathfrak{p}}/K]$ par l'isomorphisme $\mathrm{Gal}(H_{\mathfrak{g}\mathfrak{p}}/K) \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{g}\mathfrak{p}} \cdot K_\infty/K_\infty)$ (resp. $\mathrm{Gal}(H_{\mathfrak{g}\mathfrak{p}}/K) \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{g}\mathfrak{p}^n}/K_{n-1})$). En passant par une somme sur $\mathrm{Gal}(F^{\varphi}_{\mathfrak{h}}/K)$, on démontre l'égalité où Δ_k^v est la fonction sur $U^v(H(E_{\mathfrak{g}\mathfrak{p}}))$ introduite au §2.3:

$$\Delta_k(\bar{u}(\alpha)) = [\ker \varphi] \sum \varphi^{-1}(\mathfrak{B}) \Delta_k^v((\sigma_{\mathfrak{B}} u(\alpha))_v).$$

Par ailleurs, on a $\sigma_{n,\mathfrak{B}} = [\mathfrak{B}, H_{\mathfrak{g}\mathfrak{p}^n}/K] \cdot [(b_n), H_{\mathfrak{g}\mathfrak{p}^n}/K]^{-1}$ avec $b_n \in \mathcal{O}(K)$, $b_n \equiv 1 \bmod \mathfrak{g}\mathfrak{p}$. Soit d le degré $[H(E_{\mathfrak{p}}) : K]$, en utilisant (1) et (3) avec $\rho = \rho_n$, on trouve $b_n^d \equiv \langle \psi(\mathfrak{B}) \rangle^d \bmod p^n$. En notant que $\langle \psi(\mathfrak{B}) \rangle \rho_n$ est bien défini modulo $\Omega_\infty \cdot \mathcal{O}(K)$, d'après (10) et (16) on obtient

$$\sigma_{n,\mathfrak{B}} i_\infty^{-1} \theta(\rho + \rho_n, \alpha) = i_\infty^{-1} \theta(\rho + \langle \psi(\mathfrak{B}) \rangle^{-1} \rho_n, \alpha\mathfrak{B}),$$

ce qui compte tenu du lemme 11 et de la prop. 4 donne

$$F_{(\sigma_{\mathfrak{B}} u(\alpha))_v}(\exp_G z) = F_{u_v(\alpha\mathfrak{B})}(\exp_G \langle \psi(\mathfrak{B}) \rangle^{-1} z)$$

d'où encore, cf. lemme 6 et définition de Δ_k^v pour $k \geq 0$, $k \equiv i \bmod(p-1)$

$$\Delta_k^v((\sigma_{\mathfrak{B}} u(\alpha))_v) = \langle \psi(\mathfrak{B}) \rangle^{-k} G^i_{u_v(\alpha\mathfrak{B})}(c^k - 1).$$

Pour obtenir la proposition, il suffit de remarquer-cf. (3), (10) et lemme 6 – que $\varphi_i(\mathfrak{B})^{-1} \psi(\mathfrak{B})^{-k} G^i_{u_v(\alpha\mathfrak{B})}(c^k - 1)$ ne dépend de $\mathfrak{B}$ que par son image dans $Cl(\mathfrak{g})$: On a $C = [\ker \varphi]$ si $m = 0$, et $C = [\ker \varphi](p-1)/e(\mathfrak{g})$ si $m = 1$.

DÉMONSTRATION DU THÉORÈME 4': Choisissons un isomorphisme

$e_\Phi U \xrightarrow{\sim} A[[T]]$, cf. prop. 1, et prenons α comme dans le lemme 14. Notons $g(T, \varphi)$ l'image de $\bar{u}(\alpha)$ (resp. u_1 l'image de la série 1) par l'isomorphisme précédent (resp. l'isomorphisme réciproque). On a donc (cf. arguments pour (22)):

$$e_\Phi Y_\infty \xrightarrow{\sim} A[[T]]/(g(T, \varphi)) \text{ et } \Delta_k(\bar{u}(\alpha)) = g(c^k - 1, \varphi)\Delta_k(u_1),$$

pour tout $k \geq 0$, cf. lemme 15. On déduit de la proposition 5 et de la remarque 9 que $g(T, \varphi)$ divise $f(T, \varphi)$.

Addendum

1. L'hypothèse (ii) du §0, n'est pas nécessaire, cf. la rédaction de mon exposé au séminaire Delange-Pisot–Poitou 1979–1980 (Paris). Il faut alors choisir convenablement E en fonction de φ.

2. Dans la proposition 3 et la définition de $b_k(\varphi)$ (§3.2 et 3.4), il y a lieu de rajouter le terme en s_2 pour $k = 2$.

3. On peut définir $L_\mathfrak{p}(s, \nu)$ pour ν sauvagemment ramifié: en reprenant la méthode du texte, on trouve que $f(T, 1)$, considérée dans le corps des fractions de $A'[[T]]$, ne diffère de $1/T$ que par une série inversible de $A'[[T]]$. La situation est similaire au cas cyclotomique classique.

4. Dans les théorèmes 5 et 5', il convient d'entendre par C_n le groupe des unités elliptiques de F_n, au sens de [20] §5, p. 47; le Ω_0 du texte est trop gros pour que (21) soit surjective pour φ non ramifié.

BIBLIOGRAPHIE

[1] N. ARTHAUD: On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication I. *Comp. Math. 37* (1978) 209–232, (II à paraître).

[2] P. CASSOU-NOGUES: On $\mathfrak{p}$-adic L-functions for elliptic curves I et II, (à paraître).

[3] J. COATES et W. SINNOTT: Integrality properties of the values of partial zeta functions. *Proc. London math. Soc., 34* (1977) 365–384.

[4] J. COATES et A. WILES: On the conjecture of Birch and Swinnerton-Dyer. *Inv. math., 39* (1977) 223–251.

[5] J. COATES et A. WILES: Kummer's criterion for Hurwitz numbers. *Kyoto conference on Algebraic Number Theory*, ed. by Iyanagua, Jap. Soc. for the promotion of Science 1977, pp. 9–23.

[6] J. COATES et A. WILES: On p-adic L-functions and elliptic units. *J. Austr. math. Soc. (Series A) 26* (1978) 1–25.

[7] R. COLEMAN: Division values in local fields. *Inv. math., 53* (1979) 91–116.

[8] R. GILLARD: Remarques sur les unités cyclotomiques et les unités elliptiques. *J. of Number Th., 11* (1979) 21–48.

[9] R. GILLARD: Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions II. *Ann. de l'Inst. Fourier, 29* (1979) 4, 1–15.

[10] R. GILLARD et G. ROBERT: Groupes d'unités elliptiques. *Bull. Soc. math. France, 107* (1979) 305–317.
[11] K. IWASAWA: On Z_l-extensions of algebraic number fields. *Ann. of math., 98* (1973) 246–326.
[12] N. KATZ: Formal groups and p-adic interpolation. *Astérisque 41–42* (1977) 55–65.
[13] N. KATZ: p-adic interpolation of real analytic Einsenstein Series. *Ann. of math., 104* (1976) 459–571.
[14] S. LANG: *Elliptic Functions*, Addison-Wesley, 1973.
[15] S. LANG: *Cyclotomic fields*, Springer-Verlag, 1978.
[16] S. LICHTENBAUM: On p-adic L-functions associated to elliptic curves. *Inv. math., 56* (1980) 19–55.
[17] J. LUBIN: One parameter formal Lie groups over p-adic integer rings. *Ann. of math., 80* (1964). 464–484.
[18] J. MANIN et M. VISHIK: p-adic Hecke series for imaginary quadratic fields. *Math. Sbornik, 95* (1974) 357–383.
[19] K. RIBET: *Fonctions L p-adiques et théorie d'Iwasawa*, cours rédigé par P. SATGÉ. Pub. math. Orsay (1979).
[20] R. ROBERT: Unités elliptiques. *Bull. Soc. math. France, mém. 36* (1971).
[21] G. ROBERT: Nombres de Hurwitz et unités elliptiques. *Ann. scient. Ec. Norm. Sup., 11* (1978) 297–389.
[22] J.-P. SERRE et J. TATE: Good reduction of abelian varieties. *Ann. of math., 88* (1968) 492–517.
[23] G. SHIMURA: *Introduction to the arithmetic theory of automorphic functions.* Iwanami Shoten, 1971.

(Oblatum 21-VIII-1979)

Laboratoire de Mathématiques Pures – Institut Fourier
dépendant de l'Université Scientifique et
Médicale de Grenoble associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)