BULLETIN DE LA S. M. F.

JACQUES TILOUINE

Fonctions L p-adiques à deux variables et $\mathbb{Z}_2^p$-extensions

Bulletin de la S. M. F., tome 114 (1986), p. 3-66

<http://www.numdam.org/item?id=BSMF_1986__114__3_0>

Bull. Soc. math. France,
114, 1986, p. 3-66.

FONCTIONS L p-ADIQUES A DEUX VARIABLES ET Z_p^2-EXTENSIONS

PAR

Jacques TILOUINE (*)

RÉSUMÉ. — Soit E une courbe elliptique définie sur un corps de nombres F, à multiplication complexe par le corps quadratique imaginaire K, telle que $F(E_{tors})/K$ soit abélienne. Pour presque tout nombre premier p, décomposé dans K, on donne une construction de la fonction L p-adique à deux variables attachée à la courbe E/F, généralisant celle de Yager (qui traitait la situation $F=K$), et à l'aide de cette fonction, on décrit, pour beaucoup de nombres premiers p, le groupe des points de E rationnels sur la Z_p^2-extension de F, composée de F et de la Z_p^2-extension de K.

ABSTRACT. — Let E/F be an elliptic curve with complex multiplication by K and such that $F(E_{tors})/K$ is abelian. We give, for almost all prime p which splits in K, a construction of the p-adic L function with two variables attached to the curve E/F, by generalizing Yager's technique. Furthermore, by using this function, we describe, up to torsion, the Mordell-Weil group of points of E rational on the Z_p^2-extension of F deduced from the one of K by compositum.

PLAN

(*) Texte reçu le 14 novembre 1983, révisé le 18 septembre 1985.

J. TILOUINE, Département de Mathématiques, Bât 425, Université Paris-Sud, 91405 Orsay Cedex.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE — 0037-9484/1986/01 3 64/$ 8.40

1. Introduction

1.1. Situation du problème

Soit F un corps de nombres et E/F une courbe elliptique définie sur F. Par le théorème de Mordell-Weil, on sait que le groupe $E(F)$ des points de E rationnels sur F est de type fini. Le problème central de l'arithmétique des courbes elliptiques est l'étude du rang $g_{E/F}$ de ce groupe. Une question importante dans cette direction est de déterminer la variation de ce rang lorsqu'on remplace le corps de base F par une extension finie. Le but de ce travail est d'apporter une contribution modeste à l'étude de ce problème lorsque la courbe E est à multiplication complexe par l'anneau des entiers $\mathcal{O}$ d'un corps quadratique imaginaire K contenu dans F. Comme on n'a pas de résultats d'algébricité des valeurs spéciales des fonctions L attachées à une courbe quelconque E/F avec multiplication complexe, on est conduit à introduire l'hypothèse de Shimura (*cf.* [19], théorème 7.44) : (S) l'extension $F(E_{\text{tors}})$ est abélienne sur K, où E_{tors} désigne l'ensemble des points de torsion de E. Nos résultats sur la variation du rang sont exprimés en termes de propriétés de fonctions L p-adiques à deux variables associées à E/F pour certains choix de nombres premiers rationnels p. Précisons donc ces choix. On suppose d'abord que p n'appartient pas à l'ensemble exceptionnel $\Sigma_{E/F}$ constitué des nombres premiers rationnels q tels que : $q=2$ où 3, la courbe E/F a mauvaise réduction en une place de F au-dessus de q, où q est ramifié dans F. D'autre part, on suppose que la courbe E/F a bonne réduction ordinaire en chaque place de F au-dessus

de p (ceci équivaut au fait que p est décomposé dans K, disons $(p)=\mathfrak{P}\mathfrak{P}^*$). Comme on l'explique en détail dans le chapitre 2, on construit une fonction L $\mathfrak{P}$-adique à deux variables, essentiellement unique, qui interpole des valeurs spéciales de fonctions L complexes associées à E/F (*voir* théorème 2.11.4 pour un énoncé précis). La technique de construction de cette fonction repose sur le travail récent de YAGER [29], [30] (qui traite le cas le plus simple $F=K$), d'après une idée qui remonte à COATES-WILES [5]. Une construction voisine a été donnée simultanément par DE SHALIT ([16], [17]), qui utilise aussi la technique de Yager. Notons que ces approches sont conceptuellement plus simples que celles de MANIN-VISHIK [31] et KATZ [12] qui utilisent des formes modulaires. Cependant, à cause de la présence d'un facteur parasite (noté $P(a, b)$ dans la formule du théorème 2.11.4), on est amené dans l'appendice à modifier la construction donnée au chapitre 2. Pour un p satisfaisant les hypothèses précédentes et premier au degré de F sur K, on obtient une branche « primitive » $G^{(1,\,0)}$ de la fonction L $\mathfrak{P}$-adique. C'est une série formelle à deux variables à coefficients dans un anneau p-adique complet I, qui interpole des valeurs spéciales de fonctions L complexes primitives et non affectées du facteur parasite. C'est à l'aide de cette branche primitive qu'on va énoncer le théorème central.

1.2. ÉNONCÉ DES RÉSULTATS

Soit $K_{\infty,\,\infty}$ la $\mathbb{Z}_p^2$-extension de K et $F'_{\infty,\,\infty}=FK_{\infty,\,\infty}$, on note $\Omega'_{\infty,\,\infty}$ le sous-groupe de torsion de $E(F'_{\infty,\,\infty})$, et pour toute $\mathbb{Z}_p$-extension L de F contenue dans $F'_{\infty,\,\infty}$, on note Ω_L le sous-groupe de torsion de $E(L)$. Soit Γ le groupe de Galois de $F'_{\infty,\,\infty}/F$, il est isomorphe à $\mathbb{Z}_p^2$. Grâce aux hypothèses sur p, on voit que la restriction des automorphismes induit un isomorphisme de Γ avec le groupe de Galois de $K_{\infty,\,\infty}$ sur K, on obtient donc une action de la conjugaison complexe c sur Γ qui fournit une décomposition $\Gamma=\Gamma^+\times\Gamma^-$ où

$$\Gamma^+=\{\gamma\in\Gamma;\ c\gamma c=\gamma\}\qquad\text{et}\qquad\Gamma^-=\{\gamma\in\Gamma,\ c\gamma c=\gamma^{-1}\}.$$

On note F_∞^+ la $\mathbb{Z}_p$-extension de F fixée par Γ^- et F_∞^- celle fixée par Γ^+. Ce sont les $\mathbb{Z}_p$-extensions cyclotomique et anticyclotomique. Soient σ et τ des générateurs topologiques de Γ^+ et Γ^- respectivement. Ils fournissent un isomorphisme de I-algèbres de $I[[S, T]]$ à $I[[\Gamma]]$ donné par $(S, T)\mapsto(\sigma-1, \tau-1)$. Par construction, la série $G^{(1,\,0)}$ est un élément de $I[[\Gamma]]$, on note $\mathscr{G}(S, T)$ son antécédent par l'isomorphisme ci-dessus.

Introduisons aussi le diviseur critique Θ défini dans [10] qui joue un rôle crucial dans l'étude par Greenberg de l'extension anticyclotomique.

THÉORÈME CENTRAL. — *Soit p un nombre premier satisfaisant les conditions ci-dessous :*

(i) $p \notin \Sigma_{E/F}$ et $p \nmid d$;

(ii) *la courbe E a bonne réduction ordinaire en chaque place au-dessus de p;*

(iii) *pour chaque place v de F au-dessus de p, p ne divise pas le nombre de points de la courbe réduite de E en v, rationnels sur le corps résiduel de F en v (i.e. p n'est pas anormal au sens de B. Mazur), supposons qu'il existe un entier $k \geqslant 0$ et une unité $u(S, T)$ de $I[[S, T]]$ tels que :*

$$\mathcal{G}(S, T) = \Theta^k . u(S, T),$$

alors

(1) *si $k = 0$, le groupe $E(F'_{\infty, \infty})$ est de torsion;*

(2) *sans condition sur k, on a :*

$$E(F'_{\infty, \infty})/\Omega'_{\infty, \infty} = E(F_\infty^-)/\Omega_{F_\infty^-},$$

(3) *pour toute $\mathbb{Z}_p$- extension L de F disincte de F_∞^- et contenue dans $F'_{\infty, \infty}$, le rang du groupe $E(L)/\Omega_L$ est fini.*

COMMENTAIRES. — (i) R. GREENBERG a remarqué en utilisant la conjecture principale qu'au moins lorsque la courbe est définie sur $\mathbb{Q}$, les seules valeurs possibles pour l'entier k semblent être 0 et 1 (il s'agit d'un raisonnement heuristique !).

(ii) On peut rapprocher le cas $k = 0$ avec un théorème de B. PERRIN-RIOU (corollaire 3.6 de [16]). Pour l'énoncer rappelons que le groupe de Shafarevitch-Tate $Ш_{E/L}$ de la courbe E/L est défini comme le noyau du morphisme produit des restrictions locales aux places finies,

$$\prod_v \mathrm{res}_v : \quad H^1(L, E) \to \prod_v H^1(L_v, E),$$

et le groupe de Selmer $S_{F'_{\infty, \infty}}$ est défini par l'exactitude de la suite :

$$0 \to E(F'_{\infty, \infty}) \otimes_{\mathcal{O}} (K_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}) \to S_{F'_{\infty, \infty}} \to Ш_{E/F'_{\infty, \infty}}[\mathfrak{P}^\infty] \to 0$$

(*cf.* 16, § 1). On sait alors que le dual de Pontrjagin de $S_{F'_{\infty, \infty}}$ est un $\mathbb{Z}_p[[\Gamma]]$-module de type fini et de torsion, on peut donc parler de sa série caractéristique. Le théorème s'énonce alors : si cette série caractéristique

est une unité, alors le groupe $E(F_{\infty,\infty})$ est de torsion et la composante $\mathfrak{P}$-primaire de $Ш_{E/F_{\infty,\infty}}$ est finie. Mais pour s'assurer que la série caractéristique est une unité, il faut supposer entre autre la trivialité de la partie $\mathfrak{P}$-primaire de $Ш_{E/F}$, ce qu'on ne sait pas vérifier en général. Dans le théorème prouvé dans ce travail, on n'obtient aucun renseignement sur le groupe de Shavarevitch-Tate de $E/F_{\infty,\infty}$, mais on ne fait aucune hypothèse quant à la finitude de celui de E/F.

1.3 Exemples

(1) *Cas* $k=0$. Remarquons d'abord que lorsque le nombre de Tamagawa de la courbe E/F est non nul (*cf.* chapitre II, § 3), on peut prouver aisément comme au lemme 12 de [14], que l'ensemble des nombres premiers p satisfaisant les hypothèses (i) à (iii) et tels que $\mathcal{G}(S, T)$ soit une unité, a une densité analytique >0. Donnons en outre quelques exemples numériques de cette situation lorsque E est définie sur $\mathbb{Q}$ et $F=K$.

(*a*) $E\,|\,y^2=x^3-x$, possède multiplication complexe par $\mathbb{Z}[i]$, on trouve dans la table de Birch et Swinnerton-Dyer la valeur

$$\sqrt{D_K}/2\times\tau(E/K)=2^{-4},$$

et on voit qu'il n'y a pas de nombres anormaux pour cette courbe, donc on conclut : si $p\equiv 1\ (4)$, si L est une p-extension abélienne finie non ramifiée hors de $(a+ib)$ et $(a-ib)$ avec $a^2+b^2=p$, du corps $K=\mathbb{Q}(i)$, alors $E(L)$ est fini.

(*b*) $E\,|\,y^2+xy=x^3-x^2-2x-1$, $E=X_0(49)$, à multiplication par $\mathbb{Z}[(1+\sqrt{-7})/2]$, on calcule $\sqrt{D_K}/2\times.\,\tau(E/K)=1/4$, donc si $p\equiv 1$, 2 ou 4 (mod. 7) et $p\neq 2$, alors pour toute p-extension L finie abélienne non ramifiée hors de

$$\left(a+b\frac{1+\sqrt{-7}}{2}\right)\quad\text{et}\quad\left(a+b-b\frac{1+\sqrt{-7}}{2}\right)$$

où $p=a^2+ab+2b^2$, de $K=\mathbb{Q}(\sqrt{-7})$, le groupe $E(L)$ est fini.

(*c*) $E\,|\,y^2=x^3-30x-56$, à multiplication par $\mathbb{Z}[\sqrt{-2}]$, on trouve $\sqrt{D_K}/2\,\tau(E/K)=4$, d'où la conclusion : si $p\equiv 1$ ou 3 (mod. 8) et $p\neq 3$, alors pour toute p-extension abélienne finie non ramifiée hors de $(a+b\sqrt{-2})$ et $(a-b\sqrt{-2})$ où $a^2+2b^2=p$ de $K=\mathbb{Q}(\sqrt{-2})$, on a $E(L)$ fini.

(2) *Cas général* ($k=0$ *ou* $\geqslant 1$). — On ne sait pas s'il y a une infinité de nombres p satisfaisant les hypothèses (i) à (iii) et pour lesquels $k=1$ convient. Mais on peut trouver dans les tables de [2] beaucoup d'exemples qui conviennent. Citons :

(*a*) $E\,|\,y^2=x^3=x^3-6x$, est à multiplication par $\mathbb{Z}[i]$ et $E(\mathbb{Q})$ est de rang 1. Par le théorème de Greenberg, on sait que Θ divise $\mathscr{G}$ et on trouve pour $p=5$ que $G^{(1,\,0)}(u^5-1,\,0)$ ne diffère de 5 que par une unité 5-adique, donc pour la $\mathbb{Z}_5^2$-extension de $\mathbb{Q}(i)$, les conclusions (2) et (3) du théorème central sont valables.

(*b*) $E\,|\,y^2=x^3-49x$ est à multiplication complexe par $\mathbb{Z}[i]$, et $E(\mathbb{Q})$ de même est de rang 1 donc Θ divise $\mathscr{G}$ pour tout p satisfaisant (i) à (iii). Pour $p=5$, on voit de plus que $G^{(1,\,0)}(u^5-1,\,0)$ est associé à 5, donc les conclusions (2) et (3) sont valides.

(*c*) $E\,|\,y^2=x^3-2x$ est de rang 1 et à multiplication par $\mathbb{Z}[i]$. Mais 5 est anormal et $25\,|\,G^{(1,\,0)}(u^5-1,\,0)$ on voit donc que le quotient G/Θ n'est pas une unité. On ne contrôle pas par le théorème central la variation du rang de cette courbe le long de la $\mathbb{Z}_5^2$-extension de $\mathbb{Q}(i)$.

2. Construction de la fonction L $\mathfrak{P}$-adique à deux variables

2.1. La courbe E/F et sa restriction des scalaires

La référence générale pour ce paragraphe est le paragraphe 4 de [9].

Soit E une courbe elliptique définie sur un corps de nombres F, à multiplication complexe par l'anneau des entiers $\mathcal{O}$ du corps quadratique imaginaire K. On suppose $K\subset F$, c'est-à-dire que tous les endomorphismes de E sont définis sur F, et on fixe une fois pour toutes une identification $\mathcal{O}=\mathrm{End}_F(E)$, de sorte que $\alpha\in\mathcal{O}$ agisse sur le F-espace vectoriel $H^0(E,\,\Omega^1_{E/F})$ comme l'homothétie de rapport $\alpha\in F$. Pour chaque α de $\mathcal{O}$, on note E_α le noyau de l'endomorphisme α de E, et si $\mathfrak{a}$ est un idéal de $\mathcal{O}$, on note $E_{\mathfrak{a}}$ l'intersection des E_α pour α parcourant $\mathfrak{a}$. On désigne par E_{tors} la réunion des E_α pour α parcourant $\mathcal{O}$. Dans ce travail, on utilisera de façon essentielle l'hypothèse (S) l'extension $F(E_{\mathrm{tors}})/K$ est abélienne.

Pour toute extension algébrique galoisienne K_2/K_1, on note $G(K_2/K_1)$ le groupe de Galois correspondant. On abrège $G(F/K)=H$, et on note d le degré de l'extension F/K. On observe que le groupe des points de E rationnels sur F n'est pas stable sous l'action de H et pour pallier à ce défaut, on est conduit (*cf.* [11], [28], chap. 1) à introduire la variété

abélienne $B = R_K^F(E)$ restriction des scalaires de F à K de la courbe E. Au paragraphe 4 de [9] sont données des conditions équivalentes à (S) faisant intervenir la variété B. On a besoin ici que de certaines d'entre elles, et nous allons les rappeler. Pour ce faire, on énonce d'abord l'importante proposition suivante. Soit A une variété abélienne définie sur un corps de nombres k, à multiplication complexe sur k par le corps de type CM L et soit θ un isomorphisme : $L \xrightarrow{\sim} \mathrm{End}_k(A) \otimes \mathbb{Q}$. On note J_k le groupe des idèles de k.

PROPOSITION 2.1.1. — *Pour A et θ comme ci-dessus, il existe un caractère de Hecke algébrique $\chi : J_k \to L^\times$, uniquement déterminé par les propriétés suivantes :*

(i) *pour tout α de $k^\times$, $\chi(\alpha)$ est l'élément de $L^\times$ égal au déterminant de l'homothétie de rapport α vue comme L-endomorphisme du L-espace vectoriel $H^0(A, \Omega^1_{A/k})$;*

(ii) *si S est un ensemble fini de places de k contenant les places de mauvaise réduction et les places à l'infini, si $x \in J_k$ et $x_v = 1$ pour tout v de S, on a*

$$\chi(x) = \prod_{v \notin S} \pi_v^{\mathrm{ord}_v(x_v)},$$

où π_v désigne l'entier de L tel que $\theta(\pi_v)$ soit le relèvement à la variété A de l'endomorphisme de Frobenius de la variété A_v, réduite de A en v.

Preuve. — C'est la formulation par Serre et Tate (théorème 10 de [18]) du théorème 1, chap. 13, p. 110 de [21]. Le caractère χ de la proposition s'appelle le caractère de Serre-Tate de A/k. On applique d'abord ce résultat à la courbe E définie sur F; on note, dans ce cas, ψ le caractère de Serre-Tate obtenu; on a en particulier pour $\alpha \in F^\times$, $\psi(\alpha) = N_{F/K}\alpha$. De plus, par le théorème de complète réductibilité de Poincaré, la variété B est isogène sur K à un produit de variétés abéliennes simples B_i $(i = 1, \ldots, r)$ définie sur K. On peut alors énoncer :

PROPOSITION 2.1.2. — *De l'hypothèse (S), il résulte que chaque composante simple B_i de B est de multiplicité 1 et est à multiplication complexe sur K par un corps de type CM T_i i.e. $T_i \xrightarrow{\sim} \mathrm{End}_K(B_i) \otimes \mathbb{Q}$. Soit de plus Φ_i le caractère de Serre-Tate de B_i/K, on a la relation : $\Psi = \Phi_i \circ N_{F/K}$ pour chaque $i = 1, \ldots, r$.*

La preuve de ce résultat est donnée au théorème 4.1 de [9]. Remarquons que le type CM de T_i est égal à l'ensemble des plongements de T_i dans $\mathbb{C}$

au-dessus de K puisque tous les endomorphismes de B_i sont définis sur K, c'est-à-dire que le corps réflexe de T_i coïncide avec K. De plus, par définition des B_i on a : $\mathrm{End}_k(B)\otimes\mathbb{Q}=\prod_{i=1}^{r} T_i$, on définit donc le caractère Φ de Serre-Tate de B par ses composantes $\Phi_i\, i=1,\ldots,r$, c'est donc un caractère continu de J_K vers $(\mathrm{End}_K(B)\otimes\mathbb{Q})$ muni de la topologie discrète, on peut donc parler de son conducteur f qui est un idéal de $\mathcal{O}$, et de son avatar, encore noté Φ, défini sur I_f, monoïde des idéaux de $\mathcal{O}$ premiers à f, et à valeurs dans $\mathrm{End}_K B$.

2.2. Plongements complexes

On fixe un modèle normal de Weierstrass de la courbe E sur F, et une forme différentielle de première espèce sur $E: y^2=4x^3-g_2x-g_3$, g_2 et $g_3\in F$, $\omega=dx/y$. On se donne alors un plongement complexe de $\bar{\mathbb{Q}}$, noté ι_∞ de sorte que l'image par ι_∞ de l'invariant algébrique $j(E)$ soit égale à l'invariant analytique $j(\mathcal{O})$ associé à la classe neutre des idéaux de K. On peut dès lors regarder l'ensemble $E^{\iota_\infty}(\mathbb{C})$, qu'on abrège en $E_{\mathbb{C}}$, comme une surface de Riemann de genre 1, contenue dans $\mathbb{P}^2(\mathbb{C})$, et la forme différentielle ω fournit une base de l'espace vectoriel de dimension un sur $\mathbb{C}$, $H^0(E, \Omega^1_{E/\mathbb{C}})$. De plus par l'accouplement d'intégration, on obtient un plongement de $H_1(E_{\mathbb{C}}, \mathbb{Z})$ dans $\mathbb{C}$, son image est un réseau qu'on note $\mathscr{L}$. Inversement, la donnée de $\mathscr{L}$ redonne $E_{\mathbb{C}}$ par la paramétrisation de Weierstrass :

$$W(.,\mathscr{L}):\quad \mathbb{C}/\mathscr{L}\xrightarrow{\sim} E_{\mathbb{C}},$$
$$z+\mathscr{L}\mapsto(z^3.\mathfrak{P}(z,\mathscr{L}), z^3.\mathfrak{P}'(z,\mathscr{L}), z^3).$$

Remarquons encore qu'à cause du choix de ι_∞ précisé ci-dessus, le $\mathcal{O}$-module $\mathscr{L}$ est libre. On fixe une base $\{\Omega\}$ de $\mathscr{L}$; Ω est un nombre complexe transcendant, comme il résulte aisément du théorème de Gelfond-Schneider.

Comme K est contenu dans F, il est aussi plongé dans $\mathbb{C}$ par ι_∞ et donc, on dispose d'un Grössencharakter ψ attaché à la courbe, au sens de Deuring-Weil, l'autre étant $\bar{\psi}$ (*voir* [19], théorème 5.5). Le caractère ψ est défini avec une notation évidente par la formule : pour tout $x\in J_F$

$$\psi(x)=\frac{\iota_\infty(\Psi(x))}{(N_{?,\mathfrak{r}}(x))_\infty}.$$

Notons $\mathscr{T} = \mathrm{End}_K(B) \otimes \mathbb{Q}$. Pour chaque élément v de $\mathrm{Hom}_K(\mathscr{T}, \mathbb{C})$, on définit également un Grössencharakter φ, attaché à la variété B/K, par la formule : pour tout x de J_K,

$$\varphi_v(x) = \frac{v(\Phi(x))}{x_\infty}.$$

Soit encore $\hat{H}$ le groupe des caractères complexes de H. On rappelle le résultat suivant (lemme 4.8 et son corollaire dans [9]) :

PROPOSITION 2.2.1. — (i) *pour tout* $v \in \mathrm{Hom}_K(\mathscr{T}, \mathbb{C})$, *on a* $\psi = \varphi_v \circ N_{F/K}$;

(ii) *pour* v_0 *fixé arbitraire, on a :*

$$\{\varphi_{v_0} \chi \in \hat{H}\} = \{\varphi_v,\ v \in \mathrm{Hom}_K(\mathscr{T}, \mathbb{C})\},$$

(iii) *le conducteur f de Φ est le plus petit commun multiple du conducteur de l'extension F/K et du conducteur de* φ_{v_0}.

Convention. — Lorsqu'on ne veut pas préciser l'élément v, on note seulement $\varphi = \varphi_v$.

2.3. FONCTION L DE HASSE-WEIL ET NOMBRE DE TAMAGAWA

Comme la courbe E/F est à multiplication complexe, on sait que sa mauvaise réduction est de type additif (*cf.* [18], théorème 6). Par conséquent, la fonction de Hasse-Weil de cette courbe peut être définie dans le demi-plan $\mathrm{Ré}(s) > 3/2$, par le produit eulérien :

$$L(E/F, s) = \prod_{v \text{ bonne reduction}} (1 - a_v N v^{-s} + N v^{1-2s})^{-1}.$$

Ici $N v$ désigne le cardinal du corps résiduel k_v de F en v, et a_v est la trace de l'endomorphisme de Frobenius. DEURING [8] a démontré qu'on peut décomposer cette fonction en produit de deux fonctions L de Hecke, à savoir :

$$L(E/F, s) = L(\psi, s)\, L(\bar{\psi}, s).$$

Il en résulte, en particulier, que la fonction L de Hasse-Weil a un prolongement analytique à tout le plan et y satisfait une équation fonctionnelle. On aura seulement besoin de la valeur en $s = 1$ de cette fonction.

On définit comme dans [3] des facteurs locaux m_v pour chaque place v de F :

Si v est une place archimédienne, on note

$$\Omega_{v,\,i}=\int_{\gamma_{v,\,i}}\omega\,(i=1,\,2)\qquad\text{où}\quad\{\gamma_{v,\,i}\}_{i=1,\,2}$$

est une base fixée de l'homologie entière de $E(F_v)$ (bien sûr $F_v=\mathbb{C}$), et on pose :

$$m_v=\frac{1}{2}\left|\Omega_{v,\,1}\bar{\Omega}_{v,\,2}-\bar{\Omega}_{v,\,1}\Omega_{v,\,2}\right|.$$

Si v est une place non archimédienne de bonne réduction, et $\omega_{\min,\,v}$ désigne la forme différentielle dx_v/y_v associée à un modèle minimal de E en v, on pose :

$$m_v=\left|\omega/\omega_{\min,\,v}\right|_v,$$

et si E a mauvaise réduction en v, on pose :

$$m_v=\left|\omega/\omega_{\min,\,v}\right|_v\times(E(F_v):E_0(F_v)).$$

$E_0(F_v)$ désignant le sous-groupe de $E(F_v)$ des points dont la réduction est non singulière.

DÉFINITION 2.3.1. — On appelle nombre de Tamagawa de E/F le nombre $\tau(E/F)=\prod_v m_v^{-1}\times L(E/F,\,1)$, le produit étant étendu à toutes les places v de F ce qui a du sens puisque $m_v=1$ pour presque tout v.

Rappelons que la conjecture de Birch et Swinnerton-Dyer prédit que si $\tau(E/F)$ est non nul, alors :

(i) le groupe $E(F)$ est de torsion,

(ii) on a l'égalité :

$$\tau(E/F).\frac{|D_F|^{1/2}}{2^d}=\frac{\#(Ш_{E/F})}{(\#E(F))^2}.$$

Sous l'hypothèse (S), le théorème de N. Arthaud affirme que (i) est vrai. Le point (ii) n'est évidemment pas connu, mais le théorème de rationalité du premier membre de l'égalité (ii) est prouvé, pour une courbe vérifiant (S), dans [9], proposition 7.8. On rappelle aussi que pour tout idéal $\mathfrak{a}$ de

$\mathcal{O}$ premier au conducteur f de Φ, $\Phi(\mathfrak{a})$ induit une isogénie, qu'on notera $\Phi(\mathfrak{a})_E$, de E à E^σ, pour $\sigma=(\mathfrak{a}, F/K)$, et qu'il y a $\Lambda(\mathfrak{a})\in F^\times$ tel que l'on ait :

$$\Phi(\mathfrak{a})_E^*(\omega^\sigma)=\Lambda(\mathfrak{a})\times\omega.$$

Pour les propriétés des nombres $\Lambda(\mathfrak{a})$ qu'on utilisera par la suite, *cf.* [9], § 4, ou [17] (5.4)-(5.8). Posons

$$m'=\prod_{v\,\infty}|\omega/\omega_{\min,\,v}|_v^{-1}$$

et fixons un générateur $\delta_{F/K}$ du discriminant relatif de F/K. On note $N_{k/\mathbb{Q}}$ la norme absolue de K.

PROPOSITION 2.3.2. — *On a l'égalité :*

$$\tau(E/F)\frac{|D_F|^{1/2}}{2^d}=2^{-\alpha}.3^{-\beta}.(\prod_{\mathfrak{a}}N\mathfrak{a})^{-1}$$
$$\times m'\times N_{K/\mathbb{Q}}(\prod_{\mathfrak{a}}(\Lambda(\mathfrak{a})\Omega)^{-1}\times\delta_{F/K}^{1/2}\times L(\bar{\psi},\,1)),$$

où α *et* β *sont deux entiers* $\geqslant 0$, *et* $\mathfrak{a}$ *parcourt un système arbitraire d'idéaux de* $\mathcal{O}$ *premiers à* f *dont les symboles d'Artin relatifs à* F/K *décrivent exactement* H.

Preuve. — On a $L(E/F,\,1)=L(\bar{\psi},\,1)\overline{L(\bar{\psi},\,1)}$, et on fait les remarques suivantes sur les facteurs locaux m_v.

Si v est archimédienne, v correspond à un plongement complexe qui s'écrit de façon unique $\iota_\infty\circ\sigma$ pour un σ de H, et on a :

$$m_v=|\Lambda(\mathfrak{a})\Omega|^2\times N\mathfrak{a}^{-1}\times\frac{|D_K|^{1/2}}{2}.$$

En effet, soit $(\gamma_1,\,\gamma_2)$ une base de $H_1(E(\mathbb{C}),\,\mathbb{Z})$ et $(\gamma_1',\,\gamma_2')$ une base de $H_1(E^\sigma(\mathbb{C}),\,\mathbb{Z})$, notons $(\gamma_1^{\mathfrak{a}},\,\gamma_2^{\mathfrak{a}})$ l'image par

$$\Phi(\mathfrak{a})_2:\quad H_1(E(\mathbb{C}),\,\mathbb{Z})\to H_1(E^\sigma(\mathbb{C}),\,\mathbb{Z})\ \text{de}\ (\gamma_1,\,\gamma_2).$$

Comme $\operatorname{Ker}\Phi(\mathfrak{a})_E=E_{\mathfrak{a}}$, on sait par la suite exacte d'homologie qu'il y a $A\in M_2(\mathbb{Z})$ telle que :

$$\begin{pmatrix}\gamma_1^{\mathfrak{a}}\\ \gamma_2^{\mathfrak{a}}\end{pmatrix}=A\begin{pmatrix}\gamma_1'\\ \gamma_2'\end{pmatrix}\qquad\text{et}\qquad\det A=\#E_{\mathfrak{a}}=N\mathfrak{a},$$

par conséquent :

$$\begin{pmatrix} \int_{\gamma_1}^{\mathfrak{a}} \omega^\sigma \\ \int_{\gamma_2}^{\mathfrak{a}} \omega^\sigma \end{pmatrix} = A \begin{pmatrix} \int_{\gamma_1} \omega^\sigma \\ \int_{\gamma_2} \omega^\sigma \end{pmatrix}$$

or,

$$\int_{\gamma_i}^{\mathfrak{a}} \omega^\sigma = \int_{\gamma_i} \Phi(\mathfrak{a})_E^* \omega^\sigma = \Lambda(\mathfrak{a}) \int_{\gamma_i} \omega \qquad (i=1, 2),$$

donc en reportant dans la définition de m_v on trouve :

$$|\det A| \times m_v = |\Lambda(\mathfrak{a})\Omega|^2 \times \frac{|D_K|^{1/2}}{2}.$$

Si v est une place de mauvaise réduction, il est prouvé dans [24], p. 46 que $(E(F_v): E_0(F_v))$ divise 12.

On applique alors ces remarques pour transformer $\tau(E/F)$ et on utilise la proposition 7.2 de [9], affirmant que $\sqrt{\delta_{F/K}} \prod_{\mathfrak{a}} (\Lambda(\mathfrak{a})\Omega)^{-1} \times L(\bar{\Psi}, 1) \in K$. On obtient ainsi le résultat.

2.4. Les nombres premiers considérés et les objets qui en dépendent

Soit p un nombre premier $\neq 2,3$ au-dessus duquel la courbe E/F a bonne réduction ordinaire. On sait que ceci entraîne que p est décomposé dans K. Notons $\mathfrak{P}$ et $\mathfrak{P}^*$ les facteurs premiers de $p\mathcal{O}$. On note $\mathcal{O}_{\mathfrak{P}}$ le complété $\mathfrak{P}$-adique de $\mathcal{O}$. On considère l'anneau I, complété du produit tensoriel par $\mathcal{O}_{\mathfrak{P}}$ de l'anneau des entiers de $F(E_{\mathfrak{P}^\infty})$. On dispose donc d'un plongement $\iota_{\mathfrak{P}}$ de $F(E_{\mathfrak{P}^\infty})$ dans $I \otimes \mathbb{Q}_p$, qui induit une identification désormais tacite entre le complété $\mathfrak{P}$-adique de K et $\mathbb{Q}_p$. Soit de plus G le groupe de Galois de $F(E_{p^\infty})/F$; comme l'a remarqué Weil on peut définir, pour tout caractère de Hecke algébrique de la forme $\Lambda = \Psi^a \bar{\Psi}^b$, avec a et b dans $\mathbb{Z}$, un caractère $\lambda_{\mathfrak{P}}$ de G dans $\mathbb{Z}_p^*$ (*cf.* [26]); en particulier, $\psi_{\mathfrak{P}}$ est le caractère d'action de G sur $E_{\mathfrak{P}^\infty}$, et $\bar{\psi}_{\mathfrak{P}}$ donne l'action de G sur $E_{\mathfrak{P}^{*\infty}}$. On ajoute dorénavant l'hypothèse que p n'est pas ramifié dans F, et on sait alors qu'on obtient un isomorphisme :

$$\psi_{\mathfrak{P}} \times \bar{\psi}_{\mathfrak{P}} : \quad G \xrightarrow{\sim} \mathbb{Z}_p^\times \times \mathbb{Z}_p^+.$$

On suppose également que le modèle de Weierstrass choisi est minimal en chaque place au-dessus de p. On pose pour n'importe quelle place v de F au-dessus de p: $\pi=\psi(v)$. On sait (DEURING [8]) que π est un générateur de l'idéal de $\mathcal{O}: N_{F/K} v$. On introduit alors les notations :

NOTATIONS 2.4.1. — (i) Pour n et m deux entiers >0 arbitraires, on pose :

$$F_m=F(E_{\pi^m+1}), \qquad \mathcal{F}_n=F(E_{\pi^n+1}), \qquad F_{n,m}=F_m\cdot\mathcal{F}_n,$$

et

$$F_\infty=\bigcup_{m\geq 0} F_m, \qquad \mathcal{F}_\infty=\bigcup_{n,m} F_{n,m}.$$

(ii) pour $\mathfrak{g}$ un idéal fixé, multiple principal de f et premier à p, on pose :

$$\mathcal{R}_m=F_m(E_\mathfrak{g}), \qquad \mathcal{R}_{n,m}=F_{n,m}=F_{n,m}(E_\mathfrak{g}),$$

et $\mathcal{R}_\infty=\bigcup_{m\geq 0}\mathcal{R}_m$.

(iii) en désignant par $\mathcal{O}_T$ l'anneau des entiers d'un corps de nombres T, on pose

$$J=\mathcal{O}_F\otimes_\mathcal{O}\mathcal{O}_\mathfrak{P}, \qquad I_m=\mathcal{O}_{F_m}\otimes\mathcal{O}_\mathfrak{P}, \qquad I'_m=\mathcal{O}_{R_m}\otimes\mathcal{O}_\mathfrak{P}.$$

LEMME 2.4.2. — (i) *Pour tout idéal* $\mathfrak{g}$ *de* $\mathcal{O}$ *multiple de* f, *le corps* $F(E_\mathfrak{g})$ *coïncide avec le corps des rayons modulo* $\mathfrak{g}$ *de* K.

(ii) $\mathcal{F}_n/F$ *est une extension cyclique totalement ramifiée en chaque place* v *de* F *au-dessus de* $\mathfrak{P}$, *de degré égal à* $q^n\varphi(q)$ *où* $q=\#k_v=Nv$, *et* φ *est l'indicatrice d'Euler. Le conducteur de* $\mathcal{F}_n$ *sur* K *est égal à* $f\pi^{n+1}$.

(iii) F_m/F *est non ramifiée en chaque place* v *divisant* $\mathfrak{P}$ *et le nombre* g_k *de places de* $F(E_{\mathfrak{P}^{k+1}})$ *au-dessus de* v *est de la forme :*

$$g_k=g_0p^k \quad \text{si} \quad k=0,\ldots,K,$$
$$g_k=g_0p^K \quad \text{si} \quad k\geq K,$$

où $K=\mathrm{ord}_\mathfrak{P}(\log_\mathfrak{P}(\pi))-1$.

(iv) *Les extensions* F_m *et* $\mathcal{F}_n$ *sont linéairement disjointes sur* F.

Preuve. — (i) C'est le lemme 4.7 de [9].

(ii) Ce fait classique est prouvé dans le chapitre 2 du cours de COATES [3].

(iii) F_m/F n'est pas ramifiée en v puisque le conducteur de F_m/K est $f\bar{\pi}^{m+1}$ par le point (ii). De plus, en faisant agir $G(F(E_{\mathfrak{P}^{*k}})/F)$ sur $E_{\mathfrak{P}^{*k}}$, on obtient le diagramme commutatif :

$$\begin{array}{ccc} G(F(E_{\mathfrak{P}^{*k}})/F) & \tilde{\to} & (\mathcal{O}/\mathfrak{P}^{*k})^{\times} \\ \cup & & \cup \\ D_v & \tilde{\to} & \langle \pi \rangle_k^{\mathbb{Z}}, \end{array}$$

où D_v désigne le groupe de décomposition de w/v où w est n'importe quelle place de $F(E_{\mathfrak{P}^{*k}})$ divisant v (parce que l'extension est abélienne), et $\langle \pi \rangle_k^{\mathbb{Z}}$ désigne le groupe cyclique engendré par l'image de π dans $(\mathcal{O}/\mathfrak{P}^{*k})^{\times}$. Les lignes sont des isomorphismes par le lemme 2.5 de [3], on voit alors que l'indice des groupes de droite du diagramme est de la forme voulue.

Le point (iv) résulte clairement de (ii) et (iii).

2.5. Le groupe formel de la courbe et les isogénies formelles

Rappelons d'abord que toutes les courbes E^{σ}, $\sigma \in H$ sont F-isogènes. Ceci résulte directement de l'invariance sous H du Grössencharakter ψ de E/F, et du théorème 10.2.1 de [11]. On voit cela plus explicitement à l'aide des morphismes $\Phi(\mathfrak{a})_E : E \to E^{\sigma}$, qui sont non nuls par la formule (4.10) de [9] : pour

$$P \in E_{\mathfrak{g}} \quad \text{avec } (\mathfrak{g}, \mathfrak{a}) = 1, \qquad P^{(\mathfrak{a}, F(E_{\mathfrak{g}})/K)} = \Phi(\mathfrak{a})_E(P).$$

On sait aussi que $\operatorname{Ker} \Phi(\mathfrak{a})_E = E_{\mathfrak{a}}$. Donnons une preuve directe de cette affirmation : si $\alpha \in \mathfrak{a}$, $\alpha \equiv 1 (f)$, on a

$$\alpha \mathcal{C} = \mathfrak{a}\mathfrak{b} \qquad \text{et} \qquad \Phi(\mathfrak{b})\Phi(\mathfrak{a}) = \alpha \quad \text{dans } \operatorname{End}_K(B),$$

donc on a l'inclusion :

$$\operatorname{Ker} \Phi(\mathfrak{a})_E \subset \bigcap_{\alpha \in \mathfrak{a}} E_{\alpha},$$

et cette intersection coïncide avec $E_{\mathfrak{a}}$ par le lemme d'approximation. De plus comme B est autoduale et que la dualité des isogénies coïncide avec la conjugaison complexe de $\operatorname{End}_K(B)$, on a :

$$\sharp \operatorname{Ker} \Phi(\mathfrak{a})_E = d^{\circ} \Phi(\mathfrak{a})_E = \Phi(\mathfrak{a})_E)^* = \mathrm{N}\,\mathfrak{a} = \sharp E_{\mathfrak{a}},$$

d'où l'égalité.

Plus généralement pour $\tau \in H$, on note $\Phi(\mathfrak{a})_{E^\tau}$ l'isogénie de E^τ dans $E^{\sigma\tau}$ induite par $\Phi(\mathfrak{a})$ et on voit aisément que $\Phi(\mathfrak{a})_E^\tau = \Phi(\mathfrak{a})_{E^\tau}$. On introduit alors le groupe formel $\hat{E}$ défini sur $J \cap F$ associé à la courbe E vue sur J, le paramètre t de $\hat{E}$ étant fixé par $t = -2x/y$. Comme E a bonne réduction ordinaire au-dessus de p, le groupe $\hat{E}$ est de hauteur 1, et est un module formel sur $\mathcal{O}_{\mathfrak{P}}$ qu'on a identifié à $\mathbb{Z}_p$, on peut en faire une théorie très analogue à celle de Lubin-Tate (elle est exposée dans [22]).

On note $\hat{\mathbb{G}}_a$ le groupe formel additif, vu sur $J \otimes \mathbb{Q}_p$. On note $\log_E$ le logarithme elliptique de $\hat{E}$, c'est-à-dire l'unique isomorphisme de $\hat{E}$ à $\hat{\mathbb{G}}_a$ tel que $d/dt \log_E(t)|_{t=0} = 1$; il est défini sur F, et satisfait la relation suivante : Soit

$$E_1(J) = \cap_{v \mid \mathfrak{P}} E_{1,v}(J)$$

où $E_{1,v}(J)$ est le noyau de la réduction en v de $E(J)$, pour $\omega = dx/y$ vue sur J, on a :

$$\omega|_{E_1(J)} = d(\log_{(t)}).$$

On note $\mathbf{e}_E$ l'isomorphisme inverse de $\log_E$; il satisfait l'égalité :

$$t = \mathbf{e}_E(z) = -\frac{2\mathfrak{P}(z, \mathscr{L})}{\mathfrak{P}'(z, \mathscr{L})} = z + \frac{1}{10} g_2 z^3 + \dots$$

Si l'on remplace E par E^σ pour un σ de H, on obtient aisément les formules :

$$\hat{E}^\sigma = E^\sigma, \quad \log_{E^\sigma}(t) = (\log_E)^\sigma(t), \qquad \mathbf{e}_{E^\sigma}(z) = (\mathbf{e}_E)^\sigma(z).$$

Si on note (x_σ, y_σ) un point de E^σ, on note t_σ le paramètre sur E^σ défini par $-2x_\sigma/y_\sigma = t_\sigma$.

Soit maintenant λ une isogénie de E vers E^σ définie sur J; par restriction à $E_1 = \cap_{v \mid \mathfrak{P}} E_{1,v}$ où $E_{1,v}$ est le noyau de la réduction en v, on définit une isogénie $[\lambda] : \hat{E} \to \hat{E}^\sigma$, caractérisée par la propriété que pour toute J-algèbre A complète pour la topologie de son radical, le diagramme suivant soit commutatif :

$$\begin{array}{ccc} E_1(A) & \xrightarrow{\lambda|} & E_1^\sigma(A) \\ {\scriptstyle t}\downarrow & & \downarrow{\scriptstyle t_\sigma} \\ \hat{E}(\mathrm{rad}\ A) & \xrightarrow{[\lambda]} & \hat{E}^\sigma(\mathrm{rad}\ A) \end{array}$$

les applications verticales étant données par :

$$(x, y) \mapsto t = -\frac{2x}{y} \quad \text{et} \quad (x_\sigma, y_\sigma) \mapsto t_\sigma = -\frac{2x_\sigma}{y_\sigma}.$$

Lorsque $\lambda = \Phi(\mathfrak{a})_E$, on abrège : $[\Phi(\mathfrak{a})_E] = [\Phi(\mathfrak{a})]$.

LEMME 2.5.1. — *Pour tout idéal* $\mathfrak{a}$ *de* $\mathcal{O}$ *premier à* f, *on a :*

(i) $[\Phi(\mathfrak{a})](t) \equiv \Lambda(\mathfrak{a})\, t \pmod{t^2}$,

(ii) $\operatorname{Ker}[\Phi(\mathfrak{a})] = (\hat{E})_\mathfrak{a}$, *et en particulier, si* $(\mathfrak{a}, \mathfrak{P}) = 1$ $[\Phi(\mathfrak{a})]$ *est un isomorphisme de* $\hat{E}$ *à* $\hat{E}^\sigma$.

Preuve. — Par la définition même de $\Lambda(\mathfrak{a})$, on a l'égalité :

$$\Phi(\mathfrak{a})(W(z, \mathscr{L})) = W(\Lambda(\mathfrak{a})\, z, \mathscr{L}_\sigma),$$

et pour $P = W(z, \mathscr{L})$, on a : $t_\sigma(\Phi(\mathfrak{a})(P)) = [\Phi(\mathfrak{a})](t)$ par définition de l'isogénie formelle, donc

$$[\Phi(\mathfrak{a})](t) = t_\sigma(W(\Lambda(\mathfrak{a})\, z, \mathscr{L}_\sigma)) = \mathbb{E}_{E^\sigma}(\Lambda(\mathfrak{a})\, z) \equiv \Lambda(\mathfrak{a}) \times z \pmod{z^2},$$

et comme $z \equiv t \pmod{t^2}$, on obtient la congruence (i). Pour le point (ii), il suffit de remarquer que $\operatorname{Ker}(\Phi(\mathfrak{a})_E)|_{E_1} = E_\mathfrak{a} \cap E_1$, et de transposer cette égalité dans $\hat{E}$.

2.6. LES ISOMORPHISMES ENTRE LE GROUPE FORMEL MULTIPLICATIF ET LE GROUPE FORMEL DE LA COURBE

Soit $I^{n.r.}$ le complété p-adique de l'anneau $\varinjlim_{(n,\, p)=1} I[\mu_n]$ qui s'identifie au produit des extensions non ramifiées maximales des anneaux locaux, en nombre fini, qui composent I. Notons φ_0 le Frobenius absolu (arithmétique) agissant sur $I^{n.r.}$. On va démontrer (à la main) le résultat suivant :

PROPOSITION 2.6.1. — *Pour toute unité* γ *de* $I^{n.r.}$, *telle que :* $\gamma^{\varphi_0 - 1} = \Lambda(\mathfrak{P})/p$, *il existe un unique isomorphisme* $\eta : \mathbb{G}_m \to E$ *tel que* $\eta'(0) = \gamma$, *et* η *est alors défini sur* I *donc en fait* $\gamma \in I$.

Preuve. — Elle est analogue à la construction de la fin de l'article de LUBIN et TATE [15].

(*a*) Cherchons d'abord une série $\eta(T) \in I^{n.r.}[[T]]$ telle que

$$\eta^{\varphi_0}([p]_{\mathbb{G}_m}(T)) = [\Phi(\mathfrak{P})] \circ \eta(T),$$

et dont la dérivée à l'origine soit γ. En dérivant à l'origine les deux membres, on trouve $\gamma^{\varphi_0 - 1} = \Lambda(\mathfrak{P})/p$, puis on procède par approximations successives : supposons qu'on dispose d'un polynôme η_r de degré $\leqslant r$ tel que

$$\eta_r^{\varphi_0}([p]_{\mathbb{G}_m}(T)) \equiv [\Phi(\mathfrak{P})] \circ \eta_r(T) \quad (\text{modulo } T^{r+1}),$$

cherchons $\eta_{r+1}(T) = \eta_r(T) + x\,T^{r+1}$, où $x \in I^{n \cdot r}$, tel que

$$\eta_{r+1}^{\varphi_0}([p](T)) \equiv [\Phi(\mathfrak{P})]\,\eta_{r+1}(T) \quad (\text{mod } T^{r+2}).$$

En développant cette expression, on est amené à résoudre : $x^{\varphi_0} p^{r+1} - x\,\Lambda(\mathfrak{P}) = a$, où a est donné par :

$$\eta_r^{\varphi_0}([p]_{\mathfrak{g}_m} T) \equiv [\Phi(\mathfrak{P})]\,\eta_r(T) + a\,T^{r+1} \quad (\text{mod } T^{r+2}).$$

Réduisons cette équation modulo p :

$$\bar{\eta}_r^{(p)}(T^p) \equiv (\bar{\eta}_r(T))^p + \bar{a}\,T^{r+1} \quad (\text{mod. } T^{r+2}),$$

parce que $\overline{[\Phi(\mathfrak{P})]}(T) = T^p$, par définition même de $\Phi(\mathfrak{P})_E : E \to E^{\sigma_{\mathfrak{P}}}$ comme relèvement du morphisme de Frobenius $\tilde{E}_v \to \tilde{E}_v^{(p)}$. Donc $\bar{a} = 0$ et ainsi, $p \mid a$. Or, il est facile de voir que $\Lambda(\mathfrak{P})/p$ est une unité de J par exemple en utilisant la propriété de 1-cocycle de Λ : si f est le degré résiduel de F sur K, on a :

$$\pi = \Lambda(\mathfrak{P}^f) = \Lambda(\mathfrak{P})^{1 + \varphi_0 + \cdots + \varphi_0^{f-1}},$$

donc $|\pi|_p = |\Lambda(\mathfrak{P})|_p^f$, et comme $\pi\mathcal{O} = \mathfrak{P}^f$, on a $|\pi|_p = |p|_p^f$. On conclut donc que pour chaque $r \geqslant 1$, il existe un x unique de $I^{n \cdot r}$ répondant au problème. D'où l'existence et l'unicité de η.

(*b*) Montrons alors que η est un isomorphisme de $\mathbb{G}_m$ à $\hat{E}$. Rappelons d'abord que E et $\mathbb{G}_m$ étant de hauteur 1, leur anneau d'endomorphismes total est forcément égal à $\mathbb{Z}_p$ (c'est un $\mathbb{Z}_p$-module libre de rang inférieur à la hauteur, égale ici à 1, pour les détails, *cf.* LUBIN [14]). Par conséquent les endomorphismes de $\hat{E}$ s'approximent par des endomorphismes globaux de E.

Montrons que :

(i) $\hat{E}(\eta\,\mathfrak{X},\ \eta\,\mathfrak{y}) = \eta(\mathbb{G}_m(\mathfrak{X},\ \mathfrak{y}))$,

(ii) $\eta([a]_{\mathfrak{g}_m} T) = [a]_E\,\eta(T)$.

Posons $F(\mathfrak{X}, \mathfrak{y}) = \eta^{-1} \circ \hat{E}(\eta\,\mathfrak{X}, \eta\,\mathfrak{y})$; on va montrer que ce groupe formel est le groupe de Lubin-Tate associé à $f(T) = [p]_{G_m}(T)$. On a d'abord

$$F(\mathfrak{X}, \mathfrak{y}) \equiv \mathfrak{X} + \mathfrak{y} \pmod{(\mathfrak{X}, \mathfrak{y})^2},$$

et de plus $F^{\varphi_0}(f(\mathfrak{X}), f(\mathfrak{y})) = f(F(\mathfrak{X}, \mathfrak{y}))$, en effet :

$$F^{\varphi_0}(f(\mathfrak{X}), (\mathfrak{y})) = (\eta^{-1})^{\varphi_0} \circ ([\Phi(\mathfrak{P})]\,\mathfrak{X}, [\Phi(\mathfrak{P})]\,\mathfrak{y}),$$

parce que $\eta^{\varphi_0}(f(T)) = [\Phi(\mathfrak{P})]\,\eta(T)$ (c'est le point (a)).

De plus, par définition de $[\Phi(\mathfrak{P})]$, on a :

$$\hat{E}^{\varphi_0}([\Phi(\mathfrak{P})]\,\mathfrak{X}, [\Phi(\mathfrak{P})]\,\mathfrak{y}) = [\Phi(\mathfrak{P})](\hat{E}(\mathfrak{X}, \mathfrak{y})),$$

et on applique à nouveau (a) pour conclure.

De même pour $C(T) = \eta^{-1} \circ [a]_{\hat{E}} \circ \eta(T)$, on voit que $C(T) \equiv T \pmod{T^2}$, et on montre que $C^{\varphi_0}(f(T)) = f(C(T))$ en utilisant les égalités

$$[a]^{\varphi_0}_{\hat{E}} \circ [\Phi(\mathfrak{P})] = [a]_{\hat{E}^{\varphi_0}} \circ [\Phi(\mathfrak{P})] = [\Phi(\mathfrak{P})] \circ [a]_{\hat{E}},$$

qui résultent de la définition de $[\Phi(\mathfrak{P})]$ lorque $a \in \mathcal{O}$ et se déduisent de là par densité de $\mathcal{O}$ dans $\mathbb{Z}_p$, pour tout a, et il reste à prouver le lemme :

Soit $f(T)$ une série formelle à une variable à coefficients dans $I^{n,r}$, telle que

$$\begin{cases} f(T) \equiv \bar{\omega}\,T & (\mathrm{mod}\ T^2), \\ f(T) \equiv T^p & (\bar{\omega}\,I^{n,r}[[T]]), \end{cases}$$

$\bar{\omega}$ désignant une uniformisante de $I^{n,r}$. Alors, étant donné une forme linéaire $l(\mathfrak{X}_1, \ldots, \mathfrak{X}_n)$, il existe une unique série $F(\mathfrak{X}_1, \ldots, \mathfrak{X}_n)$ telle que

$$F(\mathfrak{X}_1, \ldots, \mathfrak{X}_n) \equiv l(\mathfrak{X}_1, \ldots, \mathfrak{X}_n) \qquad \mathrm{mod}(\mathfrak{X}_1, \ldots, \mathfrak{X}_n)^2,$$
$$F^{\varphi_0}(f(\mathfrak{X}_1), \ldots, f(\mathfrak{X}_n)) = f(F(\mathfrak{X}_1, \ldots, \mathfrak{X}_n)).$$

Preuve. — (Strictement analogue au lemme 1.1 de [15]), on procède par approximations successives :

On pose $F_1 = l$, et si l'on a construit un polynôme F_r de degré $\leqslant r$ tel que :

$$F_r(f(\mathfrak{X}_1), \ldots, f(\mathfrak{X}_n)) \equiv f(F_r(\mathfrak{X}_1, \ldots, \mathfrak{X}_n)) \pmod{(\mathfrak{X}_1, \ldots, \mathfrak{X}_n)^{r+1}},$$

on cherche F_{r+1} sous la forme $F_r+\Delta_{r+1}$, où Δ_{r+1} est un polynôme homogène de degré $(r+1)$ en $\mathfrak{X}_1, \ldots, \mathfrak{X}_n$.

On voit facilement qu'on est amené à résoudre :

$$\bar{\omega}\Delta_{r+1}-\bar{\omega}^{\varphi_0^{r+1}}\Delta_{r+1}^{\varphi_0} \equiv F_r^{\varphi_0}(f(\mathfrak{X}_1), \ldots, f(\mathfrak{X}_n))$$
$$-f(F_r(\mathfrak{X}_1, \ldots, \mathfrak{X}_n)) \qquad (\mathrm{mod}\ (\mathfrak{X}_1, \ldots, \mathfrak{X}_n)^{r+2}),$$

or, en réduisant le second membre de cette congruence modulo $\bar{\omega}$, on trouve $\bar{F}_r^{(p)}(\mathfrak{X}_1^p, \ldots, \mathfrak{X}_n^p)-(\bar{F}_r(\mathfrak{X}_1, \ldots, \mathfrak{X}_n))^p=0$, donc tous les coefficients du second membre sont divisibles par $\bar{\omega}$, d'où l'on tire aisément l'existence et l'unicité de F_{r+1}, et, par récurrence, de F.

On applique ce lemme à $f(T)=[p]_{\mathbb{G}_m}(T)$ et, pour $n=1$ à $C(T)$, resp. pour $n=2$ à $F(\mathfrak{X}, \mathfrak{y})$, d'où l'on conclut que η est un isomorphisme de $\mathbb{G}_m$ à $\hat{E}$.

(c) Montrons qu'un tel isomorphisme est toujours défini sur I. On a vu dans (a) que η est défini sur I^{nr}. On voit facilement, d'autre part, que le corps résiduel de I en une place quelconque est le composé de la $\mathbb{Z}_p$-extension de $\mathbb{F}_p$, et de l'unique extension de degré $f\times(p-1)/g_0$ (g_0 désignant le nombre de places de $F(E_{\mathfrak{P}^*})$ au-dessus d'une place v de F divisant $\mathfrak{P}$). Par conséquent, I est le sous-anneau de I^{nr} fixé par les automorphismes de I de la forme $\lambda=\varphi_0^{\nu}$ où $\nu\in\mathbb{Z}$ vérifie

$$\nu\equiv 0 \,\mathrm{mod}.\,(f\times(p-1)/g_0) \qquad \text{et} \qquad \nu_p=0,$$

en notant ν_p la projection $\hat{\mathbb{Z}}\to\mathbb{Z}_p$ de ν. Or, on sait que $\eta^{\varphi_0}([p]T)=[\Phi(\mathfrak{P})]\eta(T)$, donc en appliquant $\varphi_0(f-1)$-fois à cette égalité, et en notant $\varphi=\varphi_0^f$, le Frobenius relatif à F, on trouve : $\eta^{\varphi}([Nv](T))=[\pi]_{\hat{E}}\eta(T)$, et en posant $f_0=(p-1)/g_0$, on tire l'égalité :

$$\eta^{\varphi^{f_0}}([Nv^{f_0}]T)=[\pi^{f_0}]_{\hat{E}}\eta(T),$$

d'où l'on tire par une petite remarque :

$$\eta^{\varphi^{f_0}}([\bar{\pi}^{f_0}]T)=\eta(T).$$

La remarque s'énonce : si $f([\pi]T)=g([\pi]T)$, $f, g\in(I^{nr}[[T]])^{\times}$ alors $f=g$.

Mais on a vu que l'indice g_0 du groupe de décomposition de $F(E_{\mathfrak{P}^*})$ sur F en v est égal à l'indice du sous-groupe engendré par π mod $\mathfrak{P}^*$ dans $(\mathcal{O}/\mathfrak{P}^*)^{\times}$, ainsi $\bar{\pi}^{f_0}\equiv 1\,(\mathfrak{P})$.

Soit maintenant $\lambda = \varphi_0^{\nu}$, avec $\nu = f_0 f \nu'$, $\nu'_p = 0$; on a :

$$\eta^{\lambda}(T) = \eta^{(\varphi^{f_0})^{\nu'}}([\bar{\pi}^{f_0 \nu'}]T) \quad \text{car } \bar{\pi}^{f_0 \nu'} = \bar{\pi}^{f_0 \nu_p} = 1$$

donc $\eta^{\lambda}(T) = \eta(T)$.

Remarque. — Les points (*a*) et (*b*) peuvent aussi être obtenus à l'aide du théorème de TATE [25], en utilisant l'accouplement de WEIL (*voir* [29]).

2.7. SUITES COHÉRENTES DE FONCTIONS SUR LE GROUPE FORMEL

On fixe un idéal g de $\mathcal{O}$ multiple principal de f, premier à p. Soit $(\mathfrak{a}, \mathfrak{c})$ un couple d'ideaux de $\mathcal{O}$, premiers entre eux, $\mathfrak{a} = (\alpha)$ étant principal premier à $\mathfrak{g}p$, et $\mathfrak{c}$ étant premier à $\mathfrak{g}\mathfrak{P}^*$. Soit $\sigma = (\mathfrak{c}, F/K)$, on introduit la fonction rationnelle sur la courbe E^{σ} :

$$r = r_{(\mathfrak{a}, \mathfrak{c})} = \alpha^{12} \prod'_{P \in E^{\sigma}_{\mathfrak{a}}} (x_{\sigma} - x_{\sigma}(P))^6 / \Delta^{\sigma},$$

qui est définie sur F et ne dépend que de la classe d'isomorphisme de E^{σ}. Choisissons de plus une suite $\underline{Q} = (Q_m)(m = 0, 1, 2, \ldots)$ de points de $g\bar{\pi}^{m+1}$-torsion de E, tels que $\bar{\pi} Q_{m+1} = Q_m$ pour tout $m \geqslant 0$. On a noté, au paragraphe 4, $\mathcal{R}_m$ le corps des points de $g\bar{\pi}^{m+1}$-torsion, et soit $\mathcal{R}_{\infty} = \bigcup_{m \geqslant 0} \mathcal{R}_m$. Notons $\tau = (\mathfrak{c}, \mathcal{R}_{\infty}/K)$. On pose pour chaque entier $m \geqslant 0$

$$r_{(\mathfrak{a}, \mathfrak{c}, \underline{Q}, m)}(P) = \prod_{\delta \in G(\mathcal{R}_m/F_m)} r(P + Q_m^{\tau\delta}).$$

On voit facilement que cette fonction rationnelle sur E^{σ} est définie sur F_m. On rappelle que $t = t_1$ désigne le paramètre du groupe formel $\hat{E}$. On introduit les fonctions sur $\hat{E}$:

$$\theta_m(t) = \theta_{(\mathfrak{a}, \mathfrak{c}, \underline{Q}, m)}(t) = r_{(\mathfrak{a}, \mathfrak{c}, \underline{Q}, m)}(\Phi(\mathfrak{c})_E(P([\bar{\pi}^{-(m+1)}](t)))),$$

où le point $P([\bar{\pi}^{-(m+1)}]t)$ est l'unique point de E_1 dont le paramètre sur $\hat{E}$ vaut $[\bar{\pi}]^{-(m+1)}(t)$.

PROPOSITION 2.7.1. — *Pour tout* $m \geqslant 0$,

(i) $\theta_m(t)$ *est une unité de* $I_m[[t]]$;

(ii) $N_m \theta_{m+1}(t) = *.\theta_m(t)$ (*propriété de cohérence*);

(iii) *on a l'équation fonctionnelle au niveau* m :

$$\prod_{\omega \in \hat{E}_{\mathfrak{P}}} \theta_m(t[+]_{\hat{E}} \omega) = *.\theta_m^{(\mathfrak{P})}(t).$$

les étoiles dans (ii) *et* (iii) *désignent des constantes dans* $F^\times \cap J^\times$, *la norme de* (ii) *est la norme « semi-locale » de* I_{m+1} *à* I_m (*i.e.* $N_{F_{m+1}/F_m} \otimes \mathrm{Id}_{\mathcal{O}_\mathfrak{P}}$, *prolongé de* $I_{m+1}[[t]]$ *à* $I_m[[t]]$), *et dans* (iii), *on note* $\theta_m^{(\mathfrak{P})}$ *la fonction* $\theta_{(\alpha,\, c\mathfrak{P},\, \underline{Q},\, m)}$.

Preuve. — (i) Pour prouver que tous les coefficients de θ_m sont v-entiers, on est ramené à voir que pour tout $R \in E_\alpha^\sigma \setminus \{0\}$ et $\delta \in G(\mathcal{R}_m/F_m)$, l'expression $(x_\sigma(P_\sigma + Q_m^{\tau\delta}) - x_\sigma(R))^6/\Delta^\sigma$ devient après substitution de t_σ dans P_σ, une série de t_σ à coefficient dans $F(E_{g\,\alpha\bar{\pi}^{m+1}})$ tous v-entiers.

Or, par la formule d'addition, on a :

$$x_\sigma(P_\sigma + Q_m^{\tau\delta}) = \frac{1}{4}\left(\frac{y_\sigma(P_\sigma) - y_\sigma(Q_m^{\tau\delta})}{x_\sigma(P_\sigma) - x_\sigma(Q_m^{\tau\delta})}\right)^2 - x_\sigma(P_\sigma) - x_\sigma(Q_m^{\tau\delta})$$

et on sait que :

$$x_\sigma(P_\sigma) = \frac{1}{2} + \frac{g_2^\sigma}{4} t_\sigma^2 + \frac{g_3^\sigma}{4} t_\sigma^4 + \ldots,$$

$$y_\sigma(P_\sigma) = -\frac{2}{t_\sigma^3} + \frac{g_2^\sigma}{2} t_\sigma + \ldots,$$

tous les coefficients étant dans $F \cap J$.

Comme $\alpha g \bar{\pi}$ et $\mathfrak{P}$ sont étrangers, on voit que : $E_{\alpha g \bar{\pi}}^\sigma \cap E_1^\sigma(\bar{F}_v) = \{0\}$, donc les coordonnées de $Q_m^{\tau\delta}$ et R sont v-entières, et en développant $x_\sigma(P_\sigma + Q_m^{\tau\delta})$ on obtient l'intégralité.

Pour montrer que $\theta_m(0)$ est une v-unité on utilise un lemme.

LEMME 2.7.2. — *Soient* E *et* E' *deux courbes elliptiques définies sur le corps local* F_v, *et* $\alpha : E \to E'$ *une isogénie définie sur* F_v. *Soient* λ_v *et* λ_v' *les hauteurs locales de Néron respectives sur* E *et* E', *on a alors la formule : pour tout* $P \in E(\bar{F}_v)$ *tel que* $\alpha P \neq 0$:

$$\lambda_v'(\alpha P) = (d^0 \alpha)\lambda_v(P) + \frac{1}{12} v(r_\alpha(P)),$$

où

$$r_\alpha(P) = \mu(\alpha) \prod_{R \in E_\alpha}' (x(P) - x(R))^6/\Delta$$

et

$$\mu(\alpha) = \lim_{P \to 0}\left(\frac{x(P)}{x'(\alpha P)}\right)^6 \frac{\Delta'}{\Delta}.$$

COMMENTAIRE. — Ce lemme est dû à J. Tate (lettre à J.-P. Serre) et est prouvé dans [1].

On l'applique à E^σ et à l'endomorphisme de cette courbe défini par $\alpha \in \mathcal{O}$. On voit alors que $\mu(\alpha) = \alpha^{12}$ et $r_\alpha(P) = r_{(a,\ c)}(P)$. On prend successivement les points $Q_m^{\tau\delta}$, δ parcourant $G(\mathscr{R}_m/F_m)$, et on obtient que $v(r_{(a,\ c,\ \underline{Q},\ m)}) = 0$.

Pour prouver (ii) et (iii), on a besoin du lemme :

LEMME 2.7.3. — *Soit* b *un idéal de* $\mathcal{O}$ *premier à* αf, *alors on a l'égalité :*

$$\prod_{\sigma,\ R \in E_b^{\sigma_c}} r(P+R) = c_{b,\ c} \cdot r^{(b)}(\Phi(b)_{E^{\sigma_c}}^{\sigma_c}(P)),$$

où $r^{(b)} = r_{(a,\ cb)}$, *et* $c_{b,\ c}$ *est un élément de* $F^\times$ *indépendant de* P.

Preuve. — Il suffit de comparer les diviseurs des deux membres. On trouve que le membre de gauche présente un zéro d'ordre 12 en chaque point $R+S$ ou $R \in E_b^{\sigma_c}$ et $S \in E_\alpha^{\sigma_c} \setminus \{0\}$, et un pôle d'ordre $12(N\alpha - 1)$ en chaque point R de $E_b^{\sigma_c}$. De même le membre de droite présente un zéro d'ordre 12 en chaque point de $\Phi(b)_E^{-1}(E_\alpha^{\sigma_c \sigma_b} \setminus \{0\})$ puisque $\Phi(b)_E^{\sigma_c}$ est étale sur E^{σ_c}, et comme b et α sont étrangers, on voit que l'ensemble des zéros du membre de droite est l'ensemble des $R+S$, $R \in E_b^{\sigma_c}$, $S \in E_\alpha^{\sigma_c} \setminus \{0\}$, idem pour les pôles, donc ces deux fonctions rationnelles sur E^{σ_c} et définies sur F, diffèrent par une constante $c_{b,\ c} \in F^+$.

On pouve alors (ii) en exprimant $N_m \theta_{m+1}(t_\sigma)$ comme un double produit sur

$$G(F_{m+1}/F_m) \qquad \text{et} \qquad G(\mathscr{R}_{m+1}/F_{m+1})$$

qu'on transforme en produit sur

$$G(\mathscr{R}_{m+1}/\mathscr{R}_m) \qquad \text{et} \qquad G(\mathscr{R}_{m+1}/F_{m+1})$$

ce qui est loisible puisque $\mathscr{R}_m$ et F_{m+1} sont disjoints sur F_m et de composé $\mathscr{R}_{m+1}$, on applique $\mathscr{R}_m$ et F_{m+1} sont disjoints sur F_m et de composé $\mathscr{R}_{m+1}$, on applique alors une version faible du lemme ci-dessus à $\Phi(b)_E = \bar{\pi}$ pour obtenir (ii).

Le point (iii) résulte immédiatement du lemme.

2.8. — LES DÉRIVÉES LOGARITHMIQUES

On introduit comme dans [29] les dérivées logarithmiques qui interviennent dans la construction qu'on a en vue. Notons d'abord

$D_{\hat{E}}=(1/\log'_{\hat{E}}(t))(d/dt)$ l'unique dérivation invariante par translation sur $\hat{E}$, est normalisée par $D_{\hat{E}}t=1$. Remarquons que $\log'_{\hat{E}}(t)\in 1+tJ[[t]]$ parce qu'on a choisi un modèle sur E minimal au-dessus de $\mathfrak{P}$.

NOTATION 2.8.1. — Pour tout $m\geqslant 0$, on note.

(i) Tr_m la trace (semi-locale) de $I_{m+1}[[t]]$ à $I_m[[t]]$ déduite de $Tr_{F_{m+1}/F_m}\otimes \mathrm{Id}_{\mathcal{O}_{\mathfrak{P}}}$ de I_{m+1} à I_m.

(ii) $j_m(t)=D_{\hat{E}}\log\theta_m(t)=(d/dz)\log(\theta_m\circ e_{\hat{E}}(z))\big|_{z=\log_{\hat{E}}(t)}$ (resp. $j_m^{(\mathfrak{P})}(t)$ désigne l'analogue de $j_m(t)$, où l'on a remplacé θ_m par $\theta_m^{(\mathfrak{P})}=\theta_{(a,\,c\,\mathfrak{P},\,\underline{Q},\,m)}$).

PROPOSITION 2.8.2. — *Pour tout $m\geqslant 0$, on a :*

(i) $j_m(t)\in I_m[[t]]$, *et* $\mathrm{Tr}_m(j_{m+1}(t))=j_m(t)$.

(ii) $\sum_{\omega\in\hat{E}_{\mathfrak{P}}} j_m(t[+]\omega)=\Lambda(\mathfrak{P})^{\sigma_c}\times j_m^{(\mathfrak{P})}(t)$.

Preuve. — (i) résulte immédiatement de la proposition 2.7.1; (i) et (ii), en appliquant le logarithme des séries formelles aux deux membres de l'égalité (ii), et en remarquant que $\log\circ N_m=\mathrm{Tr}_m\circ\log$;

(ii) résulte de la congruence $[\Phi(\mathfrak{P})]^{\sigma}(t_\sigma)\equiv\Lambda(\mathfrak{P})^{\sigma}.t_\sigma$ modulo t_σ^2, prouvée au lemme 2.5.1, et la proposition 2.7.1, (iii).

On peut alors définir, en passant à la limite sur m une série à deux variables analogue à celle du théorème 5 de [29] :

PROPOSITION 2.8.3. — (i) *Soit* (a, c) *fixé comme au paragraphe* 7, *il existe une unique série* $j(t, w_2)=j_{(a,\,c)}(t, w_2)\in I[[t, w_2]]$, *telle que, pour tout* $m\geqslant 0$, *on ait :*

$$j(t, w_2)\equiv\sum_{\tau\in G(F_m/F)} j_m^{\tau}(t)\times(1+w_2)^{\bar{\psi}_{\mathfrak{P}}(\tilde{\tau})}\qquad (\mathrm{mod.}\,(1+w)^{q^{m+1}}-1),$$

où $\tilde{\tau}$ *désigne un prolongement arbitraire à* F_∞ *de l'automorphisme* τ *de* F_m/F.

(ii) *De plus, cette série vérifie l'équation fonctionnelle :*

$$\sum_{\omega\in\hat{E}_{\mathfrak{P}}} j(t[+]\omega, w_2)=\Lambda(\mathfrak{P})^{\sigma_c}\times j^{(\mathfrak{P})}(t, w_2),$$

où

$$j^{(\mathfrak{P})}=j_{(a,\,c\,\mathfrak{P})}.$$

On rappelle que $q=Nv$.

Preuve. — Comme l'anneau $I[[t, w_2]]$ est complet pour la topologie (p, t, w_2)-adique, il suffit de voir que la suite (u_m) des membres de droite

de la congruence est de Cauchy. Remarquons d'abord que si on compose $\tilde{\tau}$ avec un automorphisme τ' qui fixe F_m, on a la congruence :

$$(1+w_2)^{\bar{\Psi}_{\mathfrak{P}}(\tilde{\tau}\tau')} \equiv (1+w_2)^{\bar{\Psi}_{\mathfrak{P}}(\tilde{\tau})} \bmod .\ ((1+w_2)^{q^{m+1}}-1)$$

ecar

$$\bar{\Psi}_{\mathfrak{P}}(\tau') \equiv 1 \,(\text{mod. } q^{m+1}),$$

ce qui prouve que les termes de la suite sont bien définis pour le modulo considéré. Et en utilisant la formule $\mathrm{tr}_m j_{m+1} = j_m$, on prouve comme dans le théorème 5 de [29] la congruence $u_{m+1} \equiv u_m (\mathrm{mod}\,(1+w_2)^{q^{m+1}}-1)$ d'où le résultat. Quant à (ii), il résulte immédiatement de l'équation fonctionnelle pour les $g_m(t_\sigma)$.

On a noté (t, w_2) les deux variables car la première est le paramètre de $\hat{E}$ tandis que la seconde est essentiellement de nature multiplicative. On aura à remplacer t par la variable w_1 de $\mathbb{G}_m$, parce que la théorie de la mesure sur $\mathbb{Z}_p^2$ donne lieu à des formules qui s'écrivent agréablement sur le groupe multiplicatif.

2.9. Le formalisme de l'intégration p-adique a deux variables

On note $C(\mathbb{Z}_p^2, I)$ l'espace des fonctions continues de $\mathbb{Z}_p^2$ dans I, muni de la norme de convergence uniforme sur $\mathbb{Z}_p^2$, et on pose la :

Définition 2.9.1. — On appelle mesure sur $\mathbb{Z}_p^2$ à valeurs dans I toute forme I-linéaire de $C(\mathbb{Z}_p^2, I)$ dans I, on note M leur ensemble. On note $\int_{\mathbb{Z}_p^2} f.d\mu$ au lieu de $\mu(f)$.

On rappelle le théorème de Mahler :

Théorème 2.9.2. — *Pour toute fonction f continue sur $\mathbb{Z}_p^2$, à valeurs dans I, il existe une unique suite $(a_{n_1 n_2})$ d'éléments de I, tendant vers zéro quand $(n_1, n_2) \to \infty$, telle que :*

$$f(x_1, x_2) = \sum_{n_1,\, n_2 \geq 0} a_{n_1 n_2} \binom{x_1}{n_1} . \binom{x_2}{n_2}.$$

et

$$\| f \| = \mathrm{Max}_{n_1,\, n_2 \geq 0} |a_{n_1,\, n_2}|_I.$$

On note pour $x \in I$, $x = (x_w)_w$, w parcourant l'ensemble des places de $F(E_{p^\infty})$ au-dessus de $\mathfrak{P}$, $|x|_I = \mathrm{Max}_w |x_w|_p$.

On en tire aisément la proposition :

PROPOSITION 2.9.3. — *L'application* $I[[w_1\, w_2]] \to M$ *qui a la série*

$$S = \sum_{n_1,\, n_2 \geq 0} c_{n_1 n_2} w_1^{n_1} w_2^{n_2}$$

associe la forme linéaire μ_S *définie par*

$$\mu_S\left(\binom{x_1}{n_1}\binom{x_2}{n_2}\right) = c_{n_1 n_2}$$

pour tout couple $(n_1\, n_2)$ *d'entiers* ≥ 0, *est un isomorphisme isométrique, la norme sur* $I[[w_1, w_2]]$ *étant définie par*

$$\|S\| = \mathrm{Sup}_{n_1,\, n_2 \geq 0} |c_{n_1,\, n_2}|_I.$$

On donne alors un formulaire précisant la correspondance $S \mapsto \mu_S$. On notera $w_1 [+]_{G_m} w_2 = w_1 + w_2 + w_1 w_2$ la loi du groupe formel multiplicatif.

PROPOSITION 2.9.4. — (i) *Pour tout* $S \in I[[w_1, w_2]]$, *on a :*

$$\int_{\mathbb{Z}_p^2} (1+w_1)^{x_1} (1+w_2)^{x_2}\, d\mu_S(x_1, x_2) = S(w_1, w_2).$$

(ii) *Si la série S satisfait la congruence*

$$S(w_1, w_2) \equiv \sum_{0 \leq k \leq p^N - 1,\ 0 \leq j \leq p^M - 1} b_{k,\, j} (1+w_1)^k (1+w_2)^j$$
$$\text{modulo}\,((1+w_1)^{p^N} - 1,\ (1+w_2)^{p^M} - 1),$$

alors

$$\int_{(k + p^N \mathbb{Z}_p) \times (j + p^M \mathbb{Z}_p)} d\mu_S = b_{k,\, j}.$$

(iii) *Si* φ *est localement constante sur* $\mathbb{Z}_p^2$, *c'est-à-dire provient d'une fonction sur* $\mathbb{Z}/_{p^N\mathbb{Z}} \times \mathbb{Z}/_{p^M\mathbb{Z}}$, *notons* $\hat{\varphi}$ *sa transformée de Fourier définie par :*

$$\hat{\varphi}(\zeta_1, \zeta_2) = \frac{1}{p^{N+M}} \times \sum_{0 \leq x_1 \leq p^N,\ 0 \leq x_2 \leq p^M} \varphi(x_1, x_2)\, \zeta_1^{x_1} \zeta_2^{x_2}$$

pour $(\zeta_1, \zeta_2) \in \mu_{pN} \times \mu_{pM}$.

Alors, on a la formule : $\varphi \times d\mu_S = d\mu_T$, *où*

$$T(w_1, w_2) = \sum_{(\zeta_1, \zeta_2)} \hat{\varphi}(\zeta_1, \zeta_2) S(w_1 [+]_{G_m} (\zeta_1 - 1), w_2 [+]_{G_m} (\zeta_2 - 1)),$$

la somme étant étendue aux couples (ζ_1, ζ_2) *de* $\mu_{p^N} \times \mu_{p^M}$.

(iv) *En posant*

$$D_i = (1 + w_i) \frac{d}{dw_i} \qquad (i = 1, 2),$$

on a :

$$x_1^{n_1} x_2^{n_2} d\mu_S = d\mu_{D_1^{n_1} D_2^{n_2} S}.$$

(v) *Pour tout* $S \in I[[w_1, w_2]]$, *notons* $\tilde{S}(w_1, w_2)$ *la série à coefficients dans* I *:*

$$S(w_1, w_2) - \frac{1}{p} \sum_{\zeta_1 \in \mu_p} S(w_1 [+]_{G_m} (\zeta_1 - 1), w_2)$$

et soit $1_{\mathbb{Z}_p^\times \times \mathbb{Z}_p}$ *la fonction caractéristique de* $\mathbb{Z}_p^\times \times \mathbb{Z}_p$, *on a :* $1_{\mathbb{Z}_p^\times \times \mathbb{Z}_p} \times d\mu_S = d\mu_{\tilde{S}}$.

Preuve. — Ce formulaire est strictement analogue au cas d'une variable, traité par KATZ dans [13].

Une opération importante de l'intégration p-adique, dont nous aurons usage est la transformation de Leopoldt, que nous rappelons brièvement. Soit (i_1, i_2) un couple d'entiers modulo $p-1$, on définit la branche de la transformation de Leopoldt associée à ce couple comme suit. Pour $x \in \mathbb{Z}_p^\times$, on note $x = \omega(x) \langle x \rangle$, où $\omega(x)$ est l'unique racine $(p-1)$-ième de l'unité telle que $x \equiv \omega(x)$ (mod. p), et $\langle x \rangle \in 1 + p\mathbb{Z}_p$. Pour chaque mesure $\mu \in M$, on pose :

$$\Gamma^{(i_1, i_2)} \mu(s_1, s_2) = \int_{(\mathbb{Z}_p^\times)^2} \langle x_1 \rangle^{s_1} \langle x_2 \rangle^{s_2} \omega^{i_1}(x_1) \omega^{i_2}(x_2) d\mu$$

et on vérifie aisément qu'on a ainsi défini une application continue de $\mathbb{Z}_p^2$ dans I. On sait en fait que les fonctions de $\Gamma^{(i_1, i_2)}(M)$ sont plus que

continues : elles sont analytiques au sens suivant. Fixons désormais deux générateurs topologiques u_1 et u_2 de $1+p\mathbb{Z}_p$, alors :

PROPOSITION 2.9.5. — *Soit* $\mu \in M$ *et* $(i_1, i_2) \in (\mathbb{Z}/(p-1)\mathbb{Z})^2$, *il existe une unique série* $A_\mu^{(i_1, i_2)} \in I[[w_1, w_2]]$ *telle que pour tout* $(s_1, s_2) \in \mathbb{Z}_p^2$, *on ait :*

$$(\Gamma^{(i_1, i_2)}\mu)(s_1, s_2) = A_\mu^{(i_1, i_2)}(\mu_1^{s_1} - 1, u_2^{s_2} - 1).$$

Preuve. — On peut écrire $\langle x \rangle = u_i^{l_i(x)} (i = 1, 2)$ pour $x \in \mathbb{Z}_p^\times$, où $l_i : \mathbb{Z}_p^\times \to \mathbb{Z}$ est le logarithme de base u_i; on obtient donc le développement :

$$\langle x \rangle^s = \sum_{n \geq 0} \binom{l_i(x)}{n} (u_i^s - 1)^n \qquad \text{pour} \quad i = 1, 2,$$

la convergence de la série étant uniforme en s, ce qui permet en revenant à la définition de $\Gamma^{(i_1, i_2)}\mu$ de permuter intégrale et somme, ce qui donne le résultat.

Fixons un isomorphisme $\eta : \mathbb{G}_m \xrightarrow{\sim} \hat{E}$, qu'on précisera plus loin.

Posons $h(w_1, w_2) = \eta'(0) \times j(\eta(w_1), w_2)$. On applique à h l'opération (v) de la proposition 2.9.4, et soit $\mu = \mu_{(a, c)}$ la mesure associée à $\tilde{h}$.

LEMME 2.9.6. — *La mesure* μ *est concentrée sur* $\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$.

Preuve. — Il suffit de prouver que μ_h est concentrée sur $\mathbb{Z}_p \times \mathbb{Z}_p^\times$ et d'appliquer le (v) de la proposition.

Or, soit N un entier ≥ 1, a et b deux entiers compris entre 0 et $p^N - 1$. Soit $\mathbf{1}$ la fonction caractéristique de $(a, pb) + p^N\mathbb{Z}_p^2$, on veut prouver que $\mu_h(\mathbf{1}) = 0$. Or par la proposition 2.9.4 (iv), il suffit de voir que les $b_{k, j}$ définis par :

$$h(w_1, w_2) \equiv \sum_{0 \leq k, j < p^N} b_{k, j}(1 + w_1)^k (1 + w_2)^j$$

modulo $((1 + w_1)^{p^N} - 1, (1 + w_2)^{p^N} - 1)$, sont nuls pour $j \equiv 0 (p)$.

Mais les seuls exposants de $(1 + w_2)$ qui interviennent dans cette congruence sont les unités p-adiques $\bar{\psi}_{\mathfrak{P}}(\bar{\tau})$ donc on a bien $b_{k, j} = 0$ pour $j \equiv 0 (p)$.

On transporte alors cette mesure sur G à l'aide de l'isomorphisme $\psi_{\mathfrak{P}} \times \bar{\psi}_{\mathfrak{P}}^{-1} : G \xrightarrow{\sim} \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$, on obtient une mesure encore notée $\mu = \mu_{(a, c)}$. On définit des séries $\mathscr{G}^{(i_1, i_2)}$, par :

$$\mathscr{G}^{(i_1, i_2)}(u_1^{s_1} - 1, u_2^{s_2} - 1) = \Gamma^{(i_1 - 1, -i_2)}\mu(s_1 - 1, -s_2)$$

pour s_1 et $s_2 \in \mathbf{Z}_p$. C'est-à-dire que pour tout couple (a, b) d'entiers congru à (i_1, i_2) modulo $(p-1)$, on a :

$$\mathscr{G}^{(i_1, i_2)}(u_1^a - 1, u_2^b - 1) = \int_G \psi_{\mathfrak{P}}^a \bar{\psi}_{\mathfrak{P}}^b(\sigma) \frac{d\mu(\sigma)}{\psi_{\mathfrak{P}}(\sigma)}.$$

On se propose de calculer explicitement cette intégrale pour certains couples (a, b). Pour cela, on rappelle quelques propriétés des séries d'Eisenstein et leur lien avec les valeurs spéciales de fonctions L.

2.10. Nombres d'Eisenstein

Posons tout entier $k \geqslant 1$, $z \in \mathbf{C}$ et s dans $\mathbf{C}$ de partie réelle plus grande que $(k/2)+1$, on note :

$$H_k(s, z, \mathscr{L}) = \sum'_{\omega \in \mathscr{L}} \frac{\overline{(z+\omega)}^k}{|z+\omega|^{2s}}$$

le prime qui affecte de signe de somme signifie qu'on omet $\omega = -z$ si $z \in \mathscr{L}$. Il est bien connu que cette fonction de s *a un prolongement méromorphe à* $\mathbf{C}$, avec au plus un pôle simple en $s=1$, qui n'apparaît que si $z \in \mathscr{L}$ et $k=1$. On note $\mathscr{L}_\sigma$ le réseau associé à $(E^\sigma, \omega^\sigma)$ et on rappelle qu'on a calculé le facteur local en la place archimédienne associée à σ :

$$m_\sigma = |\Lambda(\mathfrak{a})\Omega|^2 \times N\mathfrak{a}^{-1} \times (|D_K|^{1/2}/2) \qquad \text{où} \quad (\mathfrak{a}, F/K) = \sigma.$$

On définit alors les séries d'Eisenstein dont on aura usage :

Définition 2.10.1. — On dit qu'un couple (a, b) d'entiers est admissible si $a > -b \geqslant 0$.

Définition 2.10.2. — Soit (a, b) un couple admissible, on définit la série d'Eisenstein normalisée de poids (a, b) par la formule :

$$E_{a,b} = (a-1)! \left(\frac{\pi}{m_\sigma}\right)^{-b} H_{a-b}(z, a, \mathscr{L}_\sigma).$$

(On rappelle qu'une fonction $F(z, \omega_1, \omega_2)$ est dite de poids (a, b) si pour tout $\lambda \in \mathbf{C}$, on a : $F(\lambda z, \lambda\omega_1, \lambda\omega_2) = \lambda^{-a}\bar{\lambda}^{-b}F(z, \omega_1, \omega_2)$. Pour $b=0$, on abrège $E_{(a,b)} = E_a$.

LEMME 2.10.3. — *Pour tout couple admissible* (a, b), *il existe un polynôme* $P_{a,b} \in \mathbb{Z}[\mathfrak{X}_1, \ldots, \mathfrak{X}_{a-b}]$ *de degré* $1-b$ *et de poids* $a-b$ *tel que :*

$$2^{-b} E_{a,b} = P_{a,b}(E_1, \ldots, E_{a-b}),$$

de plus

$$P_{a,b}(\mathfrak{X}_1 \ldots \mathfrak{X}_{a-b}) = (-2)^{-b} \mathfrak{X}_a + Q_{a,b}(\mathfrak{X}_1 \ldots \mathfrak{X}_{a-b}),$$

avec

$$d^0_{\mathfrak{X}_1} Q_{a,b} < -b.$$

Preuve. — Notons $E_{a,b}(z, \mathscr{L}) = E_{a,b}(z, \omega_1, \omega_2)$ et $m_1 = m(\omega_1, \omega_2)$. On introduit les opérateurs différentiels

$$\partial = -\frac{\partial}{\partial z} \quad \text{et} \quad D = \frac{-m(\omega_1, \omega_2)}{\pi} \left(\bar{\omega}_1 \frac{\partial}{\partial \omega_1} + \bar{\omega}_2 \frac{\partial}{\partial \omega_2} + \bar{z} \frac{\partial}{\partial z} \right).$$

On vérifie facilement les formules :

$$Dm(\omega_1, \omega_2) = 0, \qquad \partial D = D\partial, \qquad \partial H_k(z, s, \mathscr{L}) = s H_{k+1}(z, s+1, \mathscr{L})$$

et :

$$DH_k(z, s, \omega_1, \omega_2) = s H_{k+2}(z, s+1, \omega_1, \omega_2),$$

donc

$$\partial E_{(a,b)} = E_{(a+1,b)},$$
$$D E_{(a,b)} = E_{(a+1,b-1)}.$$

On en déduit par récurrence l'égalité :

$$E_{(a,b)} = \partial^{a+b-1} \circ D^{-b} E_1.$$

Or on prouve dans la théorie des séries d'Eisenstein (*cf.* [27], chapitre VI, § 6, formule 9) l'égalité :

$$DE_1 = E_{(2,-1)} = -E_1 E_2 + \frac{1}{2} E_3.$$

En appliquant alors ∂^{n-1} à cette égalité et en développant par la formule de Leibniz, on obtient :

$$E_{(n+1,-1)} = -E_1 E_{n+1} + \frac{1}{2} \left(E_{n+2} - \sum_{h-1}^{n-1} \binom{n}{h} E_{h+1} E_{n-h+1} \right).$$

On tient déjà le polynôme $P_{n+1,\,-1}$ qui est de la forme souhaitée. Pour obtenir $P_{a,\,b}$ on applique à l'égalité ci-dessus l'opérateur D^m en remplaçant DE_1 par $-E_1E_2+(1/2)E_3$ à chacun de ses occurences. Par récurrence sur m, il est clair que $P_{a,\,b}$ satisfait les propriétés requises.

Remarque. — L'admissibilité du couple (a, b) est apparue essentielle pour cette construction de $P_{a,\,b}$, qui à son tour se révèlera l'outil crucial pour les calculs du paragraphe suivant. C'est pourquoi, malgré que pour tout couple (a, b) tel que $a\geqslant 1$, $b\leqslant 0$, on ait un résultat d'algébricité de $L(\psi^a\bar{\psi}^b, 1)$ on ne peut pas par notre méthode interpoler directement ces nombres.

On rassemble maintenant les propriétés de rationalité et d'intégralité des valeurs particulières des séries d'Eisenstein, qui nous seront utiles.

NOTATIONS 2.10.4. — Pour tout $m\geqslant 0$, on pose

$$g_m=g\,\bar{\pi}^{m+1} \qquad \text{et} \qquad \rho_m=\frac{\Omega}{g_m}.$$

Si de plus (a, b) est un couple admissible, on appelle $E_{a,\,b}(\rho_m, \mathscr{L})$ un nombre d'Eisenstein. On le note $E_{a,\,b}(\rho_m)$ quand il n'y a pas d'ambiguïté sur le réseau $\mathscr{L}$. On suppose désormais que les points $Q_m(m=0, 1, 2.:.)$ qui ont permis de définir les fonctions θ_m sont donnés par :

$$Q_m=W(\rho_m, \mathscr{L}).$$

On rappelle alors le lemme qui établit le lien entre les fonctions θ_m et les nombres d'Eisenstein (*voir* corollaire 1.7 de [9]).

LEMME 2.10.5. — *Pour tout entier $k\geqslant 1$ on a :*

$$\frac{d^k}{dz^k}\log\theta_m\circ e_{\tilde{E}^\sigma}(z)\big|_{z=0}=12(-1)^k\times\bar{\pi}^{-(m+1)k}$$
$$\times\Lambda(c)^k\times\sum_B\{N\mathfrak{a}\times E_k(\Lambda(c)\psi(B)\rho_m, \mathscr{L}_\sigma)$$
$$-(\Lambda(\mathfrak{a})^\sigma)^k E_k(\Lambda(\mathfrak{a}c)\psi(B)\rho_m, \mathscr{L}_{\sigma\sigma_\mathfrak{a}})\}.$$

où $\theta_m=\theta_{(a,\,c,\,\underline{Q},\,m)}$, $\sigma=(c, F/K)$ et où B parcourt un système quelconque d'idéaux de $\mathcal{O}_F$ premiers à $\mathfrak{g}\mathfrak{P}^*$ dont les symboles d'Artin $(B, \mathscr{R}_m/F)$ décrivent exactement le groupe $G(\mathscr{R}_m/F_m)$.

Remarque. — Comme $\theta_m \circ e_{\hat{E}}$ est une série de z à coefficients dans F_m, on voit que le second membre est dans F_m, et plus précisément, on a la :

PROPOSITION 2.10.6. — *Pour tout couple admissible (a, b) et pour tout entier $m \geqslant 0$:*

(1) $E_{a,b}(\rho_m) \in \mathscr{R}_m$ *et pour tout idéal* $\mathfrak{c}$ *de* $\mathcal{O}$ *premier à* $\mathfrak{g}\mathfrak{P}^*$ *et* B *de* $\mathcal{O}_F$ *premier à* $\mathfrak{g}\mathfrak{P}^*$, *on a :*

$$E_{a,b}(\rho_m, \mathscr{L})^{(\mathfrak{c}, \mathscr{R}_m/K)} = E_{a,b}(\Lambda(\mathfrak{c})\rho_m, \mathscr{L}_\sigma) \qquad \text{où} \quad \sigma = (\mathfrak{c}, F/K),$$

et

$$E_{a,b}(\rho_m)^{(B, \mathscr{R}_m/F)} = E_{a,b}(\psi(B)\rho_m);$$

(2) (α) $\bar{g}_m \times E_1(\rho_m) \in I'_m$,

(β) *Si* $a > 1$, *soit* s *le plus petit entier* > 0 *tel que* a *ne soit congru ni à* 0 *ni à* 1 modulo $(p-1)q^s$, *alors, pour tout* $m \geqslant s$, *on a* $q^s \times (\bar{g}_m)^{-b} E_{a,b}(\rho_m) \in I'_m$,

(γ) *Si* $a > 1$, *il existe un entier* $m_{a,b} \geqslant 0$ *tel que pour* $m \geqslant m_{a,b}$ *on ait :*

$$(\bar{g}_m)^{-b} E_{a,b}(\rho_m) \equiv (-\bar{g}_m E_1(\rho_m))^{-b} \times E_a(\rho_m) \text{ modulo } \pi^{m - m_{a,b}}.$$

Preuve. — L'énoncé (1), précisant la rationalité des nombres d'Eisenstein résulte du lemme précédent et du lemme 2.10.3, qui exprime $E_{a,b}(\rho_m)$ rationnellement à l'aide des $E_k(\rho_m)$ $(1 \leqslant k \leqslant a-b)$. Les détails sont donnés au théorème (6.2) de [9].

Le résultat de (2) est dû à YAGER [30] dont nous reprenons la démonstration s'appuyant sur une variante du lemme 2.10.5. Soit $\mathscr{P}_m$ l'ensemble des idéaux principaux $\mathfrak{a} = (\alpha)$ de $\mathcal{O}$, avec $\alpha \equiv 1$ $(\mathfrak{g}\bar{\pi}^{m+1})$, et $\mathscr{F}_m$ l'ensemble des familles $(n_\mathfrak{a})_{\mathfrak{a} \in \mathscr{P}_m}$ indexées par $\mathscr{P}_m$ d'entiers relatifs presque tous nuls, tels que $\sum_{\mathfrak{a} \in \mathscr{P}_m} n_\mathfrak{a}(N\mathfrak{a} - 1) = 0$. Soit $\underline{n} = (n_\mathfrak{a})_{\mathfrak{a} \in \mathscr{P}_m}$ une famille de $\mathscr{F}_m$, notons $R_m = R_{(\underline{n}, \mathcal{O}, \underline{Q}, m)}$ la fonction rationnelle sur E : $R_m(P) = r(P + Q_m)$. On a alors l'égalité, pour tout $k \geqslant 1$:

$$\frac{d^k}{dz^k} \log R_m \circ W(z, \mathscr{L})\big|_{z=0} = 12(-1)^k (k-1)! \sum_{\mathfrak{a} \in \mathscr{P}_m} n_\mathfrak{a}(N\mathfrak{a} - \alpha^k) \times E_k(\rho_m).$$

D'autre part, le membre de gauche de cette égalité est dans I'_m car $R_m \circ W(z, \mathscr{L})$, vue comme série de t, a ses coefficients dans I'_m, et vaut une unité de I'_m en $z = 0$. On est alors ramené à voir que la valuation π-adique de l'élément de $\mathcal{O}$: $S_n = \sum_{\mathfrak{a} \in \mathscr{P}_m} n_\mathfrak{a}(N\mathfrak{a} - \alpha^k)$ est égale à s, pour un choix convenable de $\underline{n}$.

Choisissons pour cela une racine $(p-1)$-ième non triviale de 1 dans $\mathcal{O}_{\mathfrak{P}}$, notée ζ_1. Si $k \equiv 0$ ou 1 modulo $p-1$, choisissons arbitrairement une autre racine $(p-1)$-ième de 1, non triviale ζ_2. Si $k \not\equiv 0$ ou 1 mod $p-1$, soit l le représentant de k compris entre 2 et $p-2$. L'équation dans

$$\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} = \mathbb{F}_p : \quad \sum_{j=1}^{k-1} \mathfrak{X}^j = \sum_{j=1}^{l-1} \zeta_1^j$$

a au plus $p-3$ solutions dans $\mathbb{F}_p$, donc il existe une racine $(p-1)$-ième de 1, ζ_2 non triviale telle que

$$\sum_{j=1}^{l-1} \zeta_2^j \not\equiv \sum_{j=1}^{l-1} \zeta_1^j \text{ mod. } \mathfrak{P}.$$

Choisissons α_1 et α_2 satisfaisant les congruences :

$$\alpha_1 \equiv \alpha_2 \equiv 1 \text{ mod. } \mathfrak{g}, \qquad \alpha_1 \equiv 1 + \bar{\pi}^{m+1} \text{ mod. } \bar{\pi}^{m+2}$$

et

$$\alpha_2 \equiv 1 \text{ mod } \bar{\pi}^{m+2}, \qquad \alpha_1 \equiv \zeta_1 \text{ mod } \pi^{m+1}$$

et

$$\alpha_2 \equiv \zeta_2 (1+q) \text{ mod } \pi^{m+1}.$$

Choisissons enfin une famille $\underline{n}$ telle que $n_a = 0$ si $a \neq (\alpha_1)$ et (α_2), et telle que

$$n_{(\alpha_1)} = \alpha_2 \bar{\alpha}_2 - 1 \qquad \text{et} \qquad n_{(\alpha_2)} = -(\alpha_1 \bar{\alpha}_1 - 1).$$

Si $k \not\equiv 0,\ 1 \text{ mod } p-1$, on trouve

$$S_{\underline{n}} \equiv -(\zeta_1 - 1)(\zeta_2 - 1)\left(\sum_{j=1}^{l-1} \zeta_2^j - \sum_{j=1}^{l-1} \zeta_1^j\right) \not\equiv 0 \text{ mod. } \mathfrak{P},$$

et $s = 0$ convient.

Si $k \equiv 0$ (mod. $p-1$) et $k \not\equiv 0 \text{ mod } (p-1)q^s$, on trouve

$$S_{\underline{n}} \equiv (\zeta_1 - 1)((1+q)^k - 1) \not\equiv 0 \quad (\text{mod. } \pi^{s+1}),$$

si $k \equiv 1$ (mod $p-1$) et $k \not\equiv 1 \text{ mod } (p-1)q^s$, on obtient :

$$S_{\underline{n}} \equiv \zeta_2 (1+q)((1+q)^{k-1} - 1) \not\equiv 0 \quad (\text{mod. } \pi^{s+1}),$$

enfin pour $k = 1$, toujours avec le même $\underline{n}$, on obtient $S_{\underline{n}} \sim \pi^{m+1}$, ce qui achève de prouver les points α et β.

En outre, on a l'égalité (où $d^0_{E_1} Q_{a,\,b} < -b$) :

$$(\bar{g}_m)^{-b} E_{a,\,b}(\rho_m) = (-\bar{g}_m E_1(\rho_m))^{-b} E_a(\rho_m) + (\bar{g}_m/2)^{-b} Q_{a,\,b}(E_k(\rho_m)).$$

Donc si $a > 1$ et s est tel que $a \not\equiv 0,1 \mod (p-1)q^s$, posons $m_{a,\,b} = s(a-b)+b$, on voit que pour $m \geqslant m_{a,\,b}$,

$$q^{-b(m+1)-(m-m_{a,\,b})} \times Q_{a,\,b}(E_1(\rho_m), \ldots, E_{a-b}(\rho_m)) \in I'_m,$$

donc, que la congruence voulue a bien lieu.

On peut maintenant préciser le choix de la période $\mathfrak{P}$-adique adaptée à nos calculs.

PROPOSITION 2.10.7. — *La suite des nombres $\gamma_{\mathfrak{P},\,\mathfrak{g},\,m} \in I'_m$ définis par*

$$\gamma_{\mathfrak{P},\,\mathfrak{g},\,m} = -\bar{g}_m \cdot E_1(\rho_m) \qquad (m = 0, 1, 2, \ldots)$$

est de Cauchy et converge vers un élément de I noté $\gamma_{\mathfrak{P},\,\mathfrak{g}} = \gamma_{\mathfrak{P}}$ indépendant du choix d'un idéal $\mathfrak{g}$, multiple principal de f et premier à p. On a de plus pour

$$\tau = (\mathfrak{c},\, F(E_{\mathfrak{g}\mathfrak{P}^\infty})/K) : \quad \gamma^{\tau}_{\mathfrak{P}} = \frac{N\mathfrak{c}}{\Lambda(\mathfrak{c})} \times \gamma_{\mathfrak{P}}.$$

Enfin, pour presque tout p ordinaire, $\Omega_{\mathfrak{P}} = \gamma_{\mathfrak{P}}^{-1}$ est une unité de I qui est la dérivée à l'origine d'un isomorphisme de groupes formels de $\mathbb{G}_m$ à $\hat{E}$.

Preuve. — Pour montrer que $\{ \gamma_{\mathfrak{P},\,\mathfrak{g},\,m} \}_{m \geqslant 0}$ est de Cauchy, on utilise la propriété de distribution des nombres d'Eisenstein

$$\bar{\pi} \times E_1(\rho_m) = \sum_B E_1(\psi(B)\rho_{m+1}),$$

la somme étant étendue à un ensemble d'idéaux B de $\mathcal{O}_F$ premiers à $\mathfrak{g}\mathfrak{P}^*$, dont les symboles d'Artin relatifs à $\mathcal{R}_{m+1}/F$ décrivent exactement $G(\mathcal{R}_{m+1}/\mathcal{R}_m)$. Cette formule résulte immédiatement de la formule (5), chapitre VI de [27]. De plus, il est aisé de tirer du lemme 2.10.5 la relation :

$$E_1(\psi(B)\rho_{m+1}) - \bar{\psi}(B) E_1(\rho_{m+1}) \in I'_{m+1}.$$

En outre, comme on a :

$$\sum_B \bar{\psi}(B) = q + \pi^{m+1} q \times \frac{q-1}{2},$$

on déduit la congruence :

$$\bar{\pi} E_1(\rho_m) \equiv \pi^{m+1} q E_1(\rho_{m+1}) \text{ modulo } \pi^{m+1} I'_{m+1},$$

et comme $q = \pi\bar{\pi}$, on conclut :

$$-\bar{g}_m E_1(\rho_m) \equiv -\bar{g}_{m+1} E_1(\rho_{m+1}) \text{ modulo } \pi^{m+1} I'_{m+1}.$$

D'ailleurs, toujours par la formule (5) chapitre VI de [27], en posant

$$\rho_{m,\,\mathfrak{g}} = \frac{\Omega}{g_m} \quad \text{et} \quad \rho_{m,\,\mathfrak{h}} = \frac{\Omega}{h\bar{\pi}^{m+1}} \quad \text{où } \mathfrak{h} = (h),$$

on a :

$$\frac{h}{g} \times E_1(\rho_{m,\,\mathfrak{g}}) = \sum_B E_1(\psi(B)\rho_{m,\,\mathfrak{h}}),$$

où B parcourt un ensemble en bijection avec $G(F(E_{\mathfrak{h}\bar{\pi}^{m+1}})/F(E_{\mathfrak{g}\bar{\pi}^{m+1}}))$ par le symbole d'Artin.

Donc, par le même argument que ci-dessus, on obtient la congruence $\gamma_{\mathfrak{P},\,\mathfrak{g},\,m} \equiv \gamma_{\mathfrak{P},\,\mathfrak{h},\,m} (\text{mod } \pi^{m+1} I''_m)$ où I''_m où l'on a remplacé $\mathfrak{g}$ par $\mathfrak{h}$. De plus, la suite de Cauchy $\{\gamma_{\mathfrak{P},\,\mathfrak{g},\,m}\}$ converge dans $I^{n.r.}$ et on a $\gamma_{\mathfrak{P},\,\mathfrak{g}} = \gamma_{\mathfrak{P},\,\mathfrak{h}}$ si $\mathfrak{g} \mid \mathfrak{h}$. On note alors $\gamma_{\mathfrak{P},\,\mathfrak{g}} = \gamma_{\mathfrak{P}}$ pour un $\mathfrak{g}$ quelconque. Posons maintenant $\tau = (\mathfrak{c}, F(E_{\mathfrak{g}\mathfrak{P}^\infty})/K)$, $\mathfrak{c}$ étant un idéal de $\mathcal{O}$ premier à $\mathfrak{g}\mathfrak{P}^*$. Toujours par le même argument, on voit que

$$\gamma_{\mathfrak{P},\,\mathfrak{g},\,m}{}^{\tau} \equiv \frac{N\mathfrak{c}}{\Lambda(\mathfrak{c})} \gamma_{\mathfrak{P},\,\mathfrak{g},\,m} \bmod \frac{\pi^{m+1}}{\Lambda(\mathfrak{c})},$$

d'où à la limite, l'égalité : $\gamma_{\mathfrak{P}}^{\tau} = N(\mathfrak{c})/\Lambda(\mathfrak{c})\,\gamma_{\mathfrak{P}}$. Étudions alors la divisibilité par p de l'élément $\gamma_{\mathfrak{P}}$ de $I^{n.r.}$. En utilisant la congruence (2) (iii) de la proposition 2.10.6, on est ramené à montrer que $\pi^{-b(m+1)} \times E_{a,\,b}(\rho_m)$ est, pour presque tout p ordinaire, une unité lorsque m est assez grand. Or, on prouve comme dans [4] la formule liant nombres d'Eisenstein et valeurs spéciales de fonctions L partielles. Rappelons que pour $\sigma \in G(\mathcal{R}_m/K)$, on définit une fonction L partielle par la formule

$$L(\bar{\varphi}^{a-b}, \sigma, s) = \sum_{\mathfrak{a}} \frac{\bar{\varphi}^{a-b}(\mathfrak{a})}{N\mathfrak{a}^s},$$

la somme portant sur les idéaux de $\mathcal{O}$ premiers à $\mathfrak{g}\mathfrak{P}^*$ et tel que $(\mathfrak{a}, \mathcal{R}_m/K) = \sigma$. Cette fonction se prolonge en une fonction entière. On peut

donc prendre sa valeur en $s=a$. En outre, pour φ tel que $\varphi \circ N_{F/K}=\psi$, on note

$$\mathscr{L}_{\varphi}(a, b, \sigma)=(a-1)!\left(\frac{2i\pi}{\sqrt{D_K}}\right)^{-b}\Omega^{-(a-b)}L(\bar{\varphi}^{a-b}, \sigma, a).$$

On a alors la formule (corollaire 5.7 de [9]), où l'on pose $\tau=(\mathfrak{c}, \mathscr{R}_m/K)$:

$$(*)\quad \pi^{-(m+1)b}E_{a,\,b}(\Lambda(\mathfrak{c})\rho_m, \mathscr{L}_{\sigma_{\mathfrak{c}}})=g_m^a\times\bar{g}^b(\varphi(\mathfrak{c})/\Lambda(\mathfrak{c}))^{a-b}\times\mathscr{L}_{\varphi}(a, b, \tau),$$

dont on reprendra la preuve dans un cas plus compliqué au chapitre 3. Cette formule fondamentale fournit le lien entre entre les nombres d'Eisenstein et les valeurs spéciales de fonctions L partielles. Or, il est prouvé au corollaire 4.11 de [9] que $\varphi(\mathfrak{c})/\Lambda(\mathfrak{c})=\beta(\sigma)$ ne dépend que de $\sigma=(\mathfrak{c}, F/K)$. On trouve donc que :

$$\sum_{\sigma\in H}\beta(\sigma)^{-(a-b)}\times(\mathrm{Tr}_{\mathscr{R}_m/F}(\pi^{-(m+1)b}\times E_{a,\,b}(\rho_m)))^{\sigma}$$
$$=g_m^a\times\bar{g}^b\times\left(1-\frac{\bar{\varphi}^{a-b}(\mathfrak{P}^*)}{N\mathfrak{P}^{*a}}\right)\times(a-1)!$$
$$\times\left(\frac{2i\pi}{\sqrt{D_K}}\right)^{-b}\Omega^{-(a-b)}L_{\mathfrak{g}}(\bar{\varphi}^{a-b}, a).$$

De plus, si $a>1$ et $b\neq 0$, on voit facilement que le facteur d'Euler du membre de droite est une unité $\mathfrak{P}$-adique de J, et si $a>2-b$, on voit que $L_{\mathfrak{g}}(\bar{\varphi}^{a-b}, a)\neq 0$ (cette valeur s'exprime en effet par un produit eulérien convergent). On fixe alors un tel couple (a, b). Pour tout p ordinaire premier à l'élément $(2i\pi/\sqrt{D_K})^{-b}\Omega^{-(a-b)}L_{\mathfrak{g}}(\bar{\varphi}^{a-b}, a)$ de F indépendant de p, on voit que $\gamma_{\mathfrak{P}}$ est une unité.

En tout cas pour *tout* p ordinaire $\neq 2,3$ on peut poser

$$\gamma_{\mathfrak{P}}=p^{r_{\mathfrak{P}}}.\gamma_{\mathfrak{P}}^0, \qquad \text{où} \quad \gamma_{\mathfrak{P}}^0$$

est une unité de $I^{m,r}$, puisque $\gamma_{\mathfrak{P}}\neq 0$. Pour presque tout p, $r_{\mathfrak{P}}$ est nul. De plus pour tout p ordinaire non ramifié dans F (et $\neq 2,3$), on voit en utilisant la proposition 2.6.1 que $\gamma_{\mathfrak{P}}^0$ est la dérivée à l'origine d'un isomorphisme de groupes formels défini sur I, de $\hat{E}$ à $\hat{\mathbb{G}}_m$, dont on note η l'inverse. On pose de plus $\Omega_{\mathfrak{P}}=1/\gamma_{\mathfrak{P}}^0$. On a donc; $\eta'(0)=\Omega_{\mathfrak{P}}$. C'est désormais le choix de période $\mathfrak{P}$-adique et d'isomorphisme de $\mathbb{G}_m$ à $\hat{E}$ qu'on sous-entendra.

2.11. Fonctions L $\mathfrak{P}$-adiques a deux variables

Reprenons d'abord le calcul d'intégrale posé à la fin du paragraphe 9. Soit

$$\Delta_a \mathscr{L}_\varphi(a, b, \sigma_c) = N\mathfrak{a}\, \mathscr{L}_\varphi(a, b, \sigma_c) - \varphi^a \bar{\varphi}^b(\mathfrak{a})\, \mathscr{L}_\varphi(a, b, \sigma_{ca}).$$

Proposition 2.11.1. — *On a, pour tout couple* (a, b) *admissible :*

$$\Omega_{\mathfrak{P}}^{-(a-b)} \times \int_G \psi_{\mathfrak{P}}^a \bar{\psi}_{\mathfrak{P}}^b \times \frac{d\mu}{\psi_{\mathfrak{P}}}(\mathfrak{a}, \mathfrak{c}) = 12(-1)^a g^a p^{r\mathfrak{P}^b} \times \varphi^a \bar{\varphi}^b(\mathfrak{c})$$

$$\times (\Delta_a \mathscr{L}_\varphi(a, b, \sigma_c) - \frac{\varphi^a \bar{\varphi}^b(\mathfrak{P})}{N\mathfrak{P}} \Delta_a \mathscr{L}_\varphi(a, b, \sigma_{c\mathfrak{P}})),$$

où le membre de droite qui est a priori *dans* $\iota_\infty(F)$ *est vu dans* I *via* $\iota_{\mathfrak{P}} \circ \iota_\infty^{-1}$.

Preuve. — Posons $I = \int_G \psi_{\mathfrak{P}}^{a-1} \bar{\psi}_{\mathfrak{P}}^{-b} d\mu$. Par définition de la mesure $\mu = \mu_{(\mathfrak{a}, \mathfrak{c})}$ sur G, on a l'égalité : $I = D_1^{a-1} D_2^{-b} \tilde{h}(0, 0)$ d'où pour tout $m \geqslant 0$, la congruence (*voir* [29], formule (17))

$$I \equiv \Omega_{\mathfrak{P}} \sum_{\tau \in G(F_m/F)} \frac{d^{a-1}}{dz_1^{a-1}} (j_m^\tau(\eta(e^{z_1} - 1))$$

$$- \frac{\Lambda(\mathfrak{P})^\sigma}{N\mathfrak{P}} \times j_m^{(\mathfrak{P})^\tau}(\eta(e^{z_1} - 1))\big|_{z_1 = 0} \times \bar{\psi}_{\mathfrak{P}}(\tilde{\tau})^{-b} \text{ modulo } \pi^{m+1}.$$

Or, par le lemme 2.10.5, en posant

$$\tau = (B, F_m/F), \qquad j_m = j_{(\mathfrak{a}, \mathfrak{c}, m)} \quad \text{et} \quad \sigma = (\mathfrak{c}, F/K),$$

on a l'égalité :

$$\frac{d^{a-1}}{dz_1^{a-1}} j_m^\tau(\eta(e^{z_1} - 1))\big|_{z_1 = 0} = 12(-1)^a \times \Omega_{\mathfrak{P}}^{a-1} \times \Lambda(\mathfrak{c})^a$$

$$\times \bar{\pi}^{-(m+1)a} \times \sum_B \{N\mathfrak{a}\, E_a(\Lambda(\mathfrak{c})\psi(BB_\tau)\rho_m, \mathscr{L}_\sigma)$$

$$- (\Lambda(\mathfrak{a})^\sigma)^a E_a(\Lambda(\mathfrak{ac})\psi(BB_\tau)\rho_m, \mathscr{L}_{\sigma\sigma_\mathfrak{a}})\},$$

parce que

$$j_m^\tau \circ \eta(e^{z_1} - 1) = \frac{d}{dz_1} \log \theta_m^\tau(\mathbf{e}_{\hat{E}}(\Omega_{\mathfrak{P}} z_1)),$$

et :

$$[\Phi(\mathfrak{c})]\circ[\bar{\pi}^{-(m+1)}]\circ \mathbf{e}_{\hat{E}}(z)=\mathbf{e}_{\hat{E}^{\sigma_{\mathfrak{c}}}}(\Lambda(\mathfrak{c})\,\bar{\pi}^{-(m+1)}\times z).$$

On utilise alors la formule :

$$\Omega_{\mathfrak{P}}^{\tilde{\tau}}=\bar{\psi}_{\mathfrak{P}}(\tilde{\tau})^{-1}.\Omega_{\mathfrak{P}} \qquad \text{pour} \quad \tilde{\tau}\in G(F_\infty/F),$$

qui est un cas particulier de (7). Donc :

$$E_a(\psi(BB_\tau)\Lambda(\mathfrak{c})\,\rho_m,\,\mathscr{L}_\sigma)\times\bar{\psi}_{\mathfrak{P}}(\tilde{\tau})^{-b}=N\mathfrak{c}^b\times\Lambda(\mathfrak{c})^{-b}\times\gamma_{\mathfrak{P}}^{0\,b}$$
$$\times\left\{E_a(\Lambda(\mathfrak{c})\,\psi(B)\,\rho_m,\,\mathscr{L}_\sigma)\left(\frac{\Lambda(\mathfrak{c})}{N\mathfrak{c}}\gamma_{\mathfrak{P}}^0\right)^{-b}\right\}^{\tilde{\tau}}$$

et donc en utilisant la proposition 2.10.6, (2), (γ), et la congruence

$$\gamma_{\mathfrak{P}}\equiv-\bar{g}_m E_1(\rho_m)\equiv-\bar{g}_m E_1(\psi(B)\rho_m) \pmod{\pi^{m+1}}$$
$$\text{pour} \quad (B,\,F_m/F)=\mathrm{Id}_{F_m},$$

on obtient la congruence suivante. Posons :

$$\Delta_{\mathfrak{a}}E^{\tau}_{a,\,b}(m,\,B,\,\mathfrak{c})=N\mathfrak{a}\,E_{a,\,b}(\Lambda(\mathfrak{c})\,\psi(BB_\tau)\,\rho_m,\,\mathscr{L}_\sigma)$$
$$-(\Lambda(\mathfrak{a})^{\sigma_{\mathfrak{c}}})^a\times E_{a,\,b}(\Lambda(\mathfrak{a}\mathfrak{c})\,\psi(BB_\tau)\,\rho_m,\,\mathscr{L}_{\sigma_{\mathfrak{a}\mathfrak{c}}}),$$

alors on a :

$$I\equiv 12(-1)^a\Omega_{\mathfrak{P}}^{a-b}p^{r_{\mathfrak{P}}b}\bar{\pi}^{-(m+1)a}\sum_{\tau\in G(F_m/F)}$$
$$\times\sum_B\{\Delta_{\mathfrak{a}}E^{\tau}_{a,\,b}(m,\,B,\,\mathfrak{c})-\frac{\Lambda(\mathfrak{P})}{N\mathfrak{P}}\Delta_{\mathfrak{a}}E^{\tau}_{a,\,b}(m,\,B,\,\mathfrak{c}\mathfrak{P})\}\ \text{modulo}\ \pi^{m+1}.$$

En utilisant alors la formule (*), et la transitivité des fonctions L partielles de conducteur fixé, pour les corps K et $\mathscr{R}_m$, on obtient le résultat de l'énoncé.

Lorsqu'il est nécessaire de préciser, on note $I=I_{(\mathfrak{a},\,\mathfrak{c})}(a,\,b)$.

La considération de la structure de la formule de la proposition 2.11.1, suggère d'introduire les objets suivants. Soit $\mathscr{P}$ l'ensemble des idéaux principaux de $\mathcal{O}$ de la forme $\mathfrak{a}=(\alpha)$ avec $\alpha\equiv 1 \bmod \mathfrak{g}$, et $\mathscr{F}$ l'ensemble des familles $\underline{n}=(n_{\mathfrak{a}})_{\mathfrak{a}\in\mathscr{P}}$ d'éléments de $\mathbb{Z}$ presque tous nuls telles que $\sum_{\mathfrak{a}\in\mathscr{P}}n_{\mathfrak{a}}(\bar{N}\mathfrak{a}-1)=0$.

Pour une telle famille $\underline{n}$, on pose :

$$I_{(\underline{n},\,\mathfrak{c})}(a,\,b)=\sum_{\mathfrak{a}\in\mathscr{P}}n_{\mathfrak{a}}\times I_{(\mathfrak{a},\,\mathfrak{c})}(a,\,b),$$

et pour chaque χ de $\hat{H}$, et pour tout couple admissible, on considère la quantité :

$$\sum_{\sigma \in H} \bar{\chi}(\sigma)(\varphi^a \bar{\varphi}^b)^{-1}(\mathfrak{c}) I_{(\underline{n}, \mathfrak{c})}(a, b).$$

Or, après avoir évalué cette expression à l'aide de la proposition précédente, on est amené à former l'analogue $\mathfrak{P}$-adique de l'égalité :

$$\Pi_{\chi \in \hat{H}} L_{\mathfrak{g}\mathfrak{P}^*}(\bar{\varphi}^{a-b} \cdot \bar{\chi}, s) = L_{\mathfrak{g}\mathfrak{P}^*}(\bar{\psi}^{a-b}, s).$$

où $\mathfrak{g}\mathfrak{P}^* = \mathfrak{g}\mathfrak{P}^* \mathcal{O}_F$.

On introduit donc une fonction L $\mathfrak{P}$-adique auxiliaire $L^0_{\mathfrak{P}}$ qui associe à un caractère $\lambda_{\mathfrak{P}} = \psi^a_{\mathfrak{P}} \bar{\psi}^b_{\mathfrak{P}}$, où (a, b) est admissible, le nombre :

$$\Pi_{\chi \in \hat{H}}\left(\sum_{\sigma \in H} \bar{\chi}(\sigma) \times (\varphi^a \bar{\varphi}^b)^{-1}(\mathfrak{c}) I_{(\underline{n}, \mathfrak{c})}(a, b)\right).$$

PROPOSITION 2.11.2. — *La fonction $L^0_{\mathfrak{P}}$ se prolonge par continuité en une fonction de* $\mathrm{Hom}_{\mathrm{Cont}}(G, I^\times)$ *dans I, possédant les propriétés suivantes :*

(i) *pour tout couple (i_1, i_2) d'entiers modulo $p-1$, il existe une série $G_0^{(i_1, i_2)} \in I[[T_1, T_2]]$, telle que pour tout couple admissible (a, b) congru à (i_1, i_2)* modulo $p-1$, *on ait pour $\lambda_{\mathfrak{P}} = \psi^a_{\mathfrak{P}} \bar{\psi}^b_{\mathfrak{P}}$:*

$$L^0_{\mathfrak{P}}(\lambda_{\mathfrak{P}}) = G_0^{(i_1, i_2)}(u_1^a - 1, u_2^b - 1).$$

(ii) *pour tout couple admissible (a, b) et $\lambda = \psi^a \bar{\psi}^b$, on a l'égalité dans $\bar{\mathbb{Q}}$:*

$$\iota_{\mathfrak{P}}^{-1}(\Omega_{\mathfrak{P}}^{-(a-b)d} L^0_{\mathfrak{P}}(\lambda_{\mathfrak{P}})) = \iota_\infty^{-1}((12(-1)^a g^a)^d \times \{S_n(a, b)\}^d$$
$$\times \left\{\Pi_{v \mid \mathfrak{P}}\left(1 - \frac{\check{\lambda}(v)}{Nv}\right)\left(1 - \frac{\lambda(v)}{Nv}\right)\right\} \times p^{r_{\mathfrak{P}} bd} \times ((a-1)!)^d \left(\frac{2\pi i}{\sqrt{D_K}}\right)^{-bd}$$
$$\times \Omega^{-(a-b)d} \times L_{\mathfrak{g}}(\bar{\psi}^{a-b}, a)).$$

où l'on note $S_{\underline{n}}(a, b) = \sum_{\mathfrak{a} = (\alpha) \in \mathcal{P}} n_{\mathfrak{a}}(N\mathfrak{a} - \alpha^a \bar{\alpha}^b)$, et où $\check{\lambda}$ désigne le caractère défini par $\check{\lambda}(\mathfrak{a}) = N\mathfrak{a}/\lambda(\bar{\mathfrak{a}})$.

Preuve. — On identifie dans la formule donnant $L^0_{\mathfrak{P}}(\lambda_{\mathfrak{P}})$ l'expression d'un déterminant de Dedekind :

$$L^0_{\mathfrak{P}}(\psi^a_{\mathfrak{P}} \bar{\psi}^b_{\mathfrak{P}}) = \pm \det_{\mathfrak{c}_1, \mathfrak{c}_2}((\varphi^a \bar{\varphi}^b)^{-1}(\mathfrak{c}_1 \mathfrak{c}_2) I_{(\underline{n}, \mathfrak{c}_1 \mathfrak{c}_2)}(a, b)),$$

c_1, c_2 parcourant indépendamment un système quelconque d'idéaux de $\mathcal{O}$ premiers à $g\mathfrak{P}^*$ dont les symboles d'Artin relatifs à F/K décrivent H sans répétition. On a donc :

$$L^0_{\mathfrak{P}}(\psi^a_{\mathfrak{P}}\bar{\psi}^b_{\mathfrak{P}}) = \pm(\varphi^a\bar{\varphi}^b)^{-1}\left(\prod_c c^2\right) \times \det_{c_1,\, c_1}(I_{(n,\, c_1 c_2)}((a, b)),$$

or on a : $\left(\prod_c c^2, F/K\right) = \mathrm{Id}_F$; car dans un groupe abélien fini le produit des carrés des éléments du groupe est toujours trivial. Il existe donc un idéal $\mathscr{C}$ de $\mathcal{O}_F$ tel que : $N_{F/K}\mathscr{C} = \prod_c c^2$, et donc le membre de droite vaut :

$$\lambda^{-1}(\mathscr{C})\ \det_{c_1,\, c_2}(I_{(n,\, c_1 c_2)}(a, b)),$$

qui est clairement un élément de I, et possède la propriété (i) parce que les intégrales $I_{(n,\, c_1 c_2)}$ étant uniformément convergentes peuvent se développer en séries de $u_1^a - 1$ et $u_2^b - 1$.

La formule (ii) provient de la substitution dans l'expression de $L^0_{\mathfrak{P}}(\lambda_{\mathfrak{P}})$, du résultat de la proposition précédente, et des formules :

$$\Pi_{\chi \in \hat{H}}\left(1 - \frac{\varphi^a\bar{\varphi}^b\bar{\chi}(\mathfrak{P})}{N\mathfrak{P}}\right) = \prod_{v \mid \mathfrak{P}}\left(1 - \frac{\psi^a\bar{\psi}^b(v)}{Nv}\right)$$

$$L_{g\widehat{\mathfrak{P}}^*}(\bar{\psi}^{a-b}, a) = L_{\mathfrak{g}}(\bar{\psi}^{a-b}, a) \times \prod_{v^* \mid \mathfrak{P}^*}\left(1 - \frac{\bar{\psi}^{a-b}(v^*)}{Nv^{*a}}\right)$$

et

$$\frac{\bar{\psi}^{a-b}(v^*)}{Nv^{*a}} = \frac{\bar{\chi}(\bar{v}^*)}{N\bar{v}^*}.$$

On se ramène alors à une fonction L complexe primitive. Soit pour cela $\mathfrak{f}_{a-b}$ le conducteur dans $\mathcal{O}_F$ du caractère $\bar{\psi}^{a-b}$, c'est aussi le conducteur de $\lambda = \psi^a\bar{\psi}^b$. On a :

$$L_{\mathfrak{g}}(\bar{\psi}^{a-b}, a) = \prod_{v \mid \mathfrak{g}\mathcal{O}_F,\ v \nmid \mathfrak{f}a-b}\left(1 - \frac{\bar{\psi}^{a-b}(v)}{Nv^a}\right) \times L_{\mathrm{prim}}(\bar{\psi}^{a-b}, a).$$

Maintenant, on va appliquer l'équation fonctionnelle à la fonction $L_{\mathrm{prim}}(\bar{\psi}^{a-b}, s)$ pour relier le membre de droite de (*) au nombre $L(\lambda, 1)$. Rappelons l'équation :

Soit

$$\Lambda\left(\left(\frac{\psi}{|\psi|}\right)^k, s\right) = \left(\frac{(2\pi)^d}{\sqrt{|D_F|}.N\mathfrak{f}_k}\right)^{-s}\Gamma\left(s + \frac{k}{2}\right)^d.L\left(\frac{\bar{\psi}^k}{|\psi|^k}, s\right),$$

alors, il existe un nombre algébrique de module 1, $W(\bar{\psi}^k)$, tel que pour tout s de $\mathbb{C}$, on ait ;

$$\Lambda\left(\frac{\bar{\psi}^k}{|\psi|^k}, s\right) = W(\bar{\psi}^k) \times \Lambda\left(\frac{\psi^k}{|\psi|^k}, 1-s\right).$$

On l'applique à $s=(a+b)/2$, $k=a-b$, et on obtient après un petit calcul utilisant que $D_F=(-1)^d.|D_F| = D_K^d \times N\mathcal{D}_{F/K}$:

$$(a-1)!^d\left(\frac{2i\pi}{\sqrt{D_K}}\right)^{-bd} \Omega^{-kd} L_{\text{prim}}(\bar{\psi}^k, a) = W(\bar{\psi}^k)$$
$$\times \sqrt{N(\mathcal{D}_{F/K}\mathfrak{f}_k)}^{-b} \times \left(\frac{(2i\pi)^d}{\sqrt{D_F N\mathfrak{f}_k}}\right)^{a-1}$$
$$\times ((-b)!)^d \times \Omega^{-kd} \times L_{\text{prim}}(\lambda, 1).$$

N désignant la norme des idéaux de F à $\mathbb{Q}$ i.e. $NB = \#(\mathcal{O}_F/B)$ et $\mathcal{D}_{F/K}$ la différente relative de F/K.

Et on prouve alors le lemme d'interpolation du signe de l'équation fonctionnelle.

LEMME 2.11.3. — *Pour tout couple* (i_1, i_2) *d'entiers modulo* $p-1$, *il existe un nombre algébrique* $c_{i_1-i_2}$ *qui ne prend que de la classe* modulo $p-1$ *de* i_1-i_2, *et qui est une unité* $\mathfrak{P}$*-adique, et il existe une série* $\sum^{(i_1, i_2)} \in \mathbb{Z}[[T_1, T_2]]$ *inversible dans l'anneau* $\mathbb{Z}_p[[T_1, T_2]]$, *tels que pour tout couple* (a, b) *congru à* (i_1, i_2) modulo $p-1$:

$$c_{i_1-i_2} \times \Sigma^{(i_1, i_2)}(u_1^a - 1, u_2^b - 1)$$
$$= \sqrt{N(\mathcal{D}_{F/K}\mathfrak{f}_k)}^{-b} \times W(\bar{\psi}^k) \times \sqrt{D_F N\mathfrak{f}_{i_1-i_2}}^{a-1}$$

Preuve. — On rappelle la formule ([10], proposition 1) $W(cc') = W(c)\,W(c')\,c(\mathfrak{f}_{c'})\,c'(\mathfrak{f}_c)$ où $W(c)$ désigne le signe dans l'équation fonctionnelle d'un caractère c des classes d'idèles de F et $\mathfrak{f}_c$ son conducteur, cette formule étant valide lorsque les types à l'infini de c et c' ont le même signe. C'est-à-dire, si pour chaque place v à l'infini, en posant

$$c_v(z) = \left(\frac{z}{|z|}\right)^{n_v} \quad \text{et} \quad c_v(z) = \left(\frac{z}{|z|}\right)^{n'_v} \quad \text{alors } n_v \times n'_v \geqslant 0.$$

On note k_0 le représentant de i_1-i_2 modulo $p-1$, compris entre 0 et $p-2$, et on applique la formule précédente à :

$$c=\left(\frac{\bar{\psi}}{|\psi|}\right)^{k-k_0} \qquad \text{et} \qquad c'=\left(\frac{\bar{\psi}}{|\psi|}\right)^{k_0},$$

où $k=a-b$ est congru à k_0 modulo $p-1$ et $k\geqslant k_0$. On développe alors $W(\bar{\psi}^{k-k_0})$ par la formule de décomposition locale ([23], p. 94) en remarquant que, comme $k-k_0\equiv O(p-1)$ et que $p\equiv 1$ modulo m (en désignant par m le nombre de racines de l'unité de K), $\bar{\psi}^{k-k_0}$ n'est pas ramifié. On trouve :

$$W(\bar{\psi}^{k-k_0})=(-i)^{d(k-k_0)}\times\frac{\bar{\psi}^{k-k_0}(\mathscr{D}_{F/\mathbf{Q}})}{\sqrt{(N\mathscr{D}_{F/F})\times|D_K|^{dk-k_0}}},$$

où $\mathscr{D}_{F/\mathbf{Q}}$ est la différente absolue de F. Après un petit calcul, on trouve donc l'expression suivante du membre de droite de l'égalité du lemme :

$$W(\bar{\psi}^{k_0})\sqrt{D_F N\mathfrak{f}_{k_0}}^{k_0-1}\times\bar{\psi}^{k-k_0}(\mathfrak{A})\times\sqrt{D_K}^{bd},$$

où l'on a posé $\mathfrak{A}=\mathscr{D}_{F/\mathbf{Q}}\mathfrak{f}_{k_0}$. Or on prouve aisément que pour tout entier n divisible par m et pour $\mathfrak{A}$ un idéal de $\mathcal{O}_F$ arbitraire, en notant $N_{F/K}(\mathfrak{A})=(\alpha)$, on a : $\psi^n(\mathfrak{A})=\alpha^n$. On pose donc

$$c_{i_1-i_2}=W(\bar{\psi}^{k_0})\sqrt{D_F N\mathfrak{f}_{k_0}}^{k_0-1},$$

et

$$\Sigma^{(i_1,\,i_2)}(u_1^a-1,\,u_2^b-1)=\alpha^{k-k_0}\sqrt{D_K}^{bd}.$$

On sait de plus que le nombre algébrique $W(\bar{\psi}^{k_0})$ n'est divisible que par des idéaux divisant $N\mathfrak{f}_{k_0}$, donc on voit que $c_{i_1-i_2}$ est un nombre algébrique premier à $\mathfrak{P}$. Il est clair en outre que $\Sigma^{(i_1,\,i_2)}$ est une unité de $\mathbf{Z}_p[[T_1,\,T_2]]$. On introduit encore les notations :

$$P(a,\,b)=p^{r\mathfrak{P}bd}\prod_{v\nmid\mathcal{O}_F,\ \text{et}\ v\nmid\mathfrak{f}_{a-b}}\left(1-\frac{\bar{\psi}^{a-b}(v)}{Nv^a}\right).$$

et

$$\mathrm{Eul}_p(\lambda)=\prod_{v\mid\mathfrak{P}}\left(1-\frac{\check{\lambda}(v)}{Nv}\right)\left(1-\frac{\lambda(v)}{Nv}\right).$$

On peut alors énoncer le théorème :

THÉORÈME 2.11.4. — *Il existe un unique couple* $(\Omega_p, L_{\mathfrak{P}})$ *constitué d'un élément de* $I^\times$ *et d'une fonction continue de* $\mathrm{Hom}_{\mathrm{cont}}(G, I^\times)$ *dans* I, *tel que pour chaque couple* (i_1, i_2) *d'entiers modulo* $p-1$, *les propriétés suivantes soient satisfaisantes :*

(i) *il existe une série* $G^{(i_1, i_2)}(T_1, T_2) \in I[[T_1, T_2]]$ *telle que pour tout couple d'entiers* (a, b) *congru à* (i_1, i_2) modulo $p-1$, *et* $\lambda_{\mathfrak{P}} = \psi_{\mathfrak{P}}^a \bar{\psi}_{\mathfrak{P}}^b$, *on ait :*

$$L_{\mathfrak{P}}(\lambda_{\mathfrak{P}}) = G^{(i_1, i_2)}(u_1^a - 1, u_2^b - 1),$$

(ii) *pour tout couple admissible* (a, b) *congru à* (i_1, i_2) modulo $(p-1)$, *et* $\lambda = \psi^a \bar{\psi}^b$, *on a l'égalité dans* $\bar{\mathbb{Q}}$:

$$\iota_{\mathfrak{P}}^{-1}(\Omega_{\mathfrak{P}}^{-(a-b)d} L_{\mathfrak{P}}(\lambda_{\mathfrak{P}})) = \iota_\infty^{-1}\left(c_{i_1 - i_2} \times \mathrm{Eul}_p(\lambda) \times P(a, b) \times (-b)!^d (2i\pi)^{d(b-1)} \left(\frac{\Omega}{2i\pi}\right)^{-(a-b)} L_{\mathrm{prim}}(\lambda, 1)\right).$$

Preuve. — Il suffit d'interpoler $(12(-1)^a g^a)^d$ par une unité de $\mathbb{Z}_p[[T_1]]$ ce qui est trivial, et $S_n(a, b)$ par un élément de $\mathbb{Z}_p[[T_1, T_2]]$. On applique pour cela le résultat du lemme 28 de [29] qui se transpose sans modification. On peut donc diviser par une unité de $\mathbb{Z}_p[[T_1, T_2]]$ la série $G_0^{(i_1, i_2)}$ de la proposition 2.11.2 pour $(i_1, i_2) \not\equiv (0,0)$ ou $(1,1)$ mod$(p-1)$, puis voir comme au théorème 29 de [29] qu'on peut encore conclure pour $(i_1, i_2) \equiv (0,0)$. Le cas $(1,1)$ reste en suspens (ça n'aura pas d'importance dans la suite) puisque Yager fait usage d'un prolongement de L au quadrant $a \geqslant 1$, $b \leqslant 0$ qui n'est pas prouvé dans notre situation. On utilise alors le lemme d'interpolation du signe de l'équation fonctionnelle pour conclure.

3. — Calculs de valeurs spéciales de fonctions L

3.1. LA $\mathbb{Z}_p^2$-EXTENSION DU CORPS DE MULTIPLICATION COMPLEXE

En prenant pour chaque entier $n \geqslant 0$ la p-extension maximale contenue dans le corps des rayons de K modulo $p^n \mathcal{O}$, on voit facilement qu'on construit une $\mathbb{Z}_p^2$-extension $K(p)$ de K. On sait de plus que le groupe de Galois de la composée de toutes les $\mathbb{Z}_p$-extensions d'un corps de nombres de degré δ, avec r_2 plongements imaginaires, est un $\mathbb{Z}_p$-module libre de

rang compris entre r_2+1 et δ. Pour le corps K, on voit donc qu'il n'y a qu'une $\mathbb{Z}_p^2$-extension, coïncidant de plus avec la composée de toutes les $\mathbb{Z}_p$-extensions de K. A cause du lemme 2.4.2, on voit que la composée de F et de cette $\mathbb{Z}_p^2$-extension coïncide avec la plus grande p-sous-extension de $\mathscr{F}_\infty/F$. On introduit les notations :

NOTATIONS 3.1.1. — On note K_m le corps de conducteur $\bar{\pi}^{m+1}$ contenu dans $K(p)$, et $\mathscr{K}_n$ le corps de conducteur $\mathfrak{P}^{n+1}$ contenu dans $K(p)$, et $K_{n,m}$ le composé de K_m de $\mathscr{K}_n$.

LEMME 3.1.2. — *Si p est premier à $d=[F:K]$, les corps F et K_m (resp. F et $\mathscr{K}_n$) sont disjoints sur K, de composé la plus grande p-sous-extension de F_m/F (resp. de $\mathscr{F}_n/F$).*

Preuve. — On voit d'abord que K_m est disjoint sur K du corps de Hilbert $\mathscr{R}_{(1)}$ de K et donc de toute extension abélienne de K contenant $\mathscr{R}_{(1)}$ et non ramifiée en $\mathfrak{P}^*$, par exemple : F, $\mathscr{R}_g$, $\mathscr{F}_n$. En effet, pour $\mathscr{R}_{(1)}$, c'est l'hypothèse $p \nmid d$ (car $[\mathscr{R}_{(1)}:K]$ divise d), puis pour L/K non ramifiée en $\mathfrak{P}^*$, on a :

$$K_m \cap L = K_m \cap \mathscr{R}_{(1)} = K.$$

On voit alors que

$$[K_m : K] = q^m \times q/p \qquad \text{où} \quad q = \pi.\bar{\pi},$$

en effet la p-partie du groupe des classes de rayons modulo π^{m+1} est isomorphe à celle de $(\mathcal{O}/\pi m+1)^\times$, qui compte $q^m \times q/p$ éléments. Donc $F.K_m$ est de la forme voulue. Il en va de même pour $F\mathscr{K}_n$.

On ajoute désormais aux hypothèses du chapitre II sur le nombre premier p considéré, que p ne divise pas d. On peut alors définir les corps et leurs groupes qui interviendront dans le calcul :

NOTATIONS 3.1.3. — On note $F'_{n,m}$ (resp F'_m, $\mathscr{F}'_n$) la plus grande p-sous-extension de F contenue dans $F_{n,m}$ (resp. F_m, $\mathscr{F}_n$) et $\Gamma_{n,m}$ son groupe de Galois sur F. Le groupe $\Gamma_{n,m}$ est aussi identifié au groupe de $K_{n,m}$ sur K. C'est encore le quotient de Γ par le sous-groupe engendré par $\gamma_1^{p^n}$ et $\gamma_2^{p^m}$.

3.2. INTÉGRALES LIÉES A UN CARACTÈRE D'ORDRE FINI DE Γ

Soit ρ un caractère d'ordre fini de Γ, il se factorise à travers $\Gamma_{n,m}$ en un caractère encore noté ρ. Quand on le considérera à valeurs $\mathfrak{P}$-adiques

(i.e. dans l'algèbre $I[\mu_{p^\infty}]=\varprojlim_N I[\mu_{p^N}]$), on le notera $\rho_{\mathfrak{P}}$. On se propose d'évaluer $L_{\mathfrak{P}}(\lambda_{\mathfrak{P}}\rho_{\mathfrak{P}})$, où, pour chaque couple admissible, on note $\lambda_{\mathfrak{P}}$ l'avatar $\mathfrak{P}$-adique du caractère $\lambda=\psi^a\bar{\psi}^b$. De plus, à l'aide de l'isomorphisme $\psi_{\mathfrak{P}}\times\bar{\psi}_{\mathfrak{P}}$ de Γ à $(1+p\mathbb{Z}_p)\times(1+p\mathbb{Z}_p)$, on fixe une base $\{\gamma_1, \gamma_2\}$ de Γ sur $\mathbb{Z}_p$, telle que

$$\psi_{\mathfrak{P}}\times\bar{\psi}_{\mathfrak{P}}(\gamma_1)=(u_1, 1),\ \psi_{\mathfrak{P}}\times\bar{\psi}_{\mathfrak{P}}(\gamma_2)=(1, u_2).$$

DÉFINITION 3.2.1. — On dira que ρ est primitif par rapport à la première variable si le caractère modulaire ξ défini ci-dessous est primitif au sens habituel :

$$\xi:\ (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times\to I[\mu_{p^\infty}]^\times\times \bmod p^{n+1}\mapsto \rho(\gamma_1^{l_1^{(x)}}\times \mathrm{Id}_{F_m'}),$$

où l'on note pour $\sigma\in G(\mathscr{F}_n'/F)$ et $\tau\in G(F_m'/F)$, $\sigma\times\tau$ l'élément de $\Gamma_{n,m}$ dont les restrictions sur $\mathscr{F}_n'$ et F_m' sont respectivement σ et τ. On abrégera souvent (incorrectement) en $\xi_1(x)=\rho(\gamma_1^{l_1^{(x)}})$.

On suppose désormais ρ primitif par rapport à la première variable.

CONVENTION 3.2.2. — On note encore ρ le caractère des idéaux de F premiers à p, défini par $\mathfrak{a}\mapsto\rho((\mathfrak{a}, F_{n,m}'/K))$ et on adopte la convention suivante : si v est une place de F au-dessus de $\mathfrak{P}$ (resp. de $\mathfrak{P}^*$), on pose :

$$\rho(v)=\begin{cases}0 & \text{si } \rho(\gamma_1)\neq 1,\\ \rho((v, F_m'/F) & \text{pour } m\gg 0 \text{ si } \rho(\gamma_1)=1.\end{cases}$$

$$\left(\text{resp. } \rho(v)=\begin{cases}0 & \text{si } \rho \text{ est ramifié en } v,\\ \rho((v, \mathscr{F}_n'/F)) & \text{sinon}\end{cases}\right).$$

On suppose pour l'instant $n\geqslant 0$, c'est-à-dire que $\rho(\gamma_1)\neq 1$, on verra que la modification à apporter si $\rho(\gamma_1)=1$ est minime. Soit Y_n l'automorphisme de $F_{n,m}'$ sur K, défini par ses restrictions aux sous-extensions $\mathscr{K}_n$ et F_m' disjointes sur K par :

$$(Y_n, \mathscr{K}_n/K)=(\mathfrak{gb}_n, \mathscr{K}_n/K)\qquad\text{et}\qquad(Y_n, F_m'/K)=\varphi_0^{n+1}$$

et soit $y_{n,c}=Y_n|_F\cdot(c, F/K)$, où φ_0 est le Frobenius de F_m' sur K en $\mathfrak{P}$). Notons $\tilde{\rho}$ un prolongement arbitraire de ρ à $G(F_{n,m}'/K)$. On pose les notations :

$$\mathscr{L}_{\varphi,\tilde{\rho}}(a, b, c)=(a-1)!\left(\frac{2i\pi}{\sqrt{D_K}}\right)^{-b}\Omega^{-(a-b)}L(\bar{\varphi}^{a-b}\tilde{\rho}^{-1}, y_{n,c}, a)$$

et

$$\Delta_a \mathscr{L}_{\varphi\tilde{\rho}}(a, b, c) = \mathrm{N}\,\mathfrak{a}\, \mathscr{L}_{\varphi, \tilde{\rho}}(a, b, c) - \varphi^a \bar{\varphi}^b(\mathfrak{a}).\, \mathscr{L}_{\varphi, \tilde{\varphi}}(a, b, ac).$$

Soit I_ρ l'intégrale $\int \psi_{\mathfrak{P}}^a \bar{\psi}_{\mathfrak{P}}^b \rho\, d\mu/\psi_{\mathfrak{P}}$. On la calcule dans la :

PROPOSITION 3.2.3. — *On a l'égalité :*

$$\Omega_{\mathfrak{P}}^{-(a-b)} I_\rho = 12(-1)^a g^a . p^{r\mathfrak{P}b} . \frac{\tau_1(\rho, \zeta_1)}{p^{n+1}} . (\tau_n/\Omega)^{-a} \times \overline{(\tau_n/\Omega)}^{-b}$$
$$\times \tilde{\rho}(Y_n . (c, F_{n,m}/K)) . \varphi^a \bar{\varphi}^b(c\mathfrak{d}_n) \times \Delta_a \mathscr{L}_{\varphi, \tilde{\rho}}(a, b, c),$$

où $\tau_1(\rho, \zeta_1)$ *est une somme de Gauss associée à* ρ, *définie dans la démonstration. On pratique encore l'abus de notation qui identifie le membre de droite avec son image par* $\iota_{\mathfrak{P}} \circ \iota_\infty^{-1}$.

Preuve. — Évaluons $I_\rho = I_{a,c}(a, b, \rho) = \int \psi_{\mathfrak{P}}^a \bar{\psi}_{\mathfrak{P}}^b \rho \frac{d\mu}{\psi_{\mathfrak{P}}}$. On obtient aisément par la formule (iii), proposition 2.9.4, l'égalité :

$$I_\rho = \sum_{a_1 \bmod p^{n+1},\ a_2 \bmod q^{m+1}} \xi_1 \otimes \xi_2^{-1}(\zeta_1^{a_1}, \zeta_2^{a_2}) D_1^{a-1} D_2^{-b} \tilde{h}(\zeta_1^{a_1} - 1, \zeta_2^{a_2} - 1),$$

où

$$\xi_i(x) = \rho(\gamma_i^{l_i(x)}) \quad (i = 1, 2).$$

Le conducteur exact de ξ_1 est p^{n+1}, celui de ξ_2 divise q^{m+1}. On a fixé de plus ζ_1 (resp. ζ_2) une racine primitive (p^{n+1})-ième (resp. (q^{m+1})-ième) de 1. Le choix de ζ_1 interviendra par la suite, mais il s'avère que celui de ζ_2 n'a pas d'importance parce que les quantités qui la font intervenir se détruiront au cours des calculs.

En utilisant alors la définition de h, et l'équation fonctionnelle de j (proposition 2.8.3) on obtient :

$$(D_1^{a-1} D_2^{-b} \tilde{h})(\zeta_1^{a_1} - 1, \zeta_2^{a_2} - 1) \equiv \Omega_{\mathfrak{P}} \times \sum_{\tau \in G(F_m/F)} (D_1^{a-1}(j_m^\tau \circ \eta)(\zeta_1^{a_1} - 1)$$
$$- \frac{\Lambda(\mathfrak{P})^a}{N\mathfrak{P}} . D_1^{a-1}(j_m^{(\mathfrak{P})^\tau} \circ \eta)(\zeta_1^{a_1} - 1)) \times \bar{\psi}_{\mathfrak{P}}^{-b}(\tilde{\tau}) \times \zeta_2^{a_2 \bar{\psi}_{\mathfrak{P}}(\tilde{\tau})}.$$

Cette congruence a lieu modulo π^{m+1}, m est donc astreint à tendre vers $+\infty$.

Cette congruence n'est jamais une égalité, mais ceci uniquement à cause du facteur $\bar{\psi}_{\mathfrak{P}}(\tilde{\tau})$ qui introduira la période $\mathfrak{P}$-adique.

D'autre part, par définition de la transformée de Fourier d'une fonction sur un groupe abélien fini, on voit que

$$\xi_1 \otimes \xi_2^{-1}(\zeta_1^{a_1}, \zeta_2^{a_2}) = \frac{1}{p^{n+1}q^{m+1}}\Big(\sum_{x_1 \bmod p^{n+1}} \xi_1(x_1)\zeta_1^{-a_1x_1}\Big) \times \Big(\sum_{x_2 \bmod q^{m+1}} \xi_2^{-1}(x_2).\zeta_2^{-a_2x_2}\Big),$$

et en regroupant dans l'expression de I_ρ ci-dessus les termes en x_2 et a_2, on trouve l'expression :

$$\sum_{a_2,\, x_2} \xi_2^{-1}(x_2)\zeta_2^{-a_2x_2}\zeta^{a_2}\bar{\Psi}_{\mathfrak{P}}(\tilde{\tau}),$$

qui vaut $q^{m+1}\xi_2^{-1}(\bar{\Psi}_{\mathfrak{P}}(\tilde{\tau}))$.

De plus, comme ξ_1 est primitif, on peut faire apparaître la somme de Gauss

$$\tau_1(\rho, \zeta_1) = \sum_{x_1 \bmod p^{n+1}} \xi_1(x_1)\zeta_1^{x_1},$$

et on prouve la formule intermédiaire :

LEMME 3.2.4. — *Si* $\rho(\gamma_1) \neq 1$, *on a :*

$$I_\rho \equiv \Omega^a \times \frac{\tau_1(\rho, \zeta_1)}{p^{n+1}} \sum_{a_1 \bmod p^{n+1},\ \tau \in G(F_m/F)} \rho^{-1}(\gamma_1^{l_1(a_1)} \times \tau) \times \bar{\psi}^{-b}(\tilde{\tau}) \times D_{\hat{E}}^{a-1} j_m^{\tau}([a_1]v_n) \text{ modulo } \pi^{m+1},$$

où, pour tout $n \geqslant 0$, v_n *est le point primitif de* p^{n+1}*-torsion sur* $\hat{E}$, *défini par* $v_n(\zeta_1 - 1)$.

Preuve. — Il suffit de voir, dans l'expression de I_ρ que

$$(D_1^{a-1}(j_m^{\tau} \circ \eta))(\omega_1) = \Omega_{\mathfrak{P}}^{a-1} \times D_{\hat{E}}^{a-1} j_m^{\tau}(\eta(\omega_1)),$$

et que

$$\sum_{a_1 \bmod p^{n+1}} \xi_1^{-1}(a_1) \times D_1^{a-1}(j_m^{(\mathfrak{P})\tau} \circ \eta)(\zeta_1^{a_1} - 1) = 0,$$

parce que

$$[\Phi(\mathfrak{P})] \circ \eta(\zeta_1^{a_1} - 1) = \eta^{\varphi_0}(\zeta_1^{a_1 p} - 1),$$

et que ξ_1 est primitif, donc,

$$\sum_{a_1 \bmod p^{n+1},\ a_1 \equiv 1 \bmod p^n} \xi_1^{-1}(a_1) = 0.$$

On évalue alors $D_E^{a-1} j_m^{\tau}([a_1] v_n)$. Pour cela, choisissons pour chaque $n \geqslant 0$, un élément ε_n *de* $\mathcal{O}$ tel que $\varepsilon_n \bar{\pi} \equiv 1 \pmod{\mathfrak{P}^{n+1}}$, et un élément $\tau_n \in \mathfrak{P}^{-(n+1)} \mathcal{L}/\mathcal{L}$, tel que $W(\tau_n, \mathcal{L})$ ait pour paramètre v_n. On peut alors écrire $\tau_n/\Omega . \mathcal{O} = \mathfrak{d}_n/(\mathfrak{P}^{n+1})$, où $\mathfrak{d}_n$ est un idéal de $\mathcal{O}$, premier à un ensemble fini pour l'instant arbitraire, mais contenant $\mathfrak{P}$. On voit facilement que $\mathfrak{P}^* \mathfrak{d}_{n+1}$ et $\mathfrak{d}_n$ sont dans la même classe des rayons modulo $\mathfrak{P}^{n+1}$.

LEMME 3.2.5. — *Pour chaque entier a_1 premier à p, et tout $\tau \in G(F_m/F)$, on a :*

$$D_E^{a-1} j_m^{\tau}([a_1] v_n) = 12(-1)^a . \Lambda(c)^a . \bar{\pi}^{-(m+1)a} \times \sum_B \{ N\mathfrak{a} \, E_a(a_1 \varepsilon_n^{m+1} \Lambda(c) \tau_n + \Lambda(c) \psi(BB_\tau) \rho_m, \mathcal{L}_{\sigma_c}) - (\Lambda(a)^{\sigma_c})^a \times E_a(a_1 \varepsilon_n^{m+1} . \Lambda(ac) \tau_n + \Lambda(ac) \psi(BB_\tau) \rho_m, \mathcal{L}_{\sigma_{ac}}) \}.$$

Preuve. — Tout-à-fait analogue à celle du lemme 2.10.5, en remarquant que $e_E(\varepsilon_n \tau_n) = [\bar{\pi}^{-1}] v_n$.

On procède alors comme dans la preuve de la proposition 2.11.1. Remarquons toutefois que l'égalité qui donne I_p pour un m assez grand, est remplacée au cours du calcul par une congruence, parce que la période $\mathfrak{P}$-adique n'est qu'approximée par des nombres d'Eisenstein. Plus précisément, en posant

$$\rho_{B,\tau}(n, m) = a_1 \varepsilon_n^{m+1} \tau_n + \psi(BB_\tau) \rho_m,$$

et en notant $\tilde{\tau}$ un prolongement arbitraire de τ à $\mathcal{R}_\infty$, on voit en utilisant 2.10.7, que :

$$(1) \quad \bar{\psi}_{\mathfrak{P}}(\tilde{\tau})^{-b} \times E_a(\Lambda(c) \rho_{B,\tau}(n, m), \mathcal{L}_\sigma) = (\gamma_{\mathfrak{P}}^0)^b \times \{ E_a(\rho_{B,\tau}(n, m), \mathcal{L}) \times (\gamma_{\mathfrak{P}}^0)^{-b} \}^{\tilde{\tau}\sigma_c}.$$

$$(2) \quad \gamma_{\mathfrak{P}} \equiv -\bar{g}_m E_1(\rho_{B,\tau}(n, m)) \bmod \pi^{m - m(n)},$$

où $m(n)$ est en entier $\geqslant 0$ ne dépendant que de n. En effet la suite de terme général $-\bar{g}_m E_1(\rho_{1,1}(n, m))(m = (m = 1, 2, \ldots)$ est de Cauchy dans $I[E_{\mathfrak{P}^{n+1}}]$, et est adjacente à $-\bar{g}_m E_1(\rho_m)$, donc converge vers $\gamma_{\mathfrak{P}}$.

On déduit des deux remarques ci-dessus la congruence, valable pour tout m suffisamment grand (n étant fixé)

$$I_p \equiv 12(-1)^a p^{r\mathfrak{P}^b} \Omega_{\mathfrak{P}}^{a-b} . \Lambda(c)^a \bar{\pi}^{-(m+1)a} \frac{\tau_1(\rho, \zeta_1)}{p^{n+1}} \times$$

$$\times \sum^{\tau \in G(F_m/F)} \sum_B \{ N\mathfrak{a}\, \bar{g}_m^{-b} E_{a,\,b}(\Lambda(\mathfrak{c})\, \rho_{B,\,\tau}(n,\,m),\, \mathscr{L}_{\sigma_\mathfrak{c}})$$
$$-(\Lambda(\mathfrak{a})^{\sigma_\mathfrak{c}})^a\, \bar{g}_m^{-b} E_{a,\,b}(\Lambda(\mathfrak{a}\mathfrak{c})\, \rho_{B,\,\tau}(n,\,m),\, \mathscr{L}_{\sigma_{\mathfrak{a}\mathfrak{c}}})) \bmod \pi^{m-m(n)}.$$

On transforme alors les nombres d'Einsenstein en fonction L partielle.

PROPOSITION 3.2.5. — *Pour $\tau \in G(F_m/F)$, on a :*

$$\bar{g}_m^{-b} \sum_B E_{a,\,b}(\Lambda(\mathfrak{c})\, \rho_{B,\,\tau}(m,\,m),\, \mathscr{L}_\sigma) = (a-1)!\, g_m^a\, (\overline{\tau_n/\Omega})^{-b} \times \Lambda(\mathfrak{c})^{b-a}$$
$$\times \varphi^{a-b}(\mathfrak{c}) \frac{\bar{\varphi}^{a-b}(\mathfrak{d}_n)}{N\mathfrak{d}_n^{-a}} \times \left(\frac{2i\pi}{\sqrt{D_k}}\right)^{-b} \times \Omega^{-(a-b)} L(\bar{\varphi}^{a-b},\, \upsilon_{a_1,\,\tau},\, a),$$

où $\upsilon_{a_1,\,\tau} \in G(\mathscr{K}_n F_m/K)$ est défini par ses restrictions aux deux corps disjoints sur K, $\mathscr{K}_n$ et F_m :

$$(\upsilon_{a_1,\,\tau},\, \mathscr{K}_n/K) = (a_1\, g\, \mathfrak{d}_n\, \mathfrak{c},\, \mathscr{K}_n/K),$$

et

$$(\upsilon_{a_1,\,\tau},\, F_m/K) = \tau\varphi_0^{n+1}(\mathfrak{c},\, F_m/K),$$

où : $\varphi_0 = (\mathfrak{P},\, F_m/K)$ est le Frobenius en $\mathfrak{P}$.

Preuve. — Par définition de $E_{a,\,b}$ on est ramené à prouver l'égalité :

$$(\Lambda(\mathfrak{c})\,\Omega)^b\, \overline{(\Lambda(\mathfrak{c})\,\Omega)^b} \times N\mathfrak{c}^{-b} \times H_{a,\,-b}(\Lambda(\mathfrak{c})\, \rho_{B,\,\tau}(n,\,m),\, a,\, \mathscr{L}_\sigma)$$
$$= g_m^a\, (\tau_n/\Omega)^{-a} (\tau_n/\Omega)^{-b} \times \Lambda(\mathfrak{c})^{b-a} \varphi^{a-b}(\mathfrak{c}) \times \frac{\bar{\varphi}^{a-b}(\mathfrak{d}_n)}{N\mathfrak{d}_n^{-a}}$$
$$\times \Omega^{-(a-b)} L(\bar{\varphi}^{a-b},\, \upsilon_{a_1,\,B,\,\tau},\, a)$$

où $\upsilon_{a_1,\,B,\,\tau}$ est le prolongement de $\upsilon_{a_1,\,\tau}$ à $\mathscr{K}_n \mathscr{R}_m$ tel que

$$\upsilon_{a_1,\,B,\,\tau}|_{\mathscr{R}_m} = \tau\varphi_0^{n+1}(\mathfrak{c} \times N_{F/K}(B),\, \mathscr{R}_m/K).$$

Or, pour $\mathscr{R}\mathrm{e}(s) > (a-b)/2 + 1$, on a :

$$H_{a-b}(\Lambda(\mathfrak{c})\, \rho_{B,\,\tau}(n,\,m),\, s,\, \mathscr{L}_\sigma) = \frac{(\tau_n/\Omega \times \Lambda(\mathfrak{c})\,\Omega/g_m)^{a-b}}{|\tau_n/\Omega \times (\Lambda(\mathfrak{c})\,\Omega/g_m|^{2s}}$$
$$\times H_{a-b}(x_{n,\,m},\, s,\, g_m \mathfrak{P}^{n+1}.(\mathfrak{c}\mathfrak{d}_n)^{-1}),$$

où $x_{n,\,m} = a_1\, \varepsilon_n^{m+1}\, g_m + (\tau_n/\Omega)^{-1}.\psi(BB_\tau)$ est un élément de $K^\times$ de dénominateur $\mathfrak{d}_n$.

Fixons alors φ un Grössencharakter tel que $\varphi \circ N_{F/K} = \psi$, on a la formule :

$$H_{a-b}(x_{n,m}, s, g_m \mathfrak{P}^{n+1}(\mathfrak{cd}_n)^{-1}) = \left(\frac{\bar{\varphi}^{a-b}(\mathfrak{cd}_n)}{N(\mathfrak{cd}_n)^s}\right)^{-1} \times L(\bar{\varphi}^{a-b}, \upsilon_{a_1, B, \tau, s}).$$

Pour le voir, introduisons l'ensemble $\mathcal{J}$ des idéaux entiers $\mathfrak{a}$ de k, premiers à gp, dont le symbole d'Artin relatif à $\mathcal{K}_n \mathcal{R}_m$ est $\upsilon_{a_1, B, \tau}$ Il faut montrer que l'application $(\mathfrak{cd}_n)^{-1} \to \mathcal{J}$ qui à un élément γ de $(\mathfrak{cd}_n)^{-1}$ associe l'idéal $\mathfrak{cd}_n(x_{n,m} + g_m(\tau_{n/\Omega})^{-1}\gamma)$ est bijective. Elle est injective puisque g_m est multiple de f, qui sépare les racines de l'unité de K. On voit aisément que cette fonction prend bien ses valeurs dans I. Soit maintenant $\mathfrak{a} \in I$. On a en particulier l'égalité :

$$(\mathfrak{a}, \mathcal{R}_m/K) = (\mathfrak{c}\mathfrak{P}^{n+1}.N_{F/K} BB_\tau, \mathcal{R}_m/K),$$

d'où l'on tire aisément que $\mathfrak{a} = \mathfrak{cd}_n.(.\tau_n/\Omega)^{-1}\psi(BB_\tau) + g_m\alpha)$ où α a ses pôles concentrés dans $\mathfrak{cd}_n$. De plus, on a :

$$(\mathfrak{a}, \mathcal{K}_n/K) = (\mathfrak{cd}_n(g_m\alpha), \mathcal{K}_n/K) = (a_1 g \mathfrak{d}_n \mathfrak{c}, \mathcal{K}_n/k),$$

donc $(\alpha\bar{\pi}^{m+1}) = (a_1\delta)$ où $\delta \in K^\times$ et $\delta \equiv 1 \bmod^\times \mathfrak{P}^{n+1}$ on peut donc choisir α tel que : $\alpha = a_1 \varepsilon_n^{m+1} + \gamma$, γ ayant ses pôles dans $\mathfrak{cd}_n$ et étant de valuation $\mathfrak{P}$-adique plus grande que $n+1$. En reportant la valeur de α dans l'expression de $\mathfrak{a}$, on voit que γ est un antécédent de $\mathfrak{a}$, d'où la surjectivité. Ce qui achève la preuve de la proposition 2.2.5. On revient alors à la preuve de la proposition 3.2.3. En reportant dans l'expression de I_ρ, on a à considérer la somme :

$$\sum_{(a_1, \tau)} \rho^{-1}(\gamma_1^{l(a_1)} \times \tau).L(\bar{\varphi}^{a-b}, \upsilon_{a_1, \tau}, a).$$

Fixons un prolongement arbitraire $\tilde{\rho}$ de ρ à $G(F'_{n,m}/K) = \Gamma_{n,m} \times H$. On voit facilement que si les entiers a_1 sont congrus à 1 modulo f, ce qu'on peut supposer, alors $\gamma_1^{l(a_1)}$ et $((a_1, \mathcal{K}_n/K)$ coïncident sur $\mathcal{K}_n$, puisque pour $P \in E_{\mathfrak{P}^{n+1}}$ de paramètre t, on a par définition :

$$\gamma_1^{l(a_1)}(t) = [\langle a_1 \rangle]t,$$

où le diamant d'un élément de $\mathbb{Z}_p^\times$ est sa projection sur $1 + p\mathbb{Z}_p$.

Or, on a :

$$((a_1), \mathcal{F}_n/K)P = \Phi((a_1))_E P = a_1 P,$$

donc, on voit que sur la p-extension $\mathscr{K}_n/K$, l'automorphisme $((a_1), \mathscr{F}_n/K) \circ \gamma_1^{l(a_1)}$, d'ordre divisant $p-1$, est trivial. Par conséquent, la somme ci-dessus vaut :

$$\tilde{\rho}(\eta_n \cdot (\mathfrak{c}, F'_{n,m}/K)) \times L(\bar{\varphi}^{a-b} \times \tilde{\rho}^{-1}, y_{n,\mathfrak{c}}, a),$$

où η_n est l'automorphisme de $F'_{n,m}/K$, défini par

$$(\eta_n, \mathscr{K}_n/K) = (g\mathfrak{d}_n, \mathscr{K}_n/K),$$
$$(\eta_n, F'_m/K) = \varphi_0^{n+1}.$$

et $y_{n,\mathfrak{c}} = \eta_{n|F} \cdot (\mathfrak{c}, F/K)$, la fonction L partielle étant relative au conducteur $g\mathfrak{P}^{n+1}\bar{\mathfrak{P}}^{m+1}$ $(m \geqslant 0)$. En mettant alors ces résultats ensemble, on obtient la formule de la proposition 3.2.3.

3.3. Fin du calcul

Soit maintenant n un élément quelconque de $\mathscr{F}$, on peut évidemment prolonger la fonction auxiliaire $L^0_{\mathfrak{P}}$ (dépendant de n), par extension des scalaires, en une fonction continue de $\mathrm{Hom}_{\mathrm{cont}}(G, I[\mu_{p^\infty}]^\times)$ dans $I[\mu_{p^\infty}]$ et on a le :

Lemme 3.3.1. — *Pour tout caractère* ρ *d'ordre fini de* Γ, *et tout couple admissible* (a, b), *avec* $\lambda = \psi^a \bar{\psi}^b$, *on a*

$$L^0_{\mathfrak{P}}(\lambda_{\mathfrak{P}} \rho_{\mathfrak{P}}) = \prod_{\chi \in H} \left(\sum_{\sigma \in H} \bar{\chi}(\sigma) \tilde{\rho}^{-1}((\mathfrak{c}, F'_{n,m}/K)) (\varphi^a \bar{\varphi}^b)^{-1}(\mathfrak{c}), I_{(\underline{n}, \mathfrak{c}, \rho)}\right)$$

(n, m) *étant tel que* ρ *se factorise à travers* $\Gamma_{n,m}$, *et* $\tilde{\rho}$ *désignant un prolongement arbitaire fixé de* ρ *à* $G(F'_{n,m}/K)$.

Preuve. — Par la définition de $L^0_{\mathfrak{P}}$, en notant $\mathscr{C}$ un idéal de $\mathcal{C}_F$ tel que $N_{F/K}\mathscr{C} = \prod_{\mathfrak{c}} \mathfrak{c}^2$, $\mathfrak{c}$ parcourant un ensemble d'idéaux de $\mathcal{C}$ premiers à p, et $(\mathfrak{c}, F/K) = \sigma$ décrivant H, on a :

$$L^0_{\mathfrak{P}}(\lambda_{\mathfrak{P}} \rho_{\mathfrak{P}}) = \lambda_{\mathfrak{P}} \rho_{\mathfrak{P}}(\mathscr{C}^{-1}) \times \det_{\mathfrak{c}_1, \mathfrak{c}_1} \left\{ \int_G \lambda_{\mathfrak{P}} \rho_{\mathfrak{P}} \frac{d\mu_{(\underline{n}, \mathfrak{c}_1 \mathfrak{c}_2)}}{\psi_{\mathfrak{P}}} \right\},$$

où $\rho_{\mathfrak{P}}(\mathscr{C}) = \rho_{\mathfrak{P}}((\mathscr{C}, F'_{n,m}/F))$.

Or, par la formule du déterminant de Dedekind, on voit facilement que les membres de droite de la formule ci-dessus et de celle du lemme coïncident.

En utilisant alors le résultat de la proposition 3.2.2, on obtient la formule de la :

PROPOSITION 3.3.1. — *On a l'égalité :*

$$\iota_{\mathfrak{P}}^{-1}(\Omega_{\mathfrak{P}}^{-(a-b)d} \times L_{\mathfrak{P}}^{0}(\lambda_{\mathfrak{P}}\rho_{\mathfrak{P}})) = \iota_{\infty}^{-1}\left((12(-1)^a g^a)^d \times p^{r_{\mathfrak{P}}bd}\left(\frac{\tau_1(\rho,\zeta_1)^d}{p^{n+1}}\right)\right.$$
$$\times (\tau_n/\Omega)^{-ad}\overline{(\tau_n/\Omega)}^{-bd}.\,\rho(Y_n^d).\,\varphi^a\bar{\varphi}^b(\mathfrak{d}_n^d) \times (S_{\underline{n},\rho}(a,b))^d$$
$$\left.\times \Pi_{\chi\in\hat{H}}\left\{(a-1)!\left(\frac{2i\pi}{\sqrt{D_K}}\right)^{-b}\Omega^{-(a-b)}L(\bar{\varphi}^{a-b}\tilde{\rho}^{-1}\bar{\chi},\,a)\right\}\right),$$

où $S_{\underline{n},\rho}(a,b)$ *est la somme analogue à* $S_{\underline{n}}(a,b)$ *où l'on a remplacé* $\varphi^a\bar{\varphi}^b$ *par* $\varphi^a\bar{\varphi}^b\rho$.

Remarque. — (i) La présence de $\mathfrak{d}_n$ *et de* τ_n/Ω dans la formule compense l'arbitraire du choix de la racine primitive ζ_1 dans la somme de Gauss $\tau_1(\rho,\zeta_1)$.

(ii) Noter l'absence du tilde sur $\rho(Y_n^d)$, parce que Y_n^d fixe F.

(iii) La fonction L qui apparaît ne contient pas les facteurs d'Euler aux places divisant $g\mathfrak{P}$, elle n'est donc pas primitive.

On procède alors comme au chapitre 2, paragraphe 11. On voit d'abord, pour $\lambda=\psi^a\bar{\psi}^b$, que :

$$\Pi_{\chi\in\hat{H}}L(\bar{\varphi}^{a-b}.\tilde{\rho}^{-1}.\bar{\chi},\,a) = \prod_{v\mid\mathfrak{P}}\left(1-\frac{\check{\widehat{\lambda\rho}}(v)}{Nv}\right)$$
$$\times\prod_{v\mid\mathfrak{P},\,v\nmid\mathfrak{f}_{a-b}}\left(1-\frac{\bar{\psi}^{a-b}.\rho^{-1}(v)}{Nv^a}\right)\times L_{\text{prim}}(\bar{\psi}^{a-b}\rho,\,a),$$

où l'on note $\rho(v)=\rho((v,F_\infty/F))$ pour toute place v finie de F étrangère à p, et $\hat{\widehat{\lambda\rho}}(v)$ est défini par la convention 3.2.2 lorsque $v\mid\mathfrak{P}$. Noter qu'on a toujours $\lambda\rho(v)=\lambda(v).\rho(v)$, car les conducteurs de λ et ρ sont premiers entre eux dans $\mathcal{O}_F$.

Ensuite on applique l'équation fonctionnelle à la fonction L primitive, isolée grâce à la formule précédente. On trouve, avec $k=a-b$:

$$((a-1)!)^d\left(\frac{2i\pi}{\sqrt{D_K}}\right)^{-bd}\Omega^{-kd}\times L_{\text{prim}}(\bar{\psi}^k\bar{\rho},\,a) = W(\bar{\psi}^k\bar{\rho})\times\sqrt{N(\mathscr{D}_{F/F}\mathfrak{f}_k\mathfrak{f}_\rho)}^{-b}$$
$$\times\left(\frac{(2i\pi)^d}{\sqrt{D_F N(\mathfrak{f}_k\mathfrak{f}_\rho)}}\right)^{a-1}\times((-b)!)^d\Omega^{-kd}L_{\text{prim}}(\lambda\rho,\,1),$$

où $\mathfrak{f}_\rho$ est le conducteur de ρ vu comme caractère des idèles de F, c'est un idéal de $\mathcal{O}_F$ dont le support est concentré au-dessous de p.

On applique alors la formule ([23]...) :

$W(cc') = W(c)\,W(c').\,c(\mathfrak{f}_{c'}).\,c'(\mathfrak{f}_c)$, où $W(c)$ désigne le signe dans l'équation fonctionnelle d'un caractère c des classes d'idèles de F (on note par abus de notation $W(\Psi^k\bar{\rho})$ pour $W(\Psi^k\rho/|\psi|^k)$), valable ici pour $c=\Psi^k$ et $c'=\bar{\rho}$ car $(\mathfrak{f}_\rho, \mathfrak{f}_k)=1$, et que le type à l'infini de ρ est 0, pour obtenir la :

PROPOSITION 3.3.3. — *Pour tout caractère ρ d'ordre fini de Γ, tel que $\rho(\gamma_1)\neq 1$, on a l'égalité :*

$$\iota_{\mathfrak{P}}^{-1}(\Omega_{\mathfrak{P}}^{-d(a-b)} L_{\mathfrak{P}}(\lambda_{\mathfrak{P}}\rho_{\mathfrak{P}})) = \iota_\infty^{-1}(c_{i_1-i_2}\times \mathrm{Eul}_p(\lambda\rho) \times P_\rho(a,b)\times\varepsilon_\rho(a,b)\times(\tau_n/\Omega)^{-ad}\times W(\rho)\times\left(\frac{\tau_1(\rho,\zeta_1)}{p^{n+1}}\right)^d \times((-b)!)^d(2i\pi)^{d(b-1)}.\left(\frac{\Omega}{2i\pi}\right)^{-(a-b)d}\times L_{\mathrm{prim}}(\lambda\rho,1)),$$

où $P_\rho(a,b)$ est l'analogue de $P(a,b)$ obtenu en remplaçant Ψ^{a-b} par $\Psi^{a-b}\times\rho$ (resp. λ par $\lambda\rho$).

Où

$$\varepsilon_\rho(a,b) = \frac{\lambda}{|\lambda|}(\mathfrak{f}_\rho)\times\rho^{-1}(\mathfrak{f}_{k_0})\times(\tau_n/\Omega)^{-bd}\times\rho(Y_n^d)\times\varphi^a\bar{\varphi}^b(\mathfrak{d}_n^d)$$

est un nombre algébrique, unité $\mathfrak{P}$-adique.

Remarques. — (i) L'expression $(\tau_n/\Omega)^{-ad}(\tau_1(\rho,\zeta_1)/p^{n+1})^d$ a pour valuation $\mathfrak{P}$-adique $(n+1)d(a-(1/2))$.

(ii) Le signe de l'équation fonctionnelle de ρ, noté $W(\rho)$ est une racine de l'unité d'ordre d'une puissance de p au signe près, comme me l'a fait remarqué R. Greenberg. En effet, en utilisant la décomposition en facteurs locaux de $W(\rho)$, on constate que cette expression diffère par une racine de l'unité de $\prod_{v\mid p,\ v \text{ places de } F} W(\rho_v)$. Or en une telle place, ρ_v est soit non ramifié, soit sauvagement ramifié parce qu'il est d'ordre une puissance de p, et par le corollaire 1, page 96 de [23], on peut conclure.

(iii) Pour chaque place v de F au-dessus de $\mathfrak{P}$, on a : $\rho(v)=0$ par l'hypothèse que $\rho(\gamma_1)\neq 1$, c'est-à-dire que ρ est ramifié en chaque place v au-dessus de $\mathfrak{P}$. Par contre on n'a pas forcément $\check{\rho}(v)=0$, car il se peut que $\rho(\gamma_2)=1$.

PROPOSITION 3.3.3 *bis.* — *Lorsque* $\rho(\gamma_1)=1$, *l'égalité de la proposition précédente est encore valable en remplaçant par* 1 *les quantités* τ_n/Ω, $\tau_1(\rho, \zeta_1)/p^{n+1}$, $\mathfrak{d}_n$ *et* Y_n.

Preuve. — Il suffit de reprendre tous les calculs en prenant garde que dans la proposition 3.2.2, le facteur relatif à $j_m^{(\mathfrak{P})}$ ne disparaît plus parce que le caractère ξ_1 est trivial. Cette différence introduira les facteurs d'Euler en $v \mid \mathfrak{P}$ dans le résultat final. La conduite des calculs, tout à fait analogue à la précédente n'est pas détaillée.

COMMENTAIRES. — On verra dans l'appendice qu'essentiellement la série $G^{(i_1, i_2)}(T_1, T_2)$ est divisible par la série qui interpole les $P(a, b)$ lorsque $(i_1, i_2)=(1,0)$. En appelant encore $G^{(1,0)}$ le quotient, on a le corollaire fondamental :

COROLLAIRE 3.3.4. — *Pour tout caractère* ρ *d'ordre fini, on a :*

$$\iota_{\mathfrak{P}}^{-1}(\Omega_{\mathfrak{P}}^{-d} G^{(1,0)}(u_1\rho(\gamma_1)-1, \rho(\gamma_2)-1))$$

$$=\iota_\infty^{-1}\left(c_1 \prod_{v \mid \mathfrak{P}}\left(1-\frac{\psi\rho(v)}{Nv}\right)\left(1-\frac{\check{\widehat{\psi}}\rho(v)}{Nv}\right)\right.$$

$$\left.\times \varepsilon_\rho \times (\tau_n/\Omega)^{-d} \times \left(\frac{\tau_1(\rho, \zeta)}{p^{n+1}}\right)^d \times \Omega^{-d} L_{\text{prim}}(\psi\rho, 1)\right),$$

où $\varepsilon_\rho = W(\rho).\varepsilon_p(1,0)$ *est une unité p-adique, algébrique.*

3.4. DÉMONSTRATION DU THÉORÈME CENTRAL LORSQUE $k=0$

Soit n et m deux entiers positifs ou nuls. On se propose de démontrer que le groupe $E(F'_{n,m})$ des points de E rationnels sur $F'_{n,m}$, est de torsion. On va pour cela montrer que $L(\psi_{E/F'_{n,m}}, 1)$ est non nul, ce qui entraîne le résultat par le théorème de N. Arthaud. Soit $\Gamma_{n,m}$ le groupe des caractères complexes de $\Gamma_{n,m}=G(F'_{n,m}/F)$. On a la décomposition :

$$L(\psi_{E/F'_{n,m}}, 1)=\prod_{\rho \in \hat{\Gamma}_{n,m}} L(\psi\rho, 1),$$

où toutes les fonctions L qui interviennent sont primitives. On remarque que chaque facteur du produit ci-dessus, peut être vu après normalisation comme la valeur en $(u_1\rho(\gamma_1)-1, \rho(\gamma_2)-1)$ de la série $G^{(1,0)}$ qui a tous ses coefficients dans I.

On fait alors la remarque évidente mais cruciale :

$$G^{(1,0)}(u_1\,\rho(\gamma_1)-1,\ \rho(\gamma_2)-1)\equiv G^{(1,0)}(u_1-1,\ 0)\bmod(\mathrm{rad}\,I[\mu_{p^\infty}]),$$

ce qui se traduit, en utilisant la formule A.2.3 de l'appendice et le corollaire 3.3.4, par la congruence :

PROPOSITION 3.4.1. — *Pour tout caractère* ρ *d'ordre fini de* Γ :

$$\varepsilon_\rho\,\mathrm{Eul}_p(\psi\rho).(\tau_n/\Omega)^{-d}\left(\frac{\tau_1(\rho,\zeta_1)}{p^{n+1}}\right)^d\Omega^{-d}L(\psi\rho,\ 1)\equiv\mathrm{Eul}_p(\psi)\times\Omega^{-d}\times L(\psi,\ 1)$$

$$\text{modulo}\,(\text{rad.}\,I[\mu_{p^\infty}]),$$

où l'on a identifié les deux membres de la congruence, a priori dans $\iota_\infty(\bar{\mathbb{Q}})$ *avec leur image par* $\iota_{\mathfrak{P}}\circ\iota_\infty^{-1}$.

De cette congruence et des hypothèses sur p, à savoir que $\tau(E/F)$ et p sont étrangers (donc aussi $L(\psi,\ 1)$ et p), et que p est non anormal, ce qui entraîne facilement que $\mathrm{Eul}_p(\psi)$ (donc aussi $\mathrm{Eul}_p(\psi\rho)$) est une unité $\mathfrak{P}$-adique, on déduit que le nombre

$$(\tau_n/\Omega)^{-d}\left(\frac{\tau_1(\rho,\zeta_1)}{p^{n+1}}\right)^d\left(\frac{\Omega}{2i\pi}\right)^{-d}L(\psi\rho,\ 1)$$

est une unité p-adique, et en particulier, n'est pas nul. Ceci a lieu pour chaque caractère ρ de Γ, par conséquent les nombres $L(\psi\rho,\ 1)$ sont tous non nuls.

Remarques 3.4.2. — (i) Soit $\mathfrak{f}_\rho(\mathfrak{P})$ un générateur quelconque de l'idéal $\mathfrak{f}_\rho$. J engendré par le conducteur de ρ dans l'anneau J (l'anneau J est « principal » bien que non intègre) alors, si $a\sim b$ signifie que a/b est une unité de l'anneau $J[\mu_{p^\infty}]$, on a :

$$\mathfrak{f}_\rho(\mathfrak{P})\sim\left((\tau_n/\Omega)^{-1}\times\left(\frac{\tau_1(\rho,\zeta_1)}{p^{n+1}}\right)\right)^2.$$

En effet, on sait que

$$\tau_1(\rho,\zeta_1)\times\tau_1(\bar{\rho},\zeta_1)=\xi_1(-1)p^{n+1}\qquad\text{et}\qquad\tau_1(\bar{\rho},\zeta_1)=\zeta_1(-1)\overline{\tau_1(\rho,\zeta_1)},$$

or $\tau_1(\rho,\zeta_1)\in\underline{\mathbb{Q}(\zeta_{p^{n+1}})}$, qui est totalement ramifiée en p, donc les nombres $\tau_1(\rho,\zeta_1)$ et $\tau_1(\rho,\zeta_1)$ sont associés dans $\mathbb{Q}(\zeta_{p^{n+1}})$ et ont pour valuation p-adique $(n+1)/2$. On en tire que dans $J[\mu_{p^{n+1}}]$, on a :

$$\left|(\tau_n/\Omega)^{-1}.\frac{\tau_1(\rho,\zeta_1)}{p^{n+1}}\right|^2=|\mathfrak{f}_\rho(\mathfrak{P})|.$$

(ii) Par la Führerdiskriminantenproduktsformel, on a l'égalité $D_{F'_{n,m}/F} = \prod_{\rho \in \Gamma_{n,m}} \mathfrak{f}_\rho$. De plus on voit facilement que les $\mathfrak{P}$-parties des idéeaux de K : $D_{F'_{n,m}/K}$ et $N_{F/K}(D_{F'_{n,m}/F})$ sont égales parce que l'extension F/K n'est pas ramifiée en $\mathfrak{P}$. Soit v une place de F au-dessus de $\mathfrak{P}$, alors les v-parties des idéaux de $F(N_{F/K}\mathfrak{f}_\rho)\mathcal{O}_F$ et $\mathfrak{f}_\rho^d$ sont égales. En effet, si l'on note ρ^F et ρ^K les caractères des classes d'idèles de F et K déduits de ρ, on a la formule : $\rho^F = \rho^K \circ N_{F/K}$ parce que $F_{n,m}$ est la composée des extensions disjointes F et $K_{n,m}$. Donc la valuation v-adique du conducteur $\mathfrak{f}_\rho$ de ρ^F au-dessus d'une place $\mathfrak{q}$ de K, non ramifiée dans F/K, ne dépend pas de $v \mid \mathfrak{q}$. Par conséquent, en rassemblant ces observations, on conclut, que si l'on fixe $D_{F'_{n,m}/K}(\mathfrak{P})$ un générateur arbitraire de l'idéal $D_{F'_{n,m}/K}\mathcal{O}_{\mathfrak{P}}$, on a :

$$D_{F'_{n,m}/K}(\mathfrak{P}) \sim \prod_{\rho \in \hat{\Gamma}_{n,m}} \mathfrak{f}_\rho(\mathfrak{P})^d.$$

(iii) On tire des deux remarques précédentes la conclusion que :

$$\sqrt{D_{F'_{n,m}/K}(\mathfrak{P})} \times \left(\frac{\Omega}{2i\pi}\right)^{-[F'_{n,m}:K]} \times L(\psi_{E/F'_{n,m}}, 1)$$

est une unité de J, ce qui donne une formulation plus précise du résultat prouvé ci-dessus. On tire encore de cela, en utilisant la proposition 2.3.2 que le nombre de Tamagawa $\tau(E/F'_{n,m})$ est non nul. Par contre, on ne contrôle plus sa divisibilité par p.

3.4. Démonstration du point 2 du théorème central

Notation 3.4.1. — Soit K_∞^+ la $\mathbb{Z}_p$-extension cyclotomique de K, K_n^+ le n-ième corps intermédiaire de K_∞^+/K, et K_∞^- la $\mathbb{Z}_p$-extension anticyclotomique, c'est-à-dire dihédrale sur $\mathbb{Q}$, et K_m^- le m-ième corps intermédiaire de K_∞^- sur K. On note $F_n^+ = FK_n^+$, $F_\infty^+ = FK_\infty^+$, $F_m^- = FK_m^-$ et $F_\infty^- = FK_\infty^-$. Notons $F'_{\infty,\infty} = \bigcup_{n,m} F'_{n,m}$ le composé de F et de la $\mathbb{Z}_p^2$-extension de K.

Considérons la série $G = G^{(1,0)}$ construite dans l'appendice et supposons pour simplifier qu'on a choisi les générateurs topologiques u_1 et u_2 de $1 + p\mathbb{Z}_p$ égaux à un même u. On effectue alors le changement de variables (« changement d'axes » faisant passer du repère constitué des $\mathbb{Z}_p$-extensions $\mathfrak{P}$-ramifiée et $\mathfrak{P}^*$-ramifiée aux $\mathbb{Z}_p$-extensions cyclotomique et anticyclotomique)

$$S = T_1 + T_2 + T_1 T_2, \quad T = \frac{1+T_1}{1+T_2} - 1$$

et posons

$$\mathcal{G}(S, T)=G(T_1, T_2).$$

Introduisons le diviseur critique de Greenberg $\Theta=1+S-u$, et supposons que l'on ait : $\mathcal{G}(S, T)=\Theta^k\times(\text{unité})$. On se propose de démontrer sous cette hypothèse, en désignant encore par p un nombre premier différent de 2 et 3 non ramifié dans F et de bonne réduction ordinaire, que les groupes $E(F_\infty^-)$ et $E(F'_{\infty,\infty})$ ne diffèrent que par une partie de torsion. On va utiliser pour cela le théorème de Rubin que nous rappelons :

THÉORÈME 3.4.2. — *Soit E/F une courbe elliptique satisfaisant l'hypothèse (S), M/F une extension abélienne finie et soit ρ un caractère de M/F. Si le nombre $L(\psi\rho, 1)$ n'est pas nul, alors le groupe $(E(M)\otimes\mathbb{C})^{(\rho^{-1})}$ est trivial.*

Soit alors m et n deux entiers $\geqq 0$, on a la décomposition

$$E(F_m^- F_n^+)\otimes\mathbb{C}=E(F_m^-)\otimes\mathbb{C}\oplus(\oplus_{\rho\neq 1}(E(F_m^- F_n^+)\otimes\mathbb{C})^{(\rho)}),$$

où le caractère ρ parcourt l'ensemble des caractères non triviaux de F_n^+ sur F, ou de $F_m^- F_n^+$ sur F_m^- ce qui est équivalent, puisque F_m^- et F_n^+ sont disjoints sur F. Remarquons alors que F et K_∞^- sont abéliens sur K et que $F_m^-(E_{\text{tors}})$ coïncide avec $F(E_{\text{tors}})$, par conséquent la courbe E/F_m^- satisfait l'hypothèse (S). Il suffit donc de montrer que pour chaque caractère ρ de $F_m^- F_n^+$ sur F_m^- non trivial, on a $L(\psi_{E/F_m}\times\rho, 1)\neq 0$. Fixons un prolongement de ρ à $G(F_m^- F_n^+/K)$ encore noté ρ. En appliquant la formule du corollaire 3.3.4, on est ramené à montrer que

$$G(u.\rho(\gamma_1)-1, \rho(\gamma_2)-1)\neq 0.$$

C'est-à-dire, que

$$\mathcal{G}\left(u.\rho(\gamma_1\gamma_2)-1, u.\rho\left(\frac{\gamma_1}{\gamma_2}\right)-1\right)\neq 0.$$

Or, par hypothèse, cette quantité diffère d'une unité p-adique par le facteur $u.(\rho(\gamma_1\gamma_2)-1)$. On remarque alors que $\gamma_1\gamma_2$ est un générateur topologique de $G(F'_{\infty,\infty}/F_\infty^-)$. En effet, soit $\mathbb{N}_p$ le caractère de Γ à valeurs dans $\mathbb{Z}_p^\times$ déduit de la norme des idéaux de F par le procédé de Weil (*cf.* [26]). Ce caractère se factorise à travers le groupe $G(F_\infty^+/F)$, et fournit un isomorphisme de ce groupe avec $1+p\mathbb{Z}_p$. Or, F_∞^+ et F_∞^- sont disjoints sur F et $\mathbb{N}_p(\gamma_1\gamma_2)=u^2$ est un générateur de $1+p\mathbb{Z}_p$, donc $\gamma_1\gamma_2$ est un

générateur de $G(F_\infty^+/F) \approx G(F'_{\infty,\infty}/F_\infty^-)$. Ainsi, pour tout caractère ρ non trivial, on a : $\rho(\gamma_1\gamma_2) \neq 1$ et on en déduit $(E(F_m^- F_n^+) \otimes \mathbb{C})^{(\rho)} = 0$. On a alors le petit lemme évident.

LEMME 3.4.2. — *Soit G un groupe abélien fini d'exposant g, et M un G-module qui est un $\mathbb{Z}$-module sans torsion, alors si $M \otimes \mathbb{Q}(\zeta_g) = M^G \otimes \mathbb{Q}(\zeta_g)$ on a $M = M^G$.*

Preuve. — Soit $x \in M$, il y a $\lambda \in \mathbb{Z}[\zeta_g]$ tel que $\lambda x \in M^G \otimes \mathbb{Z}[\zeta_g]$ (l'action de G sur $\mathbb{Q}(\zeta_g)$ est supposée triviale) alors pour tout σ de G on a : $(\lambda x)^\sigma = \lambda x$; donc $\lambda.(x^\sigma - x) = 0$ et comme M est sans $\mathbb{Z}$-torsion, et que $\mathbb{Z}[\zeta_g]/\mathbb{Z}$ est libre, on a $x^\sigma = x$ pour tout σ de G, ainsi $x \in M^G$.

On l'applique au groupe $G = G(F_m^- F_n^+/F_m^-)$, au module : $E(F_m^- F_n^+)$ modulo torsion, et on conclut que les groupes $E(F_m^- F_n^+)$ et $E(F_m^-)$ coïncident modulo torsion. En passant alors à la limite inductive en n et m, on trouve que les groupes $E(F'_{\infty,\infty})/\Omega'_{\infty,\infty}$ et $E(F_\infty^-)/\Omega_\infty^-$ sont égaux, où l'on a noté $\Omega'_{\infty,\infty}$ (resp. Ω_∞^-) les groupes de torsion de $E(F'_{\infty,\infty})$ (resp. de $E(F_\infty^-)$). C'est le point 2 du théorème central.

COMMENTAIRES. — (i) Lorsque la courbe E est définie sur $\mathbb{Q}$ (et que $F = K$) et que le signe de l'équation fonctionnelle de la fonction L de Hasse-Weil $L(E/\mathbb{Q}, s)$ est égal à -1, les résultats récents de Gross-Zagier joints à la généralisation par Rohrlich du théorème de Greenberg [10], impliquent que $E(K_\infty^-)$ n'est pas de type fini.

(ii) R. Greenberg a remarqué, en supposant vraie la conjecture principale, que Θ^2 ne divise pas la série $G^{(1,0)}$, ce qui limite l'énoncé du théorème aux valeurs 0 et 1 de l'entier k.

On a encore la conséquence suivante du corollaire 3.3.4, qui est le point 3 du théorème central.

PROPOSITION 3.4.2. — *Supposons encore que $\mathcal{G}(S, T)$ ne diffère du diviseur de Greenberg Θ que par une unité dans l'algèbre $I[[S, T]]$, alors pour toute $\mathbb{Z}_p$-extension L de F contenue dans $F'_{\alpha,\alpha}$ et distincte de F_α^-, le rang du groupe $E(L)$ modulo torsion est fini.*

Preuve. — Si la conclusion était fausse, alors par le théorème de Rubin, il y aurait une infinité de caractères de L/F tels que $L(\psi\rho, 1) = 0$. Soit L_{n_0} un corps intermédiaire de L/K admettant un caractère non trivial ρ avec $L(\psi\rho, 1) = 0$, et non contenu dans F_∞^-, ce qui est possible pour n_0 assez grand puisque $L \neq F_\alpha^-$. Soient alors m et n deux entiers positifs tels que $F_m^- F_n^+ \supset L_{n_0}$. On a $F_m^+ F_m^- L_{n_0}$ donc le caractère $\rho_{F_m^-}$ de $F_m^- F_n^+/F_m^-$, défini

par $\rho_{F_m^-}(\sigma)=\rho(\sigma|_{L_{n_0}})$ est non trivial, et l'on a : $L(\psi_{E/F_m^-}\rho_{F_m^-}, 1)=0$, puisque dans la factorisation du membre de gauche apparaît $L(\psi\rho, 1)$ qui est nul. Mais ceci contredit le fait que $L(\psi_{E/F_m^-}\rho_{F_m^-}, 1)$ diffère par une unité de $\rho(\gamma_1\gamma_2)-1$, qui est non nul.

APPENDICE

Bien que l'on ne sache pas en général se débarrasser du facteur parasite $P(a, b)$ du théorème 2.11.4, on se propose ici de montrer comment modifier légèrement la construction du chapitre 2 pour obtenir une série $G^{(1,0)}$ dont la valeur en (u_1^a-1, u_2^b-1) pour un couple admissible (a, b) congru à (1,0) modulo M (multiple de $p-1$ premier à p, fixé ci-dessous) est donnée par le membre de droite de 2.11.4 (ii) où le facteur parasite $P(a, b)$ est remplacé par $p^r\mathfrak{P}^{bd}$. On devra supposer pour mener à bien cette construction que p ne divise pas le degré d de F sur K.

1. Restriction des scalaires et descente de la courbe

On reprend les notations du chapitre 2, paragraphe 1. Soit f_i l'idéal de $\mathcal{O}$ conducteur du caractère de Serre-Tate Φ_i attaché à la variété abélienne B_i/K $(i=1, \ldots, r)$. Soit $\mathcal{R}_{f_i}$ le corps des rayons modulo f_i et $F_i=\mathcal{R}_{f_i}\cap F$.

PROPOSITION A.11. — (i) *Le conducteur de F_i/K est un diviseur de f_i, qui en diffère au plus aux places divisant 2 ou 3.*

(ii) *La courbe elliptique E/F a un modèle E_i/F_i, isomorphe à E sur F, déterminé à isomorphisme F_i-rationnel près par son caractère de Serre-Tate $\Psi_{E_i/F_i}=\Phi_i\circ N_{F_i/K}$.*

Preuve. — Prouvons d'abord le point (ii). On rappelle que pour toute extension L/K finie abélienne du corps quadratique imaginaire K, contenant le corps de Hilbert $\mathcal{R}_{(1)}$ de K, étant donnés une valeur j de l'invariant modulaire sur une classe d'idéaux de K et un caractère de Hecke algébrique $\chi : J_L\to K^\times$, qui coïncide avec $N_{L/K}$ sur $L^\times$, il existe une courbe elliptique E/L telle que $j(E)=j$ et $\Psi_{E/L}=\chi$, en désignant par $\Psi_{E/L}$ le caractère de Serre-Tate de E/L. La démonstration de ce résultat dû à Shimura [20] est donnée dans le livre de GRÖSS ([11], théorème 9.1.3) et se transpose sans difficulté au cas ci-dessus. On considère alors le caractère de Hecke

algébrique $\Psi_i = \Phi_i \circ N_{F_i/K}$ qui vaut la norme sur $F_i^\times$. Vérifions qu'il applique J_{F_i} dans $K^\times$. Soit F_i' le sous-corps de F attaché par la théorie du corps de classes au groupe des idèles de K envoyées par Φ_i dans $K^\times$, qui est ouvert et contient $K^\times$. On a clairement $\Phi_i \circ N_{F_i'/K}(J_{F_i'}) \subset K^\times$. On a l'inclusion $F_i' \subset \mathscr{R}_{f_i}$, parce que $\mathrm{Ker}\,\Phi_i \supset W_{f_i}$ (groupe des idèles congrues à 1 modulo f_i) et donc $F_i' \subset F_i$. Comme il est, de plus, clair que $\mathscr{R}_{(1)} \subset F_i$, on conclut en appliquant la proposition rappelée ci-dessus. Pour le point (i), considérons $\mathfrak{q}$ un idéal premier de $\mathcal{O}$ ne divisant ni 2 ni 3. Soit $x \in J_K$ une idèle telle que $x_w = 1$ pour tout $w \neq \mathfrak{q}$, et telle que $x_\mathfrak{q} \equiv 1 \bmod [f_i'(\mathfrak{q})]$ où $f_i'(\mathfrak{q})$ désigne la $\mathfrak{q}$-composante du conducteur du groupe d'idèles $\Phi_i^{-1}(K^\times)$. On a donc $\Phi_i(x) \in K^\times$ et il existe $\alpha \in K^\times$ tel que $\alpha \in \mathrm{Ker}\,\Phi_i$. Or, si q est le nombre premier que divise $\mathfrak{q}$, il y a un entier $f > 0$ tel que $x_\mathfrak{q}^{q^f} \equiv 1 \,(\mathrm{mod}\, f_i(\mathfrak{q}))$ — ici $f_i(\mathfrak{q})$ désigne la $\mathfrak{q}$-partie du conducteur f_i de Φ_i. — On en déduit que $\alpha^{q^f} = 1$, or $K^\times \cap \mu_{q^\infty} = \{1\}$, donc $\alpha = 1$. C'est-à-dire que $f_i(\mathfrak{q}) \mid f_i'(\mathfrak{q})$ comme la divisibilité inverse est évidente, on a l'égalité souhaitée.

Remarque A.1.2. — La variété abélienne $\mathrm{Res}_K^{F_i}(E_i)$ est K-isogène à un produit $\prod B_j$ étendu à une partie J de $\{1, \ldots, r\}$ qui contient i, mais n'est pas K-simple en général comme le prouve une contre-exemple de D. Rohrlich (lettre à N. Schappacher). Cependant les conducteurs f_j des caractères de Serre-Tate des variétés abéliennes B_j qui interviennent dans $\mathrm{Rés}_K^{F_i}(E_i)$ sont des diviseurs de f_i à cause de la formule :

$$P.P.C.M.\,(\mathrm{Cond}\,(F_i/K), f_i) = f_i = P.P.C.M._{j \in J}(f_j)$$

(prouvée à la proposition 2.2.1).

2. Construction de la série $G^{(1,0)}$ « *primitive* »

On fixe pour l'instant un entier i entre 1 et 2. Soit (E_i, ω_i) un modèle E_i sur F_i, il existe $c_i \in F^\times$ tel que $\omega_i = c_i \omega$ et donc on peut choisir comme base du réseau $\mathscr{L}_i = c_i \mathscr{L}$, le nombre $\Omega_i = c_i \Omega$ (on suppose bien sûr que les modèles considérés ont bonne réduction en p, donc c_i est une unité p-adique). On choisit un idéal $\mathfrak{g}_i = (g_i)$ multiple principal de f_i, ayant le même support. On recommence la construction du chapitre 2, paragraphe 7 en remplaçant E/F et $\mathfrak{g}$ par E_i/F_i et $\mathfrak{g}_i$. Notons que la courbe E_i/F_i satisfait l'hypothèse (S). On obtient des fonctions $\theta_{i,m}$ sur le groupe formel $\hat{E}_i$ de

E_i, qui vérifient les formules de la proposition 2.7.1 et on construit la série $j_i(t, \omega_2)$ de la proposition 2.8.3 par le même procédé. D'où une mesure $\mu_i = \mu_{i,\mathfrak{a},c}$ sur $G_i = G(F_i(E_{i,p^\infty})/F_i)$ qui est isomorphe à G par restriction puisque F et $F_i(E_{i,p^\infty})$ sont disjoints sur F_i (p est non ramifié dans F). Cette mesure vérifie la formule suivante. On note encore $\psi_{\mathfrak{P}}$ et $\bar{\psi}_{\mathfrak{P}}$ les caractères déduits de ψ_{E_i/F_i} à la Weil, ce qui est légitime après l'identification $G_i \approx G$.

Soit $\sigma \in G(F_i/K)$ et φ un Grössencharakter de K déduit de Φ_i. Pour tout couple admissible (a, b) congru à $(1,0)$ modulo $p-1$, posons

$$\mathscr{L}_{\varphi,\,\text{prim.}}(a, b) = (a-1)!\left(\frac{2i\pi}{\sqrt{D_K}}\right)^{-b} \times \Omega^{-(a-b)} L_{\text{prim.}} L(\bar{\varphi}^{a-b}, \sigma, a)$$

où

$$L_{\text{prim.}}(\bar{\varphi}^{a-b}, \sigma, s) = \sum_{\mathfrak{a}} \frac{\bar{\varphi}^{a-b}(\mathfrak{a})}{N\mathfrak{a}^s},$$

la somme étant étendue aux idéaux $\mathfrak{a}$ de $\mathcal{O}$, premiers à $f_i\mathfrak{P}^*$ et tels que l'on ait : $(\mathfrak{a}, F_i/K) = \sigma$. Notons $\Omega_{\mathfrak{P}}$ la période $\mathfrak{P}$-adique introduite dans la proposition 2.10.7 (noter que, pas plus que pour la période complexe servant à définir $\mathscr{L}_{\varphi,\,\text{prim}}$, cette période ne dépend pas de (i)).

PROPOSITION A.2.1. — *Pour $(a, b) \equiv (1, 0) \bmod (p-1)$, (a, b) étant admissible, on a*

$$\Omega_{\mathfrak{P}}^{-(a-b)} \int_G \psi_{\mathfrak{P}}^a \bar{\psi}_{\mathfrak{P}}^b \frac{d\mu_i}{\psi_{\mathfrak{P}}} = 12(-1)^a g_i^a p^r \mathfrak{P}^b \varphi^a \bar{\varphi}^b(\mathfrak{c})$$

$$\times (\Delta_{\mathfrak{a}} \mathscr{L}_{\varphi,\,\text{prim.}}(a, b, \sigma_{\mathfrak{c}}) - \frac{\varphi^a \bar{\varphi}^b(\mathfrak{P})}{N\mathfrak{P}} \Delta_{\mathfrak{a}} \mathscr{L}_{\varphi,\,\text{prim.}}(a, b, \sigma_{\mathfrak{c}\mathfrak{P}})).$$

Preuve. — Remarquons que la suite de terme général

$$-\bar{g}_i \pi^{m+1} E_1\left(\frac{\Omega_i}{g_i \bar{\pi}^{m+1}}, \mathscr{L}_i\right)$$

converge vers $c_i^{-1} \gamma_{\mathfrak{P}}$. On le voit en montrant par le raisonnement de la proposition 2.10.7 que $\gamma_{\mathfrak{P},\mathfrak{g}_i} = \gamma_{\mathfrak{P}}$ pour tout idéal $\mathfrak{g}_i$ différent de 1. Ensuite le calcul de l'intégrale est exactement identique au cas de la proposition 2.11.1. Il apparaît des nombres $\Lambda_i(\mathfrak{c})$ possédant les mêmes vertus que les $\Lambda(\mathfrak{c})$ et qui ne figurent pas dans le résultat final. Lors de la

transformation des nombres d'Eisenstein en valeurs de fonctions L partielles, on obtient des expressions du type $L(\bar{\varphi}^{a-b}, \sigma, a)$ où $\sigma \in G(\mathscr{R}_{i,m}/K)$, en désignant, pour tout $m \geqslant 0$, par $\mathscr{R}_{i,m}$ le corps des rayons de K de conducteur $g_i \bar{\pi}^{m+1}$; mais par la remarque A.1.2, ce corps coïncide avec le corps engendré sur F_i par les points de $g_i \bar{\pi}^{m+1}$-torsion de E_i. C'est pourquoi, après avoir pris la trace sur F_i on obtient les nombres $\mathscr{L}_{\varphi, \text{prim.}}(a, b, \sigma)$. Enfin, par homogénéité, les c_i disparaissent dans les deux membres puisque $\Omega_i = c_i \Omega$ et $\Omega_{\mathfrak{P}, i} = c_i \Omega_{\mathfrak{P}}$.

Pour chaque entier i entre 1 et r, on note $\mathscr{P}_i$ l'ensemble des iéaux principaux de $\mathcal{O}$ de la forme $\mathfrak{a} = (\alpha)$ avec $\alpha \equiv 1 \bmod \mathfrak{g}_i$, et $\mathscr{F}_i$ l'ensemble des familles $= (n_\mathfrak{a})_\mathfrak{a} \in \mathscr{P}_i$ d'éléments de $\mathbb{Z}$ presque tous nuls, telles que $\sum_\mathfrak{a} n_\mathfrak{a}(N\mathfrak{a} - 1) = 0$.

Pour une telle famille n, on pose :

$$I_{(i, \underline{n}, \mathfrak{c})}(a, b) = \sum_{\mathfrak{a} \in \mathscr{P}_i} n_\mathfrak{a} \int_G \psi_\mathfrak{P}^a \bar{\psi}_\mathfrak{P}^b \frac{d\mu_{i, \mathfrak{a}, \mathfrak{c}}}{\psi_\mathfrak{P}}.$$

Considérons alors la fonction f suivante :

$$(a, b) \mapsto \prod_{i=1}^r \prod_{\varphi \sim B_i} \{ \sum_{\mathfrak{c} \sim F_i/K} (\varphi^a \bar{\varphi}^b)^{-1}(\mathfrak{c}) I_{(i, \underline{b}, \mathfrak{c})}(a, b) \},$$

où $\varphi \sim B_i$ signifie que φ parcourt l'ensemble des Grössencharaktere déduits de Φ_i, et $\mathfrak{c} \sim F_i/K$ signifie que $\mathfrak{c}$ parcourt un ensemble d'idéaux de $\mathcal{O}$ premiers à f_i, dont les symboles d'Artin relatifs à F_i/K décrivent exactement $G(F_i/K)$. Rappelons que l'on désigne par d le degré de F sur K. On est conduit, pour interpoler p-adiquement la fonction f, à introduire l'hypothèse que p ne divise pas d. Supposons-la désormais satisfaite.

Soit T_i' la clôture galoisienne de T_i, et $I \otimes_\mathcal{O} T_i'$ le module galoisien sous l'action de $\mathrm{Aut}(\mathbb{C})$, défini par $\sigma(i \otimes t') = i \otimes \sigma(t')$ pour $\sigma \in \mathrm{Aut}(\mathbb{C})$, $i \in I$, $t' \in T_i'$. Notons ω_i' (resp. $\langle \, . \, \rangle_i$) la projection de $(I \otimes_\mathcal{O} T_i')^\times$ sur son sous-groupe μ_i de torsion d'ordre premier à p (resp. sur son pro-p-sous-groupe de Sylow). Soit $m_i = \# \mu_i$ et soit $m = ppcm_{i=1, \ldots, r}(m_i)$, c'est un entier premier à p et divisible par $p - 1$.

PROPOSITION A.2.2. — *Si $p \mid d$, il existe une série $G^*(T_1, T_2)$ à coefficients dans I telle que pour tout couple admissible (a, b) congru à $(1, 0)$ modulo m, on ait*

$$G^*(u_1^a - 1, u_2^b - 1) = f(a, b).$$

Preuve. — L'obstruction à l'interpolation de la fonction f provient des termes $\varphi^a \bar{\varphi}^b(c)$. Or si $(a, b) \equiv (1, 0)$ modulo m, et si φ est un Grössencharakter de B_i/K, on a :

$$\varphi^a \bar{\varphi}^b(c) = \omega_i'(\varphi(c)) . \langle \psi^a \bar{\psi}^b(c\mathcal{O}_F) \rangle_i^{1/d}$$

et la fonction $(a, b) \mapsto \langle \psi^a \bar{\psi}^b(c\mathcal{O}_F) \rangle$ est une fonction d'Iwasawa provenant de la série :

$$(1+T_1)^{l_1 (\psi(c\mathcal{O}_F))/d} \times (1+T_2)^{l_2 (\bar{\psi}(c\mathcal{O}_F))^d}.$$

En outre, pour chaque i fixé, la série à deux variables qui interpole

$$(a, b) \mapsto \prod_{\varphi \sim B_i} \left(\sum_{c \sim F_i/K} \omega_i'(\varphi(c))^{-1} \times \langle \psi^a \bar{\psi}^b(c\mathcal{O}_F) \rangle^{1/d} \times I_{(i, n, c)}(a, b) \right),$$

a ses coefficients dans I parce qu'on sait que les Grössencharaktere associés à une composante simple fixée B_i/K forment un espace homogène sous l'action de $\mathrm{Aut}(\mathbb{C})$, donc les éléments $\omega_i'(\varphi(c))$ sont conjugués sous $\mathrm{Aut}(\mathbb{C})$.

Supposons de plus que l'on se limite aux couples admissibles (a, b) congrus à $(1, 0)$ modulo *m.d.*, alors, en développant $f(a, b)$, on trouve une expression analogue à la formule (ii) de la proposition 2.11.2, mais où la fonction L qui intervient est primitive, à cause de l'égalité :

$$\prod_{i=1}^{r} \prod_{\varphi \sim B_i} L_{\mathrm{prim}}(\bar{\varphi}^{a-b}, a) = L_{\mathrm{prim}}(\bar{\psi}^{a-b}, a),$$

qui résulte de la relation $a - b \equiv 1 \ (d)$ et de la formule bien connue

$$\Pi_{\chi \in \hat{H}} L_{\mathrm{prim}}(\bar{\varphi}^{a-b}\chi, a) = L_{\mathrm{prim}}(\bar{\psi}^{a-b}, a).$$

On procède ensuite exactement comme au paragraphe 11 pour construire la série $G^{(1,0)}$ satisfaisant l'analogue de la formule (ii) du théorème 2.11.4 sans le terme parasite $P(a, b)$.

Remarque. — Notons $M = m.d.$ La formule d'interpolation pour $G^{(1,0)}$ n'est valable que si $(a, b) \equiv (1,0) \bmod M$, (et en supposant $p \nmid d$). Cependant pour l'application qu'on avait en vue, c'est-à-dire la formule 3.3.4, on a l'analogue du lemme 3.3.1.

LEMME A.2.3. — *Pour tout caractère* ρ *d'ordre fini de* Γ, *on a*

$$G^*(u_1 \rho(\gamma_1) - 1, \rho(\gamma_2) - 1) = \prod_{i=1}^{r} \prod_{\varphi \sim B_i} \Big\{ \sum_{c \sim F_i/K} \tilde{\rho}^{-1}((c, F'_{i, n, m}/K)) \times \varphi^{-1}(c) \times \int_G \rho(\sigma) \, d\mu_{i, a, c}(\sigma) \Big\},$$

où $\tilde{\rho}$ *est le prolongement de* ρ *à* $G(F'_{i,n,m}/K)$ *défini par :*

$$\tilde{\rho}((\mathfrak{c}, F'_{i,n,m}/K)) = \rho((\mathfrak{c}\mathcal{O}_F, F'_{i,n,m}/F_i))^{1/d}.$$

Preuve. — En substituant à (T_1, T_2) le couple $(u_1\rho(\gamma_1)-1, \rho(\gamma_2)-1)$ on fait apparaître la quantité $\rho_{\mathfrak{P}}^{1/d}(\gamma_1^{l_1(\psi(\mathfrak{c}\mathcal{O}_F))}\gamma_2^{l_2(\bar{\psi}(\mathfrak{c}\mathcal{O}_F))})$. Or, par définition même de $\psi_{\mathfrak{P}}$, on a l'égalité :

$$\psi_{\mathfrak{P}}((\mathfrak{A}, \mathscr{F}'_n/F)) = \psi(\mathfrak{A})$$

pour tout idéal $\mathfrak{A}$ de $\mathcal{O}_F$ premier au conducteur de ψ et à p, par conséquent,

$$\rho(\gamma_1^{l_1(\psi(\mathfrak{c}\mathcal{O}_F))}\gamma_2^{l_2(\bar{\psi}(\mathfrak{c}\mathcal{O}_F))}) = \rho((\mathfrak{c}, F'_{n,m}/F)).$$

On peut aussi descendre à F_i, par l'isomorphisme de restriction :

$$G(F'_{n,m}/F) \xrightarrow{\sim} G(F'_{i,n,m}/F_i).$$

Ces remarques achèvent de justifier le corollaire 3.3.4.

BIBLIOGRAPHIE

[1] BERNARDI (D.). — Hauteur p-adique sur les courbes elliptiques, in *Sém. de Théorie des Nombres*, 79-80, Birkhaüser.

[2] BERNARDI (D.), GOLDSTEIN et STEPHENS (N.). — Notes p-adiques sur les courbes elliptiques, à paraître in *J. de Crelle*.

[3] COATES (J.). — *Cours polycopié H. Weyl lectures*, Princeton, 1979.

[4] COATES (J. and WILES (A.). — On the conjecture of Birch and Swinnerton-Dyer (*inv. Math.*, vol. 39, 1977, p. 223-251).

[5] COATES (J.) and WILES (A.). — On p-adic L functions and elliptic units (*J. of the Austral. Math. Soc.*, vol. 26, 1978, p. 1-25).

[6] DE SHALIT (E.). — *Thesis*, Princeton, 1983.

[7] DE SHALIT (E.) et YAGER (R.). — Article à paraître.

[8] DEURING (M.). — Die Zetafunktion einer algebräischen Kurve vom Geschlechte Eins (*Nachr. Akad. Wiss. Gött.*, 1953, p. 85-94).

[9] GOLDSTEIN (C.) et SCHAPPACHER (N.). — Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe (*J. de Crelle*, vol. 327, 1981, p. 184-218).

[10] GREENBERG (R.). — On the conjecture of Birch and Swinnerton-Dyer (*Inv. Math.*, vol. 72, 1983, p. 241-265.

[11] GROSS (B.). — Arithmetic on elliptic curves with complex multiplication (*Lect. Notes n° 776*, Springer, 1980).

[12] KATZ (N.). — p-adic interpolation of real analytic Eisenstein series (*Ann. of Math.*, vol. 104, 1976, p. 459-571).

[13] KATZ (N.). – p-adic L functions via moduli of elliptic curves, in *Proc. of Symp. in Pure Math.*, Arcata, A.M.S., 1975.

[14] LUBIN (J.). – One parameter formal Lie groups over $\mathfrak{P}$-adic integer rings (*Ann. of Math.*, vol. 80, 1964, p. 464-484).

[15] LUBIN (J.) and TATE (J.). – On formal groups with formal complex multiplication in local fields (*Ann. of Math.*, vol. 81, 1965, p. 380-387).

[16] PERRIN-RIOU (B.). – Groupe de Selmer d'une courbe elliptique à multiplication complexe (*Comp. Math.*, vol. 43, 1981, p. 387-417).

[17] RUBIN (K.). – Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer (*Inv. Math.*, vol. 64, 1981, p. 455-470).

[18] SERRE J.-P. and TATE (J.). – Good reduction of abelian varieties (*Ann. of Math.*, vol. 88, 1968, p. 492-517).

[19] SHIMURA (G.). – *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten Publ., 1971.

[20] SHIMURA (G.). – On the zeta function of an abelian variety with complex multiplication (*Ann. of Math.*, vol. 94, 1971, p. 504-533).

[21] SHIMURA (G.) and TANIYAMA (Y.). – *Complex multiplication of abelian varieties and its application to number theory*, Pub. of Math. Soc. of Japan, 1951.

[22] SOUTO-MEÑENDEZ (J.-M.). – On the extensions of local fields generated by torsion points of some formal groups (*J. of Algebra*, vol. 81, 1983, p. 58-69).

[23] TATE (J.). – Local constants, in *Algebraic number fields*, A. FRÖHLICH éd., Academic Press, 1980.

[24] TATE (J.). – Algorithm for determining the type of a singular fiber in an elliptic pencil, in *Modular functions of one variable*, IV (*Lect. Notes* n° 476, Springer, 1970).

[25] TATE (J.). – On p-divisible groups, in *Proceed. of the conf. in Driebergen*, Springer, 1966.

[26] WEIL (A.). – On a certain type of characters of the idele-class group of an algebraic number field, in *uvres Scientifiques*, 1955*c*, tome 2, Springer, 1978.

[27] WEIL (A.). – *Elliptic functions according to Kronecker and Eisenstein*, Erg. der Math. Wiss. n° 88, Springer, 1976.

[28] WEIL (A.). – *Adeles and algebraic groups*, Birkhäuser, 1980.

[29] YAGER (R.). – On p-adic L functions with two variables (*Ann. of Math.*, vol. 115, 1982, p. 411-449).

[30] YAGER (R.). – p-adic measures on Galois groups (*Inv. Math.*, vol. 76, 1984, p. 331-343).

[31] MANIN (Y.) and VISHIK (M.). – p-adic Hecke series for imaginary quadratic fields (*Math. Sbornik*, vol. 95, 1974, p. 357-383).