SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

ROLAND GILLARD

Unités elliptiques et fonctions L p-adiques

Séminaire de théorie des nombres de Grenoble, tome 8 (1979-1980), exp. n° 1, p. 1-18

<http://www.numdam.org/item?id=STNG_1979-1980__8__A1_0>

Séminaire de Théorie des Nombres
11, 18 et 25 octobre 1979
Grenoble

UNITES ELLIPTIQUES ET FONCTIONS L $\mathfrak{p}$-ADIQUES

par

Roland GILLARD

Le but de cette rédaction est de construire des fonctions L $\mathfrak{p}$-adiques, dans le cas elliptique de hauteur 1, débarrassées de tout facteur parasite. L'exposé oral résumait [5]. Ici, on supprime une hypothèse restrictive peu naturelle de cet article en choisissant pour chaque caractère une courbe elliptique convenable (cf. §1.5). Ceci permet, sous des hypothèses assez faibles, d'obtenir l'analogue de résultats arithmétiques classiques dans le cas cyclotomique. Pour le détail des démonstrations, on renvoie à [5].

1. - CONSTRUCTION DE FONCTIONS L $\mathfrak{p}$-ADIQUES

1.1. NOTATIONS.

Soient K un corps quadratique imaginaire et p un nombre premier $\neq 2$ ou 3 se décomposant en deux facteurs distincts $\mathfrak{p}$ et $\mathfrak{p}'$ dans K. On identifie les nombres algébriques dans $\mathbb{C}$ et $\overline{\mathbb{Q}}_p$ via des inclusions $\overline{\mathbb{Q}} \subset \mathbb{C}$ et $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ fixées dans la suite : ceci définit un prolongement v à $\overline{\mathbb{Q}}$ de la valuation $\mathfrak{p}$-adique de K. Pour toute extension L de K ou de $\mathbb{Q}_p$, on note $\mathcal{O}(L)$ l'anneau des entiers de L et $\mathcal{O}(L)^*$ le groupe de ses unités ; dans le premier cas, on note L^v le complété de L pour la valuation v. et, si $[L:K]$ est fini, $h(L)$ le nombre de classes de L. Ainsi $\mathcal{O}(L^v)^*$ est identifié à $\mathbb{Z}_p^*$. Si $a \in \mathbb{Z}_p^*$, on le décompose en $\omega(a)$ racine de 1 et $\langle a \rangle$ dans le groupe multipli-

catif $1+p\mathbb{Z}_p$.

Pour $\mathfrak{g}$ idéal entier de K , on note $H_{\mathfrak{g}}$ (resp. $Cl(\mathfrak{g})$) le corps (resp. le groupe) des classes de rayon modulo $\mathfrak{g}$ de K ; on désigne par $e(\mathfrak{g})$ le nombre de racines de 1 dans K congrues à 1 modulo $\mathfrak{g}$ et par g le plus petit entier rationnel > 0 dans $\mathfrak{g}$. On pose $e = e((1))$. Soit I le monoïde des idéaux entiers de K . On fixe une application ρ (resp. $\mathfrak{h}$) de I dans K (resp. dans I), avec $\rho(\mathfrak{g})\cdot\mathfrak{g} = \mathfrak{h}(\mathfrak{g})$ et $\mathfrak{h}(\mathfrak{g})$ premier à $\mathfrak{g}$. On suppose ρ faiblement additive, i.e. on suppose que

$$\rho(\mathfrak{g}_1\cdot\mathfrak{g}_2) = \rho(\mathfrak{g}_1)+\rho(\mathfrak{g}_2)$$

pour $\mathfrak{g}_1$ et $\mathfrak{g}_2$ premiers entre eux.

Soit ν un caractère (de dimension 1) $\neq 1$ de $Cl(\mathfrak{g})$ à valeurs dans $\overline{\mathbb{Q}}^*$. La fonction L qui lui est associée est prolongeable à $\mathbb{C}$ et on a (cf. par exemple [8] chap. 21, théorème 3 et chap. 22, théorème 2) si ν est primitif :

$$L(1,\nu) = -2\pi(6\sqrt{d}\,T(\nu)\,g e(\mathfrak{g}))^{-1} \sum_{C\in Cl(\mathfrak{g})} \nu(C)^{-1}\log|\varphi_{\mathfrak{g}}(C)| \quad , \qquad (1)$$

où $T(\nu)$ désigne la somme de Gauss attachée à ν . La définition de l'invariant $\varphi_{\mathfrak{g}}(C)$ de Siegel-Ramachandra est rappelée ci-dessous. Cette formule est le point de départ pour les formules du nombre des classes (cf. infra (9)). Les fonctions L $\mathfrak{p}$-adiques devront vérifier une formule analogue.

1.2. UNITES ELLIPTIQUES.

1.2.1. Cas $\mathfrak{g} \neq 1$. Pour $L = w_1\mathbb{Z}\oplus w_2\mathbb{Z}$ réseau dans $\mathbb{C}$, avec $\operatorname{Im}\frac{w_1}{w_2} > 0$, on introduit pour $z \in \mathbb{C}$

$$\left.\begin{aligned} \sigma(z,L) &= z \prod_{\substack{\omega\in L\\ \omega\neq 0}} (1-\tfrac{z}{\omega})\exp(\tfrac{z}{\omega}+\tfrac{1}{2}(\tfrac{z}{\omega})^2) \\ \zeta(z,L) &= \sigma'(z,L)/\sigma(z,L) \quad , \end{aligned}\right\} \qquad (2)$$

$\Delta(L)$ le discriminant de L , $s_2(L) = \lim\limits_{s\to 0^+} \sum\limits_{\substack{\omega\in L\\ \omega\neq 0}} \dfrac{1}{\omega^2|\omega|^{2s}}$,

$\eta(z,L) = s_2(L)z + \frac{\pi}{a(L)}\bar{z}$, $a(L) = \frac{w_1\bar{w}_2 - w_2\bar{w}_1}{2i}$ et

les "fonctions θ", homogènes de degré 0 en z et L :

$$\left.\begin{aligned} \theta(z,L) &= \Delta(L)\exp(-6s_2(L)\,z^2)\,\sigma(z,L)^{12} \\ \varphi(z,L) &= \Delta(L)\exp(-6\eta(z,L)z)\,\sigma(z,L)^{12} \end{aligned}\right\} \qquad (3)$$

notées respectivement $\theta^{(12)}(z,L)$ et $\varphi^{(12)}(z,L)$ dans [9].

La fonction θ est plus simple à définir et c'est donc elle qui est utilisée dans les articles récents sur les unités elliptiques mais Robert a utilisé φ dans son mémoire définissant les unités elliptiques ; d'ailleurs l'équation fonctionnelle de φ s'écrit plus simplement que celle de θ :

$$\forall z \in \mathbb{C}\ ,\ \forall w \in L\ ,\quad \varphi(z+w,L) = \varphi(z,L)\,.\exp 6(\eta(w,L)z - \eta(z,L)w). \qquad (4)$$

Considérons alors, pour $\mathfrak{A}$ idéal entier de K premier à $\mathfrak{g}$, l'élément $\varphi^{\mathfrak{g}}(\rho(\mathfrak{g}),\mathfrak{A}^{-1})$: utilisant (4) on voit qu'il ne dépend que de la classe $C(\mathfrak{A}\cdot\mathfrak{h}(\mathfrak{g}))$ de $\mathfrak{A}\mathfrak{h}(\mathfrak{g})$ dans $Cl(\mathfrak{g})$. Ceci permet de poser

$$\varphi^{\mathfrak{g}}(\rho(\mathfrak{g}),\mathfrak{A}^{-1}) = \varphi_{\mathfrak{g}}(C(\mathfrak{A}\mathfrak{h}(\mathfrak{g})))\ ,$$

et de définir ainsi $\varphi_{\mathfrak{g}}(C)$ pour tout $C \in Cl(\mathfrak{g})$.

Considérons maintenant $I_{\mathfrak{g}}$ le monoïde des idéaux entiers de K premiers à $6.\mathfrak{f}^*.\mathfrak{g}$, où $\mathfrak{f}^*$ est un idéal fixé (cf. 1.3), ainsi que l'idéal $J_{\mathfrak{g}}$ de $\mathbb{Z}[I_{\mathfrak{g}}]$ formé des $\alpha = \sum \alpha(\mathfrak{A})\mathfrak{A}$ vérifiant

$$\sum \alpha(\mathfrak{A}) = \sum \alpha(\mathfrak{A})\,N(\mathfrak{A}) = 0\ . \qquad (5)$$

Pour $\alpha \in J_{\mathfrak{g}}$, posons

$$\theta(z,\alpha) = \prod_{\mathfrak{A}\in I_{\mathfrak{g}}} \theta(z,\mathfrak{A}^{-1})^{\alpha(\mathfrak{A})}\ . \qquad (6)$$

Le résultat clef de [9] est que $\theta(\rho(\mathfrak{g}),\alpha)$ est la puissance d'ordre (*) $e(\mathfrak{g})$ d'un élément de $\mathcal{O}(H_{\mathfrak{g}})^*$; d'où la définition

---

(*) en fait $12\,e(\mathfrak{g})$.

$$\Omega_{\mathfrak{g}} = \left\{ x \in H^*_{\mathfrak{g}} \mid x^{e(\mathfrak{g})} \in \{\theta(\rho(\mathfrak{g}),\alpha)\}_{\alpha \in J_{\mathfrak{g}}} \right\} ,$$

en fait indépendante des choix de ρ et de $\mathfrak{f}^*$.

1.2.2. Cas $\mathfrak{g} = 1$. Choisissons un idéal $\mathfrak{A}$ dans C^{-1} , $C \in Cl((1))$. Soit a un générateur de l'idéal principal $\mathfrak{A}^{h(K)}$ et choisissons une racine d'ordre $h(K)$, $\varphi_{(1)}(C)$, de $a^{12}\Delta^{h(K)}(\mathfrak{A})$: $|\varphi_{(1)}(C)|$ ne dépend que de $C \in Cl((1))$. Définissons $I_{\mathfrak{g}}$ comme plus haut et introduisons l'idéal $J_{(1)}$ formé des $\alpha = \sum \alpha(\mathfrak{A}) \cdot \mathfrak{A}$ vérifiant

$$\sum \alpha(\mathfrak{A}) = 0 \quad \text{et} \quad \prod \mathfrak{A}^{\alpha(\mathfrak{A})} \text{ principal.} \qquad (5 \text{ bis})$$

Alors, d'après [9] ,

$$\theta(\alpha) \underset{\text{dfn}}{=} \prod (a^{12}\Delta(\mathfrak{A})^{h(K)})$$

est la puissance d'ordre $e.h(K)$ d'une unité de $H_{(1)}$: d'où la définition

$$\Omega_{(1)} = \left\{ x \in H^*_{(1)} \mid x^{e.h(K)} \in \{\theta(\alpha)\}_{\alpha \in J_{(1)}} \right\} .$$

1.2.3. Pour F/K extension abélienne de conducteur $\mathfrak{g}$, on introduit le groupe des unités elliptiques propres

$$\Omega_F = N_{H_{\mathfrak{g}}/F}(\Omega_{\mathfrak{g}}) \qquad (7)$$

et le groupe des unités elliptiques

$$C_F = \mu_F \prod_{K \subsetneq F' \subseteq F} \Omega_{F'} , \qquad (8)$$

où μ_F est le sous-groupe de torsion de $\mathcal{O}(F)^*$. Rappelons que, d'après [9] § 2.3, théorème 2, la norme définit une application $\Omega_F \longrightarrow \Omega_{F'}$, qui est surjective si les conducteurs de F et F' ont les mêmes facteurs premiers.

Supposons le p-groupe de Sylow de $Gal(F/K)$ cyclique et p premier à $h(K)$, alors d'après [4] (théorèmes 5 et 6, compte tenu de la différence entre $\Omega_{F \cap H_{(1)}}$ et le Ω_{ξ_0} de [4]) ,

$$h(F) \sim [\mathcal{O}(F)^* : C_F] , \qquad (9)$$

sauf dans des cas pathologiques qui n'interviennent pas dans la suite ; la formule $a \sim b$ signifie que les deux membres a et $b \in \overline{\mathbb{Q}}_p^*$ ne diffèrent que par une unité p-adique.

1.3. OBJETS ATTACHES A UNE COURBE ELLIPTIQUE AUXILIAIRE.

1.3.0. Soient H/K une extension abélienne finie de degré et de conducteur premiers à p, et E une courbe elliptique définie sur $\mathcal{O}(H)$. On note $\mathfrak{f}_H$ le produit des idéaux premiers de H où E a mauvaise réduction et $\mathfrak{f}^*$ (utilisé en 1.2) la norme de $\mathfrak{f}_H$ sur K. On suppose que le réseau de $\mathbb{C}$ correspondant aux périodes de E dans le paramétrage de Weierstrass

$$\xi : z \longrightarrow (\wp(z), \wp'(z))$$

est de la forme $\Omega_\infty \mathcal{O}(K)$, et que p et $\Delta(\Omega_\infty \mathcal{O}(K))$ sont premiers entre eux. Ainsi H contient $H_{(1)}$. Pour $\mathfrak{g} \in I$, on note $E_\mathfrak{g}$ le groupe des points de $\mathfrak{g}$-torsion de E et $H(E_\mathfrak{g})$ l'extension engendrée par les coordonnées de ces points. Ainsi $\xi(\rho(\mathfrak{g})\Omega_\infty) \in E_\mathfrak{g}$.

1.3.1. Grossencaractères (cf. [11] § 7.8) : on note ψ_H le grossencaractère de E sur H : ses valeurs sont dans K^*. On montre (*) qu'on peut changer H et E (en conservant les hypothèses ci-dessus) de façon que ψ_H s'écrive sous la forme

$$\psi_H = \psi_K \circ N_{H/K} \tag{10}$$

où ψ_K est un grossencaractère de K et $N_{H/K}$ la norme ; soit $\mathfrak{f}$ le conducteur de ψ_K. L'extension N engendrée sur K par les valeurs de ψ_K est finie, non ramifiée en $\mathfrak{p}$ et $\mathfrak{p}'$. Pour $\mathfrak{A}$ idéal entier de K premier à $\mathfrak{p}$ et $\mathfrak{f}$, $\psi_K(\mathfrak{A})$ est une unité de N^v : on note $\underline{w}(\mathfrak{A})$ la racine de 1 dans N^v congrue à $\psi_K(\mathfrak{A})$ modulo p et on définit $\langle \psi_K \rangle(\mathfrak{A})$ en prenant, dans $1+p\mathbb{Z}_p$, la racine d'ordre $[H:K]$ de $\langle \psi_K(\mathfrak{A}.\mathcal{O}(H)) \rangle$. On vérifie alors que

$$\psi_K = \underline{w} \cdot \langle \psi_K \rangle . \tag{11}$$

(*) cf. plus loin § 1.5.

Rappelons ([11], §7.8) que (10) signifie que pour chaque $\mathfrak{g}$ l'extension $H(E_{\mathfrak{g}})/K$ est abélienne.

1.3.2. Groupe formel. Soit $\hat{E}$ le complété formel de E le long de la section unité : c'est le groupe formel défini sur $\mathcal{O}(H^V)$ obtenu en prenant $W = -2x/y$ comme paramètre. On sait que, après extension à $A' \underset{\text{dfn}}{=} \mathcal{O}(\widehat{\mathbb{Q}_p^{nr}})$ ($\widehat{\mathbb{Q}_p^{nr}}$ étant le complété de l'extension non ramifiée maximale de $\mathbb{Q}_p$), il existe un isomorphisme du groupe formel multiplicatif $\underline{G}_m$ dans $\hat{E}$: il existe $\eta(T) \in A'[[T]]$, série inversible pour la composition, telle qu'on ait les identités de séries formelles

$$\eta(T_1+T_2+T_1T_2) = \eta(T_1) +_{\hat{E}} \eta(T_2)$$
$$\eta((1+T)^a-1) = [a](\eta(T)) ,$$

en notant $+_{\hat{E}}$ (resp. $[a]$) l'addition formelle (resp. la multiplication formelle par $a \in \mathbb{Z}_p$).

1.4. FONCTION L p-ADIQUE L_E .

1.4.1. Pour L réseau de $\mathbb{C}$ la série

$$H_k(z,k+s,L) \underset{\text{dfn}}{=} \sum_{\omega \in L} \frac{(\bar{z}+\bar{\omega})^k}{|z+\omega|^{2(k+s)}} \qquad (12)$$

définit une fonction de s analytique pour $\mathrm{Re}(s) > 1-\frac{k}{2}$, prolongeable en une fonction analytique sur $\mathbb{C}$. Désignons par $E_k^*(z,L)$ sa valeur pour $s = 0$. On a ainsi des formules (comparer à [1]) :

$$\left(\frac{d}{dz}\right)^k \log \theta(z,L) = \begin{cases} 12[E_1^*(z,L) + \frac{\pi}{a(L)}\bar{z}] & \text{si } k=1 , \\ -12\, E_2^*(z,L) & \text{si } k=2 , \\ 12(-1)^{k-1}(k-1)!\, E_k^*(z,L) & \text{si } k \geq 3 . \end{cases} \qquad (13)$$

$$E_k^*(z,L) = \begin{cases} \zeta(z,L) - z\, s_2(L) - \frac{\pi}{a(L)}\bar{z} & \text{si } k=1 , \\ \wp(z,L) + s_2(L) & \text{si } k=2 , \\ \frac{(-1)^k}{(k-1)!}\, \wp^{(k-2)}(z,L) & \text{si } k \geq 3 . \end{cases} \qquad (14)$$

Pour $z = 0$, dans (12) on remplace la sommation du 2ème membre par celle sur les $\omega \in L$, $\omega \neq 0$; de même dans $\zeta(z,L)$ et $\wp(z,L)$: $\zeta(z,L)$ doit être remplacé par $\zeta(z,L) - \frac{1}{z}$ et $\wp(z,L)$ par $\wp(z,L) - \frac{1}{z^2}$ dans (14).

1.4.2. Soit ν un caractère de conducteur $\mathfrak{g}_0$. On note $\mathfrak{g}$ le p.p.c.m. de $\mathfrak{g}_0$ et $\mathfrak{f}$. On définit un nombre algébrique en posant

$$L_k(\nu) = (12\sqrt{d}\, e(\mathfrak{g})g)^{-1}(1-\frac{\nu(\mathfrak{p})}{N(\mathfrak{p})})\,\nu(\mathfrak{h}(\mathfrak{g}))\sum \nu(C)^{-1}\log \varphi_{\mathfrak{g}}(C) \quad \text{si } k = 0$$

et

$$= (-1)^{k-1}(k-1)!\,(\sqrt{d}\, e(\mathfrak{g}))^{-1}(1-\frac{\nu(\mathfrak{p})\psi_K^k(\mathfrak{p})}{N(\mathfrak{p})})\sum \nu(\mathfrak{B})^{-1}$$
$$\psi_K(\mathfrak{B})^{-k} E_k^*(\rho(\mathfrak{g}),\mathfrak{B}^{-1})\Omega_\infty^{-k} \quad \text{si } k > 0 ,$$

cf. notations de 1.1 ; dans la première somme C parcourt $Cl(\mathfrak{g})$ et log désigne le logarithme dans $\overline{\mathbb{Q}}_p$ (prolongé en posant $\log p = 0$). Dans la deuxième somme $\mathfrak{B}$ parcourt un système de représentants de $Cl(\mathfrak{g})$ et on vérifie que la somme ne dépend pas du choix du système. Soulignons par contre la dépendance des choix de ρ et E .

Le caractère ν se décompose en une partie modérée φ (pour $\mathfrak{p}$) et une partie sauvage $\underline{\pi}$ totalement ramifiée en $\mathfrak{p}$ d'ordre une puissance de p ; on voit facilement qu'il existe un caractère d'ordre une puissance de p , $\pi : \mathbb{Z}_p^* \longrightarrow \overline{\mathbb{Q}}_p^*$ tel que

$$\underline{\pi} = \pi \circ \langle \psi_K \rangle .$$

Avec les notations de 1.2.2, on a aussi $\underline{\pi}(\mathfrak{A}) = \pi(a)^{1/h(K)}$ pour $\mathfrak{A} \in I$, $\mathfrak{A}$ premier à $\mathfrak{p}$. Pour $k \in \mathbb{Z}$, on pose $\varphi_k = \varphi \cdot \underline{\omega}^{-k}$, $\nu_k = \nu \cdot \underline{\omega}^{-k}$. On peut montrer :

LEMME 1. - *Il existe un unique entier* i *tel que le conducteur de* φ_i *soit premier à* $\mathfrak{p}$ *et vérifiant* $0 < i < p$.

On introduit alors

$$\tau(\nu) = \sum_{\lambda=1}^{p^m} \omega^{-i}(\lambda)\,\pi^{-1}(\lambda)\,\zeta_m^{\lambda} ,$$

où p^m désigne le conducteur de $\omega^i \cdot \pi$, et ζ_m la racine de l'unité image par η^{-1} du point $\xi(\rho(\mathfrak{p}^m)\Omega_\infty)$ de $E_{\mathfrak{p}^m}$ (identifié au point correspondant de $\hat{E}$).

En reprenant les constructions de [5] , on obtient ainsi une série $f_E(T,\varphi) \in A'[[T]]$ (et dépendant de ρ !) . On pose alors, après avoir choisi un générateur c de $1+p\mathbb{Z}_p$,

$$L_E(s,\nu) = f_E(\pi(c)c^{1-s}-1\ ,\ \varphi) \ .$$

THEOREME 1. - *On a*

$$L_E(1-k,\nu) = \eta'(0)^k . \tau(\nu_k)^{-1} . L_k(\nu_k) \ .$$

Soient $\mathfrak{g}_0$ le conducteur de φ et $\mathfrak{g}$ le p.p.c.m. de $\mathfrak{g}_0$ et $\mathfrak{f}$: on déduit du théorème 1 que l'élément

$$B_E(\varphi) = \Sigma \varphi(\mathfrak{B})^{-1} E_j^*(\rho(\mathfrak{g}),\mathfrak{B}^{-1})\Omega_\infty^{-j} \ ,$$

avec $j = i$ (resp. $j = p$) si $i \neq 1$ (resp. si $i = 1$) est dans A' et ne dépend pas modulo p du choix du système d'idéaux $\mathfrak{B}$ représentant $Cl(\mathfrak{g})$. Comme $(1 - \dfrac{\nu(\mathfrak{p})\,\psi_K^j(\mathfrak{p})}{N\mathfrak{p}})$ est inversible dans A' , on obtient :

COROLLAIRE. - *Pour que la série* $f_E(T,\varphi)$ *soit inversible dans* $A'[[T]]$, *il faut et il suffit que* $B_E(\varphi)$ *ne soit pas dans* $p.A'$.

1.5. SUR LE CHOIX DE E .

Pour définir $L_0(\nu)$, on a sommé sur $Cl(\mathfrak{g})$. La sommation sur $Cl(\mathfrak{g}_0)$ garde un sens. Ainsi, en posant

$$\mathfrak{L}(\nu) = (12\sqrt{d}\,e(\mathfrak{g}_0)g_0)^{-1}(1-\frac{\nu(\mathfrak{p})}{N\mathfrak{p}})\,\nu(\mathfrak{h}(\mathfrak{g}_0))\Sigma\nu(C)^{-1}\log\varphi_{\mathfrak{g}_0}(C) \ ,$$

on déduit de [9] § 2.3 que

$$L_0(\nu) = \mathfrak{L}(\nu)\cdot\nu(\mathfrak{h}(\mathfrak{g})\mathfrak{h}(\mathfrak{g}_0)^{-1}).\prod_{\mathfrak{q}\mid\mathfrak{f}}(1-\nu(\mathfrak{q})) \ . \qquad (15)$$

PROPOSITION 1. - Pour chaque caractère φ modérément ramifié en $\mathfrak{p}$, on peut choisir H et E (cf. 1.3) de façon que $\prod_{\mathfrak{q}\mid\mathfrak{f}} (1-\varphi(\mathfrak{q}))$ soit non nul.

La démonstration de la proposition 1 est faite en 1.5.3 et 1.5.4.

1.5.1. Conséquence de la proposition 1 : soit φ un caractère modérément ramifié en $\mathfrak{p}$; on suppose que φ n'est pas d'ordre une puissance de p (sinon cf. 1.6 ; φ est alors non ramifié en $\mathfrak{p}$). Considérons alors la série

$$H_E(T,\varphi) = \frac{\varphi(\mathfrak{h}(\mathfrak{g}))}{\varphi(\mathfrak{h}(\mathfrak{g}_0))} \cdot \frac{(1+T)^{\ell(\mathfrak{h}(\mathfrak{g}))}}{(1+T)^{\ell(\mathfrak{h}(\mathfrak{g}_0))}} \prod_{\mathfrak{q}\mid\mathfrak{f}} (1-\varphi(\mathfrak{q})(1+T)^{\ell(\mathfrak{q})})$$

où, pour $\mathfrak{B}$ idéal de K premier à $\mathfrak{p}$, $\ell(\mathfrak{B})$ est l'entier p-adique défini par l'égalité

$$\langle b\rangle = c^{\ell(\mathfrak{B})\cdot h(K)} ,$$

avec b générateur de l'idéal principal $\mathfrak{B}^{h(K)}$; ainsi on a $\pi(\mathfrak{B}) = \pi(c)^{\ell(\mathfrak{B})}$. Si E et H sont choisis comme dans la proposition précédente $H_E(T,\varphi)$ est inversible : si on pose

$$f(T,\varphi) = \frac{f_E(T,\varphi)}{H_E(T,\varphi)} , \quad L_{\mathfrak{p}}(s,\nu) = f(\pi(c)c^{1-s}-1,\varphi) , \qquad (16)$$

alors $f(T,\varphi)$ est toujours dans $A'[[T]]$, et de plus

$$f(\pi(c)-1,\varphi) = L_{\mathfrak{p}}(1,\nu) = \tau(\nu)^{-1}\mathfrak{L}(\nu) . \qquad (17)$$

Ceci prouve en particulier que la fonction $L_{\mathfrak{p}}$ construite ci-dessus ne dépend plus de E (plus précisément, partant de deux courbes elliptiques E et E' vérifiant les conditions de la proposition, on constate qu'elles deviennent isomorphes sur A' ; en utilisant cet isomorphisme pour rendre compatible les choix de η, les séries $f(T,\varphi)$ associées coïncident puisqu'elles prennent les mêmes valeurs pour $\zeta-1$, ζ racine de 1 d'ordre une puissance de p) .

Remarque. - Partant de E et H comme dans 1.3.1, on déduit de (15) et (17) l'égalité $f_E(T,\varphi) = H_E(T,\varphi)\cdot f(T,\varphi)$.

1.5.2. Dans la situation de 1.3.0, considérons un modèle $y^2 = 4x^3 - g_2x - g_3$ de E, avec g_2 et g_3 dans $\mathcal{O}(H)$ et posons $\Delta = g_2^3 - 27g_3^2$. Soit I un idéal premier de H, premier à 2 et 3.

LEMME 2. - La courbe elliptique E a bonne réduction pour I si et seulement si la valuation I-adique de Δ est divisible par 12 ; dans tous les cas, cette valuation est divisible par $12/e$.

Démonstration. - Tout modèle de Weierstrass de E est de la forme

$$y^2 = 4x^3 - g'_2x - g'_3 \quad \text{avec} \quad g'_2 = u^4 g_2 \ , \ g'_3 = u^6 g_3 \quad \text{et} \quad \Delta' = u^{12}\Delta . \tag{18}$$

Si E a bonne réduction en I, on peut trouver $u \in H$ tel que $\Delta' = u^{12}\Delta$ soit premier à I ; la réciproque se démontre en utilisant l'intégralité de l'invariant g_2^3/Δ de E. Dans tous les cas, E possède une H-forme E' (cf. [10] théorème 9, corollaire 1) qui a bonne réduction en I : on peut choisir un modèle (18) avec Δ' premier à I et on vérifie alors que u^e est dans H, d'où la fin du lemme.

1.5.3. Cas où $K = \mathbb{Q}(\sqrt{-1})$ ou $\mathbb{Q}(\sqrt{-3})$. Choisissons une courbe elliptique E, admettant $\mathcal{O}(K)$ comme anneau de multiplications complexes, définie par une équation de Weierstrass avec g_2 et g_3 dans $\mathcal{O}(K)$; on suppose que E a bonne réduction pour $\mathfrak{p}$ et les diviseurs premiers de 2 et 3. Considérons l'ensemble $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ des idéaux premiers de K où E a mauvaise réduction et vérifiant $\varphi(\mathfrak{q}_i) = 1$. Soit $\mathfrak{q}$ un idéal premier de K, premier à 2,3 et $\mathfrak{p}$, et vérifiant $\varphi(\mathfrak{q}) \neq 1$. Choisissons des générateurs q, $q_1, \ldots, q_r$ de $\mathfrak{q}, \mathfrak{q}_1, \ldots, \mathfrak{q}_r$. On peut trouver des éléments $q'_1, \ldots, q'_r \in K$, premiers à 2,3 et $\mathfrak{p}$, engendrant des idéaux premiers $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_r$ et vérifiant

$$\varphi(\mathfrak{q}) \cdot \varphi(\mathfrak{q}'_i) = \varphi(\mathfrak{q}_i) = 1 \tag{19}$$

$$\frac{q \cdot q'_i}{q_i} \equiv 1 \bmod e^3 . \tag{20}$$

Posons alors $\alpha = \prod (\frac{qq_i'}{q_i})^{n_i}$, où n_i est tel que la valuation q_i-adique de Δ soit $n_i \cdot 12/e$ (cf. lemme 2), et $u = \sqrt[e]{\alpha}$. Définissons E' par son modèle (18). De (20), on déduit que l'extension $K(u)/K$ est non ramifiée pour les diviseurs premiers de 2 et 3 dans K , ce qui entraîne la bonne réduction de E' (compte-tenu de celle de E) pour ces diviseurs. On déduit alors du lemme et de (19) que les idéaux premiers q' de K où E' a mauvaise réduction sont premiers à 2 , 3 , p et vérifient $\varphi(q') \neq 1$. Les conditions de 1.3 sont clairement vérifiées par $H = K$ et la courbe elliptique E' : si on choisit g_2 et g_3 avec p premier à Δ , p est encore premier à Δ' .

1.5.4. Cas $e = 2$. Choisissons une courbe elliptique E , admettant $\mathcal{O}(K)$ comme anneau de multiplications complexes, définie par une équation de Weierstrass avec g_2 et g_3 dans $\mathcal{O}(H_{(1)})$; on suppose que E a bonne réduction pour les diviseurs premiers de 2 et 3 (cf. [11] , chap.5 et [10] théorème 9, corollaire 1). Soit q un idéal premier de K décomposé dans $K/\mathbb{Q}$ premier à 2 , 3 et Δ , et vérifiant $\varphi(q) \neq 1$. On choisit un point t non nul de E_q . D'après [11] , 7.8.8, on peut énoncer :

> LEMME 3. - Il existe une courbe elliptique E' définie sur H_q et un isomorphisme $E \longrightarrow E'$ tel que l'image t' de t soit rationnel sur H_q . Dans ces conditions, les points de torsion de E' engendrent sur H_q des extensions qui sont abéliennes sur K .

Représentons E' par (18) , l'élément u correspondant à l'isomorphisme $E \longrightarrow E' : (x,y) \longrightarrow (u^2x, u^3y)$. Comme t' appartient à H_q , on en déduit immédiatement que $H_{(1)}(E_q) = H_q(u)$ et que u^2 appartient à H_q . Soient I un idéal premier de H_q , premier à 2 , 3 et q , et $I_{(1)}$ l'idéal premier de $H_{(1)}$ au-dessous de I .

LEMME 4. - Les conditions suivantes sont équivalentes :

i) la valuation $\mathfrak{I}$-adique de u^2 est impaire,

ii) $\mathfrak{I}$ est ramifié dans $H_{(1)}(E_q)/H_q$,

iii) E a mauvaise réduction en $\mathfrak{I}_{(1)}$,

iv) la valuation $\mathfrak{I}_{(1)}$-adique de Δ est congrue à 6 modulo 12 .

La partie difficile est ii) $\Leftrightarrow$ iii), cf. [1] , lemme 4. La partie iii) $\Leftrightarrow$ iv) provient du lemme 2.

LEMME 5. - Soit E' comme dans le lemme 3 ; alors E' a bonne réduction pour tous les idéaux premiers de H_q premiers à q .

Démonstration. - Soit $\mathfrak{I}$ un idéal premier de H_q , premier à q . Si $\mathfrak{I}$ divise 2 ou 3 , l'assertion résulte de l'isomorphisme entre E et E' sur $H_{(1)}(E_q)$, de la non ramification de $\mathfrak{I}$ dans $H_{(1)}(E_q)/H_q$ et de la bonne réduction de E en $\mathfrak{I}$. Si $\mathfrak{I}$ est premier à 2 et 3 , il suffit d'appliquer le lemme 2 à E' et $\Delta' = u^{12}\cdot\Delta$: si la valuation $\mathfrak{I}_{(1)}$-adique de Δ est congrue à 0 (resp. 6) modulo 12, la valuation $\mathfrak{I}$-adique de u^2 est paire (resp. impaire) donc la valuation $\mathfrak{I}$-adique de Δ' est congrue à 0 modulo 12 .

Pour démontrer la proposition, il suffit donc de remplacer E et $H_{(1)}$ par E' et $H = H_q$.

1.6. COMMENTAIRES.

1.6.1. Replaçons-nous dans la situation de 1.4.2. Remarquons que pour tout idéal $\mathfrak{B}$ de K premier à $\mathfrak{f}$, on a $\psi_K(\mathfrak{B})\cdot\overline{\psi_K(\mathfrak{B})} = N(\mathfrak{B})$; en effet les deux membres ne diffèrent que par une racine de 1 (car, cf. [11] , pour $\mathfrak{A}$ idéal de H premier au conducteur de ψ_K , l'élément $\psi_K(\mathfrak{A})$ de K engendre l'idéal $N_{H/K}(\mathfrak{A})$) et sont tous les deux réels > 0 . Ceci permet de démontrer les formules

$$\begin{aligned}\sum \nu(\mathfrak{B})^{-1}\,\psi^{-k}(\mathfrak{B})\,E_k^*(\rho(y),\mathfrak{B}^{-1}) &= [\nu(\mathfrak{h}(g))\,\psi^k(\mathfrak{h}(g))\,\rho(g)^{-k}]\;L(k,\bar{\nu}\cdot\bar{\psi}^{-k})\\ &= [\nu(\mathfrak{h}(g))\,\psi^k(\mathfrak{h}(g))\,\rho(g)^{-k}]\;L(0,\nu^{-1}\cdot\psi^{-k})\ ,\end{aligned}$$

qui expriment nos sommes en termes de fonctions L attachées aux grossencaractères (définies en sommant sur les idéaux entiers de K premiers à $\mathfrak{g}$) ; ceci fait le lien avec les résultats de [1] et les constructions de [7], §9.4. Notons à ce sujet que si θ désigne un caractère de Dirichlet de conducteur divisible par $\mathfrak{f}$, on a $H_E(T,\theta) = 1$, $f(T,\varphi) = f_E(T,\varphi)$. Ceci généralise la situation où $h(K) = 1$, $H = K$ et où θ décrit l'action galoisienne sur $E_\mathfrak{p}$, cf. [1], lemme 4.

1.6.2. Dans [5], nous avons fait l'hypothèse que l'indice de ramification de $\mathfrak{p}$ dans F_φ, corps associé au noyau de φ dans $Cl(\mathfrak{g}_0)$ ($\mathfrak{g}_0$ conducteur de φ), divise $p-1/e$; ceci nous a permis de construire une série $f'(T,\varphi) \in A'[[T]]$ dont la valeur en $\pi(c)-1$ est $\mathfrak{L}(\nu)\cdot T(\nu)^{-1}\cdot\nu(\mathfrak{h}(\mathfrak{g}_0))^{-1}$ ($T(\nu)$ désignant la somme de Gauss usuelle, cf.1.1). Le lien entre les deux séries est donc

$$f(T,\varphi) = f'(T,\varphi)\cdot T(\varphi_i)\,\varphi_i(\mathfrak{h}(\mathfrak{g}_0)) \ . \qquad (21)$$

L'avantage de $f'(T,\varphi)$ est son indépendance du choix de ρ, comparer avec 1.6, ci-dessous. Sa construction n'utilise qu'<u>une</u> courbe elliptique choisie indépendamment de φ. Ceci permet de <u>définir</u> encore $f(T,\varphi)$ lorsque φ <u>est d'ordre une puissance de</u> p (donc F_φ/K est non ramifiée en $\mathfrak{p}$), en conservant les formules (17) et (21).

1.6.3. <u>Changement de</u> η. On sait que η peut être modifié par multiplication formelle par un élément $b \in \mathbb{Z}_p^*$. Ainsi ζ_m est transformé en $\zeta_m^{b^{-1}}$, $\tau(\nu_k)$ en $\omega^{k-i}(b)\,\pi(b)^{-1}\,\tau(\nu_k)$ et $\eta'(0)$ en $b\eta'(0)$. Ainsi $f_E(T,\varphi)$ (et donc $f(T,\varphi)$) est multiplié par la série $\omega^i(b)\,(1+T)^{\ell((b))}$ (il suffit de comparer les valeurs en $\pi(c)-1$).

1.6.4. <u>Changement de</u> ρ. Avec les notations suivant le théorème 1, dans la définition de L_E n'interviennent que les valeurs de $\rho(\mathfrak{g}\mathfrak{p}^m) = \rho(\mathfrak{g}) + \rho(\mathfrak{p}^m)$ pour $m \in \mathbb{N}$.

1.6.4.1. <u>Changement de</u> $\rho(\mathfrak{g})$. Comme $\rho(\mathfrak{g})$ n'intervient que par sa valeur modulo $\mathcal{O}(K)$, on peut supposer que la nouvelle valeur est $b\rho(\mathfrak{g})$,

avec $b \in K$ premier à $\mathfrak{g}$. Ainsi $\rho(\mathfrak{g}\mathfrak{p}^m)$ devient $b_m\rho(\mathfrak{g}\mathfrak{p}^m)$ (modulo $\mathcal{O}(K)$) avec $b_m \equiv 1 \bmod \mathfrak{p}^m$, $b_m \equiv b \bmod \mathfrak{g}$. En reportant dans le formule du théorème 1, on voit que $L_E(1-k,\nu)$ est multiplié par

$$\nu_k((b_m))\,\psi_K((b_m))^k/b_m^k = \nu((b_m))\,\frac{\langle\psi_K((b_m))\rangle^k}{b_m^k} = \nu((b_m)) \text{ si } m > 0 .$$

Compte-tenu de $b_m/b \equiv 1 \bmod \mathfrak{g}$, $b_m \equiv 1 \bmod \mathfrak{p}^m$,

$$\nu((b_m)) = \varphi_i((b))\underline{\omega}^i((b_m)) = \varphi_i(b)\underline{\omega}^i((b))\underline{\omega}^i((\tfrac{b_m}{b})) = \varphi(b)\omega^i(\tfrac{b_m}{b}) = \varphi(b)\omega^{-i}(b) .$$

Ainsi $f_E(T,\varphi)$ est multipliée par $\varphi(b)\omega^{-i}(b)$; attention, en général $\omega(b) \neq \underline{\omega}((b))$! On vérifie à l'aide de (16) le même phénomène pour $f(T,\varphi)$.

1.6.4.2. Changement de $\rho(\mathfrak{p}^m)$: on peut supposer que la nouvelle valeur est de la forme $b_m\rho(\mathfrak{p}^m)$, avec $b_m \in K$, b_m premier à $\mathfrak{p}$; ainsi $\rho(\mathfrak{g}\mathfrak{p}^m)$ est multiplié (mod $\mathcal{O}(K)$) par b'_m avec $b'_m \equiv 1 \bmod \mathfrak{g}$, $b'_m \equiv b_m \bmod \mathfrak{p}^m$. Ainsi on a $\psi_K((b'_m)) = b'_m$ et $L_k(\nu)$ est multiplié par $\nu((b'_m)) = (\omega^i\pi)(b'_m) = (\omega^i\pi)(b_m)$. Ceci est compensé par le changement de ζ_m dans $\tau(\nu)$. Ainsi $f_E(T,\varphi)$ et $f(T,\varphi)$ ne dépendent pas du choix des $\rho(\mathfrak{p}^m)$.

2. - APPLICATIONS ARITHMETIQUES

2.1. FORMULE p-ADIQUE DU NOMBRE DE CLASSES ET CRITERE DE KUMMER.

Soient F/K une extension abélienne et Δ son groupe de Galois. On suppose que p ne divise ni $h(K)$ ni le degré (fini) $[F:K]$. Désignons par K_∞ la $\mathbb{Z}_p$-extension de K non ramifiée en dehors de $\mathfrak{p}$ et par F_∞ l'extension composée $F\cdot K_\infty$; soit S l'ensemble des places de F_∞ au-dessus de $\mathfrak{p}$. Notons F_n la sous-extension de degré p^n dans F_∞/F , F_n^w son complété, U_n^w le p-groupe de Sylow de $\mathcal{O}(F_n^w)^*$ pour chaque $w \in S$. Posons $U_n = \prod_{w\in S} U_n^w$, $C_n = C_{F_n}$ (cf.(8)) ; soit δ l'application diagonale $F_n \longrightarrow \prod_{w\in S} F_n^w$ et désignons par $\overline{\mathcal{O}(F_n)^*}$ (resp. $\overline{C}_n$)

la fermeture de $U_n \cap \delta(\mathcal{O}(F_n)^*)$ (resp. $U_n \cap \delta(C_n)$) dans U_n. La formule suivante résume les formules de nombre de classes ; M_n y désigne la p-extension abélienne, non ramifiée en dehors de $\mathfrak{p}$, maximale de F_n. On note R le régulateur p-adique, $\Delta(F_n)$ le discriminant sur K, w_n le nombre de racines de 1 dans F_n.

PROPOSITION 2. - On a :

$$[U_n : \overline{C}_n(1+p\mathbb{Z}_p)] \sim p^n \frac{R(\mathcal{O}(F_n)^*)h(F_n)}{w_n \cdot \sqrt{\Delta(F_n)}} \prod_{\nu \neq 1} \left(1 - \frac{\nu(\mathfrak{p})}{N(\mathfrak{p})}\right) \sim p^n \prod_{\nu \neq 1} L_{\mathfrak{p}}(1,\nu)$$

$$\sim [\mathrm{Gal}(M_n/F_\infty)] ,$$

où dans les produits ν parcourt l'ensemble des caractères $\neq 1$ de $\mathrm{Gal}(F_n/K)$ définis et irréductibles sur $\overline{\mathbb{Q}}_p$.

Soient $\Lambda \neq 1$ un caractère de Δ défini et irréductible sur $\mathbb{Q}$ et $e_\Lambda \in \mathbb{Z}_p[\Delta]$ l'idempotent associé. Comme $U_n/\overline{C}_n$ et $\mathrm{Gal}(M_n/F_n)$ sont des $\mathbb{Z}_p[\Delta]$-modules, on peut comparer leurs Λ-composantes :

THEOREME 2. - On a

$$[e_\Lambda(U_n/\overline{C}_n)] \sim \prod_{\zeta^{p^n}=1} \prod_{\varphi} f(\zeta - 1, \varphi) \sim [e_\Lambda \mathrm{Gal}(M_n/F_n)]$$

où le produit est pris sur l'ensemble des racines de 1 d'ordre divisant p^n et sur l'ensemble des composants irréductibles de Λ sur $\overline{\mathbb{Q}}_p$.

Notons $\mathcal{C}(F_n)$ le p-groupe des classes de F_n. Choisissons E comme en 1.5 et $B_E(\varphi)$ comme en 1.4 (avec E comme en 1.5).

COROLLAIRE. - Les affirmations

i) p divise $[e_\Lambda \mathcal{C}(F_n)]$,

ii) p divise $[e_\Lambda \mathrm{Gal}(M_n/F_n)]$,

iii) p divise $B_E(\varphi)$ dans A' pour au moins un composant irréductible φ de Λ sur $\overline{\mathbb{Q}}_p$,

sont reliées par les implications i) $\Rightarrow$ ii) $\Leftrightarrow$ iii) .

Remarque. - Si p divise $[e_\Lambda C(F_n)]$, on peut aussi écrire une condition nécessaire relative à $\mathfrak{p}'$.

Question. - Le corollaire précédent est-il encore valide en remplaçant Λ par un caractère défini et irréductible sur $\mathbb{Q}_p$?

2.2. STRUCTURE GALOISIENNE DE Y_∞ .

Les considérations de 2.1 conduisent à introduire la limite $Y_\infty = \varprojlim U_n/\overline{C}_n$ (pour les normes relatives) et à penser que les modules galoisiens Y_∞ et $\mathrm{Gal}(M_\infty/F_\infty)$, M_∞ étant défini comme M_n mais en substituant F_∞ à F_n , ont des structures galoisiennes voisines. C'est ce qui motive l'étude de Y_∞ . Soit toujours φ un caractère de Δ défini et irréductible sur $\overline{\mathbb{Q}}_p$. Notons e_Φ l'idempotent associé : le $\mathbb{Z}_p[\Delta]$-module $e_\Phi \mathbb{Z}_p[\Delta]$ est simple. Si A désigne l'anneau engendré sur $\mathbb{Z}_p$ par l'image de Δ par φ , le prolongement de φ induit un isomorphisme

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

En utilisant la décomposition en produit direct

$$\mathrm{Gal}(F_\infty/K) \simeq \mathrm{Gal}(F_\infty/F)\cdot\Delta ,$$

on peut munir $e_\Phi Y_\infty$ d'une structure de $A[[T]]$-module : l'action de $1+T$ est égale à la restriction de l'automorphisme de $\bigcup_{n\in\mathbb{N}} H(E_{\mathfrak{p}^n})/H(E_\mathfrak{p})$ défini par $\zeta(\rho(\mathfrak{p}^n)\Omega_\infty) \longrightarrow \zeta(c\rho(\mathfrak{p}^n)\Omega_\infty)$, c choisi comme en 1.4.2.

Soit, pour $w \in S$, μ^w la partie de torsion de la réunion des U_n^w ; on vérifie facilement que c'est un groupe fini. On peut considérer $(\varprojlim \mu^w)^{e_\Phi}$ comme un $A[[T]]$-module fini. Comme ce module est monogène, il est de la forme $A[[T]]/\mathfrak{a}$ pour un idéal $\mathfrak{a}$ de $A[[T]]$. De [6] , on déduit que le $A[[T]]$ module $e_\Phi U$ est isomorphe à $\mathfrak{a}$. De même, soit $\mathfrak{B}$ l'idéal maximal de $A[[T]]$ si $e_\Phi \overline{C}_n$ admet de la torsion (ce qui n'arrive que si Φ est le caractère défini sur $\mathbb{Q}_p$ décrivant l'action galoisienne sur $\sqrt[p]{1}$; la torsion dans $e_\Phi \overline{C}_n$ se réduit alors au groupe engendré par $\sqrt[p]{1}$) et $A[[T]]$ lui-même sinon.

THEOREME 3. - *Il existe une série* $g(T,\varphi) \in A[[T]]$ *ne différant de* $f(T,\varphi)$ *que par une unité dans* $A'[[T]]$ *telle que* $\mathfrak{A}$ *contienne* $g(T,\varphi)\mathfrak{B}$ *et que*

$e_\Phi Y_\infty \simeq \mathfrak{A}/g(T,\varphi)\mathfrak{B}$.

Désignons par ω_n la série $(1+T)^{p^n}-1$.

COROLLAIRE 1. - *On a un isomorphisme*

$e_\Phi(U_n/\overline{C}_n) \simeq \mathfrak{A}/(g(T,\varphi)\mathfrak{B},\omega_n)$

si $\varphi(p) \neq 1$ *et une suite exacte*

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

sinon.

La complication $\mathfrak{A} \neq A[[T]]$ arrive effectivement même dans des cas où $\mathfrak{B} = A[[T]]$, cf. cas anormal de [1] .

Remarquons que si $\mathfrak{B}$ n'est pas inclus dans $\mathfrak{A}$, la série $g(T,\varphi)$ n'est pas inversible ; des théorèmes 2 et 3, on déduit donc , en notant Λ la somme des conjugués de φ sur $\mathbb{Q}$, le corollaire suivant.

COROLLAIRE 2. - *Si* $\mathfrak{B}$ *n'est pas inclus dans* $\mathfrak{A}$, *les groupes* $e_\Phi Y_\infty$ *et* $e_\Lambda \mathrm{Gal}(M_\infty/F_\infty)$ *sont infinis*.

Exemple 1. $K = \mathbb{Q}(\sqrt{-3})$, E d'équation $y^2 = x^3-5$, $p = 37$ et $\varphi = \theta$ (cf. 1.6.1).

Exemple 2. Soit χ le caractère de Dirichlet correspondant à l'action galoisienne sur $\sqrt[p]{1}$ et $\tilde{\varphi} = \chi\varphi^{-1}$. Si $\tilde{\varphi}$ est non trivial et vérifie $\tilde{\varphi}(p) = 1$ alors on a $\mathfrak{A} \subsetneq \mathfrak{B} = A[[T]]$.

BIBLIOGRAPHIE

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

[2] J. COATES et A. WILES - Kummer's criterion for Hurwitz numbers, Kyoto conference on Algebraic Number Theory, ed. by Iyangua, Jap. Soc. for the promotion of Science, (1977), pp.9-23.

[3] J. COATES et A. WILES - On p-adic L functions and elliptic units, J. Austral. Math. Soc. (series A), 26 (1978), pp. 1-25.

[4] R. GILLARD - Remarques sur les unités cyclotomiques et les unités elliptiques, J. of number Th., 11 (1979), pp. 21-48.

[5] R. GILLARD - Unités elliptiques et fonctions L p-adiques. Comp. Math. à paraître.

[6] K. IWASAWA - On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Maths, 98 (1973), pp. 246-326.

[7] N. KATZ - p-adic interpolation of real analytic Eisenstein series, Ann. of Maths, 104 (1976), pp. 459-571.

[8] S. LANG - Elliptic functions, Addison Wesley, (1973).

[9] G. ROBERT - Unités elliptiques, Bull. Soc. Math. France, mém. 36 (1973).

[10] J.P. SERRE et J. TATE - Good reduction of abelian varieties, Ann. of Maths, 88 (1968), pp. 492-517.

[11] G. SHIMURA - Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten, 1971.

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