SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

ROLAND GILLARD

Séries d'Eisenstein et critère de Kummer

Séminaire de théorie des nombres de Grenoble, tome 10 (1981-1982), exp. n° 2, p. 1-15

<http://www.numdam.org/item?id=STNG_1981-1982__10__A2_0>

Séminaire de Théorie des Nombres
10 juin 1982
Grenoble

SERIES D'EISENSTEIN ET CRITERE DE KUMMER

par Roland GILLARD

Ce texte résulte d'un travail avec G. Robert. Il s'agit dans la partie 1 de généraliser son article [Rob] en considérant des séries d'Eisenstein de niveau N. La partie 2 développe un critère de Kummer pour les extensions abéliennes d'un corps quadratique imaginaire K pour un nombre premier inerte. Les congruences entre séries d'Eisenstein sont alors rapprochées de l'involution de Leopoldt sur les caractères de Dirichlet de K.

1. - CONGRUENCES ENTRE SERIES D'EISENSTEIN

1.0. - FORMES MODULAIRES (cf. [KATZ])

On fixe p un nombre premier ≥ 5 et N un entier premier à p et ≥ 3. Soit R un anneau (commutatif). On considère les triplets $\mathcal{T} = (E, \omega, \beta)$ formés d'une courbe elliptique E définie sur R, d'une forme différentielle $\omega \in H^0(E, \Omega^1_{E/R})$ toujours $\neq 0$ et d'un isomorphisme de schémas en groupes finis sur R.

1.0.1. $\underset{\sim}{\mu_N} \times \underset{\sim}{\mathbb{Z}/N\mathbb{Z}} \longrightarrow E[N]$,

où $E[N]$ désigne le noyau de la multiplication par N dans E. On suppose que β respecte les formes symplectiques naturelles des deux membres de 1.0.1.

Une forme modulaire de niveau (arithmétique) N de poids n ($n \in \mathbb{N}$) sur un anneau B est une loi f qui à chaque triplet $\mathcal{T}$ défini sur une B-algèbre R associe un élément $f(\mathcal{T})$ de R en respectant les hypothèses suivantes :

i) $f(\mathcal{T})$ ne dépend que de la classe d'isomorphie de $\mathcal{T}$;

ii) f est compatible à l'extension des scalaires ;

iii) f est homogène : $f(E, \lambda\omega, \beta) = \lambda^{-n} \cdot f(E, \omega, \beta)$, pour $\lambda \in R^*$;

iv) f est "définie à l'infini".

On note $M_n(B)$ l'ensemble de ces formes modulaires et $M(B)$ la somme directe $M(B) = \bigoplus_{n \geq 0} M_n(B)$.

EXEMPLE 1. - Si $B = \mathbb{C}$, la donnée de $f \in M_n(B)$ revient à se donner une fonction holomorphe $\underline{f}$ sur $GL^+ = \{(\omega_1, \omega_2) \in \mathbb{C}^2 \mid \mathrm{Im} \frac{\omega_2}{\omega_1} > 0\}$ vérifiant certaines conditions. En effet, à $(\omega_1, \omega_2) \in GL^+$ on associe la courbe algébrique E définie par la variété analytique $\mathbb{C}/\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, cf. paramétrage de Weierstrass $z \xrightarrow{\xi} (\wp(z), \wp'(z))$; ω est choisie telle que $\xi^*(\omega) = dz$ et on pose $\beta(\exp \frac{2\pi i a}{N}, \frac{b}{N}) = \xi(\frac{a\omega_1 + b\omega_2}{N})$.

On a alors $\underline{f}(\omega_1, \omega_2) = f(E, \omega, \beta)$. Si on pose $\underline{f}(\tau) = \underline{f}(1, \tau)$, $q_N = \exp \frac{2\pi i \tau}{N}$, $\underline{f}$ admet un développement de Fourier :

1.0.2. $\underline{f}(\tau) = \sum a_i q_N^i$;

La condition iv) implique que $a_i = 0$ pour $i < 0$.

Soit $B((q_N)) = \{ \sum_{i >> -\infty} a_i q_N^i , a_i \in B \}$. Au moyen de la "courbe de Tate", on peut définir un triplet $\mathcal{T}_\infty$ sur $\mathbb{Z}((q_N))$. Ceci permet d'associer

à tout B et $f \in M_n(B)$ un élément $f(\mathcal{T}_\infty)$ dans $B((q_N))$ redonnant 1.0.2 lorsque $B = \mathbb{C}$.

EXEMPLE 2. - Posons $G = (\mathbb{Z}/N\mathbb{Z})^2$ et notons B^G l'ensemble des applications de G dans l'anneau B. Si B est une $\mathbb{Z}_{(p)}$-algèbre, $\mathbb{Z}_{(p)} = \mathbb{Z}[(1/\ell)_\ell$, ℓ premier $\neq p]$, pour $f \in B^G$, on définit $G_{n,f} \in M_n(B)$ (si pour $n \equiv 0$ ou $2 \bmod p-1$, f vérifie

1.0.3. $\sum_{a=0}^{N-1} f(a,0) = \sum_{b=0}^{N-1} f(0,b) = 0$)

par

1.0.4. $$G_{n,f}(\mathcal{T}_\infty) = a_0 + \sum_{i\geq 1} q_N^i \sum_{dd'=i} d^{n-1} f(d,d') ,$$

avec $a_0 = \frac{1}{2} L(1-n, f(\cdot,0))$ $(= \frac{1}{2} L(0, f(\cdot,0)+f(0,\cdot))$ si $n = 1)$.

VARIANTES. - Si B est intègre, on peut considérer

1.0.5. $$E_{n,f} = G_{n,f} / a_0 \text{ si } a_0 \neq 0 \text{ et}$$

1.0.6. $$S_{n,f} = \frac{2(-1)^n}{(n-1)!} G_{n,f}$$

a priori définies seulement sur le corps des fractions de B.

LIEN AVEC L'EXEMPLE 1. - Si $(\omega_1, \omega_2) \in GL^+$, on a

1.0.7. $$S_{n,f}(\omega_1, \omega_2) = \sum_{\ell \in \frac{1}{N}L/L} g(\ell) E_n^*(\ell, L)$$

avec $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$,

1.0.8. $$E_n^*(\ell, L) = \sum (\ell+\omega)^{-n} ,$$

somme sur les $\omega \in L$ tels que $\ell+\omega \neq 0$ si $n \geq 3$ et variante usuelle (cf. [We] chap. VIII) si $n=1$ ou 2 et

1.0.9. $$g\left(\frac{a\omega_1+b\omega_2}{N}\right) = \frac{1}{N} \sum_{b=0}^{N-1} f(n,b) \exp -\frac{2\pi i a n}{N} .$$

1.1. - LE RESULTAT

Introduisons d'abord trois involutions.

① Sur $D = \mathbb{N} \cap [1, p^2]$. A n on associe $n^* \in D$ tel que $n^* + pn \equiv p+1 \bmod p^2-1$. On précise par $1^* = p^2$ et $(p^2)^* = 1$.

② Sur B^G . A f on associe $f^\#$ définie par

$$f^\#(a,b) = f(bp, \frac{a}{p}) \ .$$

③ Sur $\mathbb{C}^G$, en reprenant les notations de 1.0.9. et en identifiant G et $\frac{1}{N} L/L$. A g , reliée à f par 1.0.9, on associe $g^\natural$, reliée à $f^\#$, par

$$g^\natural(\ell) = \frac{1}{N} \sum_{\ell'} g(\ell')\, e_N(\ell', \ell)^p \ ,$$

où e_N est relié au déterminant dans la base ω_1 , ω_2 de L :

$$e_N(\ell', \ell) = \exp 2\pi i N \det(\ell', \ell) \ .$$

Désignons par $\mathcal{O}$ l'anneau des entiers d'une extension finie de $\mathbb{Q}$ et $\mathcal{O}_{(p)} = \mathcal{O} \otimes \mathbb{Z}_{(p)}$. A $n \in D$, on associe $b_n \in \mathbb{Z}_{(p)}$ comme dans [Rob] ; écrivons n sous la forme

1.1.1. $n = k + \nu(p-1)$, $k \in [1, p]$;

si $n \in D$ et $n < pk$, $b_n = \dfrac{\nu!}{(p-k+\nu)!}$, si $n \geq pk$, $b_n = 1/b_{n^*}$.

1.1.2. THEOREME. - Soit $\mathcal{T} = (E, \omega, \beta)$ un triplet défini sur $\mathcal{O}_{(p)}$ tel que $E_{p-1}(\mathcal{T})$ soit dans $p \cdot \mathcal{O}_{(p)}$. Alors,

1.1.2.1. $S_{n,f}(\mathcal{T}) \in \mathcal{O}_{(p)}$ pour $n \in D$.

1.1.2.2. $\left[S_{n^*,f} - b_n \left(\dfrac{N E_{p+1}}{12} \right)^{\frac{n^*-n}{p+1}} S_{n,f^\#} \right] (\mathcal{T}) \in p\mathcal{O}_{(p)}$,

si n n'est pas congru à $0, 1, 2, 3, p-2$ mod $p-1$ ou si $n = 1$.

1.2. - PRINCIPE DE LA DEMONSTRATION

La démonstration a la même structure que celle de [Rob], mais l'introduction d'un niveau nécessite des raisonnements modulaires (i.e. en termes de problèmes de modules) pour acquérir des renseignements sur $M = M(\mathbb{Z}_p)$; si $N = 1$, M est simplement une algèbre de polynômes à deux indéterminées.

Soient $\Lambda = E_{p-1}/p$ et $L = M[\Lambda]$. Posons $U = \operatorname{Spec} M[1/\Delta]$, $\mathcal{U} = \operatorname{Spec} L[1/\Delta]$. Soit X (resp. X_1) la courbe modulaire projective (resp. le champ algébrique) liée au problème de modules pour les couples (E, β) (resp. les courbes elliptiques E) : U apparaît comme isomorphe à $X \otimes_{X_1} U_1$, U_1 étant défini comme U mais avec $N = 1$; $\mathcal{U}$ est l'éclaté de Néron de U le long du lieu supersingulier dans la fibre en p. Cette interprétation fournit des propriétés de lissité. Par ailleurs, U et $\mathcal{U}$ représentent des foncteurs en $\mathbb{Z}_p$-algèbres :

$$U(R) = \operatorname{Hom}_{alg}(M[1/\Delta], R) \simeq \left\{\begin{array}{l}\text{classes d'isomorphie des } \mathcal{J} \text{ définis} \\ \text{sur } R\end{array}\right\}$$

$$\mathcal{U}(R) = \operatorname{Hom}_{alg}(L[1/\Delta], R) \simeq \left\{\begin{array}{l}\text{couples } ([\mathcal{J}], r) \text{ avec } [\mathcal{J}] \text{ classe} \\ \text{d'isomorphie de } \mathcal{J}, \ \mathcal{J} \text{ défini sur } R \\ \text{et } r \in R \text{ tel que } r \cdot p = E_{p-1}(\mathcal{J})\end{array}\right\} .$$

Soient B (resp. Ω) l'anneau des entiers d'une extension finie (resp. maximale) non ramifiée de $\mathbb{Q}_p$ et K son corps des fractions. Les considérations précédentes permettent de démontrer un critère pour qu'une forme soit dans L.

1.2.1. THEOREME. - Soit $f \in M \otimes_{\mathbb{Z}_p} K$. Pour que f soit dans $L \otimes_{\mathbb{Z}_p} B$, il faut et il suffit que pour tout $\mathcal{J} \in \mathcal{U}(\Omega)$, $f(\mathcal{J})$ soit dans Ω (a priori $f(\mathcal{J})$ est dans le corps des fractions de Ω).

Pour démontrer 1.1.2.1, il suffit de vérifier que $f \to S_{n,f}$ définit une application de $\mathbb{Z}_p^G$ dans L, ce qui peut se vérifier au moyen de 1.2.1.

Pour 1.1.2.2., on gradue L par le poids en donnant à Λ le poids $p-1$ et on filtre $\bar{L}_n$, réduction modulo p de la composante de poids n, en posant (cf. 1.1.1) :

$$\bar{L}_n^{(t)} = \left\{ f = \sum_t^{\nu} a_i \Lambda^{\nu-i} \ , \ a_i \in M_{k+i(p-1)} \right\} \bmod p \ .$$

Pour démontrer que

$$\varphi_n(f) = S_{n^*,f} - b_n \left(\frac{NE_{p+1}}{12}\right)^{\frac{n^*-n}{p+1}} S_{n,f}$$

est dans pL_{n^*}, on montre que

a) $\varphi_n(f) \in \bar{L}_{n^*}^{(k+1)}$;

b) $f \to \varphi_n(f)$ définit une application $\mathcal{H}$-linéaire où $\mathcal{H}$ désigne une algèbre d'opérateurs de Hecke, ceci pour une action convenable de $\mathcal{H}$ sur $\mathbb{Z}_p^G$.

c) $\mathrm{Hom}_{\mathcal{H}}(\mathbb{Z}_p^G, \bar{L}_{n^*}^{(k+1)}) = 0$.

Les restrictions importantes dans 1.1.2.2 s'introduisent dans c) : en effet, la méthode consiste comme dans [Rob] à diminuer les indices en considération en utilisant l'application

$$M_n/E_{p-1} M_{n-p+1} \longrightarrow M_{n+p+1}/E_{p-1} M_{n+2}$$

définie par la multiplication par E_{p+1}. La difficulté est que l'application précédente ne définit un isomorphisme en caractéristique p que pour n assez gros.

2. - CRITERE DE KUMMER SUPERSINGULIER

2.0. - LE PROBLEME

Soient K un corps quadratique imaginaire tel que p reste premier dans K et F/K une extension abélienne de degré premier à p de groupe de Galois Δ. Désignons par $Cl(F)$ le groupe des classes d'idéaux de F. On souhaite discuter la condition

2.0.1. $p \nmid |Cl(F)|$.

Pour ceci introduisons $\mathcal{O}(F)$ l'anneau des entiers de F et C son groupe d'unités elliptiques. On a alors ([G-R]), si p ne divise pas le nombre de classes de K, ce que nous supposerons désormais :

2.0.2. THEOREME. - La condition 2.0.1 est équivalente à

2.0.3. $p \nmid [\mathcal{O}(F)^* : C]$.

2.1. - TRADUCTION MULTIPLICATIVE SEMI-LOCALE

On suppose que F contient le groupe μ_p des racines $p^{\text{ièmes}}$ de l'unité. Pour toute place w de F au-dessus de p, on note F^w le complété et $\mathcal{O}(F^w)$ son anneau d'entiers. On introduit le groupe des unités semi-locales $U = \prod_w \mathcal{O}(F^w)^*$. On dit que $\alpha \in \mathcal{O}(F^w)^*$ est primaire si l'extension $F^w(\sqrt[p]{\alpha})/F^w$ est non ramifiée. Ceci permet d'introduire le produit U_{pr} des groupes d'unités locales primaires $\mathcal{O}(F^w)^*_{pr}$. On a un homomorphisme Δ-équivariant :

$$C/C^p \xrightarrow{\Lambda} U/U_{pr} .$$

2.1.1. PROPOSITION. - La condition 2.0.3 est équivalente à

2.1.2. Λ est injective.

En effet, Λ se factorise en $C/C^p \xrightarrow{\Lambda_1} \mathcal{O}(F)^*/\mathcal{O}(F)^{*p} \xrightarrow{\Lambda_2} U/U_{pr}$. 2.0.1 implique l'injectivité de Λ_2 (théorie de Kummer) et 2.0.3 est équivalente à la surjectivité ou l'injectivité de Λ_1. 2.1.1 résulte donc de 2.0.2.

2.2. - TRADUCTION ADDITIVE SEMI-LOCALE

2.2.0. Notons $\mathcal{O}_p(F)$ le complété p-adique de $\mathcal{O}(F)$. Nous allons construire un $\mathbb{Z}_p[\Delta]$-isomorphisme

$$\delta : U/U_{pr} \longrightarrow \mathcal{O}_p(F)/p\mathcal{O}_p(F) .$$

Choisissons une place v de F au-dessus de p et notons $\Delta^v \subset \Delta$ son groupe de décomposition. Par extension des scalaires, il suffit de construire

$$\delta^v : \mathcal{O}(F^v)^*/\mathcal{O}(F^v)^*_{pr} \longrightarrow \mathcal{O}(F^v)/p\mathcal{O}(F^v) .$$

Si F <u>a été choisie assez grande</u>, F^v contient une uniformisante t telle que

2.2.0.1. $t^{p^2-1} = -p\epsilon$,

ϵ étant une unité de K^v, le complété de K. Soit $u \in \mathcal{O}(F^v)^*$. On représente u sous la forme $u = f_u(t)$ où $f_u(t) \in \mathcal{O}(F_0^v)[[T]]^*$ (avec $\mathcal{O}(F_0^v)$ anneau des entiers de F_0^v, la sous-extension non ramifiée maximale de F^v/K^v). Soit $Frob \in Gal(F_0^v/\mathbb{Q}_p)$ l'automorphisme de Frobenius. On le fait agir sur $\mathcal{O}(F_0^v)[[T]]$ de façon naturelle sur les coefficients et par $T \to T^p$. Si $h \in \mathcal{O}(F_0^v)[[T]]^*$ s'écrit $h(T) = h(0)[1+g(T)]$, avec $g(T) \in T\mathcal{O}(F_0^v)[[T]]$, on prolonge le logarithme p-adique en posant

$$\log h(T) = \log h(0) + \sum_{i \geq 1} (-1)^{i-1} \frac{g(T)^i}{i} .$$

Ceci permet de définir la série $\ell_u(T)$ par

2.2.0.2. $$\ell_u(T) = \sum_{m \geq 0} \ell_m(u)\, T^m = \frac{1}{p} \log \frac{f_u(T)^p}{Frob\, f_u(T)} ,$$

en fait dans $\mathcal{O}(F_0^v)[[\ T]]$. On introduit alors l'opérateur ∇ par $\nabla x = \mathrm{Frob}\,(\varepsilon\,.\,x)$ si $x \in F_0^v$. Pour $n \in \mathbb{Z}$, on pose $f(n) = \frac{n}{p} + p^2 - 1 \in \mathbb{Q}$; f^i désigne l'application itérée i fois. On introduit (*) alors pour $n \in [0, p^2-2]$, n entier

$$\delta_n(u) = \sum_{i=0}^{\infty} \nabla^i \ell_{f^i(n)}(u) ,$$

avec la convention que $\ell_x(u) = 0$ si $x \notin \mathbb{N}$, ce qui fait que la somme précédente contient au plus trois termes ; l'intérêt de $\delta_n(u)$ provient de son indépendance du choix de f_u représentant u . Finalement, on pose

2.2.0.3. $\delta^v(\bar{u}) =$ classe de $\sum \delta_n(u)\, t^n$ modulo p ,

où $\bar{u}$ désigne la classe de u .

2.2.0.4. THEOREME. - <u>L'application</u> δ <u>est un</u> $Z_p[[\Delta]]$ <u>-isomorphisme</u>.

En effet, on vérifie en utilisant les unités $1-\alpha t^n$, $\alpha \in \mathcal{O}(F^v)$ que δ^v est surjective et on compte les dimensions. Quant à l'action de Δ^v , on note qu'en fait $\Delta^v \simeq I \times J^v$, avec $I = \mathrm{Gal}(F^v/F_0^v) \simeq \mathrm{Gal}(K^v(t)/K^v)$ et $J^v = \mathrm{Gal}(F_0^v/K^v)$. L'action de I sur les coefficients des séries ci-dessus est triviale et envoie t sur ηt avec η racine de 1 d'ordre p^2-1 , $\eta \in K^v$. L'action de J^v se fait uniquement sur les coefficients.

Pour étudier l'image de C/C^p par Λ nous sommes donc amenés, via δ , à analyser plus en détail la structure de $\mathcal{O}_p(F)/p\mathcal{O}_p(F)$.

2.2.1. Bases d'entiers : soit $\alpha \in \mathcal{O}(F_0^v)$, engendrant une base normale sur $\mathcal{O}(K^v)$. Introduisons $\alpha' = \sum_0^{p^2-2} t^n$ et $\beta = \alpha\alpha'$.

(*) d'après une lettre de G. Henniart à G. Robert ; cependant la numérotation des indices était inadaptée à l'action de Δ^v .

2.2.1.1. LEMME. - L'élément β est une base normale de $\mathcal{O}(F^v)$ sur $\mathcal{O}(K^v)$. Par extension des scalaires, β considéré dans $\mathcal{O}_p(F)$ en est une base normale sur $\mathcal{O}_p(K) = \mathcal{O}(K^v)$.

Démonstration. Soit $x \in \mathcal{O}(F^v)$: x s'écrit sous la forme

$$x = \sum x_{j,n}\, j(\alpha) t^n ,$$

somme sur les $j \in J^v$ et les $n \in [0, p^2-2]$, avec $x_{j,n} \in \mathcal{O}(K^v)$. Désignons par ω le caractère sur I^v tel que $\forall i \in I^v$, $i(t) = \omega(i)\, t$ alors

$$t^n = \frac{1}{p^2-1} \sum_{i \in I} \omega(i)^{-n} i(\alpha') ,$$

ce qui montre que x s'exprime comme combinaison linéaire à coefficients dans $\mathcal{O}(K^v)$ des conjugués de β .

Pour discuter l'injectivité de Λ , il est naturel de découper le problème grâce à l'action de $\mathbb{Z}_p[\Delta]$. Considérons φ un caractère de Δ défini et irréductible sur $\mathbb{Q}_p$, clôture algébrique de $\mathbb{Q}_p$ contenant F^v , φ non trivial ; on note Φ (resp. Φ_1, resp. Φ_p) la somme des conjugués de φ sur $\mathbb{Q}_p$ (resp. de φ sur K^v , resp. de φ^p sur K^v) . Deux cas peuvent se produire :

1) $K^v \subset \mathbb{Q}_p(\varphi(\Delta))$, alors φ et φ^p ne sont pas conjugués sur $\mathbb{Q}_p$ et $\Phi = \Phi_1 + \Phi_p$, $\Phi_1 \neq \Phi_p$.
2) $K^v \not\subset \mathbb{Q}_p(\varphi(\Delta))$, φ et φ^p sont alors conjugués sur $\mathbb{Q}_p$ et $\Phi = \Phi_1 = \Phi_p$.

Dans tous les cas φ définit par linéarité un isomorphisme

2.2.1.2. $$e_{\Phi_1} \mathcal{O}(K^v)[\Delta] \xrightarrow{\varphi}_{\sim} \mathcal{O}(K^v)[\varphi(\Delta)] ,$$

e_{Φ_1} désignant l'idempotent relatif à Φ_1 dans $\mathcal{O}(K^v)[\Delta]$. Soit $x \in \mathcal{O}_p(F)$: on peut écrire $x = X\beta$ avec $X \in \mathcal{O}(K^v)[\Delta]$. Pour calculer $\varphi(X)$ au moyen de x , on utilise la résolvante :

$$T_\varphi(x) = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \varphi(\sigma)^{-1} (\sigma x)_v ,$$

où $(\sigma x)_v$ désigne la composante sur $\mathcal{O}(F^v)$ de $\sigma x \in \mathcal{O}_p(F) = \prod_w \mathcal{O}(F^w)$.
On démontre facilement le résultat suivant où $n \in [0, p^2-2]$ est défini par $\varphi(i) = \omega^n(i)$ si $i \in I$.

2.2.1.3. LEMME. - L'élément $T_\varphi(x)$ ne diffère de $\varphi(X)\cdot t^n$ que par une unité de $\bar{\mathbb{Q}}_p$ indépendante de x .

Notons n' l'entier n relatif à φ^p ; on a :

2.2.2. PROPOSITION. - La condition 2.0.1 est équivalente à

2.2.3. Pour tout u dans C mais non dans C^p et pour tout φ comme plus haut, $\varphi \neq 1$, p ne divise pas simultanément $T_\varphi(\delta \wedge u)\cdot t^{-n}$ et $T_{\varphi^p}(\delta \wedge u)\cdot t^{-n'}$.

Remarquons qu'il suffit, par 2.2.1.2, de ne considérer qu'un caractère par classe de conjugaison sur $\mathbb{Q}_p$. De plus si φ rentre dans le cas 2) la condition se simplifie en $p \nmid T_\varphi(\delta \wedge u)\cdot t^{-n}$.

2.3. - APPLICATION AUX UNITES ELLIPTIQUES

2.3.1. Choix de l'uniformisante t . Soit E une courbe elliptique définie sur le corps de Hilbert H de K , admettant bonne réduction en p et ayant $\mathcal{O}(K)$ comme anneau de multiplications complexes ; on note Ω_∞ sa période réelle > 0 . On considère $\hat{E}$ le groupe formel associé sur le complété $\mathcal{O}(K^v)$ de $\mathcal{O}(H)$ en v ; ainsi le schéma formel $\hat{E}$ est isomorphe à $\mathrm{Spf}\, \mathcal{O}(K^v)[[T]]$ et on peut faire en sorte que "la" différentielle invariante soit de la forme $h(T^{p^2-1})dT$ avec $h(T) \in \mathcal{O}(K^v)[[T]]$, $h(0) = 1$.
On choisit alors pour t la valeur de T en un point de p-torsion sur $\hat{E}$.
La formule 2.2.0.1 résulte alors du théorème de préparation de Weierstrass appliqué dans $\mathcal{O}(K^v)[[T^{p^2-1}]]$.

2.3.2. Choisissons φ comme en 2.2.1. La théorie du corps de classes nous permet d'identifier φ à un caractère de Dirichlet sur le groupe des idéaux de K. Si le conducteur de φ est $\mathfrak{g}_1 = \mathfrak{g}$ ou $\mathfrak{g}\mathfrak{p}$ (avec $\mathfrak{g}$ premier à $\mathfrak{p}$), on dit que φ est de type modulo p égal à n si pour tout $a \in \mathcal{O}(K)$ congru à 1 modulo $\mathfrak{g}$ on a $\varphi(a) \equiv a^n \bmod \mathfrak{p}$: l'entier n coïncide avec celui de 2.2.1 d'après les théories de la multiplication complexe et du corps de classes.

Avec les notations de [Gi] 1.1, 1.2 et 1.4, on introduit

$$b_n(\alpha) = 12(-1)^{n-1} \sum \alpha(\mathfrak{A}) E_n^*(\rho(\mathfrak{g}), \mathfrak{A}^{-1}) \Omega_\infty^{-n} \quad \text{si} \quad n > 0$$

$$b_0(\alpha) = \frac{1}{p} \log \theta(\rho(\mathfrak{g}), \alpha)^{p-\mathrm{Frob}} \quad \text{si} \quad \mathfrak{g} \neq 1$$

$$\frac{1}{p} \log \theta(\bar{\alpha})^{p-\mathrm{Frob}} \quad \text{si} \quad \mathfrak{g} = 1 \ ;$$

ici log désigne toujours le logarithme p-adique. On a posé $\bar{\alpha} = \sum \alpha(\mathfrak{A}) \mathfrak{A}^{-1}$ de sorte que la loi de réciprocité s'explicite par $[\mathfrak{B}, H/K]\, \theta(\bar{\alpha}) = \theta(\overline{\alpha\mathfrak{B}})$. Compte tenu de la définition de δ_n et de la différence entre T et z, paramètres sur $\hat{E} \otimes K^v$, on définit

$$\mathcal{E}_n(\alpha) = b_n(\alpha) \quad \text{si} \quad n = 0 \quad \text{ou} \quad (n,p) = 1$$

$$\mathcal{E}_n(\alpha) = \left[\frac{b_{kp}(\alpha) - \mathrm{Frob}\, b_k(\alpha)}{k\,p}\right] + \mathrm{Frob}\left[\epsilon \frac{b_{k+p^2-1}(\alpha)}{k+p^2-1} - \frac{b_k(\alpha)}{p}\right] \quad \text{si} \quad n = kp,\ k > 1.$$

D'après 2.2.0, $\mathcal{E}_n(\alpha) \in \mathcal{O}_p(H_{\mathfrak{g}})$: si $n = kp$, $k > 1$ les deux crochets sont déjà dans $\mathcal{O}_p(H_{\mathfrak{g}})$ (cf. [Rob] lemme 16 pour le premier) ; pour φ comme en 2.3.2 et n son type modulo p, on pose

$$B_\alpha(\varphi) = \sum \varphi(\mathfrak{B})^{-1} \mathcal{E}_n(\alpha\mathfrak{B}) \ ,$$

somme prise sur un système de représentants du groupe des classes de rayon $\mathfrak{g}$ premiers à $\mathfrak{p}$ et au conducteur de E. En notant que $\theta(z, \alpha\cdot(b)) = \theta(z \cdot b^{-1}, \alpha)$, que $b\rho(\mathfrak{g})$ et $\rho(\mathfrak{g})$ définissent le même point de torsion sur E pour $b \equiv 1 \bmod \mathfrak{g}$ et que $[b]\,t = [\omega(b)]\,t = \omega(b)t$ (ω désigne le caractère de Teichmuller dans K^v) on obtient deux expressions pour l'unité $\theta(\rho(\mathfrak{g}\mathfrak{p}), \alpha b)$, on en déduit que pour tout b dans $\mathcal{O}(K)$ congru à 1 mod $\mathfrak{g}$,

on a $\varepsilon_n(\alpha b) = \omega(b)^n \varepsilon_n(\alpha)$ si bien que $B_\alpha(\psi)$ ne dépend pas modulo p du choix des $\mathfrak{B}$.

2.3.2.1. LEMME. - Soit x un générateur de l'idéal de Ω engendré par les sommes $\sum \alpha(\mathfrak{A})\varphi(\mathfrak{A})$, $\alpha \in J_{\mathfrak{g}}$, cf[Gi] ; on peut prendre $x = p$ si φ est le caractère de Dirichlet χ décrivant l'action galoisienne sur les racines $p^{\text{ièmes}}$ de l'unité et $x = 1$ sinon.

Ceci résulte de la définition de $J_{\mathfrak{g}}$ (réécrite sous forme d'une suite exacte) et du lemme A-1 de [G-R] .

Posons $B(\varphi) = B_\alpha(\varphi)\,[\sum \alpha(\mathfrak{A})\,\varphi(\mathfrak{A})/x]^{-1}$ où α est choisi tel que le crochet soit $\not\equiv 0 \bmod p$; alors $B(\varphi) \in \Omega$ est indépendant modulo p du choix de α .

En notant que $e_\Phi(C/C^p)$ (e_Φ idempotent évident) est engendré à partir des unités $\theta(\rho(\mathfrak{g}_1), \alpha)$ (ou $\theta(\bar{\alpha})$ si $\mathfrak{g}_1 = 1$) le calcul de T_φ conduit à l'énoncé suivant. Pour $\varphi = \chi$, on y choisi un représentant u de $\delta_{p+1}(\zeta_p)$, $\zeta_p^p = 1$, $\zeta_p \neq 1$.

2.3.2.2. THEOREME. - Soient φ et Φ comme en 2.2.1, $\varphi \neq \chi$ (resp. $\varphi = \chi$) . La restriction de Λ à $e_\Phi(C/C^p)$ est injective si et seulement si $B(\varphi)$ et $B(\varphi^p)$ n'appartiennent pas à $p\Omega$ simultanément (resp. si $(\mathrm{Frob}\, u)\cdot B(\chi) - u\cdot \mathrm{Frob}\, B(\chi)$ n'appartient pas à $p\Omega$).

2.4. - INVOLUTION DE LEOPOLDT

Pour φ comme ci-dessus l'involution de Leopoldt associe $\tilde{\varphi} = \chi\varphi^{-1}$. On la modifie en introduisant $\varphi^*(\mathfrak{A}) = \tilde{\varphi}(\bar{\mathfrak{A}})$, i.e. en composant avec la conjugaison complexe. Ceci respecte les conjugaisons entre caractères sur $\mathbb{Q}_p$ et K^v , de plus $(\varphi^p)^* = (\varphi^*)^p$. On peut donc définir Φ^* , Φ_1^* , Φ_p^* en remplaçant φ par φ^* . Les résultats ne dépendent que de Φ . Si F est une extension galoisienne sur $\mathbb{Q}$, on déduit de [Leo] le résultat suivant :

2.4.0. PROPOSITION. - Les dimensions sur $\mathbb{F}_p$ de $e_\Phi[Cl(F)/Cl(F)^p]$ et $e_{\Phi^*}[Cl(F)/Cl(F)^p]$ diffèrent au plus de $\Phi(1)$.

Comme il est naturel de se demander pour $\varphi \neq \chi$ et 1 :

2.4.1. (Φ) QUESTION. - Peut-on renforcer les résultats précédents par l'équivalence $e_\Phi[Cl(F)/Cl(F)^p] \neq 0 \Leftrightarrow B(\varphi)$ et $B(\varphi^p) \in p\Omega$?

Un optimisme naif incite à renchérir sur 2.4.0 :

2.4.2. (Φ) QUESTION. - A-t-on l'égalité

$$\dim e_\Phi[Cl(F)/Cl(F)^p] = \dim e_{\Phi^*}[Cl(F)/Cl(F)^p] \ ?$$

On a donc un diagramme

$$\begin{array}{ccc} e_\Phi[Cl(F)/Cl(F)^p] \neq 0 & \overset{2.4.1\ (\Phi)\ ?}{\Longleftrightarrow} & B(\varphi) \text{ et } B(\varphi^p) \in p\Omega \\ \Big\updownarrow \ 2.4.2\ (\Phi)\ ? & & \Big\updownarrow \ 2.4.3\ (\varphi) \text{ et } 2.4.3\ (\varphi^p)\ ? \\ e_{\Phi^*}[Cl(F)/Cl(F)^p] \neq 0 & \overset{2.4.1\ (\Phi^*)\ ?}{\Longleftrightarrow} & B(\varphi^*) \text{ et } B(\varphi^{*p}) \in p\Omega \ , \end{array}$$

avec

2.4.3 (φ) QUESTION. - Les conditions $B(\varphi)$ et $B(\varphi^*)$ sont-elles équivalentes ?

Le théorème suivant qui se déduit de 1.1.2, cf. 1.0.7, répond partiellement ; n y désigne le type modulo p de φ : celui de φ^* est n^* .

2.4.4. THEOREME. - La réponse à 2.4.3 (φ) est positive si n vérifie toutes les conditions :

2.4.4.1. $n \not\equiv 0, 1, 2, 3, p-2 \mod p-1$

2.4.4.2. $p \nmid n$

2.4.4.2*. $p \nmid n^*$ (ou de façon équivalente $n \geq p+1$) .

Remarquons que la congruence $n+n^* \equiv 2 \mod p-1$ montre l'invariance de 2.4.4.1 par $n \to n^*$.

BIBLIOGRAPHIE

[Gi] GILLARD R. - Unités elliptiques et fonctions L p-adiques, Sém. Delange-Pisot-Poitou, pp. 99-122. Birkhaüser : Boston-Basel-Stuttgart, 1981.

[G-R] GILLARD R. et ROBERT G. - Groupes d'unités elliptiques, Bull. Soc. Math. France, 107 (1979), 305-317.

[Katz] KATZ N.M. - p-adic interpolation of real analytic Eisenstein series, Ann. of Math., 104 (1976), 459-571.

[Leo] LEOPOLDT H.W. - Zur Strucktur der l-klassengruppe galoisscher Zahlkörper, J. rein. u. and Math., 199 (1958), 165-174.

[Rob] ROBERT G. - Congruences entre séries d'Eisenstein dans le cas super-singulier, Inv. Math. 61 (1980), 103-158.

[We] WEIL A. - Elliptic functions according to Eisenstein and Kronecker, Springer, Berlin-Heidelberg-New-York, 1976.

- o -