Astérisque

PH. CASSOU-NOGUÈS
M. J. TAYLOR

Fonctions elliptiques et génération d'anneaux d'entiers

Astérisque, tome 147-148 (1987), p. 49-70
<http://www.numdam.org/item?id=AST_1987__147-148__49_0>

Société Mathématique de France
Astérisque 147-148 (1987), p.49-70.

FONCTIONS ELLIPTIQUES ET GÉNÉRATION D'ANNEAUX D'ENTIERS

Ph. CASSOU-NOGUES M.J. TAYLOR

INTRODUCTION :

Pour tout corps de nombres L on désigne par O_L son anneau d'entiers.

Soit N une extension abélienne, de degré fini d'un corps de nombres M, de groupe de Galois Γ. On peut considérer O_N d'une part comme O_M-algèbre et d'autre part comme module galoisien, c'est-à-dire comme module sur l'ordre associé $\wedge_{N/M}$ défini par :

$$\wedge_{N/M} = \{\lambda \in M[\Gamma] \mid \lambda O_N \subset O_N\}$$

C'est un problème central de la théorie algébrique des nombres que de construire un générateur de N sur M. Lorsque l'on sait résoudre ce problème pour l'extension (N/M), on peut se poser le problème analogue pour les anneaux d'entiers :

(i) O_N est-il une O_M-algèbre monogène et peut-on dans ce cas construire un élément θ tel que $O_N = O_M[\theta]$?
(ii) O_N est-il un $\wedge_{N/M}$-module libre et peut-on dans ce cas construire un élément ω tel que $O_N = \wedge_{N/M} \cdot \omega$?

Lorsque $M=\mathbb{Q}$ le théorème de Kronecker-Weber permet de se ramener aux extensions cyclotomiques. La réponse à la question (i) est donnée dans ce cas par le résultat classique :

Théorème 1 - *Soit f un entier >0, ξ_f une racine primitive f-ième de 1 et N (resp. N^+) l'extension $\mathbb{Q}(\xi_f)$ (resp. $\mathbb{Q}(\xi_f+\xi_f^{-1})$). Alors :*

(i) $O_N = \mathbb{Z}[\xi_f]$
(ii) $O_{N^+} = \mathbb{Z}[\xi_f+\xi_f^{-1}]$

La réponse à la question (ii) est fournie par le théorème suivant de Léopoldt, [L] :

Théorème 2 - *Soit* N *une extension abélienne finie de* $\mathbb{Q}$, *de groupe de Galois* Γ. *Alors* O_N *est un* $\wedge_{N/\mathbb{Q}}$*-module libre et l'on a l'égalité :*

$$O_N = \wedge_{N/\mathbb{Q}} \cdot T_N$$

où T_N *est décrit à partir des sommes de Gauss de caractères de* Γ.

Depuis la fin du siècle dernier on sait décrire les extensions abéliennes d'un corps quadratique imaginaire. C'est la théorie de la multiplication complexe. Par contre peu de résultats sur la génération des anneaux d'entiers étaient connus. Le but de cet article est d'étudier les problèmes (i) et (ii) pour certaines extensions abéliennes d'un corps quadratique imaginaire et de développer une "théorie de la multiplication complexe entière". Nos références sont [T_3], [T_4], [T_5] et [CN-T].

Plus précisément nous considérons un corps quadratique imaginaire K, de discriminant $d_K < -4$ dans lequel 2 est décomposé. Nous fixons un idéal Ω de O_K et un point primitif Ψ de $4O_K$-division de $\mathbb{C}/\Omega$. Pour tout idéal f nous désignons par K(f) le corps de classes de rayon f de K. Dans le §5, nous démontrons l'analogue elliptique suivant du théorème 1.

Théorème 3 - *Soient* f *un idéal impair de* O_K, α *un point primitif de* f *division de* $\mathbb{C}/\Omega$ *et* L (*resp.* L^+) *l'extension* K(4f) (*resp.* K(4).K(f)) *de* E=K(4). *Alors on a :*

(i) $O_L = O_E[T(\alpha+\Psi)]$
(ii) $O_{L^+} = O_E[T(\alpha)]$

où T *est la fonction de Fueter associée à* (Ω,Ψ) *définie en* (1-1).

Considérons maintenant un idéal premier $\mathfrak{p}$ de O_K, engendré par $\lambda \equiv \pm 1 \bmod. 4O_K$. Nous démontrons dans le §7 cet "analogue elliptique" du théorème de Léopoldt.

Théorème 4 - *Soient* r *et* m *des nombres entiers tels que* $r \geqslant m \geqslant 1$ (*resp.* $r > m \geqslant 1$) *si* $\mathfrak{p}$ *est décomposé (resp. inerte) dans* K. *Soient* N(*resp.* M) *le corps* $K(4\mathfrak{p}^{r+m})$ (*resp.* $K(4\mathfrak{p}^r)$) *et* $R_N = O_M + 2O_N$. *Alors* R_N *est un* $\wedge_{N/M}$*-module libre et, pour tout point* α *primitif de* $\mathfrak{p}^{m+r}$*-division de* $\mathbb{C}/\Omega$, *on a l'égalité :*

$$R_N = \wedge_{N/M} \cdot \frac{D(\alpha)}{D(\lambda^m \alpha)}$$

où D *est la fonction elliptique associée à* (Ω,Ψ) *définie au §1.*

Il est clair que la démonstration de ce théorème nécessite la connaissance de l'ordre associé $\wedge_{N/M}$. Par l'examen des composantes locales de cet ordre on se ramène à l'étude de l'ordre associé de certaines extensions de corps locaux obtenues par adjonction de points de division d'un groupe formel de Lubin-Tate. La description de ces ordres, ainsi que l'étude de la structure galoisienne dans cette situation, est faite dans le §6. Nos résultats sont explicites et complets. La démonstration du théorème 4 nous conduit également à étudier certaines résolvantes elliptiques d'Abel et Hermite au §4. La relation (4.7) satisfaite par ces résolvantes joue ici le rôle de la relation classique liant sommes de Gauss et conducteurs de caractères abéliens.

§ 1 - FONCTIONS DE FUETER

Ce sont les fonctions elliptiques introduites par Fueter en 1924, [F] que nous utilisons pour décrire les anneaux d'entiers.

Dans ce paragraphe nous rappelons leurs définitions et nous énonçons leurs propriétés utiles à notre étude.

Les égalités entre fonctions elliptiques que nous obtenons sont en général démontrées en vérifiant l'égalité de leurs diviseurs et en montrant qu'elles sont égales en un point "bien choisi"

Soit Ω un réseau de $\mathbb{C}$. Nous désignons par Ω_4 l'ensemble des points u de $\mathbb{C}/\Omega$ tels que $4u=0$ et $2u\neq 0$.

A tout couple (Ω,Ψ), où Ω est un réseau de $\mathbb{C}$ et Ψ un élément de Ω_4, nous associons une fonction elliptique pour Ω définie par :

$$T_\Omega(z;\Psi) = \frac{\wp_\Omega(\Psi) - \wp_\Omega(2\Psi)}{\wp_\Omega(z) - \wp_\Omega(2\Psi)} \tag{1-1}$$

et un nombre complexe

$$t_\Omega(\Psi) = \frac{12\wp_\Omega(2\Psi)}{\wp_\Omega(\Psi) - \wp_\Omega(2\Psi)} \tag{1-2}$$

où $\wp_\Omega$ est la fonction de Weierstrass associée à Ω. La fonction $T_\Omega(;\Psi)$ est par définition la fonction de Fueter associée à (Ω,Ψ).

Lorsque Ω et Ψ sont fixés, nous désignons par T la fonction $T_\Omega(;\Psi)$ et par t le nombre complexe $t_\Omega(\Psi)$.

Remarque - A chaque réseau Ω on peut associer différentes fonctions T et différents nombres complexes t correspondant aux différents choix de Ψ. Pour les applications arithmétiques le choix d'un "bon Ψ" sera important.

On déduit des propriétés de la fonction de Weierstrass que T est une fonction paire, de degré 2, et de diviseur

$$(T)=2(0)-2(2\Psi) \tag{1-3}$$

En outre on démontre que T satisfait la "formule d'inversion".

$$T(z).T(z+2\Psi)=1 \tag{1-4}$$

Il est maintenant naturel de considérer la dérivée de T. En fait, on observe qu'il est préférable d'introduire une certaine "normalisation" de cette dérivée. Nous fixons une fois pour toute une racine carrée de $\wp(\Psi)-\wp(2\Psi)$ et nous posons $\xi=z(\wp(\Psi)-\wp(2\Psi))^{1/2}$. Nous définissons la dérivée normalisée T_1 de T par :

$$T_1(z)=\frac{dT(z)}{d\xi}=\frac{dT(z)}{dz}(\wp(\Psi)-\wp(2\Psi))^{-1/2} \tag{1-5}$$

Il est immédiat que T_1 est une fonction elliptique pour Ω de degré 3. Puisqu'elle est impaire, elle s'annule aux points de 2-division de $\mathbb{C}/\Omega$ où elle est finie et l'on a :

$$(T_1)=(0)+(\sigma_1)+(\sigma_2)-3(2\Psi) \tag{1-6}$$

où σ_1 et σ_2 sont les points de 2-division de $\mathbb{C}/\Omega$ différents de 0 et de 2Ψ.

Les fonctions T et T_1 sont liées par l'équation

$$T_1^2=T(4T^2+tT+4) \tag{1-7}$$

Nous appelons (1-7) "l'équation de Fueter" du tore complexe $\mathbb{C}/\Omega$. On vérifie que le discriminant du polynôme $X(4X^2+tX+4)$ est égal à t^2-2^6.

Le quotient T_1/T est naturellement appelé dérivée logarithmique "normalisée" de T et noté D. La fonction D est elliptique pour Ω, impaire, de degré 2, et son diviseur est donné par

$$(1\text{-}8) \qquad (D) = (\sigma_1) + (\sigma_2) - (0) - (2\Psi)$$

Elle satisfait la relation

$$(1\text{-}9) \qquad D(z+\sigma_1)^2 D(z)^2 = t^2 - 2^6$$

La quantité t^2-2^6 joue un rôle important dans notre étude. On démontre de manière élémentaire [CN-T], IV, (1-18), que t^2-2^6 est racine du polynôme

$$(1\text{-}10) \qquad X^3 + 2^4.3X^2 + (2^8.3 - j)X + 2^{12}$$

où j désigne la valeur en Ω de la fonction modulaire.

Remarque - Pour un réseau Ω donné on peut montrer que t^2-2^6 ne dépend en fait que de 2Ψ. Les racines de (1-10) sont donc les nombres complexes t^2-2^6 correspondant aux 3 choix possibles de 2Ψ.

Nous terminons ce paragraphe par les formules d'addition, de différence, et de multiplication satisfaites par les fonctions de Fueter.

Proposition 1.11 - (Formule d'addition)

$$T(u+v) = \frac{[D(u)+D(v)]^2}{4(1-T(u)T(v))^2} T(u)T(v)$$

d'où l'on peut déduire :

Corollaire 1.12 - (Formule de différence)

$$(T(u)-T(v))^2 (T(u+v)-T(u-v) = T(u+v)T(u-v)T_1(u)T_1(v)$$

Pour tout entier n impair nous définissons les polynômes

$$(1\text{-}13) \qquad \begin{cases} Z_1(X) = 1 \\ Z_n(X) = \prod_{\beta}' (X - T(\beta)), \quad n > 1 \end{cases}$$

$$(1\text{-}14) \qquad \begin{cases} N_1(X)=1 \\ N_n(X)=n\prod_{\beta}{}'(X-T(\beta+2\Psi)), \quad n>1 \end{cases}$$

où β parcourt un 1/2 système des points de n-division non nuls de $\mathbb{C}/\Omega$. On a alors les résultats suivants.

Proposition 1.15 - (Formule de multiplication)

Pour tout entier impair n

$$(i) \qquad T(nu) = \frac{T(u)\ Z_n^2(T(u))}{N_n^2(T(u))}$$

(ii) Les polynômes $Z_n(X)$ *et* $N_n(X)$ *sont à coefficients dans* $\mathbb{Z}[t]$. *En outre ils vérifient les relations :*

$$X^{(n^2-1)/2}\ Z_n(1/X)=(-1)^{(n-1)/2}\ N_n(X)$$

$$Z_n(0) = (-1)^{(n-1)/2}.n\ ,\ N_n(0) = (-1)^{(n-1)/2}$$

Remarque : Pour un analogue de (1-15) lorsque n est un entier pair, on peut se reporter à [CN-T], IV, (3.3), (3.6) et (3.7).

§ 2 - VALEURS SINGULIÈRES DES FONCTIONS DE FUETER

Nous étudions le comportement arithmétique des valeurs prises par les fonctions de Fueter en des points de division dans le cas de la multiplication complexe.

On considère le corps quadratique imaginaire K comme sous-corps de $\mathbb{C}$ via un plongement choisi une fois pour toute. On considère les fonctions de Fueter associées à (Ω,Ψ) où Ω est un idéal de O_K et Ψ un élément de Ω_4. On sait que dans ce cas la valeur en Ω de la fonction modulaire est un entier algébrique. On déduit alors de (1-10) que t est un entier algébrique tel que t^2-2^6 divise 2^{12}. Ceci implique que pour tout entier $n\geq 1$ les coefficients de $Z_n(X)$ et $N_n(X)$ sont des entiers algébriques.

On déduit de (1.15) et de son analogue pour n pair que pour tout point de division α de $\mathbb{C}/\Omega$, d'ordre impair, alors $T(\alpha)$ et $T(\alpha+\Psi)$ sont des entiers algébriques et même que $T(\alpha+\Psi)$ est une unité. En utilisant l'équation de Fueter de $\mathbb{C}/\Omega$ on en déduit que $T_1(\alpha)$ et $T_1(\alpha+\Psi)$ sont des entiers algébriques.

Nous pouvons maintenant étudier de manière précise les valuations de ces entiers.

Proposition 2.1 - *Soit* $\upsilon \in O_K$ *tel que* $\upsilon \equiv 1 \bmod 2O_K$ *et soit* $\{\alpha\}$ *l'ensemble des points de* υ*-division de* $\mathbb{C}/\Omega$. *Alors :*

(i)
$$\varepsilon_\upsilon \, T(\upsilon z) = \prod_{\alpha} T(z+\alpha)$$

où
$$\varepsilon_\upsilon = \begin{cases} 1 & \text{si } \upsilon \equiv \pm 1 \bmod 4O_K \\ -1 & \text{sinon} \end{cases}$$

(ii)
$$\eta_\upsilon \, (t^2-2^6)^{\frac{(N(\upsilon)-1)}{4}} \, T_1(\upsilon z) = \prod_{\alpha} T_1(z+\alpha)$$

où η_υ *est une racine 4ième de l'unité et où* N *désigne la norme de* K *sur* $\mathbb{Q}$.

En utilisant (i) et (ii) lorsque $z \to 0$ ou $z = \Psi$ on en déduit :

Corollaire 2.2 - *Sous les hypothèses de (2.1) on a :*

(i)
$$\varepsilon_\upsilon \, \upsilon^2 = \prod_{\alpha \neq 0}^{(N(\upsilon)-1)} T(\alpha)$$

(ii)
$$\eta_\upsilon \, \upsilon (t^2-2^6)^{\frac{(N(\upsilon)-1)}{4}} = \prod_{\alpha \neq 0} T_1(\alpha)$$

(iii)
$$\eta_\upsilon (t^2-2^6)^{\frac{(N(\upsilon)-1)}{4}} = \prod_{\alpha \neq 0} T_1(\alpha+\Psi)$$

On rappelle que x et y de $\overline{\mathbb{Q}}^*$ sont dits associés lorsque xy^{-1} est une unité. On note alors $x \sim y$.

Un idéal f de O_K est primaire s'il est égal à la puissance d'un idéal premier de O_K. On dit qu'il est impair si l'on a :

$$f + 2O_K = O_K$$

On déduit de (2.1) et (2.2).

Proposition 2.3 - *Soit* f *un idéal entier et impair de* O_K *et soient* α *et* β *des points primitifs de* f*-division de* $\mathbb{C}/\Omega$. *Alors :*

(i) $\quad T(\alpha) \sim T(\beta)$

(ii) $\quad T(\alpha+\Psi) \sim 1$

(iii) *si* f *n'est pas primaire,* $T(\alpha) \sim 1$.

(IV) *si* $f=\mathfrak{p}^r$ *où* $\mathfrak{p}$ *est un idéal premier de* O_K, *dans une extension "suffisamment grande"* L *et* K, *on a l'égalité :*

$$T(\alpha)\, O_L = \prod_{\mathfrak{P}/\mathfrak{p}} \mathfrak{P}$$

où $\mathfrak{P}$ *parcourt les relèvements premiers de* $\mathfrak{p}$ *dans* L.

(V) *On suppose* $t^2-2^6 \sim 1$. *Alors* $T_1(\alpha+\Psi) \sim 1$ *et si* f *n'est pas primaire,* $T_1(\alpha) \sim 1$.

Remarque - Les propriétés satisfaites par les valeurs $T(\alpha)$ nous conduisent à les considérer comme des analogues elliptiques des éléments $1-\xi_f$ où ξ_f désigne une racine primitive f-ième de l'unité.

En examinant (2.2) (iii) et (2.3) (V) on observe que la valuation pour les idéaux premiers au-dessus de 2 des valeurs singulières de T_1 dépend de t^2-2^6. On peut déterminer explicitement le comportement de t^2-2^6 selon le choix de Ψ dans Ω_4. On exprime pour cela t^2-2^6 comme quotient de valeurs de fonctions Δ et on utilise le principe de développement en séries de Fourier des formes modulaires. On obtient en particulier le résultat suivant :

Proposition 2.4 - *Si* 2 *est décomposé dans* K *et si* Ψ *est un point primitif de* $4O_K$*-division de* $\mathbb{C}/\Omega$. *Alors :*

$$t^2-2^6 \sim 1$$

§ 3 - GÉNÉRATION DE CORPS

Soit $\mathfrak{f}$ un idéal de O_K. La théorie de la multiplication complexe, (Fueter, Hasse, Weber), permet d'obtenir des générateurs explicites de l'extension $K(\mathfrak{f})$ de K. Ces résultats nous permettent de décrire les extensions de K obtenues par adjonction des valeurs singulières des fonctions de Fueter.

Les symboles Ω et Ψ sont ceux définis aux paragraphes précédents. On désigne par $J(K)$ (resp. $U(K)$) le groupe des idéles (resp. idèles unités) de K et par $J^{\mathfrak{f}}(K)$ (resp. $U_{\mathfrak{f}}(K)$) le sous-groupe des idèles (resp. idèles unités) de K, premières avec $\mathfrak{f}$ (resp. $\equiv 1 \bmod^* \mathfrak{f}$). Le groupe $J^{\mathfrak{f}}(K)$ opère naturellement sur le groupe I_K des idéaux fractionnaires de O_K par :

$$J^{\mathfrak{f}}(K) \times I_K \to I_K$$

$$(u, \mathfrak{M}) \to u.\mathfrak{M} = (u).\mathfrak{M} \tag{3.1}$$

où (u) est le contenu de u.

En outre, si $\mathfrak{M}$ désigne un idéal de O_K, on définit une opération naturelle de $J^{\mathfrak{f}}(K)$ sur le groupe des points de $\mathfrak{f}$-division $(\mathbb{C}/\mathfrak{M})_{\mathfrak{f}}$ de $\mathbb{C}/\mathfrak{M}$ par :

$$J^{\mathfrak{f}}(K) \times (\mathbb{C}/\mathfrak{M})_{\mathfrak{f}} \to (\mathbb{C}/\mathfrak{M})_{\mathfrak{f}}$$

$$(u, \alpha) \to u.\alpha = \lambda\alpha \tag{3.2}$$

où λ est un élément de O_K choisi tel que $\lambda \equiv u \bmod^* \mathfrak{f}$. Pour tout élément u de $J^{\mathfrak{f}}(K)$ on note (u,K) l'élément du groupe de Galois de $K(\mathfrak{f})$ sur K associé à u par l'application d'Artin. Si M et N sont 2 extensions de K on désigne par $M.N$ le compositum de M et N.

Puisque $d_K < -4$ on rappelle que dans ce cas la fonction de Weber associée au réseau Ω est la fonction elliptique défini par :

$$h_\Omega(z) = -2^7 3^5 \frac{g_2(\Omega) g_3(\Omega)}{\Delta(\Omega)} \wp_\Omega(z) \tag{3.3}$$

où $g_2(\Omega) = 60 \sum_{\omega \neq 0} \omega^{-4}$, $g_3(\Omega) = 140 \sum_{\omega \neq 0} \omega^{-6}$ et $\Delta(\Omega) = g_2^3(\Omega) - 27 g_3^2(\Omega)$

On a le théorème suivant :

Théorème 3.4 - *Soit* α *un point primitif de* f*-division de* $\mathbb{C}/\Omega$. *Alors :*

(i) $h_\Omega(\alpha) \in K(f)$

(ii) Pour tout élément u *de* $J^f(K)$, *on a l'égalité :*

$$h_\Omega(\alpha)^{(u^{-1},K)} = h_{u.\Omega}(u.\alpha)$$

En utilisant la fonction de Weber on obtient les nouvelles expressions pour les fonctions de Fueter :

$$t_\Omega(\Psi) = 12 h_\Omega(2\Psi)\,(h_\Omega(\Psi) - h_\Omega(2\Psi))^{-1}$$

(3.5)
$$T_\Omega(z;\Psi) = \frac{h_\Omega(\Psi) - h_\Omega(2\Psi)}{h_\Omega(z) - h_\Omega(2\Psi)}$$

Ceci nous permet de déduire de (3.4) :

Théroème 3.6 - *Si* Ψ *est un point primitif de* $4O_K$*-division de* $\mathbb{C}/\Omega$, *alors on a l'égalité :*

$$K(t_\Omega(\Psi)) = K(4)$$

où K(4) *désigne le corps de classes de rayon* $4O_K$ *de* K.

Théorème 3.7 - *Soient* f *un idéal entier, non trivial et impair de* O_K *et* α *un point primitif de* f*-division de* $\mathbb{C}/\Omega$. *Alors*

(i) $K(4)\,(T(\alpha+\Psi)) = K(4f)$

(ii) $K(4)\,(T(\alpha)) = K(4).K(f)$

(iii) Pour tout élément u *de* $U_4(K)$ *on a l'égalité :*

$$T(\alpha)^{(u^{-1},K)} = T(u.\alpha)$$

où T *désigne la fonction de Fueter associée à* (Ω,Ψ).

On peut ici considérer les extensions $(K(4f)/K(4))$ comme les analogues des extensions cyclotomiques et les extensions $(K(4).K(f)/K(4)$ comme les analogues des sous-extensions réelles maximales de ces extensions.

On définit le polynôme ;

$$S_f(X)=\prod_{\beta}{}' (X-T(\beta))$$

où $\{\beta\}$ parcourt un 1/2 système des points primitifs de f-division de $\mathbb{C}/\Omega$. On démontre que $S_f(X)$ est un polynôme à coefficients entiers de $K(t)[X]$. Compte tenu de (3.6) c'est un polynôme de $K(4)[X]$. Le polynôme $S_f(X)$ est le polynôme minimal de $T(\alpha)$ sur $K(4)$. C'est l'analogue d'un polynôme cyclotomique.

§ 4 - FONCTIONS RÉSOLVANTES

Les problèmes de structures galoisiennes conduisent en général a étudier le comportement de certaines résolvantes de Lagrange. Dans le cas elliptique que nous considérons il en est de même. Les résultats du §6 reposent de façon essentielle sur la détermination de la décomposition en idéaux premiers de l'idéal engendré par certaines résolvantes elliptiques introduites par Abel et Hermite, [A], [H].

Les notations sont celles du paragraphe précédent. Soit $\mathfrak{p}$ un idéal premier de O_K tel que $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$. Pour tout entier $m\geqslant 1$ on désigne par $E[\mathfrak{p}^m]$ le groupe des points de $\mathfrak{p}^m$-division de $\mathbb{C}/\Omega$ et par $\hat{E}[\mathfrak{p}^m]$ le groupe des homomorphismes de $E[\mathfrak{p}^m]\to\mathbb{C}^*$.

Soit φ un élément de $\hat{E}[\mathfrak{p}^m]$, on définit la fonction résolvante associée à φ comme la fonction elliptique

$$\mathfrak{R}_m(\varphi)(z)=\sum_{u\in E[\mathfrak{p}^m]} D(z+u)\varphi(u) \tag{4.1}$$

où D est la dérivée logarithmique de la fonction T définie au §1.

Remarques -

1) Le groupe $E[\mathfrak{p}^m]$ est naturellement muni d'une structure de $O_K/\mathfrak{p}^m$-module. Plus précisemment si γ est un point primitif de $\mathfrak{p}^m$-division, alors on a l'égalité :

$$E[\mathfrak{p}^m] = (O_K/\mathfrak{p}^m).\gamma$$

Ceci nous permet de donner à la résolvante $\mathfrak{R}_m(\varphi)$ l'expression :

$$(4.2) \qquad \mathfrak{R}_m(\varphi)(z) = \sum_{w \in O_K/\mathfrak{p}^m} D(z+w\gamma)\tilde{\varphi}(w)$$

où $\tilde{\varphi}$ est le caractère additif de $O_K/\mathfrak{p}^m$ défini par :

$$\tilde{\varphi}(w) = \varphi(w\gamma), \quad \forall w \in O_K/\mathfrak{p}^m$$

2) Soient μ_{p^m} le groupe des racines p^m-ièmes de l'unité et $\langle , \rangle_{p^m}$ l'accouplement de Weil :

$$(4.3) \qquad E[p^m] \times E[p^m] \to \mu_{p^m}$$

$$(u,v) \to \langle u,v \rangle_{p^m}$$

En utilisant l'isomorphisme de dualité induit par (4.3) on vérifie qu'on peut associer à tout caractère φ de $E[\mathfrak{p}^m]$ un élément v de $E[\bar{\mathfrak{p}}^m]$, où $\bar{\mathfrak{p}}$ désigne le conjugué de $\mathfrak{p}$ dans K, tel que :

$$\varphi(u) = \langle v,u \rangle_{p^m}, \quad \forall u \in E[\mathfrak{p}^m]$$

On en déduit l'égalité :

$$(4.4) \qquad \mathfrak{R}_m(\varphi)(z) = \sum_{u \in E[\mathfrak{p}^m]} D(z+u)\langle v,u \rangle_{p^m}$$

Nous nous restreignons dorénavant aux hypothéses du §7. Nous supposons que $\mathfrak{p}$ est non ramifié dans K et totalement décomposé dans $K(4)$. L'idéal $\mathfrak{p}$ est alors engendré par un élément λ de O_K tel que $\lambda \equiv \pm 1 \bmod 4O_K$.

On montre alors le résultat suivant :

Théroème 4.5 -

(i) Si φ est le caractère unité de $E[\mathfrak{p}^m]$, alors on a :

$$D^{-1}(\lambda^m z)\ \mathfrak{R}_m(\varphi)(z)=\lambda^m$$

(ii) Si φ est un caractère de $E[\mathfrak{p}^m]$, différent du caractère unité, alors il existe un élément θ, non nul, de $E[\bar{\mathfrak{p}}^m]$, dépendant de φ, tel qu'on ait :

$$D^{-2}(\lambda^m z)\mathfrak{R}_m(\varphi)(z)\mathfrak{R}_m(\bar{\varphi})(z)=\lambda^{2m}\prod_{k=1}^{2}\frac{\wp(\lambda^m z+\sigma_k)-\wp(\theta)}{\wp(\sigma_k)-\wp(\theta)}$$

où $\bar{\varphi}$ désigne le caractère complexe conjugué de φ.

La démonstration de (i) est immédiate. Il suffit de prendre la dérivée logarithmique des 2 membres de l'égalité (2.1) (i) avec $\upsilon=\lambda^m$. La démonstration de (ii) est techniquement plus délicate, (cf [CN-T], VI (1.7)).

On démontre par la technique des formes modulaires et notamment en utilisant leur développement en séries de Fourier :

Théorème 4.6 - *Soient r et m des nombres entiers tels que $r\geq m\geq 1$ (resp. $r>m\geq 1$) si $\mathfrak{p}$ est décomposé (resp. inerte) dans K et soit α un point primitif de $\mathfrak{p}^{m+r}$-division de $\mathbb{C}/\Omega$, alors on a :*

$$\prod_{k=1}^{2}\frac{\wp(\lambda^m\alpha+\sigma_k)-\wp(\theta)}{\wp(\sigma_k)-\wp(\theta)}\sim 4(t^2-2^6)^{-1/6}$$

où θ est l'élément de $E[\bar{\mathfrak{p}}^m]$ défini en (4.5).

On déduit de (4.5) et (4.6) :

Corollaire 4.7 - *Soient r et m des nombres entiers tels que $r\geq m\geq 1$ (resp. $r>m\geq 1$) si $\mathfrak{p}$ est décomposé (resp. inerte) dans K et soit α un point primitif de $\mathfrak{p}^{m+r}$ division de $\mathbb{C}/\Omega$, alors on a :*

(i) Si φ est le caractère unité de $E[\mathfrak{p}^m]$.

$$D^{-1}(\lambda^m\alpha)\mathfrak{R}_m(\varphi)(\alpha)\ =\ \lambda^m$$

(ii) Si φ est un caractère de $E[\mathfrak{p}^m]$, différent du caractère unité

$$D^{-2}(\lambda^m\alpha)\ \mathfrak{R}_m(\varphi)(\alpha).\mathfrak{R}_m(\bar{\varphi})(\alpha)\sim 4\lambda^{2m}(t^2-2^6)^{-1/6}$$

§ 5 - STRUCTURE D'ALGÈBRE (démonstration du théorème 3)

La démonstration de ce théorème est élémentaire. Nous nous contentons d'indiquer ici sa méthode. Le lecteur peut se reporter à [CN-T], XI, pour sa démonstration complète.

On pose $\beta=\alpha+\Psi$. On déduit de (2.3)(ii) et (3.7)(i) l'inclusion :

(5.1) $\qquad O_L \supset O_E[T(\beta)]$

Soit δ_1 (resp. δ_2) le discriminant de O_L (resp. $O_E[T(\beta)]$) sur O_E. Pour démontrer (i) il suffit de vérifier l'égalité

(5.2) $\qquad \delta_1=\delta_2$

On calcule δ_1 par la théorie du corps de classe, en utilisant la "Führerdiskriminante produktformel" de Hasse.

Pour calculer δ_2 on utilise la formule d'Euler Compte tenu de (3.7)(iii) elle s'exprime par l'égalité :

$$\delta_2=N_{L/E}\ (\prod_a T(\beta)-T(a\beta)).O_E$$

où $N_{L/E}$ désigne la norme de L sur E et où $\{a\}$ parcourt un système de représentants des éléments, différents de 1, de $U_4(K)/U_{4f}(K)$.

On utilise la formule de différence (1.12) pour vérifier

$$(T(\beta)-T(a\beta))^2 \sim T(a-1)\beta$$

d'où l'on déduit :

$$\delta_2^2=N_{L/E}(\prod_a T((a-1)\beta)).O_E$$

On utilise alors (2.3) pour calculer la valuation de δ_2 en toute place qui divise f. On vérifie (5.2).

Remarque - Les résultats de ce paragraphe suggèrent une généralisation "elliptique" des résultats récents de M.N. Gras [G] sur la non monogénéité des anneaux d'entiers de sous-extensions de certaines extensions cyclotomiques.

§ 6 - STRUCTURE GALOISIENNE LOCALE

Le but de ce paragraphe est de décrire la structure galoisienne des anneaux d'entiers de certaines extensions d'un corps local obtenues par adjonction de points de division d'un groupe formel de Lubin Tate.

Les notations sont les notations standard de la théorie des groupes formels ([S]).

Soient p un nombre premier, $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$ et L une extension de $\mathbb{Q}_p$, de degré fini, contenue dans $\overline{\mathbb{Q}}_p$. On note O_L (resp. $\mathfrak{p}_L$) l'anneau (resp. l'idéal) de valuation de L et q le cardinal de son corps résiduel.

On fixe une uniformisante λ et on désigne par F un groupe de Lubin-Tate à coefficients dans O_L associé à λ. Pour toute extension M de L, d'idéal de valuation $\mathfrak{p}_M$, la relation :

$$a \underset{F}{+} b = F(a,b)$$

définit une nouvelle structure de groupe sur $\mathfrak{p}_M$ qu'on note $F(M)$.

Pour tout élément u de O_L on note $[u](X)$ l'unique endomorphisme $g(X)$ de F tel que $\left.\frac{dg(X)}{dX}\right|_{X=0} = u$.

On considére $F(\overline{\mathbb{Q}}_p)$ muni de sa structure de O_L-module induite par :

$$O_L \times F(\overline{\mathbb{Q}}_p) \to F(\overline{\mathbb{Q}}_p)$$

$$(u,a) \to a^{[u]} = [u](a) \tag{6.1}$$

Pour tout entier m on désigne par G_m le groupe des points de $\mathfrak{p}_L^m$-division de $F(\overline{\mathbb{Q}}_p)$, c'est à dire le groupe des éléments x de $F(\overline{\mathbb{Q}}_p)$, tel que

$$x^{[u]} = 0 \ , \ \forall u \in \mathfrak{p}_L^m$$

Il est clair que G_m est muni d'une structure naturelle de $O_L/\mathfrak{p}_L^m$-module.

On sait par la théorie des groupes formels de Lubin-Tate :

Théorème 6.1 -

(i) G_m *est un* O_L*-module isomorphe à* $\mathfrak{p}_L^{-m}/O_L$

(ii) Soit L_m *l'extension de* L *obtenue par adjonction des éléments de* G_m*. Alors* L_m *est une extension abélienne totalement ramifiée de* L *de degré* $q^{m-1}(q-1)$

(iii) Pour toute unité u *de* O_L *et tout élément* x *de* G_m *on a l'égalité :*

$$x^{(u^{-1},L)} = x^{[u]}$$

On fixe dorénavant des nombres entiers r et m tels que $r \geqslant m \geqslant 1$. On désigne par N(resp. M) l'extension L_{m+r} (resp. L_r) et par Γ le groupe de Galois de N sur M.

On sait par (**6.1**) que l'application d'Artin induit un isomorphisme

$$\Gamma \simeq \frac{1+\mathfrak{p}_L^r}{1+\mathfrak{p}_L^{m+r}} \tag{6.2}$$

En outre, puisque $r \geqslant m$, l'application $1+y \to y$ induit un isomorphisme

$$\frac{1+\mathfrak{p}_L^r}{1+\mathfrak{p}_L^{m+r}} \simeq \mathfrak{p}_L^r/\mathfrak{p}_L^{m+r} \tag{6.3}$$

On peut alors munir Γ de la structure de $O_L/\mathfrak{p}_L^m$-module induite de celle de $\mathfrak{p}_L^r/\mathfrak{p}_L^{m+r}$, via les isomorphismes (**6.2**) et (**6.3**).

Soit α un point primitif de $\mathfrak{p}_L^{m+r}$ division de $F(\overline{\mathbb{Q}}_p)$. Pour tout élément γ de Γ il est immédiat que $\alpha^{\gamma} -_F \alpha \in G_m$.

On en déduit un isomorphisme de Kummer :

$$\Gamma \simeq G_m$$

$$\theta : \gamma \to \alpha^{\gamma} -_F \alpha \tag{6.4}$$

On vérifie facilement que θ est un isomorphisme de $O_L/\mathfrak{p}_L^m$-module.

Pour tout entier $i \geqslant 0$ on définit l'élément σ_i de $M[\Gamma]$ par :

$$\sigma_i = \lambda^{-m} \sum_{\gamma \in \Gamma} \theta^i(\gamma)(\gamma - 1) \tag{6.5}$$

Dans [T_5] M.J. Taylor démontre :

Théorème 6.6 -

(i) $\wedge_{N/M} = O_M + \sum_{i=0}^{q^m - 2} O_M \cdot \sigma_i$

(ii) O_N ***est un*** $\wedge_{N/M}$***-module libre, de rang*** 1 ***et l'on a :***

$$O_N = \wedge_{N/M} \cdot y$$

pour tout élément y ***non nul de*** N ***de valuation*** $q^m - 1$.

Le lecteur peut se reporter à [CN-T], IX, pour une démonstration complète de ce théorème.

Remarques -

1) Lorsque $L = \mathbb{Q}_p$, $\lambda = p$ et $F(X,Y) = (1+X)(1+Y) - 1$, on a alors $N = \mathbb{Q}_p(\xi_p{}^{r+m})$ et $M = \mathbb{Q}_p(\xi_p{}^{r})$. On peut démontrer en utilisant (6.6) que $\wedge_{N/M}$ est, dans ce cas, égal à l'ordre maximal de $M[\Gamma]$.

2) Soient $s \geqslant 1$ et β un point primitif de $\mathfrak{p}_L^s$-division. On sait que le polynôme minimal de β sur L est un polynôme d'Eisenstein. On a donc l'égalité :

$$O_{L_s} = O_L[\beta]$$

§ 7 - STRUCTURE GALOISIENNE GLOBALE

Le but de ce paragraphe est d'une part d'établir quelques corollaires du Théorème 4 et d'autre part d'esquisser les différentes étapes de sa démonstration.

Par souci de simplicité nous avons supposé 2 décomposé dans K. Cette hypothèse n'est pas nécessaire. On peut se reporter à [T_4] et [CN-T], X pour le résultat le plus général.

Les notations sont celles de l'introduction et des §1 à 5 On rappelle que R_N est l'ordre de O_M dans N défini par :

$$R_N = O_M + 2O_N \tag{7.1}$$

Si $\mathfrak{q}$ est une place de M qui divise 2 alors $\mathfrak{q}$ est non ramifiée dans N et on sait par un résultat de E. Noether que O_N est localement libre en cette place sur son ordre associé. Puisqu'en toute place $\mathfrak{q}$ de M qui ne divise pas 2 les complétés de R_N et O_N en $\mathfrak{q}$ coïncident, on déduit du théorème 4.

Corollaire 7.2 - *Sous les hypothèses du théorème 4, alors* O_N *est un module localement libre de rang* 1 *sur son ordre associé.*

On pose $\Sigma = \sum_{\gamma \in \Gamma} \gamma$ et on désigne par I_N l'idéal de $\Lambda_{N/M}$ engendré par 2 et $\lambda^{-m}\Sigma$. On peut démontrer l'égalité

$$R_N = O_N \cdot I_N \tag{7.3}$$

On obtient alors comme conséquence de (7.3)

Corollaire 7.4 - *Sous les hypothèses du théorème 4, alors* O_N *est un* $\Lambda_{N/M}$*-module libre si et seulement si* I_N *est un* $\Lambda_{N/M}$*-module libre.*

Remarque - L'obstruction à ce que O_N soit un $\Lambda_{N/M}$-module libre provient donc de I_N, qui est un "analogue elliptique" des modules de Swan des algèbres de groupe.

Lorsque $\mathfrak{p}$ est décomposé dans K, le groupe Γ est cyclique. On désigne par γ un générateur de Γ. Dans ce cas on obtient :

Corollaire 7.5 - *Sous les hypothèses du théorème 4 et lorsque* $\mathfrak{p}$ *est décomposé dans* K, *alors* O_N *est un* $\Lambda_{N/M}$*-module libre de rang* 1 *et l'on a l'égalité :*

$$O_N = \Lambda_{N/M}\left(\frac{1+\gamma}{2}\right) \cdot \frac{D(\alpha)}{D(\lambda^m \alpha)}$$

Démonstration -

Nous esquissons maintenant les 3 étapes de la démonstration du théorème 4. On pose

$$a = D(\alpha)/D(\lambda^m\alpha)$$

Etape 1 - Etude de a -

Proposition 7.6 -

(i) $a \in R_N$

(ii) Pour tout idéal $\mathfrak{q}$ ***de*** N ***au dessus de*** $\mathfrak{p}$, ***la valuation de*** a ***en*** $\mathfrak{q}$ ***est égale à*** q^m-1 ***où*** q ***est égal à*** $N(\mathfrak{p})$.

En utilisant (3.7) on vérifie que $a \in N$. Puis on déduit des résultats du §2 que $a \in O_N$, vérifie $a \equiv 1 \bmod 2$ et satisfait (ii).

Si F est un corps de nombres et $\mathfrak{P}$ une place finie de F on note $F_{\mathfrak{P}}$ (resp. $O_{F,\mathfrak{P}}$) le complété de F (resp. O_F) en $\mathfrak{P}$. Si B est un O_F-module on pose :

$$B_{\mathfrak{P}} = O_{F,\mathfrak{P}} \otimes_{O_F} B$$

Si x et y sont des éléments de $\bar{\mathbb{Q}}^*$ on écrit x/y (resp. $x \sim y$) lorsque yx^{-1} est un entier (resp. une unité) en toute place au-dessus de $\mathfrak{P}$.

Pour démontrer le théorème 4 il suffit de démontrer, pour toute place finie $\mathfrak{P}$ de M, l'égalité :

(7.7) $$R_{N/M,\mathfrak{P}} = \wedge_{N/M,\mathfrak{P}} \cdot a$$

On distingue suivant les places de M.

Etape 2 - $\mathfrak{P}/\mathfrak{p}$

Puisque $\mathfrak{p}$ est impair alors $R_{N,\mathfrak{P}}=O_{N,\mathfrak{P}}$. On se ramène dans ce cas à un problème local. On observe qu'il suffit de montrer pour toute place $\mathfrak{q}$ de N au-dessus de $\mathfrak{P}$ l'égalité :

$$O_{N\mathfrak{q}}=\Lambda_{N_{\mathfrak{q}}/M_{\mathfrak{P}}}.a \tag{7.8}$$

Or l'extension $(N_{\mathfrak{q}}/M_{\mathfrak{P}})$ est une extension de corps local du type considéré dans le §6. On déduit (7.8) de (**6.6**)(ii) et (**7.6**)(ii).

Etape 3 -$\mathfrak{P}\nmid\mathfrak{p}$

On note ε le caractère unité de Γ. A tout caractère χ de Γ on associe l'idempotent e_χ de $M[\Gamma]$ défini par :

$$e_\chi = \frac{1}{|\Gamma|}\sum_{\alpha\in\Gamma}\chi(\gamma^{-1}).\gamma$$

On démontre le critére algébrique suivant :

Proposition 7.9 - *Soit* d *un élément de* R_N. *Alors pour tout idéal premier* $\mathfrak{P}$ *de* M, $\mathfrak{P}\nmid\mathfrak{p}$ *on a :*

$2 \underset{\mathfrak{P}}{/} |\Gamma|e_\chi d$ *(resp.* $1 \underset{\mathfrak{P}}{/} |\Gamma|e_\chi d$*) si* $\chi\neq\varepsilon$ *(resp.* $\chi=\varepsilon$*).*

En outre si $2\underset{\mathfrak{P}}{\sim}|\Gamma|e_\chi d$ *(resp.* $1 \underset{\mathfrak{P}}{\sim} |\Gamma|e_\chi.d$*) lorsque* $\chi\neq\varepsilon$ *(resp.* $\chi=\varepsilon$*) on a l'égalité :*

$$R_{N,\mathfrak{q}}=\Lambda_{N/M,\mathfrak{q}}.d$$

On utilise ce critère pour démontrer (7.8).

On a l'isomorphisme d'Artin :

$$U_{4\mathfrak{p}}{}^{r}(K)/U_{4\mathfrak{p}}{}^{r+m}(K) \simeq \Gamma \tag{7.10}$$

On a également l'isomorphisme de groupe :

$$U_{4\mathfrak{p}}{}^{r}(K)/U_{4\mathfrak{p}}{}^{r+m}(K) \simeq E[\mathfrak{p}^m]$$

$$u \to \frac{(u-1)}{\lambda^r}(\lambda^r\alpha) \tag{7.11}$$

A tout caractère χ de Γ on peut associer via (7.10) et (7.11) un caractère φ de $E[\mathfrak{p}^m]$ et l'on vérifie l'égalité :

$$(7.12) \qquad |\Gamma|e_\chi.a = D^{-1}(\lambda^m\alpha)\mathfrak{R}_m(\varphi)(\alpha)$$

On déduit de (4.7) et (7.9) :

$$\begin{cases} |\Gamma|e_\chi a = \lambda^m \text{ , si } \chi=\varepsilon \\ |\Gamma|e_\chi a = D^{-1}(\lambda^m\alpha)\mathfrak{R}_m(\varphi)(\alpha) \sim 2\lambda^m \text{ , si } \chi\neq\varepsilon \end{cases}$$

d'où l'égalité (7.8) dans ce cas.

BIBLIOGRAPHIE

[A] N. ABEL - Oeuvres complètes, ed. Sylow and Lie, Christiana (1881).

[CN-T] Ph. CASSOU-NOGUES - M.J. TAYLOR -Elliptic functions and Rings of integers, Birkhaüser, à paraitre.

[F] R. FUETER - Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen, 1 und 2, Leipzig - Berlin, 1924.

[G] M.N. GRAS - Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geqslant 5$, à paraitre.

[H] C. HERMITE - Extraits de 2 lettres de C. HERMITE à M. JACOBI, J. für reine angew. Math., 32 (1846).

[L] H.W. LEOPOLDT - Uber die Hauptordmung der ganzen Elementen eines abelschen Zahlkörpers, J. für reine angew. Math, 201 (1959), 119-149.

[S] J. P. SERRE - Algebraic Number Theory, ed. CASSELS et FROHLICH, 1965.

[T_1] M.J. TAYLOR - Group laws and normal bases, J. für reine angew Math., 337 (1982), 121-140.

[T_2] M.J. TAYLOR - Relative Galois module structure of rings of integers and elliptic functions, Math. Proc. Cam. Phil. Soc., 94 (1983), 389-397.

[T_3] M.J. TAYLOR - Relative Galois module structure of rings of integers and elliptic functions II, Ann. of Math, 121 (1985), 519-535.

[T_4] M.J. TAYLOR - Relative Galois module structure of rings of integers and elliptic functions III, à paraitre.

[T_5] M.J. TAYLOR - Formal groups and the Galois module structure of local rings of integers, J. für reine angew. Math, 358 (1985), 97-103.

Ph. CASSOU-NOGUES
L.A. au C.N.R.S. n°226
U.E.R de Mathématiques
Université de Bordeaux I
33405 TALENCE CEDEX
FRANCE

M.J. TAYLOR
UMIST
PO Box 88
MANCHESTER M60 1QD
ENGLAND