Journal de Théorie des Nombres de Bordeaux

Anupam Srivastav

Modules de Swan et courbes elliptiques à multiplication complexe

Journal de Théorie des Nombres de Bordeaux 2e série, tome 2, nº 1 (1990), p. 41-48

<http://www.numdam.org/item?id=JTNB_1990__2_1_41_0>

Séminaire de Théorie des Nombres,
Bordeaux **2** *(1990), 41-48*

Modules de Swan et courbes elliptiques à multiplication complexe

par ANUPAM SRIVASTAV

1. Introduction

A/ Modules de Swan

Soient G un groupe fini et $C\ell(\mathbb{Z}[G])$ le groupe des classes des $\mathbb{Z}[G]$-modules localement libres. On associe à tout entier s, premier à l'ordre G, le module de Swan

$$< s, \sigma >= s\mathbb{Z}[G] + \sigma\mathbb{Z}[G]$$

où $\sigma = \sum_{g\in G} g$.

Le module $< s, \sigma >$ est localement libre sur $\mathbb{Z}[G]$. On note $[s, \sigma]$ la classe qu'il définit dans $C\ell(\mathbb{Z}[G])$. On montre pour tous les entiers s et t premiers à l'ordre de G l'égalité dans $C\ell(\mathbb{Z}[G])$:

$$[s, \sigma] + [t, \sigma] = [st, \sigma].$$

On note $|G|$ l'ordre de G. On définit le sous-groupe de Swan de $T(\mathbb{Z}[G])$ par :

$$T(\mathbb{Z}[G]) = \{[s, \sigma] \quad / \quad (s, |G|) = 1\}.$$

C'est un sous-groupe fini de $C\ell(\mathbb{Z}[G])$ annulé par $|G|$, [Sw],[U].

THÉORÈME 1.

a) *Si G est cyclique, $T(\mathbb{Z}[G]) = \{0\}$.*
b) *Si p est un nombre premier, $p > 2$, et si G est un p-groupe, alors $T(\mathbb{Z}[G])$ est un groupe cyclique d'ordre $p^{-1}|G|$.*

Le résultat b) conjecturé par Ullom a été démontré par Taylor dans $[T_1]$, Théorème 2-5.

B/ Stucture des anneaux d'entiers

Soient L un corps de nombres et N une extension galoisienne et finie de L. On pose $\Gamma = Gal(N/L)$. Si E est un corps de nombres on note O_E

Manuscrit reçu le 23 décembre 1989

son anneau d'entiers. On définit l'ordre associé à O_N comme l'ordre de O_L dans $L[\Gamma]$

$$\Lambda_{N/L} = \{\lambda \in L[\Gamma] \quad / \quad \lambda O_N \subset O_L\}.$$

On peut considérer O_N comme module galoisien, c'est-à-dire comme module sur $\mathbb{Z}[G]$, $O_L[\Gamma]$ ou $\Lambda_{N/L}$. On utilise parfois la théorie des modules de Swan pour étudier la structure galoisienne de O_N ; c'est notamment le cas dans le théorème suivant, $[T_1]$, Théorème 3-1 démontré également par S.Chase.

THÉORÈMÉ 2. *Si l'extension (N/L) est modérément ramifiée alors O_N est un $\mathbb{Z}[G]$-module stablement isomorphe à la codifférente de N sur L.*

On verra d'autres exemples de cette méthode dans les paragraphes 2 et 3.

2. Modèle de Fueter

Soit Ω un réseau de $\mathbb{C}$. On note Ω_4 l'ensemble des points ψ de $\mathbb{C}/\Omega$ tels que $4\psi = 0$ et $2\psi \neq 0$.

Pour tout couple $(\Omega, \psi), \psi \in \Omega_4$, on définit une courbe elliptique $E_{\Omega,\psi}$, d'équation affine

$$y^2 = 4x^3 + t_{\Omega,\psi}x^2 + 4x$$

et un isomorphisme analytique de $\mathbb{C}/\Omega$ sur les points complexes de $E_{\Omega,\psi}$ donné par :

$$\begin{aligned} \mathbb{C}/\Omega \to \quad & E_{\Omega,\psi}(\mathbb{C}) \\ z \to \quad & \begin{cases} (x(z), y(z), 1) & \text{si } z \notin \Omega \\ (0,1,0) & \text{si } z \in \Omega \end{cases} \end{aligned}$$

avec $x(\psi) = 1$ et $x(2\psi) = 0$.

On dit que $E_{\Omega,\psi}$ est le modèle de Fueter associé à (Ω, ψ). On obtient par changement de coordonnées le modèle de Fueter associé à (Ω, ψ) à partir du modèle de Weierstrass associé à Ω, ([CN-T], IV). Le discriminant de la courbe elliptique $E_{\Omega,\psi}$ est donné par :

$$\Delta(E_{\Omega,\psi}) = 4(t_{\Omega,\psi}^2 - 2^6).$$

Soit K un corps quadratique imaginaire de discriminant $d_K < -4$, dans lequel 2 est décomposé. On fixe une fois pour toute un plongement de K

dans $\mathbb{C}$ et l'on considère K comme sous-corps de $\mathbb{C}$ via ce plongement. On pose $\Omega = O_K$ et on choisit ψ tel que 2ψ soit un point primitif de 2 division de $\mathbb{C}/\Omega$. Si $\mathfrak{f}$ est un idéal de O_K on note $K(\mathfrak{f})$ le corps de classes de K de rayon $\mathfrak{f}$.

Ph. Cassou-Noguès et M.J. Taylor démontrent dans [CN-T], IX, Proposition 5-4 et Théorème 5-10.

PROPOSITION 1.

a) *On a l'égalité* $K(4) = K(t_{\Omega,\psi})$.
b) $t^2_{\Omega,\psi} - 2^6$ *est une unité algébrique.*

Ainsi la courbe elliptique $E_{\Omega,\psi}$ est définie sur $K(4)$, à multiplication complexe par O_K et possède bonne réduction en dehors de 2. On fixe dorénavant (Ω, ψ) et on écrit $E(\text{resp.}\, t)$ pour $E_{\Omega,\psi}(\text{resp.}\, t_{\Omega,\psi})$.

Soit $\mathfrak{p}$ un idéal premier, non ramifié, principal de O_K, tel que $\mathfrak{p} = \lambda O_K$ avec

$\lambda \equiv \pm 1\, mod. 4O_K$. On pose :

$$N = K(4\mathfrak{p}^{r+m}), \quad L = K(4\mathfrak{p}^r), \; \Gamma = Gal(N/L)$$

avec $r \geq m \geq 1$(resp. $r > m \geq 1$) si $\mathfrak{p}$ est décomposé (resp. inerte) dans $(K/\mathbb{Q})$. On définit le nombre premier p par $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

On étudie O_N comme module sur son ordre associé $\Lambda = \Lambda_{N/L}$. Dans $[T_2]$, M.J. Taylor a démontré

THÉORÈME 3.

a) O_N *est un* Λ*-module localement libre.*
b) O_N *est libre sur* Λ *si et seulement si le module de Swan* $< 2, \sigma > \Lambda$ *est libre sur* Λ.

Ce théorème ramène donc l'étude de la structure de O_N comme Λ-module à celle de l'idéal $< 2, \sigma > \Lambda$ de Λ.

On considère deux cas :

Cas I : $\mathfrak{p}$ est décomposé dans $(K/\mathbb{Q})$.
Le groupe Γ est alors un p-groupe cyclique avec $p \neq 2$. Puisque $T(\mathbb{Z}[\Gamma]) = \{1\}$ on en déduit que $< 2, \sigma >$ est libre sur $\mathbb{Z}[\Gamma]$ et donc libre sur Λ.

Cas II : $\mathfrak{p}$ est inerte dans $(K/\mathbb{Q})$.
Le groupe Γ est non cyclique d'ordre p^{2m} et $T(\mathbb{Z}[\Gamma])$ est cyclique d'ordre p^{2m-1}, (Théorème 1). On désigne par $T(\Lambda, \mathbb{Z})$ le sous-groupe du groupe de classes $C\ell(\Lambda)$ engendré par les éléments $[s, \sigma]$ tels que $p \nmid s$.

On démontre dans $[S_2]$

PROPOSITION 2. *L'ordre du groupe $T(\Lambda, \mathbb{Z})$ divise p^{m-1}*

Ainsi si $m = 1$, l'élément $[s, \sigma]$ est trivial dans $C\ell(\Lambda)$ et, puisque Λ est commutatif, $< 2, \sigma > \Lambda$ est un Λ-module libre.

Ce résultat suggère que le module $< 2, \sigma > \Lambda$ est peut-être toujours libre sur Λ. On démontre effectivement ce résultat. Nous en esquissons maintenant la démonstration.

On note $E[p^m]$ le sous-groupe des points de E annulé par p^m. On pose $F = O_K/p^m O_K$. Les groupes Γ et $E[p^m]$ sont naturellement munis d'une structure de F-module. En fait ce sont des F-modules libres de rang 1. Soit γ (resp. α) une base de Γ (resp. $E[p^m]$) sur F.

La description de Λ comme algèbre de Hopf est explicitement donnée dans $[T_2]$,

Théorème 3, par ses composantes locales en chaque place de L. Nous rappelons cette description.

Soit $\mathfrak{P}$ est un idéal premier de O_L. Si $\mathfrak{P} \nmid \mathfrak{p}$ alors $\Lambda_{\mathfrak{P}} = O_{L_{\mathfrak{P}}}[\Gamma]$. Si $\mathfrak{P}|\mathfrak{p}$ alors $\Lambda_{\mathfrak{P}}$ est défini, via un groupe formel de Lubin-Tate, de la manière suivante :

Soit $\mathfrak{P}_N$ l'unique relèvement premier de $\mathfrak{P}$ dans N. On choisit un plongement h de $\overline{\mathbb{Q}}$ dans $\overline{\mathbb{Q}_p}$ dont la restriction à N définit $\mathfrak{P}_N$. On note K' (resp. L', resp. N') l'adhérence de $h(K)$ (resp. $h(L)$, resp. $h(N)$) dans $\overline{\mathbb{Q}_p}$. Il existe un groupe formel de Lubin-Tate, $\Phi \in K'[[X, Y]]$, tel qu'on ait :

$$N' = K'(\omega_{m+r}) \text{ et } L' = K'(\omega_r)$$

où, pour tout entier s, ω_s désigne un point primitif de p^s-division de Φ. Le groupe des points de p^n-division de Φ est un F-module libre de rang 1. On a l'égalité :

$$\Lambda_{\mathfrak{P}} = \{p^{-m} \sum_{f \in F} \theta(\omega_m f)\gamma f, \theta \in O_{L'}[[X]]/[p^m]\}$$

On remarque qu'on peut associer au modèle de Fueter un groupe formel $\Phi \in O_{K'}[[X, Y]]$. La relation entre les groupes Φ et Φ_1 est étudiée dans $[S_2]$, section 7.

Soit σ_1 et σ_2 les points de 2-division de $\mathbb{C}/\Omega$ différents de 0 et 2ψ. On définit, à une constante près, la fonction D, elliptique pour Ω, par son diviseur :

$$(D) = (\sigma_1) + (\sigma_2) - (0) - (2\psi).$$

On définit l'élément résolvant ρ, associé à $\{\alpha, \gamma\}$ par :

$$\rho = p^{-m} \sum_{f \in F} D(p^m \psi)^{-1}.D(\alpha f + \psi).\gamma.f.$$

On montre que $p^m \rho \in O_L[\Gamma]$. En utilisant la description de Λ, on démontre dans $[S_1]$

PROPOSITION 3. *Si $\rho \in \Lambda$, alors $< 2, \sigma > \Lambda$ est libre sur Λ.*

Enfin on démontre dans $[S_2]$

THÉORÈME 4. *L'élément résolvant $\rho \in \Lambda$.*

On déduit des Théorèmes 3 et 4 et de la Proposition 3 :

COROLLAIRE. *Sous les hypothèses du Théorème 3, O_N est libre sur son ordre associé.*

3. Courbes elliptiques

Dans $[T_3]$ Taylor considère le problème de structure galoisienne suivant. Il s'agit d'une généralisation de la question étudiée dans le paragraphe 2.

On considère K un corps quadratique imaginaire et E une courbe elliptique à multiplication complexe par O_K. On suppose que E est définie sur une extension L de K et qu'elle a partout bonne réduction. Soient $\mathfrak{M}$ un idéal de O_K et G le groupe des points de $\mathfrak{M}$ division de E. Par raison de simplicité on suppose $\mathfrak{M} = \mathfrak{p}^m$ où $\mathfrak{p}$ est un idéal premier principal, $\mathfrak{p} = \pi O_K$ et $m \geq 1$. On suppose en outre que les points de G sont rationnels sur L, i.e. l'inclusion :

$$G \subset E(L).$$

(Le lecteur peut se reporter à [S-T] pour le cas général).

Si $P \in E(L)$ on pose :

$$G_P = \{R \in E(\overline{\mathbb{Q}}) / \pi R = P\}$$

On considère l'algèbre $Map(G_P, \overline{\mathbb{Q}})$ les applications des G_P dans $\overline{\mathbb{Q}}$, où l'addition et la multiplication sont les opérations naturelles.

Soit $\Omega_L = Gal(\overline{\mathbf{Q}}/L)$. Ce groupe opère sur G_P et $\overline{\mathbf{Q}}$. Il opère donc sur $Map(G_P, \overline{\mathbf{Q}})$

par :

$$(\omega f)(R) = \omega(f(\omega^{-1}R)), \forall \omega \in \Omega_L.$$

On définit :

$$L_P = Map(G_P, \overline{\mathbf{Q}})^{\Omega_L}$$

c'est la L-algèbre des applications de G_P dans $\overline{\mathbf{Q}}$ qui commutent avec l'action de Ω_L.

L'algèbre de groupe $A = L[G]$ opère sur L_P par :

$$\left(f.\sum_g a_g g\right)(R) = \sum_g f(g+R)a_g, \forall R \in G_P.$$

On remarque que L_P est un espace homogène principal sur A.

On se place maintenant au niveau des anneaux d'entiers. On définit un ordre de Hopf de O_L dans A qu'on note Λ. Comme dans le paragraphe 2 il est défini par ses composantes locales : Si $\mathfrak{P} \nmid \mathfrak{p}, \Lambda_{\mathfrak{P}} = O_{L_{\mathfrak{P}}}[G]$, si $\mathfrak{P}|\mathfrak{p}, \Lambda_{\mathfrak{P}}$ est défini à l'aide d'un groupe formel de $O_{L_{\mathfrak{P}}}[[X, Y]]$ associé à la courbe E, ([T_3]). Soit O_P la clôture intégrale de O_L dans L_P. On note que O_P n'est pas en général stable par l'action de Λ. On introduit :

$$\widetilde{O}_P = \{x \in O_P / x\Lambda \subset O_P\}.$$

C'est le plus grand Λ-module contenu dans O_P. Taylor démontre dans [T_3] :

Proposition 4.

a) *$\widetilde{O}_P$ est un ordre de O_L dans L_P.*
b) *$\widetilde{O}_P$ est un Λ-module localement libre.*

On peut considérer grâce à b) la classe $[\widetilde{O}_P]$ de $\widetilde{O}_P$ dans $C\ell(\Lambda)$.

On note ψ l'application :

$$\begin{aligned}\psi :\ & E(L) \to C\ell(\Lambda)\\ & P \ \to [\widetilde{O}_P]\end{aligned}$$

Théorème 5([T_3]).

a) *ψ est un homomorphisme de groupe.*
b) *$\psi(E(L))$ est annulé par l'ordre du groupe G.*

Pour une version plus générale de a) le lecteur peut se reporter à l'exposé de Taylor dans ce volume.

Soit $E(L)_{torsion}$ le sous-groupe de torsion de $E(L)$. On peut facilement montrer grâce au Théorème 5 que le sous-groupe des points de torsion annulés par un idéal de O_K premier à $\mathfrak{p}$ est contenu dans le noyau de ψ. En fait Taylor conjecture dans [T_3].

CONJECTURE: $E(L)_{torsion} \subset Ker\psi$.

On démontre dans [S-T].

THÉORÈME 6. *Soit ℓ un nombre premier décomposé dans O_K. On suppose $\mathfrak{p} \nmid \ell$ et $E[\ell^2] \subset E(L]$. Alors $E(L)_{torsion} \subset Ker\psi$.*

On remarque que dans ce cas $(1 - \zeta_\ell, \sigma)\Lambda$ est libre sur Λ, où ζ_ℓ désigne une racine primitive ℓ-ième de l'unité.

Soit w_K le nombre de racines de l'unité contenu dans K.

THÉORÈME 7 ([S-T]). *Si $\mathfrak{p}$ est premier à w_K, alors*

$$E(L)_{torsion} \subset Ker\psi$$

Pour certains résultats pour $\mathfrak{p}|2$ voir [CN-S].

BIBLIOGRAPHIE

[CN-S] Ph. CASSOU-NOGUES, A. SRIVASTAV, *On Taylor's conjecture for Kummer orders.* to appear.

[CN-T] Ph. CASSOU-NOGUES, M.J. TAYLOR, *Rings of integers and elliptic functions*, Progress in Mathematics **66** (1987). Birkhauser

[S 1] A. SRIVASTAV, *Swan modules and elliptic functions*, Illinois Jour. Math. **32** **(3)** (1988), 462–483.

[S 2] A. SRIVASTAV, *A note on Swan modules,.* to appear in Indian Jour. Pure and Applied Math.

[S-T] A. SRIVASTAV, M.J. TAYLOR, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. **99**, (1990), 165–184.

[Sw] R.-G SWAN, *Periodic resolutions for finite groups*, Ann. of Math. **72** (1960), 267–291.

[T 1] M.J. TAYLOR, *Classgroups of group rings*, LMS Lecture Notes **91**. Cambridge University Press 1984.

[T 2] M.J. TAYLOR, *Relative Galois module structure of rings of integers and elliptic functions III*, Proc. L.M.S.(3) **51** (1985), 415–431.

[T 3] M.J. TAYLOR, *Mordell-Weil groups and the Galois module structure of rings of integers*, Illinois Jour. Math. **32** **(3)** (1988), 428–452.

[U] S.-V. ULLOM, *Non trivial lower bounds for class groups of integral group rings*, Illinois Jour. Math. **20** (1976), 361–371.

SPIC Science fondation
East Cost Chambers
92 G.N. Chetty road
600017 Madras - INDIA