

ANUPAM SRIVASTAV

**Modules de Swan et courbes elliptiques à multiplication complexe**

*Journal de Théorie des Nombres de Bordeaux*, tome 2, n° 1 (1990), p. 41-48

[http://www.numdam.org/item?id=JTNB\\_1990\\_\\_2\\_1\\_41\\_0](http://www.numdam.org/item?id=JTNB_1990__2_1_41_0)

© Université Bordeaux 1, 1990, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

## Modules de Swan et courbes elliptiques à multiplication complexe

par ANUPAM SRIVASTAV

### 1. Introduction

A/ Modules de Swan

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

$$\langle s, \sigma \rangle = s\mathbf{Z}[G] + \sigma\mathbf{Z}[G]$$

où  $\sigma = \sum_{g \in G} g$ .

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

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

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

$$T(\mathbf{Z}[G]) = \{[s, \sigma] \mid (s, |G|) = 1\}.$$

C'est un sous-groupe fini de  $\mathcal{Cl}(\mathbf{Z}[G])$  annihilé par  $|G|$ ,  $[Sw], [U]$ .

THÉORÈME 1.

- a) Si  $G$  est cyclique,  $T(\mathbf{Z}[G]) = \{0\}$ .
- b) Si  $p$  est un nombre premier,  $p > 2$ , et si  $G$  est un  $p$ -groupe, alors  $T(\mathbf{Z}[G])$  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/ Structure 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  $O_E$

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

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

On peut considérer  $O_N$  comme module galoisien, c'est-à-dire comme module sur  $\mathbf{Z}[G]$ ,  $O_L[\Gamma]$  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<sub>1</sub>], Théorème 3-1 démontré également par S.Chase.

**THÉORÈME 2.** *Si l'extension  $(N/L)$  est modérément ramifiée alors  $O_N$  est un  $\mathbf{Z}[G]$ -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  $\Omega$  un réseau de  $\mathbf{C}$ . On note  $\Omega_4$  l'ensemble des points  $\psi$  de  $\mathbf{C}/\Omega$  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  $\mathbf{C}/\Omega$  sur les points complexes de  $E_{\Omega, \psi}$  donné par :

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

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

On dit que  $E_{\Omega, \psi}$  est le modèle de Fueter associé à  $(\Omega, \psi)$ . On obtient par changement de coordonnées le modèle de Fueter associé à  $(\Omega, \psi')$  à partir du modèle de Weierstrass associé à  $\Omega$ ,  $([CN-\Gamma], IV)$ . 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  $d_K < -1$ , 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  $\psi$  tel que  $2\psi$  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)  $t_{\Omega, \psi}^2 - 2^6$  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  $(\Omega, \psi)$  et on écrit  $E$  (resp.  $t$ ) pour  $E_{\Omega, \psi}$  (resp.  $t_{\Omega, \psi}$ ).

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

$\lambda \equiv \pm 1 \pmod{4O_K}$ . On pose :

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

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<sub>2</sub>], M.J. Taylor a démontré

**THÉORÈME 3.**

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

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

On considère deux cas :

Cas I :  $\mathfrak{p}$  est décomposé dans  $(K/\mathbb{Q})$ .

Le groupe  $\Gamma$  est alors un  $p$ -groupe cyclique avec  $p \neq 2$ . Puisque  $T(\mathbb{Z}[\Gamma]) = \{1\}$  on en déduit que  $\langle 2, \sigma \rangle$  est libre sur  $\mathbb{Z}[\Gamma]$  et donc libre sur  $\Lambda$ .

Cas II :  $\mathfrak{p}$  est inerte dans  $(K/\mathbb{Q})$ .

Le groupe  $\Gamma$  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  $T(\Lambda, \mathbf{Z})$  divise  $p^{m-1}$*

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

Ce résultat suggère que le module  $\langle 2, \sigma \rangle \Lambda$  est peut-être toujours libre sur  $\Lambda$ . 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  $\Gamma$  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  $\gamma$  (resp.  $\alpha$ ) une base de  $\Gamma$  (resp.  $E[p^m]$ ) sur  $F$ .

La description de  $\Lambda$  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  $\overline{\mathbf{Q}}$  dans  $\overline{\mathbf{Q}}_p$  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  $\overline{\mathbf{Q}}_p$ . 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  $s$ ,  $\omega_s$  désigne un point primitif de  $p^s$ -division de  $\Phi$ . Le groupe des points de  $p^n$ -division de  $\Phi$  est un  $F$ -module libre de rang 1. On a l'égalité :

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

On remarque qu'on peut associer au modèle de Fueter un groupe formel  $\Phi \in O_{K'}[[X, Y]]$ . La relation entre les groupes  $\Phi$  et  $\Phi_1$  est étudiée dans  $[S_2]$ , section 7.

Soit  $\sigma_1$  et  $\sigma_2$  les points de 2-division de  $\mathbf{C}/\Omega$  différents de 0 et  $2\psi$ . On définit, à une constante près, la fonction  $D$ , elliptique pour  $\Omega$ , par son diviseur :

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

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

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

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

PROPOSITION 3. Si  $\rho \in \Lambda$ , alors  $\langle 2, \sigma \rangle \Lambda$  est libre sur  $\Lambda$ .

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

par :

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

On définit :

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

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

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

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

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  $\Lambda$ . 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  $\Lambda$ . On introduit :

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

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

PROPOSITION 4.

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

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

On note  $\psi$  l'application :

$$\begin{aligned} \psi : E(L) &\rightarrow Cl(\Lambda) \\ P &\rightarrow [\tilde{O}_P] \end{aligned}$$

THÉORÈME 5( $[T_3]$ ).

- a)  $\psi$  est un homomorphisme de groupe.
- b)  $\psi(E(L))$  est annihilé 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  $\psi$ . En fait Taylor conjecture dans [T<sub>3</sub>].

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

On démontre dans [S-T].

THÉORÈME 6. Soit  $\ell$  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  $\Lambda$ , où  $\zeta_\ell$  désigne une racine primitive  $\ell$ -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