JOURNAL OF NUMBER THEORY 52, 267–279 (1995)

Structure galoisienne d'anneaux d'entiers et courbes elliptiques sans multiplication complexe

ABDELMEJID BAYAD

Institut für Mathematik, Universität Augsburg, Universitätsstrasse 8, 86159 Augsburg, Germany

Communicated by P. Roquette

Received March 3, 1993

In this paper we state the problem of Galois module structure of rings of integers of extensions attached to the elliptic curves without complex multiplication and admitting a rational point of finite order. Our main aim is to give the first results related to this problem. These results are an analogous to the results of others, concerning ray class fields in the complex multiplication case.

1. INTRODUCTION ET RÉSULTATS

Plusieurs auteurs, ces dernières années, ont étudié le problème de la structure galoisienne des anneaux d'entiers, en tant que modules, de certaines extensions attachées aux courbes elliptiques. Les résultats connus dans cette direction ne le sont que sous les hypothèses suivantes:

On se donne une courbe elliptique E définie sur un corps K telle que:

(1-1) E a bonne réduction partout sur K

(1-2) E a multiplication complexe.

[11], [12], [31], [38], [39], [40] et d'autres.

Pour toute extension N de K, on notera par O_N l'anneau des entiers de N. Maintenant, on s'intéresse au problème de la structure galoisienne d'anneaux d'entiers des extensions obtenues par adjonction des points de division d'une courbe elliptique E définie sur un corps de nombres K et vérifiant la situation générale suivante:

(1-3) E n'a pas bonne réduction partout sur K.

(1-4) E n'a pas nécessairement multiplication complexe.

Hypothèses de notre contribution. On se donne un nombre premier $l, l \geqslant 7$. Soient ξ_l une racine primitive l-ième de l'unité et K un corps de nombres supposé linéairement disjoint de $\mathbb{Q}(\xi_l)$.

641/52/2-7

0022-314X/95 $6.00

On désigne par (E, P) le couple formé d'une courbe elliptique E définie sur K qui est munie d'un point P d'ordre l et rationnel sur K, nous supposons en outre que P définit un point régulier modulo tout premier où la courbe E a mauvaise réduction.

Par raison de simplicité, dans ce travail on ne considère que des couples (E, P) tels que:

E soit de bonne réduction au-dessus de l et l non ramifié dans K ou bien soit de mauvaise réduction de type multiplicatif en tout premier $\mathfrak{p}$ au-dessus de l et $(v_{\mathfrak{p}}(j(E)), l) = 1$.

Nous associons à tout couple (E, P) une somme de Gauss "elliptique" $G_p(P, Q)$ où Q est un point d'ordre l, n'appartenant pas au sous-groupe engendré par P, p est un nombre premier différent de l. On note par $E[l]$ le groupe des points d'ordre l. On sait, d'après [1], [3] et [4], que $G_p(P, Q) \in K(E[l])$ et $G_p(P, Q)^l \in K(\xi_l)$. On pose $F = K(\xi_l)$.

Soit G le groupe de Galois de l'extension $K(E[l])$ sur F, obtenue par adjonction des coordonnées des points de l-division de la courbe elliptique E sur K. D'après le théorème de la base normale, toute extension N sur F, de degré finie, est un module libre sur l'algèbre de groupe $F[\Gamma]$, où $\Gamma = \mathrm{Gal}(N/F)$, de rang 1. Donc O_N est un $O_F[\Gamma]$-module et nous savons que: pour que O_N soit localement libre sur $O_F[\Gamma]$, il faut et il suffit que l'extension (N/F) soit modérément ramifiée [27].

Lorsque l'extension n'est pas modérément ramifiée, on introduit l'ensemble:

$$\mathfrak{U}_{N/F} = \{x \in F[\Gamma] \mid xO_N \in O_N\}$$

c'est l'ordre associé à l'extension N dans $F[\Gamma]$. Dans notre situation nous savons que $\mathfrak{U}_{K(E[l])/F}$ est le seul ensemble sur lequel $O_{K(E[l])}$ puisse être localement libre, c'est pour cette raison qu'on s'intéresse à la structure de $O_{K(E[l])}$ sur $\mathfrak{U}_{K(E[l])/F}$.

Avant d'énoncer notre résultat, on considère une classe A des couples (E, P), définit ci-dessous.

Soit $\mathscr{D}_{E/K}$ le discriminant minimal de la courbe elliptique E définie sur K.

Classe A. Formée de tout couple (E, P) où $\mathscr{D}_{E/K}$ possède une décomposition dans O_K de la forme suivante

$$\mathfrak{p}_0^{r_0}\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_s^{r_s}$$

tel qu'il existe un élément $a \in K(E[l])$ et $a \notin F$ vérifiant

$$a^l O_F = \prod_{\substack{\mathfrak{p}_i \mid \mathscr{D}_{E/K} \\ (r_i, l) = 1}} \mathfrak{B}_i, \qquad 0 \leqslant i \leqslant s$$

où les $\mathfrak{B}_i$ sont les relèvements premiers des $\mathfrak{p}_i$ dans O_F.

Remarques (1-5). (1) Les classes d'isomorphismes des couples (E, P) sont classifiées par la courbe modulaire $X_1(l)$, [13].

(2) La classe A contient les couples (E, P) où E possède un modèle minimal global sur $K(E[l])$, en tant que courbe elliptique sur $K(E[l])$, et $\mathscr{D}_{E/K(E[l])}$ est sans facteur carré.

Le résultat principal qu'on a en vue peut alors s'énoncer de la manière suivante:

THÉORÈME (1-6). *Soit (E, P) un élément de la classe A. On a alors*

$O_{K(E[l])}$ est un $\mathfrak{U}_{K(E[l])/F}$-module libre de rang 1 et engendré par θ, où $\theta = \sum_{i=0}^{l-1} a^i$.

Le plan de ce travail est le suivant:

Le paragraphe 2 contient une étude détaillée de l'extension $(K(E[l])/F)$, dans une situation générale, puis au paragraphe 3 on explicite, à l'aide de certaines fonctions elliptiques et modulaires, un générateur de $K(E[l])$ sur l'algèbre de groupe $F[G]$. Au paragraphe 4, on étudie la structure de $O_{K(E[l])}$ en tant que module sur $\mathfrak{U}_{K(E[l])/F}$ et on donne la démonstration de notre résultat au paragraphe 5.

2. ÉTUDE DE L'EXTENSION $(K(E[l])/F)$

Pour tout entier n naturel non nul, on note par $E[n]$ l'ensemble des points de n-division de la courbe elliptique E sur K et on désigne par

$$S_E = \{\mathfrak{p} \text{ premier de } K\colon v_{\mathfrak{p}}(j(E)) < 0\}$$

et

$$S_{E,l} = S_E \cup \{\text{tout premier de } K \text{ au dessus de } l\}$$

et par $j(E)$ l'invariant modulaire de E sur K.

Dans ce paragraphe nos hypothèses sont assez générales. Soit E une courbe elliptique sur K, munie d'un point P d'ordre l et rationnel sur K et K supposé linéairement disjoint de $\mathbb{Q}(\xi_l)$, vérifiant : (1-3), (1-4) et (2-1) avec

(2-1) $(v_{\mathfrak{p}}(j(E)), l) = 1$ pour tout $\mathfrak{p}|l$ lorsque E a mauvaise réduction en $\mathfrak{p}$

On se propose de montrer le résultat suivant

THÉORÈME 2-2. *On a les propriétés suivantes*:

(a) *L'extension* $(K(E[l])/F)$ *est cyclique de degré* l *et son groupe de Galois* G *est représentable matriciellement par*

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \qquad \text{avec} \quad b \in \mathbb{F}_l$$

(b) *L'extension* $(K(E[l])/F)$ *est non ramifiée en dehors de* $S_{E,l}$.

(c) *Soit* $\mathfrak{p} \in S_{E,l}$, *non au-dessus de* l. *Alors on a*:

$\mathfrak{p}$ *se ramifie totalement dans* $(K(E[l])/F)$ *si et seulement si* $(v_{\mathfrak{p}}(j(E)), l) = 1$.

(d) *Sous la condition* (2-1), *l'extension* $(K(E[l])/F)$ *est totalement ramifiée en* l.

LEMME 2-4. *La courbe* E *a mauvaise réduction de type multiplicatif en tout premier* $\mathfrak{p} \in S_{E,l}$, *non au-dessus de* l.

On sait, [37] VII, Théorème 6-1, que si la réduction n'est pas de type multiplicatif décomposé, le sous-groupe $E_0(K)$, des points de $E(K)$ dont la réduction est un point non singulier, possède un point d'ordre l. Puisque $\mathfrak{p}$ n'est pas au-dessus de l, ce point définit par réduction un élément d'ordre l du groupe des points non singuliers de la courbe réduite. On en déduit, grâce à [36] VII, (2-1), (3-1) et (5-1), que la réduction ne peut être que multiplicative.

LEMME 2-5.

$$F \subset K(E[l]).$$

En effet, pour chaque $T \in E[l]$ il existe $T' \in E[l^2]$, f et g deux fonctions Ω-elliptiques tels que:

$$T = lT', \qquad (f) = l(T) - l(0) \qquad \text{et} \qquad (g) = \sum_{R \in E[l]} (T' + R) - (R).$$

Ω est le réseau associé à E en tant que variété complexe. On a alors: $(g^l) = (f_l)$, où $f_l: z \mapsto f(lz)$. Donc, on peut choisir g telle que:

$$g^l = f_l$$

et soit $S \in E[l]$, on a:

$$g(z+S)^l = f(lz + lS) = f(lz) = g(z)^l.$$

Ainsi, cela nous permet de définir l'accouplement de Weil e_l par:

$$e_l\colon E[l] \times E[l] \mapsto \mu_l$$
$$(S, T) \mapsto e_l(S, T).$$

et $e_l(S, T) = g(z+S)/g(z)$.

On déduit le lemme (2-4), grâce à [37] III (8-1) et du fait que $g(z+S)/g(z) \in K(E[l])$.

Démonstration du théorème (2-2):

Soit $\{P, Q\}$ une base de $E[l]$ sur $\mathbb{F}_l$ et $\omega \in \mathrm{Gal}(K(E[l])/F)$. On a alors:

$$P^\omega = P$$
$$Q^\omega = a_\omega Q + b_\omega P, \qquad a_\omega \in \mathbb{F}_l^* \qquad \text{et} \qquad b_\omega \in \mathbb{F}_l$$

On a donc

$$e_l(P, Q)^\omega = e_l(P^\omega, Q^\omega) = e_l(P, Q)^{a_\omega}.$$

et comme $e_l(P, Q) \in F$ alors $a_\omega = 1$. D'où le (a) du théorème (2-2).

Comme pour chaque $\mathfrak{p} \notin S_{E,l}$, la courbe E a bonne réduction, alors d'après le critère de Néron-Ogg-Shafarevich, [20] Chap. 15 (3.3), et [36] §2 cor 2.(b) l'extension $(K(E[l])/K)$ est non ramifiée en dehors de $S_{E,l}$. D'où (b) de (2-2)

Montrons (c) de (2-2).

Soit $\mathfrak{p} \in S_{E,l}$, $\mathfrak{p}$ n'est pas au-dessus de l. Nous posons $r = v_\mathfrak{p}(j(E))$, $r > 0$.

Soit $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, dont la valuation discrète associée est $v_\mathfrak{p}$ qu'on suppose normalisée.

Nous associons à $j(E)$ l'unique élément de q de $K_\mathfrak{p}^*$, dont la valuation est r, tel que:

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \ldots$$

Nous posons:

$$h_2 = 5 \sum_{n \geq 1} \frac{n^3 q^n}{(1-q^n)}, \qquad h_3 = \frac{1}{12} \sum_{n \geq 1} \frac{(7n^5 + 5n^3)\, q^n}{(1-q^n)}.$$

Nous considérons la courbe de Tate

$$E_q\colon Y^2 + XY = X^3 - h_2 X - h_3$$

d'origine le point O, [30] §3 et [37] Appendix C, §14.

Soit $\bar{K}_\mathfrak{p}$ une clôture algébrique de $K_\mathfrak{p}$. Nous notons ϕ_q l'isomorphisme de modules galoisiens

$$\phi_q : \bar{K}_\mathfrak{p}^*/q^{\mathbb{Z}} \mapsto E_q(\bar{K}_\mathfrak{p}) \tag{2-5}$$
$$\begin{cases} w \mapsto (X(w), Y(w)), & \text{si} \quad w \notin q^{\mathbb{Z}} \\ w \mapsto O, & \text{si} \quad w \in q^{\mathbb{Z}}. \end{cases}$$

avec:

$$\begin{cases} X(w) = \sum_{n \in \mathbb{Z}} \dfrac{q^n w}{(1-q^n w)^2} - 2 \sum_{n \geqslant 1} \dfrac{nq^n}{(1-q^n)} \\ Y(w) = \sum_{n \in \mathbb{Z}} \dfrac{q^{2n} w^2}{(1-q^n w)^3} + \sum_{n \geqslant 1} \dfrac{nq^n}{(1-q^n)}. \end{cases}$$

où $\bar{K}_\mathfrak{p}^*$ et $E_q(\bar{K}_\mathfrak{p})$ sont munis de leur structure naturelle de $\mathrm{Gal}(\bar{K}_\mathfrak{p}/K_\mathfrak{p})$-module.

Il existe une plus petite extension L de $K_\mathfrak{p}$, non ramifiée, sur laquelle E et E_q deviennent isomorphes, et l'on a $[L: K_\mathfrak{p}] \leqslant 2$. Nous déduisons, via (2-5), un isomorphisme de module galoisien entre $E(\bar{K}_\mathfrak{p})$ et $\bar{K}_\mathfrak{p}^*$, que nous fixons.

Si $S \in E(\bar{K}_\mathfrak{p})$, nous appelons paramètre de S et notons $\lambda(S)$, tout représentant dans $\bar{K}_\mathfrak{p}^*$ de son image dans $\bar{K}_\mathfrak{p}^*/q^{\mathbb{Z}}$. Ainsi, un point S, d'ordre n, de E est de paramètre:

$$\lambda(S) = \xi_n^u q^{v/n}, \qquad 0 \leqslant u, \quad v < n, \quad (u, v, n) = 1$$

où $q^{1/n}$ (resp. ξ_n) est une racine n-ième de l'unité de q (resp. 1) dans $\bar{K}_\mathfrak{p}$.

Alors l'extension $(K_\mathfrak{p}(E[l])/K_\mathfrak{p})$ est ramifiée si et seulement si $(L(E[l])/L)$ est ramifiée. Or nous savons que $L(E[l]) = L(\xi_l, q^{1/l})$.

Ainsi, on déduit de nos hypothèses la démonstration de (c) (2-2).

Maintenant, soit $\mathfrak{p}$ au-dessus de l:

Si la courbe a bonne réduction en $\mathfrak{p}$, elle est partout au-dessus de l, alors on sait, [14] II prop (1.9) (i)] que l'extension $(K(E[l])/K)$ est ramifiée en tout $\mathfrak{p}$ au-dessus de l.

Si la réduction de la courbe est mauvaise en $\mathfrak{p}$, elle est partout au-dessus de l. En outre, la réduction est multiplicative. Donc, on applique à nouveau la théorie des courbes de Tate ci-dessus. Or, on sait que $(v_\mathfrak{p}(j(E)), l) = 1$, cela achève la démonstration du théorème (2-2).

3. Construction de générateurs galoisiens de $(K(E[l])/F)$

Ce paragraphe regroupe les principales définitions et propriétés de certaines fonctions que nous utilisons pour construire nos générateurs. On fixe un couple de nombres premiers distincts (l, p), $l \geqslant 7$. A tout couple (E, P)

qui satisfait les hypothèses de notre "contribution", on associe une somme de Gauss. Cette somme est la somme introduite et étudiée dans [3], [4] et [10].

Les notations sont standards.

Si T est un point primitif de p^2-division et S un point de p-division de E tels que $\{S, pT\}$ constitue une base de $E[p]$ sur $\mathbb{F}_l$, on définit une fonction sur E, à constante multiplicative près, par la donnée de son diviseur:

$$(D) = \sum_{k=0}^{p-1} (S + kR) - (kR), \qquad \text{où} \quad R = pT. \tag{3-1}$$

DÉFINITION 3-2. Si Q est un point d'ordre l de E n'appartenant pas à $\mathbb{Z}P$, on pose:

$$\mathscr{R}(P, Q, S, T) = \sum_{u \in \mathbb{F}_l} \frac{D(Q + uP; S, R)}{D(T; S, R)} \cdot e_l(Q, uP)^{-1}$$

où e_l est l'accouplement de Weil sur les points de l-division.

Pour se débarrasser de la dépendance du choix de S et T, on associé à un tel couple (E, P) la somme suivante:

$$G_p(P, Q) = \begin{cases} p^{-(p^4-p^3)} \cdot \displaystyle\prod_{T \in E'[p^2]} \prod_{S \in E''[p]} \mathscr{R}(P, Q, S, T), \\ \qquad\qquad \text{si } E \text{ a bonne réduction en } l \\ (lp)^{-(p^4-p^3)} \cdot \displaystyle\prod_{T \in E'[p^2]} \prod_{S \in E''[p]} \mathscr{R}(P, Q, S, T), \\ \qquad\qquad \text{si } E \text{ a mauvaise réduction en } l. \end{cases} \tag{3-3}$$

où $E'[p^2]$ désigne l'ensemble des points d'ordre p^2 de (E/K) et $E''[p]$ désigne un système de représentants des points non nuls de $E[p]/\langle pT \rangle$. C'est cet élément qui donne des générateurs de Galois de $(K(E[l])/F)$. On sait, [1], [3] et [4], que nos sommes ont les propriétés suivantes:

PROPOSITION 3-4.

(1) *$G_p(P, Q) \in K(E[l])$ et $G_p(P, Q)^l \in F$.*

(2) *Soit $\omega \in Gal(K(E[l])/K)$ tel que:*

$$Q^\omega = a_\omega Q + b_\omega P \qquad \text{avec} \quad a_\omega \in \mathbb{F}_l^* \quad \text{et} \quad b_\omega \in \mathbb{F}_l$$

alors on a:

$$G_p(P, Q)^\omega = e_l(P, Q)^{p^2(p-1)^2(p+1)a_\omega b_\omega} G_p(P, a_\omega Q)$$

et $G_p(P, Q)$ est un entier algébrique de $K(E[l])$.

(3) *$G_p(P, Q)$ est une unité en dehors de $S_{E,l}$.*

(4) *L'idéal engendré par $G_p(P, Q)$ dans $K(E[l])$ est ambigu pour l'extension $(K(E[l])/F)$.*

Pour tout élément x de $\mathbb{Q}$, on note $\{x\}$ sa partie fractionnaire.

DÉFINITION 3-5. Si $\Gamma = \mathrm{Gal}(F/K)$, on définit un élément de Stickelberger $\theta_2'(p) \in \mathbb{Q}[\Gamma]$ par:

$$\theta_2'(p) = (p^3 - p^2) \sum_{t=1}^{l-1} \gamma(t)\, \sigma_t^{-1}$$

où

$$\gamma(t) = (p^2 - p)\, \beta(t) + \sum_{s=1}^{p-1} \alpha(t, s)$$

et où $\alpha(t, s)$ et $\beta(t)$ sont définis par:

$$\alpha(t, s) = -tp \left\{\frac{a}{pl}\right\} + lp \inf\left(\frac{t}{l}, \left\{\frac{pt}{l}\right\}\right),$$

$$\beta(t) = \frac{l}{p}\left(\frac{t}{l}\left\{\frac{pt}{l}\right\} + \inf\left(0, 1 - \frac{t}{l} - \left\{\frac{pt}{l}\right\}\right)\right)$$

avec $a = lsx + pty$ où $x, y \in \mathbb{Z}$ sont choisis tels que $lx - py = 1$.

LEMME 3-6. *Si P définit un point régulier de la courbe réduite modulo tout premier $\mathfrak{p}$ où la courbe a mauvaise réduction. On a alors:*

$$G_p(P, Q)^l\, O_F = \begin{cases} I^l\left(\prod_{\mathfrak{p} \in S_E} \mathfrak{B}^{r_\mathfrak{p}}\right)^{l\theta_2'(p)}, & \text{si } E \text{ a bonne réduction en } l \\ I^l\left(\prod_{\mathfrak{p} \in S_{E,l}} \mathfrak{B}^{r_\mathfrak{p}}\right)^{l\theta_2'(p)}, & \text{si } E \text{ a mauvaise réduction en } l. \end{cases}$$

et où I est un idéal entier de F.

Ce lemme, modulo l, est déjà connu dans [1] et [4]. Il reste le cas au-dessus de l.

Lorsqu'il y a bonne réduction en l, d'après la proposition (3-4) (3), on a : $G_p(P, Q)$ est une unité en l.

Dans le cas de mauvaise réduction en l, on sait que la réduction est de type multiplicatif. On utilise donc, la théorie des courbes de Tate pour déterminer la valuation de $G_p(P, Q)$ aux places au-dessus de l. Les techniques sont les mêmes que dans [1] Chap. IV et Appendice I, et les formules

qu'on obtient sont les mêmes que celles du cas au-dessus de p. C'est pour cette raison qu'on les adopte et on en déduit le lemme (3-6).

COROLLAIRE 3-7. *Soit (l, p) un couple de nombres premiers distincts et vérifiant $(p^2-1, l)=1$. On a alors*:

$$K(E[l]) = F(G_p(P, Q))$$

En effet, d'après (3-4), on sait que: $G_p(P, Q) \in K(E[l])$, $G_p(P, Q)^l \in F$ et pour tout $\omega \in \mathrm{Gal}(K(E[l])/F)$, on a

$$G_p(P, Q)^\omega = e_l(P, Q)^{p^2(p-1)^2(p+1)b_\omega} \cdot G_p(P, Q).$$

Comme P définit un point régulier dans la courbe réduite, modulo tout premier $\mathfrak{p}$ où la courbe a mauvaise réduction et $(p^2-1, l)=1$, on a alors: $G_p(P, Q) \notin F$. D'où le corollaire (3-7).

Remarque 3-8. La définition, dans (3-5), des $\alpha(t, s)$ et $\beta(t)$ ne dépend pas du choix de x et y.

4. STRUCTURE GALOISIENNE D'ANNEAUX D'ENTIERS

Dans ce paragraphe, on décrit l'ordre associée $\mathfrak{U}_{K(E[l])/F}$ et on étudie la structure galoisienne de $O_{K(E[l])}$ en tant que module sur $\mathfrak{U}_{K(E[l])/F}$. On rappelle que nos hypothèses sont précisement ceux citées à l'introduction.

Soit $\mathfrak{B}$ un idéal premier de O_F. Si $\mathfrak{B}$ n'est pas au-dessus de l, soit $\mathfrak{a}$ un relèvement premier de $\mathfrak{B}$ dans $K(E[l])$, alors l'extension $(K(E[l])_\mathfrak{a}/F_\mathfrak{B})$ est modérément ramifiée et par le théorème de Noether, on a

$$\mathfrak{U}_{K(E[l])_\mathfrak{a}/F_\mathfrak{B}} = O_{F_\mathfrak{B}}[G]. \tag{4-1}$$

Maintenant, on considère $\mathfrak{B}|l$. Soit $\mathfrak{a}$ l'unique premier de $K(E[l])$ au-dessus de $\mathfrak{B}$. L'extension $(K(E[l])_\mathfrak{a}/F_\mathfrak{B})$ est sauvagement ramifiée, de Kummer cyclique de degré premier l.

On a le résultat suivant

PROPOSITION 4-2. *Soit $\mathfrak{B}$ un premier de F, on a*

$$\mathfrak{U}_{K(E[l])_\mathfrak{a}/F_\mathfrak{B}} = \begin{cases} \mathcal{M}_\mathfrak{B}, \text{ l'ordre maximal}, & \text{si } \mathfrak{B} \mid l \\ O_{F_\mathfrak{B}}[G], & \text{sinon.} \end{cases}$$

et $O_{K(E[l])}$ est localement libre sur $\mathfrak{U}_{K(E[l])/F}$.

Soit $a \in K(E[l])$ et $a \notin F$ tel que:

$$a^l O_F = \prod_{\substack{\mathfrak{P} \mid \mathscr{D}_{E/K} \\ (v_{\mathfrak{P}}(j(E)), l) = 1}} \mathfrak{B} \tag{4-3}$$

L'élément a est associé à un couple (E, P) de la classe A. Donc, on a un élément de F tel que:

$v_{\mathfrak{B}}(a^l) = 1$ pour tout premier $\mathfrak{B}$ où la courbe a mauvaise réduction et a^l est une unité en dehors de $S_{E,l}$. Lorsqu'il y a bonne réduction en l, grâce au critère de Hecke [18] Th. 119, on sait que $v_{\mathfrak{B}}(a^l) = 0$ et $a^l = 1 \pmod{(1-\xi_l)}$ car l est totalement ramifiée dans $(K(E[l])/K)$ et non ramifiée dans K, en outre on peut supposer que $a^l \neq 1 \pmod{(1-\xi_l)^2}$ sinon $K(E[l])_a = F_{\mathfrak{B}}$, $\forall \mathfrak{B} \mid l$.

Alors, le polynôme $X^l - a^l$ est un polynôme d'Eisenstein, on sait [17] Th. 24, que cela implique que:

$$O_{K(E[l])_a} = O_{F_{\mathfrak{B}}}[a], \qquad \text{pour tout premier } \mathfrak{B} \text{ de } F \tag{4-4}$$

En outre, soit σ un générateur du groupe $G = \mathrm{Gal}(K(E[l])/F)$ tel que: $\sigma(a) = \xi_l a$. Soit $\mathfrak{B} \mid l$, on obtient

$$Tr_{K(E[l])_a/F_{\mathfrak{B}}}(O_{K(E[l])_a}) = Tr_{K(E[l])_a/F_{\mathfrak{B}}}(O_{F_{\mathfrak{B}}}[a] = lO_{F_{\mathfrak{B}}}. \tag{4-5}$$

Or on sait, [34] et [8], que l'égalité (4-5) implique que:

$$\frac{le_0}{l-1} - 1 \leqslant t \leqslant \frac{le_0}{l-1} \tag{4-6}$$

où e_0 est le nombre de ramification absolu de F en $\mathfrak{B}$ et t est le nombre de ramification de $(K(E[l])_a/F_{\mathfrak{B}})$, [34] Chap. IV.

Or, on sait que $l-1 \mid e_0$ car $\xi_l \in F$, alors la double inégalité (4-6) devient:

$$t = \frac{le_0}{l-1} - 1 \qquad \text{et} \qquad t = (l-1) \pmod{l} \qquad \text{ou} \quad t = \frac{le_0}{l-1} = 0 \pmod{l}. \tag{4-7}$$

Ceci montre, [15] Chap. II, Th. 3, que:

$$\mathfrak{U}_{K(E[l])_a/F_{\mathfrak{B}}} = \mathscr{M}_{\mathfrak{B}}. \tag{4-8}$$

Donc, [15] Chap. II, $O_{K(E[l])}$ est localement libre sur $\mathfrak{U}_{K(E[l])/F}$.

5. Démonstration de notre résultat

On pose

$$\theta = \sum_{i=0}^{l-1} a^i. \tag{5-1}$$

On a alors le résultat suivant:

Proposition 5-2.

$$O_{K(E[l])_a} = \theta \cdot \mathfrak{U}_{K(E[l])_a/F_{\mathfrak{B}}}.$$

En effet, soit $\mathfrak{B}$ premier de F. Si $\mathfrak{B}$ n'est pas au-dessus de l, on sait que l'extension $(K(E[l])/F)$ est modérément ramifiée en $\mathfrak{B}$.

Soit χ (resp. σ) le générateur de $\hat{G}$ (resp. G), défini par: $\chi(\sigma) = \xi_l^{-1}$, (resp. $\sigma(a) = \xi_l a$)

D'une part nous avons vérifié que

$$\prod_{i=0}^{l-1} (\theta \mid \chi^i)^2 = l^{2l} a^{l(l-1)},$$

où

$$(\theta \mid \chi^i) = \sum_{j=0}^{l-1} \chi^i(\sigma^j)\, \sigma^j(\theta) = l a^i.$$

D'autre part, les seuls idéaux qui se ramifient dans $(K(E[l])/F)$ sont les diviseurs premiers de $a^l O_F$ et les idéaux au-dessus de l, donc le discriminant de cette extension s'écrit comme suit:

$$d_{K(E[l])_a/F_{\mathfrak{B}}} = \left(\prod_{\mathfrak{p} \mid \mathfrak{D}_{E/K}}^{(v_{\mathfrak{p}}(j(E)),\, l) = 1} \mathfrak{B} \right)^{l-1}.$$

Ce qui montre que $\{\theta^\sigma\}_{\sigma \in G}$ est une base normale de $O_{K(E[l])_a}$ sur $O_{F_{\mathfrak{b}}}[G]$, d'où la proposition en dehors de l.

Soit, maintenant $\mathfrak{B} \mid l$. D'après (4-4) et (4-5), il suffit de montrer que:

$$e_{\chi^j}(a^i) \in O_{F_{\mathfrak{B}}}[a]. \tag{5-3}$$

avec

$$e_{\chi^j} = \frac{1}{l} \sum_{t=1}^{l-1} \chi^{-j}(\sigma^t)\, \sigma^t.$$

Or $e_{\chi^j}(a^i) = a^i$ (resp. 0) si $i = j$ (sinon). Donc, d'après (4-7) et [7], on sait que:

$$\mathscr{M}_{\mathfrak{B}} = \sum_{j=0}^{l-1} O_{K(\xi_l)\mathfrak{B}} e_{\chi^j}. \tag{5-4}$$

D'où (5-3).

On en déduit de (4-1), (4-2), (4-3), (4-4), (4-8), (5-2) (5-3) et (5-4) notre théorème (1-6).

Remarque 5-5. Il est très intéressant de savoir l'ensemble de tous les éléments (E, P) où le théorème (1-6) reste vrai.

BIBLIOGRAPHIE

1. A. BAYAD, Résolvantes elliptiques et éléments de Stickelberger, *Pub. école doctorale Bordeaux I* (1992).
2. A. BAYAD, "Théorème de Stickelberger elliptique," à paraître dans la "Revue arithmétique de Caen," (1993).
3. A. BAYAD ET W. BLEY, "Sommes arithmétiques et éléments de Stickelberger elliptiques," à paraître dans *Manuscripta Mathematica*.
4. A. BAYAD ET PH. CASSOU-NOGUÈS, à paraître.
5. A. M. BERGÉ, Arithmétique d'une extension galoisienne à groupe d'inertie cyclique, *Ann. Inst. Fourrier Grenoble* **28**, No. 4 (1978), 17–44.
6. F. BERTRANDIAS ET M. J. FETRON, Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local, *C.R. Acad. Sci. Paris Sér. A* **274** (1972), 1330–1333.
7. F. BERTRANDIAS, Décomposition du Galois Module des entiers d'une extension cyclique de degré premier d'un corps de nombres ou d'un corps local, *Ann. inst. Fourier* **29** (1979), 33–48.
8. F. BERTRANDIAS, Entiers d'une p-extension cyclique d'un corps local, *C.R. Acad. Sci. Paris* **286** (1978), 1083–1086.
9. A. BRUMER ET KRAMER, The rank of elliptic curves, *Duke Math. J.* **44**, No. 4 (1977).
10. PH. CASSOU-NOGUÈS ET M. J. TAYLOR, Un élément de Stickelberger quadratique, *J. Number Theory* **37** (1991), 307–342.
11. PH. CASSOU-NOGUÈS ET M. J. TAYLOR, "Elliptic Functions and Rings of Integers," Progress in Math., Vol. 66, Birkhäuser, Basel, 1987.
12. S. P. CHAN, Modular function, elliptic function and Galois module structure, *J. Reine Angew. Math.* (1987), 67–82.
13. P. DELIGNE ET M. RAPOPORT, "Les schémas de modules de courbes elliptiques," Modular functions of one variable II, Lectures Notes in Mathematics, Vol. 349, Springer, Berlin/Heidelberg/New York, 1973.
14. E. DE SHALIT, "Iwasawa Theory of Elliptic Curves with Complex Multiplications," Perspectives in Mathematics, Vol. 3, Academic Press, New York, 1987.
15. M. J. FERTON, "Sur l'anneau des entiers d'extensions cycliques de degré p et d'extensions déidrales de degré $2p$ d'un corps local," Thèse de Doctorat de 3-ième Cycle présentée à l'université de Grenoble, 1972.
16. A. FRÖHLICH, "Galois Module Structure of Integers," Ergebnisse der Mathematik, Folge 3, Band 1, Springer-Verlag, Berlin/New York, 1983.

17. A. FRÖHLICH ET M. J. TAYLOR, "Algebraic Number Theory," Cambridge Studies in Advanced Mathematics, Vol. 27, Cambridge University Press, Cambridge, U.K., 1991.
18. M. HARRIS, Kubert-Lang units and elliptic curves without complex multiplication, *Comp. Math.* **41**, Fasc. 1 (1980), 127–136.
19. E. HECKE, "Lectures on the Theory of Algebraic Numbers," Graduate Texts in Mathematics, Springer-Verlag, New York, 1981.
20. D. HUSEMÖLLER, "Elliptic Curves," Graduate Texts in Mathematics, Vol. 111, Springer-Verlag, New York, 1987.
21. S. LANG, "Complex Multiplication," Grundlehren der mathematischen Wissenschaften, Vol. 255, A series of comprehensive studies in mathematics, Springer-Verlag, New York, 1983.
22. S. LANG, "Elliptic Functions," Advanced Book Program., Addison-Wesley, Reading, Mass., 1974.
23. S. LANG, "Elliptic Curves: Diophantine Analysis," Grundlehren der mathematischen Wissenschaften, Vol. 231, A series of comprehensive studies in mathematics, Springer-Verlag, New York, 1978.
24. R. LONG, "Algebraic Number Theory," Pure and applied mathematics, A series of monographs and text books, 1977.
25. J. LUBIN ET J. TATE, Formal complex multiplication in local field, *Ann. Math.* **81** (1965), 380–387.
26. R. MACKENZIE ET G. WHAPLES, Artin Schreier equations in characteristic zero, *Amer. J. Math.* **78** (1956), 473–485.
27. E. NOETHER, Normal Basisbeikörpen ohne höhere Verzweigung, *J. Reine Angew. Math.* **167** (1932), 147–152.
28. A. P. OGG, Elliptic curves and wild ramification, *Amer. J. of Math.* **89** (1967), 1–21.
29. F. OORT ET J. TATE, Group schemes of prime order, *Ann. Sci. E.N.S.* **3** (1970), 1–21.
30. P. ROQUETTE, "Analytic Theory of Elliptic Function over Local Fields," Vandenhoeck and Ruprecht in Göttingen, 1970.
31. R. SCHERTZ, Galoismodulstruktur und elliptische Funktionen, *J. Number Theory* **39** (1991), 287–326.
32. J. P. SERRE, "Sur les représentations modulaires de degré 2 de Gal($\mathbb{Q}/\mathbb{Q}$)," *Duke Math. J.* **54**, No. 1 (1987), 179–230.
33. J. P. SERRE, "Abelian l-adic Representations and Elliptic Curves," Benjamin, 1968.
34. J. P. SERRE, "Corps locaux," Hermann, Paris, 1968.
35. J. P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
36. J. P. SERRE ET J. TATE, Good reduction of abelian varieties, *Ann. Math. (2)* **88** (1968), 492–517.
37. J. H. SILVERMAN, "The Arithmetic of Elliptic Curves," Graduate Texts Mathematics, Vol. 106, Springer-Verlag, New York, 1985.
38. A. SRIVASTAV ET M. J. TAYLOR, Elliptic curves with complex multiplication and Galois module structure, *Invent. Math.* **99** (1990), 165–184.
39. M. J. TAYLOR, Relative Galois module structure of rings of integers and elliptic functions II, *Ann. Math.* **121** (1985), 519–535.
40. M. J. TAYLOR, Modell-Weil groups and the Galois module structure of rings of integers, *Illinois J. Math.* **32**, No. 3 (1988).