THEORIE DES NOMBRES
BESANCON

Années 1986/87-1987/88
Fascicule 1

MODELE DE DEURING ET MONOGENEITE DES ANNEAUX D'ENTIERS DES CORPS DE RAYONS D'UN CORPS QUADRATIQUE IMAGINAIRE DANS LE CAS 3 RAMIFIE

Vincent FLECKINGER

Modèle de Deuring et monogénéité des anneaux d'entiers des corps de rayons d'un corps quadratique imaginaire dans le cas 3 ramifié

par Vincent Fleckinger

I Introduction:

Notations: Soit $\Omega=\mathbb{Z}\tau+\mathbb{Z}$ un réseau de $\mathbb{C}$, on note $P(z;\tau)$, $\sigma(z;\tau)$ les fonctions de Weierstrass, $g_2(\tau)$, $g_3(\tau)$, $\Delta(\tau)$, $j(\tau)$ et $\eta(\tau)$ les éléments modulaires qui lui sont associés. En particulier on a l'équation :

$$P'^2(z;\tau) = 4\,P^3(z;\tau) - g_2(\tau)\,P(z;\tau) - g_3(\tau)$$

On utilisera aussi la fonction de Weber définie par:

$$h(z;\tau)=-2^7\,3^5\,\frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)}\,P(z;\tau).$$

Le symbole $\approx$ désigne la relation d'équivalence "associé à".

Soient $k=\mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire dans lequel 3 est ramifié et A_k son anneau des entiers. On pose :

$$\tau_d = \begin{cases} 1+i\sqrt{-d}\,, & \text{si } d \equiv 2,3 \mod 4 \\ \dfrac{-1+i\sqrt{-d}}{2}\,, & \text{si } d \equiv 1 \mod 4 \end{cases}$$

On remarque que $\mathbb{Z}[\tau_d] = A_k$ et que l'idéal premier au-dessus de (3) est $P=(\tau_d-1,3)$, c'est-à-dire :

$$(\tau_d-1,3)^2=(3).$$

La courbe elliptique $\mathbb{C}/A_k$ admet donc le point $(\tau_d-1)/3$ comme point primitif de P-division. On peut alors lui associer une fonction α, modulaire de niveau 9, définie par :

$$\alpha(t) = -\,\frac{h^2((\tau-1)/3;\tau)-j(\tau)(j(\tau)-1728)}{j(\tau)(j(\tau)-1728)}\;\;\frac{g_2(\tau)\eta^4((\tau-1)/3)}{2(2i\pi)^4\,\eta^{12}(\tau)} \qquad (1)$$

et telle que la courbe $y^2 + \alpha(\tau)xy + y=x^3$ soit un modèle de Deuring de la courbe elliptique $\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})$.

L'invariant modulaire est donné par (cf [D]):

$$j(\tau)(\alpha^3(\tau)-27) = \alpha^3(\tau)(\alpha^3(\tau)-24)^3$$

et le discriminant du modèle est $D= \alpha^3(\tau)-27$.
On pose enfin $\alpha_d = \alpha(\tau_d)$.

Le but de l'article est de fournir des résultats de monogénéité pour les anneaux d'entiers des corps de classes de k de rayons associés à des modules f, premiers avec P. Plus précisement on démontre le résultat suivant:

Théorème : *Soit un idéal entier de* k, *premier avec 3, alors l'anneaux des entiers du corps des classes de rayons associé au module est monogène sur l'anneau des entiers du corps des classes de Hilbert de* k.

Ce résultat est à rapprocher des résultats déjà obtenus dans [C-N,T 1], [C.-N,T 2], [F 1], [F 2], [C 1], [C 2] sur la monogénéité des anneaux d'entiers des corps de classes de rayons d'un corps quadratique imaginaire.

II Le corps $k(\alpha_d)$:

Puisque la fonction α est modulaire de niveau 9 on peut affirmer que α_d est dans $k^{(9)}$. Ce corps est de dimension 27 sur le corps de classes de Hilbert H de k. D'autre part, d'après [F1], α_d^3 engendre le corps $k^{(P)} = H$; il en résulte que le corps $k(\alpha_d)$ est au plus de dimension 3 sur H. Il nous faut donc déterminer les principaux sous-groupes de Galois du groupe $Gal(k^{(9)}/H)$.
Puisque $P = (\tau_d-1,3)$ on peut choisir τ_d-1 comme uniformisante locale en P.

Soient alors les idèles :

$x_d=(x_v)$ $\quad x_v=1$ si $v\neq P$, $x_v=\tau_d$ sinon,

$y_d=(y_v)$ $\quad y_v=1$ si $v\neq P$, $y_v=4$ sinon,

$z_d=(z_v)$ $\quad z_v=1$ si $v\neq P$, $z_v=3\tau_d-2$ sinon.

On obtient alors le tableau, selon la valeur du discrimant d_k modulo 9:

d_k	Type	$k^{(9)}/H$	$k^{(9)}/k^{(3)}$	$k^{(9)}/k^{(3P)}$
-3	(3,3,3)	(x_d, y_d, z_d)	(y_d, z_d)	z_d
3	(9,3)	(x_d, y_d)	(x_d^3, y_d, z_d)	x_d^3

Donnons maintenant l'action de ces idèles sur la fonction modulaire a, en utilisant la loi de réciprocité de Shimura [Sh]. On détermine d'abord l'action des idèles sur le réseau A_k , cette action nous est donnée, localement, sous la forme d'une matrice ; ici, il suffit de considérer la transformation pour la place *P*.

Soit $a_d = Tr_{k/q}(\tau_d)$ et $b_d=N_{k/q}(\tau_d)$.

x_d agit par l'intermédiaire de la matrice $\begin{pmatrix} a_d & -b_d \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_d & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b_d \end{pmatrix}$

y_d agit par l'intermédiaire de la matrice $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 & -9 \\ 9 & & -2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix} \bmod 9$

z_d agit par l'intermédiaire de la matrice $\begin{pmatrix} 3a_d-2 & -3b_d \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ 3 & -2 \end{pmatrix} \bmod 9$

dans les deux cas où cet idèle intervient.

Pour obtenir l'action de ces idèles on rappelle d'abord l'action de $Sl_2(\mathbb{Z})$ sur la fonction êta de Dedekind cf [R]:

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = e(a,b,c,d)\ \sqrt{-i(c\tau+d)}\ \eta(\tau)$$

avec $e(a,b,c,d)=\left(\frac{c}{d}\right) i^{(1-c)/2}\ \exp\left(\frac{i\pi}{12}(bd(1-c^2)+c(a+d))\right)$ si c est impair.

L'action des matrices de la forme $\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ porte sur les coefficients de fouriers des fonctions modulaires part l'intermédiaire du détermi-nant : $\exp(\frac{2i\pi}{9}) \rightarrow \exp(\frac{2in\pi}{9})$.

Pour déterminer cette dernière action, il suffit d'écrire le développe--ment de Fourier de $\alpha(\tau)$ en la pointe infinie, On remarque que le premier facteur de $\alpha(\tau)$ dans (1) est modulaire de niveau 3, et que les matrices utilisées ont un déterminant congru à 1 modulo 3. Il suffit donc d'écrire le développement de Fourier en la pointe infinie du second facteur soit:

$$\alpha(t)= \frac{h^2((\tau-1)/3;\tau)-j(\tau)(j(\tau)-1728)}{j(\tau)(j(\tau)-1728)} \quad \frac{\exp(8i\pi/9)}{24} \quad \exp(-8i\pi\tau/9)(1+\cdots)$$

On obtient alors :

$$\alpha_d{}^{(x_d^{-1},k)} = \exp(5b_d+4a_db_d-4)\frac{2i\pi}{9})\alpha_d$$

$$\alpha_d{}^{(y_d^{-1},k)} = \exp(\frac{4i\pi}{3})\alpha_d$$

$$\alpha_d{}^{(z_d^{-1},k)} = \alpha_d$$

en particulier α_d appartient à $k^{(3P)}$ et n'appartient pas à $k^{(3)}$. On en déduit, puisque $k(\alpha_d)$ est abélienne, que le conducteur de $k(\alpha_d)$ est $3P$. Le discriminant de l'extension $k(\alpha_d)/H$ est donc (27). Ce qui montre que l'idéal engendré par α_d^3 est un cube dans H, soit $(\alpha_d^3)=A^3$

.

Proposition 1: *L'idéal A est principal dans H.*

Démonstration : D'après la structure des groupes abéliens finis, si N est un sous groupe maximal de $Gal(k(\alpha_d)/k)$ vérifiant la propriété :

$$N \cap Gal(k(\alpha_d)/H)=\{e\},$$

alors $Gal(k(\alpha_d)/k)/N$ est un 3-groupe cyclique. Soit L le sous-corps de $k(\alpha_d)$ invariant par N, il est alors de dimension 3 sur $L \cap H$. Puisque H contient les racines cubiques de l'unités, $L'=L(\exp(2i\pi/3))$ est une extension cyclique de k, de degré 3 sur $L' \cap H$.

D'après la théorie de kummer il existe λ dans $L' \cap H$ tel que $L'=L'(\sqrt[3]{\lambda})$

Le discriminant de $L'/ L' \cap H$ est aussi égal à (27), et l'idéal (λ) est de

la forme B^3 dans $L' \cap H$. De plus L' étant abélienne pour tout σ dans $Gal(L' \cap H/k)$, $\sigma(B)/B$ est principal. D'après le théorème de Terada [T], B devient principal dans le corps des genres de $L' \cap H$ c'est-à-dire H. La théorie de Kummer permet alors d'affirmer que A est aussi principal.

Corollaire :

Il existe dans $k(\alpha_d)$ *une unité* ε *telle que* $\varepsilon\,\alpha_d$ *appartient à* H.

III Démonstation du théorème principal:

Soit $y^2 + \alpha(\tau)xy + y = x^3$ le modèle de Deuring de la courbe elliptique $E=\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})$. On peut paramétrer ce modèle à l'aide de la fonction :

$$x(z;\tau)= \alpha^2(\tau)\frac{12h((\tau-1)/3;\tau)}{h(z;\tau)-h((\tau-1)/3;\tau)}$$

Spécialisons la valeur de τ à τ_d, et posons $F(z)= (\varepsilon^2\, x(z;\tau_d))^{-1}$. Par construction de F et d'après les résultats classiques de multiplication complexe (cf [Sh]), si β est un point primitif de f-division, $f \neq P$, alors le corps $H(F(\beta))$ est égal à $k(f)$.

Les propriétés arithmétiques des valeurs $F(\beta)$ pour un point β primitif de f division (f, P)=1 sont connues cf [F1] :

Proposition 2: *Soient f un idéal de A_k premier avec P, et β un point primitif de f-division de* E.

Si f est composé, alors $F(\beta)$ *est une unité;*

Si f premier divise 2 *alors* $(F(\beta)^m) \approx f^2$ *avec* $m=[k^{(f)}:k]$

Si $f=\mathcal{Q}^{2}$, $\mathcal{Q}$ *premier divise* 2 *alors* $(F(\beta)^m) \approx \mathcal{Q}^{2}$ *avec* $m=[k^{(f)}:k]$

Si f est de la forme $\mathcal{Q}^{n}$,$\mathcal{Q}$ *premier, alors* $(F(\beta)^m) \approx \mathcal{Q}$ *avec* $m=[k^{(f)}:k]$.

Pour démontrer le théorème principal il nous reste à évaluer les différences $F(\beta)-F(\beta)^\sigma$ lorsque σ décrit le groupe de Galois de l'extension $k^{(f)}/H$. D'après la loi de réciprocité de Shimura (cf [Sh]), si u est un idèle unité de k, alors $F(\beta)^{(u^{-1},k)}=F(u\beta)$ où $u\beta$ désigne le point primitif de f-division obtenu en multipliant β par un représentant dans A_k de u mod* f. Or :

$$F(\beta)-F(u\beta)=F(\beta)\,\frac{h(u\beta;\tau_d)-h(\beta;\tau_d)}{h(u\beta;\tau_d)-h((\tau_d-1)/3;\tau_d)} \qquad (2)$$

La valuation de $F(\beta)$ étant connue, il nous reste à déterminer celle du second facteur. Pour cela on utilise la factorisation de celui-ci à l'aide des fonctions de Siegel :

$$g(z;\tau) = e^{(-\eta(z;\tau)z/2)}\,\sigma(z;\tau)\,\Delta(\tau)^{1/12}$$

En effet on à l'égalité:

$$\frac{h(x;\tau) - h(y;\tau)}{h(z;\tau) - h(t;\tau)} = \frac{g(x+y;\tau)g(x-y;\tau)g^2(z;\tau)g^2(t;\tau)}{g(z+t;\tau)g(z-t;\tau)g^2(x;\tau)g^2(y;\tau)} \qquad (3)$$

La valuation des fonctions de Siegel $g(x;\tau)$ en un point de division x de E est connue dans le cas de la multiplication complexe (cf [K-L]) . Si φ désigne la fonction d' Euler sur les idéaux de k, on obtient :

$g(x;\tau)^{\varphi(q^n)} \approx q$ si x est primitif de q^n division, q premier

$g(x;\tau)$ si l'annulateur de x est composé.

Dans le cas qui nous intéresse, on obtient:

$$\frac{h(u\beta;\tau_d) - h(\beta;\tau_d)}{h(u\beta;\tau_d)-h((\tau_d-1)/3;\tau_d)} \approx g((u-1)\beta;\tau_d)g((u+1)\beta;\tau_d)g^2((\tau_d-1)/3;\tau_d)g^{-2}(u\beta;\tau_d)$$

Puis:

$$\frac{F(\beta)-F(u\beta)}{1-\rho} \approx g((u-1)\beta;\tau_d)g((u+1)\beta;\tau_d) \qquad (4)$$

Le calcul de la norme de $k^{(f)}/H$ du produit :

$$\prod_{\sigma \neq id} \left[\frac{F(\beta)-F(\beta)^\sigma}{1-\rho}\right]$$

donne alors le discriminant de l'extension $k^{(f)}/H$, que l'on obtient en utilisant la théorie du corps de classes (les calculs sont tout à fait analogues à ceux fait dans [C.-N,T 1] et [F 1]).

Mais puisque $F(\beta)/(1-\rho)$ n'est pas un entier algébrique, il faut pour conclure, mettre en evidence un entier a de H, vérifiant :

$$F(\beta) \equiv a \text{ modulo } (1-\rho)$$

Montrons d'abord ce résultat pour F(r), où r est un d'ordre 2. On obtient le polynôme donnant les points F(r) à partir de [F1] soit:

$$4\varepsilon^{-6} + \varepsilon^{-4}\,\alpha_d^2\,X + 2\varepsilon^{-2}\,\alpha_d\,X^2 + X^3 = 0$$

Mais le discriminant du modèle de Deuring est $\alpha_d^3 - 27$ et, d'après [F1], on a :

$$(\alpha_d^3 - 27)^2 = \frac{\Delta((\tau_d-1)/3)}{\Delta(\tau_d)}$$

Puisque le réseau engendré par τ_d-1 et 3 est en fait l'idéal P, l'idéal engendré par α_d^3 -27 est alors P^6 =(27) cf [L]. En particulier 3 divise $\varepsilon^{-2}\,\alpha_d$, ce qui montre que $F(r)^3 \equiv -4\varepsilon^{-6}$ mod 3 dans le corps $k^{(2)}$.
Mais $-4\varepsilon^{-6}$ appartient à H et les idéaux divisant P ne se ramifie pas dans $k^{(2)}/H$, donc il existe un entier a de H tel que P divise F(r)-a. Le résultat provient alors du fait que, dans H, $P = (1-\rho)$. Dans le cas général, on constate en utilisant les formes de Siegel, que :

$$\frac{F(r)-a}{1-\rho} - \frac{F(\beta)-a}{1-\rho} = \frac{F(r)-F(\beta)}{1-r}$$

est un entier algébrique, ce qui donne évidemment que $\frac{F(\beta)-a}{1-\rho}$ est aussi un entier algébrique.
Le discriminant du sous-anneau $A_H\left[\frac{F(\beta)-a}{1-\rho}\right]$ de $A_{k(f)}$, sur A_H, calculé à partir de la formule d'Euler est alors égal à celui de A_H.Il y a donc égalité entre ces deux anneaux, ce qui démontre le théorème.

Bibliographie

[C 1] J. Cougnard : Générateurs de l'anneau des entiers des corps de classes de $\mathbb{Q}(i)$ de rayon impair et points de division de $Y^2 = X^3 - X$, J. of Number Theory, à paraître.

[C 2] J. Cougnard : Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers, Acta Arithmetica, à paraître.

[C.-N, T 1] Ph. Cassou-Noguès, M. J. Taylor : Elliptic functions and rings of integers, Progress in Mathematics n° 66 Birkhauser 1987.

[C.-N, T 1] Ph. Cassou-Noguès, M. J. Taylor : Unités modulaires et monogénéité d'anneaux d'entiers, à paraître.

[D] M. Deuring : Die Typen der Multiplikatorenringe elliptisher Funktionen korper, Abh. Math. Sem. Hamburg, 14, 1941, (197-272).

[F 1] V. Fleckinger : Monogénéité de l'anneau des entiers de certains corps de rayon, Ann.Sci. Inst.Fourier Grenoble , à paraître (1988).

[F 2] V. Fleckinger : Génération de bases d'entiers à partir de la courbe $Y^2 = 4X^3 + 1$, Séminaire de Théorie des Nombres de Besançon, à paraître.

[K L] D.Kubert, S. Lang : Modular units, Grundlehren d. math. Wissenschaften 244, Springer Verlag, (1981).

[L] S. Lang : Elliptic funcions, Addison Wesley 1973.

[R] H. Rademacher : Topics in Analytic Number Theory, Springer Verlag.

[Sh] G. Shimura : Introduction to the arithmetic theory of automorphic function. Iwanami Shoten, Publishers and Princeton University Press,1971.

[T] F. Terada : A principal idéal Theorem in the genus field, Tôhoku Math. Journal 23 (1971) p. 687-718.

Vincent Fleckinger
Laboratoire de Mathématiques
U.A. CNRS 741
Facultés des Sciences
F-25030 Besançon Cedex