ANNALES DE L'INSTITUT FOURIER

VINCENT FLECKINGER

Monogénéité de l'anneau des entiers de certains corps de classes de rayon

Annales de l'institut Fourier, tome 38, n° 1 (1988), p. 17-57

<http://www.numdam.org/item?id=AIF_1988__38_1_17_0>

Ann. Inst. Fourier, Grenoble
38, 1 (1988), 17-57

MONOGÉNÉITÉ DE L'ANNEAU DES ENTIERS DE CERTAINS CORPS DE CLASSES DE RAYON

par Vincent FLECKINGER

Introduction.

Si k est un corps de nombres, on note A_k son anneau d'entiers. Pour tout idéal $\mathcal{A}$ de A_k on note $k(\mathcal{A})$ le corps de classes de rayon $\mathcal{A}$.

Etant donné une extension abélienne finie L d'un corps de nombres K, le théorème de l'élément primitif affirme l'existence d'un élément x de L, tel que $L = K[x]$, ce qui permet de décrire la K-algèbre L. L'analogue de ce résultat pour les anneaux d'entiers est en général faux. Cependant, lorsqu'il existe un élément x de A_L tel que $A_L = A_k[x]$, on dit que A_L est monogène sur A_k. On sait que les anneaux d'entiers des corps de classes de rayons sur $\mathbf{Q}$, sont monogènes sur $\mathbf{Z}$.

M.N. Gras [G 3] et J. Cougnard [C] ont donné respectivement des conditions nécessaires de monogénéité pour les anneaux d'entiers des extensions abéliennes de $\mathbf{Q}$, et de corps quadratiques imaginaires, qui montrent que ce phénomène est très particulier.

D'autre part Ph. Cassou-Noguès et M.J. Taylor, à l'aide de la théorie de la multiplication complexe et du modèle de Fueter pour

Mots-clés : Corps de Classes – Anneaux d'entiers – Fonctions elliptiques.

les courbes elliptiques, ont démontré des théorèmes de monogénéité, et exhibé des générateurs pour les anneaux d'entiers des extensions de la forme $k(4\mathcal{A})/k(4)$ ou $k(4)k(\mathcal{A})/k(4)$, où $k(\mathcal{A})$ désigne le corps des classes de rayon du corps k, relatif à l'idéal $\mathcal{A}$, lorsque k est quadratique imaginaire dans lequel 2 est totalement décomposé, et $\mathcal{A}$ un idéal premier avec 2, [C-N, T1].

Ils en ont récemment déduit des théorèmes de monogénéité pour les extensions $k(\mathcal{A})/H$, où H désigne le corps des classes de Hilbert de k, [C-N, T2]. On peut alors se demander si ce dernier résultat se généralise sous la forme suivante :

Les anneaux d'entiers des corps des classes de rayon d'un corps k quadratique imaginaire sont monogènes sur l'anneau des entiers du corps des classes de Hilbert H de k.

Cet article donne un analogue des résultats de monogénéité de [C-N, T1] : utilisant cette fois le modèle de Deuring, $y^2+\alpha xy+y = x^3$ ([D], §5, p. 231), et considérant de nouvelles fonctions elliptiques F_Ω, définies au §4, on obtient les résultats suivants :

HYPOTHÈSES. – k est un corps quadratique imaginaire, d'anneau des entiers A_k, dans lequel 3 est décomposé : $3 = \mathfrak{p}\mathfrak{p}'$.

NOTATIONS. – H désigne le corps des classes de Hilbert de $k, K = k(9), K' = k(3)$ et E le sous-corps de K, contenant $k(3)$ et distinct de $k(3\mathfrak{p}), k(3\mathfrak{p}')$ et de $H(\zeta_g)$. Si $\mathfrak{M}$ est un idéal premier de k, on note $v_{\mathfrak{M}}$ la valuation correspondante, ou plus simplement v, lorsqu'il n'y a pas d'ambiguïté.

THÉORÈME 1. — *Soit $\mathcal{A}$ un idéal entier de k, premier avec 3. On note :*

$$L = k(9\mathcal{A}) \text{ et } M = Kk(\mathcal{A}).$$

Soit λ (resp. φ) un point primitif de $\mathcal{A}$ division, (resp. de 9-division), de $\mathbf{C}/A_k$ on pose $\beta = \lambda + \varphi$. Alors :

(i) $A_L = A_K[F(\beta)]$.

(ii) $A_M = A_K[F(\lambda)]$ *dès que* $v(\mathcal{A}) > v(2)$ *pour les places au-dessus de 2 qui divisent $\mathcal{A}$.*

On obtient même un raffinement de ce résultat :

THÉORÈME 2. — *Soit $\mathcal{A}$ un idéal entier de k, premier avec 3. On note :*

$$L = k(9\mathcal{A}),\ M'' = Ek(\mathcal{A}),\ \text{et}\ M' = K'k(\mathcal{A}).$$

Soit λ (resp. φ) un point primitif de $\mathcal{A}$ division, (resp. de 9-division), de $\mathbf{C}/A_k$ on pose $\beta = \lambda + \varphi$, alors :

(i') $A_L = A_E[F(\beta)]$.

(ii') $A_{M''} = A_E[F(\lambda)]$

(ii') *il existe une racine cubique δ de $(\alpha^3 - 27)^2$ telle que $A_{M'} = A_{K'}[\delta F(\lambda)]$ dès que $v(\mathcal{A}) > v(2)$ pour les places au-dessus de 2 qui divisent $\mathcal{A}$.*

Plan de l'article.

Le paragraphe 1 donne une paramétrisation analytique du modèle de Deuring.

Le paragraphe 2 concerne l'étude du coefficient α. On montre en particulier que α peut être exprimé comme valeur d'une forme modulaire pour $\Gamma_0(9)$.

Les paragraphes 3 et 4 concernent l'étude des valeurs aux points de division de $\mathbf{C}/\Omega$, de la première coordonnée x du modèle de Deuring.

Le paragraphe 5 contient les démonstrations des théorèmes énoncés précédemment.

Dans le paragraphe 6, on traite le cas des corps quadratiques imaginaires dont l'anneau des entiers est principal, et dans lesquel 3 est décomposé.

1. Le modèle de Deuring.

Soient Ω un réseau de $\mathbf{C}$, et P_Ω la fonction de Weierstrass associée. A tout point f non nul de 3-division de $\mathbf{C}/\Omega$, on associe la fonction :

$$x_\Omega(z;f) = \frac{P_\Omega(z) - P_\Omega(f)}{P'_\Omega(f)^{2/3}}$$

où $P'_\Omega(f)^{1/3}$ désigne une racine cubique de $P'_\Omega(f)$ fixée une fois pour toute. Sachant que les zéros de P'_Ω sont les points de 2-division, on a $P'_\Omega(f) \neq 0$. Lorsque Ω et f sont fixés sans ambiguïté, on note x cette fonction et P la fonction P_Ω.

On déduit des propriétés de la fonction P que x est une fonction elliptique pour Ω, paire, de diviseur :

$$(x) = (f) + (-f) - 2(0).$$

On désigne maintenant par x_1 la dérivée normalisée de x :

$$x_1(z) = \frac{x'(z)}{P'_\Omega(f)^{1/3}} \cdot$$

Enfin on pose :

$$\alpha_\Omega(f) = \frac{12P^2_\Omega(f) - g_2(\Omega)}{2P'_\Omega(f)^{4/3}} \cdot$$

PROPOSITION 1.1. — *On a l'équation :*

$$x_1^2 = 4x^3 + \alpha^2 x^2 + 2\alpha x + 1.$$

Démonstration. — Posons $e = P(f)$ et $\lambda = P'(f)^{-2/3}$. On déduit de la définition de x_1 et de l'équation de Weierstrass, l'égalité :

$$x_1^2(z) = \lambda^3(4P^3(z) - g_2P(z) - g_3). \tag{1.2}$$

Soit $h(z) = 4x^3 + \alpha^2 x^2 + 2\alpha x + 1$. On déduit de la définition de x l'égalité :

$$h(z) = 4\lambda^3 P^3 + (\alpha^2\lambda^2 - 12\lambda^3 e)P^2 + (12\lambda^3 e^2 - 2\alpha^2\lambda^2 e + 2\alpha\lambda)P - 4\lambda^3 e^3 + \alpha^2\lambda^2 e^2 - 2\alpha\lambda e + 1. \tag{1.3}$$

Il suffit donc de vérifier :

$$\alpha^2 = 12\lambda e;\ 2\alpha = \lambda^2(12e^2 - g_2);\ \lambda^3(4e^3 - g_2 e - g_3) = 1. \tag{1.4}$$

Les deux dernières équations sont vérifiées par définition de α et λ. Le système est compatible si et seulement si :

$$48\lambda e = \lambda^4(12e^2 - g_2)^2\ ,$$

soit encore :

$$48e^4 - 24e^2 g_2 - 48 g_3 e - g_2^2 = 0\,. \tag{1.5}$$

Or on sait, (cf. [L 2], chap. 2, §1, égalité (6)), que les racines du polynôme

$$48X^4 - 24g_2X^2 - 48g_3X - g_2^2$$

forment l'ensemble $\{P(f),\ f$ non nul de 3-division dans $\mathbb{C}/\Omega\}$, ce qui achève la démonstration.

COROLLAIRE 1.6. — *On a les égalités suivantes :*

$$\text{(i)} \qquad \alpha^3(f) = \frac{288P^2(f)}{12P^2(f) - g_2}$$

$$\text{(ii)} \qquad x(z,f) = \alpha^2(f)\frac{P(z) - P(f)}{12P(f)}\ .$$

On écrit d'abord $\alpha^3 = (\alpha^2)^2/\alpha$.

Les égalités (i) et (ii) sont alors les conséquences immédiates de (1.4).

Remarque. — On appelle modèle de Deuring de la courbe elliptique E définie par $\mathbb{C}/\Omega$, l'équation (1.1).

On passe du modèle de Deuring habituel (voir par exemple [D]) $y^2 + \alpha xy + y = x^3$ à l'équation (1.1) en faisant le changement de variable :

$$x_1 = 2y + \alpha x + 1.$$

PROPOSITION 1.7. — *Soit D le discriminant du modèle de Deuring de la courbe elliptique E, on a :*

(i) $D = \alpha^3 - 27$

(ii) *D est racine du polynôme $X^4 + 36X^3 + 270X^2 + (756 - j)X + 3^6$ où j désigne l'invariant modulaire de E.*

En utilisant les formules dues à John Tate ([L 1], App. 1, § 1, p. 299), on obtient

$$D = \alpha^3 - 27 \text{ et } (\alpha^3 - 27)j = \alpha^3(\alpha^3 - 24)^3.$$

On en déduit immédiatement (i) et (ii).

Remarque 1.8 — L'égalité

$$j(\Omega) = \frac{12^3 g_2(\Omega)}{\Delta(\Omega)} = \frac{\alpha_\Omega^3(f)(\alpha_\Omega^3(f) - 24)^3}{\alpha_\Omega^3(f) - 27}$$

joue un rôle important dans le paragraphe suivant.

PROPOSITION 1.9. — *On a les relations :*

(i) $x(z)x(z+f)x(z+2f) = -1$,

(ii) $x_1(z)x_1(z+r)x_1(z+s)x_1(z+r+s) = D$,

où $\{r, s, r+s\}$ sont les points non nuls de 2-division de $\mathbb{C}/\Omega$.

Démonstration. — La fonction $x(z)x(z+f)x(z+2f)$ est de diviseur nul, elle est donc constante. Faisons tendre z vers 0, on obtient les limites suivantes :

$z^2x(z)$ tend vers $P'(f)^{-2/3}$,

$x(z+f)/z$ tend vers $x'(f) = P'(f)^{1/3}$, et

$x(z+2f)/z$ tend vers $x'(2f) = x'(-f) = -P'(f)^{1/3}$.

Ce qui donne le résultat (i).

Le diviseur de la fonction $x_1(z)x_1(z+r)x_1(z+s)x_1(z+r+s)$ est nul, cette fonction est donc constante. Faisons tendre z vers 0, on obtient les limites suivantes :

$z^3x_1(z)$ tend vers $-2/P'(f)$

$x_1(z+r)/z$ tend vers $x_1'(r)$,

$x_1(z+s)/z$ tend vers $x_1'(s)$,

$x_1(z+r+s)/z$ tend vers $x_1'(r+s)$.

En dérivant l'égalité (1.1) on obtient :

$$x_1'x_1 = (6x^2 + \alpha^2 x + \alpha)x'$$

soit encore :

$$x_1' = (6x^2 + \alpha^2 x + \alpha)P'(f)^{1/3}.$$

Le produit $x_1'(r)x_1'(s)x_1'(r+s)$ est donc égal au 16-ième du résultant des polynômes :

$$(6x^2 + \alpha^2 x + \alpha)P'(f)^{1/3} \quad \text{et} \quad 4x^3 + \alpha^2 x^2 + 2\alpha x + 1,$$

soit :

$$\frac{P'(f)(27 - \alpha^3)}{2}$$

finalement on obtient :

$$\frac{-2x_1'(r)x_1'(s)x_1'(r+s)}{P'(f)} = D \cdot$$

Ce qui démontre (ii).

II. Etude du coefficient α.

Le but de ce paragraphe est d'exprimer $\alpha_\Omega(f)$ comme valeur de certaines formes modulaires de niveau 9.

En utilisant les propriétés d'homogénéité des fonctions $P_\Omega(z)$ et $g_2(\Omega)$, on déduit de ((1.6),(i)) que $\alpha^3_\Omega(f)$ est homogène de degré 0, c'est-à-dire :

$$\alpha^3_{\lambda\Omega}(\lambda f) = \alpha^3_\Omega(f)$$

pour tout λ élément de $\mathbb{C}^*$.

Si $\Omega = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ où $\tau = \omega_1/\omega_2$ appartient au demi-plan de Poincaré, noté $\mathfrak{h}$, on en déduit :

$$\alpha^3_\Omega(f) = \alpha^3_{\Omega_\tau}(u\tau + v)$$

où (u, v) est élément de $((1/3\mathbb{Z})/\mathbb{Z})^2$, $(u, v) \neq (0, 0)$ et $\Omega_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$. Puisque $\alpha^3_\Omega(f) = \alpha^3_\Omega(-f)$ il nous suffit donc d'étudier les fonctions $A_{(u,v)}$ définies sur $\mathfrak{h}$ par :

$$A_{(u,v)}(\tau) = \alpha^3_{\Omega_\tau}(u\tau + v)$$

avec (u, v) dans $T = \{(0, 1/3),\ (1/3, 0),\ (1/3, 1/3),\ (1/3, -1/3)\}$.

Pour tout entier n on note ζ_n une racine primitive n-ième de 1.

PROPOSITION 2.1. – *Les fonctions $A_{(u,v)}$ sont des fonctions modulaires pour $\Gamma(3)$ et l'on a :*

$$(A_{(0,1/3)} - 27)^2 = 3^{12}\frac{\Delta(3\tau)}{\Delta(\tau)}$$

$$(A_{(1/3,1/3)} - 27)^2 = \frac{\Delta\left(\frac{\tau+1}{3}\right)}{\Delta(\tau)}$$

$$(A_{(1/3,-1/3)} - 27)^2 = \frac{\Delta\left(\frac{\tau-1}{3}\right)}{\Delta(\tau)}$$

$$(A_{(1/3,0)} - 27)^2 = \frac{\Delta\left(\frac{\tau}{3}\right)}{\Delta(\tau)}$$

où Δ désigne la fonction delta usuelle.

Démonstration. — Puisque $SL_2(\mathbb{Z})$ opère sur $((1/3)\mathbb{Z}/\mathbb{Z})^2$ on en déduit une action naturelle de ce groupe sur l'ensemble des fonctions $A_{(u,v)}$:

$$(s, A_{(u,v)}) \longmapsto A_{(u,v)s^{-1}} .$$

On vérifie aisément l'égalité :

$$A_{(u,v)}(s^{-1}\tau) = A_{(u,v)s^{-1}}(\tau) . \tag{2.2}$$

Soient :

$$s_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad s_1 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

On déduit de (2.2) :

$$\begin{cases} A_{(0,1/3)}(s_0\tau) = A_{(1/3,0)}(\tau) \\ A_{(0,1/3)}(s_1\tau) = A_{(1/3,1/3)}(\tau) \\ A_{(0,1/3)}(s_2\tau) = A_{(1/3,-1/3)}(\tau). \end{cases} \tag{2.3}$$

Donc $SL_2(\mathbb{Z})$ opère transitivement sur l'ensemble $\{A_{(u,v)}\}$ et le stabilisateur de $A_{(0,1/3)}$ est $\Gamma_0(3)$. Pour démontrer (2.1) il suffit donc, grâce à (2.3) de vérifier que $A_{(0,1/3)}$ est une fonction modulaire pour $\Gamma_0(3)$ et satisfait l'égalité :

$$(A_{(0,1/3)}(\tau) - 27)^2 = 3^{12}\frac{\Delta(3\tau)}{\Delta(\tau)} . \tag{2.4}$$

Montrons, pour commencer, que $A_{(0,1/3)}$ est modulaire pour $\Gamma_0(3)$. Par (1.6) nous obtenons :

$$A_{(0,1/3)}(\tau) = \frac{288P^2_{\Omega_\tau}(1/3)}{12P^2_{\Omega_\tau}(1/3) - g_2(\Omega_\tau)} . \tag{2.5}$$

D'autre part d'après la définition de α, $A_{(0,1/3)}$ est sans pôle sur $\mathfrak{h}$. On déduit alors des propriétés des fonctions P et g_2 et de

(2.5) que $A_{(0,1/3)}$ est une fonction holomorphe sur $\mathfrak{h}$. Etudions son comportement aux pointes $\{\infty, 0\}$ de Γ_0 (3). On pose $q = e^{2i\pi\tau}$ et $q_z = e^{2i\pi z}$.

D'après ([L 1], chap. 4, prop. 3 et 4) on a, pour la pointe infinie, les développements de Fourier suivants :

$$(2.6)\qquad \begin{cases} g_2(\Omega_\tau) = \dfrac{(2i\pi)^4}{12}\left(1 + 240\sum_{n=1}^{\infty}\dfrac{n^3 q^n}{1-q^n}\right) \\ P_{\Omega_\tau}(z) = (2i\pi)^2\left(\dfrac{1}{12} + \sum_{m\in\mathbb{Z}}\dfrac{q^m q_z}{(1-q^m q_z)^2} - 2\sum_{n=1}^{\infty}\dfrac{nq^n}{1-q^n}\right). \end{cases}$$

De (2.5) et (2.6) on obtient :

$$(2.7)\qquad A_{(0,1/3)}(\tau) = 27 + 729q + o(q).$$

On remarque en outre que les coefficients de Fourier du développement (2.7) appartiennent à $\mathbb{Q}$.

Puisque $s_0(\infty) = 0$ pour obtenir le développement de Fourier de $A_{(0,1/3)}$ en la pointe 0, il suffit de déterminer le développement de Fourier de $A_{(1/3,0)}$ en la pointe ∞. Grâce à (2.5) et (2.6) on a :

$$(2.8)\qquad A_{(1/3,0)}(\tau) = q^{-1/3} + o(q^{1/3}).$$

On conclut de (2.7) et (2.8) que $A_{(0,1/3)}$ est une fonction modulaire pour $\Gamma_0(3)$ et holomorphe sur $\mathfrak{h}$.

On considère la fonction :

$$B(\tau) = \frac{(A_{(0,1/3)}(\tau) - 27)^2}{3^{12}(\Delta(3\tau)/\Delta(\tau))}.$$

On sait que les fonctions $\Delta(\tau)$ et $\Delta(3\tau)$ sont holomorphes et sans zéro sur $\mathfrak{h}$. $A_{(0,1/3)}(\tau) - 27$ est holomorphe sur $\mathfrak{h}$, et est égal au discriminant associé à un modèle de Deuring de $\mathbb{C}/\Omega_\tau$, donc ne s'annule pas sur $\mathfrak{h}$. B est donc une fonction modulaire pour $\Gamma_0(3)$ holomorphe et sans zéros sur $\mathfrak{h}$.

Par [L 1], Chap. 18, §4, (8) on obtient :

$$(2.9)\qquad 3^{12}\Delta(3\tau)/\Delta(\tau) = 3^{12}q^2 + o(q^2).$$

De (2.7) et (2.9) on déduit que B est holomorphe et sans zéro en la pointe ∞. Comme B ne peut avoir à la fois un zéro, et un pôle en la pointe 0, B est holomorphe sur $\mathfrak{h}$ et aux pointes. B est donc constante et sa valeur se déduit du développement de Fourier à l'infini, soit $B = 1$. Ce qui achève la démonstration du théorème (2.1).

De (1.8) on déduit l'égalité :

$$A^3_{(u,v)}(\tau) = 12^3 \frac{g_2^3(\tau)(A_{(u,v)} - 27)}{\Delta(\tau)(A_{(u,v)} - 24)^3}. \tag{2.10}$$

On introduit alors la fonction êta de Dedekind définie par :

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty}(1 - q^n) \tag{2.11}$$

et on rappelle l'égalité :

$$(2i\pi)^{12}\eta^{24}(\tau) = \Delta(\tau). \tag{2.12}$$

Il est alors facile de déduire de (2.1), (2.10) et (2.12) une racine cubique de $A_{(u,v)}$. Soit $(u, v) \in ((1/3)\mathbb{Z}/\mathbb{Z})^2$ on pose :

$$\begin{cases} l_{(0,1/3)}(\tau) = \dfrac{108}{(2i\pi)^4} \dfrac{g_2(\tau)\eta^4(3\tau)}{\eta^{12}(\tau)(A_{(0,1/3)}(\tau) - 24)} \\ l_{(u,v)}(\tau) = \dfrac{12}{(2i\pi)^4} \dfrac{g_2(\tau)\eta^4(u\tau + v)}{\eta^{12}(\tau)(A_{(u,v)}(\tau) - 24)} \\ \qquad \text{si } (u, v) \neq (0, 0), (0, 1/3). \end{cases} \tag{2.13}$$

COROLLAIRE 2.14.

(i) $l_{(0,1/3)}$ *est une fonction modulaire pour* $\Gamma_0(9)$, *rationnelle sur* $\mathbb{Q}(\zeta_g)$ *telle que* $l^3_{(0,1/3)} = A_{(0,1/3)}$.

(ii) $l_{(u,v)}$ *pour* $(u, v) \neq (0, 0)$ *et* $(0, 1/3)$ *est une fonction modulaire pour* $\Gamma(9)$ *rationnelle sur* $\mathbb{Q}(\zeta_g)$, *telle que* $l^3_{(u,v)} = A_{(u,v)}$.

Démonstration. — Les démonstrations de (i) et (ii) sont semblables. On se limite à la démonstration de (i). On pose $l(\tau) = l_{(0,1/3)}(\tau)$.

D'après (2.1) et (2.13) on a $l(\tau)^3 = \pm A_{(0,1/3)}(\tau)$, dont l n'admet pas de pôle sur $\mathfrak{h}$. On déduit alors des propriétés de la fonction η que l est holomorphe sur $\mathfrak{h}$. On connaît l'action de $SL_2(\mathbb{Z})$ sur la fonction êta de Dedekind, voir [R]

$$\eta\Big(\frac{a\tau+b}{c\tau+d}\Big) = \varepsilon(a,b,c,d)\sqrt{\frac{c\tau+d}{i}}\eta(\tau)$$

avec $\varepsilon(a,b,c,d) = \Big(\frac{c}{d}\Big) i^{(i-c)/2} e^{(i\pi/12)(bd(1-c^2)+c(a+d))}$

pour c impair

et $\varepsilon(a,b,c,d) = \Big(\frac{c}{d}\Big) e^{\pi id/4} e^{(i\pi/12)(ac(1-d^2)+d(b-c))}$

pour d impair,

où $\Big(\frac{c}{d}\Big)$ désigne le symbole de Jacobi.

On obtient alors si s est un élément de $\Gamma_0(3)$, défini par $s(\tau) = (a\tau+b)/(3c\tau+d)$:

$$\eta\Big(3\frac{a\tau+b}{3c\tau+d}\Big) = \eta\Big(\frac{a3\tau+3b}{c3\tau+d}\Big) = \varepsilon(a,3b,c,d)\eta(3\tau)$$

d'où

$$l_{(0,1/3)}(s(\tau)) = \frac{\varepsilon(a,3b,c,d)^4}{\varepsilon(a,b,3c,d)^{12}} l_{(0,1/3)}(\tau)$$

puis, si c est impair, on a :

$$\frac{\varepsilon(a,3b,c,d)^4}{\varepsilon(a,b,3c,d)^{12}} = \frac{i^{(1-c)} e^{\pi i(3bd(1-c^2)+c(a+d))/3}}{i^{(1-3c)} e^{\pi i(bd(1-9c^2)+3c(a+d))}}$$
$$= e^{-8\pi ic(a+d)/3} = e^{-2\pi ic(a+d)/3}$$

et si d est impair :

$$\frac{\varepsilon(a,3b,c,d)^4}{\varepsilon(a,b,3c,d)^{12}} = \frac{e^{\pi id} e^{\pi i(ac(1-d^2)+d(3b-c))/3}}{e^{3\pi id} e^{\pi i(3ac(1-d^2)+d(b-3c))}} = e^{-8\pi i(ac(1-d^2)-cd)/3}$$

où plus simplement, sachant que $ad \equiv 1 \bmod 3$, donc $a \equiv d \bmod 3$:

$$l(s(\tau)) = e^{2\pi ica/3} l(\tau).$$

On vérifie immédiatement que $l_{(0,1/3)}$ est invariante pour $\Gamma_0(9)$. Donc $l_{(0,1/3)}$ est modulaire pour $\Gamma_0(9)$. Il est immédiat d'après (2.7) et (2.11) que les développements de Fourier en $e^{2i\pi\tau/9}$ de $l_{(0,1/3)}$ ont leurs coefficients dans $\mathbb{Q}(\zeta_9)$. On en déduit grâce à la proposition 6.9 de [Sh] que $l_{(0,1/3)}$ est rationnelle sur $\mathbb{Q}(\zeta_9)$. D'après l'égalité (2.10) on a :

$$l(\tau)^3 = \pm A_{(0,1/3)} ,$$

la comparaison des coefficients de Fourier en la pointe ∞, donne l'égalité :

$$l(\tau)^3 = A_{(0,1/3)} .$$

COROLLAIRE 2.15. – $l_{(0,1/3)}(\tau)$ *appartient à* $\mathbb{Q}(j(\tau), j(9\tau))$.

Cela résulte de (2.14), et des théorèmes 5 et 7 de [L 1], Chap. 6, §4.

III. Formules de multiplication.

On fixe un réseau Ω et un point f, non nul de 3-division de $\mathbb{C}/\Omega$. Les fonctions x, x_1 et α considérées sont définies par ce choix.

Puisque $(z \longmapsto x(nz))$ est une fonction elliptique paire pour Ω, il existe $N_n(X)$ et $D_n(X)$ dans $\mathbb{C}[X]$ tels que :

$$x(nz) = \frac{N_n(x(z))}{D_n(x(z))}.$$

En effet la fonction x étant une fonction affine de la fonction P de Weierstrass, le corps des fonctions elliptiques paires, relatives au réseau Ω, est $\mathbb{C}(x(z))$. On s'intéresse alors aux polynômes $N_n(X)$ et $D_n(X)$.

La formule d'addition de la fonction P nous donne :

$$P(2z) = -2P(z) + \frac{1}{4}\left(\frac{P''(z)}{P'(z)}\right)^2. \tag{3.1}$$

On a alors :

PROPOSITION 3.2.

$$x(2z) = \frac{x^4(z) - \alpha x^2(z) - 2x(z)}{x_1^2(z)}.$$

Démonstration. — D'après la définition de x, on a :

$$P(z) = x(z)P'(f)^{2/3} + P(f);\ P'(z) = x'(z)P'(f)^{2/3};$$

$$P''(z) = x''(z)P'(f)^{2/3}$$

soit encore en utilisant la fonction x_1 et la proposition 1.1 :

$$P(z) = x(z)P'(f)^{2/3} + P(f);\ P'(z) = x_1(z)P'(f);$$

$$P''(z) = (6x^2 + \alpha^2 x + \alpha)P'(f)^{4/3}.$$

Puis en utilisant (3.1) et l'égalité :

$$\alpha^2 = \frac{12P(f)}{P'(f)^{2/3}}$$

on obtient :

$$x(2z) = -2x(z) - \frac{\alpha^2}{4} + \frac{(6x^2 + \alpha^2 x + \alpha)^2}{4x^3 + \alpha^2 x^2 + 2\alpha x + 1}$$

le résultat s'en déduit.

Soit $n \geq 0$. On définit les polynômes :

(3.3)
$Q_1(X) = 1 = Q_2(X)$

$Q_{2n+1}(X) = (2n+1)\Pi'(X - x(u))$, si $n \geq 1$, où u parcourt un demi-système de représentants des points non nuls de $(2n+1)$-division de $\mathbb{C}/\Omega$, (c'est-à-dire que $\{-u, u\}$ parcourt un système complet).

$Q_{2n}(X) = 2n\Pi'(X - x(x))$, si $n \geq 1$, où u parcourt un demi-système de représentants des points non nuls de $2n$-division, non annulés par 2, de $\mathbb{C}/\Omega R(X) = (4X^3 + \alpha^2 X^2 + 2\alpha X + 1)^2$.

Pour tout entier $n \geq 0$ (resp. ≥ 1) on pose :

(3.4) $f_{2n+1}(z) = Q_{2n+1}(x(z))$, (resp. $f_{2n}(z) = x_1(z)Q_{2n}(x(z))$).

Après une transformation affine des formules de multiplication pour la fonction P de Weierstrass ([L 2], chap. 2, § 1), on obtient :

$$x(nz) = x(z) - \frac{f_{n+1}(z)f_{n-1}(z)}{f_n^2(z)}, \text{ si } n \geq 2 \tag{3.5}$$

et

$$\begin{cases} f_4 & = x_1(2z)x_1(z)^4 \\ f_{2n+1} & = f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}, \text{ si } n \geq 2 \\ f_{2n}f_2 & = f_n(f_{n+2}f_{n-1}^2 - f_{n+1}^2 f_{n-2}), \text{ si } n \geq 3. \end{cases} \tag{3.6}$$

De (3.2), (3.4) et (3.5) on déduit :

$$Q_3(X) = 3X^4 + \alpha^2 X^3 + 3\alpha X^2 + 3X \tag{3.7}$$

et de (3.2), (3.4) et (3.6) :

$$Q_4(X) = 2X^6 + \alpha^2 X^5 + 5\alpha X^4 + 10X^3 - \alpha X - 1\ . \tag{3.8}$$

A partir de (3.4) et de (3.6) on obtient les relations de récurrence suivantes :

$$\begin{cases} Q_{4n} & = Q_{2n}(Q_{2n+2}Q_{2n-1}^2 - Q_{2n-2}Q_{2n+1}^2 \\ Q_{4n+1} & = RQ_{2n+2}Q_{2n}^3 - Q_{2n+1}^3 Q_{2n-1} \\ Q_{4n+2} & = Q_{2n+1}(Q_{2n+3}Q_{2n}^2 - Q_{2n-1}Q_{2n+2}^2) \\ Q_{4n+3} & = Q_{2n+3}Q_{2n+1}^3 - RQ_{2n+2}^3 Q_{2n}. \end{cases} \tag{3.9}$$

THÉORÈME 3.10.

(i) *$Q_n(X)$ est un polynôme de $\mathbb{Z}[\alpha][X]$, de coefficient dominant égal à $n/(n,2)$, où $(n,2)$ désigne le pgcd de n et 2,*

(ii) *$Q_n(0) = 1$ si n est congru à 1 ou 2 modulo 6,*

(iii) *$Q_n(0) = -1$ si n est congru à 4 ou 5 modulo 6,*

(iv) *$Q_n(0) = 0$ et $Q_n'(0) = n$ si n est congru à 3 modulo 6,*

(v) *$Q_n(0) = 0$ et $Q_n'(0) = -n$ si n est congru à 0 modulo 6.*

Puisque les polynômes $R(X)$ et $Q_k(X)$ sont éléments de $\mathbb{Z}[\alpha][X]$, pour $1 \leq k \leq 4$, on démontre (i) par récurrence sur n à

partir de (3.9). De même la démonstration de (ii), (iii), (iv) et (v) se fait par récurrence sur n.

COROLLAIRE 3.11. – *Pour tout entier $n \geq 2$ on a l'égalité :*

$$x(nz) = \frac{N_n(x(z))}{D_n(x(z))}$$

où $N_n(X)$ est un polynôme unitaire de degré n^2 de $\mathbb{Z}[\alpha][X]$, et $D_n(X)$ est un polynôme degré $n^2 - 1$ de $\mathbb{Z}[\alpha][X]$.

Démonstration. — D'après la définition des Q_n, on vérifie que le degré de Q_{2n} est $(2n^2 - 2)$ et que celui de $Q_{2,+1}$ est $2n^2 + 2n$.

Grâce à (3.5) on obtient :

$$(3.12)\quad \begin{cases} N_{2n}(X) & = X(4X^3 + \alpha^2 X^2 + 2\alpha X + 1)Q_{2n}^2(X) \\ & \qquad -Q_{2n-1}(X)Q_{2n+1}(X) \\ D_{2n}(X) & = (4X^3 + \alpha^2 X^2 + 2\alpha X + 1)Q_{2n}^2(X). \end{cases}$$

On en déduit immédiatement le résultat dans ce cas.

De même :

$$\begin{aligned} N_{2n+1}(X) &= XQ_{2n+1}^2(X) - (4X^3 + \alpha^2 X^2 + 2\alpha X + 1) \\ &\qquad Q_{2n}(X)Q_{2n+2}(X) \\ D_{2n+1}(X) &= Q_{2n+1}^2(X). \end{aligned}$$

Et le résultat est encore immédiat.

Remarque. — On déduit de (3.10) (iv) et (v) que si $(n, 3) = 1$ alors $N_n(0) = 0$.

IV. Multiplication complexe.

On suppose dorénavant que Ω est un idéal du corps quadratique imaginaire k de discriminant inférieur à -4. Le tore $\mathbb{C}/\Omega$ est alors à multiplication complexe par l'anneau des entiers A_k de k.

On fixe un point f de 3-division de $\mathbb{C}/\Omega$.

Puisque $j(\Omega)$ est un entier algébrique on sait par (1.7) (ii) que α est un entier algébrique.

Enfin H désigne le corps des classes de Hilbert de k.

PROPOSITION 4.1. — *On a les égalités suivantes :*

Si f est primitif de 3-division, alors $k(\alpha^3(f)) = k(3)$.

Si 3 est décomposé dans k, $3 = \mathfrak{p}\mathfrak{p}'$ et si f est primitif de $\mathfrak{p}$ ou $\mathfrak{p}'$-division, alors $k(\alpha^3(f)) = H$.

Démonstration. — Soit h la première fonction de Weber :

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

De (1.6) (i), on déduit l'expression de α^3 :

$$\alpha^3(f) = \frac{288h^2(f)}{12h^2(f) - \dfrac{2^{14}3^{10}g_2^3 g_3^2}{\Delta^2}} = \frac{24h^2(f)}{h^2(f) - \dfrac{2^{12}3^9 g_2^3 g_3^2}{\Delta^2}};$$

mais on a :

$$j = 12^3 \frac{g_2^3}{\Delta} \text{ et } \Delta = g_2^3 - 27g_3^2, \text{ d'où } 27\frac{g_3^2}{\Delta} = \frac{j}{12^3} - 1,$$

on en déduit :

$$\alpha^3(f) = \frac{24h^2(f)}{h^2(f) - j(j - 12^3)}.$$

On constate que c'est une fonction homographique de h^2 à coefficient dans $\mathbb{Q}(j)$. De l'égalité (1.5), et de l'expression de $h(f)$ en fonction de $P(f)$, on déduit :

$$48h^4(f) - 2^{17}3^{11}\frac{g_2^3 g_3^2}{\Delta^2}h^2(f) + 2^{25}3^{16}\frac{g_2^3 g_3^4}{\Delta^3}h(f) - 2^{28}3^{20}\frac{g_2^6 g_3^4}{\Delta^4} = 0$$

puis

$$h^4(f) - 6j(j - 12^3)h^2(f) + 8j(j - 12^3)^2 h(f) - 3j^2(j - 12^3)^2 = 0.$$

Si $j = 0$, alors $k = \mathbb{Q}(\zeta_3)$ de discriminant -3, et si $j = 12^3$ alors $k = \mathbb{Q}(\zeta_4)$ de discriminant -4. Donc sous l'hypothèse faite sur le discriminant de k, $j(j - 12^3)$ est non nul, et $k(j, h(f)) = k(j, h^2(f))$.

D'après (1.7) (ii), j appartient à $\mathbb{Q}(\alpha^3(f))$. On en conclut que $h^2(f)$ appartient à $\mathbb{Q}(\alpha^3(f))$, donc $k(\alpha^3(f)) = k(j, h(f))$.

Si f est primitif de 3-division, d'après ([L 1], chap. 10, § 3) on a $k(j, h(f)) = k(3)$.

Si f est primitif de $\mathfrak{p}$ (ou $\mathfrak{p}'$)-division, alors $k(j, h(f)) = k(\mathfrak{p})$ (ou $k(\mathfrak{p}')$), mais ces deux corps coïncident avec le corps de classes de Hilbert H de k.

Dans la suite, on désigne par α une racine cubique de α^3, engendrant le corps de rupture du polynôme $X^3 - \alpha^3$ sur $k(\alpha^3)$.

COROLLAIRE 4.2. — *Supposons que l'idéal* 3 *est décomposé dans* k, $3 = \mathfrak{p}\mathfrak{p}'$ *alors :*

(i) *Si f est primitif de 3-division, $k(\alpha)$ est le sous-corps E de K, contenant $k(3)$ et distinct de $k(3\mathfrak{p})$, $k(3\mathfrak{p}')$ et de $H(\eta_9)$. De plus $\alpha^3 - 27$ est une unité.*

(ii) *Si f est primitif de $\mathfrak{p}$ (resp. $\mathfrak{p}'$)-division, alors $k(\alpha) = H$. De plus on a : $(\alpha^3 - 27) = \mathfrak{p}^6$ (resp. $(\alpha^3 - 27) = \mathfrak{p}'^6$).*

Démonstration. — D'après 2.14, et ([L 1], Chap. 10, § 2, corollaire du théorème 2) les quantités $l_{(u,v)}(\tau)$, où $(u, v) \in ((1/3)\mathbb{Z}/\mathbb{Z})^2$ sont dans $k(9)$.

(i) Soit f un point primitif de 3-division. D'après 4.1, $k(\alpha^3) = k(3)$, et puisque 3 est décomposé dans k, $k(3) = H(\zeta_3)$.

Supposons d'abord que $f = 1/3$, puisque $k(\alpha^3)$ contient η_3, on peut alors choisir

$$\alpha(f) = l_{(0,1/3)}(\tau) .$$

Soient :

u l'idèle unité de k défini par $u_{\mathfrak{p}} = 4$, $u_{\mathfrak{p}'} = 4$, et $u_v = 1$ pour les autres places.

u' l'idèle unité de k défini par $u'_{\mathfrak{p}} = 4$, $u'_{\mathfrak{p}'} = 7$, et $u'_v = 1$ pour les autres places.

Le groupe $k^* < u > U_9$ correspond alors au sous-corps E de K, et $k^* < u' > U_9$ à $H(\zeta_9)$.

L'action de l'automorphisme (u, k) sur $l_{(0,1/3)}(\tau)$ est donné par la matrice diagonale :

$$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

Celle-ci laisse $l_{(0,1/3)}(\tau)$ fixe, donc $k(l_{(0,1/3)}(\tau))$ est contenu dans E.

De même l'action de (u', k) sur $l_{(0,1/3)}(\tau)$ est donnée par la matrice de déterminant 28 :

$$\frac{1}{\tau_1 - \tau_2}\begin{pmatrix} 4\tau_1 - 7\tau_2 & 3\tau_1\tau_2 \\ -3 & (7\tau_1 - 4\tau_2 \end{pmatrix}$$
$$= \frac{1}{\tau_1 - \tau_2}\begin{pmatrix} 4\tau_1 - 7\tau_2 & 3\tau_1\tau_2/28 \\ -3 & (7\tau_1 - 4\tau_2)/28 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 28 \end{pmatrix}$$

où (τ_1, τ_2) désigne le plongement de τ dans $\mathbb{Q}_3^2 = k_{\mathfrak{p}}k_{\mathfrak{p}'}$, donné par les racines du polynôme minimal de τ sur $\mathbb{Q}$. En effet on peut écrire dans $\mathbb{Q}_3^2$, l'action de u' sur le réseau $(\tau_1, \tau_2)\mathbb{Z}_3 + (1,1)\mathbb{Z}_3$:

$$(4\tau_1, 7\tau_2) = \frac{1}{\tau_1 - \tau_2}((4\tau_1 - 7\tau_2)(\tau_1, \tau_2) + 3\tau_1\tau_2(1,1))$$
$$(4,7) = \frac{1}{\tau_1 - \tau_2}(-3(\tau_1, \tau_2) + (7\tau_1 - 4\tau_2)(1,1)).$$

Comme 3 est totalement décomposé dans k, $\tau_1 - \tau_2$ est inversible dans $\mathbb{Z}_3$, et on déduit alors de l'action de $Sl_2(\mathbb{Z})$ sur $l_{(0,1/3)}$ que $l_{(0,1/3)}(\tau)$ n'est pas invariant par (u', k). On conclut alors que $k(l_{(0,1/3)}(\tau)) = E$.

On déduit le résultat dans le cas général, en utilisant le fait que E/k est galoisienne, et que le groupe $\mathrm{Gal}(k(3)/H)$ permute transitivement les $\alpha^3(f)$, où f est primitif de 3-division.

La deuxième partie de (i) résulte de [L 1], Chap. 12, § 2, Théorème 6 et de son corollaire, et de l'expression (2.1) de $\alpha^3 - 27$.

(ii) Si f est primitif de $\mathfrak{p}$ ou $\mathfrak{p}'$-division, on sait que α^3 appartient à H. D'autre part l'extension $k(\alpha)/H$ est abélienne, puisque contenue dans $k(9)$. Comme 3 est non ramifié dans H, H ne contient pas de racine primitive 3-ième de l'unité. On en conclut que α^3 est un cube dans H, et α désigne alors l'unique racine cubique de α^3 dans H (les deux autres sont dans $H(\zeta_3) = k(3)$).

La deuxième partie de (ii) résulte aussi de [L 1], Chap. 12, § 2, Théorème 6 et de son corollaire, et de l'expression (2.1) de $\alpha^3 - 27$.

Dans la suite, on se fixe un point f primitif de 3-division dans $\mathbf{C}/A_k$, et on choisit une racine cubique α correspondante.

PROPOSITION 4.3. – *Soit β un élément d'ordre n de $\mathbf{C}/\Omega$ avec $\beta \neq \pm f$. Alors :*

(i) *Si $(n,3) = 1, 1/x(\beta)$ est un entier algébrique et une unité en dehors de n.*

(ii) *Si $(n,3) \neq 1, 1/x(\beta)$ est un nombre algébrique et un entier en dehors de n.*

C'est une conséquence du théorème 3.10 et des formules (3.12), sachant que α est un entier algébrique.

Soit β un point d'ordre n de $\mathbf{C}/\Omega$ où $\beta \neq \pm f$. La proposition 4.3 nous conduit à considérer la nouvelle fonction elliptique pour Ω définie par :

$$F_\Omega(z; f) = \frac{1}{x_\Omega(z; f)}. \tag{4.4}$$

Lorsque Ω et f sont fixés, on note encore F cette fonction.

Soit $\mathcal{A}$ un idéal de A_k premier avec 3. Nous posons :

$$S_\mathcal{A}(X) = \Pi(X - F(\beta)),$$

où β parcourt un demi-système des points primitifs de $\mathcal{A}$-division de $\mathbf{C}/\Omega$.

PROPOSITION 4.5. – *Soit $\mathcal{A}$ un idéal entier de A_k premier avec 3. Alors $S_\mathcal{A}(X)$ est à coefficients dans $A_k[\alpha]$.*

Démonstration. — On a, par (1.6), l'égalité :

$$F(z) = \frac{12h(f)}{\alpha^2(h(z) - h(f))}. \tag{4.6}$$

On pose $R_\mathcal{A}(X) = \Pi(Y - \alpha^2 F(\beta))$.

Soit β un point primitif de $\mathcal{A}$-division de $\mathbf{C}/\Omega$.

Par un théorème classique de la multiplication complexe dû à Fueter, on sait que $k(j, h(\beta)) = k(\mathcal{A})$ dès que β est primitif de $\mathcal{A}$-division, ([L 1], chap. 10, Th. 7 et son corollaire). $\alpha^2 F(\beta)$ est donc dans $k(3)k(J)$. D'autre part si u est un idèle unité de k, congru à 1 modulo 3, alors d'après la loi de réciprocité de Shimura on a l'égalité :

$$(\alpha^2 F(\beta))^{(u^{-1},k)} = \alpha^2 F(u\beta)$$

où (u^{-1}, k) désigne l'automorphisme d'Artin.

D'après l'expression de $\alpha^2 F(\beta)$ en fonction de $h(\beta)$, il est clair que si u et u' sont deux idèles unités congrus à ± 1 mod 3,

$$\alpha^2 F(u\beta) = \alpha^2 F(u'\beta) \text{ si et seulement si } h_2(u\beta) = h^2(u'\beta).$$

Or dès que k est distinct de $\mathbb{Q}(i)$ et de $\mathbb{Q}(\zeta_3)$, ce qui est réalisé ici, les seuls isomorphismes de la courbe mise sous la forme de Weierstrass classique sont l'identité et $(P, P') \longmapsto (P, -P')$, et ils laissent $h(u\beta)$ invariant.

L'égalité $h(u\beta) = -h(u'\beta)$ implique que la transformation

$$(P, P') \longmapsto (-P, iP')$$

est un isomorphisme de la courbe, ce qui est contradictoire, d'où

$$h^2(u\beta) = h^2(u'\beta) \text{ équivaut à } h(u\beta) = h(u'\beta).$$

On en déduit que le groupe de Galois de $(k(3)k(\mathcal{A})/k(3))$ opère transitivement et sans point fixe sur ces éléments. Ceci démontre que $R_{\mathcal{A}}(Y)$ est un polynôme minimal de $\alpha^2 F(\beta)$ sur $k(3)$.

Soit φ l'indicateur d'Euler défini sur les idéaux de A_k.

On a l'égalité :

$$S_{\mathcal{A}}(X) = \frac{1}{\alpha^{\varepsilon\varphi(\mathcal{A})}} R_{\mathcal{A}}(\alpha^2 X)$$

où $\varepsilon = 1$ (resp. 2) si $\mathcal{A}$ ne divise pas $2A_k$ (resp. $\mathcal{A}$ divise $2A_k$).

Puisque $k(3) = k[\alpha^3]$, ceci démontre que $S_{\mathcal{A}}(X)$ est dans $k(\alpha)[X]$. Comme les éléments $F(\beta)$ sont des entiers algébriques quand $(\mathcal{A}, 3) = 1$, on en conclut que $S_{\mathcal{A}}(X)$ est dans $A_{k[\alpha]}[X]$.

Remarque. — On a aussi démontré que si $\mathcal{A}$ est un idéal entier de k premier avec 3, alors $k(3)k(\mathcal{A}) = k(3)(\alpha^2 F(\beta))$.

On montre de même :

$$k(\alpha)k(\mathcal{A})(\alpha^2 F(\beta)); k(9)k(\mathcal{A}) = k(9)(\alpha^2 F(\beta))$$
$$\text{et } k(9\mathcal{A}) = k(3)(F(\beta')),$$

où β' est primitif de $9\mathcal{A}$-division dans $\mathbf{C}/\Omega$.

PROPOSITION 4.7. – *Soit ω un élément de A_k tel que $\omega \equiv \pm 1$ mod 3. Alors :*

$$F(\omega z) = c \prod_{\gamma} F(z - \gamma)$$

où γ parcourt l'ensemble des points de ω-division de $\mathbf{C}/\Omega$ et $c^3 = (-1)^{N(\omega)-1}$.

Démonstration. — Les deux membres de l'égalité admettent le même diviseur :

$$\sum_{\gamma} (2(\gamma) - (\gamma + f) - (\gamma + 2f)).$$

Ces deux fonctions sont donc proportionnelles.

Il existe donc $c \neq 0$ tel que :

$$F(\omega z) = c \prod_{\gamma} F(z - \gamma).$$

On en déduit l'égalité :

$$F(\omega z) \cdot F(\omega(z + f)) \cdot F(\omega(z + 2f))$$
$$= c^3 \prod_{\gamma} F(z - \gamma) \cdot F(z + f - \gamma) \cdot F(z + 2f - \gamma)$$

d'où en utilisant (1.9) on obtient l'égalité $c^3 = (-1)^{N(\omega)-1}$.

COROLLAIRE 4.8. – *Soit $\mathcal{A}$ un idéal de A_k premier avec 3. Soient λ et λ' deux points primitifs de $\mathcal{A}$-division de $\mathbf{C}/\Omega$. Alors :*

(i) *$F(\lambda)$ et $F(\lambda')$ sont associés.*

(ii) *Si* $\mathfrak{q}$ *est un diviseur premier de* $\mathcal{A}$, *tel que* $\mathcal{A} = \mathcal{A}'\mathfrak{q}^r$, *alors* $(F(\lambda))$ *divise* $\mathfrak{q}^{2r}$. *En particulier, si* $\mathcal{A}$ *n'est pas égal à la puissance d'un idéal premier de* A_k, $F(\lambda)$ *est une unité.*

Démonstration. — Puisque $F(\lambda)$ et $F(\lambda')$ sont deux entiers algébriques, il suffit de démontrer que $F(\lambda)$ divise $F(\lambda')$, et que $F(\lambda')$ divise $F(\lambda)$. Puisque λ et λ' sont primitifs de $\mathcal{A}$-division, il existe ω premier avec $\mathcal{A}$ tel que $\lambda' \equiv \omega\lambda \bmod \Omega$. Puisque $(\mathcal{A}, 3) = 1$ on peut supposer $\omega \equiv \pm 1 \bmod 3$. Grâce à (4.7) on a :

$$F(\lambda') = F(\lambda) \prod_{\gamma \neq 0} F(\lambda - \gamma)$$

les éléments $F(\lambda - \gamma)$ sont aussi des entiers algébriques, car $\lambda - \gamma$ est d'ordre premier à 3. Donc $F(\lambda)$ divise $F(\lambda')$.

Pour démontrer (ii) il est commode de démontrer le lemme suivant.

LEMME 4.9. – *Soit* ω *un élément de* A_k *vérifiant* $\omega \equiv \pm 1$ *mod* 3. *Alors :*

$$\omega^2 = c \prod_{\gamma \neq 0} F(\gamma)$$

où γ *parcourt l'ensemble des points non nuls de* ω*-division de* $\mathbb{C}/\Omega$.

Démonstration. – Il suffit de faire tendre z vers 0 dans l'égalité

$$\frac{F(\omega z)}{F(z)} = c \prod_{\gamma \neq 0} F(z - \gamma)$$

déduite de (4.7).

Soit $\mathfrak{q}$ un diviseur premier $\mathcal{A}$. On pose $\mathcal{A} = \mathfrak{q}^r\mathcal{A}'$, avec $(\mathcal{A}', \mathfrak{q}^r) = 1$ et on choisit ω dans A_k tel que :

$\omega \equiv 1 \bmod 3\mathfrak{q}^r$

$\omega \equiv 0 \bmod \mathcal{A}'$.

Le point $\omega\lambda$ de $\mathbb{C}/\Omega$ est donc nul de $\mathfrak{q}^r$-division. Par (4.7) on sait que $F(\lambda)$ divise $F(\omega\lambda)$. On choisit des générateurs ω_1 et ω_2 de $\mathfrak{q}^r$, congrus à 1 modulo 3.

On sait que $\omega_1(\omega\lambda) = \omega_2(\omega\lambda) = 0$. Donc $F(\omega\lambda)$ divise ω_1^2 et ω_2^2, puis $\mathfrak{q}^{2r}$.

On conclut que $F(\lambda)$ divise $\mathfrak{q}^{2r}$. Ce qui achève la démonstration du corollaire 4.8.

On pose :

$$Z_{\mathcal{A}}(X) = \prod_{\beta}(X - F(\beta)) \tag{4.10}$$

où β parcourt un demi-système des points de $\mathcal{A}$-division de $\mathbb{C}/\Omega$.

PROPOSITION 4.11. – *Soit $\mathcal{A}$ un idéal entier de k, premier avec (3). Alors le polynôme $Z_{\mathcal{A}}(X)$ est à coefficients dans $A_{k[\alpha]}$ et l'on a l'égalité :*

$$(Z_{\mathcal{A}}(0)) = \mathcal{A}(\mathcal{A}, 2).$$

Démonstration. — Le polynôme $Z_{\mathcal{A}}(X)$ est égal au produit $\Pi S_{\mathfrak{q}}(X)$ où $\mathfrak{q}$ parcourt les diviseurs de $\mathcal{A}$.

On déduit alors de (4.5) que $Z_{\mathcal{A}}(X)$ appartient à $A_{k[\alpha]}$.

Pour déterminer le terme constant, on commence par montrer le lemme suivant.

LEMME 4.12. – *Soit θ un point non nul de 2-division de $\mathbb{C}/\Omega$. Alors :*

(i) *Si 2 est décomposé dans $k/\mathbb{Q}$, avec $2 = \mathfrak{q}\mathfrak{q}'$,*

$(F(\theta)) = \mathfrak{q}^2$ *si θ est de $\mathfrak{q}$-division*

$(F(\theta)) = \mathfrak{q}'^2$ *si θ est de $\mathfrak{q}'$-division*

$F(\theta)$ *est une unité dans les autres cas.*

(ii) *Si 2 est ramifié dans $k/\mathbb{Q}$, avec $2A_k = \mathfrak{q}^2$,*

$(F(\theta)) = \mathfrak{q}^2$ *si θ est de $\mathfrak{q}$-division.*

$(F(\theta)) = \mathfrak{q}$ *sinon.*

(iii) *Si 2 est inerte dans $k/\mathbb{Q}$,*

$(F(\theta)) = (2A_k)^{2/3}$.

Démonstration. — Soient $\{r, s, r+s\}$ l'ensemble des points non nuls de 2-division. D'après 1.1, en utilisant la définition de F, on obtient l'égalité :

$$4 = F(r)F(s)F(r+s). \tag{4.13}$$

Sous les hypothèses de (i) et (iii) on déduit le résultat de (4.8) et (4.13).

On suppose $2 = \mathfrak{q}^2$ ramifié dans $k/\mathbb{Q}$.

Soit, par exemple r le point primitif de $\mathfrak{q}$-division alors, d'après (4.13), $F(r)$ divise $\mathfrak{q}^4$. Puisque s et $r+s$ sont de $\mathfrak{q}^2$-division, il existe ω dans A_k, congru à 1 modulo 3 et tel que $\omega s \equiv r$ et donc d'après (4.7), il existe une racine sixième de l'unité c, telle que :

$$F(r) = c \prod_{\omega\gamma=0} F(s-\gamma).$$

L'idéal (ω) est de la forme $\mathfrak{q}\mathfrak{D}$, avec $(\mathfrak{q}, \mathfrak{D}) = 1$, donc si γ est un point de ω-division, la valuation en $\mathfrak{q}$ de l'annulateur de $s-\gamma$ est donc comprise entre 1 et 2.

Si cet annulateur est $\mathfrak{q}$, alors $s-\gamma = r$, ce qui donne $\gamma = r+s$, mais cela est impossible car $r+s$ est de $\mathfrak{q}^2$-division.

L'annulateur de $s-\gamma$ est donc :

soit $\mathfrak{q}^2$ c'est-à-dire $s-\gamma = s$ ou $r+s$, puis $\gamma = 0$ ou r,

soit $\mathfrak{q}\mathfrak{D}'$ où $\mathfrak{D}'$ est un idéal entier distinct de A_k et divisant $\mathfrak{D}$, et $F(s-\gamma)$ est une unité. On en déduit que $F(r)$ est associé à $F(s)F(r+s)$. Comme d'autre part on sait que $F(s)$ et $F(r+s)$ sont associés l'égalité (4.13) ne laisse alors plus le choix, d'où (ii), ce qui achève la démonstration du lemme.

On déduit du lemme que la proposition est vraie dès que $\mathcal{A}$ divise 2. Supposons pour commencer que $\mathcal{A}$ est principal engendré par $\omega \equiv \pm 1 \bmod 3$. On pose $(\mathcal{A}, 2) = \mathcal{A}'$. D'après (4.9) on a :

$$(\mathcal{A}\mathcal{A}'^{-1})^2\mathcal{A}'^2 = \Big(\prod_{\beta} F(\beta)\Big)^2 (Z_{\mathcal{A}'}(0))$$

où β parcourt un demi-système de représentants des points de $\mathcal{A}$-division non annulés par 2.

Puisque la proposition est vraie pour $\mathcal{A}'$, on en déduit :

$$\left(\prod_{\beta} F(\beta)\right) = \mathcal{A}\mathcal{A}'^{-1}$$

et donc :

$$(Z_{\mathcal{A}}(0)) = \mathcal{A}\mathcal{A}'. \tag{4.14}$$

La proposition est donc démontrée dans ce cas.

On traite maintenant le cas général :

D'après le lemme d'approximation il existe λ dans A_k, congru à 1 modulo 3, tel que $\mathfrak{q} = \lambda\mathcal{A}^{-1}$ soit un idéal entier de A_k premier avec $\mathcal{A}$. Il est clair que $Z_{\mathcal{A}}(X)$ divise $Z_{(\lambda)}(X)$. Soit $G(X)$ le quotient de ces deux polynômes, $G(X)$ appartient donc à $A_{k[\alpha]}[X]$ et, puisque $\lambda \equiv 1 \bmod 3$, on déduit de (4.14) :

$$(\lambda)((\lambda), 2) = (Z_{(\lambda)}(0)) = (Z_{\mathcal{A}}(0))(G(0)). \tag{4.15}$$

Puisque $(\mathfrak{q}, \mathcal{A}) = 1$ on a :

$$(\lambda)((\lambda), 2) = \mathcal{A}(\mathcal{A}, 2)\mathfrak{q}(\mathfrak{q}, 2). \tag{4.16}$$

Soit alors $F(\sigma)$ une racine de $Z_{\mathcal{A}}(X)$ (resp. $G(X)$) ; l'annulateur de σ est soit un idéal premier avec $\mathfrak{q}$ (resp. premier avec $\mathcal{A}$), soit divisible par au moins deux idéaux premiers distincts. On déduit de (4.8) que $(Z_{\mathcal{A}}(0))$ (resp. $G(0)$) est premier avec $\mathfrak{q}$ (resp. $\mathcal{A}$).

De (4.16) on déduit :

$$(Z_{\mathcal{A}}(0)) = \mathcal{A}(\mathcal{A}, 2).$$

Ce qui achève la démonstration de la proposition 4.11.

COROLLAIRE 4.17. – *Soient $\mathfrak{q}$ un idéal premier de k, ne divisant pas 3 et λ un point primitif de $\mathfrak{q}^n$-division, où n est un entier non nul. Dans la clôture algébrique de k choisie, on a l'égalité suivante, entre idéaux :*

$$(f(\lambda))^{\varphi(\mathfrak{q}^n)} = \mathfrak{q}^2.$$

Démonstration. — On remarque que :

$$Z_{q^n}(X) = S_{q^n}(X)\, Z_{q^{n-1}}(X). \tag{4.18}$$

Si q^{n+1} ne divise pas 2, l'égalité (4.18) et la proposition (4.11), donnent :

$$(S_{q^{n+1}}(0)) = q,$$

puis le corollaire 4.8 donne le résultat car deg $S_{q^n}(X) = \varphi(q^n)/2$.

Si q^n divise 2, (4.18) et (4.11), donnent :

$$(S_{q^n}(0)) = q^2,$$

et le corollaire (4.8) donne le résultat car deg $S_{q^n}(X) = \varphi(q^n)$.

COROLLAIRE 4.19.

(i) *Si* $n\lambda = \pm f$, *avec* $n \neq \pm 1$, *alors* $F(\lambda)$ *est l'inverse d'un entier.*

(ii) *Si* λ *est un point non nul de torsion, dont l'annulateur est premier avec* 3 *et si* μ *désigne un point de torsion, distinct de* $\pm f$, *d'ordre une puissance de* 3, *alors* $F(\lambda + \mu)$ *est une unité.*

Démonstration. — (i) provient du fait que $x(\lambda)$ est racine de $N_n(X)$ qui est un polynôme unitaire à coefficients entiers.

Posons $\beta = \lambda + \mu$. Soit n l'ordre de λ, $n\beta$ est donc un point d'ordre une puissance de 3, et $x(n\beta)$ est une 3-unité.

D'autre part $N_n(x(\beta)) - x(n\beta)D_n(x(\beta)) = 0$. Or $N_n(X) - x(n\beta)D_n(X)$ est un polynôme unitaire, dont les coefficients sont des 3-entiers et dont le terme constant $x(n\beta)D_n(0)$ est non nul et associé à $x(n\beta)$. Donc $x(\beta)$ est une 3-unité.

Soit m l'ordre de μ, $m\beta$ est un point d'ordre premier à 3, donc $x(m\beta)$ est une unité pour les places divisant 3.

D'autre part $N_m(x(\beta)) - x(m\beta)D_m(x(\beta)) = 0$, et $N_m(X) - x(m\beta)D_m(X)$ est un polynôme unitaire, dont les coefficients sont des entiers aux places divisant 3, et dont le terme constant $N_m(0)$ vaut ± 1. Donc $x(\beta)$ est une unité pour les places divisant 3. $x(\beta)$ est alors une unité, ainsi que $F(\beta)$. Ce qui démontre (ii).

Remarque 4.20. – Conservons les notations de (4.19). Dès que $x(\beta)$ est entier, $x_1(\beta)$ l'est aussi. De plus on a :

$$x_1(\beta)x_1(\beta+r)x_1(\beta+s)x_1(\beta+r+s) = \alpha^3 - 27.$$

De même $x_1(\beta+r)$, $x_1(\beta+s)$ et $x_1(\beta+r+s)$ sont des entiers algébriques dès que λ n'est pas d'ordre 2, et ils sont alors des unités en dehors des places divisant $\alpha^3 - 27$.

Si λ est d'ordre 2, par exemple $\lambda = r$, alors $x_1(\beta)$, $x_1(\beta+s)$ et $x_1(\beta+r+s)$ sont des entiers, et $x_1(\beta+r) = x_1(\mu)$ est un 3-entier, on en conclut que $x_1(\beta)$ est un entier et une 3-unité.

V. Etude de la structure algébrique des anneaux d'entiers.

L'étude des propriétés arithmétiques des $F(\lambda)$ où λ est un point de torsion, va nous permettre d'établir des résultats de monogénéités des anneaux d'entiers de certains corps de rayon du corps de base.

HYPOTHESES :

(i) Le corps k est une extension quadratique imaginaire de $\mathbb{Q}$. Dans ce cas, si $A_k = \tau\mathbb{Z} + \mathbb{Z}$, la courbe elliptique correspondante est à multiplication complexe par l'anneau A_k.

(ii) On suppose que 3 se décompose dans k : $3 = \mathfrak{p}\mathfrak{p}'$.

(iii) On choisit φ primitif de 9-division, $f = 3\varphi$, il existe (u, v) élément de $((1/3\mathbb{Z}/\mathbb{Z})^2$ tel que $f = u\tau + v$. On pose alors $\alpha = l_{(u,v)}(\tau)$.

NOTATIONS :

Si $\mathcal{A}$ est un idéal entier de $k, U_{\mathcal{A}}$ désigne le groupe des idèles unités de k, $a = (a_v)$, telles que $v(a_v - 1) \geq v(\mathcal{A})$ pour toute place v divisant $\mathcal{A}$.

On note $\sim$ la relation d'équivalence sur les éléments non nuls de la clôture algébrique de k définie par : $a \sim b$ si et seulement si a/b est une unité.

Sous ces hypothèses, d'après (4.2) le modèle de Deuring est défini sur $H(\alpha) = E$, et admet une bonne réduction partout ($\alpha^3 - 27$ est une unité).

Remarque. — On obtient en utilisant (4.2), (1.7) (i) et (1.8), que j est une unité pour les places divisant 3, cas particulier d'un résultat plus général, qui dit que j est une unité pour toutes les places décomposées de $k/\mathbb{Q}$ (cf. $[G, Z]$).

Démonstration du théorème 1. — On sait déjà d'après (4.4) et (4.19), que $F(\beta)$ est une unité de L, donc A_L contient $A_K[F(\beta)]$. Pour démontrer l'égalité, il suffit de montrer que leur discriminant sur A_K sont égaux.

1) Calcul du discriminant d_1 de A_L sur A_K.

On utilise la théorie du corps de classes, et la formule de Hasse pour le discriminant.

Les seuls idéaux premiers de K qui divisent d_1 divisent $\mathcal{A}$. De plus d_1 est ambige relativement à l'extension K/k, donc on peut le considérer comme un idéal de k. Si d_1' désigne le discriminant de L/k, on a $v_{\mathfrak{q}}(d_1) = v_p(d_1')/[K : k]$ pour tout idéal premier $\mathfrak{q}$ de K au-dessus d'un idéal p de k, non ramifié dans K/k. Soit donc p un idéal premier de k divisant $\mathcal{A}$, et r la valuation de $\mathcal{A}$ en p : $r = v_p(\mathcal{A})$. On peut écrire : $\mathcal{A} = lp^r$ avec $(p, l) = 1$.

Notons q la norme de p sur $\mathbb{Q}$.

Pour $1 \leq s \leq 0$, il y a exactement $[k(9lp^s) : k] - [k(9lp^{s-1}) : k]$ caractères du Gal (L/k) dont le conducteur est de valuation s en p. On a :

si $s > 1$, $[k(9lp^s) : k] - [k(9lp^{s-1}) : k]$
$$= [k(9l) : k](q^{s-1}(q-1) - q^{s-2}(q-1)),$$

si $s = 1$, $[k(9lp) : k] - [k(9l) : k] = [k(9l) : k](q-2)$.

Le discriminant de L/k admet donc pour valuation en p :

$$[k(9l):k]\Big(q-2+\sum_{s-2}^{r} s[q^{s-1}(q-1)-q^{s-2}(q-1)]$$
$$=[k(9l):k](rq^r-(r+1)q^{r-1}\Big)$$

mais p est non ramifié dans K/k, donc :

$$v_{\mathfrak{q}}(d_1)=[k(9l):K](rq^r-(r+1)q^{r-1})$$

pour tout idéal $\mathfrak{q}$ de K au-dessus de p.

2) Calcul du discriminant d_2 :

On utilise la formule d'Euler :

$$d_2=N_{L/K}\Big(\prod_{\sigma\neq id}(F(\beta)-F(\beta)^{\sigma})\Big). \tag{5.1}$$

Commençons par démontrer le lemme :

LEMME 5.2. – *Soit* a *un élément non trivial de* $U_9/U_{9\mathcal{A}}$, *alors :*

$$(F(\beta)-F(a\beta))^2\sim F((a-1)\beta).$$

Démonstration. — A l'aide de la formule de la différence pour la fonction P de Weierstrass ([L 2], Chap. II, § 1), on obtient celle correspondante à la fonction x, puis pour la fonction F l'égalité :

$$\begin{aligned}(F(u)-F(v))^2(F(u+v)-F(u-v))\\ =F(u+v)F(u-v)F(u)^2F(v)^2x_1(u)x_1(v).\end{aligned} \tag{5.3}$$

Remarquons alors que $F(\beta), F(a\beta)$ sont des unités (prop. 4.19).

- Soit λ est distinct de r, s, et $r+s$, alors $x_1(\beta)$, $x_1(a\beta)$ sont aussi des unités (cf. (4.20)).
- Soit λ appartient à $\{r,\ s,\ r+s\}$, par exemple $\lambda=r$, alors $F(\beta+r)=F(\varphi)$ est une unité car $F(\varphi)F(\varphi+f)F(\varphi+2f)=-1$, et les éléments $F(\varphi)$, $F(\varphi+f)$, $F(\varphi+2f)$ sont des inverses d'entiers (prop. (4.19)).

$F(\beta+s)$ et $F(\beta+r+s)$ étant aussi des unités, on en déduit encore que $x_1(\beta)$ est une unité, de même pour $x_1(a\beta)$. En remplaçant u par β et v par $a\beta$ dans (5.3), on obtient :

(5.4) $(F(\beta)-F(a\beta))^2(F((a+1)\beta)-F((a-1)\beta)) \sim F((a+1)\beta)F((a-1)\beta)$.

1^{er} cas $a \equiv -1 \bmod \mathcal{A}$.

Alors on a les égalités $(a+1)\beta = 2\varphi$ et $(a-1)\beta = 2\lambda$.

$F(2\varphi)$ est une unité (mêmes raisons que pour $F(\varphi)$), et $F(2\lambda)$ est un entier si λ n'appartient pas à $\{r,\ s,\ r+s\}$. $F(2\varphi)-F(2\lambda)$ est un entier, premier avec $F(2\lambda)$, qui divise $F(2\lambda)$, c'est donc une unité.

Si λ appartient $\{r,\ s,\ r+s\}$, alors $a\beta = \beta$, et $\mathcal{A}$ divise (2), donc a est trivial dans $U_9/U_{9\mathcal{A}}$.

2^e cas $a \neq -1 \bmod \mathcal{A}$.

Alors on a l'égalité : $(a+1)\beta = \omega + 2\varphi$, où ω est non nul et admet un annulateur premier avec 3. On sait que $F((a+1)\beta) \sim 1$ et que $F((a-1)\beta)$ est un entier algébrique et une unité en dehors de $\mathcal{A}$. On déduit alors de (5.3) que $F((a+1)\beta)-F((a-1)\beta)$ est un entier algébrique premier avec $F((a-1)\beta)$.

Conclusion $F((a+1)\beta)-F((a-1)\beta)$ est une unité, ce qui achève la démonstration du lemme.

Le groupe de Galois de $k(9\mathcal{A})/k(9)$ est isomorphe à $U_9/U_{9\mathcal{A}}$; de la formule d'Euler, et de la loi de réciprocité de Shimura, on déduit :

$$d_2 = N_{L/K}\Big(\prod_a (F(\beta)-F(a\beta))\Big)$$

où le produit porte sur un système de représentants des classes non triviales de $U_9/U_{9\mathcal{A}}$.

Le lemme (5.2) permet d'écrire :

$$d_2^2 = N_{L/K}\Big(\prod_a F((a-1)\beta)\Big)A_k = N_{L/K}\Big(\prod_a F((a-1)\lambda)\Big)A_K.$$

Il reste à calculer la valuation de d_2^2 en une place $\mathfrak{q}$.

D'après (4.8), cette valuation est nulle sauf peut-être pour les places de K divisant $\mathcal{A}$.

Soit donc p une place de k, divisant $\mathcal{A}$, $\mathfrak{q}$ au-dessus de p dans K, et r la valuation de $\mathcal{A}$ en p, $\mathcal{A} = p^r l$.

Si $S_a = N_{L/K}(F((a-1)\lambda))$, on a d'après (4.17) :

$v_{\mathfrak{q}}(S_a) = 0$ si $(a-1)\lambda$ n'est pas p-primaire,

$v_{\mathfrak{q}}(S_a) = 2\,[k(9\mathcal{A}) : K]/\varphi(p^s) = 2k[(9l) : K]q^{r-s}$
si $(a-1)\lambda$ est primitif d'ordre p^s.

D'autre part $(a-1)\beta$ est primitif d'ordre p^s si et seulement si a appartient à $(U_{9lp^{r-s}}/U_{9lp^r}) - U_{9lp^{r-s+1}}/U_{9lp^r}$. Cet ensemble a pour cardinal :

$$q^{s-1}(q-1) \text{ si } r > s \geq 1, \text{ et } q^{r-1}(q-2) \text{ si } s = r.$$

D'où

$$v_{\mathfrak{q}}(d_2^2) = 2[k(9l) : K]\Big(q^{r-1}(q-2) + \sum_{s=1}^{r-1} q^{r-s}(q^s - q^{s-1})\Big)$$

soit :

$$v_a(d_2^2) = 2[k(9l) : K](rq^r - (r+1)q^{r-1}).$$

On obtient donc l'égalité des deux discriminants. C.Q.F.D.

La démonstration de (ii) est un peu plus technique :

Soit $x_{\mathcal{A}}$ l'idèle défini par : $(x_{\mathcal{A}})_v = -1$ si v divise $\mathcal{A}$, $(x_{\mathcal{A}})_v = 1$ sinon, et X l'extension abélienne de k correspondante au sous-groupe $k^* < x_{\mathcal{A}} > U_{9\mathcal{A}}$ du groupe des idèles de k.

X est donc contenue dans $K(9\mathcal{A})$, et contient $k(9) = K$, $k(\mathcal{A})$, et donc $Kk(\mathcal{A})$.

De plus $x_{\mathcal{A}}$ est d'ordre 2 dans $U_9/U_{9\mathcal{A}}$, d'où :

$$[K(9\mathcal{A}) : X] = 2 = [K(9\mathcal{A}) : Kk(\mathcal{A})].$$

On en déduit que $X = Kk(\mathcal{A})$.

LEMME 5.5. – *Soit* $\mathfrak{q}$ *un idéal premier de* k *ne divisant pas* 3, n *un entier tel que* $\mathfrak{q}^n$ *ne divise pas* 2, *et* λ *un point primitif de* $\mathfrak{q}^n$*-division dans* $\mathbb{C}/\Omega$. *Si* a *est un élément non trivial de* $U_9/ < x_{\mathfrak{q}^n} > U_{9\mathfrak{q}^n}$, *alors* $(F(\lambda) - F(a\lambda)$ *est une unité en dehors des places divisant* $\mathfrak{q}$.

Démonstration. — En effet d'après la formule de la différence (5.3), en posant $u = \lambda$ et $v = a\lambda$, on obtient :

$$[F(\lambda) - F(a\lambda)]^2[F((a+1)\lambda) - F((a-1)\lambda)]$$
$$= F((a+1)\lambda)F((a-1)\lambda)F(\lambda)^2F(a\lambda)^2x_1(\lambda)x_1(a\lambda).$$

On sait déjà que $F((a+1)\lambda)$, $F((a-1)\lambda)$, $F(\lambda)$ et $F(a\lambda)$ sont des entiers algébriques divisant une puissance de P.

Considérons alors les égalités :

$$x_1(\lambda)x_1(\lambda+r)x_1(\lambda+r+s)x_1(\lambda+r+s) = \alpha^3 - 27$$

$$F^3(\lambda)x_1^2(\lambda) = 4 + \alpha^2F(\lambda) + 2\alpha F^2(\lambda) + F^3(\lambda)$$

déduite de (1.9) (ii) de (1.1) et de la définition de F.

Or d'après l'hypothèse sur n et λ, $\lambda + r$, $\lambda + s$ et $\lambda + r + s$ ont leur annulateur divisible par deux idéaux premiers distincts, les quantités $x_1(\lambda + r)$, $x_1(\lambda + s)$ et $x_1(\lambda + r + s)$ sont des entiers (cf. 4.20). $x_1(\lambda)$ est alors l'inverse d'un entier divisant $F^3(\lambda)$; c'est une unité en dehors de P. Il en est de même pour $x_1(a\lambda)$. Le lemme est donc démontré.

Si $\mathfrak{q}$ est un idéal premier de k, ne divisant pas 3, alors d'après le corollaire (4.17), $S_{\mathfrak{q}^n}(X)$ est un polynôme d'Eisenstein en toute place de K divisant $\mathfrak{q}$, dès que $\mathfrak{q}^n$ ne divise pas 2.

Sous cette hypothèse sur n, (ii) est vérifié localement pour toute place de K divisant $\mathfrak{q}$. Mais comme les discriminants intervenants sont des unités en dehors de ces places, le résultat est vrai globalement.

Supposons maintenant $\mathcal{A}$ divisible par au moins deux idéaux premiers distincts. On démontre alors le lemme suivant :

LEMME 5.6. — *Soit $\mathcal{A}$ un idéal premier avec 3, vérifiant :*

- $\mathcal{A}$ est divisible par deux idéaux premiers distincts,

- $v(\mathcal{A}) > v(2)$ pour toutes les places divisant 2.

Si λ est primitif de $\mathcal{A}$-division, et si a est un élément non trivial de $U_9/ < x_{\mathcal{A}} > U_{9a}$, alors on a :

$$(F(\lambda) - F(a\lambda))^2 \sim F((a+1)\lambda)F((a-1)\lambda).$$

Démonstration. — Un raisonnement analogue à celui fait dans la démonstration du lemme (5.2), permet d'établir

$$(F(\lambda)-F(a\lambda))^2(F((a+1)\lambda)-F((a-1)\lambda)) \sim F((a+1)\lambda)F((a-1)\lambda).$$

D'autre part si un idéal premier $\mathfrak{q}$ de M divise la quantité $F((a+1)\lambda) - F((a-1)\lambda)$ il divise $F((a+1)\lambda)$ et $F((a-1)\lambda)$, soit alors p une place de k au-dessous de $\mathfrak{q}, (a-1)\lambda$ et $(a+1)\lambda$ ont alors pour annulateurs respectifs des puissances de p. Mais alors l'annulateur de 2λ est une puissance de p, ce qui contredit l'une des deux hypothèses faites sur $\mathcal{A}$. D'où le résultat.

La fin de la démonstration du théorème 1 (ii) est alors analogue à celle de (i) :

Soit p un idéal premier de k, divisant $\mathcal{A}, \mathcal{A} = lp^r$ avec $(l,p) = 1$, alors si $(a-1)\lambda$ est primitif de p^s-division, $(ax_{\mathcal{A}} + 1)\lambda$ est aussi primitif de p^s-division.

Comme a et $ax_{\mathcal{A}}$ sont dans la même classe, il suffit donc de s'intéresser à la contribution des $F((a-1)\lambda)$, quitte à multiplier par 2 la valuation obtenue.

Comme l'intersection de $U_{9lp^{r-s}}$ et de $< x_{\mathcal{A}} > U_{9lp^{r-s+1}}$ est $U_{9lp^{r-s+1}}$, il y a donc exactement

$$[U_{9lp^{r-s}} : U_{9lp^r}] - [U_{9lp^{r-s+1}} : U_{9lp^r}]$$

classes d'idèles a distinctes tels que $(a-1)\lambda$ soit primitif de p^s-division, soit :

$$(q^s - q^{s-1}) \text{ si } r > s \geq 1, \text{ et } (q^r - 2q^{r-1}) \text{ si } s = r.$$

La valuation du discriminant $A_K[F(\lambda)]$ sur A_K en une place $\mathfrak{q}$ de K au-dessus de p est donc le double de celle obtenue à l'aide des $F((a-1)\lambda)$:

$$v_{\mathfrak{q}}(d_2'^2) = 2[Kk(l) : K](q^{r-1}(q-2) + \sum_{s=1}^{r-1} q^{r-s}(q^s - s^{s-1}))$$

donc

$$v_{\mathfrak{q}}(d_2') = [Kk(l) : K](rq^r - (r+1)q^{r-1}).$$

D'autre part l'extension K/k n'est pas ramifiée au-dessus de $\mathcal{A}$, la valuation du discriminant de $Kk(\mathcal{A})$ sur K en une place divisant $\mathcal{A}$, est donc la même que celle du discriminant de $k(\mathcal{A})$ sur k. On peut donc utiliser la première partie de la démonstration pour calculer cette valuation; on constate alors que cette valuation est bien celle de d_2'.

COROLLAIRE 5.7. — *Soit $\mathcal{A}$ un idéal entier de k, premier avec 3. On note $K = k(9)$ et $M = Kk(\mathcal{A})$. Alors :*

A_M est monogène sur A_K dès que $\mathcal{A}$ n'est pas de la forme $2\mathcal{A}'$, où $\mathcal{A}'$ est premier avec 6.

Démonstration. — Supposons 2 inerte dans $k/\mathbb{Q}$, alors la condition sur $\mathcal{A}$ dans le théorème 1, est équivalente à celle de (5.7).

Supposons 2 ramifié dans $k/\mathbb{Q}$, $(2) = \mathfrak{q}^2$ alors si $\mathcal{A} = \mathfrak{q}\mathcal{A}'$, avec $(\mathcal{A}', 6) = 1$, $k(\mathcal{A}) = k(\mathcal{A}')$ et le théorème 1 permet de conclure.

Supposons enfin 2 décomposé dans $k/\mathbb{Q}$, $(2) = \mathfrak{q}\mathfrak{q}'$.

Si $\mathcal{A} = \mathfrak{q}\mathcal{A}'$ avec $(\mathcal{A}', \mathfrak{q}) = 1$, ou $\mathcal{A} = \mathfrak{q}'\mathcal{A}'$ avec $(\mathcal{A}', \mathfrak{q}') = 1$, alors $k(\mathcal{A}) = k(\mathcal{A}')$ et le théorème 1 permet de conclure. On remarque que dans ce cas les résultats de [C-N, T 2] sont plus forts lorsque $\mathcal{A}'$ est impair, puisque dans ce cas il y a monogénéité sur l'anneau des entiers de H.

En fait puisque l'on sait que $k(\alpha) = E$, et $k(\alpha^3) = H(\zeta_3)$, il est possible de raffiner les résultats :

DEMONSTRATION DU THEOREME 2 :

LEMME 5.8.

(i) *Le discriminant de l'extension E de $K' = k(3)$ est 27.*

(ii) *L'extension K/E est non ramifiée.*

Démonstration. — On calcule d'abord le discriminant de A_E sur A_k en utilisant la formule de Hasse :

Si χ est un caractère de Gal (E/k) vérifiant $\chi(1 + \mathfrak{p}) = 1$, alors $\chi(u) = 1$, où u est l'idèle défini précédemment, donc $\chi(1 + \mathfrak{p}') = 1$.

Le nombre de caractères de Gal (E/k) de $\mathfrak{p}$ composante de conducteur $\mathfrak{p}^2$ est égal à :

$$[N/k] - [k(3) : k] = 4[H : k].$$

Le nombre de caractères de Gal (E/k) de $\mathfrak{p}$ composante de conducteur $\mathfrak{p}$ est égal à :

$$[k(3) : k] - [k(\mathfrak{p}') : k] = [H : k].$$

On en conclut que la valuation en $\mathfrak{p}$ du discriminant de E sur k est $9[H : k]$.

On obtient donc que le discriminant $\Delta(E/k)$ de E' sur k est $3^{9[H:k]}$.

De même le discriminant $\Delta(K'/k)$ de K' sur k est $3[H : k]$.

On en déduit que celui de E sur K' est 27, par utilisation de la formule de composition des discriminants ([Se], III, § 4, prop. 8) :

$$\Delta(E/k) = N_{K'/k}(\Delta(E/K'))\Delta(K'/k)^{[E:K']}.$$

Soit $\Delta(E/K') = 27$.

De même le discriminant de $k(9) = K$, sur k est $3^{27[H:k]}$. L'extension K/E est donc de discriminant 1, elle est non ramifiée, ce qui démontre le lemme.

L'extension K/E est de degré 3, non ramifiée et de groupe de Galois :

$$< u > U_9/U_9 \ ,$$

où u est l'idèle défini précédemment, cf. (4.2).

Or $ua\beta = a\lambda+4\varphi$, $(ua-1)\beta = (a-1)\lambda+3\varphi$, $(ua+1)\beta = (a+1)\lambda+5\varphi$.

En utilisant la proposition (4.19) on obtient :

$F(\beta)$, $F(ua\beta)$, $x_1(\beta)$ et $x_1(ua\beta)$ sont des unités

$F((ua+1)\beta)$ est une unité,

$F((ua-1)\beta)$ est l'inverse d'un entier,

donc $[F((ua-1)\beta)-F((ua+1)\beta)]/F((ua-1)\beta)$ est un entier, et même une unité ainsi que $[F(\beta)-F(ua\beta)]^2$. On a donc :

$$N_{L/2}\Big(\prod_{i=0}^{2}\prod_{a}(F(\beta)-F(au^i\beta)\Big)A_E$$
$$= N_{K/E}\Big(N_{L/K}\Big(\prod_{a}(F(\beta)-F(a\beta)\Big)\Big)A_E.$$

D'après le théorème 1 et la formule de transitivité des discriminants, le second membre de l'égalité ci-dessus est le discriminant de l'extension L/E ce qui démontre (i').

Puisque les extensions K/E et $Ek(\mathcal{A})/E$ sont arithmétiquement disjointes, et que $F(\lambda)$ appartient en fait à $Ek(\mathcal{A})$, il est clair que : $A_{Ek(\mathcal{A})} = A_E[F(\lambda)]$ ce qui démontre (ii').

LEMME 5.9. – *Soit* $K' = k(3)$.

(i) $K'(\alpha) = K'((\alpha^3-27)^{1/3})$,

(ii) *il existe une racine cubique* δ *de* $(\alpha^3-27)^2$, *telle que* $\delta\alpha^{-2}$ *appartienne à* K'.

Démonstration. — On sait ([7], Chap. 18, § 5) et (Chap. 10, corollaire du théorème 2) que $j^{1/3}$ est une forme modulaire rationnelle sur $\mathbf{Q}$, de niveau 3, donc que $j(\tau)^{1/3}$ est élément de $k(3) = K'$. L'égalité de la remarque (1.8) et la proposition (4.1), permet alors d'affirmer que $\alpha^3/(\alpha^3-27)$ est un cube dans $k(3)$. (i) se déduit alors de la théorie de Kummer, et (ii) est immédiat.

Pour démontrer (ii'') on remarque que $E = K'(\alpha) = K'(\delta)$.

D'après (4.6) et (5.8), $\delta F(\lambda)$ est dans $K'k(\mathcal{A})$.

Puisque δ est une unité de E, on déduit de (ii')

$$A_{M''} = A_{Ek(\mathcal{A})} = A_E[\delta F(\lambda)].$$

D'autre part on a le lemme suivant :

LEMME 5.10. – $A_E = A_{K'}[\delta]$.

Démonstration. — En effet puisque δ est une unité de E, A_E contient $A_{K'}[\delta]$, et le discriminant de $A_{K'}[\delta]$ sur $A_{K'}$, que l'on calcule

en utilisant la formule d'Euler, est 27. Le résultat se déduit alors du lemme 5.8.

On déduit du lemme et de l'égalité $A_{Ek(\mathcal{A})} = A_E[\delta F(\lambda)]$, l'égalité :

$$A_{Ek(\mathcal{A})} = A_E[\delta F(\lambda)] = A_{K'[\partial]}[\delta F(\lambda)].$$

On obtient alors l'égalité $A_{K'k(\mathcal{A})} = A_{K'}[\delta F(\lambda)]$ en utilisant le fait que le groupe de Galois de l'extension $Ek(\mathcal{A})/K'k(\mathcal{A})$ est isomorphe par restriction à celui de l'extension E/K'.

Ce qui achève la démonstration de (ii'').

VI. Exemples.

Le but de ce paragraphe est de calculer les valeurs de α correspondantes aux courbes $\mathbf{C}/A_k$ lorsque k est quadratique imaginaire, d'anneau des entiers A_k principal, dans lequel 3 est totalement décomposé.

On sait que $\mathbf{Q}(\sqrt{-2})$ et $\mathbf{Q}(\sqrt{-11})$ sont les seuls corps vérifiant ces hypothèses, mais nous retrouverons en fait ce résultat, ainsi que les invariants modulaires correspondants au cours du calcul.

Si A_k est principal, alors $H = k$, et d'après la proposition (4.1) le polynôme

$$X^4 + 36X^3 + 270X^2 + (756 - j)X + 3^6$$

est produit d'un polynôme irréductible de degré 2, dont les racines sont des unités, et d'un autre polynôme, de degré 2, dont les racines sont dans k.

Soit f un point primitif de 3-division, alors $\alpha^3(f) - 27$ est une unité, donc sa norme sur k est une unité ε de k, soit ± 1 (car 3 ne se décompose pas dans $\mathbf{Q}(i)$ et $\mathbf{Q}(\rho)$ avec $\rho^3 = 1$).

On peut donc écrire l'égalité suivante :

$$X^4+36X^3+270X^2+(756-j)X+3^6 = (X^2-aX+\varepsilon)(X^2-bX+\varepsilon^{-1}3^6)$$

où a et b sont dans k.

On obtient alors le système :

$$(6.2)\qquad \begin{cases} a+b=-36 \\ \varepsilon+\varepsilon^{-1}3^6+ab=270 \\ -a\varepsilon^{-1}3^6-b\varepsilon=756-j. \end{cases}$$

Supposons d'abord que $\varepsilon=-1$, alors le système (6.2) devient :

$$(6.3)\qquad \begin{cases} a+b=-36 \\ ab=1000 \\ 729a+b=756-j \end{cases}$$

et a et b sont les racines du polynôme $X^2+36X+1000$, soit :

$\{a,b\}=\{-18+26i,\ -18-26i\}$, ce qui conduit à $k=\mathbb{Q}(i)$. Or ceci est impossible.

Donc $\varepsilon=+1$, et le système (6.2) devient :

$$(6.4)\qquad \begin{cases} a+b=-36 \\ ab=-460 \\ -729a-b=756-j \end{cases}$$

et a et b sont les racines du polynôme $X^2-36X-460$, soit :

$\{a,b\}=\{10,\ -46\}$.

1) $a=10$ et $b=-46$, alors $j=8000$.

Alors $\alpha^3(f)-27$ est racine de $X^2-10X+1$.

$\alpha^3(f)-27=5\pm\sqrt{6}$ puis $\alpha^3(f)=32\pm2\sqrt{6}$.

$\alpha(f)$ est une racine cubique de $32\pm2\sqrt{6}$.

Or d'après la proposition 4.1, $k(3)=k(\alpha^3(f))$, donc ici $k(3)$ est une extension de degré 4 sur $\mathbb{Q}$, contenant $\mathbb{Q}(\zeta_3)=\mathbb{Q}(\sqrt{-3})$, et $\mathbb{Q}(\sqrt{6})$. Donc $k(3)=\mathbb{Q}(\sqrt{-3},\ \sqrt{-2})$.

Le sous-corps k est donc le sous-corps quadratique imaginaire de $\mathbb{Q}(\sqrt{-3},\ \sqrt{-2})$, distinct de $\mathbb{Q}(\sqrt{-3})$, soit $k=\mathbb{Q}(\sqrt{-2})$. L'anneau des entiers de $\mathbb{Q}(\sqrt{-2})$ est $\mathbb{Z}[\sqrt{-2}]$, et l'invariant modulaire associé est donc $j=8000$.

Dans k on a la décomposition suivante :

$$3 = (1 - \sqrt{-2})(1 + \sqrt{-2}).$$

Soit f un point primitif de $(1 \pm \sqrt{-2})$-division, alors $\alpha^3(f) - 27$ est la racine de l'équation : $X^2 + 46X + 729 = 0$, associée à $(1 \pm \sqrt{-2})^6$.

Or ces racines sont $-23 \pm 10\sqrt{-2}$, ce qui donne pour α^3 les valeurs suivantes : $2(2 \pm 5\sqrt{-2})$ ces deux valeurs sont bien des cubes dans k :

$$(-2 + \sqrt{-2})^3 = 2(2 - 5\sqrt{-2}) \text{ et } (-2 - \sqrt{-2})^3 = 2(2 + 5\sqrt{-2}),$$

d'où les valeurs de α :

si f est primitif de $(1 - \sqrt{-2})$-division $\alpha(f) = -2 + \sqrt{-2}$,

si f est primitif de $(1 + \sqrt{-2})$-division $\alpha(f) = -2 - \sqrt{-2}$.

2) $a = -46$ et $b = 10$, alors $j = -32768 = -2^{15}$.

Alors $\alpha^3(f) - 27$ est racine de $X^2 + 46X + 1$.

$\alpha^3(f) - 27 = -23 \pm 4\sqrt{33}$ puis $\alpha^3(f) = 4 \pm 4\sqrt{33}$.

Un raisonnement analogue à celui du 1) donne :

$$k(3) = \mathbb{Q}(\sqrt{-3}, \sqrt{33}).$$

Le sous-corps k est donc le sous-corps quadratique imaginaire de $\mathbb{Q}(\sqrt{-3}, \sqrt{33})$ distinct de $\mathbb{Q}(\sqrt{-3})$, soit $k = \mathbb{Q}(\sqrt{-11})$.

L'invariant modulaire associé à l'anneau des entiers de k, $\mathbb{Z}[(1 + \sqrt{-11})/2]$ est donc $j = -2^{15}$.

Soit f un point primitif de $(1 \pm \sqrt{-11})/2$-division, alors $\alpha^3(f) - 27$ est la racine de l'équation : $X^2 - 10X + 729 = 0$, associée à $((1 \pm \sqrt{-11})/2)^6$.

Soit $\alpha^3(f) - 27 = 5 \pm 8\sqrt{-11}$, puis $\alpha^3(f) = 8(4 \pm \sqrt{-11})$.

Or $(-1 - \sqrt{-11})^3 = 8(4 + \sqrt{-11})$ et $(-1 + \sqrt{-11})^3 = 8(4 - \sqrt{-11})$, donc

si f est primitif de $(1 + \sqrt{-11})/2$-division, $\alpha(f) = -1 - \sqrt{-11}$,

si f est primitif de $(1 - \sqrt{-11})/2$-division, $\alpha(f) = -1 + \sqrt{-11}$.

BIBLIOGRAPHIE

[C-N, T 1] Ph. CASSOU-NOGUES et M.J. TAYLOR, Elliptic functions and rings of integers, Birkhauser, Progress in Mathematics, 66, 1987.

[C-N, T 2] Ph. CASSOU-NOGUES et M.J. TAYLOR, A note on Elliptic curves and the monogeneity of rings of integers, à paraître.

[C] J. COUGNARD, Conditions nécessaires de monogénéité. Application aux extensions cycliques de degré premier $l \geq 5$ d'un corps quadratique imaginaire, J. London Math. Soc., (2) 37 (1988), 73-87.

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

[G 1] M.-N. GRAS, Lien entre le groupe des unités et la monogénéité des corps cubiques cycliques, Publ. math. Fac. Sciences de Besançon, Théorie des Nombres, 1975-76.

[G 2] M.-N. GRAS, $\mathbb{Z}$-base d'entiers $1, \theta, \theta^2, \theta^3$ dans les extensions cycliques de degré 4 de $\mathbb{Q}$, Publ. Math. Fac. Sciences de Besançon, Théorie des Nombres, 1980-81.

[G 3] M.-N. GRAS, Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de $\mathbb{Q}$, Pub. Mat. Fac. Sci. Besançon, 1983-1984.

[G, Z] B. GROSS, D. ZAGIER, On singular moduli, J. reine angew. Math., 355 (1985), 191-220.

[L 1] S. LANG, Elliptic Functions, Addison Wesley, 1973.

[L 2] S. LANG, Elliptic Curves Diophantine Analysis, Springer-Verlag, Berlin Heidelberg New York, 1978.

[L 3] S. LANG, Algebraic Number Theory, Addison-Wesley, Reading, MA, 1970.

[Li] J. LIANG, On the integral basis of the maximal real subfield of a cyclotomic field, J. reine angew. Math., 286/87 (1976), 223-226.

[R] H. RADEMACHER, Topics in Analytic Number Theory, Springer-Verlag.

[S] J.-P. SERRE, Corps locaux, Hermann, Paris, 1968.

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

Manuscrit reçu le 13 février 1987.

Vincent FLECKINGER,
Faculté des Sciences et des Techniques
Laboratoire de Mathématiques
Route de Gray
25030 Besançon Cedex.