JOURNAL OF NUMBER THEORY 30, 140–155 (1988)

Génération de l'anneau des entiers des corps de classes de $\mathbb{Q}(i)$ de rayon impair et points de division de $y^2 = x^2 - x$

JEAN COUGNARD

UA n° 741 du CNRS, Laboratoire de Mathématiques, UFR Sciences, F-25030 Besançon, Cedex, France

Communicated by M. Waldschmidt

Received September 28, 1987

Given odd ideals $\mathfrak{f}$ of the ring of Gauss integers $\mathbb{Z}[i]$ we describe the rings of integers of the ray class fields of $\mathbb{Q}(i)$ with conductors $\mathfrak{f}$. We prove that these rings have power basis over $\mathbb{Z}[i]$ and we give an explicit algorithm to obtain the irreducible polynomials of the generators.

Dans tout ce qui suit i est une racine carrée de -1 et pour chaque corps de nombres algébriques K on désigne par $\mathbb{Z}_K$ son anneau des entiers. On se propose de démontrer le résultat suivant:

THÉORÈME 1. *Soit $\mathfrak{f}$ un idéal entier impair de $\mathbb{Z}[i]$ et $K = \mathbb{Q}(i)^{(\mathfrak{f})}$ le corps de classes de $\mathbb{Q}(i)$ de rayon $\mathfrak{f}$, il existe un élément θ de $\mathbb{Z}_K$ tel que $\mathbb{Z}_K = \mathbb{Z}[i][\theta]$.*

Ce travail fait suite à un article consacré à la monogénéité de l'anneau des entiers des extensions cycliques de degré premier $l \geqslant 5$ d'un corps quadratiquc imaginaire [3]. De la comparaison du théorème 1 de l'article précité et de celui énoncé ci-dessus, on déduit:

COROLLAIRE. *Les seules extensions cycliques de degré l premier $\geqslant 5$ de $\mathbb{Q}(i)$ dont l'anneau des entiers soit $\mathbb{Z}[i]$-monogène sont les suivantes:*

(a) *les corps de classes de $\mathbb{Q}(i)$ de rayon $(2+i)^2$, $(2-i)^2$;*

(b) *les corps composés de $\mathbb{Q}(i)$ et du sous-corps réel maximal du corps des racines p-ièmes de l'unité avec $p = 2l+1$ premier;*

(c) *les corps de classes de $\mathbb{Q}(i)$ de rayon $\mathfrak{p}$ avec $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p}) = 4l+1$ premier.*

0022-314X/88 $3.00

Ce travail doit beaucoup à la lecture du livre de Ph. Cassou-Noguès et M.-J. Taylor [1].

A leur manière (voir également [2]) on étudie les propriétés arithmétiques des points de division de la courbe elliptique $E=\mathbb{C}/\mathbb{Z}[i]$; l'élément θ est la valeur d'une fonction définie sur E en un point de division convenablement choisi (cf. Th. 4).

Les formules de récurrence associées à la multiplication complexe sur E permettent de calculer explicitement les polynômes $\mathrm{Irr}(\theta, \mathbb{Q}(i))$.

1. Le modèle de Fueter modifié

Soit la courbe elliptique $E=\mathbb{C}/\mathbb{Z}[i]$ paramétrons la tout d'abord par la fonction $\mathfrak{p}$ de Weierstrass, définie par

$$\mathfrak{p}(z)=\frac{1}{z^2}+\sum_{\omega\in\mathbb{Z}[i]-\{0\}}\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2},$$

et sa dérivée $\mathfrak{p}'$ liées par l'équation $\mathfrak{p}'(z)^2=4\mathfrak{p}(z)^3-g_2\,\mathfrak{p}(z)$ où $g_2=60\sum_{\omega\in\mathbb{Z}[i]-\{0\}}(1/\omega^4)$. Les développements de $\mathfrak{p}$ et $\mathfrak{p}'$ en séries de fractions rationnelles montrent que $\mathfrak{p}(iz)=-\mathfrak{p}(z)$; $\mathfrak{p}'(iz)=i\mathfrak{p}'(z)$. La fonction $\mathfrak{p}'$ s'annule aux points $\sigma_1=\frac{1}{2}$, $\sigma_2=i/2$, $\sigma_3=(1+i)/2$. L'équation de Weierstrass montre que $\mathfrak{p}$ s'annule en un des points σ_i, les relations précédentes et le fait que $\mathfrak{p}$ ait pour ordre 2 montrent que c'est en σ_3 et que $4\mathfrak{p}(\sigma_j)^2=g_2$ pour $j=1, 2$. Posons:

$$T(z)=\frac{\mathfrak{p}(1/2)}{\mathfrak{p}(z)}. \tag{1}$$

La seconde fonction de Weber étant $h_E(z)=(2^8\cdot 3^4)/g_2\,\mathfrak{p}(z)^2=(2^6\cdot 3^4)/T(z)^2$, on en déduit que pour un idéal entier $\mathfrak{f}$ de $\mathbb{Z}[i]$ le corps de classes de $\mathbb{Q}(i)$ de rayon $\mathfrak{f}$ est engendré sur $\mathbb{Q}(i)$ par les valeurs que la fonction T^2 prend aux points primitifs de $\mathfrak{f}$-division de E. Par définition de T on a:

$$T(z)=\mathfrak{p}(1/2)\,z^2+o(z^3),\qquad T(1/2)=1,\qquad T(i/2)=-1. \tag{2}$$

Le diviseur de la fonction T est égal à:

$$(T)=2(0)-2(\sigma_3). \tag{3}$$

De (3) et de (2) on déduit la formule d'inversion:

$$T(z)\,T(z+\sigma_3)=-1. \tag{4}$$

Définissons:

$$T_1(z) = \frac{i}{2}\,\mathfrak{p}(1/2)^{-1/2}\,T'(z).$$

Le diviseur de la fonction T_1 est égal:

$$(T_1) = (0) + (\sigma_1) + (\sigma_2) - 3(\sigma_3). \tag{5}$$

En reportant $\mathfrak{p}$ et $\mathfrak{p}'$ exprimés en fonction de T et T_1 on obtient:

$$T_1^2 = T^3 - T. \tag{6}$$

Pour faciliter la démonstration des formules du paragraphe suivant on peut donner des équivalents pour la fonction T_1 aux points de 2-division:

$$\begin{aligned} T_1(z + 1/2) &= -2i\mathfrak{p}(1/2)^{1/2}\,z + o(z) \\ T_1(z + i/2) &= -2i\mathfrak{p}(1/2)^{1/2}\,z + o(z) \\ T_1(z) &= i\mathfrak{p}(1/2)^{1/2}\,z + o(z) \end{aligned} \tag{7}$$

et $\lim_{z \mapsto 0} z^3 T_1(z + \sigma_3) = i\mathfrak{p}(1/2)^{-3/2}$.

On définit également, pour faciliter l'écriture de la formule d'addition, la fonction D telle que $D(z) = T_1(z)/T(z)$, c'est une fonction impaire de diviseur:

$$(D) = \left(\frac{1}{2}\right) + \left(\frac{i}{2}\right) - (0) - \left(\frac{1+i}{2}\right).$$

On constate immédiatement que la fonction $z \mapsto D(z)\,D(z + \frac{1}{2})$ a un diviseur nul. En évaluant à l'origine on obtient:

$$D(z)\,D(z + \tfrac{1}{2}) = 2.$$

De même, en prenant la dérivée logarithmique de la relation d'inversion (4):

$$D(z) + D(z + \sigma_3) = 0. \tag{8}$$

2. Formulaire pour la courbe $Y^2 = X^3 - X$

Les formules qui suivent s'obtiennent de la même manière que les formules analogues pour le modèle de Fueter, on renvoie donc à [1] pour les démonstrations.

Formule d'addition:

$$T(u+v) = -\frac{[D(u)+D(v)]^2\, T(u)T(v)}{(1+T(u)T(v))^2}. \tag{9}$$

On en déduit la formule de duplication:

$$T(2u) = T(u)\frac{(4-4T(u)^2)}{(1+T(u)^2)^2} \tag{10}$$

et la *formule de soustraction*:

$$(T(u)-T(v))^2\,(T(u+v)-T(u-v)) = -4T(u+v)\,T(u-v)\;T_1(u)\;T_1(v). \tag{11}$$

En remplaçant v par iv, et en tenant compte de $T(iv) = -T(v)$ on obtient une nouvelle formule qui multipliée par (11) donne

$$\begin{aligned}[T(u)^2 - T(v)^2]^2\,(T(u+v)-T(u-v))(T(u+iv)-T(u-iv)) \\ = 16iT(u+v)\,T(u-v)\,T(u+iv)\,T(u-iv)\;T_1(u)^2\;T_1(v)^2\end{aligned} \tag{12}$$

formule du produit pour la fonction T: Soit $v \in 1+(1+i)\mathbb{Z}[i]$ et $\{\alpha\}$ l'ensemble des points de v-division de $\mathbb{C}/\mathbb{Z}[i]$, on a alors:

$$T(vz) = \varepsilon_v \prod_{\alpha} T(z+\alpha) \qquad \text{avec} \quad \varepsilon_v = 1 \qquad \text{si} \quad v \equiv 1 \bmod 2,\ \varepsilon_v = -1 \text{ sinon.} \tag{13}$$

On en déduit, en divisant par $T(z)$, et en faisant tendre z vers 0

$$v^2 = \varepsilon_v \prod_{\substack{\alpha \neq 0 \\ v\alpha = 0}} T(\alpha). \tag{14}$$

En utilisant le diviseur de T_1 et les équivalents aux points de 2 division on démontre:

$$T_1(z)\;T_1(z+1/2)\;T_1(z+i/2)\;T_1(z+\sigma_3) = 2^2$$

d'où l'on déduit la formule du produit pour la fonction T_1:

$$\eta_v 2^{(N(v)-1)/2} T_1(vz) = \prod_{\substack{\alpha \\ v\alpha = 0}} T_1(z+\alpha) \qquad \text{avec } \eta_v \text{ racine quatrième de 1.} \tag{15}$$

En divisant par $T_1(z)$, faisant tendre z vers 0, et utilisant un équivalent pour $T_1(z)$ au voisinage de $z=0$, on obtient la relation:

$$\eta_v \cdot v \cdot 2^{(N(v)-1)/2} = \prod_{\substack{\alpha \neq 0 \\ v\alpha = 0}} T_1(\alpha). \tag{16}$$

3. Multiplication complexe de la courbe $Y^2 = X^3 - X$

Pour $v \in \mathbb{Z}[i]$ la fonction $z \mapsto T(vz)$ est une fonction paire, c'est donc une fraction rationelle en $T(z)$. Choisissons $v \equiv 1 \ (1+i)$ et définissons

$$Z_v(X) = \prod_{\beta}'' (X - T(\beta))(X - T(i\beta)) = \prod_{\beta}'' (X^2 - T(\beta)^2)$$

$$N_v(X) = v \prod_{\beta}'' (X - T(\beta + \sigma_3))(X - T(i\beta + \sigma_3)) = v \prod_{\beta}'' (X^2 - T(\beta + \sigma_3)^2)$$

où $\prod_{\beta}''$ désigne le produit sur un système de représentants des orbites des points de v-division non nuls pour l'action des automorphismes de la courbe elliptique.

Proposition 1. *La fonction T vérifie la formule de multiplication*

$$T(vz) = T(z) \frac{Z_v(T(z))^2}{N_v(T(z))^2}. \tag{17}$$

Démonstration. Comme dans [1] on compare les diviseurs de chacun des membres ce qui donne l'égalité à une constante multiplicative près. On remplace ensuite z par $z + \sigma_3$ et on fait tendre z vers 0 en tenant compte de ce que les racines de Z_v et N_v sont inverses les unes des autres.

En utilisant la formule de duplication $T(2u) = T(u) \cdot ((-4T(u)^2 + 4)/(1 + T(u)^2)^2)$ notons $z_2(X) = -4X^2 + 4$, $N_2(X) = X^2 + 1$.

Proposition 2. *Les polynômes N_v, Z_v vérifient les formules de récurrence*:

$$\begin{aligned} Z_{v-2}^2 \cdot N_2^2 - z_2 \cdot N_{v-2}^2 &= Z_v Z_{v-4} \\ Z_{v-2i}^2 \cdot N_2^2 + z_2 N_{v-2i}^2 &= Z_v \cdot Z_{v-4i}. \end{aligned} \tag{18}$$

Démonstration. On considère les fonctions $T((v-2)z) - T(2z)$ et

$$T(z) \frac{Z_v(T(z))\, Z_{v-4}(T(z))}{N_2(T(z))^2\, N_{v-2}(T(z))^2},$$

on procède comme dans la proposition précédente pour obtenir l'égalité de ces deux fonctions. On remplace $T((v-2)z)$ et $T(2z)$ au moyen de (10) et (17) puis on réduit au même dénominateur et on obtient la première des deux formules; la seconde s'obtient de manière analogue.

PROPOSITION 3. *Les polynômes Z_v et N_v sont liés par les relations*:

$$Z_v = c_v X^{(N(v)-1)/2} N_v(1/X)$$

$$N_v = \delta c_v X^{(N(v)-1)/2} Z_v(1/X)$$

où $c_v^4 = 1$ et $\delta = \pm 1$.

Démonstration. On calcule $T(z)$ aux points $(1+i)/4$, $(1+i)/4+1/2$, $(1+i)/4+i/2$, $(1+i)/4+(1+i)/2$, $1/2$, $i/2$ et on constate que ces points sont les seuls où $T^2(z)$ est égal à son inverse. On en déduit que les polynômes Z_v et N_v sont premiers entre eux. On remplace z par $z+\sigma_3$ ce qui donne

$$\frac{1}{T(vz)} = \frac{1}{T(z)}\left[\frac{Z_v(1/T(z))\,T(z)^{(N(v)-1)/2}}{N_v(1/T(z))\,T(z)^{(N(v)-1)/2}}\right]^2 = \frac{1}{T(z)}\cdot\frac{N_v(T(z))^2}{Z_v(T(z))^2}$$

ce qui donne les formules de la proposition avec $c \in \mathbb{C}^*$. Donc en particulier $Z_v(0) = c_v v$, $N_v(0) = \delta c_v$ mais $Z_v(0)\,N_v(0) = v\prod'_\beta T(\beta)\,T(\beta+\sigma_3) = v$ ($\prod'$ est produit sur un demi-système des points $\pm\beta$ non nuls de v division. Il suffit de connaître $Z_v(0)$ pour déterminer c_v et δ.

PROPOSITION 4. *On a les égalités suivantes*:

$$Z_4 = 1, \qquad N_1 = 1, \qquad Z_i = 1, \qquad N_i = i$$

$$Z_3 = Z_{3i} = X^4 + 6X^2 - 3, \qquad N_3 = 3X^4 - 6X^2 - 1 = -iN_{3i}$$

$$Z_{1+2i} = X^2 - (1+2i), \qquad N_{1+2i} = (1+2i)\,X^2 - 1,$$

$$Z_{2+i} = X^2 + i(2+i), \qquad N_{2+i} = (2+i)\,X^2 - i$$

$$Z_{3+2i} = X^6 + (-11+10i)\,X^4 + (7-4i)\,X^2 + 3 + 2i,$$

$$N_{3+2i} = (3+2i)\,X^6 + (7-4i)\,X^4 + (-11+10i)\,X^2 + 1$$

$$Z_{2+3i} = X^6 - (11+10i)\,X^4 + (7+4i)\,X^2 + 3 - 2i,$$

$$N_{2+3i} = (2+3i)\,X^6 + (-4+7i)\,X^4 + (10-11i)\,X^2 + i.$$

Démonstration. Pour $v = 1, i$: cela résulte immédiatement de la définition de Z_v, N_v.

Pour $v = 3$: on démontre, en utilisant toujours la même méthode, que $T(z) - T(2z) = T(z)\,Z_3(T(z))/N_2^2(T(z))$ puis on applique la formule de duplication et on réduit au même dénominateur; quand on a Z_3 la proposition précédente donne immédiatement N_3. La définition de Z_v montre que $Z_{3i} = Z_3$ ce qui donne immédiatement N_{3i}.

Pour $v = 1+2i$ on démontre que

$$T(2z) - T(iz) = T(z)\,\frac{Z_{1+2i}(T(z))\,Z_{2+i}(T(z))}{N_2(T(z))^2}.$$

Par identification on en déduit que: $Z_{1+2i}\cdot Z_{2+i}=X^4-2X^2+5=[X^2-(1+2i)][X^2-1+2i]$ sachant que $Z_v(0)=cv$ avec $c^4=1$ on en déduit Z_{1+2i} et Z_{2+i} puis, au moyen de la proposition précédente, N_{1+2i}, N_{2+i}.

Pour $v=3+2i$ on démontre que

$$T(1+2iz)-T(2z)=T(z)\cdot\frac{Z_{3+2i}(T(z))\,Z_{2+i}(T(z))}{N_2(T(z))^2\,N_{1+2i}(T(z))^2}.$$

Comme on connait Z_{2+i} et N_{1+2i}, en remplaçant par leur expression, on obtient Z_{3+2i} d'où l'on déduit N_{3+2i}.

Pour $v=2+3i$, ce nombre est associé au conjugué de $3+2i$. Comme la conjugaison complexe est un automorphisme continu de $\mathbb{C}$ on en déduit que Z_{2+3i} est le polynôme dont les coefficients sont conjugués de ceux de Z_{3+2i}. La proposition précédente donne alors N_{2+3i}.

THÉORÈME 2. *Pour $v\in 1+(1+i)\,\mathbb{Z}(i)$ les polynômes Z_v et N_v appartiennent à $\mathbb{Z}[i][X]$ et $Z_v(0)=c_v v$, $N_v(0)=c_v^{-1}$ où c_v est une racine quatrième de l'unité telle que $c_v^2=1$ si $v\equiv 1$ modulo 2, $c_v^2=-1$ sinon.*

Démonstration. Si Z_{v-2}, N_{v-2}, Z_{v-4} appartiennent à $\mathbb{Z}[i][X]$ le membre de gauche de la première des formules (18) appartient à $\mathbb{Z}[i][X]$. Comme Z_{v-2} est unitaire et de même degré que N_{v-2} il en résulte que Z_vZ_{v-4} est un polynôme unitaire de $\mathbb{Z}[i][X]$. On divise par Z_{v-4} ce qui montre qu'alors Z_v est un polynôme unitaire de $\mathbb{Z}[i][X]$. La Proposition 3 montre que sous ces conditions $N_v\in\mathbb{Z}[i][X]$. Un raisonnement analogue peut être appliqué à la seconde des formules (18). On peut alors utiliser les valeurs déjà calculées de Z_v, N_v pour démontrer le théorème, lorsque $\mathrm{Im}(v)\geqslant 0$, $\mathrm{Re}(v)\geqslant 0$, en faisant une récurrence parallèlement aux axes. Comme Z_v ne dépend que de l'idéal engendré par v, ce polynôme appartient à $\mathbb{Z}[i][X]$ quel que soit v, et il en est donc de même pour N_v.

Si on évalue en 0 les formules (18) on obtient:

$$c_{v-2}^2\cdot(v-2)^2-4c_{v-2}^2=(v-4)\,vc_vc_{v-4}\quad\text{soit}\quad c_v^2-2=c_vc_{v-4}\quad\text{soit}$$
$$c_v^2c_{v-4}^2=1\text{ si }c_{v-2}^2=c_{v-4}^2,\text{ on en déduit }c_v^2=c_{v-4}^2\text{ et }c_v=c_{v-4},$$

on procède de même avec l'autre formule. Ce qui termine la démonstration.

COROLLAIRE 1. *Soit $v\in 1+(1+i)\,\mathbb{Z}[i]$ et α un point de v-division de $\mathbb{C}/\mathbb{Z}[i]$ alors $T(\alpha)$ et $T_1(\alpha)$ sont des entiers algébriques.*

COROLLAIRE 2. *Pour $v\in 1+(1+i)\,\mathbb{Z}[i]$, les polynômes N_v vérifient les formules de récurrence*:

$$\begin{aligned}N_{v-2}^2N_2^2+X^2z_2Z_{v-2}^2&=N_vN_{v-4}\\ N_{v-2i}^2N_2^2-X^2z_2Z_{v-2i}^2&=N_vN_{v-4i}.\end{aligned}\tag{19}$$

Démonstration. Dans les formules de récurrence (18) on utilise la proposition 3 et la relation $c_{\nu-2}^2 = c_\nu c_{\nu-4}$.

Remarque. Les formules de récurrences (18) et (19) associées aux valeurs de Z_ν, N_ν calculées dans la proposition 3 permettent de déterminer explicitement les polynômes Z_ν, N_ν.

4. Transformation des formules de récurrence

On a remarqué au premier paragraphe que pour un idéal entier $\mathfrak{f}$ et α un point primitif de $\mathfrak{f}$ division de $\mathbb{C}/\mathbb{Z}[i]$ la valeur $T(\alpha)^2$ engendrait sur $\mathbb{Q}(i)$ le corps de classes de rayon $\mathfrak{f}$. En particulier si β est tel que $(1+2i)\beta \in \mathbb{Z}[i]$, $\beta \notin \mathbb{Z}[i]$. Les calculs de polynômes de la proposition 3 montrent qu'alors $T(\beta)^2 = 1+2i$. Des essais numériques suggèrent que si α est un point de $\mathfrak{f}$ division de E $T(\alpha)^2 - T(\beta)^2$ possède des propriétés de divisibilité: plus précisément, si on substitue $4X^2+1+2i$ à X^2 dans les polynômes Z_ν et N_ν calculés dans la proposition 3, on obtient des polynômes dont les coefficients sont des entiers divisibles par $4^{(N(\nu)-1)/4}$ ce qui laisse penser que pour tout point α de E d'annulateur impair on a $T(\alpha)^2 \equiv 1+2i$ (4).

Définition. On note $\tilde{Z}_\nu$ (resp. $\tilde{N}_\nu$) le polynôme de $\mathbb{Q}(i)[X]$ obtenu en substituant $4X^2+1+2i$ à X^2 dans Z_ν (resp. N_ν) puis en divisant par $2^{(N(\nu)-1)/2}$.

Théorème 3. *Les polynômes $\tilde{Z}_\nu$, $\tilde{N}_\nu$ appartiennent à $\mathbb{Z}[i][X]$ et $\tilde{Z}_\nu$ congrue à $\tilde{N}_\nu$ modulo $(1+i)\mathbb{Z}[i][X]$.*

Démonstration. Calculons $\tilde{Z}_\nu$, $\tilde{N}_\nu$ pour $\nu = 1,\ 1+2i,\ 2+i$:

$$\nu = 1,\ \tilde{Z}_1 = \tilde{N}_1,\ \nu = 1+2i,$$

$$\tilde{Z}_{1+2i} = X^2,\ \tilde{N}_{1+2i} = (1+2i)X^2 - 1 + i;$$

$$\tilde{Z}_{2+i} = X^2 + i,\ \tilde{N}_{2+i} = (2+i)X^2 + i.$$

On obtient des résultats semblables pour les valeurs de ν qui se déduisent des précédentes par multiplication par -1, $\pm i$; on constate que le résultat annoncé est vérifié pour toutes ces valeurs. En particulier on a $\tilde{Z}_\nu^2 + \tilde{N}_\nu^2 \equiv 0$ (2).

On transforme ensuite les couples de formules (18), (19). Faisons les calculs pour les formules de récurrence liant les polynômes indicés par ν, $\nu-2$, $\nu-4$. Notons A_ν (resp. B_ν) le polynôme obtenu en substituant $4X^2+1+2i$ à X^2 dans Z_ν (resp. N_ν). Cette substitution transforme $-z_2$ en $16X^2+8i$, N_2 en $16X^4+16(1+i)X^2+8i$, $X^2 z_2$ en $-64X^4-16(1+4i)X^2 + 16-8i$.

Les formules de récurrence deviennent:

$$16[A_{v-2}^2(X^4+(1+i)X^2) + X^2B_{v-2}^2] + 16i\left[\frac{A_{v-2}^2+B_{v-2}^2}{2}\right] = A_vA_{v-4}$$

$$16[B_{v-2}^2(X^4+(1+i)X^2) - (4X^4+(1+4i)X^2+1)\,A_{v-2}^2] + 16i\left[\frac{B_{v-2}^2-A_{v-2}^2}{2}\right] = B_vB_{v-4}.$$

Si on admet que le théorème est vérifié pour $v-2$ et $v-4$, on peut diviser les deux membres par $(1+i)^{N(v-4)-1+N(v)-1}$ ce qui donne

$$\tilde{Z}_{v-2}^2(X^4+(1+i)X^2) + X^2\tilde{N}_{v-2}^2 + i\left[\frac{\tilde{Z}_{v-2}^2+\tilde{N}_{v-2}^2}{2}\right] = \tilde{Z}_v\tilde{Z}_{v-4}$$

$$\tilde{N}_{v-2}^2(X^4+(1+i)X^2) - (4X^2+(1+4i)X^2-1)\,\tilde{Z}_{v-2}^2 + i\left(\frac{\tilde{N}_{v-2}^2-\tilde{Z}_{v-2}^2}{2}\right) = \tilde{N}_v\tilde{N}_{v-4} \tag{20}$$

par hypothèse de récurrence les membres de gauche appartiennent à $\mathbb{Z}[i][X]$ et $\tilde{Z}_{v-4}$ est unitaire et appartient à $\mathbb{Z}[i][X]$, on en déduit que $\tilde{Z}_v$ est un polynôme unitaire de $Z[i][X]$. Par construction le polynôme $\tilde{N}_v$ a ses coefficients qui sont des entiers en dehors de $1+i$. On peut réécrire la formule (20):

$$\tilde{Z}_v = \left(\tilde{Z}_{v-2}^2(X^4+(1+i)X^2) + X^2\tilde{N}_{v-2}^2 + i\left[\frac{\tilde{Z}_{v-2}^2+\tilde{N}_{v-2}^2}{2}\right]\right)\Big/\tilde{Z}_{v-4}$$

$$\tilde{N}_v = \left(\tilde{N}_{v-2}^2(X^4+(1+i)X^2) - (4X^2+(1+4i)X^2) \times \tilde{Z}_{v-2}^2 + i\left[\frac{\tilde{Z}_{v-2}^2+\tilde{N}_{v-2}^2}{2}\right] - (1+i)\,\tilde{Z}_{v-2}^2\right)\Big/\tilde{N}_{v-4}.$$

On constate en réduisant modulo $(1+i)$ que $\tilde{Z}_v \equiv \tilde{N}_v \bmod(1+i)$ donc les coefficients de N_v sont également entiers en $(1+i)$.

On peut procéder de la même manière avec les polynômes indicés par v, $v-2i$, $v-4i$, on obtient les formules:

$$\tilde{Z}_{v-2i}(X^4+(1+i)X^2)-X^2\tilde{N}^2_{v-2i}+i\left(\frac{\tilde{Z}^2_{v-2i}-\tilde{N}^2_{v-2i}}{2}\right)=\tilde{Z}_v\tilde{Z}_{v-4i}$$

$$\tilde{N}_{v-2i}(X^4+(1+i)X^2)+(4X^2+(1+4i)X^2-1)\,\tilde{Z}^2_{v-2i}+i\left(\frac{\tilde{Z}^2_{v-2i}+\tilde{N}^2_{v-2i}}{2}\right)=\tilde{N}_v\tilde{N}_{v-4i}.$$

On en déduit les mêmes conclusions qu'avec les formules (20). Le théorème 3 en résulte en faisant une récurrence su les $v\in 1+(1+i)\mathbb{Z}[i]$.

COROLLAIRE. (a) *Soit* $v\in 1+(1+i)\mathbb{Z}[i]$ *et* α *un point de* v*-division non nul de* $\mathbb{C}/\mathbb{Z}[i]$ *alors* $T(\alpha)^2\equiv 1+2i \pmod 4$, *en particulier* $T_1(\alpha)^2\equiv 0 \pmod 2$.

(b) *Soit* v (*resp.* v')$\in 1+(1+i)\mathbb{Z}[i]$ *et* α(*resp.* α') *au point de* v (*resp.* v') *division non nul de* $\mathbb{C}/\mathbb{Z}[i]$ *alors* $T(\alpha)-T(\alpha')\equiv 0 \pmod 2$.

Démonstration. La première assertion du (a) résulte de la construction du polynôme $\tilde{Z}_v$, la seconde de l'équation $T_1(\alpha)^2=T(\alpha)(T(\alpha)^2-1)$.

Du (a) on déduit $0\equiv T(\alpha)^2-T(\alpha')^2=(T(\alpha)-T(\alpha'))(T(\alpha)-T(\alpha')+2T(\alpha'))$ modulo 4 qui donne immédiatement le (b).

5. PROPRIÉTÉS DE DIVISIBILITÉ DES VALEURS DE T, T_1 AUX POINTS DE DIVISION D'ORDRE IMPAIR DE $\mathbb{C}/\mathbb{Z}[i]$

On se propose d'utiliser les formules (13) à (16) ainsi que le corollaire du théorème 3 pour préciser les propriétés de divisibilité des nombres $T(\alpha)$, $T_1(\alpha)$.

PROPOSITION 5. *Soient* $\mathfrak{f}$ *un idéal entier impair,* γ *et* δ *deux points primitifs de* $\mathfrak{f}$ *division de* $\mathbb{C}/\mathbb{Z}[i]$ *alors le quotient de* $T(\gamma)$ *par* $T(\delta)$ *est une unité.*

Démonstration. On peut trouver v premier à $\mathfrak{f}$, congru à 1 modulo 2 tel que $v\gamma=\delta$. La formule (13) donne $T(\delta)=T(\gamma)\prod_{\alpha\neq 0}T(\gamma+\alpha)$ où le produit est pris sur les points de v-division non nuls; $\gamma+\alpha$ étant un point de $v\mathfrak{f}$ division $T(\gamma+\alpha)$ est un entier algébrique et $T(\gamma)$ divise $T(\delta)$. La divisibilité de $T(\gamma)$ par $T(\delta)$ s'obtient de la même manière d'où le résultat.

LEMME. *Soit* $\mathfrak{f}$ *un idéal entier impair de* $\mathbb{Z}[i]$ *divisible au moins par deux idéaux premiers distincts*: $\mathfrak{f}=\mathfrak{p}^r\mathfrak{q}$ ($\mathfrak{p}$ *premier*, $\mathfrak{p}+\mathfrak{q}=\mathbb{Z}[i]$) *et* γ *un point primitif de* $\mathfrak{f}$ *division de* $\mathbb{C}/\mathbb{Z}[i]$; *si* $\mathfrak{p}^r=(\pi)$ *alors* $T(\gamma)$ *divise* π.

Démonstration. Soit $\nu\in\mathbb{Z}[i]$, vérifiant $\nu\equiv 1\ (1+i)\pi$ et $\nu\equiv O(\mathfrak{q})$; puisque γ est un point primitif de $\mathfrak{f}$-division, $\nu\gamma$ est un point primitif de $\mathfrak{p}^r$-division, en particulier il est non nul donc $T(\nu\gamma)$ est une racine de $Z_\pi(X)$ et divise $Z_\pi(0)$; mais la formule du produit montre, comme précédemment, que $T(\gamma)$ divise $T(\nu\gamma)$.

COROLLAIRE 1. *Soit* $\mathfrak{f}$ *un idéal entier impair divisible par deux idéaux premiers distincts et* ν *un point primitif de* $\mathfrak{f}$ *division de* $\mathbb{C}/\mathbb{Z}[i]$ *alors* $T(\gamma)$ *est une unité.*

DÉFINITION. Soit $\mathfrak{f}$ un idéal entier impair de $\mathbb{Z}[i]$, on note $S_\mathfrak{f}$ le polynôme $\prod''_\beta(X-T(\beta))(X-T(i\beta))=\prod''_\beta(X^2-T(\beta)^2)$ où $\prod''_\beta$ désigne le produit sur un système de représentants des orbites des points primitifs de $\mathfrak{f}$ division pour l'action des automorphismes de $\mathbb{C}/\mathbb{Z}[i]$.

Remarque. En substituant X à X^2 dans $S_\mathfrak{f}$, on obtient le polynôme irréductible de $T^2(\beta)$ sur $\mathbb{Q}(i)$.

COROLLAIRE 2. *Soit* $\mathfrak{f}$ *un idéal entier impair de* $\mathbb{Z}[i]$, *si* $\mathfrak{f}$ *est divisible par deux idéaux premiers distincts* $S_\mathfrak{f}(0)$ *est une unité, si* $\mathfrak{f}=(\pi^r)$ *où* π *est un élément irréducible de* $\mathbb{Z}[i]$ *et* r *un entier* >0 *alors* $S_\mathfrak{f}(0)$ *est associé à* π.

Démonstration. Dans le premier cas $S_\mathfrak{f}(0)$ est le produit des $T(\gamma)$ qui sont des unités, dans le second cas on utilise la décomposition $Z_{\pi^r}=S_\mathfrak{f}\cdot Z_{\pi^{r-1}}$ et le théorème 2.

De ces résultats, on peut déduire:

PROPOSITION 6. *Soient* $\mathfrak{f}=(\pi^r)$ *où* π *est un élément irréductible de* $\mathbb{Z}[i]$, r *un entier* >0 *et* α *un point primitif de* $\mathfrak{f}$ *division de* $\mathbb{C}/\mathbb{Z}[i]$, *alors* $T(\alpha)^2$ *est une uniformisante de l'unique idéal premier* $\mathfrak{B}$ *au-dessus de* $\mathfrak{p}$ *dans le corps de classes de* $\mathbb{Q}(i)$ *de rayon* $\mathfrak{f}$.

Démonstration. Puisque $\mathfrak{f}$ est une puissance d'un idéal premier principal et que $\mathbb{Z}[i]$ est principal, il n'y a qu'un idéal $\mathfrak{B}$ au-dessus de (π) dans le corps de classes de rayon $\mathfrak{f}$, cet idéal est totalement ramifié sur $\mathbb{Q}(i)$; $T(\alpha)^2$ engendre le corps de classes de rayon $\mathfrak{f}$ sur $\mathbb{Q}(i)$ et sa norme est associée à π ce qui démontre le résultat.

PROPOSITION 7. *Pour* β *point primitif de* $\mathfrak{f}$*-division avec* $\mathfrak{f}$ *idéal entier impair l'entier algébrique* $\frac{1}{2}T_1(\beta)^2$ *est associé à* $T(\beta)$.

Démonstration. On a $T_1(\alpha)^2/2 = T(\alpha)((T(\alpha)^2-1)/2)$. Soit v un générateur de $\mathfrak{f}$. La formule (16) $\eta_v \cdot v \cdot 2^{(N(v)-1)/2} = \prod_{\alpha \neq 0,\, v\alpha = 0} T_1(\alpha)$ devient:

$$\pm v^2 = \prod_{\substack{\alpha \neq 0 \\ v\alpha = 0}} \frac{T_1(\alpha)^2}{2} = \prod_{\substack{\alpha \neq 0 \\ v\alpha = 0}} T(\alpha) \prod_{\substack{\alpha \neq 0 \\ v\alpha = 0}} \left(\frac{T(\alpha)^2 - 1}{2}\right).$$

Donc d'après la formule (14) $\prod_{\alpha \neq 0,\, v\alpha = 0} ((T(\alpha)^2-1)/2)$ est une unité. Le corollaire du théorème 3 montre que les $(T(\alpha)^2-1)/2$ sont des entiers, ce sont donc des unités d'où le résultat.

6. Démonstration du théorème 1

Nous allons d'abord modifier les formules (11) et (12) en tenant compte du corollaire du théorème 3 et de la proposition 7 lorsque u et v sont des points d'ordre impair de $\mathbb{C}/\mathbb{Z}[i]$.

La formule (11) devient:

$$\left(\frac{T(u)-T(v)}{2}\right)^2 \cdot \left(\frac{T(u+v)-T(u-v)}{2}\right) = -iT(u+v)\cdot T(u-v)\frac{T_1(u)}{1+i}\cdot\frac{T_1(v)}{1+i}. \tag{21}$$

Si on transforme v en iv

$$\left(\frac{T(u)+T(v)}{2}\right)^2 \left(\frac{T(u+iv)-T(u-iv)}{2}\right) = T(u+iv)T(u-iv)\frac{T_1(u)}{1+i}\cdot\frac{T_1(v)}{1+i}. \tag{22}$$

La formule (12) devient:

$$\left[\frac{T(u)^2-1-2i-(T(v)^2-1-2i)}{4}\right]^2 \times \left(\frac{T(u+v)-T(u-v)}{2}\right)\left(\frac{T(u+iv)-T(u-iv)}{2}\right) = iT(u+v)T(u-v)T(u+iv)T(u-iv)\frac{T_1(u)^2}{2}\cdot\frac{T_1(v)^2}{2}. \tag{23}$$

Les facteurs des produits de chacun des membres des formules (21), (22), (23) sont des entiers algébriques. Le théorème que nous énonçons précise le théorème 1:

THÉORÈME 4. *Soit* $\mathfrak{f}$ *un idéal entier impair de* $\mathbb{Z}[i]$, K *le corps de classes de rayon* $\mathfrak{f}$ *de* $\mathbb{Q}(i)$ *et* α *un point primitif de* $\mathfrak{f}$ *division de* $\mathbb{C}/\mathbb{Z}[i]$ *alors* $\mathbb{Z}_K = \mathbb{Z}[i][(T(\alpha)^2 - 1 - 2i)/4]$.

Indications sur la démonstration. Le groupe de Galois de $K/\mathbb{Q}(i)$ est isomorphe, au moyen de la loi de réciprocité d'Artin, et du fait que $\mathbb{Z}[i]$ est principal et $\mathfrak{f}$ impair, à $U/U_{\mathfrak{f}}\langle i\rangle$ où U est le groupe des idèles unités de $\mathbb{Q}(i)$, $U_{\mathfrak{f}}$ le groupe des idèles unités de $\mathbb{Q}(i)$ congrus à 1 mod* $\mathfrak{f}$ et $\langle i\rangle$ le groupe des unités de $\mathbb{Z}[i]$. Nous allons diviser la démonstration en deux parties suivant que $\mathfrak{f}$ est, ou non, puissance d'un idéal premier. Dans chaque cas nous calculons le discriminant de $\mathrm{Irr}((T(\alpha)^2 - 1 - 2i)/4)$ en utilisant les formules (21) à (23) et nous montrons qu'il est égal au discriminant de $K/\mathbb{Q}(i)$ calculé comme produit des conducteurs des caractères de $\mathrm{Gal}(K/\mathbb{Q}(i))$. Rappelons que le discriminant de $\mathrm{Irr}((T(\alpha)^2 - (1+2i)/4, \mathbb{Q}(i))$ est égal à:

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i)) - \{\mathrm{id}\}} N_{K/\mathbb{Q}(i)}\left(\frac{T^2(\alpha) - (1+2i)}{4} - \sigma\left(\frac{T(\alpha)^2 - (1+2i)}{4}\right)\right)$$

$$= \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i)) - \{\mathrm{id}\}} N_{K/\mathbb{Q}(i)}\left(\frac{T(\alpha)^2 - \sigma(T(\alpha)^2)}{4}\right).$$

On sait, par la loi de réciprocité de Shimura (cf. [4, Chap. 11]) que pour $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))$ il existe $a \in U/U_{\mathfrak{f}}\langle i\rangle$ tel que $\sigma(T(\alpha)^2) = T(a\alpha)^2$. Posons donc pour $a \in U/U_{\mathfrak{f}}\langle i\rangle$ $\quad s_a = N_{K/\mathbb{Q}(i)}((T(\alpha)^2 - T(a\alpha)^2)/4)$.

a. *Démonstration lorsque* $\mathfrak{f}$ *est composé.* Choisissons $a \in U/U_{\mathfrak{f}}\langle i\rangle$, $a \neq e$ et utilisons les formules (21) à (23) avec $u = \alpha$, $v = a\alpha$. Les points $u+v$, $u-v$, $u-iv$, $u+iv$, sont des points de $\mathfrak{f}$ division. Les formules (14), (16), le corollaire 1 du théorème 2 et le corollaire du théorème 3 montrent que tous les termes facteurs des produits apparaissant dans les formules (21) à (23) sont des unités en dehors des diviseurs de $\mathfrak{f}$. Nous allons donc nous intéresser à la $\mathfrak{p}$-valuation de s_a, $\mathfrak{p}$ un diviseur premier de $\mathfrak{f}$; écrivons $\mathfrak{f} = \mathfrak{p}^s b$ avec $\mathfrak{p} + b = \mathbb{Z}[i]$. Rappelons que $T_1(u)/(1+i)$, $T_1(v)/(1+i)$ sont des unités (corollaire 1 de la proposition 5 et proposition 7). Si aucun des points $u+v$, $u-v$, $u+iv$, $u-iv$ est $\mathfrak{p}^r$-primitif ($r \leqslant s$) les membres de droite sont des unités en $\mathfrak{p}$, dans ces conditions, la valuation de s_a en $\mathfrak{p}$ est nulle. Si l'un de ces quatre points est $\mathfrak{p}^r$-primitif, il est le seul parmi eux à avoir un annulateur $\mathfrak{p}$-primaire (sinon il en serait de même pour u et v). Puisque a peut être multiplié par une puissance de i on peut

supposer que l'annulateur de $u-v$ est $\mathfrak{p}^r$. On en déduit que $T(u+v)$, $T(u+iv)$, $T(u-iv)$ sont des unités pour les places au-dessus de $\mathfrak{p}$;

$$\frac{T(u)+T(v)}{2}, \qquad \frac{T(u+iv)-T(u-iv)}{2}, \qquad \frac{T(u+v)-T(u-v)}{2}$$

sont également des unités pour les places au-dessus de $\mathfrak{p}$: les deux premiers en utilisant les formules (21), (22), le troisième comme somme d'un élément de valuation nulle et d'un élément de valuation strictement positive. Si on considère la formule (23): $[(T(u)^2-(1+2i))/4-(T(v)^2-(1+2i))/4]^4$ est associé pour les places au-dessus de $\mathfrak{p}$ à $T(u-v)^2$ qui est une uniformisante, dans le corps de classes de $\mathbb{Q}(i)$ de rayon $\mathfrak{p}^r$, pour l'unique place de ce corps au-dessus de $\mathfrak{p}$. Posons $d=[\mathbb{Q}(i)^{(b)}:\mathbb{Q}(i)]$, $q=N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p})$; on a $\mathrm{Gal}(K/\mathbb{Q}(i)^{(b)})\simeq U_b/U_\mathfrak{f}$, $\mathrm{Gal}(\mathbb{Q}(i)^{(\mathfrak{p}^r)}/\mathbb{Q}(i))\simeq U/U_{\mathfrak{p}^r}\langle i\rangle$ et donc $[\mathbb{Q}(i)^{(\mathfrak{f})}:\mathbb{Q}(i)^{(\mathfrak{p}^r)}]=4dq^{s-r}$ et par conséquent $s_a^4=N_{\mathbb{Q}(i)^{(\mathfrak{p}^r)}/\mathbb{Q}(i)}(T(u-v)^2)^{4q^{s-r}d}$ à une $\mathfrak{p}$-unité près. Sous les hypothèses que nous avons faites la $\mathfrak{p}$-valuation de s_a est dq^{s-r}.

Calculons maintenant le nombre de $a\in U/U_\mathfrak{f}\langle i\rangle$ pour lesquels il existe n tel que l'annulateur de $(1-ai^n)\alpha$ soit $\mathfrak{p}^r$. On a: $\mathfrak{p}^r(1-ai^n)\in\mathfrak{f}$, $\mathfrak{p}^{r-1}(1-ai^n)\notin\mathfrak{f}$. Soit $(1-ai^n)\in\mathfrak{f}\mathfrak{p}^{-r}$ et $(1-ai^n)\notin\mathfrak{f}\mathfrak{p}^{-r+1}$ donc $a\in U_{\mathfrak{f}\mathfrak{p}^{-r}}\langle i\rangle$, $a\notin U_{\mathfrak{f}\mathfrak{p}^{-r+1}}\langle i\rangle$ et par conséquent

$$a\in U_{b\mathfrak{p}^{s-r}}\langle i\rangle/U_{b\mathfrak{p}^s}\langle i\rangle - U_{b\mathfrak{p}^{s-r+1}}\langle i\rangle/U_{b\mathfrak{p}^s}\langle i\rangle$$

le nombre de ces a est donc q^r-q^{r-1} si $r\neq s$, $(q-1)\,q^{s-1}-q^{s-1}$ si $r=s$. En sommant sur r de 1 à s la $\mathfrak{p}$-valuation du discriminant de $\mathrm{Irr}((T(\alpha)^2-(1+2i))/4,\mathbb{Q}(i))$ est $d[q^{s-1}(q-1)-q^{s-1}-\sum_{r=1}^{s-1}q^{s-r}(q^r-q^{r-1})]=d(sq^s-(s+1)\,q^{s-1})$.

Calculons maintenant la $\mathfrak{p}$-valuation du discriminant de $K/\mathbb{Q}(i)$. Soit χ un caractère de $\mathrm{Gal}(\mathbb{Q}(i)^{(\mathfrak{p}^sb)}$ si le conducteur de χ est exactement divisible par $\mathfrak{p}^r$, χ se factorise par $\mathrm{Gal}(\mathbb{Q}(i)^{(\mathfrak{p}^rb)}/\mathbb{Q}(i))$ mais pas par $\mathrm{Gal}(\mathbb{Q}(i)^{(\mathfrak{p}^{r-1}b)}/\mathbb{Q}(i))$. Le nombre des caractères de conducteur divisible exactement par $\mathfrak{p}^r$ est égal à $[\mathbb{Q}(i)^{(\mathfrak{p}^rb)}:\mathbb{Q}(i)]-[\mathbb{Q}(i)^{(\mathfrak{p}^{r-1}b)}:\mathbb{Q}(i)]$ c'est-à-dire à $[\mathbb{Q}(i)^{(b)}:\mathbb{Q}(i)][q^{r-1}(q-1)-q^{r-2}(q-1)]$ si $r>1$ et à $[\mathbb{Q}(i)^{(b)}:\mathbb{Q}(i)](q-2)$ si $r=1$. La $\mathfrak{p}$-valuation du discriminant est donc $d[q-2+\sum_{r=2}^{s}rq^{r-2}(q-1)^2]=d(sq^s-(s+1)\,q^{s-1})$. Ceci démontre le théorème lorsque $\mathfrak{f}$ est composé.

b. *Démonstration lorsque* $\mathfrak{f}=\mathfrak{p}^s$. Prenons comme précédemment $a\in U/U_\mathfrak{f}\langle i\rangle-\{e\}$ et posons $\alpha=u$, $a\alpha=v$ dans les formules (21) à (23). Ou bien les quatre points $u+v$, $u-v$, $u+iv$, $u-iv$ sont primitifs de $\mathfrak{p}^s$-division de $\mathbb{C}/\mathbb{Z}[i]$ ou bien un et un seul d'entre eux est primitif de $\mathfrak{p}^r$ division avec $r<s$. Dans ce dernier cas, puisque a peut être multiplié par une puissance de i, on peut supposer que c'est $u-v$ qui est primitif de $\mathfrak{p}^r$ division.

On peut, comme lorsque f est composé, se restreindre au calcul de la $\mathfrak{p}$-valuation de s_a.

Notons $\mathfrak{B}$ l'unique idéal premier de $\mathbb{Q}(i)^{(\mathfrak{p}^s)}$ au-dessus de $\mathfrak{p}$.

Si les quatre points $u+v$, $u-v$, $u+iv$, $u-iv$, ont pour annulateur $\mathfrak{p}^s$, élevons la formule (23) au carré. Le membre de droite est dans K et sa valuation est égale à 6 (propositions 6 et 7). Le nombre $[(T(u)^2-1-2i)/4-(T(v)^2-1-2i)/4]^4$ a une $\mathfrak{B}$-valuation non nulle, multiple de 4 et inférieure à 6. On en déduit que pour ces valeurs de a la $\mathfrak{p}$-valuation de s_a est égale à 1.

Si $u-v$ est d'ordre $\mathfrak{p}^r$ avec $r<s$, élevons la formule (22) à la puissance 4:

$$\left(\frac{T(u)+T(v)}{2}\right)^2\left(\frac{T(u+iv)-T(u-iv)}{2}\right)^4$$

$$=T(u+iv)^4\cdot T(u-iv)^4\cdot\frac{T_1(a)^4}{4}\cdot\frac{T_1(v)^4}{4}.$$

La $\mathfrak{B}$ valuation du membre de droite est égale à 6. Il n'est pas difficile d'en déduire que $(T(u+iv)-T(u-iv))/2$ est associé à un élément de $\mathbb{Q}(i)^{(\mathfrak{p}^s)}$ dont la $\mathfrak{B}$ valuation est égale à 1.

Comme $T(u+v)^2$ (resp. $T(u-v)^2$) est uniformisante pour $\mathfrak{B}$ (resp. $\mathfrak{B}\cap\mathbb{Q}(i)^{(\mathfrak{p}^r)}$, $(T(u+v)-T(u-v))/2$ est associé à $T(u+v)$.

On élève la formule (23) au carré; on déduit des remarques précédentes que $[(T(u)^2-1-2i)/4-(T(v)^2-1-2i)/4]^4$ a même $\mathfrak{B}$-valuation que $T(u-v)^2\,T^2(u+iv)(T_1(u)^4/4)(T_1(v)^4/4)$. Il en résulte que pour les $a\in U/U_f\langle i\rangle$ tels qu'il existe un entier n vérifiant $(i^n a-1)\alpha$ a pour annulateur $\mathfrak{p}^r$, la $\mathfrak{p}$-valuation de s_a est $\frac{1}{4}(q^{s-r}+3)$, q désignant comme précédemment $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p})$. Dénombrons ces a:

$$\mathfrak{p}^r(1-i^n a)\subset\mathfrak{p}^s,\qquad \mathfrak{p}^{r-1}(1-i^n a)\not\subset\mathfrak{p}^s.$$

Soit $i^n a\in U_{\mathfrak{p}^{s-r}}$, $i^n a\notin U_{\mathfrak{p}^{s-r+1}}$ et donc

$$a\in\langle i\rangle\,U_{\mathfrak{p}^{s-r}}/\langle i\rangle\,U_{\mathfrak{p}^s}-\langle i\rangle\,U_{\mathfrak{p}^{s-r+1}}/\langle i\rangle\,U_{\mathfrak{p}^s}.$$

Pour $r<s$ le nombre de ces éléments est égal à q^r-q^{r-1}, pour $r=s$ ce nombre est égal à $q^{s-1}((q-1)/4)-q^{s-1}$. On en déduit la $\mathfrak{p}$-valuation du discriminant $\mathrm{Irr}((T(\alpha)^2-1-2i/4),\mathbb{Q}(i))$:

$$q^{s-1}\frac{(q-1)}{4}-q^{s-1}+\sum_{r=1}^{s-1}\frac{1}{4}(q^{s-r}+3)(q^r-q^{r-1})$$

$$=\frac{1}{4}[sq^s-(s+1)\,q^{s-1}-3].$$

Il reste, pour terminer, à calculer le discriminant de $\mathbb{Q}(i)^{(\mathfrak{p}^s)}/\mathbb{Q}(i)$. Les caractères de conducteur $\mathfrak{p}^r$ $(r>1)$ sont au nombre de $(q-1/4)(q^{r-1}-q^{r-2})$, ceux de conducteur $\mathfrak{p}$ sont au nombre de $(q-1/4)-1$. La $\mathfrak{p}$-valuation du discriminant est donc égale à $(q-1/4)-1+\sum_{r=2}^{s} e(q-1/4)(q^{r-1}-q^{r-2})$. Après transformation on trouve $\frac{1}{4}[sq^s-(s+1)\,q^{s-1}-3]$. Ce qui achève la démonstration du théorème.

BIBLIOGRAPHIE

1. PH. CASSOU-NOGUÈS ET M. J. TAYLOR, "Elliptic Functions and Rings of Integers," Progress in Mathematics, Vol. 66, Birkhaüser, Basel, 1986.
2. PH. CASSOU-NOGUÈS ET M. J. TAYLOR, A note on elliptic curves and the monogeneity of rings of integers, *J. London Math. Soc.* (*2*) **37** (1988), 63–72.
3. J. COUGNARD, Conditions nécessaires de monogénéité. Application aux extensions cycliques de degré $l \geqslant 5$ d'un corps quadratique imaginaire, *J. London Math. Soc.* (*2*) **37** (1988), 73–87.
4. S. LANG, "Elliptic Functions," Addison–Wesley, Reading, MA, 1973.