Astérisque

GILLES ROBERT

Régularité des idéaux premiers d'un corps quadratique imaginaire de nombre de classes un

Astérisque, tome 24-25 (1975), p. 75-80

<http://www.numdam.org/item?id=AST_1975__24-25__75_0>

Société Mathématique de France
Astérisque 24-25 (1975)

RÉGULARITÉ DES IDÉAUX PREMIERS D'UN CORPS QUADRATIQUE IMAGINAIRE DE NOMBRE DE CLASSES UN

par

Gilles ROBERT

-:-:-:-

Soit $K = \mathbb{Q}\sqrt{-d}$ un corps quadratique imaginaire dont l'anneau des entiers R est principal, c'est-à-dire que $d = 1, 2, 3, 7, 11, 19, 43, 67$ ou 163. Soir $R \subset \mathbb{C}$ un réseau tel que les invariants

$$g_2 = 60 \sum_{\gamma \in \Gamma}{}' 1/\gamma^4 \quad \text{et} \quad g_3 = 140 \sum_{\gamma \in \Gamma}{}' 1/\gamma^6$$

soient des entiers rationnels, et tels que la courbe algébrique d'équation

$$y^2 = 4x^3 - g_2 x - g_3$$

soit isomorphe au tore $\mathbb{C}/R$.

Soit $P(z)$ (fonction P de Weierstrass) la fonction elliptique relative au tore $\mathbb{C}/\Gamma$ qui satisfait à l'équation différentielle

$$P'^2 = 4P^3 - g_2 P - g_3 .$$

Définissons des nombres rationnels $E_{2k} \in \mathbb{Q}$, avec $k \geq 2$, par le développement en série de Taylor à l'origine

$$P(z) = 1/z^2 \left(1 + \sum_{k \geq 2} 2^{2k} (2k-1) E_{2k} z^{2k}\right) \quad ;$$

on a $E_4 = g_2/2^6 . 3 . 5$, $E_6 = g_3/2^8 . 5 . 7$ et l'on peut calculer les nombres E_{2k} , pour $k \geq 4$, à l'aide de la formule de récurrence

$$E_{2k}(k-3)(4k^2-1)/3 = \sum_{i=2}^{k-2} (2i-1)(2k-2i-1) E_{2i} E_{2k-2i}$$

Soit $H(z, z')$ la forme hermitienne définie pour $z \in \mathbb{C}$, $z' \in \mathbb{C}$, par

$$H(z, z') = 12 \pi \bar{z} z'/a$$

où a est l'aire d'un parallélogramme fondamental de Γ . Il existe une et une seule fonction entière $\theta^{(12)}(z)$ qui possède les propriétés suivantes propriétés (iii) et (iv) sont des conséquences de (i) et (ii)) :

(i) Pour $z \in \mathbb{C}$, $\gamma \in \Gamma$, on a

$$\theta^{(12)}(z+\gamma) = \theta^{(12)}(z) \exp(H(\gamma, z) + H(\gamma, \gamma)/2) \quad ;$$

(ii) On a $\lim_{z \to 0} \theta^{(12)}(z)/z^{12} = g_2^3 - 27 g_3^2 \neq 0$;

(iii) Les zéros de $\theta^{(12)}$ sont les points de Γ chacun d'ordre 12 ;

(iv) On a $-d^2 \log \theta^{(12)}(z)/dz^2 = 12(4E_2 + P(z))$, où $E_2 \in \mathbb{Q}$.

Cf. Robert [3] et [4] §. 1. Les nombres E_{2k} , avec $k \geq 1$, sont $\neq 0$ si et seulement si $d \neq 1$ et $\neq 3$, ou $d = 1$ et $k \equiv 0 \bmod 2$, ou $d = 3$ et $k \equiv 0 \bmod 3$.

Soit p un nombre premier $\neq 2$, $\neq 3$ et $\neq d$. Soit $\mathfrak{P}$ un idéal premier de K au-dessus de (p) . Notons K' la plus grande extension abélienne de K de conducteur $\mathfrak{P}$. Soit $t \in \mathbb{C}$ un point de $\mathfrak{P}$-division du tore $\mathbb{C}/\Gamma$, c'est-à-dire un nombre complexe t tel que :

$$\mathfrak{P} = \{\alpha \in R \mid \alpha t \in \Gamma\} .$$

Les racines de l'unité de K' et les produits

$$\prod_{i=1}^{r} \theta^{(12)}(\alpha_i t)^{m_i}$$

- où $\alpha_1, \alpha_2, \ldots, \alpha_r \in R$ sont des éléments entiers de K premiers avec $6p$ et $m_1, m_2, \ldots, m_r \in \mathbb{Z}$ des entiers rationnels tels que

$$\sum_{i=1}^{r} m_i = 0 \qquad \text{et} \qquad \sum_{i=1}^{r} m_i N(\alpha_i) = 0$$

engendrent un sous-groupe Ω du groupe E de toutes les unités de K'. Le groupe Ω ne dépend pas du choix du point t de $\mathfrak{P}$-division et est invariant pour l'action de $\mathrm{Gal}(K'/K)$.

Nous déduisons de la formule de décomposition de la fonction zêta de K', extension abélienne de K, en produit de séries L (à l'aide d'une variante de la technique déjà développée par Ramachandra [2]) le résultat suivant (cf. Robert [3] et [4] th. 16, §. 6-5) :

THÉORÈME. - *L'indice de Ω dans E est fini, il est donné par la formule*

$$\frac{E}{\Omega} = 12^{(K':K)-1} h_{K'}$$

où $h_{K'}$ désigne le nombre de classes absolu du corps K'.

Ce théorème permet de ramener l'étude de la p-composante du groupe de classes absolu de K' à celle de la p-composante du groupe E/Ω. Donnons quelques résultats dans cette direction.

On sait que le groupe $G = \mathrm{Gal}(K'/K)$ est isomorphe au quotient du groupe $(R/\mathfrak{P})^*$ par le groupe des unités de K (dont l'ordre est e, avec $e = 2$ si

$d \neq 1$ et $\neq 3$, et $e = 4$ ou 6 suivant que $d = 1$ ou 3). Soit $F_p = \mathbb{Z}/p\mathbb{Z}$ le corps premier de caractéristique p ; l'algèbre de groupe $F_p(G)$ est semi-simple, et agit naturellement sur $\Lambda = E/\Omega E^p$. Pour tout caractère irréductible χ de $F_p(G)$ posons

$$1_\chi = \sum_{g \in G} \chi(g^{-1})\, g/(G:1) \ ;$$

les nombres 1_χ appartiennent à $F_p(G)$, et nous avons

$$\Lambda = \bigoplus_\chi \Lambda . 1_\chi \ .$$

Distinguons deux situations :

1) On a $\mathfrak{P} \neq \mathfrak{P}$, d'où $N(\mathfrak{P}) = p$; le corps $R/\mathfrak{P}$ est alors isomorphe à F_p.

Les caractères irréductibles qui interviennent dans la représentation de $F_p(G)$ sur Λ sont les caractères χ_k définis sur $R/\mathfrak{P}$ par

$$\alpha \longmapsto \alpha^{ek} \quad , \quad 2 \leq ek \leq p-3 \ .$$

Ces caractères apparaissent chacun avec la multiplicité 1 ou 0 ; posons $\Lambda_{ek} = \Lambda . 1_{\chi_k}$, nous avons le résultat suivant :

THÉORÈME. - Les nombres rationnels $E_2, E_4, \ldots, E_{p-3}$ sont p-entiers ; si $\Lambda_{ek} \neq (1)$, alors $p \mid E_{ek}$.

2) On a $\mathfrak{P} = (p)$, d'où $N(\mathfrak{P}) = p^2$; le corps F_p est alors isomorphe à l'ensemble des éléments α de $R/\mathfrak{P}$ tels que $\alpha = \alpha^p$.

Les caractères irréductibles qui interviennent dans la représentation

de $F_p(G)$ sur Λ sont d'une part les caractères χ_k définis par

$$\alpha \longmapsto \alpha^{k(p+1)} \quad , \quad 1 \leq k \leq p-2 \quad ;$$

d'autre part les caractères ψ_k définis par

$$\alpha \longmapsto \alpha^{ek} + \alpha^{ek'} \quad ,$$

avec $2 \leq ek < ek' \leq p^2 - 3$ et $ek \equiv pek' \mod p^2 - 1$.

Ces caractères apparaissent chacun avec la multiplicité 1 ou 0 ; posons $\Lambda_{k(p+1)} = \Lambda.1_{\chi_k}$ et $\Lambda_{ek} = \Lambda.1_{\psi_k}$; nous avons le résultat suivant :

THÉORÈME. - Les nombres rationnels $E_2, E_4, \ldots, E_{p-1}, pE_{p+1}, E_{p+3}, \ldots, E_{p^2-3}$ sont p-entiers. Si $\Lambda_{p+1} \neq (1)$ le nombre E_{p+1} est p-entier ; si $\Lambda_{k(p+1)} \neq (1)$ avec $2 \leq k \leq p-2$ alors $p | E_{k(p+1)}$; si $\Lambda_{ek} \neq (1)$ et ek n'est pas divisible par p+1 alors $p | E_{ek}$ et $p | E_{ek'}$.

Pour le corps $K = \mathbb{Q}\sqrt{-1}$ et la courbe d'équation

$$y^2 = 4x^3 - 4x \, .$$

Hurwitz [1] a calculé les nombres $4!E_4$, $8!E_8, \ldots$ jusqu'à $48!E_{48}$. Concernant le nombre premier 7 , non décomposé dans $\mathbb{Q}\sqrt{-1}$, il résulte de sa table que les nombres $E_4, 7E_8, E_{12}, \ldots, E_{44}$ sont 7-entiers comme le demande le théorème et qu'aucun d'entre eux n'est divisible par 7 ; par conséquent l'idéal (7) est régulier pour $\mathbb{Q}\sqrt{-1}$.

-:-:-:-

BIBLIOGRAPHIE

[1] A. HURWITZ. - Über die Entwicklungskoeffizienten der lemniscatischen Funktionen. Math. Ann., Bd 51 (1899) pp. 196-226.

[2] K. RAMACHANDRA. - Some applications of Kronecker's limit formulas. Ann. of Math., n° 80 (1964) pp. 104-148.

[3] G. ROBERT. - Unités elliptiques et formules pour le nombre de classes. C.R. Acad. Sc. Paris, t. 277 (17 déc. 1973) série A, p. 1143.

[4] G. ROBERT. - Unités elliptiques et formules pour le nombre de classes des extensions abéliennes d'un corps quadratique imaginaire. Bull. Soc. math. France, mémoire 36 (1974).

-:-:-:-

Gilles ROBERT
99, rue R. Losserand
75014 PARIS