

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

THONG NGUYEN-QUANG-DO

Unités de norme (-1) d'un corps quadratique réel

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 17, n° 2 (1975-1976), exp. n° G6, p. G1-G3

http://www.numdam.org/item?id=SDPP_1975-1976__17_2_A12_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1975-1976, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

UNITÉS DE NORME (-1) D'UN CORPS QUADRATIQUE RÉEL

par NGUYEN-QUANG-DO Thong

Introduction.

Etant donné $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel, d entier positif sans facteur carré, on sait, d'après le théorème de Dirichlet, que le groupe U_K des unités de K est isomorphe à $\{\pm 1\} \times \mathbb{Z}$. Les unités positives forment donc un groupe isomorphe à $\mathbb{Z}$, dont le générateur $\eta > 1$ est appelé unité fondamentale de K . D'autre part, pour qu'un entier ε de K soit une unité, il faut et il suffit que $N(\varepsilon) = \pm 1$, où N désigne la norme de K à $\mathbb{Q}$. Problème : Quand a-t-on $N(\eta) = -1$?

On se propose ici de fabriquer, par des moyens élémentaires, une suite exacte faisant intervenir le groupe $U_K^{(1)}$ des unités de K qui sont de norme 1, puis, par la seule considération de cette suite exacte, de trouver diverses conditions nécessaires et suffisantes pour que $N(\eta) = -1$.

1. Une suite exacte ...

Soit $\mathcal{K}$ le groupe des classes d'idéaux de K . Soit $\mathcal{K}_{\text{reg}}$ le sous-groupe des classes régulières, i. e. des classes qui contiennent un idéal invariant par $\text{Gal}(K/\mathbb{Q})$. Un idéal premier de K est dit ramifié s'il divise le discriminant de K .

Soit $\mathcal{R}$ le groupe dont les éléments sont des ensembles d'idéaux premiers ramifiés, et la loi de groupe est la différence symétrique des ensembles.

THÉORÈME 1.1. - Il existe une suite exacte de groupes :

$$(*) \quad U_K^{(1)} \xrightarrow{\varphi} \mathcal{R} \xrightarrow{\psi} \mathcal{K}_{\text{reg}} \rightarrow 1.$$

Preuve. - Soit σ le générateur de $\text{Gal}(K/\mathbb{Q})$.

Pour plus de clarté, rappelons d'abord la structure des idéaux de K invariants par σ . On sait que les nombres premiers p se décomposent de trois façons possibles en produits d'idéaux premiers de K :

(**) soit $(p) = \mathfrak{p}$ et $\sigma(\mathfrak{p}) = \mathfrak{p}$

soit $(p) = \mathfrak{p}\sigma(\mathfrak{p})$ et $\mathfrak{p} \neq \sigma(\mathfrak{p})$

soit $(p) = \mathfrak{p}^2$ et $\sigma(\mathfrak{p}) = \mathfrak{p}$

Les idéaux premiers tels que $(p) = \mathfrak{p}^2$ sont les idéaux premiers ramifiés. Si J est un idéal entier invariant par σ , et si un idéal premier $\mathfrak{p}$ divise J , $\sigma(\mathfrak{p})$

divise aussi J . Donc, en tenant compte de (**), J sera de la forme : $J = (m) \prod \mathfrak{p}_i$ avec $m \in \mathbb{Z}$, et $\prod \mathfrak{p}_i$ désigne un produit fini d'idéaux premiers ramifiés distincts.

(i) Construction de φ . - Pour tout $\varepsilon \in U_K^{(1)}$, on a, d'après le théorème 90 de Hilbert, $\varepsilon = x^{-1} \sigma(x)$, où $x \in K^*$ est défini modulo $\mathbb{Q}^*$, et peut être pris entier. L'idéal (x) est invariant par σ , et s'écrit donc $(x) = (m) \prod_{i=1}^n \mathfrak{p}_i$. Posons $\varphi(\varepsilon) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. Il est clair que $\varphi(\varepsilon)$ ne dépend que de ε (pas de x), et qu'on définit ainsi un homomorphisme de $U_K^{(1)}$ dans $\mathcal{R}$.

(ii) Construction de ψ . - A tout élément $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ de $\mathcal{R}$, on associe la classe de l'idéal $\mathfrak{p}_1 \dots \mathfrak{p}_n$. Il est clair qu'on définit ainsi un homomorphisme ψ de $\mathcal{R}$ dans $\mathcal{H}_{\text{reg}}$.

L'exactitude de la suite (*) est alors évidente.

C. Q. F. D.

THÉOREME 1.2. - Soit t le nombre d'idéaux premiers ramifiés de K . Alors l'ordre de $\mathcal{H}_{\text{reg}}$ est égal à 2^{t-1} (resp. 2^{t-2}) si $N(\eta) = -1$ (resp. $+1$).

Preuve. - Il suffit de calculer l'ordre de $\text{Ker } \psi = \text{Im } \varphi = U_K^{(1)} / \text{Ker } \varphi$. Si $\varepsilon \in U_K^{(1)}$ est de la forme $x^{-1} \sigma(x)$, x entier de K , alors $\varepsilon \in \text{Ker } \varphi$ si, et seulement si, $N(x) = \pm 1$, i. e. $\varepsilon = \pm x^{-2}$.

si $N(\eta) = 1$, alors $\text{Ker } \varphi = U_K^2$ (= les carrés de U_K) et $(U_K^{(1)} : \text{Ker } \varphi) = 4$.

si $N(\eta) = -1$, alors certainement $\text{Ker } \varphi \neq (U_K^{(1)})^2$, d'après ce qui précède. Or l'on a toujours $(U_K^{(1)})^2 \subset U_K^{(1)}$, avec $(U_K^{(1)} : (U_K^{(1)})^2) = 4$. Donc

$$(U_K^{(1)} : \text{Ker } \varphi) = 2.$$

C. Q. F. D.

2. ... et ses conséquences.

Nous allons donner sous forme de corollaires des conditions nécessaires et suffisantes pour que $N(\eta) = -1$.

D'abord un résultat classique qu'on démontre d'habitude par la théorie des genres [1].

COROLLAIRE 2.1. - Le nombre h des classes d'idéaux de K est divisible par 2^{t-2} . Il est divisible par 2^{t-1} si, et seulement si, $N(\eta) = -1$.

Cela résulte immédiatement de la détermination de l'ordre du groupe $\mathcal{H}_{\text{reg}}$. On a démontré du même coup la formule suivante [2] :

COROLLAIRE 2.2. - Soit t le nombre d'idéaux ramifiés, 2^r le nombre de classes régulières. Alors $N(\eta) = (-1)^{t-r}$.

Voici maintenant un vieux résultat de Legendre :

COROLLAIRE 3.3. - Soit $K = \mathbb{Q}(\sqrt{p})$, p nombre premier. Alors

$$N(\eta) = -1 \iff p \not\equiv 3 \pmod{4}.$$

Preuve. - Si $N(\eta) = -1$, la réduction de cette équation mod p entraîne immédiatement que $p \not\equiv 3 \pmod{4}$. Réciproquement, si $p \not\equiv 3 \pmod{4}$ et $K = \mathbb{Q}(\sqrt{p})$, le discriminant de K n'a qu'un seul facteur premier, i. e. $t = 1$. Donc l'ordre de $\mathcal{K}_{\text{reg}}$ est 2^{t-1} , et $N(\eta) = -1$.

C. Q. F. D.

Le résultat de Legendre n'est qu'un cas particulier du résultat suivant [3].

COROLLAIRE 3.4. - Supposons $d \not\equiv 3 \pmod{4}$, et considérons les idéaux $(m, \sqrt{d})$, engendrés par $\sqrt{d}$, et un diviseur m de d . Le nombre de ces idéaux qui sont principaux est égal à 2 (resp. 4) si $N(\eta) = -1$ (resp. $+1$).

Preuve. - Si $d \not\equiv 3 \pmod{4}$, les diviseurs premiers p_i du discriminant sont ceux de d , et l'on sait que l'idéal premier $\mathfrak{p}_i$ au-dessus d'un tel p_i est $(p_i, \sqrt{d})$. Donc si $m = p_1 \dots p_n$ est un diviseur de d , $(m, \sqrt{d}) = \mathfrak{p}_1 \dots \mathfrak{p}_n$, et le corollaire découle immédiatement de 1.1.

C. Q. F. D.

Remarquons que les idéaux $(1, \sqrt{d})$ et $(d, \sqrt{d})$ sont toujours principaux, car égaux respectivement à (1) et $(\sqrt{d})$.

BIBLIOGRAPHIE

- [1] BOREVITCH (Z. I.) et CHAFAREVITCH (I. R.) [BOREVIČ-ŠAFAREVIČ]. - Théorie des nombres. - Paris, Gauthier-Villars, 1967 (Monographies internationales de mathématiques modernes, 8).
- [2] DESPUJOLS (P.). - Norme de l'unité fondamentale du corps quadratique absolu, C. R. Acad. Sc. Paris, t. 221, 1945, p. 684-685.
- [3] TROTTER (H. F.). - On the norms of units in quadratic fields, Proc. Amer. math. Soc., t. 22, 1969, p. 198-201.

(Texte reçu le 24 novembre 1975)

NGUYEN-QUANG-DO Thong
21 avenue des Sablons
91350 GRIGNY