NICOLE MOSER

Unités et nombre de classes d'une extension diédrale de $\mathbb{Q}$

Astérisque, tome 24-25 (1975), p. 29-35

<http://www.numdam.org/item?id=AST_1975__24-25__29_0>

Société Mathématique de France
Astérisque 24-25 (1975)

UNITÉS ET NOMBRE DE CLASSES D'UNE EXTENSION DIÉDRALE DE $\mathbb{Q}$

par

Nicole MOSER

-:-:-:-

Nous nous proposons d'étudier la structure du groupe des unités d'une extension diédrale de $\mathbb{Q}$, en tant que module sur l'algèbre du groupe de Galois, et d'en tirer quelques conséquences sur le nombre de classes.

Soit $K/\mathbb{Q}$ une extension galoisienne finie, dont on note U_K le groupe des unités, et V_K le sous-groupe des unités de torsion. Posons $E_K = U_K/V_K$, et $G = \mathrm{Gal}(K/\mathbb{Q})$.

DÉFINITION. - Une unité ε de K est dite unité de Minkowski si de l'ensemble $\{\varepsilon^s\}_{s \in G}$, on peut extraire un système d'unités fondamentales.

Il est clair que lorsque K est une extension galoisienne totalement réelle de $\mathbb{Q}$, il y a équivalence entre les deux propositions suivantes :

α) il existe dans K une unité de Minkowski ;

β) E_K est $\mathbb{Z}[G]$-monogène.

Supposons maintenant que K soit une extension galoisienne totalement réelle de $\mathbb{Q}$, de degré n. Le théorème de Dirichlet sur les unités montre que E_K est un $\mathbb{Z}$-module libre de rang $n-1$. Posons $T = \sum_{s \in G} s$; c'est un élément de l'annulateur de E_K dans $\mathbb{Z}[G]$. On vérifie aisément que pour que E_K soit $\mathbb{Z}[G]$-monogène, il faut et il suffit qu'il soit $\mathbb{Z}[G]$-isomorphe au module $R = \mathbb{Z}[G] / T\,\mathbb{Z}[G]$.

PROPOSITION 1. - <u>Pour tout sous-groupe</u> γ <u>de</u> G, <u>posons</u> $T_\gamma = \sum_{s \in \gamma} s$, <u>et notons</u> R^γ <u>l'ensemble des éléments de</u> R <u>invariants par</u> γ. <u>Alors</u>

$$R^\gamma = T_\gamma R .$$

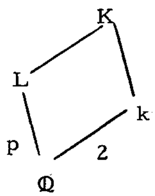
COROLLAIRE. - <u>Soit</u> K <u>une extension galoisienne totalement réelle de</u> $\mathbb{Q}$, <u>admettant une unité de Minkowski. Quelle que soit la sous extension</u> K' <u>de</u> K,

$$N_{K/K'}\, E_K = E_{K'} .$$

<u>Si de plus</u> K' <u>est galoisienne sur</u> $\mathbb{Q}$, <u>elle admet une unité de Minkowski, qui est norme sur</u> K' <u>de l'unité de Minkowski de</u> K.

ÉTUDE DU CAS DIÉDRAL TOTALEMENT RÉEL

Notations :



Le groupe de Galois G est engendré par deux générateurs, σ et τ, liés par les relations $\sigma^p = \tau^2 = 1$ et $\sigma\tau = \tau\sigma^{-1}$ La lettre L désigne le sous-corps fixe par τ, et k est le sous corps fixe par σ. De plus, nous noterons :

$\mathbb{Q}^{(p)} = \mathbb{Q}(\zeta)$ le $p^{\text{ième}}$ corps cyclotomique,

A l'anneau des entiers de $\mathbb{Q}^{(p)}$,

A_o l'anneau des entiers du sous-corps réel maximal de $\mathbb{Q}^{(p)}$.

On munit A d'une structure de $\mathbb{Z}[G]$-module en définissant l'action de σ comme la multiplication par ζ, et celle de τ comme la conjugaison complexe. M. P. Lee utilise cette structure pour donner dans [7] la classification des représentations intégrales du groupe dièdral. Ses résultats montrent que E_K est isomorphe à une, et à une seule, des sommes directes suivantes :

α) $\mathfrak{A}_1 A \oplus \mathfrak{A}_2 A \oplus S$

β) $(1-\zeta)\,\mathfrak{A}_1 A \oplus \mathfrak{A}_2 A \oplus S$

γ) $(1-\zeta)\,\mathfrak{A}_1 A \oplus (1-\zeta)\,\mathfrak{A}_2 A \oplus S$

δ) $\mathfrak{A}_1 A \oplus (\mathfrak{A}_2 A\,,\, S)$

ε) $(1-\zeta)\,\mathfrak{A}_1 A \oplus (\mathfrak{A}_2 A, S)$,

où les $\mathfrak{A}_i$ sont des idéaux de A_o, où S est le $\mathbb{Z}[G]$-module $\mathbb{Z}$, sur lequel σ agit trivialement, et τ agit comme la multiplication par -1, et où $(\mathfrak{A}_2 A\,,\, S)$ est une extension non triviale de S par $\mathfrak{A}_2 A$.

THÉORÈME 2. - Les cinq cas ci-dessus sont caractérisés par les valeurs des indices $a = (E_K : E_L E_L^{\sigma} E_k)$ et $b = (E_k : N_{K/k} E_k)$

α) $a = 1$ $b = p$

β) $a = p$ $b = p$

γ) $a = p^2$ $b = p$

δ) $a = p$ $b = 1$

ε) $a = p^2$ $b = 1$.

Remarque 1 : Dans tous les cas, $E_L = N_{K/L} E_K$.

Remarque 2 : On vérifie que le $\mathbb{Z}[G]$-module R est du type δ) .

COROLLAIRE. - Pour qu'une extension dièdrale totalement réelle admette une unité de Minkowski, il faut que $a = p$ et $b = 1$. Si de plus A_o est principal, cette condition est suffisante.

Etude du nombre de classes

Dans [8], J. Martinet étudie la décomposition d'un nombre premier p dans une extension dièdrale, ce qui permet de comparer les fonctions "zêta" des corps K , L , k et $\mathbb{Q}$. Grâce à la formule analytique du nombre de classes, on obtient la relation entre nombres de classes h et régulateurs R :

$$h_K = h_L^2 \; h_k \times \frac{R_k R_L^2}{R_K} \quad .$$

Un calcul direct sur les régulateurs permet d'énoncer alors :

PROPOSITION 3. - $h_K = a \dfrac{h_L^2 \, h_k}{p^2}$, <u>où</u> a <u>est l'indice</u> $(E_K : E_L E_{L^\sigma} E_k)$.

<u>Exemples, dans le cas</u> p = 3

D'après la proposition 3, pour que $a = 9$, il suffit que h_L et h_k soient premiers à 3 .

1) Prenons pour L le corps cubique de discriminant 1076 ; alors $k = \mathbb{Q}(\sqrt{269})$, et les tables de [2] donnent $h_L = h_k = 1$. Dans K/k , il existe un seul idéal ramifié. D'après un résultat de Kuroda, [6], si K est une extension cyclique de degré premier impair d'un corps de nombres k , ramifiée en une place finie au plus, $U_k = N_{K/k} U_K$. Donc b = 1 , et cet exemple illustre le cas ε) .

2) Si L est le corps cubique de discriminant 756, $k = \mathbb{Q}(\sqrt{21})$, et on vérifie encore que L et k sont principaux. Donc a = 9 , et $h_K = 1$. Comme il existe deux idéaux ramifiés dans K/k , la formule des classes ambiges [3] permet de conclure que b = 3 . C'est le cas γ) .

3) Considérons enfin le corps L de discriminant 229 ; $h_L = 1$, $k = \mathbb{Q}(\sqrt{229})$, $h_k = 3$ Il n'existe pas d'idéaux ramifiés dans K/k Kisilevsky énonce dans [5] le résultat suivant : si k est un corps de nombres, dont le p-groupe des classes est cyclique d'ordre p , la p-tour de classes de k est de longueur 1 . Donc la proposition 3 donne a = 3 , b vaut 1 d'après [6], et K est de type δ).

CAS DIÉDRAL IMAGINAIRE

PROPOSITION 4. - Soit $K/\mathbb{Q}$ une extension dièdrale imaginaire. Il y a deux structures de $\mathbb{Z}[G]$-modules possibles pour E_K, caractérisées par

$$\alpha)\quad a = 1 \qquad\qquad \beta)\quad a = 3 .$$

PROPOSITION 5. - Si A_o est principal, K admet une unité de Minkowski.

Remarque : Dans les deux cas, $N_{K/L}\, E_K = E_L$.

PROPOSITION 6. - $$h_K = a\,\frac{h_L^2\, h_k}{p} .$$

Cette dernière formule se trouve pour $p = 3$ dans les articles de Barrucand et Cohn [1] , et de Ishida [4]. Dans [1], des exemples sont donnés où $a = 1$ et $a = 3$.

-:-:-:-

BIBLIOGRAPHIE

[1] BARRUCAND and COHN. - Remarks on principal factors in a relative cubic field. J. Number theory t. 3, 1971, p. 226-239.

[2] BOREVIČ and SCHAFAREVIČ. - Number theory. Academic press 1966 .

[3] CHEVALLEY. - Sur la théorie du corps de classes dans les corps finis et les corps locaux. Fac. Sc. Tokyo, Sect. 1, t. 21, 1933.

[4] ISHIDA. - Fundamental units of certain algebraic number fields. Abh. math. Semin. Univ. Hamburg, t. 39, 1973.

[5] KISILEVSKY. - Some results related to Hilbert's theorem 94 . J. of Number theory, t. 2, 1970.

[6] KURODA. - Über die Klassenzahl eines relativzyklischen Zahlkörpers von Prinmzahlgrade. Proc. Japan Acad. t. 40, 1964.

[7] LEE M. -P. - Integral representations of dihedral groups of order 2p . Trans. Amer. Math. Soc. t. 110, 1964.

[8] MARTINET J. - Sur l'arithmétique des extensions galoisiennes à groupe de Galois dièdral d'ordre 2p . Ann. Inst. Fourier, tome XIX, 1969

-:-:-:-

Nicole MOSER
Université Scientifique et
Médicale de Grenoble
Institut de Mathématiques
Pures
Boîte Postale 116
38402 SAINT MARTIN
D'HÈRES