Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Jacques Payan

Sur les unités de Minkowski

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 15, n° 1 (1973-1974), exp. n° 19, p. 1-6

<http://www.numdam.org/item?id=SDPP_1973-1974__15_1_A15_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
15e année, 1973/74, n° 19, 6 p.

22 avril 1974

SUR LES UNITÉS DE MINKOWSKI

par Jean-Jacques PAYAN

Parmi les invariants d'un corps de nombres K, l'un des plus intéressants à étudier, et des plus difficiles à calculer, est le nombre de ses classes d'idéaux. On sait qu'il dépend de façon très étroite de la structure du groupe des unités et de la décomposition dans K des idéaux premiers de $\underset{\sim}{Z}$. C'est ce qu'exprime la formule

$$\lim_{s \to 1} (s-1)^t \zeta_K(s) = \frac{2^{s_K+t_K} \pi^{t_K} R_K h_K}{\omega_K \sqrt{|D_K|}}$$

(cf. [3]) liant le résidu en 1 de la fonction zêta associée à K, le discriminant D_K, le régulateur R_K, le nombre ω_K de racines de l'unité contenues dans K et le nombre de classes h_K de K.

On va s'intéresser ici à la structure du groupe des unités d'une extension galoisienne finie K de $\underset{\sim}{Q}$ comme module sur l'algèbre du groupe $G = \mathrm{Gal}\, K/\underset{\sim}{Q}$, et donner un aperçu des résultats obtenus par N. MOSER [15] dans le cas diédral, résultats qui seront exposés aux "Journées arithmétiques de Bordeaux [mai-juin 1974].

Notons U_K le groupe des unités de K, T_K le sous-groupe des racines de l'unité de K, posons $E_K = U_K/T_K$, et désignons par s_K (resp. $2t_K$) le nombre de plongements réels (resp. complexes) de K. Rappelons les deux résultats classiques suivants :

THÉORÈME (DIRICHLET). - *E_K est un $\underset{\sim}{Z}$-module libre de rang $s_K + t_K - 1$.*

Le théorème de Dirichlet s'énonce encore en disant qu'il existe $s_K + t_K - 1$ unités, $\eta_1, \ldots, \eta_{s_K+t_K-1}$, dites unités fondamentales, telles que toute unité ε de K s'écrit de manière unique $\varepsilon = \varepsilon_0 \prod_{i=1}^{s_K+t_K-1} \eta_i^{n_i}$ avec les n_i dans $\underset{\sim}{Z}$ et ε_0 dans T_K.

THÉORÈME (MINKOWSKI). - *Soit K une extension galoisienne finie de $\underset{\sim}{Q}$, il existe une unité de K qui engendre avec ses conjuguées un sous-groupe d'indice fini de U_K.*

Définition. - Une unité η de K, extension galoisienne finie de $\underset{\sim}{Q}$, sera dite de Minkowski si η forme, avec certaines de ses conjuguées, un système d'unités fondamentales de K.

Remarque 1 [15]. - Si $K/\underset{\sim}{Q}$ admet une unité de Minkowski, alors le $\underset{\sim}{Z}[G]$-module E_K est monogène. Réciproquement, si E_K est $\underset{\sim}{Z}[G]$-monogène et K/Q réelle, alors il existe une unité de Minkowski.

1. Unités de Minkowski et modules sur certains anneaux de Dedekind.

Le premier résultat substantiel sur l'existence d'unités de Minkowski a été obtenu grâce à des méthodes géométriques par H. HASSE [8] dans le cas des extensions cycliques de degré 3 . Il a été généralisé par B. A. ZEILANOV [16] qui a démontré le résultat suivant.

THÉORÈME. - Si K/Q est cyclique de degré premier p , et si le corps cyclotomique d'indice p est principal, alors K admet une unité de Minkowski.

C'est à A. BRUMER [5] qu'est dû le résultat le plus complet concernant les extensions cycliques de degré premier. Soient K/Q cyclique de degré premier p , et U_K^+ le groupe des unités de K de norme $+1$, il est évidemment $\underset{\sim}{Z}[G]$-isomorphe à E_K . Soit H_K le sous-groupe de U_K^+ formé des unités cyclotomiques de K , on sait d'une part que $[U_K^+ : H_K] = h_K$, de l'autre que H_K est $\underset{\sim}{Z}[G]$-monogène. Comme H_K et U_K^+ sont annulés par la norme $1 + \sigma + \sigma^2 + \ldots + \sigma^{p-1}$, où σ désigne un générateur de G , on les munit d'une structure de $\underset{\sim}{Z}[G]/(1 + \sigma + \ldots + \sigma^{p-1})$-module. Comme $\underset{\sim}{Z}[G]/(1 + \sigma + \ldots + \sigma^{p-1})$ est isomorphe à l'anneau A des entiers du corps cyclotomique d'indice p , on voit facilement que H est A-isomorphe à A . Cet isomorphisme se prolonge à U_K^+ dont l'image est alors un idéal fractionnaire $\mathfrak{a}^{-1}$ inverse d'un idéal entier $\mathfrak{a}$ de A . On vérifie facilement que $[U_K^+ : H_K] = N\mathfrak{a}$, et que l'existence d'une unité de Minkowski équivaut à $\mathfrak{a}$ est principal. D'où le théorème ci-dessous.

THÉORÈME (BRUMER). - Soit K une extension cyclique de degré premier p de $\underset{\sim}{Q}$; le nombre h_K de ses classes d'idéaux est norme d'un idéal entier du corps $\underset{\sim}{Q}^{(p)}$ des racines p-ièmes de l'unité. Pour que K admette une unité de Minkowski, il faut que l'un au moins des idéaux entiers de $\underset{\sim}{Q}^{(p)}$ de norme h_K soit principal, et il suffit que tous soient principaux.

En utilisant des méthodes analogues, on démontre le résultat suivant.

THÉORÈME [4]. - Soit K une extension cyclique réelle de degré 4 , 8 ou 9 de $\underset{\sim}{Q}$. Pour qu'il existe une unité de Minkowski, il faut et il suffit que, pour toute extension intermédiaire L , on ait $N_{K/L} E_K = E_L$.

Énonçons enfin une dernière propriété qui met en évidence le rôle joué par les applications-normes.

PROPRIÉTÉ [15]. - Soit K une extension galoisienne totalement réelle de $\underset{\sim}{Q}$; si K possède une unité de Minkowski η , alors, pour toute extension intermédiaire L , on a $N_{K/L} E_K = E_L$. Si, de plus, $1/\underset{\sim}{Q}$ est galoisienne, $N_{K/L}\,\eta$ est unité de Minkowski de L .

2. Structure du groupe des unités d'une extension diédrale de $\mathbb{Q}$.

Soit K une extension galoisienne de $\mathbb{Q}$ de degré $2p$, p premier impair, de groupe de Galois G défini par les générateurs σ, τ, liés par $\sigma^p = \tau^2 = 1$ et $\tau\sigma\tau^{-1} = \sigma^{-1}$. Notons L (resp. k) l'extension intermédiaire de $K/\mathbb{Q}$ invariante par τ (resp. σ).

On utilise les résultats de M. P. LEE [13] sur la classification des $\mathbb{Z}[G]$-modules de type fini, sous $\mathbb{Z}$-torsion, en les appliquant à E_K dont le $\mathbb{Z}$-rang est donné par le théorème de Dirichlet. On note A (resp. A_0) l'anneau des entiers du corps cyclotomique $\mathbb{Q}^{(p)}$ d'indice p (resp. du sous-corps réel maximal de $\mathbb{Q}^{(p)}$) et ζ une racine primitive p-ième de l'unité.

2.1. Le cas imaginaire.

THÉORÈME 2.1 (N. MOSER [15]). - *Soit K une extension diédrale imaginaire de $\mathbb{Q}$, alors E_K est $\mathbb{Z}[G]$-isomorphe à un idéal de A sur lequel σ agit comme la multiplication par ζ, et τ comme la conjugaison complexe. Cet idéal est soit de la forme $\mathfrak{a}A$ (type α), soit de la forme $(\zeta - \zeta^{-1})\mathfrak{a}A$ (type β), où $\mathfrak{a}$ est un idéal de A_0. Suivant que $E_K = E_L E_L^{\sigma}$ (resp. $[E_K : E_L E_L^{\sigma}] = p$), on se trouve dans le cas α (resp. β).*

Il est clair que E_K est $\mathbb{Z}[G]$-monogène si, et seulement si, $\mathfrak{a}$ est principal. D'autre part, on peut calculer dans ce cas particulier l'annulateur d'un générateur de E_K, et montrer que la remarque 1 se généralise, c'est-à-dire que l'existence d'une unité de Minkowski équivaut à E_K est $\mathbb{Z}[G]$-monogène, ce qui conduit à l'énoncé suivant.

COROLLAIRE [15]. - *Soit $K/\mathbb{Q}$ une extension diédrale imaginaire de degré $2p$, avec A_0 principal, alors K admet une unité de Minkowski.*

Remarque 2. - On connait des valeurs de p pour lesquelles A_0 n'est pas principal, c'est notamment le cas de $p = 257$.

Remarque 3. - Le théorème 2.1 est en fait un résultat sur les $\mathbb{Z}[G]$-modules établissant un isomorphisme entre E_K et un idéal de A ambige relativement à A_0. Dans cet isomorphisme, E_c s'identifie au sous-module invariant par τ, c'est ce qui conduit à la classification suivant l'indice $[E_K : E_L E_{L^{\sigma}}]$.

Un examen plus détaillé de ces $\mathbb{Z}[G]$-modules permet d'énoncer la propriété suivante.

PROPRIÉTÉ 2.2 [15]. - *Soit $K/\mathbb{Q}$ une extension diédrale imaginaire, alors*

$$N_{K/L}\, U_K^+ = U_L^+ .$$

2.2. Le cas réel.

Les résultats de M. P. LEE montrent que E_K est $\mathbb{Z}[G]$-isomorphe à une, et à une

seule, des sommes directes suivantes :

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

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

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

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

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

où les $\mathfrak{a}_i$ sont des idéaux entiers de A_0 , où S est isomorphe à $\underset{\sim}{Z}$ avec action triviale de σ et action de τ , définie par passage à l'opposé, et où $(\mathfrak{a}_2 A , S)$ est une extension de $\mathfrak{a}_2 A$ par S qu'il serait trop long de décrire.

On peut énoncer le théorème suivant.

THÉORÈME 2.3 [15]. - La distinction entre les cas (a), (b), (c), (d) et (e) s'opère grâce aux indices

$$[E_K : E_L E_{L\sigma} E_k] = a \quad \text{et} \quad [E_k : N_{K/h} E_K] = b$$

comme suit :

cas (α) $a = 1$ et $b = p$,

cas (β) $a = p$ et $b = p$,

cas (γ) $a = p^L$ et $b = p$,

cas (δ) $a = p$ et $b = 1$,

cas (ε) $a = p^2$ et $b = 1$.

$\underset{\sim}{Z}[G]/N\underset{\sim}{Z}[G]$, où $N = \sum_{x \in G} x$, appartient au type S .

On en déduit le corollaire suivant.

COROLLAIRE. - Soit K/Q une extension diédrale réelle, pour qu'il existe une unité de Minkowski, il faut que

$$[E_K : E_L E_{L\sigma} E_k] = p \quad \text{et} \quad E_k = N_{K/k} E_K .$$

Si, de plus, A_0 est principal, ces conditions sont suffisantes.

De la même façon que dans le cas imaginaire, on établit la propriété suivante.

PROPRIÉTÉ 2.4 [15]. - Soit K/Q une extension diédrale réelle, alors $N_{K/L} E_K = E_L$.

3. Nombre de classe et exemples.

H. HASSE a donné, dans [9], la formule suivante :

$$h_K = \frac{1}{2^x} a\, h_{k_1} h_{k_2} h_{k_3}$$

liant le nombre de classes h_K d'un corps biquadratique K , à groupe de Galois

isomorphe, au groupe de Klein, ceux de ses sous-corps quadratiques k_1 , k_2 , k_3 et l'indice $a = [U_K : U_{k_1} U_{k_2} U_{k_3}]$. Formule où x vaut 1 ou 2 suivant que K est imaginaire ou réel. N. MOSER a démontré, grâce à un calcul de régulateur, à la comparaison des fonctions zéta et des discriminants des différents corps qui interviennent, une formule analogue dans le cas diédral.

THÉORÈME 3.1 [15]. - Soit $K/\underset{\sim}{Q}$ une extension diédrale de degré $2p$, on pose

$$a = [E_K : E_L E_{L^\sigma}] \text{ si } K \text{ est imaginaire,}$$

$$a = [E_K : E_L E_{L^\sigma} E_k] \text{ si } K \text{ est réel.}$$

Alors $h_K = (a\, h_L^2\, h_k)/p$ (resp. $h_K = (a\, h_L^2\, h_k)/p^2$) si K est imaginaire (resp. réel).

Cet énoncé était connu de H. HASSE et C. MEYER [14] dans le cas $L = \underset{\sim}{Q}(\sqrt[3]{m})$ avec $m \in \underset{\sim}{Z}$, et de K. ISHIDA [10] dans le cas $p = 3$, K imaginaire.

Pour obtenir des exemples, et illustrer les classifications données en 2.2, N. MOSER utilise les résultats de la théorie du corps de classes, et ses conséquences, en particulier celles qui tournent autour de la formule des classes ambiges.

THÉORÈME A [6]. - Soient K une extension cyclique de degré p , premier impair d'un corps de nombres k , $h_{k,p}$ la p-participation au nombre de classes de k , et t le nombre d'idéaux premiers de k ramifiés dans K , alors le p-groupe des classes ambiges est d'ordre $h_{k,p}(p^{t-1}/[U_k : (U_k \cap N_{K/h} K)])$.

THÉORÈME B [12]. - Soit K une extension cyclique de degré premier impair d'un corps de nombres k , ramifiée en une place finie au plus, alors $U_k = N_{K/k} U_K$.

THÉORÈME C [11]. - Si k est un corps de nombres, dont le p-groupe des classes est cyclique d'ordre p , la p-tour des corps de classes de k est de longueur 1. Donc si K est le p-corps de classes de k , p ne divise pas h_K .

Les corps $K = \underset{\sim}{Q}(j , \sqrt[3]{m})$, où m est un entier rationnel sans facteur cubique, illustrent les deux types de $\underset{\sim}{Z}[G]$-modules E_K du cas imaginaire. Pour que $a = 3$, il suffit, d'après le théorème 3.1, que $(h_L , 3) = (h_k , 3) = 1$. C'est le cas lorsque $m = 2 , 3 , 5 , 6$ (voir les tables de [3]). Des exemples où $a = 1$ sont donnés par P. BARRUCAND et H. COHN [1], c'est le cas pour $m = 7 , 13 , 19$.

Dans le cas réel, il est moins facile de séparer les cas, le tableau ci-dessous donne quelques exemples :

Polynôme définissant L	$\Delta_{L/Q}$	$\Delta_{h/Q}$	h_k	h_L	nombre d'idéaux ramifiés dans K/h	a	b	Type de E_K	Nature de la justification
X^3-X^2-3X+1	$2^2.37$	37	1	1	1	9	1	ε	Th. B + Th. 3.1
X^3+4X-1	229	229	3	1	0	3	1	δ	Th. C + Th. 3.1
X^3-6X+2	$9^2.21$	21	1	1	2	9	3	γ	Th. A + Th. 3.1
$X^3-11X+2$	$2^2.326$	326	3	1	1	3	1	δ	Th. B + Th. 3.1

Les tables utilisées sont celles de [2] et [7].

BIBLIOGRAPHIE

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

[2] BILLEVIČ (K. K.). - Sur les unités d'un corps algébrique de degré 3 ou 4 [en russe], Mat. Sbornik, N. S. t. 40, 1956, n° 1, p. 123-136.

[3] BOREVIČ (Z. I.) and SCHAFAREVIČ (I. R.). - Number theory. - New York and London, Academic Press, 1966 (Pure and applied Mathematics. Academic Press, 20).

[4] BOUVIER (L.) et PAYAN (J.-J.). - Modules sur certains anneaux de Dedekind. Application à la structure du groupe des classes et à l'existence d'unités de Minkowski, J. für reine und angew. Math. (à paraître).

[5] BRUMER (A.). - On the groups of units of an absolutely cyclic number field of prime degree, J. Math. Soc. Japan, t. 21, 1969, p. 357-358.

[6] CHEVALLEY (C.). - Sur la théorie du corps de classes dans les corps finis et les corps locaux, Fac. of Sc. Tokyo, Sect. I, t. 21, 1933, p. 365-476.

[7] GRAS (G. et M.-N.). - Nombre de classes des corps $Q(\sqrt{m})$, Univ. Grenoble, 1972.

[8] HASSE (H.). - Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, Abh. Deutsch. Akad. Wiss. Berlin, 1948, n° 2.

[9] HASSE (H.). - Über die Klassenzahl abelscher Zahlkörper. - Berlin, Akademie-Verlag, 1952 (Mathematische Lehrbücher und Monographien. Abteilung, 2).

[10] ISHIDA (M.). - Fundamentals units of certain algebraic number fields, Abh. math. Semin. Univ. Hamburg, t. 39, 1973, p. 245-250.

[11] KISILEVSKY (H.). - Some results related to Hilbert's theorem 94, J. of Number theory, t. 2, 1970, p. 199-206.

[12] KURODA (S. N.). - Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrade, Proc. Japan Academy, t. 40, 1964, p. 623-626.

[13] LEE (M. P.). - Integral representations of dihedral groups of order 2p , Trans. Amer. math. Soc., t. 110, 1964, p. 213-231.

[14] MEYER (C.). - Die Berechnung der Klassenzahl abelscher Zahlkörper über quadratischen Zahlkörpern. - Berlin, Akad. Verlag, 1957 (Mathematische Lehrbücher und Monographien.2. Abteilung, Mathematische Monographien, 5).

[15] MOSER (N.). - Sur les unités de Minkoxski des extensions diédrales, Séminaire de Théorie des Nombres, Grenoble, 1973/74.

[16] ZEILANOV (B. A.). - Sur les unités d'un corps réel cyclique [en russe], Sb. Nauč. Soobšč. Dagestanskij Univ. Lenina, 1965/66, p. 21-23.

(Texte reçu le 25 avril 1974)

Jean-Jacques PAYAN
Institut de Mathématiques pures
Laboratoire associé au C. N. R. S.
Boîte postale 116
38402 SAINT MARTIN D'HÈRES