

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

DANIÈLE LAMBOT DE FOUGÈRES

**Bases d'entiers des corps de nombres. Discriminants. Cas des
corps quadratiques et cyclotomiques premiers**

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, n° 2 (1967-1968),
exp. n° G3, p. G1-G5

[<http://www.numdam.org/item?id=SDPP_1967-1968__9_2_A10_0>](http://www.numdam.org/item?id=SDPP_1967-1968__9_2_A10_0)

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1967-1968, 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/>

BASES D'ENTRIERS DES CORPS DE NOMBRES. DISCRIMINANTS.
CAS DES CORPS QUADRATIQUES ET CYCLOTOMIQUES PREMIERS

par Danièle LAMBOT de FOUGÈRES

1. Quelques préliminaires ([2], p. 26 à 53).

Notations : Soient A un anneau intègre, k son corps de fraction (de caractéristique 0),

K une extension algébrique de k de degré n ,

C un corps algébriquement clos contenant K ,

B la clôture intégrale de A dans K .

Si A est intégralement clos, alors, $\forall x \in B$,

$$(1) \quad \begin{cases} N_{K|k}(x) \in A, \\ \text{Tr}_{K|k}(x) \in A. \end{cases}$$

On pose : Discriminant de $(x_1, x_2, \dots, x_n) \in K^n = D(x_1, x_2, \dots, x_n)$,

$$(2) \quad D(x_1, x_2, x_3, \dots, x_n) = \det[\text{Tr}_{K|k}(x_i, x_j)] .$$

Propriétés du discriminant.

Si $y_i = \sum a_{ij} x_j$, $a_{ij} \in k$, $i = 1, 2, \dots, n$. Alors,

$$(3) \quad D(y_1, y_2, \dots, y_n) = [\det(a_{ij})]^2 D(x_1, x_2, \dots, x_n) .$$

Si $\delta_1, \delta_2, \dots, \delta_n$ sont les n k -isomorphismes de K dans C , et $x_1, x_2, \dots, x_n$ une base de K sur k , alors

$$(4) \quad D(x_1, x_2, \dots, x_n) = [\det \delta_i(x_j)]^2 \neq 0 .$$

2. Existence des bases d'entiers ([2], p. 26 à 53).

LEMME 1. - Soient A un anneau principal, M un A -module libre de rang fini n , et M' un sous- A -module de M ; alors M' est libre de rang $\leq n$.

LEMME 2. - Soient A un anneau int gralement clos, k son corps de fraction, de caract ristique 0 , K une extension de degr  fini de k , et B la fermeture int grale de A dans K ; alors B est un sous- A -module libre de rang n .

TH OREME. - Si K est un corps de nombre tel que $[K : \mathbb{Q}] = n$, B la fermeture int grale de $\mathbb{Z}$ dans K , B est un $\mathbb{Z}$ -module libre de rang n , et il existe des bases de B qui sont en m me temps des bases de K sur $\mathbb{Q}$.

Remarque. - Si $(x_1, \dots, x_n)$ et $(y_1, \dots, y_n)$ sont deux bases d'entiers de K , $\det(a_{ij}) \in \mathbb{Z}$, et la matrice des (a_{ij}) est inversible dans $\mathbb{Z}$, donc

$$(\det(a_{ij}))^2 = 1,$$

donc

$$D(x_1, \dots, x_n) = D(y_1, \dots, y_n).$$

D finition. - On appelle discriminant d'un corps de nombres, le discriminant d'une base d'entiers.

3. Base d'entiers et discriminant des corps quadratiques.

D finition. - On appelle corps quadratique, toute extension de degr  2 de $\mathbb{Q}$.

TH OREME. - Tout corps quadratique est de la forme $K = \mathbb{Q}(\sqrt{d})$, o  $d \in \mathbb{Z}$ et ne contient pas de facteurs carr s :

Si $d > 0$, K est un corps quadratique r el.

Si $d < 0$, K est un corps quadratique imaginaire.

D termination d'une base d'entiers. - Soit $\alpha + \beta \sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $\alpha, \beta \in \mathbb{Q}$; on cherchera des conditions n cessaires portant sur $\alpha = \frac{a}{c}$, $\beta = \frac{b}{c}$, pour que

$$\frac{a + b\sqrt{d}}{c} \in B, \quad \text{avec } a, b \text{ et } c \in \mathbb{Z}.$$

On peut supposer (a, b, c)  trangers, et on montre que, sous cette hypoth se, et avec d sans facteur carr , les trois nombres (a, b, c) sont  trangers deux   deux.

Ceci conduit   prendre $c = 1$ ou $c = 2$:

Pour $c = 1$, on obtient des  l ments de la forme $a + b\sqrt{d}$, $a, b \in \mathbb{Z}$.

Pour $c = 2$, $\begin{cases} \text{si } d \equiv 2, 3 \pmod{4}, \text{ on n'obtient pas d' l ments entiers,} \\ \text{si } d \equiv 1 \pmod{4}, \text{ on obtient des  l ments de la forme} \end{cases}$

$$a + b\sqrt{d}, \quad a, b \text{ étant des demi-impairs}.$$

On montre ensuite simplement le résultat suivant.

PROPOSITION.

Si $d \equiv 2, 3 \pmod{4}$, une base d'entiers de $\mathbb{Q}(\sqrt{d})$ est $(1, \sqrt{d})$.

Si $d \equiv 1 \pmod{4}$, une base d'entiers de $\mathbb{Q}(\sqrt{d})$ est $(1, \frac{1+\sqrt{d}}{2})$.

Discriminant de $\mathbb{Q}(\sqrt{d})$. - En utilisant la formule (2), il vient :

$$\text{si } d \equiv 2, 3 \pmod{4}, \quad D = 4d,$$

$$\text{si } d \equiv 1 \pmod{4}, \quad D = d.$$

4. Base d'entiers et discriminant des corps cyclotomiques premiers.

Définition. - On appelle corps cyclotomique, tout corps de nombre engendré sur $\mathbb{Q}$ par des racines de l'unité.

Un corps cyclotomique sera dit premier s'il est engendré par une racine primitive p -ième de l'unité, p étant un nombre premier impair.

PROPRIÉTÉ. - $K = \mathbb{Q}(\xi)$, $\xi^p = 1$.

En utilisant le critère d'Eisenstein, on montre que

$$P(\xi) = \xi^{p-1} + \xi^{p-2} + \dots + 1$$

est irréductible sur $\mathbb{Q}$ ([3], p. 86-87).

Critère d'Eisenstein. - Soient A un anneau principal, p un élément premier de A , et

$$F(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in A[X]$$

tel que $p \mid a_i$ pour $i = 0, 1, \dots, n-1$, et tel que $p^2 \nmid a_0$, alors $F(X)$ est irréductible sur k (corps des fractions de A).

Ceci montre que $[\mathbb{Q}(\xi) : \mathbb{Q}] = p - 1$.

THÉOREME. - Une base d'entiers de $\mathbb{Q}(\xi)$ est $(1, \xi, \dots, \xi^{p-2})$.

LEMME 1. - Si B est l'anneau des entiers de K sur $\mathbb{Z}$, alors

$$B(1 - \xi) \cap \mathbb{Z} = p\mathbb{Z}.$$

En effet, on a, de manière évidente,

$$\begin{aligned} \text{Tr}(\xi) &= -1, \\ \text{Tr}(1) &= p-1, \\ \text{Tr}(\xi^j) &= -1, \quad j = 1, 2, \dots, p-1, \\ (5) \quad \text{Tr}(1 - \xi) &= \text{Tr}(1 - \xi^2) = \dots = \text{Tr}(1 - \xi^{p-1}) = p, \end{aligned}$$

$$\begin{aligned} N(1 - \xi) &= p, \\ (6) \quad p &= (1 - \xi)(1 - \xi^2) \dots (1 - \xi^{p-1}). \end{aligned}$$

Montrons maintenant

$$(7) \quad B(1 - \xi) \cap \underline{\mathbb{Z}} = p\underline{\mathbb{Z}}, \quad p \in B(1 - \xi),$$

donc

$$p\underline{\mathbb{Z}} \subset B(1 - \xi) \cap \underline{\mathbb{Z}}.$$

Comme $p\underline{\mathbb{Z}}$ est maximal dans $\underline{\mathbb{Z}}$, on peut en déduire que $p\underline{\mathbb{Z}} = B(1 - \xi) \cap \underline{\mathbb{Z}}$ (car $B(1 - \xi) \cap \underline{\mathbb{Z}} = \underline{\mathbb{Z}}$ est impossible).

LEMME 2. - $\forall y \in B$,

$$(8) \quad \text{Tr}[y(1 - \xi)] \in p\underline{\mathbb{Z}}.$$

$$\begin{aligned} \text{Tr}[y(1 - \xi)] &= \sum_{j=1}^{p-1} y_j (1 - \xi^j), \quad (y_j) \text{ désignant les conjugués de } y. \text{ Comme} \\ 1 - \xi^j &= (1 - \xi)(1 + \xi + \xi^2 + \dots + \xi^{j-1}), \end{aligned}$$

$$\text{Tr}(y(1 - \xi)) \in B(1 - \xi),$$

donc

$$\text{Tr}(y(1 - \xi)) \in p\underline{\mathbb{Z}} \quad (\text{d'après (7)}).$$

Preuve du théorème. - Soit $x \in B$,

$$x = \sum_{i=0}^{p-2} a_i \xi^i, \quad a_i \in \mathbb{Q}, \quad i = 0, 1, \dots, p-2,$$

$$\text{Tr}[x(1 - \xi)] = a_0 \text{Tr}(1 - \xi) = a_0 p \in p\underline{\mathbb{Z}} \quad (\text{d'après (8)}),$$

donc $a_0 \in \underline{\mathbb{Z}}$, $\xi^{-1} \in B$, d'où $(x - a_0)\xi^{-1} \in B$, et par le même raisonnement, $a_1 \in \underline{\mathbb{Z}}$, etc.

Discriminant d'un corps cyclotomique premier ([1], p. 356-357).

$$D = \det(\text{Tr } \xi^{i+j}) = \begin{bmatrix} -1 & -1 & & -1 \\ -1 & -1 & \vdots & p-1 \\ \cdot & \vdots & \cdot & -1 \\ \vdots & -1 & p-1 & \vdots \\ -1 & p-1 & -1 & -1 \end{bmatrix} = (-1)^{(p-1)/2} p^{p-2},$$

$$1 \leq i \leq j \leq p-1.$$

BIBLIOGRAPHIE

- [1] BOREVIČ (Z. I.) et ŠAFAREVIČ (I. R.). - Théorie des nombres. - Paris, Gauthier-Villars, 1967 (Monographies internationales de Mathématiques modernes, 8).
- [2] SAMUEL (Pierre). - Théorie algébrique des nombres. - Paris, Hermann, 1967 (Collection "Méthodes". Mathématiques [1]).
- [3] WEISS (Edwin). - Algebraic number theory. - New York, McGraw-Hill Book Company, 1963 (International Series in pure and applied Mathematics).