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, nº 2 (1967-1968), exp. nº G3, p. G1-G5

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

Groupe d'Etudes de
THÉORIE DES NOMBRES
Année 1967/68, n° 3

4 décembre 1967

BASES D'ENTIERS 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, $\forall\ x \in B$,

$$\left\{\begin{array}{l} N_{K|k}(x) \in A \ , \\ Tr_{K|k}(x) \in A \ . \end{array}\right. \tag{1}$$

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

$$D(x_1 , x_2 , x_3 , \ldots , x_n) = \det[Tr_{K|k}(x_i , x_j)] \ . \tag{2}$$

Propriétés du discriminant.

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

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

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

$$D(x_1 , x_2 , \ldots , x_n) = [\det \delta_i(x_j)]^2 \neq 0 \ . \tag{4}$$

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 $\leqslant n$.*

LEMME 2. - Soient A un anneau intégralement clos, k son corps de fraction, de caractéristique 0 , K une extension de degré fini de k , et B la fermeture intégrale de A dans K ; alors B est un sous-A-module libre de rang n .

THÉORÈME. - Si K est un corps de nombre tel que $[K : \mathbb{Q}] = n$, B la fermeture intégrale de Z dans $\mathbb{Q}$, B est un $\mathbb{Z}$-module libre de rang n , et il existe des bases de B qui soht en même temps des bases de K sur $\mathbb{Q}$.

Remarque. - Si $(x_1 , \ldots , x_n)$ et $(y_1 , \ldots , y_n)$ 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

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

donc

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

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

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

Définition. - On appelle corps quadratique, toute extension de degré 2 de $\mathbb{Q}$.

THÉORÈME. - Tout corps quadratique est de la forme $K = \mathbb{Q}(\sqrt{d})$, où $d \in \mathbb{Z}$ et ne contient pas de facteurs carrés :

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

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

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

On peut supposer (a , b , c) étrangers, et on montre que, sous cette hypothèse, et avec d sans facteur carré, les trois nombres (a , b , c) sont étrangers deux à deux.

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

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

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

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

On montre ensuite simplement le résultat suivant.

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

$$\text{si } d \equiv 2\ ,\ 3\ \ (4), \qquad D = 4d\ ,$$
$$\text{si } d \equiv 1\ \ (4), \qquad D = d\ .$$

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

THÉORÈME. - 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,

$$\mathrm{Tr}(\xi) = -1 \quad ,$$

$$\mathrm{Tr}(1) = p - 1 \quad ,$$

$$\mathrm{Tr}(\xi^j) = -1 \, , \qquad j = 1 , 2 , \dots , p-1 \quad ,$$

(5) $$\mathrm{Tr}(1-\xi) = \mathrm{Tr}(1-\xi^2) = \dots = \mathrm{Tr}(1-\xi^{p-1}) = p \quad ,$$

$$N(1-\xi) = p \quad ,$$

(6) $$p = (1-\xi)(1-\xi^2) \dots (1-\xi^{p-1}) \quad .$$

Montrons maintenant

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

donc

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

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

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

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

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

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

donc

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

<u>Preuve du théorème</u>. - Soit $x \in B$,

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

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

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

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

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

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

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).