Astérisque

RENÉ SMADJA

Utilisation des ordinateurs dans les calculs sur les idéaux des corps de nombres algébriques

Astérisque, tome 41-42 (1977), p. 277-282

<http://www.numdam.org/item?id=AST_1977__41-42__277_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.277-282

UTILISATION DES ORDINATEURS DANS LES CALCULS SUR LES IDÉAUX DES CORPS DE NOMBRES ALGÉBRIQUES

par

René SMADJA

Cet exposé est la description de représentations matricielles des éléments et des idéaux d'une extension finie quelconque K de $\mathbb{Q}$ et de méthodes permettant d'effectuer les calculs arithmétiques dans les ordres de K. Ces représentations ont abouti pour l'instant à des tables donnant les groupes de classes ; les procédés décrits peuvent se révéler utiles dans tous les calculs faisant intervenir les idéaux des corps de nombres et la recherche d'éléments appartenant à une partie bornée d'un réseau de $\mathbb{R}^n$.

Les démonstrations et les tables numériques se trouvent dans [1].

1. NOTATIONS. Le corps $K = \mathbb{Q}(\theta)$ est donné par le polynôme minimal de $\theta, F(X) = X^n + \ldots$. On fixe un plongement de K dans $\mathbb{C}^n$ en choisissant un ordre $\theta_1, \ldots, \theta_n$ sur les racines de F ; on note s le nombre des racines réelles et $2t$ le nombre des racines imaginaires.

L'objet A étudié est un ordre de K, c'est-à-dire un réseau de rang n qui est un sous-anneau de l'anneau des entiers A_K de K.

L'ensemble des matrices à i lignes et j colonnes à coefficients dans l'ensemble X est noté $M_{i,j}(X)$.

2. REPRÉSENTATION DES ÉLÉMENTS DE A . L'anneau A est donné par une $\mathbb{Z}$-base $\mathfrak{B} = (\alpha_{n-1},\ldots,\alpha_o)$ c'est-à-dire par une matrice inversible $B \in M_{n,n}(\mathbb{C})$ représentant les coordonnées du système $(\alpha_{n-1},\ldots,\alpha_o)$ sur la base canonique de $\mathbb{C}^n$.

Tout élément ξ de A est représenté par

- la matrice $\xi_{\mathbb{Z}} \in M_{n,1}(\mathbb{Z})$ de ses coordonnées sur $\mathfrak{B}$;
- la matrice $\xi_{\mathbb{C}} \in M_{n,1}(\mathbb{C})$ de ses coordonnées sur la base canonique de $\mathbb{C}^n$.

Le passage d'une forme à l'autre se fait par multiplication par B ou B^{-1} . Une matrice M de $M_{n,1}(\mathbb{C})$ représente un élément de A si et seulement si $B^{-1}.M$ est à coefficients dans $\mathbb{Z}$. Cela permet de déterminer si un corps K' est contenu dans K ($K' \subset K \Longleftrightarrow \theta' \in A_K$) et en particulier d'énumérer les permutations σ de $\mathfrak{S}_n$ représentant les $\mathbb{Q}$-automorphismes de K dans $\mathbb{C}$ laissant K invariant (groupe de Galois si K est galoisien).

3. BASE D'ENTIERS. Lorsque K est de degré trois ou lorsque le discriminant D de F n'est pas divisible par une puissance quatrième, il suffit de résoudre des systèmes de congruences à une variable pour obtenir une $\mathbb{Z}$-base $\mathfrak{B} = (\alpha_{n-1},\ldots,\alpha_o)$ de A_K .

Dans le cas général, on obtient une telle base de A_K en cherchant α_i sous la forme $\dfrac{\theta^i + a\theta^{i-1} + \ldots + b}{c}$, où $a,\ldots,b,c$ sont des entiers naturels inférieurs à D . La représentation complexe permet d'effectuer simplement sommes et produits donc de trouver le polynôme minimal de tout élément de K : on choisit pour α_i un tel élément entier de dénominateur maximum.

Ceci ne nécessite qu'un nombre fini d'opérations.

4. REPRÉSENTATION DES IDÉAUX DE A . Soit $J = \xi_1\mathbb{Z} + \ldots + \xi_p\mathbb{Z}$ un idéal de A . L'idéal J est représenté par

- la matrice $J_{\mathbb{Z}} \in M_{n,p}(\mathbb{Z})$ du système $(\xi_1,\ldots,\xi_p)$ sur $\mathfrak{B}$;
- la matrice $J_{\mathbb{C}} \in M_{n,p}(\mathbb{C})$ de ce système sur la base canonique de $\mathbb{C}^n$.

Le passage d'une forme à l'autre se fait par multiplication à gauche par B ou B^{-1} .

Les représentations complexes permettent d'effectuer simplement les produits d'idéaux ; les représentations entières permettent de comparer les idéaux :

Proposition 1. Parmi toutes les matrices entières associées à J , il y en a une et une seule qui est triangulaire inférieure (d'ordre n) à coefficients positifs ou nuls, tels que sur chaque ligne le coefficient diagonal soit majorant strict.

Cette forme peut être obtenue à partir de n'importe quelle représentation entière de J au moyen d'un nombre fini d'opérations élémentaires sur les colonnes.

Cette matrice, canoniquement associée à J une fois $\mathfrak{B}$ choisie, est notée $J_{\mathbb{Z}\text{can}}$.

Proposition 2. L'indice de J dans A est le produit des facteurs diagonaux de $J_{\mathbb{Z}\text{can}}$. Si $\alpha_o = 1$, le dernier facteur diagonal est le générateur positif de $J \cap \mathbb{Z}$. Si $A = \mathbb{Z}[\theta]$, les facteurs diagonaux sont les facteurs invariants de J dans A .

5. LA MÉTHODE DE RÉDUCTION CONTINUELLE. A tout élément $a = (a_1,\ldots,a_{s+t})$ de $\mathbb{R}_+^{s+t}$, on associe une norme sur K , définie par $\|\xi\|_a = \sup_{i=1}^{s+t} (a_i|\xi_i|)$.

Soit J un idéal primitif (c'est-à-dire sans facteur rationnel) de A ; notons $J \cap \mathbb{Z} = m\mathbb{Z}$. L'idéal J est dit réduit (pour la norme

a) si $\|\xi\|_a \geqslant \|m\|_a$ pour tout $\xi \in J - \{0\}$.

Proposition 3. Si J est réduit pour a , il est réduit pour $1 = (1,\ldots,1)$. Il n'y a qu'un nombre fini d'idéaux réduits.

Proposition 4. Tout idéal est équivalent à un idéal réduit. On peut trouver tous les idéaux réduits équivalents à un idéal J donné en résolvant un nombre fini de systèmes d'inéquations à inconnues entières.

Indications sur la démonstration :

Si J n'est pas réduit, soit α un élément de $J - \{0\}$ minimal pour la norme 1 ; l'idéal primitif J_R déduit de $J' = \frac{N_{K/\mathbb{Q}}(\alpha)}{\alpha} J$ est réduit ; supposons donc J réduit.

Le cône $\{a \in \mathbb{R}_+^{s+t} \mid J \text{ réduit pour } a\}$ s'appuie sur un polygone dont les sommets se déduisent d'éléments de J dont tous les conjugués sont bornés ; chacun de ces sommets conduit à un idéal réduit équivalent à J ; en déterminant les cônes ainsi associés aux idéaux réduits obtenus de proche en proche, on obtient tous les idéaux réduits équivalents à J.

6. SYSTÈMES D'INÉQUATIONS. Soient J un idéal de A , $m_1,\ldots,m_{s+t}$ des nombres réels positifs. Pour énumérer les éléments ξ de J tels que $|\xi_i| \leqslant m_i$ pour $i = 1,\ldots,s+t$, on plonge K dans $\mathbb{R}^n$ et on cherche les éléments ξ de J tels que la partie réelle et la partie imaginaire de ξ_i soient comprises entre $-m_i$ et m_i .

Matriciellement, le problème se déduit du suivant :

Soient $A \in M_{n,p}(\mathbb{R})$ une matrice de rang $p = n+1-j$, et $B,C \in M_{n,1}(\mathbb{R})$. Trouver toutes les matrices $X = \begin{pmatrix} x_j \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(\mathbb{Z})$ telles que $B \leqslant A.X \leqslant C$.

On résout un tel système en encadrant chacune des variables x_k successivement compte tenu des valeurs prises par les précédentes. On décompose tout d'abord ce système en systèmes partiels $B' \leqslant A'.X \leqslant C'$

correspondant à des matrices principales carrées A' ; le calcul de A'^{-1} permet de déduire de l'encadrement de $A'.X$ un encadrement de X et en particulier de x_j ; on regroupe les encadrements ainsi obtenus et on fait varier x_j entre ces bornes. Pour chaque valeur de x_j , on a à résoudre un système analogue en $x_{j+1},\ldots,x_n$, auquel on applique le même procédé.

7. CALCUL DU GROUPE DES CLASSES. La méthode décrite dans la proposition 4 permet d'associer à tout idéal J un idéal réduit J_R ; elle permet également d'obtenir tous les idéaux réduits principaux de A à partir de l'idéal réduit A . Les procédés décrits au paragraphe 4 indiquent comment faire des produits et des comparaisons d'idéaux.

Soit E un ensemble totalement ordonné d'idéaux engendrant toutes les classes (par exemple les idéaux premiers de degré inférieur ou égal à $\frac{n}{2}$ et de norme inférieure à la constante de Minkowski). On construit à partir de E une suite de composition à quotients cycliques du groupe des classes :

Soit $G = \{1,cl(P_1),\ldots,cl(P_k)\}$ un sous-groupe du groupe des classes (construit avec une partie de E) et P l'élément suivant de E . On calcule tout d'abord P_R , $(P.P_1)_R,\ldots,(P.P_k)_R$; si aucun de ces idéaux réduits n'est principal, la classe de P n'est pas dans G . On fait les mêmes calculs en remplaçant P par P^2 puis P^3 ,... jusqu'à trouver une puissance de P dont la classe est dans G . On remplace alors G par le groupe $\langle G,P\rangle$ ainsi obtenu et on continue.

Le groupe des classes est obtenu lorsque E est épuisé ou lorsque le nombre de classes est suffisant (dans le cas où celui-ci est connu par ailleurs).

8. UNITÉS. En effectuant les produits des facteurs permettant de passer d'un idéal réduit à un idéal réduit voisin, on peut obtenir un

système générateur du groupe des unités ; pour les corps quadratiques et cubiques, on aboutit directement à un système d'unités fondamentales.

9. RÉSULTATS ACTUELS. Un programme utilisant ces procédés a été écrit dans le cas général et utilisé sur de nombreux corps de degré trois et quatre pour obtenir une base d'entiers, le groupe de Galois et le groupe des classes ; la durée des calculs est très raisonnable.

10. GÉNÉRALISATIONS. L'anneau $\mathbb{Z}$ peut être remplacé par tout anneau euclidien dans lequel on connaît un système de représentants modulo les unités. Le corps $\mathbb{C}$ peut être remplacé par un corps quelconque, pourvu que l'on sache y faire travailler un ordinateur, $\mathbb{C}(X_1,\ldots,X_m)$ par exemple.

-:-:-:-

BIBLIOGRAPHIE

[1] René SMADJA.- Calculs effectifs sur les idéaux des corps de nombres algébriques. Département de mathématiques-informatique Luminy (Mars 1976)

René SMADJA
Département de mathématiques-informatique de Luminy
Laboratoire de mathématiques pures associé au C.N.R.S.
70, route Léon Lachamp
13288 MARSEILLE CEDEX 2