PUBLICATIONS DU DÉPARTEMENT DE MATHÉMATIQUES DE LYON

JEAN COUGNARD

Quelques questions sur les entiers algébriques Aspects algorithmiques

Publications du Département de Mathématiques de Lyon, 1989, fascicule 1A
, p. 95-101

<http://www.numdam.org/item?id=PDML_1989___1A_95_0>

QUELQUES QUESTIONS SUR LES ENTIERS ALGEBRIQUES
Aspects Algorithmiques

par
Jean COUGNARD

Cet exposé est avant tout destiné à des étudiants de D.E.A. et ne ne prétend pas donner des démonstrations savantes. Il a simplement l'ambition, plus modeste de montrer que sur bien des questions des progrès théoriques ont été obtenus mais que souvent les algorithmes pour concrétiser ces théorèmes d'existence font encore défaut.

Soient k un corps et P un polynôme de $k[X]$, on sait facilement voir si ce polynôme a ou non une racine dans $\mathbf{Q}$. S'il n'en a pas, on construit un sur-corps de k dans lequel P possède au moins une racine: c'est ce qui a été fait fait pour les polynômes à cœfficients réels en construisant le corps des nombres complexes. Du même coup, tous les polynômes à cœfficients réels, et à fortiori à cœfficients rationnels trouvaient toutes leurs racines. Cela permet de décomposer un polynômes en produit de polynômes irréductibles. Il est donc possible de commencer faire des calculs dans les corps de nombres algébriques.

Dans une première partie, on évoque quelques problèmes naturels sur les corps de nombres algébriques (mais pas tous!) et quels sont leurs analogues pour les anneaux d'entiers. Dans la seconde, on donne brièvement des indications pour la construction de l'anneau des entiers d'un corps de nombres algébriques.

A-RÉSULTATS ET PROBLÈMES

§1 CORPS DE NOMBRES ALGÉBRIQUES

Soient $\mathbf{Q}$ le corps des nombres rationnels et $P \in \mathbf{Q}[X]$ un polynôme irréductible de degré n, on construit le corps de rupture de P: $k = \mathbf{Q}[X]/(P)$.

Ce corps est bien entendu un $\mathbf{Q}$-espace vectoriel de dimension n et si θ est la classe de X, on sait qu'il existe une base <<naturelle>> de $k/\mathbf{Q}$ à savoir $1, \theta, \ldots, \theta^{n-1}$.

Si l'extension est galoisienne sur $\mathbf{Q}$, on sait ([B]) qu'il existe une base de $k/\mathbf{Q}$ formée des conjugués d'un élément. Pour ce qui est de sa construction, on peut consulter ([P.Z]), qui est la référence pour les problèmes algorithmiques liés aux corps de nombres.

Avec ce corps arrivent ses n plongements σ_i dans $\mathbf{C}$ qui permettent de construire des applications :

la norme $N_{k/\mathbf{Q}} : k^* \to \mathbf{Q}^*$ par $N_{k/\mathbf{Q}}(x) = \prod_i \sigma_i(x)$

la trace $T_{k/\mathbf{Q}} : k \to \mathbf{Q}$ par $T_{k/\mathbf{Q}}(x) = \sum_i \sigma_i(x)$.

La seconde de ces applications conduit déjà à des problèmes intéressants. En effet, si vous considérez k comme un $\mathbf{Q}$-espace vectoriel de dimension finie n, vous avez immédiatement une forme quadratique qui apparaît:

$$(x, y) \in k \times k \mapsto T_{k/\mathbf{Q}}(xy) \in \mathbf{Q}$$

Bien entendu, on peut essayer de classer cette forme quadratique, pour cela il faut calculer:

son discriminant $\det(Tr(a_i a_j)_{i,j})$ où les a_i, $1 \leq i \leq n$ forment une base de $k/\mathbf{Q}$.

sa signature qui s'obtient à l'aide des différents plongements de k: elle est égale au nombre des plongements de k dans $\mathbf{R}$.

son invariant de Hasse-Witt, invariant un peu plus long à définir ([L]) et qui a donné lieu il y a quelques années à un article de J.P. Serre ([S]) suivi de développements dans le cadre de la construction des extensions à groupe de Galois $\tilde{A}_n$ (travaux de N. Vila [V], de J.F. Mestre [Me], T. Crespo-exposé aux Journées arithmétique de Marseille 1989, [Cr]-). On peut aussi, sur ces questions, consulter l'ouvrage de Conner et Perlis ([C.P.]). Dans ce dernier,on démontre en particulier que si $k/\mathbf{Q}$ est une extension normale de degré impair, il existe une base normale auto-duale. Dans [B.L.], Eva Bayer et H. Lenstra montrent qu'il en est ainsi pour toute extension galoisienne K/k de corps de carctéristique $\neq 2$ si et seulement si le degré de K/k est impair. Ce résultat se généralise [Ba] en caractéristique 2. On est là proche de mathématiques applicables puisque ces questions intéressent aussi bien les gens qui s'occupent du codage [M.W.] que ceux qui s'occupent de transformée de Fourier discrète [B.F.M.]. Malheureusement, on a une réponse sans algorithme.

§2 L'ANNEAU DES ENTIERS.

Avec le corps, on a aussi un anneau: l'anneau des entiers Z_k de k qui est formé des éléments de k racines d'un polynôme unitaire à cœfficients dans Z. Et toutes les questions qui étaient élémentaires (construction de bases particulières) deviennent difficiles ce qui laisse mal augurer des autres. Bien entendu avec un anneau arrivent ses éléments inversibles et ses idéaux qui sont d'une grande importance, citons par exemple un problème dont le succès médiatique ne se dément pas: le << grand théorème>> de Fermat (cf [W], premier chapitre ou [B.S.] ch.III §1). Les algorithmes essentiels permettant de déterminer l'anneau des entiers, le groupe des unités, le groupe des classes d'idéaux sont au point ([P.Z.], consulter aussi [Bu] et sa bibliographie), et même disponible en Fortran ([K]). Avant de continuer, rappelons les références qui me semblent être les premières lectures indispensables pour qui veut s'occuper des anneaux d'entiers algébriques: [B.S], [Sa].

Le premier problème que nous avions rencontré est celui de l'existence et de la construction de bases: on démontre sans trop de problème que Z_k est un Z-module de type fini, sans torsion donc libre et admettant par conséquent une base sur Z. On peut construire assez facilement une telle base, on le verra dans les sections suivantes, mais si on veut retrouver des bases ayant une allure particulière comme c'était le cas pour $k/\mathbf{Q}$, on se heurte à des problèmes difficiles.

Dans le cas d'une extension galoisienne, on se pose naturellement le problème de l'existence d'une base normale. On sait dire, à peu près ([F]), quand il en existe une, mais en dehors d'exemples canoniques on ne sait pas la construire ([M]). Le problème est très riche dans la mesure où il se trouve de manière mystérieuse relié à la constante de l'équation fonctionnelle des séries L d'Artin.

Dans tous les cas, on peut se poser la question de l'existence d'une base de la forme $1, \theta, \ldots, \theta^{n-1}$. Le problème est lié à des équations de Thue, à des relations entre S-unités et combinaisons linéaires de logarithmes et aux courbes elliptiques. Citons, en dehors des cas << triviaux>> que constituent les corps quadratiques et les corps cyclotomiques le surprenant résultat de M.N. Gras: si p est un nombre premier ≥ 5 et $k/\mathbf{Q}$ une extension cyclique de degré p, pour que Z_k possède une base de puissances il faut et il suffit que $2p+1$ soit un nombre premier ℓ et que k soit le sous corps réel maximal du corps des racines

ℓ-ièmes de l'unité; l'élément θ est alors égal à $\zeta_\ell + \zeta_\ell^{-1}$ ([G]). Mentionnons également que des résultats ont été obtenus dans le cas des extensions abéliennes des corps quadratiques imaginaires ([C.F], [CN.T], [Sc]) en liaison avec les formes modulaires et les courbes elliptiques. On notera qu'à la différence du problème précédent l'existence s'accompagne de la construction explicite.

Le troisième problème, celui de la structure quadratique fait actuellement l'objet de travaux ([T]), on peut évoquer le résultat très parlant de Erez ([E]): supposons que $k/\mathbf{Q}$ soit cyclique de degré premier impair de groupe de Galois G, alors le dual de Z_k relativement à la trace est le carré d'un idéal A_k qui possède une base normale auto-duale!

B-CONSTRUCTION DE L'ANNEAU DES ENTIERS

Je m'inspire du rapport de Smadja ([Sm]). J'ignore s'il est encore disponible, mais on retrouve les mêmes méthodes dans [P.Z.], avec de nombreuses améliorations et compléments. L'idée de base reste la même et s'inspire des travaux de Hermite et Minkowski sur la géométrie des nombres. Parmi les améliorations il convient de noter celles dues à de nouveaux algorithmes concernant les réseaux, par exemple L.L.L.

§3 REPRÉSENTATIONS CANONIQUES

Soit $k = \mathbf{Q}(\theta)$ un corps de nombres algébriques de degré n et P=Irr$(\theta, \mathbf{Q})$. On commence par classer les racines de P ce qui nous donne les différents plongements de k dans $\mathbf{C}$ de telle sorte que $\theta_1, \ldots, \theta_r$ soient réelles, $\theta_{r+1}, \ldots, \theta_{r+s}$ soient complexes réelles deux à deux non conjuguées, $\theta_{r+s+1} = \overline{\theta}_{r+1}, \ldots, \theta_{r+2s} = \overline{\theta}_{r+s}$.

A tout élément x de k, on peut associer deux matrices colonne: si $x = \sum_i a_i\theta^i$, $a_i \in \mathbf{Q}$, $0 \leq i \leq n-1$ on a $\mathbf{x_Z} = (a_0, \ldots, a_{n-1})^t$ et $\mathbf{x_C} = (x_1, \ldots, x_{n-1})^t$ où $x_i = \sum_j a_j\theta_i^j$.

On suppose qu'un sous-anneau A de k est donné par une Z-base $\alpha_{n-1}, \ldots, \alpha_0$ qui peut être representée par une matrice $n \times n$, B, à cœfficients complexes dont les colonnes sont les $\alpha_{\mathbf{j,C}}$. Une matrice colonne $\mathbf{x}$ à cœfficients complexes représente un élément de A si et seulement si $B^{-1}\mathbf{x}$ est une matrice colonne à cœfficients dans Z.

Intéressons nous aux idéaux de A. On suppose $\mathcal{I}$ donné par un système de générateurs sur Z, cas auquel on peut toujours se ramener puisque l'on connaît une Z-base de A. Si $(\mathbf{x}_1, \ldots, \mathbf{x}_p)$ sont les générateurs on peut leur associer deux matrices $\mathcal{I}_Z$ et $\mathcal{I}_C$ à cœfficients respectivement entier ou complexes à n lignes et p colonnes liées par la relation $\mathcal{I}_Z = B^{-1}\mathcal{I}_C$.

Proposition: *Parmi toutes les matrices entières associées à $\mathcal{I}$, il y en a une et une seule qui est triangulaire inférieure, d'ordre n, à cœfficients positifs ou nuls tels que le cœfficient de la diagonale principale majore strictement les éléments de sa ligne. Cette matrice peut être obtenue à partir de n'importe quelle représentation entière de $\mathcal{I}$ par opération élémentaire sur les colonnes.*

Nous appelons opération élémentaire sur les colonnes l'une des quatre opérations suivante:

-remplacement d'une colonne par addition d'une combinaison linéaire des autres colonnes.

-multiplication d'une colonne par -1.

-permutation de deux colonnes.

-suppression d'une colonne nulle.

Définition: *La matrice ainsi définie est appelée la matrice canonique de l'idéal $\mathcal{I}$, la base correspondante: la base canonique, les éléments diagonaux: les facteurs canoniques.*

Corollaire: *L'indice de $\mathcal{I}$ dans A est égal au produit des facteurs canoniques de $\mathcal{I}$.*

Corollaire: *Si A a pour discriminant Δ_A l'idéal $\mathcal{I}$ a pour discriminant le produit de Δ_A par le carré du produit des facteurs canoniques.*

Corollaire: *La norme de $\mathcal{I}$ est le produit des facteurs canoniques.*

Corollaire: *Si l'anneau A est Z-monogène, les facteurs canoniques sont les générateurs positifs des facteurs invariants du groupe abélien $\mathcal{I}$ par rapport au groupe abélien A.*

Démonstration: Notons la matrice canonique:

$$\begin{pmatrix} m_{n-1} & 0 & \dots & & \\ * & \ddots & 0 & \dots & \\ * & * & m_i & 0 & \dots \\ * & * & * & \ddots & 0 \\ * & * & * & * & m_0 \end{pmatrix}$$

et démontrons par récurrence sur i que m_i divise tous les cœfficients de la matrice extraite:

$$\begin{pmatrix} m_i & 0 & \dots \\ * & \ddots & 0 \\ * & * & m_0 \end{pmatrix}$$

la propriété est évidente pour $i = 0$. Notons β_ℓ l'élément de $\mathcal{I}$ représenté par la colonne ℓ. Supposons la propriété vérifiée jusqu'au rang i. Notons θ le générateur de A; l'élément $\theta\beta_i$ appartient $\mathcal{I}$, la colonne entière qui le représente est combinaison linéaire à cœfficients entiers de $C_{i+1}, C_i, \dots, C_0$, il en résulte que m_i est multiple de m_{i+1}. De même l'élément $(m_i/m_{i+1})\beta_{i+1} - \theta\beta_i$ appartient à $\mathcal{I}$ et est Z-combinaison linéaire de $\beta_i, \dots, \beta_0$; on en déduit que $(1/m_{i+1})\beta_{i+1}$ est combinaison linéaire à cœfficients entiers de $(1/m_i)\theta\beta_i, (1/m_i)\beta_i, \dots, (1/m_i)\beta_0$, par l'hypothèse de récurrence ces éléments sont représentés par des matrices à cœfficients entiers, il en est donc de même pour $(1/m_{i+1})\beta_{i+1}$. Ceci prouve que les éléments de la $i+1$ème colonne sont tous divisibles par m_{i+1}. Il en résulte que les $(1/m_i)\beta_i$ appartiennent tous à A, la comparaison des indices montre que c'est une base de A.

§4 CONSTRUCTION DE L'ANNEAU DES ENTIERS

On suppose que $k = \mathbf{Q}(\theta)$ où θ est racine de $F = X^n + a_1X^{n-1} + \dots + a_n$ polynôme à cœfficients entiers, on note $\Delta = df^2$ le discriminant de F avec d entier non divisible par un carré, f entier positif.

Théorème 1: *L'anneau Z_k possède une Z-base $\alpha_{n-1}, \dots, \alpha_0$ où α_i est de la forme:*

$$\alpha_i = \frac{\theta^i + a_{i,1}\theta^{i-1} + \dots + a_{i,i-1}\theta + a_{i,i}}{b_i}$$

avec $a_{i,j} \in \mathbf{N}$, $b_i \in \mathbf{N}^*$, $0 \leq a_{i,j} < b_i/b_{i-j}$. *Les conditions imposées assurent l'unicité des cœfficients* $a_{i,j}$, b_i, *de plus pour tout* i, b_i *divise* b_{i+1} *et* $\alpha_0 = b_0 = 1$.

Démonstration : Z_k est un réseau et $A \subset Z_k$, il suffit de regarder le discriminant de A pour voir que fZ_k est un idéal de A. Munissons A de la base formée des θ^i; le dernier corollaire du paragraphe précédent montre que fZ_k possède une base $(\beta_{n-1}, \ldots, \beta_0)$ déterminée de façon unique par les conditions:

$\beta_i = m_i(\theta^i + a_{i,j}\theta^{i-1} + \ldots + a_{i,i})$, $0 \leq m_i a_{i,j} \leq m_{i-j}$.

$\beta_0 = m_0$ est le plus petit entier appartenant à fZ_k, il est donc égal à f; de plus m_i divise m_{i-1}; donc $b_i = f/m_i$ est entier pour tout i et pour tout i, b_i divise b_{i-1} et $b_0 = 1$. Il ne reste plus qu'à poser $\alpha_i = f/m_i$ pour obtenir la base décrite dans l'énoncé.

Définition: *Un élément* x *de* $\mathbf{Q}(\theta)$ *est dit d'ordre* i *s'il s'écrit* $x = \sum_{j \leq i} q_j \theta^j$.

Tout élément d'ordre i est donc combinaison linéaire des éléments $\alpha_i, \alpha_{i-1}, \ldots, \alpha_0$. la proposition suivante est un élément clé pour la détermination de l'anneau des entiers.

Proposition: *Le discriminant* Δ_k *de* Z_k *est égal à* $\Delta/(b_1 \ldots b_{n-1})^2$. *Pour tout* i *et pour tout* $j \geq i$ $b_i^{[j/i]}$, *où* [ ] *désigne la partie entière, divise* b_j. *Pour tout* i, $f/(b_1 \ldots b_{i-1})$ *est divisible par* $b_i^{(n-i)+(n-2i)+\ldots+(n-[n/i]i)}$.

Démonstration : La première assertion est la conséquence immédiate du second corollaire de la proposition du paragraphe 3.

Posons $u = [j/i]$; $\alpha_i^u \theta^{j-iu}$ est un élément de Z_k d'ordre j, il est donc combinaison linéaire à cœfficients entiers de $\alpha_j, \alpha_{j-1}, \ldots, \alpha_0$, il en résulte que $1/b_i^u$ est multiple entier de $1/b_j$, ce qui démontre la seconde assertion.

Pour terminer, la première assertion nous dit que :

$$\Delta_k = d\left(\frac{f}{(b_1 \ldots b_{i-1})(b_i \ldots b_{n-1})}\right)^2$$

est un entier comme d n'est pas divisible par un carré, on en déduit que $f/(b_1 \ldots b_{i-1})$ est divisible par $b_i \ldots b_{n-1}$. La seconde propriété nous affirme que b_i divise $b_i \ldots b_{n-1}$ avec une puissance $e_i \geq [i/i] + [(i+1)/i] + \ldots + [(n-1)/i]$. Cette somme contient $n-i$ termes, supérieurs ou égaux à 1, $n-2i$ supérieurs ou égaux à 2, ... On obtient bien la valeur de l'énoncé.

Admettons la proposition suivante:

Proposition : *Soient* b_i, $a'_{i,1}, \ldots, a'_{i,i}$ *des entiers positifs tels que:*

$$\alpha'_i = \frac{\theta^i + a'_{i,1}\theta^{i-1} + \ldots + a'_{i,i}}{b'_i}$$

soit un entier algébrique. S'il n'existe pas d'entier algébrique de cet ordre avec un dénominateur plus grand, on peut choisir α'_i *comme élément d'ordre* i *de la base d'entier. Si de plus le* i*-uple* $(a'_{i,1}, \ldots, a'_{i,i})$ *est minimal pour l'ordre lexicographique, alors* $\alpha'_i = \alpha_i$.

Théorème : *La détermination de* Z_k *peut se faire au moyen d'un nombre fini d'opérations bornable effectivement en fonction de* f.

Démonstration: Supposons effectivement construits $\alpha_1, \ldots, \alpha_{i-1}$ et montrons comment obtenir l'élément suivant α_i. Pour cela notons $p_1^{v_1} \ldots p_m^{v_m}$ la décomposition en facteurs premiers de $f/(b_1 \ldots b_{i-1})$ et soit $e = (n-i) + (n-2i) + \ldots + (n - [n/i]i)$. On sait que l'on peut écrire $b_i = b_{i-1} g_i$ avec g_i entier et que b_i^e divise $p_1^{v_1} \ldots p_m^{v_m}$ ceci nous donne un nombre fini de choix possibles pour b_i, pour chacun d'eux le nombre de possibilités pour les $a_{i,j}$ est également borné.

§5 APPLICATION AUX AUTOMORPHISMES DE k

Tout **Q**-automorphisme de k est représenté par un élément σ du groupe Σ_n des permutations de n-lettres opérant sur $\theta_1, \ldots, \theta_n$, ou encore par permutation des lignes des matrices complexes représentant les éléments de k. Un élément x de Z_k étant donné par sa matrice $\mathbf{x}_C$ il est facile de savoir si $\sigma(x)$ est dans Z_k puisqu'il suffit (avec les notations du §3) que $B^{-1}\mathbf{x}_C$ soit une matrice à cœfficients entiers. Il suffit de faire l'opération avec les éléments $\alpha_0, \ldots, \alpha_{n-1}$, lorsque l'on a ainsi mis en évidence un élément σ, **Q**-automorphisme de k, on a sa matrice relativement à la base de Z_k et donc son ordre. On peut donc mettre en évidence de manière effective le groupe des automorphismes de k.

Bien entendu, il ne s'agit que des principes gnraux, à les suivres à la lettre la procédure n'est pas très efficace. Cette simple constatation explique qu'avec la multiplication des ordinateurs et des possibilités de calculs, beaucoup de gens aient travaill à l'amélioration de ces algorithmes.

La bibliographie qui suit n'est pas exhaustive mais peut indiquer des pistes d'études. Quelques travaux récents, non cités dans le texte y ont été ajoutés. Un dernier conseil à ceux qui sont tentés par la théorie des nombres et les calculs: ne pas n:'egliger la lecture régulière de Math. of Computations!

Références

[B] - N. BOURBAKI -*Algèbre Ch. V.* Hermann **1958**.

[Ba]-E.BAYER -*Self-Dual Normal Bases.* Proc. Koninglijke Nederl.Ak. Wetenschappen vol 92 n°4 **1989**, p.379-383.

[B.F.M. - T.BETH & W.FUMY & R. MÜLHFELD -*Zur Algebraischen diskreten Fourier-Transformation.* Arch. Math. vol 40 **1983**, p. 238-244.

[B.L.] - E.BAYER-FLUCKIGER & H.W. LENSTRA Jr. -*Forms in Odd Degree Extensions and Self-Dual Normal Bases.* A paraître

[B.M.O.]-A.M. BERGÉ & J. MARTINET & M. OLIVIER -*The computation of sextic fields with a quadratic subfield.*à paraître.

[B.S] - Z.I. BOREVITCH & I.R. SHAFAREVITCH -*Théorie des Nombres.* Gauthier-Villars **1967**.

[Bu] - J.BUCHMANN -*On the Computation of Units and Class Numbers by a Generalisation of Lagrange's Algorithm.* J. of Number Th. vol 26 n°1 **1987**, p. 8-30.

[C.F.] - J.COUGNARD & V. FLECKINGER -*Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité de'anneau d'entiers II.* A paraître dans Acta Arithmética **1990**.

[**C.M.**]-H. COHEN & J. MARTINET -*Class Groups of Number Fields. Numerical Heuristics.* Math. of Computations vol 48 n°177 **1987**, p.123-137.

[**CN.T**] - Ph. CASSOU-NOGUÈS & M. TAYLOR -*Elliptic functions and Rings of Integers.* Birkhaüser **1987**.

[**C.P.**] - P.E. CONNER & R.PERLIS -*A Survey of Trace Forms of Algebraic Number Fields.* World Scientific **1984**.

[**Cr**] - T.CRESPO -*Explicit Construction of $\tilde{A}_n$ Type fields.* J. of Algebra vol 127 **1989**, p.452-461.

[**E**] - B.EREZ -*The Galois Structure of the Trace Form in Extensions of Odd Prime Degree.* J. Number Th. vol 118 n°2 **1988**, p. 438-446.

[**F**] - A.FRÖHLICH -*Galois Module Structure of Algebraic Integers.* Springer Verlag **1983**.

[**G**] - M.N. GRAS -*Non Monogénéité de l'Anneau des entiers des extensions cycliques de* $\mathbf{Q}$ *de degré* $\ell \geq 5$. J. of Number Th. vol 23 n°3 **1986**, p.347-353.

[**K**]-Komputation Algebraic Number Theory- Groupe KANT (Pr. Pohst). Université de Düsseldorf. R.F.A.

[**L**] - T.Y. LAM -*The Theory of Quadratic Forms.* Benjamin **1973**.

[**M**] - R.MASSY -*Bases Normales d'Entiers relatives Quadratiques.* Preprint **1989**.

[**Ma**]-J. MARTINET -*Discriminants and Permutation Groups.* Number Theory(*R.A. Mollin Ed.*), p.359-385 W. de Gruyter.

[**Me**]-J.-F. MESTRE -*Extensions Régulières de* $\mathbf{Q}(t)$. A paraître dans J. of Algebra.

[**M.S.**] - F.J. McWILLIAM & N.J.A. SLOANE -*The Theory of Error Correcting Codes* North Holland **1977**.

[**P.Z.**] - M.POHST & H. ZASSENHAUS -*Algorithmic Algebraic Number Theory.* Cambridge University Press **1989**.

[**S**] - J.-P. SERRE -*Sur l'invariant de Witt de la forme* $Tr(x^2)$. Comm. Math. Helv. 59 **1984**, p.651-676.

[**Sa**] - P.SAMUEL -*Théorie Algébrique des Nombres.* Hermann **1967**.

[**Sc**] - R. SCHERTZ -*Konstruktion von Potenzganzheitsbasen in Strahlklassentkörpern über imaginär quadratischen Zahlkörpern.* J. Reine Angew. Math. 398 **1990**, p.105-129.

[**Sm**] - R.SMADJA -*Calculs Effectifs sur les Idéaux des Corps de Nombres Algébriques.* Publ. U.E.R. Sci. Luminy **1976**.

[**T**] - M.J. TAYLOR -*Rings of Integers and Trace Forms for Tame extensions of Odd Degree.* Math.Zeit. vol 202 **1989**, p.313-341.

[**V**] - N. VILA -*On Central Extensions of A_n as Galois Group over* $\mathbf{Q}$. Arch. Math. vol 44 **1985**, p.424-437 .

[**W**] - L.C. WASHINGTON -*Introduction to Cyclotomic Fields.* G.T.M 83 Springer Verlag **1982**.

U.A. 741 du C.N.R.S.
Faculté des Sciences de Besançon
25030 BESANÇON Cedex