NOTAS DE MATEMATICA

Nº 32

ALGORITHME EUCLIDIEN DANS ALGBRES ARITHMETIQUES PRINCIPALES

POR

RAJ K. MARKANDA ET VICTOR ALBIS-GONZALEZ

DEPARTAMENTO DE MATEMATICA
FACULTAD DE CIENCIAS
UNIVERSIDAD DE LOS ANDES
MERIDA - VENEZUELA

1979

ALGORITHME EUCLIDIEN DANS ALGBRES ARITHMÉTIQUES PRINCIPALES

NOTE DE RAJ K. MARKANDA ET VICTOR ALBIS-GONZALEZ

Dans cette note nous montrons que, sous certaines conditions, chaque ordre principal d'une algébre arithmétique est euclidien.

In this note we show that, under certain conditions, every principal order of an arithmetic algebra is euclidean.

Soit A un algébre simple centrale sur un corps global K tel que A satisfait la condition d'Eichler. Notre but est de montrer que, sous certaines conditions, chaque ordre principal de A es euclidien. Ceci generalise, dans un certain sens , les resultats suivant de Eichler, Queen et Weinberger.

THÉORÈME (Eichler, 1). Soit A un algébre simple centrale sur un corps de nombres algebriques K. Soit U le produit d'un infini de premiers de K qui ramifie dan A. Alors chaque ordre maximal de A es euclidien si K es euclidien mod U.

THÉORÈME(Queen, 4). Soit K un corps de functions d'une variable sur un corps fini. Soit S un ensemble non vide de valuations de K et O_S l'ensemble d'elements de K integral dans chaque valuation de K qui n'est pas dans S. Alors O_S est euclidien si O_S est principal et S posse de an moins deuv éléments.

THÉORÈME(Weinberger, 6). Soit K un corps de nombres algébriques tel que sou anneau d'entiers es principal et posse de un infini

d'unités. Alors, un hipothése de Riemann generalisee implique que l'anneau d'entiers de K est euclidien.

Soit K un corps global et soit R un domaine de Dedekind avec K comme corps de fractions. Alors, nous disons que un K-algébre simple central A satisfait la condition d'Eichler relative a R si:

(1) K es un corps de nombres algebriques, et $(A:K) \neq 4$ si A ramifie a chaque "non-R" premier de K.

00(2) K est un corps de functions, et quelque "non-R" premier de K n'est remifi dans A.

Maintenant nous definirons un groupe classe rayon $cl_A(R)$. La notation est essentiellement celle de Reiner [5] :

Nous plasons

$I(R)$ = groupe mutiplicatif de R-ideax de K

$P(R)$ = sous-groupe d'ideaux principaux de K

$Cl(R) = \frac{I(R)}{P(R)}$ = groupe classe ideal de R

S = ensemble de toute les infinis premiers de K que ramifient dans A.

$U(A) = \{\alpha \in K - \{0\} : \alpha_p > 0$ pour chaque P dans $S\}$

$P_A(R) = \{R\alpha : \alpha \in U(A)\}$ = groupe rayon (mod S).

Alors, $Cl_A(R) = \frac{I(R)}{P_A(R)}$ est defini comme le groupe classe rayon mod S.

De la definitons de $Cl(R)$ et $Cl_A(R)$ nous voyons que il existe un epimorphisme

(1) $$\sigma : Cl_A(R) \longrightarrow Cl(R)$$

Soit maintenant Λ un ordre maximal de A tel que le numeró de classe $h(\Lambda)$de Λ est 1, cést-a-dire, Λ es principal.

Pour montrer que le numeró de classe de K est 1, nous aurons besoin du Théorème suivante.

THÉORÈME(Swan, 5, p.313). Soit A une K-algèbre simple central avec la condition d'Eichler par rapport a R. Alor, l'application norme reduite induit un isomorphisme.

(2) $$\nu : Cl^{\ell}(\Lambda) \simeq Cl_A(R)$$

Ici $Cl^{\ell}(\Lambda)$ est le groupe additif de les classes d'isomorphismes de Λ-ideaux a gauche dans A.

Remarque (i) Si Λ est maximal, alors

$$Cl^{r}(\Lambda) \simeq Cl^{\ell}(\Lambda)$$

(ii) $h(\Lambda) = \#[Cl^{\ell}(\Lambda)]$ et, si Λ , Λ' son ordres maximaux de A, alors $h(\Lambda) = h(\Lambda')$.

THÉORÈME 1. Si $h(\Lambda) = 1$, alors $h(R)$ = numeró de classe de K est 1.

Preuve: immdiatement de (1), (2) et le remarque (ii).

M. Kneser et R. Swan nous ont communiqué une preuve assez simple de la Théorème de la norme d'Eichler, qui est une generalization du Satz 5 de [1]. La preuve de Swan utilise le Théorème de la norm local et le Théorème de l'approximation forte. Le cas oú K est un corps numerique, le Théorème de l'approximation forte a eté demostré par Kneser dan [2] . Pour le cas d'un corps de fonctions la preuve faite par Prasad apparait dan [3]. Nous ettablisons dessous:

Théorème de la Norme d'Eichler. Soit A une K-algèbre simple centrale avec la condition d'Eichler par rapport a R. Soit U le produit d'un infini de premiers dans K que ramifient dans A. Soit Λ un ordre maximal de A et soit I un ideal bi-latere de Λ. Soit α dans Λ et b dans R tels que

$$n(\alpha) \equiv b \pmod{I} \text{ et } b \equiv n(\alpha) \equiv 1 \pmod{U}$$

Alors, il existe β dans Λ tel que

$$\beta \equiv \alpha \pmod{I} \text{ et } n(\beta) = b$$

Ici $n(\alpha)$ est la norme reduite de α .

La preuve de cet Théorème apparaitra ailleur, dans les notes de Swan.

Nous dison que un corps global K est euclidien mod U par rapport a l'algorithme ϕ si etant donnes α, β dans R, avec $\alpha \equiv \beta \equiv 1 \pmod{U}$ ils existent γ, β dans R tels que

$$\alpha = \beta.\gamma + \delta$$

et soit $\delta = 0$ ou soit $\phi(\delta) < \phi(\beta)$ et $\delta \equiv 1 \pmod{U}$.

Théoréme Principal. Soit A un algébre simple central sur un corps global K. Soit R un domaine de Dedekind tel que le corps des quotients de R est K. Soit U le produit d'infini des premiers de K que ramifient dans A. Supposons maintenant que: (1) Si K est un corps numerique, soit U vide et R l'anneau de Dedekind de K avec un infini d'unités.

(2) Si K est un corps de fonctions, soit R de la forme 0_S, avec l'ensemble d'elements de K integral a chanque valuation de K qui n'est dans S et supposons que $\#(S) \geq 2$.

Si Λ est un ordre maximal de A avec numero de classe $h(\Lambda)=1$, alors Λ est euclidien pour un certain algorithme.

Preuve: Par Théoréme 1, $h(\Lambda) = 1$ implique que R est principal. Utilisant les resultats de Queen, Weinberger, et les suppositions dans U, on trouve que K est euclidien mod U par rapport a un certain algorithme multiplicatif ϕ.

Pour montrer que Λ est euclidien par rapport a ϕ 0 n on procede comme suit:

Soient α, β dans Λ avec β un diviseur different de zero dans A. On peut supposer que le P.G.C.D. de α et β est 1. D'autre part $n(\alpha)$ et $n(\beta)$ son dans R avec $n(\beta) \neq 0$. Etant donné que K est euclidien mod U, alors il existe d dans R tel que

$$n(\alpha) \equiv d(Rn(\beta)$$

et $d \equiv 1 \pmod{U}$, $\phi(d) < \phi(n(\beta))$

Par le Théoréme de la norme D'Eichler, il existe un entier δ avec

$$n(\delta) = d \quad \text{et} \quad \delta \equiv \alpha \pmod{\Lambda\, n(\beta)} .$$

Ceci implique que $\delta - \alpha$ est dans $\beta\Lambda$.

Donc

$$\alpha = \beta\gamma + \delta$$

pour un certain γ dans Λ . Aussi

$$\phi n\,(\delta) = \phi(d) < \phi n\,(\beta)$$

et, par consequence, Λ est euclidien par rapport a ϕ o n .

Remarque (i) Si K est un corps numerique et l'index $(A:K)$ est impaire, alors U est toujours vide .

(ii) Nous n'avons pas beaucoup d'information concernant l'algorithme mod U pour les corps numerique. Dans un autre article nous etudions cet algorithme pour les corps quadratiques reels.

Nous sommes reconnaisants a M. Kneser et R. Swan de nous avoir communique les preuves du Théoréme de le Norme D'Eichler.

(1) M. Eichler, J. Reine U. angew. Math. 179 (1938), p. 239

(2) M. Kneser, Crelle 218(1965), p. 190-203

(3) G. Prasad, Ann. of Math. 105(1977), p. 553-571

(4) C. Queen, Acta Arith. 26 (1974), p. 105-113.

(5) I. Reiner, Maximal Orders, Academic Press, 1975.

(6) P. Weinberger, Proc. Symp. Pure Math. of A.M.S. 24 (1973) P. 321-332.

PROF. Raj K. MARKANDA
UNIVERSIDAD DE LOS ANDES
MERIDA - VENEZUELA

PROF. VICTOR ALBIS-GONZALEZ
UNIVERSIDAD NACIONAL DE COLOMBIA
BOGOTA - COLOMBIA

er.-