Pub. Mat. UAB
N°20 Set. 1980
Actes VII JMHL

CONSTRUCCIÓ D'EXTENSIONS DE COSSOS DE NÚMEROS AMB ÍNDEX PREFIXAT

Pascual Llorente, Enric Nart

Secció de Matemàtiques
Universitat de Zulia (Venezuela)
Universitat Autònoma de Barcelona

ABSTRACT. *Let K be a finite number field. In a previous paper* [1], *the authors characterize the integer ideals in K which satisfy $\aleph=i(L/K)$, being L/K an extension of degree 3 or 4. In this paper we study the effective construction of such number fields $L=K(\theta)$, through the minimal polynomial of θ.*

1. Introducció.

Al llarg de tot aquest treball n denotarà el número natural 3 ó 4.

Sigui K un cos de números i A l'anell dels enters de K. Si p és un ideal primer de A denotarem per v_p la valoració de K associada a p. Sigui θ un enter algebraic sobre K de grau m i sigui

$$f_\theta(X) = X^m-\alpha_1X^{m-1}+\alpha_2X^{m-2}-\dots+(-1)^m\alpha_m \in A[X],$$

el polinomi minimal de θ sobre K. Si $D(\theta)$ és el discriminant de $f_\theta(X)$ i D és el discriminant de L/K, on $L=K(\theta)$, es té:

$$D(\theta) = i(\theta)^2\cdot D,$$

on $i(\theta)$ és l'ideal índex de θ. Sigui $i(L/K)$ l'índex de L/K, és a dir el m.c.d. dels ideals $i(\beta)$, on β varia entre els enters de L tals que $L=K(\beta)$.

definició 1. Direm que un ideal $\aleph$ de A és m-admissible si existeix una extensió L/K de grau m tal que $i(L/K)=\aleph$.

En un treball anterior [1], hem caracteritzat els ideals n-admissibles de qualsevol cos de números K. En aquest treball construim families de polinomis $f_\theta(X)\in A[X]$ de grau n tals que si $L=K(\theta)$, l'ideal $i(L/K)$ és un ideal n-admissible prefixat.

Varem veure a [1] que si $\aleph$ és un ideal n-admissible, és equivalent que $\aleph=i(L/K)$ per a un cert L, a que per a tot primer p de A amb $N(p)<n$ $(N=N_{K/\mathbb{Q}})$, p descomposi d'una determinada manera a L/K; en conseqüència, per resoldre el nostre problema és suficient trobar per a cada primer p amb $N(p)<n$, condicions congruencials mòdul una potència de p sobre els coeficients de $f_\theta(X)$ que assegurin que p descomposa a $K(\theta)/K$ de la manera adequada. Com que si $v_p(\aleph)=0$ és suficient imposar que $f_\theta(X)$ sigui p-Eisensteinià, n'hi ha prou amb considerar les descomposicions indicades en els corol.laris 1 i 2 de [1]. Les families $f_\theta(X)$ que construim tenen a més la següent interessant propietat:

$$p \mid \aleph \quad \Rightarrow \quad v_p(i(\theta)) = v_p(\aleph). \qquad (1)$$

En el cas $K=\mathbb{Q}$, Nagell a [2] dóna families de polinomis de grau n que permeten construir extensions $L/\mathbb{Q}$ tals que $i(L/\mathbb{Q})$ és un ideal n-admissible prefixat, encara que sense satisfer la propietat (1). Les families que donem en aquest treball restringides a $K=\mathbb{Q}$ no coincideixen amb les de Nagell i la seva construcció permet deduir en alguns cassos, criteris parcials per determinar $i(L/K)$ en funció de $f_\theta(X)$.

És conegut que per a tot primer p de A, $v_p(p)>0$ només per a un únic primer $p\in\mathbb{Z}$. Ens serà útil la següent definició:

definició 2. Direm que $\pi\in A$ és un uniformitzant de p si $v_p(\pi)=1$ i $\pi=p$ si $v_p(p)=1$.

2. Resultats per $n=3$.

En tota aquesta secció p indicarà un primer de A amb $N(p)=2$ i π denotarà un uniformitzant de p.

Teorema 1. Sigui θ un enter algebraic sobre K de grau 3 tal que $f_\theta(X)$ satisfà $\alpha_1\equiv 0$ (mòd.p^3). Aleshores $v_p(D(\theta))=2$ i p descomposa completament a $K(\theta)$ si i només si

$$\alpha_2 \equiv 1+\pi \ (\text{mòd.}p^2) \quad \text{i} \quad \alpha_2+\alpha_3 \equiv 7 \ (\text{mòd.}p^3).$$

Corol.lari. Si L/K és una extensió de grau 3, $p|i(L/K)$ si i només si existeix un $\theta\in L$ tal que $L=K(\theta)$ i $f_\theta(X)$ satisfà:

$$\alpha_1 \equiv 0 \ (\text{mòd.}p^3), \quad \alpha_2 \equiv 1+\pi \ (\text{mòd.}p^2), \quad \alpha_2+\alpha_3 \equiv 7 \ (\text{mòd.}p^3).$$

En aquest cas $v_p(i(\theta))=1$.

3. Resultats per $n=4$.

Teorema 2. Sigui $N(p)=3$, $\pi\in A$ un uniformitzant de p i θ un enter algebraic sobre K de grau 4 tal que $f_\theta(X)$ satisfà $\alpha_1\equiv 0$ (mòd.p^3). Aleshores $v_p(D(\theta))=2$ i p descomposa completament a $K(\theta)$ si i només si $\alpha_2\equiv -1$ (mòd.p) i

(A) $\quad v_p(\alpha_3)=1, \quad v_p(\alpha_4)>2;$ $\qquad$ ó

(B) $\quad v_p(\alpha_3)>1, \quad \alpha_4 \equiv \pi^2$ (mòd.p^3).

Corol.lari. Sigui $N(p)=3$, $\pi\in A$ un uniformitzant de p i L/K una extensió de grau 4. Aleshores, $p|i(L/K)$ si i només si existeix un $\theta\in L$ tal que $L=K(\theta)$ i $f_\theta(X)$ satisfà:

$\alpha_1 \equiv 0$ (mòd.p^3), $\quad \alpha_2 \equiv -1$ (mòd.p) $\quad$ i $\quad$ (A) ó (B) del teorema 2.

D'ara endavant denotem per p un primer de A amb $N(p)=2$, per π un uniformitzant de p i per θ un enter algebraic sobre K de grau 4.

Teorema 3. Si $f_\theta(X)$ satisfà:

$$\alpha_1 \equiv 2 \ (\text{mòd.}\, p^5), \quad \alpha_2 \equiv 1+\alpha_3 \ (\text{mòd.}\, p^3), \quad \alpha_3 \equiv \pi \ (\text{mòd.}\, p^2), \quad \alpha_4 \equiv 0 \ (\text{mòd.}\, p^3),$$

aleshores $v_p(D(\theta))=4$ i p descomposa completament a $K(\theta)$.

Teorema 4. Si $f_\theta(X)$ satisfà:

$$\alpha_1 \equiv 2 \ (\text{mòd.}\, p^5), \quad \alpha_2 \equiv 1-\pi^2 \ (\text{mòd.}\, p^4), \quad \alpha_3 \equiv \pi \ (\text{mòd.}\, p^5), \quad \alpha_4 \equiv \pi+\pi^2 \ (\text{mòd.}\, p^5),$$

aleshores $v_p(D(\theta))=4$ i $p = P_1 \cdot P_2 \cdot P_3^2$ a $K(\theta)$.

Teorema 5. Si $f_\theta(X)$ satisfà:

$$v_p(\alpha_1)=v_p(\alpha_2)=0, \qquad v_p(\alpha_3)=1, \qquad v_p(\alpha_4)=2,$$

aleshores $v_p(D(\theta))=2$ i $p = P_1 \cdot P_2$ amb $N(P_i)=p^2$, $i=1,2$ a $K(\theta)$.

Referències.

1. P.Llorente-E. Nart, Sobre l'índex d'extensions relatives de cossos de números, VII Jornadas matemáticas hispano-lusas, Sant Feliu de Guíxols, 1980.

2. T. Nagell, Les diviseurs fixes de l'index des nombres entiers, Arkiv för Mat. Bd.6, Nr.15 (1965), 269-289.