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

SOBRE L'ÍNDEX D'EXTENSIONS RELATIVES DE COSSOS DE NÚMEROS

Pascual Llorente, Enric Nart

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

ABSTRACT. *We define the index $i(L/K)$ of an extension L/K of finite number fields as the g.c.d. of the ideals $i(\theta)$, index of the integers θ of L such that $L=K(\theta)$. Then, we call an ideal $\mathfrak{a}$ of K n-admissible if there exists an extension L of K of degree n such that $\mathfrak{a} = i(L/K)$. We characterize the n-admissible ideals of any finite number field K for $n=2,3,4$.*

Sigui L/K una extensió de cossos de números de grau n. Sigui A l'anell dels enters de K i B' el conjunt dels enters θ de L tals que $L=K(\theta)$. Per a cada $\theta\in B'$ es té:

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

on $D(\theta)$ és l'ideal principal de A generat pel discriminant de θ, D és el discriminant de L/K i $i(\theta)$ és l'ideal índex de θ. Anomenarem "índex de L/K" a l'ideal de A:

$$i(L/K) = \text{m.c.d. } \{i(\theta)/\ \theta\in B'\}.$$

Si $\mathfrak{p}$ és un ideal primer de A tal que $\mathfrak{p}\nmid i(\theta)$, podem determinar la descomposició de $\mathfrak{p}$ a L/K mitjantçant la descomposició del polinomi minimal de θ en factors irreduïbles (mòd.$\mathfrak{p}$). Per tant, el problema de determinar la descomposició dels ideals primers de A a L/K queda resolt si $i(L/K)=1$, però ja Dedekind va donar exemples d'extensions sobre $\mathbb{Q}$ en que això no passava.

Sobre el problema de determinar quan un primer $\mathfrak{p}$ divideix $i(L/K)$ són coneguts els següents resultats [3, §25,6]:

<u>Teorema</u> (Dedekind). $\mathfrak{p} | i(L/K)$ si i només si $r(f) > g(f)$ per algún f, on $r(f)$ indica el nombre d'ideals primers $\mathfrak{P}$ de L tals que $\mathfrak{P} | \mathfrak{p}$ i $f = f(\mathfrak{P}/\mathfrak{p})$; i $g(f)$ indica el nombre de polinomis irreduïbles (mòd.$\mathfrak{p}$) de grau f.

<u>Corol.lari</u>. Perquè $\mathfrak{p} | i(L/K)$ és necessari que $N(\mathfrak{p}) < n$ (on $N = N_{K/\mathbb{Q}}$). En el cas en que $\mathfrak{p}$ descomposa completament a L/K aquesta condició també és suficient. En particular $i(L/K) = 1$ per a tota extensió quadràtica.

Direm que un ideal $\mathfrak{A}$ de A és "n-admissible" si existeix una extensió L/K de grau n tal que $i(L/K) = \mathfrak{A}$.

Per determinar els ideals n-admissibles de K no n'hi ha prou amb determinar quins primers $\mathfrak{p}$ divideixen $i(L/K)$ sino que també és necessari conèixer l'exponent $i_\mathfrak{p}$ amb que el divideixen. Aquest problema va ser tractat per Engstrom en el cas $K = \mathbb{Q}$ [1]. En aquest treball hem considerat el problema per a un K qualsevol i hem obtingut entre altres els següents resultats:

<u>Teorema 1</u>. Si $q = N(\mathfrak{p}) < n$ i $\mathfrak{p}$ descomposa completament a L/K es té:

$$i_\mathfrak{p} = \sum_{i=1} s_i \left(n - q^i \left(\frac{s_i+1}{2}\right)\right) \quad , \quad \text{on} \quad s_i = [n/q^i].$$

<u>Teorema 2</u>. Sigui $q = N(\mathfrak{p}) < n$. Sigui r el nombre de primers $\mathfrak{P}$ de L amb $f(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) = 1$ i sigui $t = r(1) - r$. Si per a tot $f > 1$ és $r(f) \leqslant g(f)$ i $t = 0$ ó 1, aleshores és:

$$i_\mathfrak{p} = ts_1 + \sum_{i=1} s_i \left(n - q^i \left(\frac{s_i+1}{2}\right)\right) \quad , \quad \text{on} \quad s_i = [n/q^i].$$

Ja hem vist al corol.lari del teorema de Dedekind que per a tot K, l'únic ideal 2-admissible és el total. A continuació determinarem els ideals n-admissibles per $n=3$ i 4. Amb aquest fí provem primer el següent:

Lema. Si $n=4$, $N(\mathfrak{p})=2$ i $\mathfrak{p}=\mathfrak{P}_1\mathfrak{P}_2$ a L/K amb $N(\mathfrak{P}_i)=\mathfrak{p}^2$ per $i=1,2$; aleshores $i_{\mathfrak{p}}=1$.

Ara, dels teoremes 1 i 2 i del lema es dedueix:

Corol.lari 1. Si $n=3$, $\mathfrak{p}|i(L/K)$ si i només si $N(\mathfrak{p})=2$ i $\mathfrak{p}$ descomposa completament a L/K; aleshores és $i_{\mathfrak{p}}=1$.

Corol.lari 2. Si $n=4$, $\mathfrak{p}|i(L/K)$ si i només si satisfà una de les següents condicions:

(a) $N(\mathfrak{p})=2$ i $\mathfrak{p}$ descomposa completament.
(b) $N(\mathfrak{p})=2$ i $\mathfrak{p}=\mathfrak{P}_1^2\cdot\mathfrak{P}_2\cdot\mathfrak{P}_3$.
(c) $N(\mathfrak{p})=2$ i $\mathfrak{p}=\mathfrak{P}_1\cdot\mathfrak{P}_2$, amb $N(\mathfrak{P}_i)=\mathfrak{p}^2$, $i=1,2$.
(d) $N(\mathfrak{p})=3$ i $\mathfrak{p}$ descomposa completament.

Aleshores, en el cas (a) és $i_{\mathfrak{p}}=2$, mentres que en els altres casos és $i_{\mathfrak{p}}=1$.

Aquests corol.laris mostren que si $n<5$, per a tot $\mathfrak{p}$ amb $N(\mathfrak{p})<n$, $i_{\mathfrak{p}}$ queda determinat per la descomposició de $\mathfrak{p}$ a L/K. En conseqüència, utilitzant els teoremes generals d'existència de Ore-Hasse[2], hem provat els següents:

Teorema 3. $\mathfrak{A}$ és un ideal 3-admissible de K si i només si:

$$\mathfrak{A}=\mathfrak{p}_1\cdot\ldots\cdot\mathfrak{p}_r,$$

tots diferents i amb $N(\mathfrak{p}_i)=2$, $1\leqslant i\leqslant r$.

Teorema 4. $\mathfrak{A}$ és un ideal 4-admissible de K si i només si:

$$\mathfrak{A}=\mathfrak{p}_1^2\cdot\ldots\cdot\mathfrak{p}_r^2\cdot\mathfrak{p}_{r+1}\cdot\ldots\cdot\mathfrak{p}_{r+s}\cdot\mathfrak{q}_1\cdot\ldots\cdot\mathfrak{q}_t,$$

tots diferents i amb $N(\mathfrak{p}_i)=2$, $1\leqslant i\leqslant r+s$; $N(\mathfrak{q}_j)=3$, $1\leqslant j\leqslant t$.

Del teorema de Dedekind es dedueix que el fet de que un primer $\mathfrak{p}$ amb $N(\mathfrak{p})<n$ divideixi o no $i(L/K)$ només depèn de la seva descomposició a L/K. En canvi, no passa el mateix amb el valor de $i_{\mathfrak{p}}$; en efecte, Engstrom a [1] prova que si $K=\mathbb{Q}$ $i_{\mathfrak{p}}$ queda determinat per la descomposició de $\mathfrak{p}$ si $n\leq 7$ i dóna exemples en que això no passa per a $n\geq 8$. La situació corresponent en el cas general d'extensions relatives serà objecte d'un ulterior treball.

Referències.

1. H.T.Engstrom, On the common index divisors of an algebraic field, Trans. Amer. Math. Soc. 32 (1930), 223-237.

2. H.Hasse, Zwei Existenztheoreme über algebraische Zahlkörper, Math. Ann. 95 (1925), 229-238.

3. H.Hasse, Zahlentheorie, Ak. Verlag, Berlin, 1969.