LA BASE MINIMA DE UN CAMPO DE NUMEROS ALGEBRAICOS

Por Ignacio Canals y Juan José Ortiz

Introducción

El propósito inicial de este trabajo fué el de diseñar un método de cálculo que permitiese, con el auxilio de una computadora, conocer en cada caso la base mínima de un campo de números algebráicos. En el desarrollo del mismo, unas veces ayudados por los resultados concretos obtenidos y otras veces por tratar de resolver dificultades de orden práctico, se hicieron conjeturas sobre la forma que debía tener la base mínima, que posterioremente se demostraron sin mucha dificultad.

Una base $a_1, \cdots, a_n$ de K/k, k un campo de Dedekind, se dice que es una base mínima cuando para $c_1, \cdots, c_n \in k$ se tiene $c_1a_1 + \cdots + c_na_n \in \mathfrak{O}$ ($\mathfrak{O}$, anillo de los enteros algebráicos de K sobre k), sí y sólo sí $c_1, \cdots, c_n \in \mathfrak{o}$ ($\mathfrak{o}$, anillo de los enteros de k). Para el caso en que k es un campo local, se conoce en cada caso la base mínima de una extensión finita. Pero no ocurre lo mismo para el caso de campos de números algebráicos (extensiones finitas de los racionales). Dedekind dió un ejemplo, el único que aparece en la literatura, para demostrar que no siempre una base mínima de un campo de números algebráicos consta de elementos que son lai potencias de uno dado. Dicho ejemplo es el Ejemplo 1 de este artículo. Por otra parte, no hemos podido encontrar ningún polinomio de Eisenstein, que proporcione un campo de números algebráicos con base mínima de elementos que no son potencias de uno dado. Así en el Ejemplo 4 en la Sección 2 se encuentra un elemento cuyas potencias son una base mínima. Queda pués, como una conjetura que todo polinomio de Eisenstein (con coeficientes enteros) proporciona un campo de números algebráicos con base mínima de elementos que son potencias de uno dado. El Corolario 1.5 es un acercamiento a esta conjetura. Un resultado conocido es que todo campo ciclotómico posee una base mínima con elementos que son potencias de uno dado.

El interés en conocer una base mínima es, en primer lugar, el de determinar los enteros algebráicos de la extensión correspondiente, y paralelamente conocer el discriminante del campo y por tanto los primos racionales que se ramifican en la extensión. Además la base complementaria de la base mínima determina un ideal fraccionario, cuyo inverso es la diferente del campo, que a su vez nos da todos los ideales de la extensión que son ramificados.

Sea K un campo de números algebráicos y supongamos que $K = Q(\alpha)$ donde $\alpha \in \mathfrak{O}$. Entonces se sabe que ([1], pág. 81) $\mathfrak{O} \subseteq Z + Z\alpha + \cdots + Z\alpha^{n-1}/d(\alpha)$ donde $d(\alpha) = d(1, \alpha, \cdots, \alpha^{n-1})$ es el discriminante de la base $\{1, \alpha, \cdots, \alpha^{n-1}\}$. En ([2], pág. 156) se propone como ejercicio, demostrar que los elementos de $\mathfrak{O}$ de la forma $a_i = d(\alpha)^{-1}(S_{0i} + S_{1i}\alpha + \cdots + S_{ii}\alpha^i)$ con $0 \leq i \leq n - 1$ donde S_{ii} toma el menor valor posible, son una base mínima para $Q(\alpha)/Q$.

En el presente trabajo se da una mayor información (Teorema 1.4) diciendo cómo deben ser los enteros S_{ji}, y se da un método de cálculo, para el cual se

puede escribir un programa en Fortran, que leido por una computadora resuelve el problema para un caso concreto.

Agradecemos al Centro Nacional de Cálculo las amplias facilidades que nos brindaron para el desarrollo de este trabajo.

1. Base Minima

De ahora en adelante utilizaremos la notación vectorial poniendo: $a_i = d(\alpha)^{-1}(S_{0i}, S_{1i}, \cdots, S_{ii}, 0, \cdots, 0)$, y sobreentendiendo que i varía de 0 a $n-1$.

Lema 1.1. *Sea* $K = Q(\alpha)$ *y* $\alpha \in \mathfrak{O}$. *Entonces los elementos* $a_i = d(\alpha)^{-1}(S_{0i}, S_{1i}, \cdots, S_{ii}, 0, \cdots, 0)$ *de* $\mathfrak{O}$, *donde* S_{ii} *toma el menor valor posible, forman una base mínima de* $Q(\alpha)$; *y además* S_{ii} *es divisor de la componente i-ésima de cualquier entero algebráico de la forma* $b_i = d(\alpha)^{-1}(b_{0i}, \cdots, b_{ii}, 0, \cdots, 0)$.

Demostración. Bastará considerar que $0 \leq S_{ji} < d(\alpha)$ pues en caso contrario $S_{ji} = q_{ji}d(\alpha) + R_{ji}$, y entonces $a_i - q_{ji}\alpha^j = d(\alpha)^{-1}(S_{0i}, S_{1i}, \cdots, R_{ji}, S_{ii}, \cdots, 0)$ cumple con la condición $0 \leq R_{ji} < d(\alpha)$.

Todos los a_{ii} correspondientes a los enteros algebráicos de la forma $a_i = d(\alpha)^{-1}(a_{0i}, \cdots, a_{ii}, 0, \cdots, 0)$ forman un ideal en Z, por tanto existe S_{ii} primer elemento del ideal tal que $a_{ii} = q_{ii}S_{ii}$. Entonces $a_i = d(\alpha)^{-1}(S_{0i}, S_{1i}, S_{2i}, \cdots, S_{ii}, 0, \cdots, 0)$ con S_{ii} generador del ideal correspondiente, es base mínima de $Q(\alpha)/Q$. En efecto, sea $\beta \in Q(\alpha)$ entero algebráico, entonces $\beta = d(\alpha)^{-1}(b_0, b_1, \cdots, b_{n-1})$, y se tiene que $b_{n-1} = q_{n-1}S_{n-1,n-1}$, y

$$\beta - q_{n-1}a_{n-1} = d(\alpha)^{-1}(b_{0,n-2}, b_{1,n-2}, \cdots, b_{n-2,n-2}, 0),$$

nuevamente $b_{n-2,n-2} = q_{n-2} \cdot S_{n-2,n-2}$. Por tanto llegamos $\beta - q_{n-1}a_{n-1} - q_{n-2}a_{n-2} - \cdots - q_1a_1 - q_0a_0 = 0$ con $q_i \in Z$ y el lema queda demostrado.

Lema 1.2. *Sea* $a_i = d(\alpha)^{-1}(S_{0i}, S_{ii}, \cdots, S_{ii}, 0, \cdots, 0)$ *la base mínima del lema* 1.1. *Entonces* S_{ii} *es divisor de* $d(\alpha)$, *y ponemos* $d(\alpha) = d_iS_{ii}$.

Demostración. En efecto $\alpha^i = d(\alpha)^{-1}(0, 0, \cdots, 0, d(\alpha), 0, \cdots, 0)$ es entero algebráico, por tanto $d(\alpha) = d_iS_{ii}$.

Nota. Para facilitar la impresión utilizaremos la siguiente notación.

$$p(k, t, i, d) = d_{i+k}d_{i+k+1} \cdots d_{i+t}$$

Lema 1.3. *Sea* $d(\alpha) = D_1^2 \cdot D_2$, *y* a_i *la base mínima del mínima del lema* 1.1. *Entonces* $p(0, n-1, 0, d)$ *es divisor de* D_1.

Demostración. Sea a' el vector columna de componentes a_i, α' el vector columna de componentes α^i y S una matriz $n \times n$ cuya $(i+1)$-ésima fila es $(S_{0i}, S_{1i}, \cdots, S_{ii}, 0, \cdots, 0)$; entonces obtenemos la ecuación matricial: $a' = d(\alpha)^{-1}S\alpha'$ de donde deducimos, teniendo en cuenta que $S_{ii} \times d_i = d(\alpha)$, la relación:

$$d(a_0, \cdots, a_n) = p(0, n-1, i, d)^{-2}\, d(1, \alpha, \cdots, \alpha^{n-1}),$$

$$d(1, \alpha, \cdots, \alpha^{n-1}) = D_1^2 D_2 = p(0, n-1, i, d)^2\, d(a_0, \cdots, a_n)$$

y por ser $(a_0, \cdots, a_{n-1})$ base mínima, su discriminante es el discriminante de $Q(\alpha)/Q$, y por tanto el discriminante de cualquier otra base difiere del discriminante del campo en un cuadrado perfecto. Es decir $p(0, n-1, i, d)$ es divisor de D_1.

TEOREMA 1.4. *Sea a_i la base mínima de los lemas precedentes; y sea i el menor entero tal que $S_{ii} < d(\alpha)$ (equivalentemente $d_i > 1$), es decir $a_j = \alpha^j$ para $j = 0, 1, \cdots, i-1$, entonces:*

I) $a_i = d_i^{-1}(q_{0i}, q_{1i}, \cdots, q_{i-1,i}, 1, 0, \cdots, 0)$, $0 \leq q_{j,i} < d_i$ *donde*

$$0 \leq j \leq i-1,$$

II) $a_{i+q} = p(0, q, i, d)^{-1}(q_{0,i+q}, \cdots, q_{i,i+q}, p_{i+1,i+q}\, d_i, \cdots,$

$$p_{i+k,i+q}\, p(0, k-1, i, d), \cdots, p(0, q-1, i, d), 0, \cdots, 0)$$

donde

$$1 \leq q \leq n-i-1,$$

y además se tiene que $0 \leq q_{j,i+q} < p(0, q, i, d)$ para $(j = 0, 1, \cdots, i)$ *y que* $0 \leq p_{i+k,i+q} < p(k, q, i, d)$ *para* $(k = 1, \cdots, q-1)$.

Demostración de I). Según el lema 1.2 $d(\alpha) = d_{i+t} S_{i+t}$, $(t = 0, 1, \cdots, n-2)$, y de ahí deducimos que:

$$d_i a_i - \alpha^i = d(\alpha)^{-1}(d_i S_{0,i}, \cdots, d_i S_{i-1,i}, 0, \cdots, 0) = \sum_{j=0}^{i-1} q_{ji}\alpha^j,$$

por tanto $S_{j,i} = d(\alpha) \cdot d_i^{-1} \cdot q_{j,i}$ donde $0 \leq j \leq i-1$ y de aquí $a_i = d_i^{-1}(q_{0,i}, q_{1,i}, \cdots, q_{i-1,i}, 1, 0, \cdots, 0)$.

Demostremos II) por inducción sobre q. Para $q = 1$ se tiene $d_{i+1} S_{i+1.i+1} = d(\alpha)$ y de aquí deducimos que $d_{i+1} a_{i+1} - \alpha^{i+1}$ es combinación lineal sobre los enteros de $a_0, a_1, \cdots, a_i$, por tanto:

$$d_{i+1}a_{i+1} - \alpha^{i+1} = \sum_{j=0}^{i} x_{j,i+1} a_j = d_i^{-1}(x_{0,i+1}\, d_i + q_{0,i}, \cdots, x_{i-1,i+1}\, d_i$$

$$+ q_{i-1,i}, x_{i,i+1}, 0, \cdots, 0), \; x_{j,i+1} \in Z,$$

$$a_{i+1} = p(0, 1, i, d)^{-1}(x_{0,i+1}\, d_i + q_{0,i}, \cdots, x_{i-1,i+1}\, d_{i-1,i}, x_{i,i+1},$$

$$d_i, 0, \cdots, 0).$$

Supongamos cierto II) para a_{i+p} con $p \leq q$ y demostrémoslo para $q+1$. Teniendo en cuenta que $d_{i+q+1} S_{i+q+1,i+q+1} = d(\alpha)$, se tiene $d_{i+q+1} a_{i+q+1} - \alpha^{i+q+1} = \sum_{j=0}^{i+q} x_{j,i+q+1} a_j$, y obtenemos para la componente $i+k$, con $0 \leq k \leq q$, la

siguiente expresión:

$$p(0, k, i, d)(x_{i+k,i+q+1}p(0, k, i, d)^{-1} + x_{i+k+1,i+q+1}p_{i+k,i+k+1}p(0, k+1, i, d)^{-1}$$
$$+ \cdots + x_{i+q,i+q+1}p_{i+k,i+q}p(0, q, i, d)^{-1})$$
$$= p(0, k, i, d)p(0, q, i, d)^{-1}(x_{i+k,i+q+1}p(k+1, q, i, d)$$
$$+ x_{i+k+1,i+q+1}p_{i+k,i+k+1}p(k+2, q, i, d) + x_{i+q,i+q+1}p_{i+k,i+q})$$
$$= p(0, k-1, i, d)p(0, q, i, d)^{-1}p_{i+k,i+q+1}.$$

Análogamente se encuentra la componente $i - k$, con $1 \leq k \leq i$, y se obtiene:

$$x_{i-k,i+q+1} + x_{i,i+q+1}q_{i-k,i}\,d_i^{-1} + \cdots + x_{i+q,i+q+1}q_{i-k,i+q}p(0, q, i, d)^{-1}$$
$$= p(0, q, i, d)^{-1}(x_{i-k,i+q+1}p(0, q, i, d) + x_{i,i+q+1}q_{i-k,i}p(1, q, i, d) + \cdots$$
$$+ x_{i+k,i+q+1}q_{i-k,i+k}) = p(0, q, i, d)^{-1}q_{i-k,i+q+1}.$$

Finalmente tenemos:

$$a_{i+q+1} = p(0, q+1, i, d)^{-1}(q_{0,i+q+1}, \cdots, q_{i,i+q+1}, p_{i+1,i+q+1}p(0, 0, i, d), \cdots,$$
$$p_{i+q,i+q+1}p(0, q-1, i, d), p(0, q, i, d), 0, \cdots, 0).$$

COROLARIO 1.5. *Si* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ *es un polinomio de Eisenstein con respecto al primo* p, *entonces no hay entero algebráico* β *de la forma*:

$$\beta = (1/p)(q_{0i}, q_{1,i}, \cdots, q_{i-1,i}, 1, 0, \cdots, 0) \quad \text{donde} \quad 0 \leq q_{j,i} < p.$$

Si α es raíz de $f(x)$, por la teoría de la ramificación se tiene que (p) se descompone en $Q(\alpha)$ en la forma $(p) = \mathfrak{z}^n$ donde $\mathfrak{z}$ es ideal primo de $Q(\alpha)$. Teniendo en cuenta que $f(\alpha) = 0$, se obtiene que $\operatorname{ord}_{\mathfrak{z}} \alpha = 1$.

Sean $q_{j,i} \neq 0$ y $q_{i,i} = 0$ $(t = 0, \cdots, j-1)$, obtenemos que: $\operatorname{ord}_{\mathfrak{z}} \beta = j - \operatorname{ord}_{\mathfrak{z}} p = j - n$, lo cual implica que β no es entero algebráico pues $j < n$.

En el problema número cinco se aplica este corolario.

2. Cálculo de la Base Mínima

Partiendo del polinomio irreducible $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, cuya raíz α define el campo $Q(\alpha)$ de números algebráicos, se encontrará la base mínima correspondiente.

En primer lugar se calcula el discriminante del polinomio (ver [5]) y obtenemos $d(\alpha) = D_1^2 \cdot D_2$. Por tanto los elementos de la forma: $\beta = d^{-1}(q_{0i}, \cdots, q_{i-1,i}, 1, 0, \cdots, 0)$, donde d divide a D_1, son candidatos a ser enteros algebráicos.

Se debe comenzar con $d = p$, donde p es un número primo que divide a D_1. Pues si no hay entero algebráico de la forma $p^{-1}(q_{0i}, \cdots, q_{i-1,i}, 1, 0, \cdots, 0)$, tampoco hay entero algebráico de la forma:

$$\beta = (pq)^{-1}(q_{0,i}, \cdots, q_{i-1,i}, 1, 0, \cdots, 0); \quad 0 \leq q_{j,i} < pq$$

pues en tal caso $q\beta$ sería entero algebráico, lo cual es una contradicción.

En cambio si existe un entero algebráico de la forma $\beta = p^{-1}(q_{0,i}, \cdots, q_{i-1,i}, 1, 0, \cdots, 0)$, se debe probar si existe entero algebráico con denominador múltiplo de p, hasta encontrar un múltiplo de p para el cual no haya entero algebráico con ese denominador.

Una vez encontrado el primer $a_i \neq \alpha^i$, para encontrar el a_{i+1} (según el teorema 1.4) se deben buscar enteros algebráicos de la forma:

$$\beta = (pd_i)^{-1}(q_{0,i+1}, \cdots, q_{i,i+1}, d_i, 0, \cdots, 0)$$

Para diagnosticar si β es entero algebráico se calcula su polinomio de campo con respecto a la base $(1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$, y será entero algebráico sí y sólo si este polinomio tiene coeficientes enteros ([4] Teor. 20, Pág. 89).

Una vez obtenida la matriz $A\,(n \times n)$, cuyo polinomio característico es el polinomio de campo buscado, se utiliza el método de Leverrier-Faddev para calcular coeficientes del polinomio característico ([3] Pág. 193):

Siendo $(-1)^n(x^n - p_1x^{n-1} - p_2x^{n-2} - \cdots - p_{n-1}x - p_n)$ el polinomio característico de la matriz A, obtenemos que

$$A_{i+1} = AB_i, \quad \text{tr}\,(A_{i+1}) = (i+1)p_{i+1}, \quad B_{i+1} = A_{i+1} - p_{i+1}E$$

donde E designa la matriz identidad $(n \times n)$ y $B_0 = E$.

La matriz A se calcula como sigue, sea $\beta = d^{-1}(q_{0,i+1}, q_{1,i+1}, \cdots, q_{i,i+1}, d_i, 0, \cdots, 0)$.

Sea β' el vector columna de componentes $\beta\alpha^i$ y α' el vector columna de componentes α^i, entonces existe A matriz $n \times n$ con componentes a_{ij} números enteros, tal que

$$\beta' = d^{-1}A\alpha'.$$

Cada valor calculado de tr (A_{i+1}) debe ser divisible por $(i+1)d^{i+1}$, para poder asegurar que β es entero algebráico.

Problema 2.1

Dado el polinomio $f(x) = x^3 + x^2 - 2x + 8$ encontrar la base mínima del campo de números algebráicos $Q(\alpha)$, donde α es raíz de dicho polinomio, y encontrar también el discriminante del campo.

La irreducibilidad del polinomio sobre los racionales se ve con facilidad, pues no tiene raíces racionales (los únicos candidatos son los divisores de 8).

En ([5]) se calcula el discriminante de dicho polinomio y se obtiene el valor: $D(f) = -4 \cdot 503$ y 503 es primo. Por tanto $D_1 = 2^2$. Y obtenemos como resultado:

$$a_1 = 1, a_2 = \alpha, \alpha_3 = \frac{\alpha + \alpha^2}{2}$$

que es la base mínima buscada.

Discriminante del campo $Q(\alpha) = D(f)/2^2 \;\; v \; -503$.

Es decir, el único número primo que se ramifica en $Q(\alpha)$ es 503.

Problema 2.2

Igual que el uno para $f(x) = x^3 + 111x + 5476$. Se prueba fácilmente que el polinomio es irreducible.

En ([5]) se calculó:

$$D(f) = (2\cdot 3\cdot 37)^2\cdot (3\cdot 37\cdot 149).$$

Obtenemos como resultado:

$$a_1 = 1,\ a_2 = \alpha,\ a_3 = \frac{148 + 185\alpha + \alpha^2}{222},$$

y discriminante del campo $= D(f)/222^2 = 3\cdot 37\cdot 149$.

Problema 2.3

Igual que el uno para $f(x) = x^4 + x^3 + 3x^2 + 5x - 2$.

Se prueba la irreducibilidad del polinomio sobre Q, viendo que no tiene raíces racionales y que no admite una descomposición de la forma $(x^2 + ax + b)\cdot (x^2 + cx + d)$.

En ([5]) se encuentra el valor de su discriminante: $D(f) = 2^2\cdot 2437$ y 2437 es número primo. Por tanto $D_1 = 2^2$. Obtenemos como resultado:

$$a_i = 1,\ a_2 = \alpha,\ a_3 = \alpha^2,\ a_4 = \frac{\alpha + \alpha^4}{2},$$

y discriminante del campo $= D(f)/2^2 = 2437$, que es por tanto el único primo que se ramifica en $Q(\alpha)$.

Problema 2.4

Lo mismo para $f(x) = x^3 + 6x + 34$. El polinomio es irreducible pues cumple con las condiciones del criterio de Eisenstein para el primo 2.

En ([5]) se encuentra su discriminante:

$$D(f) = 2^2\cdot 3^6\cdot 11.$$

Por tanto $D_1 = 2\cdot 3^3$. En este caso el 2 por ser ramificado según el criterio de Eisenstein, debe permanecer en el discriminante del campo $Q(\alpha)$. Obtenemos como resultado:

$$a_1 = 1,\ a_2 = \frac{1 + \alpha}{3},\ a_3 = \frac{1 + 2\alpha + \alpha^2}{9}.$$

y discriminante del campo $= D(f)/27^2 = 4\cdot 11$.

En este caso observamos que $(1, \beta, \beta^2)$ es una base mínima. Siendo $\beta = 1 + \alpha/3$, y por tanto $Q(\alpha) = Q(\beta)$.

Problema 2.5

Lo mismo, para $f(x) = x^7 + 5x^6 - 50x^5 + 5x^4 + 15x^3 - 10x^2 + 25x + 5$. En ([5]) se encontró: $D(f) = 5^6\cdot 7\cdot 29173\cdot 81256_1960193$. Obtenemos $D_1 = 5^2$ y no

$D_1 = 5^3$, pues el 5 por ser ramificado debe aparecer en el discriminante del campo. Pero en virtud del corolario 1 deducimos que $(1, \alpha, \alpha^2, \cdots, \alpha^6)$ es base mínima.

3. Programa en Fortran

Para efectuar los cálculos de la sección 2 se escribió un programa en FORTRAN para una computadora IBM 1130.

Una dificultad, a resolver en primer lugar, es que el número entero más grande que se puede manejar en esta computadora es $2^{15} - 1 = 32.767$, y en cambio para los cálculos de la sección 2 aparecen en seguida números más grandes, en concreto aparece D_1^n, que para el ejemplo número tres resulta ser $222^3 = 10_1941{,}048$. Para resolver esta dificultad, se diseñan las subrutinas DIVAR, PROMO, SUMOD, que dividen, multiplican y suman números hasta de 10 cifras en base 64, es decir, se pueden manejar números menores o iguales que:

$$\frac{(64 - 1)(64^{10} - 1)}{64 - 1} = 2^{60} - 1 = 1_3152\ 921_2504\ 606_1846\ 975.$$

Otro problema que hubo que resolver fue el de escribir un programa para descomponer un entero en factores primos, y poder así separar la parte del discriminante del polinomio que es un cuadrado perfecto. El programa que se escribió para una computadora CDC 3150 con 32K de memoria, resuelve dicho problema para números menores o iguales que $70_2363878_1869124$.

Las limitaciones que se tienen para el grado y para el tamaño de los números, se pueden ampliar si la computadora que se use tiene mayor capacidad de memoria. Basta para ello cambiar las dimensiones del arreglo IE(115, 10), Así, por ejemplo, poniendo IE(805, 20) se puede llegar hasta grado 20 y números menores o iguales que $2^{120}-1$. Lo cual se puede lograr con una computadora de 32K palabras de memoria, como por ejemplo una CDC 3150.

El tiemplo de cómputo depende del problema que se trate, y de la computadora pue se utilice. En los ejemplos que se adjuntan, el más laborioso es el número dos, en el cual hay que hacer el proceso de la sección 2, 148.222+185 = 33, 041 veces.

Para ello, la 1130 IBM (una computadora pequeña) no lo terminó en dos horas. La CDC 3150 le realizó en 20 minutos.

Antes de publicar este trabajo llegó a nuestro conocimiento el artículo: Rational Arithmetic with Integers of Indefinite Length, de Arnold Ron, Boeing Scientific Research Labs., Seattle, Wash. February, 1969, el cual contiene programas para efectuar las operaciones aritméticas elementales con enteros de tamaño indefinido, escritos en el lenguaje ensamblador de una computadora IBM 360/44. El fundamento teórico de este artículo es representar a los números en base 2^{12} debido a que esta computadora hace operaciones aritméticas con medias palabras (12 bits). La idea es pues similar a la desarrollada en este trabajo, diferenciandose en la base utilizada (en nuestro caso 2^6) debido a la estructura de la IBM 1130, y en el lenguaje Fortran.

Escuela Superior de Física y Matemáticas del IPN

Referencias

[1] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea Publishing Co., New York, 1948.
[2] P. J. McCarthy, Algebraic Extensions of Fields, Blaisdell Publishing Co., Waltham, Massachusetts, Toronto, London, 1966.
[3] W. Jennings, First Course in Numerican Methods, The MacMillan Co., New York, 1964.
[4] O. Zariski and P. Samuel, Commutative Algebra, Volume 1, D. Van Nostrand Company, Inc., Princeton, N. J., 1958.
[5] I. Canals y J. Ortiz, *Discriminante de un polinomio*, Acta Mexicana Ci. Tecn. (en prensa).