Pub. Mat. UAB
Nº 23, Febrer 1981

ALGUNOS PROBLEMAS EN LA TEORIA DE NUMEROS ALGEBRAICOS

Pascual Llorente

§1. Introducción

Uno de los problemas clásicos del Algebra consiste en la resolución de las ecuaciones

$$f(X) = a_n X^n + \ldots + a_1 X + a_0 = 0 \qquad (1)$$

donde $f(X)$ es un polinomio de grado $n > 0$ ($a_n \neq 0$) con coeficientes en el cuerpo Q de los números racionales.

El estudio de este problema conduce naturalmente a la consideración de los cuerpos K de números algebraicos, es decir, al estudio de las extensiones K/Q finitas. En efecto, a la ecuación (1) le podemos asociar el cuerpo $K = Q(\alpha_1, \ldots, \alpha_n)$ que se obtiene al adjuntar a Q las raices de $f(X)$ tomadas en el cuerpo C de los números complejos (o, más generalmente, en una clausura algebraica de Q). Entonces K/Q es una extensión finita y la Teoria de Galois nos permite obtener información sobre las ecuaciones (1) mediante el estudio de K y de su grupo de Galois $Gal(K/Q)$.

Otros problemas, igualmente clásicos, son los llamados problemas diofánticos y que, esencialmente, consisten en hallar las soluciones enteras de ecuaciones algebraicas con coeficientes en el anillo Z de los números enteros.

Sin duda, uno de los más famosos problemas diofánticos es el llamado Ultimo Teorema de Fermat (U.T.F.) que asegura que la ecuación

$$X^m + Y^m = Z^m \qquad (2)$$

no tiene solución en enteros no nulos si $m \geq 2$. Este problema fue propuesto por Fermat hacia el año 1630 y el caso $m = 4$ fue esencialmente resuelto por él mismo, aplicando su método del descenso infinito. Es suficiente considerar, entonces, los casos en que $m = p$ es un primo impar. A pesar de todos los esfuerzos realizados en estos 350 años, el problema sigue abierto.

El U.T.F. es un ejemplo (no tan excepcional como pudiera parecer) de las dificultades que suele encerrar la resolución de un problema diofántico y que contrasta con la habitual sencillez de su enunciado. Esto ha motivado la necesidad de desarrollar una serie de nuevos métodos, tanto álgebro-aritméticos como analíticos y mixtos; ha estimulado la investigación en todas las áreas de la Matemática y la creación de áreas nuevas y ha conducido a buena parte de los problemas actuales en la Teoría de Números.

En esta exposición nos proponemos mostrar, muy brevemente, cómo ciertos problemas diofánticos han originado algunos problemas centrales en la Teoría de Números Algebraicos, cómo éstos han ido evolucionando y generando a su vez nuevas preguntas y problemas, y cuál es el estado actual de los mismos.

Nos adelantamos a señalar que éste es un propósito demasiado ambicioso para un trabajo de tan pocas páginas y que su parcialidad e incompletitud apenas quedarán disimuladas por la lista de referencias que lo concluye.

Sin embargo pensamos que puede ser de alguna utilidad e interés tanto para los no especialistas en el tema, como para los estudiantes de la Licenciatura en Matemáticas. Por esto agradezco al Dr. M. Castellet haberme solicitado esta redacción para ser incluida en Publicacions de la Secció de Matemàtiques.

§2. Planteo de algunos problemas

En todo lo que sigue K denotará un cuerpo de números algebraicos. Sin pérdida de generalidad podemos suponer que $Q \subset K \subset C$. Recordemos que el grado de K/Q es la dimensión $[K: Q]$ de K como Q-espacio vectorial y que, en nuestro caso, $[K: Q] = n$ es finita. Diremos que K es un *cuerpo cuadrático* si $n = 2$; un *cuerpo cúbico* si $n = 3$; etc. Diremos que *K es real* si $K \subset R$ (cuerpo de los números reales); en caso contrario diremos que *K es imaginario*.

El Teorema del Elemento Primitivo asegura que todo K de grado n es de la forma $K = Q(\alpha)$ donde α es una raiz de (1) con f(X) irreducible en Q[X]. Particularmente importantes son los *cuerpos ciclotómicos* $K = Q(\theta_m)$ $(m > 2)$ que se obtienen adjuntando a Q una raíz primitiva m-ésima de la unidad, su grado es $n = \varphi(m)$ (función de Euler).

Es claro que todo $x \in K$ es raíz de algún polinomio de Q[X] de grado $n' \leq n$ (pues $1, x, x^2, \ldots x^n$ son Q-dependientes). El conjunto A de los $x \in K$ que son raíces de un polinomio de Z[X] mónico (el coeficiente de la mayor potencia de X es 1) constituyen un anillo que se llama *anillo de los enteros de K*.

Así como el estudio de la ecuación algebraica (1) conduce a la consideración de los cuerpos K/Q, ciertos problemas diofánticos conducen al estudio de la aritmética de los anillos de enteros algebraicos A/Z.

La idea, expresada muy brevemente, es la siguiente: Dada una ecuación diofántica (*), consideramos una extensión K/Q donde (*) pueda ser factorizada convenientemente, de modo que sea posible determinar sus soluciones en A. Si (*) no admite soluciones en A tampoco las admitirá en Z. Si (*) admite soluciones en A, deberemos determinar si algunas de ellas están en $Z = A \cap Q$.

Por ejemplo, en el caso de la ecuación (2) con m = p primo impar (U.T.F. para p), es natural considerar el cuerpo ciclotómico $K = Q(\theta_p)$. Este ejemplo no sólo es muy ilustrativo del método indicado sino que, además, es el que le dio origen. En [2] se encuentra suficientemente desarrollado.

Desde nuestro punto de vista, la mayor o menor dificultad en el estudio de la aritmética de un anillo de enteros depende de sus propiedades de factorización en primos (elementos irreducibles) y del número de éstos.

Como es sabido, Z tiene muy buenas propiedades de factorización. En efecto, Z es un D.E. (dominio euclideo) y, por lo tanto, un D.I.P. (dominios de ideales principales) y un D.F.U. (dominio de factorización única). La dificultad de la aritmética de Z radica en que posee infinitos primos. Con la intención de superar esta dificultad, se han desarrollado los métodos de localización que, si bien han demostrado ser muy fructíferos (ver [2]), no consideraremos aquí.

La aritmética de un anillo de enteros A suele ser más compleja que la aritmética de Z. Por una parte, A también contiene infinitos ideales primos y, por otra parte, las propiedades de factorización en A no son, en general, tan buenas como en Z. En efecto, A es un D.D. (dominio de Dedekind) y, por lo tanto, todo ideal de A se factoriza de manera única en un producto de ideales primos de A, pero ésto no implica que A sea un D.F.U. Se puede probar fácilmente que

$$A \text{ es D.F.U.} \iff A \text{ es D.I.P.} \qquad (3)$$

y, en general, no todos los ideales de A son principales.

En principio, este hecho constituye un serio inconveniente a la hora de intentar resolver un problema diofántico siguiendo las ideas que expusimos anteriormente: Para utilizar condiciones de divisibilidad en A, debemos

razonar sobre los ideales de A, pero lo que nos interesa es la resolución del problema diofántico en elementos de A. La correspondencia entre ideales y elementos sólo puede hacerse en el caso de ideales principales.

Lo anterior nos conduce naturalmente a plantear el siguiente problema general:

Problema 1 Para qué cuerpos K es A un D.F.U.?

Pero aún en el caso en que A no sea un D.F.U., puede ser posible utilizar el método anterior considerando una extensión adecuada de K: Es claro que si L/K es una extensión finita, L es un cuerpo de números pues $[L: Q] = [L:K][K:Q]$ es finita. Sea B el anillo de los enteros de L. Es claro que $Z \subset A \subset B$ y si B es un D.F.U. el método puede aplicarse. Luego, es natural considerar el siguiente:

Problema 2: Dado K. Existe L/K finita tal que el anillo de los enteros de L sea un D.F.U.?

Observemos que aún cuando la respuesta al Problema 2 sea negativa, el método puede ser aplicable. En efecto, si L/K es finita y B/A son sus correspondientes anillos de enteros, todo ideal Λ de A puede extenderse a un ideal $i(\Lambda) = \Lambda B$ de B y el método puede aplicarse si estos ideales son principales en B. Tenemos así el siguiente

Problema 3: Dado K. Existe L/K finita tal que todo ideal Λ de A se extiende a un ideal $i(\Lambda) = \Lambda B$ principal en el anillo B de los enteros de L?

Para estudiar la aritmética del anillo de los enteros A de K, debemos comenzar por determinar los ideales primos no nulos de A. Para ello observemos que si $P \subset A$ es un tal ideal, $P \cap Z = pZ$ es un ideal primo no nulo de Z

y, en consecuencia, P divide al ideal principal pA. (Recordemos que para ideales, $\Lambda|\Gamma$ es equivalente a $\Lambda \supset \Gamma$). Luego, la determinación de los ideales primos $P \neq (o)$ de A se reduce al conocimiento de la descomposición

$$pA = P_1^{e_1} \dots P_g^{e_g} \qquad (4)$$

de los primos $p \in Z$ (considerados como ideales principales de A) en producto de ideales primos de A.

Este es, sin duda, unos de los problemas centrales de la Teoría de Números Algebraicos.

Si en la descomposición (4), para alguno de los exponentes $e_i (i = 1 \dots g)$ se verifica $e_i > 1$, diremos que el primo p se *ramifica* en K. Estos primos suelen traer complicaciones adicionales pero, felizmente, no son muchos. En efecto, existe un invariante $D_k \in Z$, llamado el *discriminante* de K, con la propiedad siguiente:

$$p \in Z \text{ se ramifica en } K \Leftrightarrow p | D_k \qquad (5)$$

Por otra parte, se prueba que $|D_k| > 1$, es decir, siempre existe algún primo $p \in Z$ que se ramifica en K.

Para estudiar los problemas propuestos, consideremos los grupos abelianos:

I_k = grupo abeliano libre generado por los ideales primos $P \neq (o)$ de A (grupo de los ideales fraccionarios de K)

$P_k = \{A\alpha | \alpha \in K, \alpha \neq 0\} \subset I_k$ (grupo de los ideales fraccionarios principales de K)

$H(K) = I_K / P_K$ (grupo de clases de ideales de K)

Teorema 2.1 H(K) es un grupo abeliano finito

Sea h(K) el orden de H(K)("class-number" de K). Es claro que

$$A \text{ es D.I.P.} \Leftrightarrow h(K) = 1 \qquad (6)$$

El Teorema 2.1 es un resultado muy importante en la Teoría de los Números Algebraicos y el estudio de los invariantes h(K) y H(K) uno de sus problemas centrales. Como veremos enseguida, este problema incluye a los tres problemas que hemos enunciado anteriormente.

Si L/K es una extensión finita y B/A son los correspondientes anillos de enteros, la aplicación que a cada ideal Λ de A le hace corresponder el ideal $i(\Lambda) = \Lambda B$ de B, induce un homomorfismo

$$i : H(K) \to H(L)$$

entre los correspondientes grupos de clases de ideales.

Teniendo en cuenta todo lo anterior, los tres problemas enunciados admiten la siguiente formulación equivalente:

Problema 1: Para qué cuerpos K es h(K) = 1?

Problema 2: Dado K. Existe L/K finita tal que h(L) = 1?

Problema 3: Dado K. Existe L/K finita tal que i: H(K) → H(L) sea el homomorfismo trivial?

Sin embargo, la resolución de ciertos problemas diofánticos depende del valor de h(K)o, más generalmente, de ciertas propiedades del grupo H(K), y no de la respuesta a los problemas anteriores.

Por ejemplo, si $h_p = h(K)$ con $K = Q(\theta_p)$, la resolución del U.T.F. para el primo p no depende de la condición $h_p = 1$ sino de la menos fuerte:

$p \nmid h_p$(ver [2]). Otros ejemplos de problemas diofánticos cuya resolución depende de $h(K)$ o $H(K)$ pueden encontrarse en [24].

Queda justificado, entonces, plantear el siguiente problema general:

Problema 4: Estudiar la estructura de $H(K)$

Esto significa, en particular, determinar su orden $h(K)$.

Siendo $H(K)$ un grupo abeliano finito, se descompone en suma directa de sus componentes p-primarias $H_p(K)$($p \in Z$, primo) y cada una de ellas en suma directa de p-grupos cíclicos. El número $r_p(K)$ de estos sumandos directos cíclicos de $H_p(K)$ es el *p-rango* del grupo $H(K)$. Es decir, $r_p(K)$ es el mínimo número de generadores de $H_p(K)$.

Otra definición equivalente de $r_p(K)$ es la siguiente: Si $H(K)^p$ es la imagen del endomorfismo $x \dashrightarrow x^p$ de $H(K)$, $H(K)/H(K)^p$ es un Z_p-espacio vectorial y su dimensión es $r_p(K)$.

Como caso particular del Problema 4 se tiene el de determinar $r_p(K)$ para diversos valores del primo p y ya tendremos oportunidad de verificar la importancia de este problema en las secciones siguientes.

El último problema general que consideraremos es el siguiente:

Problema 5: Qué grupos abelianos finitos G se representan como $H(K)$?

Adelantémonos a decir que sólo para el Problema 3 se tiene una respuesta satisfactoria. Los otros cuatro son problemas abiertos. En particular, aún no se ha podido determinar el valor de verdad de las siguientes conjeturas:

Conjetura 1. Existen infinitos K con $h(K) = 1$

Conjetura 2. Para todo grupo abeliano finito G, existe un K con $H(K) \approx G$

En relación con esta última conjetura, Frühlich [14] obtuvo en 1962 el siguiente resultado:

Teorema 2.2 Para todo grupo abeliano finito G, existen infinitos K tales que G es una imagen homomórfica de H(K).

Con frecuencia se dice que el número h(K) es una medida de cuánto dista A de ser un D.F.U., es decir, una medida de la complejidad de la aritmética de A. Las relaciones (3) y (6) implican

$$A \text{ es D.F.U.} \Leftrightarrow h(K) = 1 \qquad (7)$$

y ésto da cierta credibilidad a la afirmación anterior. Sin embargo cabe preguntarse: En qué sentido h(K) puede interpretarse como una tal medida?

Recordemos que A D.F.U. significa que todo $\alpha \in A$ no inversible puede expresarse como producto de primos $\Pi_i \in A$ y que si se tienen dos tales factorizaciones de α

$$\alpha = \Pi_1 \cdots \Pi_s = \Pi'_1 \cdots \Pi'_t$$

entonces

$$\text{D.F.U. 1} : s = t$$

$$\text{D.F.U. 2} : \Pi_i \sim \Pi'_j \quad \text{(asociados dos a dos)}$$

Carlitz [5] en 1960 prueba

$$A \text{ es D.F.U. 1} \Leftrightarrow h(K) \leq 2 \qquad (8)$$

Las relaciones (7) y (8) permiten interpretar a h(K) como una medida, en el sentido anterior, si $h(K) = 1$ o $h(K) = 2$ pero poco indican si $h(K) = 3, 4, \ldots$. En la sección siguiente veremos otra aparente interpretación de h(K) como medida, relacionada con el Problema 3, pero que será igualmente insa-

tisfactoria. Una discusión sobre este tema puede encontrarse en [19].

Los resultados de la Teoría de Números Algebraicos expuestos en esta sección pueden encontrarse en cualquier buen texto sobre el tema, en particular en [2] y [25].

§3. Aplicaciones de la Teoría de Cuerpos de Clases

La Teoría de Cuerpos de Clases (T.C.C.), iniciada por Weber y Hilbert a finales del siglo pasado y desarrollada por un conjunto de notables aritmetistas durante la primera mitad del presente siglo, constituye un avance significativo en el desarrollo de la Teoría de Números Algebraicos.

Basicamente, la T.C.C. es un estudio de las extensiones relativas L/K finitas y abelianas (es decir, galoisianas con $\mathrm{Gal}(L/K)$ abeliano) y resuelve, entre otros, el problema de la descomposición (4) de los primos en dichas extensiones.

En esta sección veremos algunas aplicaciones de la T.C.C. a la resolución de nuestros problemas. Exposiciones de la T.C.C. pueden encontrarse, por ejemplo, en [6] y [18]. Sobre la historia de la T.C.C. puede consultarse la exposición de H. Hasse en [6, Cap. XI] y para los temas que desarrollaremos a continuación, la exposición de P. Roquette en [6, Cap. IX].

Junto a los *primos finitos* P de K, es conveniente considerar los *primos infinitos* que pueden identificarse con los $\mathbb{Q}$-isomorfismos no conjugados $\psi : K \to \mathbb{C}$. Si r_1 de ellos verifican $\psi(K) \subset \mathbb{R}$, se tiene que $n = r_1+2r_2$ y el número de primos infinitos de K es $r_K = r_1+r_2$ (r_1 primos infinitos reales y r_2 primos infinitos complejos). Un primo infinito de K se ramifica en L/K si es real y su extensión a L es compleja.

Vimos que toda extensión $K/\mathbb{Q}$ es ramificada (en algún primo) pues $|D_K| > 1$. La situación es diferente en el caso de extensiones relativas L/K.

En efecto, se tiene el siguiente

Teorema 3.1 1) Para todo K existe una máxima extensión K_1/K abeliana no ramificada. Llamaremos *cuerpo de clases de Hilbert* (C.C.H.) de K al cuerpo K_1.

2) Gal $(K_1/K) \simeq H(K)$

En particular, $[K_1 : K] = h(K)$

3) $i : H(K) \to H(K_1)$ es el homomorfismo trivial.

Observemos, en primer lugar, que el teorema anterior da una respuesta afirmativa a nuestro Problema 3. En efecto, dado K existe K_1/K de grado $h(K)$ tal que $i : H(K) \to H(K_1)$ es el homomorfismo trivial.

Esto sugiere otra interpretación de h(K) como medida de la complejidad de la aritmética de A: h(K) indicaría cuánto se debe extender A (el grado de L/K) para que todo ideal de A sea principal en B. Sin embargo, esta interpretación tampoco funciona pues existen ejemplos de cuerpos K con $h(K) = 4$ y $H(K) \simeq Z_2 \oplus Z_2$ para los cuales existe una extensión L/K de grado 2 tal que $i: H(K) \to H(L)$ es trivial. Estos ejemplos inducen a pensar que el invariante con este significado sería el exponente de H(K) y no su orden h(K), sin embargo hay ejemplos que muestran que ésto tampoco es cierto.

El Teorema 3.1 es un instrumento muy poderoso (y fructiferamente empleado) para estudiar nuestros problemas, pero la construcción efectiva del C.C.H. K_1 de K es, en general, muy difícil. Algunos resultados en esta dirección fueron obtenidos por Herz [17].

Consideremos ahora nuestro Problema 2. Es claro que si $h(K_1) = 1$, el Problema 2 tiene solución (respuesta afirmativa) para K pero, en general, ésto no sucede. Construyamos entonces la *Torre de cuerpos de clases de*

Hilbert (t.C.C.H.) de K.

$$K \subset K_1 \subset K_2 \subset \ldots.$$

donde cada cuerpo es el C.C.H. de su antecesor y sea K_∞ la unión de todos los cuerpos $K_i (i = 1,2,\ldots)$. Observemos que K_∞/Q es una extensión algebraica pero no necesariamente finita. En efecto, K_∞/Q es finita si y sólo si la t.C.C.H. de K es finita.

Teorema 3.2 El Problema 2 tiene solución para K si y sólo si la t.C.C.H. para K es finita y en tal caso, $L = K_\infty$ es la mínima solución.

Demostración: Si la t.C.C.H. para K es finita, existe un indice $j \geq 1$ tal que $K_\infty = K_i$ para todo $i \geq j$. Entonces

$$h(K_\infty) = h(K_j) = [K_{j+1} : K_j] = 1$$

y $L = K_\infty$ es una solución del Problema 2 para K.

Para completar la demostración del teorema debemos probar que si L/K es una solución del Problema 2 para K, entonces $K_\infty \subset L$. Para ello, es suficiente probar que $K_1 \subset L$ y luego razonar inductivamente.

De $h(L) = 1$ se deduce que $L_1 = L$. Por otra parte, siendo K_1/K abeliana no ramificada, LK_1/L también es abeliana no ramificada y, en consecuencia, $LK_1 \subset L_1 = L$. Luego $K_1 \subset L$.

La construcción de la t.C.C.H. para K es un problema difícil. Durante muchos años, todas las t.C.C.H. construidas eran finitas y si este fuera un hecho general (válido para todo K), quedarían resueltos los Problemas 1 y 2, incluyendo la Conjetura 1. Por eso fue muy importante el resultado negativo hallado por Golod y Shafarevich [16] en 1964 y que enunciaremos a continuación.

Diremos que L/K es una *p-extensión* ($p \in Z$, primo) si es galoisiana y Gal(L/K) es un p-grupo. Llamaremos *p-C.C.H.* de K a la máxima p-extensión $K_1^{(p)}$ de K contenida en K_1. Así como K_1 permite estudiar el grupo H(K), $K_1^{(p)}$ permite estudiar su componente p-primaria $H_p(K)$.

Consideremos entonces la *p-torre de cuerpos de clases de Hilbert* (p-t.C.C.H.) de K.

$$K \subset K_1^{(p)} \subset K_2^{(p)} \subset \ \ldots\ldots$$

donde cada cuerpo es el p-C.C.H. de su antecesor y sea $K_\infty^{(p)}$ la unión de todos los cuerpos $K_i^{(p)} (i = 1,2,\ldots)$. Es fácil ver que $K_i^{(p)}$ es la máxima p-extensión de K contenida en $K_i (i = 1,2,\ldots)$. En consecuencia, $K_\infty^{(p)} \subset K_\infty$ y si para algún primo $p \in Z$ la p-t.C.C.H. de K es infinita, entonces la t.C.C.H. de K es infinita.

Teorema 3.3. (Golod-Shafarevich)

Existe una función $\gamma(n)$ tal que $r_p(K) < \gamma(n)$ para todo K de grado n cuya p-t.C.C.H. sea finita.

En efecto, se prueba que si la p-t.C.C.H. de K es finita entonces

$$r_p(K) < 2 + 2\sqrt{r_K + \delta_{K,p}} \qquad (9)$$

donde $\delta_{K,p} = 1$ si $\theta_p \in K$ y $\delta_{K,p} = 0$ en caso contrario.

Siendo $r_K = r_1 + r_2 \leq n$, una posible elección de $\gamma(n)$ es

$$\gamma(n) = 2 + 2\sqrt{n+1}$$

Los resultados anteriores nos aseguran que si para algún primo $p \in Z$, $r_p(K)$ es "suficientemente grande" (por ejemplo, $r_p(K) \geq \gamma(n)$), entonces la t.C.C.H. para K es infinita y el Problema 2 tiene una respuesta negativa

para K.-

Vemos así cómo nuestros problemas iniciales conducen a problemas de la T.C.C., en particular a preguntas sobre la finitud de las t.C.C.H. y éstos a su vez conducen a problemas sobre la estructura del grupo H(K) y en particular, a la determinación de $r_p(K)$.

Algunos resultados sobre $r_p(K)$ obtenidos por Brumer, Roquette, Zassenhaus y otros, permiten construir infinitos K cuya t.C.C.H. es infinita.

Antes de terminar esta sección, explicitaremos algunas consecuencias del Teorema 3.3 en el caso de un cuerpo cuadrático y que utilizaremos en la sección siguiente.

Sea K un cuerpo cuadrático ($n = 2$). Si $K \subset R$ es real, entonces $r_k = 2$ y en caso contrario $r_k = 1$. Como $-1 \in K$, $\delta_{K,2} = 1$; pero para todo primo $p > 2$, $\delta_{K,p} = 0$ excepto para $K = Q(\theta_3) = Q(\sqrt{-3})$ en cuyo caso $h(K) = 1$. Teniendo en cuenta estas observaciones y la relación (9), el Teorema 3.3 nos permite concluir:

Corolario 3.4 Un cuerpo cuadrático K posee una t.C.C.H. infinita si se verifica alguna de las siguientes condiciones:

i) $r_2(K) \geq 5$ y K es imaginario

ii) $r_2(K) \geq 6$ y K es real

iii) $r_p(K) \geq 4$ y K es imaginario ($p > 2$)

iv) $r_p(K) \geq 5$ y K es real ($p > 2$)

§4. Cuerpos Cuadráticos

En el caso en que K es un cuerpo cuadrático ($n = 2$), los problemas que

hemos planteado tienen una estrecha relación con la resolución de las ecuaciones diofánticas

$$F = F(X,Y) = aX^2 + bXY + cY^2 = m \qquad (10)$$

es decir, con la representación de enteros m por formas cuadráticas binarias enteras. En esta sección daremos una idea de dicha relación y de la situación actual de nuestros problemas para esta clase de cuerpos.

Comencemos por observar que un cuerpo cuadrático K queda determinado por su discriminante $D = D_K$ (ésto no ocurre, en general, si $n > 2$). En efecto, $K = Q(\sqrt{d})$ donde $d \in Z$ es un entero libre de cuadrados y $D = d$ o $D = 4d$ según sea $d \equiv 1 \pmod 4$ o $d \equiv 2,3 \pmod 4$. Luego $K = Q(\sqrt{D})$.

Dado un entero $D \in Z$ tal que $|D| > 1$ y $D \equiv 0,1 \pmod 4$, denotaremos con H(D), h(D) y $r_p(D)$ a los correspondientes H(K), h(K) y $r_p(K)$ donde $K = Q(\sqrt{d})$ es el único cuerpo cuadrático de discriminante D.

Al estudiar los cuerpos cuadráticos K se observa una diferencia notable según que $D < 0$ (K imaginario) o que $D > 0$ (K real). El caso K real suele presentar dificulatades adicionales debidas a que el grupo multiplicativo I(A) de los inversibles de su anillo de enteros A es infinito, lo que no ocurre si K es imaginario. En efecto, si $D > 0$ existe un $\mu \in I(A)$ (inversible fundamental de A) de orden infinito y tal que $I(A) = \{\pm \mu^k | k \in Z\}$.

El estudio de H(D) y h(D) se inicia con Gauss [15] en 1801 en relación con el problema diofántico (10). Para Gauss b es un entero par, pero aquí adoptaremos un punto de vista más moderno y no pondremos restricciones sobre b. Para lo que sigue puede consultarse [13].

Es claro que es suficiente estudiar las ecuaciones diofánticas (10) en las cuales el M.C.D. $(a,b,c) = 1$ es decir, cuando F es una *forma cuadrática binaria entera primitiva* y así serán todas las formas cuadráticas que

consideremos en lo que sigue.

Diremos que dos formas cuadráticas son *equivalentes* si existe un cambio de variables lineal con coeficientes enteros y de determinante 1 que transforma una en la otra. Entonces el problema (10) no depende de la forma cuadrática F sino de la clase [F] de formas cuadráticas equivalentes a F.

A cada F se le puede asociar el entero $D = D(F) = b^2-4ac$ llamado *discriminante de F* y que sólo depende de [F]. Sea H*(D) el conjunto de las clases de equivalencia de formas cuadráticas de discriminente D. Gauss prueba el siguiente

Teorema 4.1 El cardinal h*(D) de H*(D) es finito.

Gauss resuleve el problema (10) para un discriminante D dado, es decir, determina las representaciones de m por formas cuadráticas de discriminante D. Luego, si h*(D) = 1 el problema (10) queda resuelto si D(F) = D. Sin embargo, el mismo Gauss conjetura.

Conjetura 3. Si $D < 0$, h*(D) = 1 sólo para 9 valores de D.

En su intento de resolver el problema diofántico (10), Gauss es el primero en introducir la noción de *carácter* y con ella establece una partición de H*(D) en *géneros*. Si $g_0(D)$ es el número de clases en el *género principal* G_0, entonces todos los géneros contienen $g_0(D)$ elementos y

$$h^*(D) = g_0(D).g(D) \qquad (11)$$

donde g(D) es el número de géneros.

Gauss resuelve el problema diofántico para un género G de formas cuadráticas y, en consecuencia, si $g_0(D) = 1$ el problema (10) queda resuelto si

$D(F) = D$. Sin embargo, el mismo Gauss conjetura:

Conjetura 4. Si $D < 0$, $g_0(D) = 1$ sólo para un número finito de valores de D.

Más aún, Gauss determinas 65 valores de $D < 0$ para los cuales $g_0(D)=1$, muestra como se corresponden con los 65 *números convenientes* determinados por Euler (en relación con otros problemas) y se pregunta si éstos son todos. Hasta la fecha esta pregunta sigue sin respuesta pero, como veremos, las dos últimas conjeturas han sido demostradas.

Gauss define también una *composición* de formas cuadráticas, que determina sobre $H^*(D)$ una estructura de grupo abeliano, del que G_0 es un subgrupo. Entonces prueba:

Teorema 4.2 (Teorema de duplicación de Gauss)

$$G_0 = H^*(D)^2$$

Por otra parte, Gauss determina el número de géneros $g(D)$

Proposición 4.3 Si t es el número de factores primos de D, entonces

$$g(D) = 2^{t-1}$$

Los dos últimos resultados implican el siguiente

Corolario 4.4 Si t es el número de factores primos de D, entonces

$$r_2(H^*(D)) = t-1$$

La relación que existe entre esta teoría de Gauss de formas cuadráticas y los cuerpos cuadráticos está contenida en el siguiente teorema (ver [2]).

Teorema 4.5 Si D es el discriminante de un cuerpo cuadrático K, entonces existe un homomorfismo

$$\varphi : H^*(D) \to H(D)$$

que es un isomorfismo excepto si $D > 0$ y $N(\mu) = 1$ (donde $N(\mu)$ es la norma del inversible fundamental μ de A), en cuyo caso se tiene una sucesión exacta

$$1 \to Z_2 \to H^*(D) \xrightarrow{\varphi} H(D) \to 1$$

Corolario 4.6 Si t es el número de factores primos del discriminante D de un cuerpo cuadrático K, entonces

$$r_2(D) = t-1$$

excepto si $D > 0$, $N(\mu) = 1$ y la sucesión exacta del Teorema 4.5 se parte, en cuyo caso $H^*(D) \approx Z_2 \oplus H(D)$ y

$$r_2(D) = t-2$$

Esta Teoría de los Géneros de Gauss que permite, entre otras cosas, determinar $r_2(D)$, puede ser reobtenida y generalizada mediante la aplicación de la T.C.C. (ver [17] y [18]).

En el resto de esta sección consideraremos nuestros problemas para cuerpos cuadráticos $K = Q(\sqrt{d})$ de discriminante D.

El Problema 1 de determinar aquellos D para los cuales $h(D) = 1$ depende fundamentalmente del signo de D.

En el caso $D < 0$ se tiene la Conjetura 3 de Gauss. Esta conjetura tiene una larga e interesante historia que no nos es posible detallar aquí. En particular, ha dado lugar a una serie de resultados curiosos uno de los

cuales, probados por Frobenius y Rabinovich en 1912, es el siguiente (ver [25]):

Proposición 4.7 Sea $D < 0$ y $-D \neq 3,4,8$. Entonces $h(D) = 1$ si y sólo si $D \equiv 1 \pmod 4$ y el polinomio $X^2 - X + \frac{1-D}{4}$ toma valores primos para $1 \leq X < \frac{1-D}{4}$.

Esta última condición se verifica si $-D = 19,43,67,163$. Por ejemplo, $X_2 - X + 41$ toma valores primos para $1 \leq X \leq 40$.

Por otra parte, no es muy difícil probar (ver [25]) el siguiente resultado:

Proposición 4.8 Si $D < 0$, entonces

$$A \text{ es } D.E \Leftrightarrow -D = 3,4,7,8,11.$$

Reencontramos así los 9 valores de $D < 0$ calculados por Gauss y para los cuales $h(D) = h^*(D) = 1$.

En el año 1935 Siegel prueba, usando métodos analíticos, un importante teorema (ver [25]) del que se obtiene, en particular, el siguiente

Teorema 4.9 $\lim_{D \to -\infty} h(D) = \infty$

Corolario 4.10 Para todo entero $h \geq 1$, $h(D) = h$ sólo para un número finito de valores de $D < 0$.

Finalmente en 1966, Baker [1] y Stark [30] prueban la Conjetura 3, de manera independiente y con métodos completamente diferentes. También resuelven, en 1971, el problema para $h = 2$ verificando que $h(D) = 2$ sólo para 18 valores de $D < 0$.

En 1976, Buell [4] construye una tabla de $h(D)$ y $H(D)$ para $D < 0$ y

$0 < -D < 4.10^6$, utilizando un método debido a Lehmer y Shanks (ver [28]). Esta tabla sugiere que $h(D) = 3$ para 16 valores de $D < 0$ y $h(D) = 4$ para 54 valores de $D < 0$.

En el caso $D > 0$, la situación es completamente diferente. En efecto, se tiene la siguiente

Conjetura 5 $h(D) = 1$ para infinitos $D > 0$.

Utilizando el Corolario 4.6 se prueba que $r_2(D) = 0$ ($h(D)$ impar) si $D = p$ con $p \equiv 1$ (mód. 4) primo o $D = 4p$ con $p \equiv 3$ (mod.4) primo. Recientemente Atkin (ver [23]) ha examinado estos discriminantes en diversos intervalos en el sector $0 < D < 8.10^6$ y ha observado que para más del 75% se verifica que $h(D) = 1$. A pesar de estas evidencias numéricas la Conjetura 5, al igual que la Conjetura 1, sigue siendo un problema abierto.

Por otra parte, el problema de determinar los $D > 0$ para los cuales A es un D.E. está resuelto. En efecto (ver [25]), en 1938 Heilbronn probó que son finitos y en 1950 Davenport concluye su determinación mostrando que son 16, el mayor de los cuales es $D = 76$.

Con respecto al Problema 5, se tiene la siguiente conjetura más fuerte que la Conjetura 2 y que también constituye un problema abierto:

Conjetura 6 Para todo grupo abeliano finito G, existe un D tal que

$$H(D) \approx G.$$

Si nos restringimos a $D < 0$, esta conjetura es falsa. En efecto, en 1934 Chowla [7] probó el siguiente resultado:

Teorema 4.11 $\lim_{D \to -\infty} g(D)/h(D) = 0$

Teniendo en cuenta la igualdad (11), el teorema anterior implica la Conjetura 4 y ésta a su vez implica el siguiente

Corolario 4.12 Existe un $k_0 \in Z$ tal que $H(D) \approx \mathbb{Z}_2^k$ es imposible si $D < 0$ y $k > k_0$.

Pero estos resultados dejan aún sin respuesta a una serie de preguntas que siguen siendo problemas abiertos:

Cuáles son los $D < 0$ de formas cuadráticas para los cuales $g(D) = h(D)$ (o, equivalentemente, $g_0(D) = 1$)? Son sólo los 65 calculados por Gauss? Si ésto fuera así, el Corolario 4.12 vale con $k_0 = 4$. Cabe preguntarse: Cuál es el menor valor de k_0 que hace verdadero al Corolario 4.12?

Por último: Cuál es el menor grupo abeliano finito G tal que $H(D) \not\approx G$ si $D < 0$?

Hasta hace unos años se pensaba que $G = Z_5^2$ pero Buell muestra en su tabla que si $-D = 12451$ (primo) entonces $H(D) \approx Z_5^2$. Actualmente se supone que $G = Z_3^3$. En efecto, existen 40 grupos abelianos con menos de 27 elementos y todos ellos se realizan como $H(D)$ para algún $D < 0$ pero la tabla de Buell induce a pensar que $-D_0 = 103387$ es el último D con $h(D) = 27$ mientras muestra que para todo D con $0 < -D \leq -D_0$ y $h(D) = 27$ resulta que $H(D) \approx Z_{27}$ o $H(D) \approx Z_3 \oplus Z_9$.

Ya hemos visto como los otros problemas se vinculan a la t.C.C.H. y al estudio de $r_p(K)$. En nuestro caso, el Corolario 4.6 nos permite calcular fácilmente $r_2(D)$ y, teniendo en cuenta el Corolario 3.4, podemos concluir:

Proposición 4.13 Sea K un cuerpo cuadrático de discriminante D y sea t el número de factores primos de D. Si $D < 0$ y $t \geq 6$ o si $D > 0$ y $t \geq 8$, entonces la t.C.C.H. de K es infinita.

Debemos considerar entonces los casos en que t es pequeño. Particularmente interesante es el caso en que $t = 1$, es decir cuando $D = \pm p \equiv 1 \pmod 4$ es primo. En este caso $r_2(D) = 0$ y es necesario estudiar $r_p(D)$ con $p \geq 3$.

Sea $r(D) = \max \{r_p(D) \mid p \geq 2\}$ el rango de $H(D)$, es decir, el mínimo número de generadores de $H(D)$. En todas las tablas conocidas hasta 1970, $r(\pm p) \leq 2$ y los casos en que $r(\pm p) = 2$ (es decir, $H(\pm p)$ no cíclico) eran muy raros. Esto condujo a Shafarevich a plantear en el Congreso Internacional de 1962 el problema de la posible acotación de $r(\pm p)$.

Algunos investigadores conjeturaron (verbalmente) que $r(\pm p)$ está acotado y que la cota es 2. Esto implicaría que el Teorema 3.3 de Golod-Shafarevich nunca sería aplicable en el caso $D = \pm p$.

Sin embargo Shanks [28] en 1971 da el siguiente ejemplo. Si $p = 188184253$ (que es primo!) entonces $H(p) \simeq Z_3^3$, luego $r(p) = r_3(p) = 3$. Este ejemplo muestra, además, que $G = Z_3^3$ se representa como $H(D)$.

A partir de este momento, varios especialistas centraron sus investigaciones sobre $r_3(D)$. Daremos a continuación una idea aproximada del estado actual de las mismas.

Dado D, definamos $D' = -3D$ si $D \not\equiv 0 \pmod 3$ y $D' = -D/3$ si $D \equiv 0 \pmod 3$. Es claro que la correspondencia $D \leftrightarrow D'$ define una biyección entre los cuerpos cuadráticos reales y los cuerpos cuadráticos imaginarios. Scholz [27] probó el siguiente resultado

Teorema 4.14 Si $D > 0$ entonces

$$r_3(D') = r_3(D) \quad \text{o} \quad r_3(D') = r_3(D) + 1$$

Consideraremos en primer lugar el $r_3(D)$ en el caso $D < 0$.

Si p es el primo del ejemplo de Shanks, el teorema anterior nos dice que $r_3(-3p)$ es 3 o 4 y en este caso resulta que $r_3(-564552759) = 3$. Hasta el

año 1976 se obtienen varios ejemplos de $D < 0$ tales que $r_3(D) = 3$, el menor de los cuales corresponde a $-D = 63199139$. Pero cuando Buell construye su tabla obtiene que el menor valor de $-D > 0$ tal que $r_3(D) = 3$ es $-D = 3321607$ que es primo.

El Corolario 3.4 nos muestra el interés de hallar un $D < 0$ tal que $r_3(D) \geq 4$ y, en particular, un D primo con esa propiedad. Craig [8] da el primer ejemplo de $D < 0$ con $r_3(D) = 4$ pero resulta que $-D > 400.10^{100}$ es demasiado grande. Shanks y Serafin [29] obtienen dos ejemplos de $D < 0$ con $r_3(D) = 4$ y $-D$ del orden de 10^8, pero ninguno es primo.

En 1978, Diaz y Diaz [10] obtiene 13 ejemplos de $D < 0$ con $r_3(D) = 4$ ($-D > 10^8$) y 119 ejemplos de $D < 0$ con $r_3(D) \geq 4$ ($-D > 10^{10}$). Recientemente, él mismo con Shanks y Williams [12] analizan estos 119 ejemplos y muestran que para todos ellos $r_3(D) = 4$. Entre estos ejemplos hay 13 para los cuales $-D$ es primo, siendo el menor de ellos $-D = 4724490703$. Esto muestra que $r(-p) > 3$ es posible y que el Teorema de Golod Shafarevich puede ser aplicable al caso $-D$ primo. Para otro de los ejemplos se tiene $H(D) \simeq Z_2^5 \oplus Z_3^4 \oplus Z_{25}$ y la correspondiente t.C.C.H. es infinita tanto por ser $r_2(D) = 5$ como por ser $r_3(D) = 4$.

Actualmente no se conoce ningún $D < 0$ con $r_3(D) > 4$ pero se supone que existe aunque, posiblemente, $-D$ sea muy grande.

El caso $D > 0$ es, como ocurre habitualmente, más difícil.

El primer ejemplo de Shanks sigue siendo el menor $D > 0$ conocido con $r_3(D) = 3$. Para todos los ejemplos de $D < 0$ con $r_3(D) = 4$ resulta que $r_3(D') = 3$.

Para los dos ejemplos de $r_3(D) = 3$ con $0 < -D < 4.10^6$ dados po la tabla de Buell resulta que $r_3(D') = 2$. Luego, según el Teorema 4.14, el menor $D > 0$ con $r_3(D) = 3$ debe verificar $D > 1333333$.

El autor (ver [20]) obtuvo un método para calcular $r_3(p)$ y construyó

una tabla de $r_3(p)$ con $1 < p < 10^6$. Entre ellos hay 30 con $r_3(p) = 2$ siendo el menor $p = 32009$ y el mayor $p = 946733$. Luego continuó las computaciones para $p > 1333333$ con la intención de hallar el menor p tal que $r_3(p) = 3$ pero los resultados fueron negativos. Estas computaciones hacen suponer que dicho p verifica $p > 9.10^6$.

Hasta hace muy poco tiempo, no se conocia ningún $D > 0$ con $r_3(D) > 3$. En 1977 Craig [9] da un método para construir infinitos $a \in Z$, $a < 0$ tales que si $K = Q(\sqrt{a})$ entonces $r_3(K) \geq 4$; el menor de ellos es del orden de $-a \approx 428.10^{100}$. Si K' es el correspondiente cuerpo cuadrático real, el Teorema 4.14 nos asegura que $r_3(K') \geq 3$. Recientemente Diaz y Diaz [11] probó que para éstos cuerpos K se verifica que $r_3(K') = r_3(K)$ con lo que queda probada la existencia de infinitos $D > 0$ con $r_3(D) > 3$.

§5. Otros cuerpos de números

En la sección anterior consideramos los cuerpos cuadráticos, en esta sección final veremos algunos resultados relacionados con el Problema 1 para otros cuerpos de números algebraicos.

Comencemos mostrando cómo el Corolario 4.10 es un caso particular de un resultado mucho más general probado por Uchida en 1971.

Sea K un cuerpo (de números) abeliano imaginario ($r_k = 2r_2$, $r_1 = 0$). Denotemos con $K^+ = K \cap R$ el máximo subcuerpo real de K. Es claro que K^+ es el cuerpo fijo por la conjugación compleja, luego K^+ es un cuerpo de números abeliano real y $[K: K^+] = 2$. En esta situación vale el siguiente resultado (ver [23]).

Teorema 5.1 $h(K^+) | h(K)$

Denotemos $h^+(K) = h(K^+)$. El teorema anterior asegura la existencia de

un entero $h^-(K) \geq 1$ tal que

$$h(K) = h^+(K).h^-(K) \qquad (12)$$

Entonces Uchida [31] prueba el siguiente

Teorema 5.2 Para todo entero $h \geq 1$, existe sólo un número finito de cuerpos K abelianos imaginarios para los cuales $h^-(K) \leq h$.

Corolario 5.3 $h(K) = 1$ sólo para un número finito de cuerpos K abelianos imaginarios.

En particular, existe un número finito de cuerpos abelianos imaginarios K con $h(K) = 1$ y $Gal(K/Q) \approx Z_2^k$. Sea u su número total y u(k) su número para cada $k = 1,2,\ldots$. Ya hemos visto (Conjetura 3) que $u(1) = 9$. Brown y Parry [3] determinan todos los K para $k = 2$ y obtienen que $u(2) = 47$. Finalmente Uchida [32] resuelve el caso general y obtiene que $u(3) = 17$ y $u(k) = 0$ si $k > 3$. Luego $u = 73$.

Otra clase importante de cuerpos abelianos imaginarios la constituyen los cuerpos ciclotómicos $K = Q(\theta_m)$. Denotaremos $h_m = h(K)$, $h_m^+ = h^+(K) = h(K^+)$ y $h_m^- = h^-(K)$ si $K = Q(\theta_m)$. De tal manera se tiene, por (12), que

$$h_m = h_m^+.h_m^-$$

Hemos dicho en la Sección 2 que la resolución del U.T.F. para el primo $p > 2$ depende de la condición: $p \nmid h_p$. Como puede probarse (ver [2]) que

$$p \nmid h_p^- \Rightarrow p \nmid h_p^+$$

la condición se reduce a: $p \nmid h_p^-$. El estudio completo de esta condición sigue siendo un problema abierto, a pesar de que se han conseguido resultados importantes e interesantes.

El Corolario 5.3 nos asegura que $h_m = 1$ sólo para un número finito de valores de m. Su determinación en el caso m = p primo fue obtenida por Uchida [31] quien prueba:

Teorema 5.4 $h_p = 1 \Leftrightarrow 2 < p \leq 19$

Es decir, $h_p = 1$ sólo para los 7 primeros primos impares.

Antes de considerar el caso general, resuleto por Masley [22], observemos que si m es impar, $Q(\theta_{2m}) = Q(\theta_m)$ y, por lo tanto, podemos suponer que $m \not\equiv 2 \pmod 4$.

Un resultado que ayuda a resolver el problema de determinar los m con h_m pequeño es el siguiente (ver [23]).

Teorema 5.5 $h_m^- \mid h_{mk}^-$ para todo entero $k \geq 1$.

Corolario 5.6 Si $h_m = 1$ entonces $h_p^- = 1$ para todo primo impar p divisor de m.

Finalmente Masley dá la siguiente solución completa al Problema 1 en el caso de cuerpos ciclotómicos.

Teorema 5.7 $h_m = 1$ sólo para 29 valores de $m \not\equiv 2 \pmod 4$.

Ellos son los correspondientes a los 26 cuerpos ciclotómicos de grado $n = \varphi(m) < 21$ y $m = 35, 45$ y 84 (con $n = \varphi(m) = 24$)

El Corolario 5.3 nos muestra que si deseamos probar la Conjetura 1 con K abelianos, debemos restringirnos a los K reales. Estos son, según el Teorema de Kronecher-Weber, los subcuerpos de L^+ con $L = Q(\theta_m)$ para algún m. En particular, para m = p primo y n = 3 o n = 4 cíclicos, las tablas existentes impulsan a realizar conjeturas similares a la Conjetura 5 hecha para

$n = 2$.

En el caso de K no galoisiano, digamos que Williams [33] ha calculado una tabla de cuerpos cúbicos $K = Q(\sqrt[3]{p})$ con $p \equiv 2$ (mód. 3) primo y $p < 35100$ en la que $h(K) = 1$ para casi la mitad de los valores de p considerados.

Para terminar esta exposición, daremos la idea de un método debido a Masley [22] que permite, en algunos casos, acotar el valor de h(K) y que puede ser utilizado para construir cuerpos K con $h(K) = 1$. Como veremos, este método está relacionado con el problema de los discriminantes mínimos.

Diremos que K es de tipo (r_1, r_2) si posee r_1 primos infinitos reales y su grado es $n = r_1 + 2r_2$. Siendo K_1/K una extensión no ramificada, se tiene la siguiente

Proposición 5.8 Si K es de tipo (r_1, r_2) y $h = h(K)$, entonces K_1 es de tipo (hr_1, hr_2).

El problema de los discriminantes mínimos consiste en determinar, para cada par de enteros $r_1 \geq 0$ y $r_2 \geq 0$ el entero

$$M(r_1, r_2) = \min \{ |D_K| / K \text{ de tipo } (r_1, r_2) \}$$

Este problema sólo está resuelto para algunos valores pequeños de r_1 y r_2 (ver [25] y [26]).

Los mismos métodos geométricos de Minkowski con los que se demuestra que $|D_K| > 1$ para todo K, permiten concluir que $M(r_1, r_2)$ crece con n de manera que su raíz n-ésima se mantiene superior a un valor constante.

Hace pocos años Odlyzko, utilizando métodos analíticos, obtuvo constantes $Od(r_1, r_2)$ tales que

$$M(r_1, r_2)^{1/n} > Od(r_1, r_2)$$

muy superiores a las obtenidas con los métodos de Minkowski. Estas constantes crecen con n para cada $a = r_1/n$ fijo. En [26] se encuentra una tabla de dichas constantes para a = 1 (K totalmente real) y para a = 0 (K totalmente imaginario).

Denotemos, para cada cuerpo K de grado n, $rd(K) = |D_K|^{1/n}$. Es claro que si K es de tipo (r_1, r_2) entonces

$$rd(K) > Od(r_1, r_2) \qquad (13)$$

Sea L/K una extensión de grado k y no ramificada en ningún primo finito de K. Luego su discriminante relativo es A (ideal (1) de K) y por una conocida propiedad de los discriminantes ([25], Prop. 4.8) resulta que $D_L = D_K^k$. Tomando raíz n_1-ésima en la igualdad anterior con $n_1 = [L:Q] = k.[K:Q]$ queda demostrada la siguiente

Proposición 5.9 Si L/K es una extensión finita no ramificada en los primos finitos de K, entonces rd(K) = rd(L).

Corolario 5.10 $rd(K) = rd(K_1)$

De los resultados anteriores se deduce el siguiente teorema de acotación

Teórema 5.11 Sea K de tipo (r_1, r_2). Si $rd(K) < Od(mr_1, mr_2)$ entonces $h(K) < m$.

En efecto, si $h = h(K) \geq m$ se tendría que

$$rd(K_1) = rd(K) < Od(mr_1, mr_2) \leq Od(hr_1, hr_2)$$

y K_1 no verificaría la relación (13).

Si en el Teorema 5.11 se tiene $m = 2$, ya se puede asegurar que $h(K) = 1$. En caso contrario es suficiente verificar que $r_p(K) = 0$ para todo primo $p < m$ y en algunos casos esto puede hacerse fácilmente con la ayuda de los resultados conocidos sobre $r_p(K)$.

Si $K = Q(\theta_{23})$, $h_{23} = 3$ y $K_1 = K(\theta)$ con $\theta^3 - \theta - 1 = 0$. Con el método anterior puede probarse (ver [22]) que $h(K_1) = 1$. El grado $[K_1 : Q] = 22.3 = 66$ y hasta hace muy poco éste era el ejemplo de cuerpo K con $h(K) = 1$ de mayor grado conocido.

Recientemente Martinet [21], usando ideas similares, da dos ejemplos de cuerpos K de grado $n = 116$ y $h(K) = 1$ pero muestra que con estos métodos las constantes de Odlyzko no permitirán construir tales ejemplos con $n > 190$.

REFERENCIAS

[1] BAKER, A.: Linear forms in the logarithms of algebraic numbers. Mathematika 13 (1966), p. 204-216.

[2] BOREVICH, Z.I. y SHAFAREVICH, I.R.: Number Theory, Academic Press, 1967.

[3] BROWN, E. y PARRY, C.: The imaginary bicyclic biquadratic fields with class number 1. J.Reine. Angew. Math. 266(1974) p.118-120.

[4] BUELL, D.A.: Class groups of quadratic fields. Math. Comp. 30(1976), p.610-623.

[5] CARLITZ, L.: A characterization of algebraic number fields with class number two. Proc. A.M.S. 11(1960) p. 391-392.

[6] CASSELS, J.W.S. y FRÖHLICH, A., Eds.: Algebraic Number Theory, Academic Press, 1967.

[7] CHOWLA, S.: An extension of Heilbronn's class-number theorem. Quart. J. Math., Oxford Ser. 5 (1934), p.304-307.

[8] CRAIG, M.: Irregular Discriminants. Dissertation, University of Michigan, Ann. Arbor, Mich. (1972).

[9] CRAIG, M.: A construction for irregular discriminants. Osaka J. Math. 14 (1977), p.365-402.

[10] DIAZ y DIAZ, F.: On some families of imaginary quadratic fields. Math. Comp. 32 (1978), p.637-650.

[11] DIAZ y DIAZ, F.: Sur le 3-rang des corps quadratiques reels. (Preprint)

[12] DIAZ y DIAZ, F., SHANKS, D. y WILLIAMS, H.C.: Quadratic fields with 3-rank equal to 4. Math. Comp. 33 (1979), Nº 146, p.836-840.

[13] DICKSON, L.E.: Introduction to the Theory of Numbers. University of Chicago Press, 1929, (Dover, 1957).

[14] FRÖHLICH, A.: On non-ramified extension with prescribed Galois group. Mathematika 9 (1962), p.133-134.

[15] GAUSS, C.F.: Disquisitiones Arithmeticae, Göttingen, 1801 (Traducciones: Hermann, Paris, 1910 (francés); Chelsea Pub. Co, New York, 1965 (alemán); Yale, New Haven and London, 1966 (inglés)).

[16] GOLOD, E.S. y SHAFAREVICH, I.R.: On class field towers (en ruso).

Izv. Akad, Nauk. SSSR 28 (1964) p.261-272. (Traducido al inglés en A.M.S. Transl. (2) 48, p.91-102).

[17] HERZ, C.S.: Construction of class fields. En Seminar on Complex Multiplication. Springer Lecture Notes Nº 21 (1966), Exp. VII.

[18] JANUSZ, G.J.: Algebraic Number Fields, Academic Press, 1973.

[19] KASUBE, H.E.: Unique and almost unique factorization. En number Theory - Carbondale 1979 (ed. por M.B. Nathanson) Springer Lecture Notes Nº 751, p.200-205.

[20] LLORENTE, P.: Cuerpos Cúbicos y cuerpo de clases de cuerpos cuadráticos reales. 2do Congreso de Mat. de Venezuela (1979).

[21] MARTINET, J.: Petits discriminants. Ann. Inst. Fourier 29, 1(1979), p.159-170.

[22] MASLEY, J.M.: Odlyzko bounds and class number problems. En algebraic Number Fields (ed. por A. Fröhlich) Academic Press (1977), p.465-474.

[23] MASLEY, J.M.: Where are number fields with small class number?. En Number Theory- Carbondale 1979 (ed. por M.B. Nathanson). Springer Lecture Nº 751, p.221-242.

[24] MORDELL, L.J.: Diophantine Equations. Academic Press, 1969.

[25] NARKIEWICZ, W.: Elementary and Analytic Theory of Algebraic Numbers. Polish Sci. Publ., 1974.

[26] ODLYZKO, A.M.: On conductors and discriminants. En Algebraic Number Fields (ed. por A. Fröhlich), Academic Press, 1977, p.377-408.

[27] SCHOLZ, A.: Über die Beziehung der Klassenzahlen quadratischer Körper zveinander. Crelle's J. 166(1932), p.201-203.

[28] SHANKS, D.: Class number, a theory of factorization and genera. Proc. Sym. Pure Math. XX, A.M.S. (1971), p.415-440.

[29] SHANKS, D. and SERAFIN, R.: Quadratic fields with four invariants divisible by 3. Math. Comp. 27 (1973), p.183-187.

[30] STARK, H.M.: A complete determination of the complex quadratic fields of class-number one. Michigan Math. J. 14(1967), p. 1-27.

[31] UCHIDA, K.: Class numbers of imaginary abelian number fields I, II y III. Tohoku Math. J. 23(1971), p.97-104, p.335-348 y p.573-580.

[32] UCHIDA, K.: Imaginary abelian number fields with class number one. Tohoku Math. J. 24 (1972), p.487-499.

[33] WILLIAMS, H.C.: Certain pure cubic fields with class-number one. Math. Comp. 31(1977), Nº 138, p.578-580.

Universitat Autònoma de Barcelona (España)
Universidad del Zulia (Venezuela)