UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE CIENCIAS MATEMÁTICAS
Departamento de Álgebra

TESIS DOCTORAL

Cuerpos de números cúbicos : cálculo de unidades fundamentales

MEMORIA PARA OPTAR AL GRADO DE DOCTOR
PRESENTADA POR

Francisca Canovas Orvay

DIRECTOR:

Juan Ramón Delgado Pérez

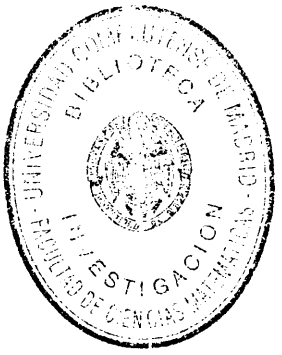
Madrid, 2015

UNIVERSIDAD COMPLUTENSE DE MADRID

Facultad de Ciencias Matemáticas

Departamento de Algebra y Fundamentos

CUERPOS DE NUMEROS CUBICOS. CALCULO DE UNIDADES FUNDAMENTALES



Francisca Cánovas Orvay

Madrid, 1990

Colección Tesis Doctorales. N.º 259/90

Edita e imprime la Editorial de la Universidad
Complutense de Madrid. Servicio de Reprografía
Escuela de Estomatología. Ciudad Universitaria
Madrid, 1990
Ricoh 3700
Depósito Legal: M-34299-1990

NC: X-53-164842-6

CUERPOS DE NUMEROS CUBICOS.

CALCULO DE UNIDADES FUNDAMENTALES.

TESIS DOCTORAL

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS MATEMATICAS

DEPARTAMENTO DE ALGEBRA Y FUNDAMENTOS

Autora: Doña Francisca Cánovas Orvay

Director: Don Juan Ramón Delgado Pérez

Fecha: Febrero de 1990

CUERPOS DE NUMEROS CUBICOS.

CALCULO DE UNIDADES FUNDAMENTALES.

DEPARTAMENTO DE ALGEBRA

FACULTAD DE CIENCIAS MATEMATICAS

UNIVERSIDAD COMPLUTENSE

28040 MADRID

A Francisco Javier, mi hijo.

A Francisco Javier, mi marido.

Porque han hecho posible esta experiencia.

RECORDATORIO

Esta tesis tiene que comenzar con la manifestación de mi recuerdo a todos los profesores del Departamento de Algebra de la Facultad de Matemáticas de la U.C.M. por el ánimo y colaboración que he recibido de ellos. En particular quiero agradecer a J.R. Delgado su ayuda pues sin ésta la tesis no se habría realizado. Quiero también mencionar a mis profesores de Geometría Algebraica Real, M.E. Alonso, M. Gamboa y C. Andradas.

Quiero recordar a todos mis compañeros de la E.T.S.I. Caminos de la U.P.M., en particular a A. Mendizábal, E. de la Rosa, C. Moreno, M. Soler y M. Fernández, para agradecer su apoyo a lo largo de todos los momentos de realización de esta tesis. Y debo volver a mencionar a M. Fernández que me ayudó a ganar la batalla con los ordenadores utilizados en la edición de esta tesis.

A los padres de Francisco Javier, mi marido, recordando su constante presencia con Francisco Javier, mi hijo.

Por último, que no en último lugar, a mis padres que, de forma indirecta, han estado presentes en todo momento.

INDICE

INTRODUCCION

INTRODUCCION

Desde un punto de vista académico, una tesis doctoral debe establecer resultados inéditos. No es sólo la novedad, empero, justificación suficiente para el espíritu crítico : por una parte, los problemas que se traten han de interesar realmente a la comunidad científica, lo cual se mide, razonablemente, por la pléyade de personas que los estudiaron con anterioridad; de otro lado, conviene que sean cuestiones con un nivel contrastado de dificultad, y de este segundo aspecto el lapso previo de investigación por otros autores suele ser testigo implacable. Estos dos requisitos, que pueden sintetizarse en la idea de raigambre, garantizan la exclusión de aquellos trabajos que, por estar planteados de modo artificial y ahistórico, resultan de exclusivo interés del propio autor. Dicho esto, consideramos delimitado con nitidez el objeto de la introducción que sigue.

En este trabajo estudiamos los cuerpos de números cúbicos, esto es, las extensiones algebraicas de Q de grado

tres*. Conocido es que los elementos de un cuerpo de números K que son enteros sobre Z forman un dominio de Dedekind, que en adelante denotaremos por R y conoceremos como el anillo de enteros algebraicos de K. Los que siguen son aspectos básicos de la aritmética de R : (i), estructura aditiva de R; (ii), el espectro primo de R; (iii), el número de clase y, (iv), la estructura multiplicativa del conjunto de unidades de R. Recordamos que R es un grupo abeliano libre cuyo rango coincide con la dimensión [K:Q] y que una base entera de R no es sino una Z-base de R; que cada ideal primo no nulo P de R yace sobre (o divide a) un único ideal primo no nulo pZ y, recíprocamente, cada primo no nulo pZ es divisible por algún primo P de R, de modo que, en el dominio de Dedekind que es R se verifica la descomposición $pR = P_1^{e1}...P_r^{er}$, siendo P_i los ideales primos que yacen sobre pZ, $e_i = e(P_i/Z)$ el índice de ramificación de P_i y $[K:Q] = e_1f_1 + ... + e_rf_r$, donde $f_i = f(P_i/Z) = |R/P_i|$ es el grado de inercia de P_i; que, por lo

---

* Los conceptos y teoremas que utilizamos en la tesis pueden encontrarse definidos o enunciados en la bibliografía que se detalla al final. No obstante, hemos creido conveniente añadir un capítulo de preliminares y, para facilitar la lectura de la introducción sin interrupciones, no dudaremos en intercalar todas las aclaraciones que sean precisas, aún a riesgo de resultar prolijos y redundantes.

que concierne a (iii), el número de clase (en adelante, h_K) es el orden (necesariamente finito) del grupo multiplicativo de ideales de R bajo la equivalencia $I \approx J$ si IJ^{-1} es un ideal fraccionario principal de R, y, finalmente, que el conjunto de unidades de R (en adelante, U_K) tiene estructura de grupo abeliano con la multiplicación, de suerte que, en virtud del teorema de las unidades de Dirichlet, U_K es finitamente generado : su torsión consiste exactamente en aquellas raíces de la unidad que están contenidas en K y el rango (sin torsión) es $r + s - 1$*.

Antes de exponer el contenido de cada capítulo de la tesis es preciso aludir a un invariante importante, a saber: el discriminante d_K, que es un entero racional igual al valor $\det(\text{traza}_{K/Q}(\alpha_i\alpha_j))$, común a toda base entera $(\alpha_1,\ldots,\alpha_n)$ de R, $n = [K:Q]$. Desde Dedekind se sabe que los primos que dividen al discriminante son justamente aquellos que ramifican en K**. En cierto modo, el discriminante permite determinar bases enteras: sea $(\alpha_1,\ldots,\alpha_n)$ una Q-base cualquiera de K y $\text{disc}(\alpha_1,\ldots,\alpha_n) = \det(\text{traza}_{K/Q}(\alpha_i\alpha_j))$ su

---

* r es el número de inmersiones reales de K y s el número de inmersiones complejas de K no conjugadas, de modo que se verifica $[K:Q] = r + 2s$.

** p ramifica en K si $e(P/Z) > 1$ para algún primo P de R que yazca sobre p.

su discriminante*; $(\alpha_1,\ldots,\alpha_n)$ es una base entera si y sólo si $\text{disc}(\alpha_1,\ldots,\alpha_n) = d_K$. En general, el cociente $\text{disc}(\alpha_1,\ldots,\alpha_n)/d_K$ coincide con el cuadrado del índice $|R:M|$ del subgrupo M de R generado por $\alpha_1,\ldots,\alpha_n$**, supuesto que cada $\alpha_i \in R$.

El capítulo I está dedicado, por este orden, a la obtención de bases minimales en cada primo, estudio del discriminante, bases enteras de ciertas familias infinitas de cuerpos cúbicos y caracterización de la monogeneidad***. Las dos primeras cuestiones se utilizan exhaustivamente a lo largo de la tesis y las dos restantes pueden entenderse como aplicaciones de las bases minimales obtenidas. Es de destacar que dichas cuestiones son resueltas en función exclusivamente de los coeficientes de un polinomio de definición.

La existencia de bases enteras está garantizada desde el punto de vista teórico. Métodos para encontrar bases enteras de un cuerpo cúbico son dados , independientemente, por

---

* Obviamente, $\text{disc}(\alpha_1,\ldots,\alpha_n)$ es un número racional, que es entero si y sólo si cada α_i es elemento de R.

** Cuando la base está formada por las potencias $1, \alpha, \ldots, \alpha^{n-1}$ de $\alpha \in R$, el correspondiente índice se llama índice de α, y se denota $i(\alpha)$.

*** Un cuerpo de números se dice monogénico si existe un entero de índice igual a 1.

Mathews ([Ma]) en 1893 y por G.T. Woronoj ([V]) en 1894. Entre los métodos para encontrar bases enteras de cuerpos de números de grado n citaremos al que da W.E.H. Berwick en 1927 ([Bel]) y, más recientemente, al de Harvey-Cohn ([HC2], th. 9.28).

Fórmulas elementales explícitas para bases enteras de un anillo de enteros han sido dadas sólo en el caso cuadrático y para ciertos tipos de cuerpos (ciclotómicos, cúbicos puros, bicuadráticos). Nosotros vamos a considerar el caso cúbico. Los primeros resultados conocidos en este caso datan de 1929 y son los de A. Adrian Albert ([A]). Sus resultados determinan bases enteras para cuerpos cúbicos en términos de funciones numéricas (función de Euler) de los coeficientes de un polinomio de definición del cuerpo en cuestión. Las expresiones a las que llega A.A. Albert son, a nuestro parecer, engorrosas y poco operativas. Con una prueba más sencilla y con resultados un poco más simples, en 1955, L. Tornheim ([To]) da una fórmula explícita de una base minimal en términos de los coeficientes de un polinomio de definición de K, cuerpo de números cúbico. Si bien deja pendiente a resolver, en cada caso particular, un sistema de congruencias a solucionar, por ejemplo, aplicando el teorema de los restos chinos.

La computación de bases enteras es sencilla, en comparación con otros problemas computacionales de la Teoría Algebraica de Números, como pueden ser el cálculo del número

de clase, la estructura del grupo de clase o la obtención de unidades fundamentales . El conocimiento de bases enteras nos permitirá en el capítulo tercero obtener sistemas fundamentales de unidades expresados por medio de coeficientes relativos a dichas bases, lo que mejora sustancialmente aquellas tablas que se limitan a dar polinomios irreducibles de dichas unidades.

A nosotros se nos ha facilitado un disco, por la Universidad de Burdeos, que permite obtener bases enteras en cuerpos generales de grado n , una vez asignados valores a los coeficientes de un polinomio de definición. Pero es claro que estos resultados computacionales se limitan a ser una secuencia de valores numéricos . En este sentido, se gana generalidad con nuestro estudio que permite obtener bases enteras en términos exclusivamente de los coeficientes de un polinomio de definición.

En este capítulo, se utiliza el teorema 9.28. de Harvey-Cohn ([HC2]), que se aplica, según los casos, a la base natural de potencias del elemento primitivo θ y a una segunda base que tiene en cuenta el entero θ_1, que juega un papel destacado en varios puntos de la tesis. Este entero θ_1 aparece por vez primera en ([D1])*.

---

* En el capítulo III se prueba un resultado que nos parece de gran importancia, a saber : existe una correspondencia

El discriminante de un cuerpo de números dado es un invariante de gran importancia. Contiene entre sus factores primos a todos los que son ramificados. También nos permite conocer el índice de un elemento dado y ya veremos la importancia que ello tiene al estudiar la descomposición en R de un primo de Z. Otra aplicación del discriminante es la identificación de bases enteras. En 1983, Pascual LLorente y Enric Nart [L,N] calculan el discriminante de un cuerpo de números cúbico.Nosotros, como corolario inmediato del estudio realizado sobre bases minimales, obtenemos el discriminante de K en términos de los coeficientes de un polinomio definición del mismo. Ambos resultados, obtenidos por vías distintas, están en concordancia.

Obtenido el discriminante de un cuerpo de números cúbico y determinada una base entera, es posible expresar el discriminante de una base de potencias como el producto del discriminante del cuerpo por un cuadrado; dicho cuadrado es el cuadrado de una forma binaria cúbica F(x,y) que se denomina forma indicial. La forma indicial se conoce en el

---

biyectiva entre cuerpos cúbicos cíclicos de discriminante p^2 y polinomios cúbicos irreducibles $x^3 - px + pq$, donde $(p,q) = 1$ y $4p - 27q^2 \in Z^2$. La prueba que damos de este hecho descansa en el previo conocimiento de θ_1. En el capítulo II, θ_1 se utiliza, en muchos casos, para poder aplicar el lema de Kummer en la descomposición de primos racionales en K.

caso cúbico puro tras M. Hall ([H]). Nosotros obtenemos dicha forma para diversas familias infinitas de cuerpos cúbicos. No conocemos otra referencia para este problema concreto.

Un cuerpo de números es monogénico cuando $F(x,y) = \pm 1$ es resoluble en enteros; dicha ecuación es una ecuación de Thue, y se conocen pocos resultados incluso para su resolubilidad. Bombieri y Schmidt ([B,S]) recientemente han publicado artículos al respecto. La caracterización que damos de la monogeneidad para familias infinitas de cuerpos cúbicos está en función de la ecuación diofántica mencionada.

El capítulo II de esta tesis es un estudio de los ideales primos de un cuerpo cúbico K arbitrario. Se resuelven los siguientes aspectos del problema :

(i) descomposición de un primo racional en el anillo de enteros de K, con la determinación, en cada caso, de los índices de ramificación y grados de inercia;

(ii) obtención de un par de generadores de cada ideal primo de K;

(iii) norma de cada ideal primo de K.

La novedad en cada apartado radica en que todo se hace en función de un polinomio de definición del cuerpo.

En 1983, Llorente y Nart ([L,N]) estudiaron el apartado (i); la solución que nosotros hemos dado a (ii) e (iii) añade

a los resultados de Llorente y Nart la descomposición exacta de los primos racionales en K. Por otra parte, los métodos que nosotros hemos utilizado en el estudio de (i) son distintos a los utilizados por Llorente y Nart, lo que está justificado porque a dichos autores no les interesa determinar quienes sean los ideales de la descomposición. En consecuencia, nuestro estudio es mucho más detallado porque cada uno de los casos que Llorente y Nart consideran encierra diversas posibilidades para cada uno de los ideales de la descomposición*.

Anteriormente, Hasse (en 1930) y Martinet y Payan (en 1967), (véase [Ha], [M,P]), estudiaron las ramificaciones de K cúbico no cíclico **. Pero, como Llorente y Nart también

---

* Así, por ejemplo, el caso $p|a$, $p|b$, $p > 3$ primo considerado por Llorente y Nart les conduce a la descomposición $p = P^3$, $p = PQ^2$, dependiendo de que $1 \leq v_p(b) \leq v_p(a)$ ó $1 = v_p(a) < v_p(b$; para determinar quienes son P y Q, de nuestro estudio se deduce que :

$$p = \begin{cases} (p,\theta^2/p)^3 \text{ si } a, b \equiv 0(p^2),\ b \not\equiv 0(p^3). \\ (p,\ \theta^2/p + \theta)(p,\ \theta^2/p + \theta - a/p)^2 \quad \text{si } a \equiv 0(p), \\ \qquad\qquad b \equiv 0(p^3),\ a \not\equiv 0(p^2). \\ (p,\ \theta^2/p)(p,\ \theta^2/p - a/p)^2 \quad \text{si } a \equiv 0(p),\ b \equiv 0(p^2), \\ \qquad\qquad a \not\equiv 0(p^2),\ b \not\equiv 0(p^3). \\ (p,\ \theta)^3 \quad \text{si } a,b \equiv 0(p),\ b \not\equiv 0(p^2). \end{cases}$$

** El caso cúbico cíclico ya estaba estudiado, véase[D,F].

destacan, sus resultados no permiten obtener la descomposición en términos de un polinomio definición del cuerpo y, en cualquier caso, sólo tratan la cuestión (i).

Finalmente, en 1989 Pohst y Zassenhaus ([P,Z]) han estudiado, desde el punto de vista computacional, la cuestión que consiste en determinar los ideales de norma menor o igual que un entero dado, con vistas a su aplicación al cálculo del número de clase*.

Todo nuestro estudio del capítulo II se basa en los resultados del capítulo anterior y la utilización del lema de Kummer**, con el recurso eventual al teorema 10.61 de Harvey-Cohn ([HC2]. Llorente y Nart también basaron su trabajo en el lema de Kummer; pero, dado que ellos mantienen invariable el elemento primitivo del cuerpo cúbico, normalmente no están en las condiciones de aplicación de dicho lema y recurren al

---

* La diferencia, por lo demás obvia, entre nuestro estudio y el punto de vista computacional estriba en que, por ejemplo, mediante los métodos del segundo se sabe que el único ideal de norma 3 del cuerpo cúbico asociado a $\theta^3 - 2\theta + 6$ es el ideal $(3,\theta)$, mientras que, a partir de nuestro trabajo se conoce que $(3,\theta)$ es el único ideal primo de norma 3 para la familia infinita de cuerpos cúbicos con polinomio de definición $x^3 - (3a + 2)x + 3b$.

** En el capítulo de preliminares se encuentra enunciado.

polígono de Newton. Nosotros evitamos esta situación del modo siguiente : dado que en el capítulo I se han obtenido bases minimales $\{ 1, \alpha_1, \alpha_2 \}$ relativas a cada primo racional p, en términos exclusivos de un polinomio de definición, se han utilizado como elementos primitivos alternativos α_1, α_2, $\alpha_1 \pm \alpha_2$ y, en un único caso, $2\alpha_1 + \alpha_2$. Y, de este modo hemos estado en condiciones de aplicar el lema de Kummer. Hemos optado por la utilización continuada de este lema porque en el caso cúbico el único primo que puede dividir al máximo común divisor de los índices de todos los enteros algebraicos es p = 2, en virtud del conocido teorema de Zylinsky (1913); más aún, cuándo 2 es el máximo común divisor de dichos índices lo determinó Engstrom en 1930, ([E]),* y Llorente y Nart ([L.N]) mejoran el resultado anterior al establecerlo en términos de los coeficientes de un polinomio de definición del cuerpo.

La descomposición exacta en K cuerpo de números cúbico de un primo racional será utilizada en el capítulo III, a la hora de construir entensiones abelianas no ramificadas de K en orden a dar criterios sobre la paridad del número de clase.

---

* En concreto, 2 es máximo común divisor de los índices de todos los enteros de K cuerpo de números cúbico si y sólo si 2 descompone completamente en K.

En el capítulo III se encuentran las conclusiones más significativas de nuestro trabajo. Dicho capítulo trata sobre los cuerpos cúbicos cíclicos (i.e., con grupo de Galois cíclico sobre el cuerpo racional) y, en gran medida, los resultados que obtenemos dependen del primer capítulo.

En primer lugar, se demuestra , en términos elementales, que el discriminante de un tal cuerpo es de la forma p^2 con $p = 3^{\delta}p_1...p_r$, $\delta \in \{0,2\}$, $p_i \equiv 1 \ (3)$ primos distintos dos a dos; la única demostración que conocemos de este hecho se debe a Heilbronn [He], quien utiliza para ello teoría del cuerpo de clase.

El segundo resultado importante de nuestro estudio de cuerpos cúbicos cíclicos establece una correspondencia biyectiva entre cuerpos cúbicos cíclicos y una agradable familia de polinomios que los definen. En concreto, se prueba que todo cuerpo cúbico cíclico K coincide con un único cuerpo cúbico cíclico $K_{(p,q)}$ generado (sobre Q) por una raíz del polinomio $x^3 - px + pq$, donde $p = 3^{\delta}p_1...p_r$ satisface las condiciones arriba citadas, q es un entero positivo tal que $(p,q) = 1$ y $4p - 27q^2 \in Z^2$. Este resultado creemos que es inédito; lo que se conoce al respecto es una correspondencia biyectiva entre los cuerpos cúbicos cíclicos y ciertos enteros algebraicos del cuerpo cuadrático $L = Q((-3)^{1/2})$, tal que si K es cúbico cíclico de discriminante p^2, se le puede asociar un único $\sigma = (\alpha + 3\beta(-3)^{1/2})/2 \in Q((-3)^{1/2})$ sujeto a las condiciones :

(i) $N_Q^L(\sigma) = p$;

(ii) $\beta > 0$, $\alpha \equiv 1(3)$ si $p \equiv 1(3)$;

(iii) $\alpha = 3\alpha'$, $\alpha' \equiv 1(3)$, $\beta \not\equiv 0(3)$ si $3|p$.

(iv) $KL = L((p\sigma)^{1/3})$.

Además, un polinomio definición de K viene dado por :

$x^3 + x^2 + ((1 - p) / 3)x - (p(3 + \alpha) - 1)/ 27$ si es no ramificado en K,

$x^3 - (p / 3)x - (\alpha p) / 27$ si 3 es ramificado en K.

Utilizando los resultados de nuestro primer Capítulo hemos sido capaces de transformar dicho polinomio de definición de K en un polinomio del tipo $x^3 - px + pq$; en esta breve introducción conviene destacar que el punto crucial para obtener lo anterior es el conocimiento del entero θ_1 obtenido por nosotros en el primer capítulo.

La filosofía subyacente a este asunto es bastante sutil; mientras que en el capítulo I se obtiene el discriminante a partir de un polinomio que defina al cuerpo, ahora el proceso se invierte : como sabemos que los cuerpos cúbicos cíclicos están caracterizados por tener discriminante p^2, el problema radica en, fijado p, determinar un polinomio con coeficientes en función de p en términos de una sencillez tal que nos permitiera efectuar los "cálculos" de todo el capítulo.

Por otra parte, el carácter de nuestros polinomios de

definición dan una regla sencilla que permite el listado de todos los cuerpos cúbicos cíclicos de discriminante dado, evitando repeticiones.

A continuación, centramos el estudio en la determinación de sistemas fundamentales de unidades para los cuerpos cúbicos cíclicos. Una somera descripción histórica de este asunto nos ayudará a situar el problema.

Lo primero que hay que resaltar es el tratamiento claramente computacional que ha sufrido el problema de las unidades: es decir, parece claro que no se puede determinar sistemas de unidades fundamentales en función de los coeficientes de un polinomio de definición, lo que se observa ya en el caso cuadrático. Dicho esto, hay que resaltar los esfuerzos teóricos que se han hecho para caracterizar las unidades fundamentales. Nos referiremos a estas dos caras de la misma moneda en el caso que nos concierne (cuerpos cúbicos cíclicos y, más generalmente, cuerpos cúbicos totalmente reales*).

Las tablas publicadas en que se listan un par de unidades fundamentales de cuerpos cúbicos totalmente reales son escasas. La primera que conocemos se debe a Billevich,

---

* Es decir, con discriminante positivo y, por tanto, con dos unidades fundamentales independientes.

([Bi]), data de 1956 y se limita a los 33 cuerpos cúbicos totalmente reales de discriminante menor que 1300. En cada caso, este autor da el discriminante del cuerpo, una base entera, un polinomio de definición y los coeficientes de un par de unidades fundamentales con respecto a la base citada. El método que utiliza Billevich es propio, pero en 1976 Steiner y Rudman [S,R] muestran las dificultades computacionales de este método para discriminantes superiores a los considerados por el propio Billevich.

La segunda de estas tablas publicadas se debe a Williams y Zarnke. Está fechada en 1972 y contiene un par de unidades fundamentales para varios cuerpos definidos por ecuaciones cúbicas irreducibles. Por ejemplo, lista los coeficientes de un par de unidades fundamentales con respecto a una base entera para todos los cuerpos cúbicos totalmente reales definidos por $x^3 - px - q = 0$, con $|p|, |q| \leq 15$. Sin embargo, no se calcula el discriminante y se echa en falta un estudio que indique cuándo pares (p, q) diferentes definen el mismo cuerpo. El método que utilizan en su estudio es el de Voronoi, al que nos referiremos más adelante.

Recientemente han aparecido dos nuevas tablas debidas a Cusick y Schoenfeld [C,L], la primera, y a Pohst y Zassenhaus, la segunda.

El trabajo de los primeros se basa en un estudio teórico previo de Cusick [C1], [C2] y, su tabla contiene un par de

unidades fundamentales de cuerpos cúbicos totalmente reales con discriminante menor que 6885.

Sus resultados vienen condicionados a nuestro entender, fuertemente porque consideran la mayor de las raíces del polinomio de definición, lo que obliga a computar las tres raíces y, en conclusión, todos sus resultados son aproximados.

Finalmente, la tabla de Pohst y Zassenhaus se incluye, como apéndice, en su libro publicado en 1989. Los cuerpos cúbicos totalmente reales que se consideran tienen discriminante menor que 1000. El tratamiento que utilizan es directo y pensamos que esto dificulta la computación.

Los estudios teóricos que han permitido obtener métodos de cálculo de unidades fundamentales en cuerpos cúbicos se deben, básicamente, a Voronoi, Berwick, Godwin y Cusick.

El de Voronoi es el más antiguo, data del siglo pasado y las referencias que conocemos destacan que es fuente de numerosos errores, hasta el punto que alguna tabla no se ha podido publicar por este motivo. Básicamente es una generalización del método de las fraccciones continuas de Lagrange.

El trabajo de Berwick [Bel] se centra en el estudio de unidades fundamentales cuando $r + s - 1 = 2$, esto es, cuando

los sistemas fundamentales de unidades constan de dos unidades. El estudio de Berwick hasta el momento no ha dado lugar a ninguna tabla; la aplicación más destacada que conocemos del trabajo de Berwick se debe a Thomas [T], que estudia unidades en órdenes cúbicos monogénicos, lo que resta generalidad a sus resultados. No obstante, dado que la familia $U = \{ Q(\theta) : \theta^3 - n\theta - (n+3)\theta - 1 = 0 , n \in Z \}$ es monogénica cuando $n(n+3) + 9$ es libre de cuadrados, le permite determinar que $\{ \theta, \theta + 1 \}$ es un sistema fundamental de unidades del anillo de enteros de $Q(\theta)$, bajo la citada condición. En cualquier caso, pensamos que en nuestra tesis se obtienen estos resultados con más sencillez. Nos referiremos a esta familia con más detalle al explicar nuestra tabla; la familia U ha sido tratada por diversos autores : Harvey-Cohn [HC1], K. Uchida [U], E. Thomas [T], M.N. Gras [G3] y M. Watabe [Wi], siendo i = 1,....,6, etc. Cómo surge la consideración de dicha familia no parece claro; al parecer H.Cohn fue el primero en tratarla, en 1956. En nuestra tesis, el estudio de esta familia U surge de un modo natural, al observar determinadas coincidencias que se verifican en nuestra tabla; de hecho, estamos en situación de asignar a los cuerpos de esta familia U polinomios de definición mucho más sencillos, a saber : $x^3 - px + p$, siendo p el discriminante del cuerpo. En este sentido, ninguno de los autores citados ha establecido una relación entre la familia U y los discriminantes a que da lugar.

El estudio de Godwin [Go1] es el que servirá de

referencia en nuestro trabajo. Cusick [C1],[C2] aporta, según él, una mejora al estudio de Godwin.

En 1960, H.J. Godwin enuncia una conjetura sobre las unidades de cuerpos cúbicos totalmente reales. Para un tal cuerpo K, define la función (que llamaremos de Godwin) $S(\alpha) = (1/2)[(\alpha - \alpha')^2 + (\alpha - -\alpha'')^2 + (\alpha'- \alpha'')^2]$ para $\alpha \in K$. La conjetura establece que si $S(\mu)$ es mínimo en el conjunto de las unidades de norma positiva distinta de la unidad y $S(\tau)$ es mínimo en el conjunto de las unidades de R de norma positiva distinta de μ^n para n entero, entonces (μ,τ) forma un sistema fundamental de unidades de K, supuesto que $S(\mu) > 9$. Veinte años después, M.N. Gras [G3] demuestra dicha conjetura en el caso particular de que K sea cúbico cíclico; dado que esta es la situación que interesa a nuestro estudio, en adelante hablaremos del teorema de Godwin en el contexto de cuerpos cúbicos cíclicos. En 1987, Ennola Veikko [Ve] ha probado la conjetura de Godwin a excepción de un número finito de casos que se pueden explicitar a partir de su demostración.

En cuanto al estudio de Cusick [C1], [C2], la diferencia sustancial respecto a Godwin consiste en considerar la función $S(\alpha) = Tr(\alpha^2)$ en lugar de la citada en el párrafo anterior.

Volviendo al contenido de la tesis, tras obtener el discriminante y un polinomio definición de K cuerpo de

números cúbico cíclico, nos proponemos deducir un método computacional de cálculo de unidades fundamentales a partir del teorema de Godwin. Del teorema de Godwin se tiene que, acerca de μ, hay que imponer las condiciones :

(i) $S(\mu)$ mínima.

(ii) μ unidad de norma positiva, $\mu \neq 1$.

Para efectuar (i), es preciso expresar los elementos del anillo de enteros de K en función de una adecuada base entera*; dicha base se obtiene en esta capítulo III sirviéndonos del primer capítulo. En principio, utilizamos el discriminante para asegurar la existencia de una determinada base entera; cómo sea de hecho, tal base se concluye una vez estudiada la función S de Godwin**.

Una vez expresada μ en función de la base se observa que $S(\alpha) = S(u\sigma + v\tau)$, donde $\alpha = x + u\sigma + v\tau$, con $x, u, v \in Z$ y $\{1,\sigma,\tau\}$ es la base entera a que hacemos referencia. Esta simplificación permitirá expresar la función S como una forma cuadrática en u y v con coeficientes enteros en lugar de una

---

* El hecho de que dicha base entera sea adecuada no es superfluo; por ejemplo, Cusick considera una base entera que depende de la mayor raíz del polinomio de definición, lo que implica el carácter aproximado de las unidades que obtiene.

** Véase comentario al lema 3.5.

forma cuadrática ternaria, que se deduciría inevitablemente del estudio de Cusick. En los teoremas 3.8 y 3.13 se determina la forma cuadrática a que hacemos referencia, el valor exacto de $S(\alpha)$ y, como conclusión, se obtiene la base entera $(1,\sigma,\tau)$ citada arriba.

En cuanto a la condición (ii), consiste en resolver la ecuación de norma $N_Q^K(x + u\,\sigma + v\tau) = 1$; dicha ecuación se estudia en las proposiciones 3.9 y 3.14, de modo que, fijados u y v la condición (ii) se limita a una ecuación cúbica en una variable entera que es función lineal de x.

Obtenida μ, y por estar en el caso cúbico cíclico, tomaremos τ igual a una conjugada de μ^*.

A la vista de estos resultados la computación de sistemas fundamentales de unidades de cuerpos cúbicos cíclicos se

---

* En el teorema de Godwin hay una condición adicional y es $S(\mu) > 9$. Dado que nosotros demostramos que $S(\alpha)$ es un múltiplo de p, siendo p^2 el discriminante del cuerpo, para cada $\alpha \in R$, los únicos casos a los que no podemos aplicar el teorema de Godwin son p = 7, 9. Estos casos están dentro de la que llamaremos familia U, y el sistema fundamental de unidades que damos para los cuerpos cúbicos cíclicos de esta familia es válido también en los casos p = 7, 9, según se deduce del estudio realizado por Thomas [T].

puede hacer sin grandes dificultades. En nuestro caso, nos hemos limitado al caso de los cuerpos cúbicos cíclicos de discriminante menor que $16 \cdot 10^6$, dado que M.N. Grass [G2] publicó una tabla (a la que luego dedicaremos un comentario) que cubría dicho rango de discriminante. Nuestra tabla especifica : todos los cuerpos cúbicos cíclicos de discriminante menor que $16 \cdot 10^6$, dando un polinomio de definición del cuerpo de la forma $x^3 - px + pq$; una base entera para dicho cuerpo; los coeficientes, respecto a dicha base, de varios sistemas de unidades fundamentales; la traza de cada unidad obtenida y el valor de la función S de Godwin para cada unidad (que no es sino el mínimo aludido de dicha función).

Por ejemplo, si K denota al único cuerpo cúbico cíclico de discriminante 1951^2, entonces $K = Q(\theta)$, donde θ es raíz del polinomio $x^3 - 1951x + 1951 \cdot 17$; una base entera es $(1, \sigma, (9\sigma + \sigma^2)/17)$, donde $\sigma = (-1 + \theta_1)/3$ y $\theta_1 = 4 \cdot 1951 - 9 \cdot 17\theta - 6\theta^2$; las siguientes unidades $2 + 3\sigma + 3((9\sigma + \sigma^2)/17)$, $-1 - 6\sigma + 3((9\sigma + \sigma^2)/17)$, $-230 - 3\sigma + 6((9\sigma + \sigma^2)/17)$ tienen traza, en valor absoluto, 231 y, tomadas de dos en dos, determinan un sistema de unidades fundamental; las unidades $1 + 3\sigma + 3((9\sigma + \sigma^2)/17)$, $-2 - 6\sigma + 3((9\sigma + \sigma^2)/17)$, $-229 - 3\sigma + 6((9\sigma + \sigma^2)/17)$ tienen traza, salvo el signo, 228 y, cualquier par de dichas unidades es un sistema fundamental. En los seis casos, se obtiene que la función S de Godwin vale $27 \cdot 1951$ y éste es el mínimo de tal función en el conjunto de las unidades

distintas de ± 1.

La única limitación de nuestra tabla viene dada por la precisión del lenguaje de programación utilizado, Fortran 77.

La tabla de Gras que hemos citado se limita a listar polinomios de definición de cuerpos cúbicos cíclicos en función del discriminante y el polinomio de definición de una unidad, dado que calcula su traza y la traza de la unidad inversa. No obtiene bases enteras ni unidades, tal como acertadamente comentan Cusick y Schoenfeld [C,L]. Es de destacar que nosotros siempre obtenemos tres sistemas de unidades fundamentales tal que la traza de una de tales unidades coincide, salvo el signo, con las trazas de la tabla de Gras.

De la bibliografía consultada, se desprende que la tabla que nosotros presentamos es la única que permite deducir consecuencias y abstraer resultados generales para determinadas familias infinitas. En concreto, en nuestra tesis conjeturamos y probamos los resultados que, a continuación, pasamos a detallar*.

---

* Más aún, "traduciendo" a nuestro lenguaje la tabla de Gras, hemos observado determinadas relaciones generales en su tabla que él mismo parece haber sido incapaz de establecer. De hecho, su tabla 4 sólo se explica por este desconocimiento.

Un análisis de la tabla de unidades fundamentales que construimos nos lleva a considerar las familias :

$U = \{ K = Q(\theta) : Irr(\theta, Q) = x^3 - px + p$ siendo $p = 3^{\delta} p_1 \cdots p_r$ con $p_i \equiv 1 \ (3)$ primo distintos dos a dos, $\delta \in \{ 0, 2 \}$, $4p - 27 \in Z^2 \}$,

$V = \{ K = Q(\theta) : Irr(\theta, Q) = x^3 - px + pq$ siendo $p = p_1 \cdots p_r, p_i \equiv 1 \ (3)$ primo y distintos dos a dos, $q > 2$, $4p - 27q^2 = 1 \}$,

$W = \{ K = Q(\theta) : Irr(\theta, Q) = x^3 - px + pq$ siendo $p = 9\, p_1 \cdots p_r$, $p_i \equiv 1 \ (3)$ primo y distintos dos a dos, $q > 2$, $4p - 27q^2 = 9$, $3 \nmid q \}$.

La primera familia U ha sido considerada, entre otros, por Harvey - Cohn [HC1], K.Uchida [U], E.Thomas [T], M.N. Gras [G3] y M. Watabe [W1],...,[W6] entre 1956 y 1984.

Para cada una de las familias U, V y W damos un sistema fundamental de unidades $\{ \mu, \mu' \}$. En cada caso, el sistema de unidades dado viene sugerido tras el análisis de la tabla; la demostración de que en efecto es un sistema de unidades fundamentales es realizada utilizando el teorema de Godwin.

Además, la unidad fundamental μ tiene, en cada caso, la buena propiedad de ser no totalmente positiva. Así, toda unidad u de R totalmente positiva (u y sus conjugados son

positivos) es necesariamente un cuadrado en R. Utilizando este hecho, construimos un criterio sobre la paridad del número de clase para las familias V y W. Lo que hace en cada caso es dar sencillas condiciones suficientes para garantizar la existencia de un elemento de R totalmente positivo que no sea un cuadrado en R y que el ideal que engendre sea un cuadrado. A continuación, enunciamos los teoremas que recogen dichos resultados:

Teorema 3.13 : Sea $K = Q(\theta)$ cuerpo de números cúbico cíclico de discriminante p^2 perteneciente a la familia U. Entonces:

(i) (σ,σ') es un sistema fundamental de unidades de K ,

(ii) K es monogénico y $(1, \sigma, \sigma^2)$ base entera de K, siendo $\sigma = (m + \theta 1)/3$, $m = ((4p - 27)^{1/2} - 3)/2)$, $\theta 1 = (4p - 9\theta - 6\theta^2)/(4p - 27)^{1/2}$ y σ' es un conjugado de σ.

Teorema 3.14: Sea $K = Q(\theta)$ cuerpo de números cúbico cíclico de discriminante p^2 perteneciente a la familia V. Entonces:

(i) K es monogénico y $(1, \theta, \theta^2)$ es base entera de K.

(ii) $\mu = 2 + 3\sigma + 3((\sigma^2 + ((q + 1)/2)\sigma)/q$ es una unidad de R. $(\sigma = (-1 + \theta 1)/3, \theta 1 = 4p - 9q\theta - 6\theta^2)$.

(iii) (μ,μ') es un sistema fundamental de unidades de K; $\mu' = -1 - 6\sigma + 3((\sigma^2 + ((q + 1)/2)\sigma)/q)$ es un conjugado de μ.

(iv) $Irr(\mu,Q) = x^3 - 3((1 + 9q)/2)x^2 + ((27q - 3)/2)x + 1$

(v) μ no es totalmente positiva.

Teorema 3.15.: Sea $K = Q(\theta)$ cuerpo de números cúbico cíclico de discriminante p^2 perteneciente a la familia W. Entonces:

(i) $(1, \theta, \theta^2/3)$ y $(1, \sigma, (((q-1)/2) + ((q-1)/2)\sigma + \sigma^2)/q)$ son bases enteras de K.

$(\sigma = \theta 1/3,\ \theta 1 = 4(p/3) - 3q\theta - 2\theta^2)$.

(ii) $\mu = (9(q-1) + 3(3q-1)\theta 1 + 2\theta 1^2)/(18q)$ es una unidad de R.

(iii) (μ,μ') es un sistema fundamental de unidades de K; μ' es un conjugado de μ,

$\mu' = (9(q-1) - 3(3q+1)\theta 1 + 2\theta 1^2)/(18q)$.

(iv) $Irr(\mu,Q) = x^3 - ((3+9q)/2)x^2 + ((9q-3)/2)x + 1$.

(v) μ no es totalmente positiva.

Teorema 3.16.: Sea $K = Q(\theta)$ cuerpo de números cúbico cíclico de discriminante p^2 perteneciente a la familia V. Si q es un cuadrado (en Z) y $(1 + 3q)/2$ no es un cuadrado en Z_{qi} para al menos un qi divisor primo de q, entonces el número de clase de K es par.

Teorema 3.17.: Sea $K = Q(\theta)$ cuerpo de números cúbico cíclico de discriminante p^2 perteneciente a la familia W. Si q es un cuadrado (en Z) y $(3 + 3q)/2$ no es un cuadrado en Z_{qi} para al menos un qi divisor primo de q, entonces el número de clase de K es par.

Para la familia U ya tenemos los criterios sobre la paridad

del número de clase dados por Harvey - Cohn [HC1] y M. Watabe [W4], [W5].

En 1935, Siegel demostró que si F es un cuerpo cuadrático imaginario con discriminante disc(F) y número de clase h_F entonces h_F ---> ∞ cuando | disc(F) | ---> ∞. Para probar esto Siegel utilizó la fórmula

$$\lim_{disc(F) \to \infty} (\log(h_F R_F)/\log(|disc(F)|^{1/2})) = 1$$

siendo R_F el regulador de F,

la cual fue establecida primero por Siegel para cuerpos cuadráticos F, y Brauer [B] para cuerpos de números algebraicos F generales (fijado el grado).

Utilizando dicha fórmula y los sistemas fundamentales de unidades obtenidos en los teoremas 3.14 y 3.15, estudiamos el comportamiento del número de clase cuando el discriminante converge a +∞ para los cuerpos de números cúbicos de la familia V y W. Los resultados obtenidos son :

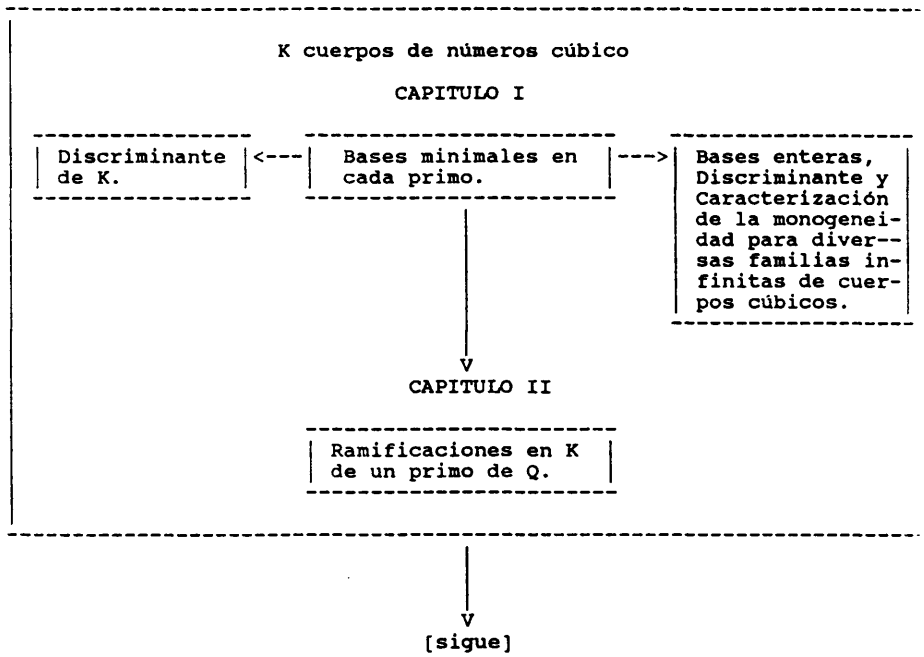
Teorema 3.18: Sea K = Q (θ) cuerpo de números cúbico cíclico de discriminante p^2 perteneciente a la familia V. Entonces $\lim_{p \to +\infty} h_K = +\infty$.

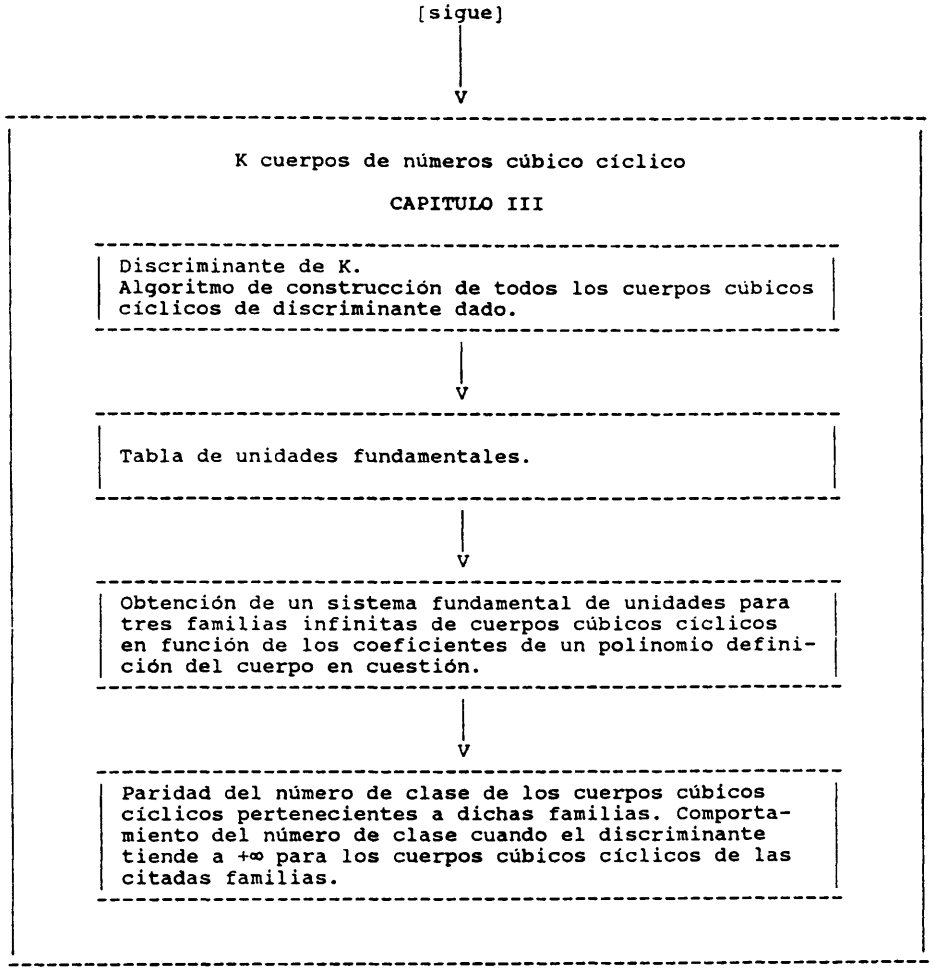
Teorema 3.19.: Sea K = Q (θ) cuerpo de números cúbico cíclico de discriminante p^2 perteneciente a la familia W. Entonces $\lim_{p \to +\infty} h_K = +\infty$.
(h_K es el número de clases de K).

Un estudio análogo para la familia U ha sido realizado, en 1983, por Watabe [W2].

Como corolario inmediato a los teoremas 3.18 y 3.19, concluimos que sólo hay un número finito de cuerpos cúbicos ciclicos en las familias V y W con número de clase igual a 1.

ESQUEMA DEL ESTUDIO REALIZADO POR LA TESIS




[sigue]
K cuerpos de números cúbico cíclico
CAPITULO III
Discriminante de K.
Algoritmo de construcción de todos los cuerpos cúbicos cíclicos de discriminante dado.
Tabla de unidades fundamentales.
Obtención de un sistema fundamental de unidades para tres familias infinitas de cuerpos cúbicos cíclicos en función de los coeficientes de un polinomio definición del cuerpo en cuestión.
Paridad del número de clase de los cuerpos cúbicos cíclicos pertenecientes a dichas familias. Comportamiento del número de clase cuando el discriminante tiende a +∞ para los cuerpos cúbicos cíclicos de las citadas familias.

CAPITULO CERO. PRELIMINARES

PRELIMINARES

En este capitulo preliminar vamos a dar las definiciones y los teoremas que vamos a utilizar a lo largo de esta tesis.

K es un cuerpo de números algebraicos si es extensión finita del cuerpo Q de los números racionales. El grado de K/Q es la dimensión [K:Q] de K como Q-espacio vectorial; [K:Q] = n es finita. Diremos que K es un cuerpo cuadrático si n = 2; un cuerpo cúbico si n = 3; etc.

El teorema del elemento primitivo asegura que todo K de grado n es de la forma $K = Q(\alpha)$ donde α es una raíz de $f(x) = a_n x^n + \ldots + a_1 x + a_0$ con f(x) irreducible en Q[x]. ($f(x) = \mathrm{Irr}\ (\alpha, Q)$).

El conjunto R de los $x \in K$ que son raíz de un polinomio de Z[x] mónico constituyen un anillo que se llama anillo de los enteros de K. R es un grupo (aditivo) abeliano libre de rango n y una base entera es una Z-base de R.

Si K es un cuerpo de números de grado n sobre Q entonces hay exactamente n Q-monomorfismos de K en C, siendo C el cuerpo de los números complejos. Sea $K = Q(\alpha)$, cada conjugado de α determina un único Q-monomorfismo de K en C.

Definición: Sean $\sigma_1, \ldots, \sigma_n$ los n Q-monomorfismos de K en C. Para $\alpha_1, \ldots, \alpha_n \in K$ definimos el discriminante de $\alpha_1, \ldots, \alpha_n$ como $\text{disc}(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2$.

Proposición: Sean $(\beta_1, \ldots, \beta_n)$ y $(\Gamma_1, \ldots, \Gamma_n)$ dos Q-bases enteras de K, entonces $\text{disc}(\beta_1, \ldots, \beta_n) = |M|^2 \text{disc}(\Gamma_1, \ldots, \Gamma_n)$ siendo M la matriz del cambio de la primera base a la segunda.

Teorema: Sean $(\beta_1, \ldots, \beta_n)$ y $(\Gamma_1, \ldots, \Gamma_n)$ dos bases enteras de R anillo de enteros de K. Entonces, $\text{disc}(\beta_1, \ldots, \beta_n) = \text{disc}(\Gamma_1, \ldots, \Gamma_n)$.

Por tanto, el discriminante de una base entera es un invariante de R y se denotará por disc(R) ó disc(K).

Supongamos $\alpha_1, \ldots, \alpha_n$ elementos de R, entonces dichos elementos forman una base entera de R si y solo si $\text{disc}(\alpha_1, \ldots, \alpha_n) = \text{disc}(R)$. Más adelante veremos que el discriminante contiene información sobre los primos de Q que ramifican en K.

Para cada primo $p \in Z$ y para cada entero $m \in Z$ denotamos con $v_p(m)$ al mayor exponente r tal que $p^r \mid m$. Diremos que una Q-base de enteros $(\alpha_1, \ldots, \alpha_n)$ es minimal en p si $v_p(\text{disc}(\alpha_1, \ldots, \alpha_n)) = v_p(\text{disc}(K))$.

El teorema 9.28. de Harvey-Cohn nos permite encontrar en

un número finito de pasos una base entera de K a partir de una Q-base de enteros de K. Enunciamos dicho teorema en el caso K cuerpo de números cúbico, que es el que nos interesa.

Teorema 9.28 de Harvey-Cohn para K cuerpo de números cúbico: sea $\{\alpha_1,\alpha_2,\alpha_3\}$ una Q-base de enteros del cuerpo cúbico K. Sea p un primo de Z, se verifica:

(1) si $\alpha_1/p \in R$ entonces $\{\alpha_1/p,\alpha_2,\alpha_3\}$ es una Q-base de enteros del cuerpo K y se verifica $v_p(\text{disc}(\alpha_1/p,\alpha_2,\alpha_3)) = v_p(\text{disc}(\alpha_1,\alpha_2,\alpha_3)) - 2$.

ó (2) si $\alpha_1/p \notin R$ entonces se verifica:

(2.1.) existe $s_0 \in \{0,1,2,\ldots,p-1\}$ tal que $(s_0\alpha_1 + \alpha_2)/p \in R$ y, entonces, $\{\alpha_1, (s_0\alpha_1 + \alpha_2)/p,\alpha_3\}$ es una Q-base de enteros del cuerpo K y se verifica $v_p(\text{disc}(\alpha_1,(s_0\alpha_1 + \alpha_2) / p, \alpha_3)) = = v_p(\text{disc}(\alpha_1,\alpha_2,\alpha_3)) - 2$.

ó (2.2.) Si $(s_0\alpha_1 + \alpha_2)/p \notin R$ para todo $s_0 \in \{0,1,2,\ldots,p-1\}$ entonces se verifica:

(2.2.1.) Existen $s_0,s_1 \in \{0,1,2,\ldots,p-1\}$ tales que $(s_0\alpha_1 + s_1\alpha_2 + \alpha_3)/p \in R$, y entonces $\{\alpha_1,\alpha_2,(s_0\alpha_1 + s_1\alpha_2 + \alpha_3)/p \}$ es una Q-base de enteros del cuerpo K y se verifica $v_p(\text{disc}(\alpha_1,\alpha_2,(s_0\alpha_1 + s_1\alpha_2 + \alpha_3)/p) = = v_p(\text{disc}(\alpha_1,\alpha_2,\alpha_3)) - 2$.

ó (2.2.2.) $\{\alpha_1,\alpha_2,\alpha_3\}$ es minimal en p.

Definición: Sea $\alpha \in R$, índice(α) = $(\text{disc}(\alpha)/\text{disc}(K))^{1/2}$.

Se verifica índice(α) $\in Z^+$. Diremos que K es monogénico si existe $\alpha \in R$ tal que índice(α) = 1, esto es, si R tiene una base entera de potencias $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

En general, R no es un dominio de factorización única (D.F.U.), pero dicha factorización única se cumple para sus ideales, dado que R es un dominio de Dedekind.

Sea L/K una extensión finita. Sea R el anillo de enteros de K y S el anillo de enteros de L. Si P es un ideal primo de R entonces $PS = P_1^{e_1} \ldots P_s^{e_s}$ de forma única, siendo P_i ideales primo de S. Por definición e_i es el índice de ramificación de P_i sobre P. S/P_i es una extensión finita de R/P, su grado f_i se denomina grado de inercia de P_i sobre P. Diremos que P es ramificado en S si y solo si algún e_i es mayor que 1. La condición necesaria y suficiente para que un primo p de Z sea ramificado en R es que $p \mid \text{disc}(R)$. Si $n = [L:K]$ entonces $\Sigma e_i f_i = n$.

En el caso L/K normal $e_1 = \ldots = e_s$ y $f_1 = \ldots = f_s$. Además, G = Gal (L/K) actúa transitivamente sobre los ideales primos de S que yacen sobre P. O sea, si Q y Q' son dos ideales primos de S que yacen sobre el mismo primo P de R, entonces existe $\sigma \in$ Gal (L/K) tal que $\sigma(Q) = Q'$.

Para estudiar la aritmética del anillo de enteros R de un cuerpo de números K, debemos comenzar por la determinación de los ideales primos no nulos de R. Ahora bien, si P es un ideal primo no nulo de R entonces $P \cap Z = pZ$ es un ideal primo no nulo de Z. Luego la determinación de ideales primos no nulos de R se reduce al conocimiento de la descomposición de los primos de Z en producto de ideales primos de R. El lema de Kummer ([M], teorema 27) es un criterio para determinar dicha descomposición.

Lema de Kummer: Sea α elemento primitivo de K cuerpo de números algebraicos. Supongamos que p es un primo de Z tal que $p \nmid$ índice(α). Sea $g(x) = Irr(\alpha,Q)$. Consideremos $g + Z_p[x] = (g_1 + Z_p[x])^{e1} \ldots (g_r + Z_p[x])^{er}$ la descomposición de $g + Z_p[x]$ en irreducibles de $Z_p[x]$. Entonces, $pR = (p, g_1(\alpha))^{e1} \ldots (p, g_r(\alpha))^{er}$. Además, el grado de inercia de $(p, g_i(\alpha))$ sobre p es igual al grado de g_i.

Hay otro criterio que, en ciertas ocasiones, puede ser muy útil en el momento de estudiar la descomposición en R de un primo p de Z:

Teorema (teorema 10.61. de [HC2]): Sea R anillo de enteros de K sea p un primo de Z. Consideremos $pR = P_1^{e1} \ldots P_s^{es}$ la descomposición de pR en ideales primos de R. Entonces, $v_p(disc(K)) = -1 + ei + h_i$ donde $h_i = 0$ si $p \nmid ei$ y $h_i > 0$ si $p \mid ei$.

En el conjunto S de los ideales no nulos de R anillo de enteros de K definimos la siguiente relación de equivalencia: I, J ideales no nulos de R, $I \approx J$ si y solo si $\alpha I = \beta J$ para algún $\alpha, \beta \in R - (0)$. El conjunto cociente $S/\approx$ es un grupo C_K abeliano finito que se llama grupo de clases de K. Su cardinal h_K se denomina número de clase de K. En relación con las propiedades de factorización de R, se tiene que R es un D.F.U. si y solo si R es un D.I.P. si y solo si $h_K = 1$.

Para todo K cuerpo de números algebraicos existe una máxima extensión K1/K abeliana no ramificada. Llamaremos cuerpo de clases de Hilbert de K al cuerpo K1. Se verifica que $Gal(K1/K) \approx C_K$ y, en particular, $[K1:K] = h_K$. Por tanto, un criterio para demostrar que el número de clase h_K es un múltiplo de un entero m es encontrar una extensión L/K abeliana no ramificada y tal que [L:K] = m.

El Teorema de las unidades de Dirichlet (teorema 38, [M]) determina la estructura del grupo de unidades de un anillo de enteros. Enunciamos a continuación dicho teorema :

Sea U el grupo de unidades de un anillo de enteros R. Sean r y 2s el número de Q-monomorfismos reales y no reales de K en C. Entonces U es el producto directo de W y V, donde W es el grupo cíclico finito de las raíces de la unidad en K y V es un grupo abeliano libre de rango r + s - 1.

Un conjunto de generadores de V se llama un **sistema fundamental de unidades de R**.

La condición necesaria y suficiente para que un elemento u de R sea una **unidad** es que su norma sea ± 1. (La **norma** de un elemento de R se define como el producto de sus conjugados y la **traza** como la suma de sus conjugados, incluida la multiplicidad).

Diremos que una unidad u de R es **totalmente positiva** cuando u y sus conjugados son positivos.

CAPITULO I. ESTUDIO MONOGRAFICO DE LOS CUERPOS DE NUMEROS CUBICOS.

1.A. Bases minimales y discriminante de K cuerpo de números cúbico.

1.B. Caracterización de la monogeneidad para diversas familias infinitas de cuerpos cúbicos.

1.A. BASES MINIMALES Y DISCRIMINANTE DE K CUERPO DE NUMEROS CUBICO.

En este primer Capítulo, realizamos un estudio de bases minimales en cada primo para K cuerpo de números cúbico. Realizamos dicho estudio en función de los coeficientes de un polinomio de definición de K. Como corolario inmediato, obtenemos el discriminante de K. Al final de este Capítulo se aplican, a modo de ejemplo, estos resultados a diversas familias infinitas de cuerpos cúbicos. En cada caso, se da una base entera, el discriminante y una caracterización de la monogeneidad en términos de la resolución de una ecuación diofántica. Estos resultados tienen carácter descriptivo y serán aplicados en los próximos capítulos. Para la obtención de bases minimales, hemos aplicado el teorema 9.28 de Harvey-Cohn [HC2, th. 9.28].

En lo que sigue, K denota a un cuerpo de números cúbico. Podemos suponer $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - ax + b$ y que no existe un primo p tal que $p^2 \mid a$, $p^3 \mid b$. Con R denotamos al anillo de enteros de K (raíces en K de un polinomio mónico con coeficientes en Z). El discriminante de θ es $4a^3 - 27b^2 = d^2q$ con q libre de cuadrados. D denota al discriminante de K. Para cada primo $p \in Z$ y para cada entero $m \in Z$ denotamos con $v_p(m)$ al mayor exponente r tal que $p^r \mid m$. Con Z denotamos al anillo de los números enteros y con Q al cuerpo de los números racionales.

En cuanto a los conceptos básicos utilizados consúltese [HC2], [M] ó [Sa].

Empezamos dando un lema de carácter técnico que será utilizado en diversas ocasiones a lo largo de toda la tesis.

Lema 1.1.: Sean x,y,z,p enteros racionales. Son equivalentes:

(i) $u = (x + y\theta + z\theta^2) / p \in R - Z$.

(ii) Existen C, D y E enteros racionales tales que:

$pC = -3x - 2az$.

$p^2D = a^2z^2 - ay^2 + 3x^2 + 4axz + 3byz$.

$p^3E = abyz^2 - 2ax^2z + by^3 - x^3 - 3bxyz -$
$- b^2z^3 + axy^2 - a^2xz^2$.

Demostración: Obviamente, $u \in R$ equivale a la existencia de $C, D, E \in Z$ tales que $u^3 + Cu^2 + Du + E = 0$. Calculando u^2, u^3, reduciendo potencias en θ hasta el orden 2 y aplicando que $\{ 1, \theta, \theta^2 \}$ es un Q-base de enteros, dicha ecuación equivale al sistema:

(1) $a^2z^3 + aCpz^2 + 3axz^2 + 3ay^2z - 3byz^2 +$
$+ 2Cpxz + Cpy^2 + Dp^2z + 3x^2z + 3xy^2 = 0$.

(2) $3a^2yz^2 - 2abz^3 + 2aCpyz + 6axyz + ay^3 - bCpz^2 -$
$- 3bxz^2 - 3by^2z + 2Cpxy + Dp^2y + 3x^2y = 0$.

(3) $-3abyz^2 + b^2z^3 - 2bCpyz - 6bxyz - by^3 + Cpx^2 +$
$+ Dp^2x + Ep^3 + x^3 = 0$.

Resolvemos dicho sistema multiplicando la ecuación (1) por -y, la (2) por z y se suman, despejándose así pC.

Finalmente se obtienen p^2D y p^3E obteniendo las condiciones dadas en (ii).

c.q.d.

En principio, en K tenemos la Q-base de enteros $\{ 1, \theta, \theta^2 \}$. Como aplicación de este lema, vamos a obtener otra segunda base. El teorema de Harvey-Cohn será aplicado a una u otra base, según el caso.

Lema 1.2.: Se verifica:

(1) $\text{disc}(\theta) = 4a^3 - 27b^2$.

(2) $\theta_1 = (4a^2 - 9b\theta - 6a\theta^2) / d$ es un entero algebraico, donde $4a^3 - 27b^2 = d^2q$ con q libre de cuadrados.

(3) $\text{disc}(1,\theta^2,\theta_1) = 3^4b^2q$.

Demostración.

(1) $$\begin{aligned}\text{disc}(\theta) &= - N^K_Q (f'(\theta)) = - N^K_Q (3\theta^2 - a) = \\ &= - N^K_Q ((3\theta^3 - a\theta) / \theta) = \\ &= - N^K_Q ((3a\theta - 3b - a\theta) / \theta) = \\ &= - N^K_Q (2a\theta - 3b) / N^K_Q (\theta).\end{aligned}$$

Pero, $N^K_Q (\theta) = -b$, y $N^K_Q (2a\theta - 3b) = 4a^3b - 27b^3$. Por tanto, $\text{disc}(\theta) = 4a^3 - 27b^2$.

(2) Por el lema 1.1. $\theta_1 \in R$ siendo, en este caso, $C = 0$, $D = -3aq$, y $E = -dq^2$.

(3) Su demostración es trivial.

c.q.d.

Damos ahora un lema análogo al 1.1. para la Q-base de enteros $\{1,\theta^2,\theta_1\}$. Igualmente, será muy utilizado a lo largo de esta memoria.

Lema 1.3.: Sean A, B y r elementos arbitrarios de Z. Son equivalentes:

(i) $(A + B\theta^2 + \theta_1) / r \in R \setminus Z$.

(ii) Se verifica el siguiente sistema de congruencias:

$-3A - 2aB \equiv 0 \ (r)$.

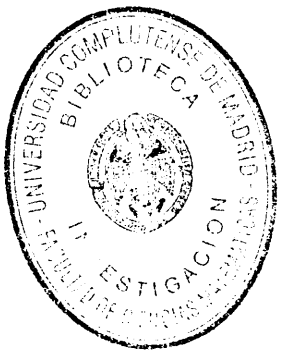
$Bdq - 3aq + a^2B^2 + 3A^2 + 4aAB \equiv 0 \ (r^2)$.

$-2aA^2B - A^3 - b^2B^3 - a^2AB^2 - dq^2 - aB^2dq -$

$-ABdq + 4a^2Bq + 3aAq \equiv 0 \ (r^3)$.

Demostración: Se aplica el lema 1.1. tomando $x = Ad + 4a^2$, $y = -9b$, $z = dB - 6a$, $p = rd$.

c.q.d.



ESTUDIO DE BASES MINIMALES EN p = 3

Ya estamos en condiciones de comenzar el estudio, propiamente dicho, de bases minimales en p = 3. Es realizado en términos, exclusivamente, de los coeficientes de un polinomio definición de K. Dicho estudio es recogido en las once siguientes proposiciones que contemplan todos los casos posibles. Se detallará la demostración de aquellas en las que el análisis del sistema de congruencias a que da lugar el teorema de Harvey-Cohn no sea de resolución inmediata.

Lema 1.4.: Sea $s_0 \in \{ -1, 0, 1 \}$. Se tiene que $(s_0 + \theta) / 3 \in R$ sii $a \equiv 3 (9)$ y ($b \equiv 1-a$ ó $b \equiv a-1 (27)$). Además, en el caso $b \equiv a-1 (27)$ es $(-1 + \theta) / 3 \in R$ y, en el caso $b \equiv 1-a (27)$ es $(1 + \theta) / 3 \in R$.

Demostración: Por el lema 1.1., $(s_0 + \theta) / 3 \in R$ sii $-3s_0 \equiv 0(3)$, $-a + 3s_0^2 \equiv 0(9)$ y $b - s_0^3 + as_0 \equiv 0(27)$. Si fuera $s_0 = 0$ implicaría $9|a$, $27|b$, caso que ha sido excluido. Luego, $s_0 = \pm 1$ de donde $a \equiv 3 (9)$ y ($b \equiv 1-a$ ó $b \equiv a-1 (27)$).

c.q.d.

Proposición 1.5.: Si $v_3(b) = 1$ y $v_3(a) \geq 2$ entonces $\{1,\theta^2,\theta_1/3\}$ y $\{1,\theta,\theta^2\}$ son minimales en 3. Además, $v_3(D) = 5$.

Demostración: Veamos, en primer lugar, que $\{1,\theta,\theta^2\}$ es minimal en 3. Para ello aplicamos el ya mencionado teorema de

Harvey-Cohn a dicha base.

$1/3 \notin R$.

Por el lema 1.4. $(s_0 + \theta) / 3 \notin R$, para $s_0 \in (-1,0,1)$.

Por el lema 1.5. $(s_0 + s_1\theta + \theta^2) / 3 \in R$ sii:

(a) $-3s_0 - 2a \equiv 0 \ (3)$.

(b) $a^2 - as_1^2 + 3s_0^2 + 4as_0 + 3bs_1 \equiv 0(9)$,

de donde deducimos que $s_0 = 0$.

(c) $-abs_1 + bs_1^3 - b^2 \equiv 0(27)$.

De la congruencia (c), deducimos que $3|s_1$ luego $s_1 = 0$ pues $s_1 \in (-1,0,1)$. Pero, $s_1 = 0 \implies 27|b^2$, absurdo. Luego, $(s_0 + s_1\theta + \theta^2) / 3 \notin R$.

Se tiene, pues, que $(1,\theta,\theta^2)$ es minimal en 3. Por otro lado, $v_3 \ (4a^3 - 27b^2) = 5$. Luego $v_3 \ (D) = 5$. Por el lema 1.3., $\theta_1 / 3 \in R$. Ahora bien, disc $(1,\theta^2,\theta_1/3) = 3^2b^2q$ y $v_3(3^2b^2q) = 5 = v_3(D)$, luego $(1,\theta^2,\theta_1/3)$ es minimal en 3.

c.q.d.

<u>Proposición 1.6.</u>: Si $v_3(b) = 2$, $v_3(a) \geq 3$ entonces $(1,\theta^2/3,\theta_1/3)$ y $(1,\theta,\theta^2/3)$ son minimales en 3 siendo $v_3(D) = 5$.

<u>Demostración:</u> En primer lugar, $\theta^2/3 \in R$ por el lema 1.1. ($C = -2a/3$, $D = a^2/9$, $E = -b^2/27$). De forma análoga a como se hizo en la proposición 1.5. se ve que $(1,\theta,\theta^2/3)$ es minimal en 3 y $v_3(D) = 5$. Ahora bien, por el lema 1.1. $\theta_1/3 \in R$ (tomando $C = 0$, $D = -3aq/9$, $E = -dq^2/27$). Disc $(1,\theta^2/3,\theta_1/3) = b^2q$ y $v_3 \ (b^2q) = 5 = v_3 \ (D)$, luego $(1,\theta^2/3,\theta_1/3)$ es minimal en 3.

c.q.d.

Proposición 1.7.: Si $v_3(a) = v_3(b) = 2$ entonces $\{1,\theta^2/3,\theta_1/3\}$ y $\{1,\theta,\theta^2/3\}$ son minimales en 3 siendo $v_3(D)=4$.

Demostración: Bajo estas hipótesis $\{1,\theta,\theta^2/3\}$ es una Q-base de enteros minimal en 3. Por ser $v_3(4a^3 - 27b^2) = 6$ se tiene $v_3(D) = 4$. También en este caso, $\theta_1/3 \in R$ y $\{1,\theta^2/3,\theta_1/3\}$ es minimal en 3 .

c.q.d.

Proposición 1.8.: En el caso $v_3(a) = v_3(b) = 1$, $\{1,\theta,\theta^2\}$ y $\{1,\theta^2,(3s_0 + 3s_1\theta^2 + \theta_1) / 9\}$ son minimales en 3; con $s_0 \in \{-1,1\}$, $s_1 \in \{-1,0,1\}$. Se satisface, además, el siguiente sistema de congruencias:

$$3dqs_1 - 3aq + 27 + 36as_0s_1 \equiv 0(81) .$$

$$-54as_1 - 27s_0 - 27b^2s_1 - 27a^2s_0s_1^2 - dq^2 - 9adqs_1^2 - 9\,dqs_0s_1 + 12a^2qs_1 + 9aqs_0 \equiv 0(3^6) .$$

Además, $v_3(D) = 3$.

Demostración: $\{1,\theta,\theta^2\}$ es minimal en 3. En efecto: $1/3 \notin R$; $(s_0 + \theta) / 3 \notin R$ ya que, por el lema 1.4., ello implicaría $3 \nmid b$; y, en tercer lugar, $(s_0 + s_1\theta + \theta^2) / 3 \notin R$ pues, aplicando el lema 1.1. se ve fácilmente que $s_0 = s_1 = 0$ y de ahí se deduce que $27 \mid b^2$, lo cual es absurdo. Además, $v_3(4a^3 - 27b^2) = v_3(D) = 3$. Considerando ahora la base $(1,\theta^2,\theta_1)$, se tiene que $\theta_1/3 \in R$ y $(s_0 + \theta^2) / 3 \notin R$ con $s_0 \in \{-1,0,1\}$. Como $V_3(\mathrm{disc}((1,\theta^2,\theta_1/3))) = 5$ necesariamente existen s_0, $s_1 \in \{-1,0,1\}$ tales que $(s_0 + s_1\theta^2 + \theta_1/3)/3 \in R$. Aplicando el lema 1.3., se deduce que $s_0 \neq 0$ y que se

safisfacen las congruencias dadas en el enunciado.

c.q.d.

Proposición 1.9.: Para $a \equiv 3(9)$, $3 \nmid b$, $b^2 \not\equiv 4(9)$ se tiene $(1, \theta^2, \theta_1)$ y $(1, \theta, \theta^2)$ son minimales en 3. Además, $v_3(D) = 4$.

Demostración: Vamos a aplicar el teorema de Harvey-Cohn a la base $(1, \theta^2, \theta_1)$.

$1/3 \notin R$, pues $R \cap Q = Z$.

$(s_0 + \theta^2)/3 \notin R$, para $s_0 \in \{-1,0,1\}$. En efecto, por el lema 1.3. si fuera $(s_0 + \theta^2)/3 \in R$ se verificaría el siguiente sistema de congruencias:

(1) $-3s_0 - 2a \equiv 0(3)$

(2) $a^2 + 3s_0^2 + 4as_0 \equiv 0(9)$

(3) $-2as_0^2 - s_0^3 - b^2 - a^2s_0 \equiv 0(27)$

Como $3 \nmid b$ de la tercera congruencia se deduce $s_0 \neq 0$. Por ser $a \equiv 0(3)$ la segunda congruencia implica $3s_0^2 + 4as_0 \equiv 0\ (9)$. Si fuera $s_0 = 1$ se tendría $3 + 4a \equiv 0(9)$ lo cual es absurdo pues se supone $a \equiv 3(9)$. Si fuera $s_0 = -1$ de la tercera congruencia se deduciría que $-2a + 1 - b^2 + a^2 \equiv 0(27)$ y, por ser $a \equiv 3(9)$, implicaría $3 + 1 - b^2 \equiv 0(9)$ lo cual es absurdo ya que se supone $b^2 \not\equiv 4(9)$.

$(s_0 + s_1\theta^2 + \theta_1)/3 \notin R$, con $s_0, s_1 \in \{-1, 0, 1\}$. En caso contrario, por el lema 1.3. se tendría:

(1) $as_1 \equiv 0(3)$.

(2) $s_1dq + 3s_0^2 + as_0s_1 \equiv 0(9)$.

(3) $-2as_0^2s_1 - s_0^3 - b^2s_1^3 - a^2s_0s_1^2 - dq^2 - adqs_1^2 - dqs_0s_1 + 4a^2qs_1 + 3aqs_0 \equiv 0(27)$.

Para razonar sobre este sistema de congruencias necesitamos calcular $s_3 = v_3(4a^3 - 27b^2)$. Obviamente, $s_3 \geq 3$. Si fuera $4a^3 - 27b^2 \equiv 0(3^5)$ se tendría $4(a/3)^3 - b^2 \equiv 0(9)$. Pero $a \equiv 3(9)$ implica $(a/3)^3 \equiv 1(9)$. Por tanto, $b^2 \equiv 4(9)$, absurdo. Tenemos, pues, que $s_3 = 3$ ó 4. Ahora bien, $s_3 = 3$ implica $4(a/3)^3 - b^2 \equiv 1(3)$ ó $4(a/3)^3 - b^2 \equiv 2(3)$. Luego $b^2 \equiv 0,3$ ó $6(9)$ ó $b^2 \equiv 2,5$ u $8(9)$ y esto es absurdo ya que en Z_9 los únicos cuadrados son 0,1,4,7. Por tanto $s_3 = 4$.

Razonamos ya sobre el sistema de congruencias. Si fuera $s_1 = 0$ de la segunda congruencia se deduciría que $3s_0^2 \equiv 0(9)$ con $s_0 \in \{-1,0,1\}$, luego $s_0 = 0$. Y, de la tercera congruencia, $-dq^2 \equiv 0(27)$, absurdo pues $s_3 = 4$. Luego, $s_1 = \pm 1$. Por otro lado, $s_0 = 0 \Longrightarrow -b^2s_1^3 - dq^2 - adqs_1^2 + 4a^2qs_1 \equiv 0(27) \Longrightarrow 9 \mid b^2s_1^3$ con $s_1 \in \{-1,0,1\}$ y $b \not\equiv 0(3) \Longrightarrow s_1 = 0$, que no puede darse. Luego, $s_0 = \pm 1$. De (2), se deduce $3 + as_0s_1 \equiv 0(9)$, luego $s_0s_1 = -1$. De (3) y teniendo en cuenta que $a \equiv 3(9)$,

$s_0 s_1 = -1$, 9 || d, 3 $\not|$ q, se tiene $-2as_1 - s_0 - s_1 b^2 - a^2 s_0 - dq^2 + dq + a^2 qs_1 + 3aqs_0 \equiv 0(27)$. Se pueden dar dos casos:

$s_0 = 1$ y $s_1 = -1$, en cuyo caso $b^2 + 2a - 1 \equiv 0(9) \Rightarrow b^2 \equiv 4(9)$ absurdo.

$s_0 = -1$ y $s_1 = 1$, en cuyo caso $-b^2 - 2a + 1 \equiv 0(9) \Rightarrow b^2 \equiv 4(9)$ absurdo.

Luego, $(1, \theta^2, \theta_1)$ es minimal en 3 y $v_3(D) = 4$. Como $s_3 = 4$ también $(1, \theta, \theta^2)$ es minimal en 3.

c.q.d.

Proposición 1.10. : Si 3 | a, 3 $\not|$ b, $a \not\equiv 3(9)$ y $b^2 \not\equiv a+1(9)$ entonces $(1, \theta^2, \theta_1/3)$ y $(1, \theta, \theta^2)$ son minimales en 3. Además $v_3(D) = 3$.

Demostración: Veamos que, bajo estas hipótesis, se tiene $s_3 = 3$. Si fuera 3 | $(4(a/3)^3 - b^2)$, como 3 $\not|$ b, se tendría 3 $\not|$ (a/3), luego $a \not\equiv 0(9)$. Por ser $a \equiv 0(3)$ y $a \not\equiv 3(9)$, necesariamente $a \equiv 6(9)$. Pero, $a \equiv 6(9)$ y $4(a/3)^3 - b^2 \equiv 0,3$ ó $6(9) \Rightarrow b^2 \equiv 5,2$ u $8(9)$. Absurdo, pues en Z_9 los cuadrados son 0,1,4 y 7. Por tanto, $4(a/3)^3 - b^2 \not\equiv 0(3)$ y $s_3 = 3$.

Afirmamos que $(1, \theta, \theta^2)$ es minimal en 3. En efecto:

$1/3 \notin R$.

$(s_0 + \theta)/3 \notin R$ con $s_0 \in (-1,0,1)$, por el lema 1.4.

$(s_0 + s_1\theta + \theta^2)/3 \notin R$ con $s_0, s_1 \in (-1,0,1)$. Si fuera de R, por el lema 1.1., se tendría el siguiente sistema de congruencias:

(1) $-3s_0 - 2a \equiv 0(3)$.

(2) $a^2 - as_1^2 + 3s_0^2 + 4as_0 + 3bs_1 \equiv$

$\equiv 0(9)$.

(3) $-abs_1 - 2as_0^2 + bs_1^3 - s_0^3 - 3bs_0s_1 -$

$- b^2 + as_0s_1^2 - a^2s_0 \equiv 0(27)$.

Veamos que $s_1 \neq 0$. Para $s_1 = 0$ se tendría $3s_0^2 + as_0 \equiv 0(9)$ y $-2as_0^2 - s_0^3 - b^2 - a^2s_0 \equiv 0(27)$. Pero, $s_0 \neq 0$; de lo contrario sería $-b^2 \equiv 0(27)$, absurdo. Luego $s_0 = \pm 1$ y $3 + as_0 \equiv 0(9)$. Como $a \not\equiv 3(9)$, necesariamente $s_0 = 1$ y, entonces, $-2a - 1 - b^2 - a^2 \equiv 0(27)$. De donde $b^2 \equiv -2a - 1(9) \Longrightarrow b^2 \equiv 5(9)$ absurdo, ya que 5 no es un cuadrado en Z_9. Luego $s_1 = \pm 1$. Tampoco, s_0 puede ser cero.

Si $s_0 = 0$:

De la segunda congruencia se deduciría $-a + 3bs_1 \equiv 0(9)$ y $-abs_1 + bs_1 + b^2 \equiv 0(27)$ $\Longrightarrow$ $a \not\equiv 0(9)$ y, como $a \equiv 0(3)$, $a \not\equiv 3(9)$, necesariamente $a \equiv 6(9)$. Luego $3bs_1 \equiv 6(9)$.

Para $s_1 = 1 \Longrightarrow 3b \equiv 6(9)$ y $-ab + b + b^2 \equiv$

$\equiv 0(27) \Longrightarrow 3b^2 + 3b - 3ab \equiv$

$\equiv 0(9) \Longrightarrow 3b^2 \equiv 3(9) \Longrightarrow$

$b^2 \equiv 1(3) \Longrightarrow b^2 \equiv 1,4$ ó

$7(9)$. Pero $b^2 \not\equiv a+1(9) \Longrightarrow$

$b^2 \not\equiv 7(9)$. Luego $b^2 \equiv 1$ ó

$4(9) \Longrightarrow b \equiv 1,8,2$ ó $7\ (9)$

y, por ser $3b \equiv 6(9)$, $b \equiv$

$\equiv 8(9)$ ó $b \equiv 2(9)$, absurdo ya que se debe verificar $-ab + b + b^2 \equiv 0(9)$ siendo $a \equiv 6(9)$.

Para $s_1 = -1$, se razona de modo totalmente análogo al caso $s_1 = 1$, llegándose también a un absurdo.

Por tanto $s_0 \neq 0$.

Queda, entonces, estudiar los posibles casos $s_0 = \pm 1$, $s_1 = \pm 1$, $a \equiv 0$ ó $6(9)$ combinados de todas las formas posibles. En cado caso se llega de forma análoga a un absurdo.

Veamos, por ejemplo, el caso $s_0 = 1$, $s_1 = 1$, $a \equiv 0(9)$:

(2) ==> $3 + 3b \equiv 0(9)$ ==> $b \equiv 2(3)$ ==> $b \equiv 2, 5$ u $8(9)$. $b \equiv 8(9)$ no puede darse pues $b^2 \not\equiv a+1(9)$.

$a \equiv 0(9)$ ==> $a \equiv 0, 9$ ó $18\ (27)$.

$b \equiv 2$ ó $5\ (9)$ ==> $b \equiv 2,11,20,5,14$ ó $23\ (27)$. Ninguno de esos posibles casos verifica la congruencia (3).

Se tiene, pues, demostrada la minimalidad de $(1, \theta, \theta^2)$ en 3, siendo $v_3(D) = 3$.

Por el lema 1.3., $\theta_1/3 \in R$. Y, como $v_3(\mathrm{disc}(1, \theta^2, \theta_1/3)) = 3 = v_3(D)$, $(1, \theta^2, \theta_1/3)$ es minimal en 3.

c.q.d.

Proposición 1.11.: Si $a \equiv 3(9)$, $b^2 \equiv a+1(27)$ entonces $\{1, (-1 + \theta^2)/3, \theta_1/3\}$ es minimal en 3. Además,

$v_3(D) = 1$ si s_3 es impar, y

$v_3(D) = 0$ si s_3 es par.

Demostración: Bajo estas hipótesis no conocemos s_3. Es, pues, más conveniente aplicar el teorema de Harvey-Cohn a la base $\{1, \theta^2, \theta_1\}$.

Veamos, en primer lugar, que $\theta_1/3 \in R$. Por el lema 1.3. ello equivale a que $-3aq \equiv 0(9)$, $-dq^2 \equiv 0(27)$. La primera congruencia es trivial ya que $a \equiv 0(3)$. En cuanto a la segunda congruencia, hay que distinguir entre que s_3 sea par o impar.

Para s_3 impar, como $3^3 \mid d^2q$, q sin cuadrados, $3 \mid q$ ==>

$3 \mid d$, $3 \mid q$, luego se verifica .

Para s_3 par, se tiene $s_3 \geq 4$, luego $4(a/3)^3 - b^2 \equiv 0(3)$.

Pero, $b^2 \equiv a+1(9)$ ==> $b^2 \equiv 4(9)$; $a \equiv 3(9)$ ==> $(a/3)^3 \equiv 1(9)$. Por tanto, $4(a/3)^3 - b^2 \equiv 0(9)$ y, así, $s_3 \geq 5$ y s_3 par ==> $s_3 \geq 6$ ==> $27 \mid d$, y también se verifica.

En segundo lugar, veamos que $(-1 + \theta^2)/3 \in R$. Por el lema 1.1. se deben satisfacer:

$-3 - 2a \equiv 0(3)$, lo cual es cierto.

$3 - 4a \equiv 0(9)$, también cierta.

$-2a + 1 - b^2 + a^2 \equiv 0(27)$, que equivale a

$b^2 \equiv (a-1)^2$ (27), lo cual es cierto pues

$(a^2 + 1 - 2a) - a - 1 = a(a - 3) \equiv 0(27)$ y, como

$b^2 \equiv a + 1$ (27) se tiene $b^2 \equiv (a - 1)^2$ (27).

Ahora bien, $disc(1,(\theta^2 - 1)/3,\theta_1/3) = b^2q$, siendo $3 \nmid b$ y q libre de cuadrados. Luego $(1, (-1 + \theta^2)/3, \theta_1/3)$ es minimal en 3 y $v_3(D) = 1$ si $3 \mid q$ y $v_3(D) = 0$ si $3 \nmid q$.

c.q.d.

Proposición 1.12.: Si $3 \nmid a$ entonces $v_3(D) = 0$ y $(1,\theta,\theta^2)$ es minimal en 3.

Demostración: Es inmediata ya que $s_3 = 0$.

Proposición 1.13.: Si $1 = v_3(a) < v_3(b)$ entonces $v_3(D) = 1$ y $(1,\theta,\theta^2/3)$ es minimal.

Demostración: Inmediata.

Proposición 1.14.: Si $a \equiv 3(9)$, $b^2 \equiv 4(9)$, $b^2 \not\equiv a+1(27)$ entonces $(1, \theta^2, \theta_1/3)$ es minimal en 3 y $v_3(D) = 3$.

Demostración: Bajo estas hipótesis no conocemos s_3. Es, pues, más conveniente aplicar el teorema de Harvey-Cohn a la base $(1, \theta^2, \theta_1)$.

Veamos, en primer lugar, que $s_3 = v_3(4a^3 - 27b^2) \geq 5$; $4(a/3)^3 - b^2 \equiv 0\ (9)$ ya que $a \equiv 3(9) \Rightarrow (a/3)^3 \equiv 1(9)$ y $b^2 \equiv 4(9)$. Luego $9 \mid d$, $3 \mid q$. Por el lema 1.1. tomando $C = 0$, $D = (-3aq)/9$ y $E = (-dq^2)/27$, que son de Z, se tiene que $\theta_1/3 \in R$. Aplicando el lema 1.1. y el 1.3., y teniendo en cuenta las hipótesis de la proposición, $(s_0 + \theta^2)/3 \notin R$ con $s_0 \in (-1,0,1)$ y $(s_0 + s_1\theta^2 + \theta_1/3)/3 \notin R$ con $s_0, s_1 \in (0,1,2)$. Y se tiene, pues, la minimalidad en 3 de la base $(1, \theta^2, \theta_1/3)$.

c.q.d.

Proposición 1.15.: Si $3 \mid a$, $a \not\equiv 3(9)$, $b^2 \equiv a+1(9)$ entonces $v_3(D) = 1$. Además :

(i) $(a \equiv 0(9),\ b \equiv 1(9))$ ó $(a \equiv 6(9),\ b \equiv 4(9)) \Longrightarrow$ $\{1, \theta, (1 - \theta + \theta^2)/3\}$ es minimal en 3.

(ii) $(a \equiv 0(9),\ b \equiv 8(9))$ ó $(a \equiv 6(9),\ b \equiv 5(9)) \Longrightarrow$ $\{1, \theta, (1 + \theta + \theta^2)/3\}$ es minimal en 3.

Demostración:

Supongamos en primer lugar $a \equiv 0(9)$. Aplicamos el teorema de Harvey-Cohn a la base $\{1, \theta, \theta^2\}$.

$(s_0 + \theta)/3 \notin R$ con $s_0 \in \{-1,0,1\}$, por el lema 1.4.

$(s_0 + s_1\theta + \theta^2)/3 \in R$ con $s_0, s_1 \in \{-1,0,1\}$ si y sólo si, por el lema 1.1., se verifican las siguientes congruencias :

(i) $-3s_0 - 2a \equiv 0(3)$.

(ii) $a^2 - as_1^2 + 3s_0^2 + 4as_0 + 3bs_1 \equiv 0(9)$.

(iii) $-abs_1 - 2as_0^2 + bs_1^3 - s_0^3 - 3bs_0s_1 - b^2 + as_0s_1^2 - a^2s_0 \equiv 0(27)$.

De la tercera congruencia se deduce que $bs_1 - s_0 - 1 \equiv 0(3)$; y de la segunda congruencia $s_0^2 + bs_1 \equiv 0(3)$. Juntando ambas congruencias tenemos que $s_0^2 + s_0 + 1 \equiv 0(3)$, luego $s_0 = 1$. De donde $bs_1 + 1 \equiv 0(3) \Longrightarrow$

$s_1 = -1$ si $b \equiv 1(9)$.

$s_1 = 1$ si $b \equiv 8(9)$.

Veamos que $a \equiv 0(9)$, $b \equiv 1(9) \Longrightarrow (1 - \theta + \theta^2)/3 \in R$. Tomemos $s_0 = 1$, $s_1 = -1$ en el sistema de congruencias del lema 1.1.. La primera congruencia se verifica trivialmente. La segunda equivale a $-3b + 3 \equiv 0(9)$, que se verifica. Y la tercera

$ab - 2a - b - 1 + 3b - b^2 + a \equiv 0(27)$ que equivale a $a(b - 1) - (b - 1)^2 \equiv 0(27)$, y también se verifica.

De forma análoga, en el caso $a \equiv 0(9)$ y $b \equiv 8(9)$ se tiene que $(1 + \theta + \theta^2)/3 \in R$. En efecto, tomando $s_0 = 1$, $s_1 = 1$ en el sistema de congruencias del lema 1.1., la primera congruencia se verifica trivialmente. La segunda congruencia equivale a $3 + 3b \equiv 0(9)$, que se verifica. Y, la tercera congruencia, $-ab - 2a + b - 1 - 3b - b^2 + a \equiv 0(27)$ que equivale a $-a(b + 1) - (b + 1)^2 \equiv 0(27)$, y también se verifica. Por ser $v_3(\text{disc}(\theta)) = 3$ entonces $v_3(D) = 1$ y el caso $a \equiv 0(9)$ queda estudiado.

Supongamos, en segundo lugar, $a \equiv 6(9)$. Necesariamente $s_3 = v_3(4a^3 - 27b^2) = 3$. En efecto, $a \equiv 6(9) \Rightarrow (a/3)^3 \equiv 2(3)$. Y como $b^2 \equiv 1(3)$ se tiene $4(a/3)^3 - b^2 \equiv 1(3)$; luego $s_3 = 3$. Aplicamos el teorema de Harvey-Cohn a la base $(1, \theta, \theta^2)$.

$(s_0 + \theta)/3 \notin R$ con $s_0 \in \{-1,0,1\}$, por el lema 1.4.

$(s_0 + s_1\theta + \theta^2)/3 \in R$ con $s_0, s_1 \in \{-1,0,1\}$ si y sólo si, por el lema 1.1., se verifican las siguientes congruencias :

(i) $-3s_0 - 2a \equiv 0(3)$.

(ii) $a^2 - as_1^2 + 3s_0^2 + 4as_0 + 3bs_1 \equiv 0(9)$.

(iii) $-abs_1 - 2as_0^2 + bs_1^3 - s_0^3 - 3bs_0s_1 - b^2 + as_0s_1^2 - a^2s_0 \equiv 0(27)$.

Pero, (ii) $\Leftrightarrow - as_1^2 + 3s_0^2 + as_0 + 3bs_1 \equiv 0(9) \Leftrightarrow - (a/3)s_1^2 + s_0^2 + (a/3)s_0 + bs_1 \equiv 0(3)$. Pero $a \equiv 6(9) \Rightarrow a/3 \equiv 2(3)$. Luego (ii) $\Leftrightarrow - 2s_1^2 + s_0^2 + 2s_0 + bs_1 \equiv 0(3)$.

Veamos que $a \equiv 6(9)$, $b \equiv 4(9) \Rightarrow (1 - \theta + \theta^2)/3 \in R$. Tomemos $s_0 = 1$, $s_1 = -1$ en el sistema de congruencias del lema 1.1..

La primera y segunda congruencia se verifican trivialmente. La tercera congruencia es $ab - a - 1 + 2b - b^2 - a^2 \equiv 0(27)$. Pero $ab - a - 1 + 2b - b^2 - a^2 = (a - 6)(b - 4) - (b - 4)^2 + 9a - (a + 3)^2 \equiv 0(27)$ ya que $a \equiv 6(9)$ y $b \equiv 4(9)$.

De forma análoga, en el caso $a \equiv 6(9)$ y $b \equiv 5(9)$ se tiene que $(1 + 9 + 9^2)/3 \in R$. En efecto, tomando $s_0 = 1$, $s_1 = 1$ en el sistema de congruencias del lema 1.1., la primera y segunda congruencia se verifican trivialmente. La tercera congruencia es $-ab - a - 1 - 2b - b^2 - a^2 \equiv 0(27)$. Pero $-ab - a - 1 - 2b - b^2 - a^2 = -(a - 6)(b - 5) - (b + 4)^2 + 54 - (a + 3)^2 \equiv 0(27)$ ya que $a \equiv 6(9)$ y $b \equiv 5(9)$.

Como $s_3 = 3 \Longrightarrow v_3(D) = 1$ y el caso $a \equiv 6(9)$ queda estudiado.

c.q.d.

ESTUDIO DE BASES MINIMALES EN p = 2

Vamos a realizar para p = 2 un estudio análogo al realizado para p = 3. Los primos 2 y 3 tienen que ser considerados como casos especiales al estudiar bases minimales ya que disc(θ) = $4a^3 - 27b^2$. Para p > 3 el estudio es ya general.

Proposición 1.16.: Si $1 = v_2(b) \leq v_2(a)$, entonces $(1,\theta^2,\theta_1)$ y $(1,\theta,\theta^2)$ son minimales en 2 siendo $v_2(D) = 2$.

Demostración: Aplicamos el teorema de Harvey-Cohn a la base $(1,\theta^2,\theta_1)$.

$1/2 \notin R$.

$(s_0 + \theta^2)/2 \notin R$ con $s_0 \in (0,1)$, ya que en caso contrario por el lema 1.1. sería:

$- 3s_0 - 2a \equiv 0(2) \Longrightarrow 2 \mid 3s_0 \Longrightarrow s_0 = 0.$

$a^2 + 3s_0^2 + 4as_0 \equiv 0(4).$

$- 2as_0^2 - s_0^3 - b^2 - a^2s_0 \equiv 0(8) \Longrightarrow 8 \mid b^2$, absurdo

$(s_0 + s_1\theta^2 + \theta_1)/2 \notin R$ con $s_0, s_1 \in (0,1)$. Caso contrario, por el lema 1.3. se tendría:

$- 3s_0 - 2as_1 \equiv 0(2) \Longrightarrow 2 \mid 3s_0 \Longrightarrow s_0 = 0.$

$s_1dq - 3aq + a^2s_1^2 + 3s_0^2 + 4as_0s_1 \equiv 0(4).$

$- 2as_0^2s_1 - s_0^3 - bs_1^3 - a^2s_0s_1^2 - dq^2 -$

$- as_1^2dq - s_0s_1dq + 4a^2s_1q + 3as_0q \equiv 0(8)$

$\Longrightarrow 4 \mid dq^2$, lo cual es absurdo ya que $s_2 = 2$, luego $2 \parallel d$, $2 \nmid q$.

c.q.d.

Proposición 1.17.: Si $2 = v_2(b) \leq v_2(a)$, entonces $\{1,\theta^2/2,\theta_1\}$ y $\{1,\theta,\theta^2/2\}$ son minimales en 2, siendo $v_2(D)=2$.

Demostración: $\theta^2/2 \in R$ por el lema 1.1. (tomando $C = -a$, $D = a^2/4$, $E = -b^2/8$).

$\{1,\theta,\theta^2/2\}$ es minimal en 2:

$1/2 \notin R$.

$(s_0 + \theta)/2 \notin R$ con $s_0 \in \{0,1\}$, pues si perteneciera a R, aplicando el lema 1.1. se deduce, de la primera congruencia $s_0 = 0$ y de la última que $8 \mid b$, lo cual es absurdo.

$(s_0 + s_1\theta + \theta^2) / 2 \notin R$, con s_0, $s_1 \in \{0,1\}$. En caso contrario, de nuevo aplicando el lema 1.1., se tendría que verificar un sistema de tres congruencias. De la primera se deduce que $s_0 = 0$, de la segunda que $s_1 = 0$ y de la tercera que $8 \mid b$, lo cual es absurdo.

Luego $\{1,\theta,\theta^2/2\}$ es minimal en 2 y $v_2(D) = 2$. Como $\{1,\theta^2/2,\theta_1\}$ es una Q-base de enteros verificando $v_2(\text{disc}\{1,\theta^2/2,\theta_1\}) = 2 = v_2(D)$, dicha base es también mininal en 2.

c.q.d.

Proposición 1.18.: Si $v_2(b) = 0$ entonces $\{1,\theta^2,\theta_1\}$ y $\{1,\theta,\theta^2\}$ son minimales en 2 y $v_2(D) = 0$.

Demostración: Inmediata.

Nota 1: Según el teorema 2 de Pascual Llorente y Enric

Nart, [L, N], para $s_2 = v_2(4a^3 - 27b^2)$ par y

$\Omega_2 = (4a^3 - 27b^2)/2^{s_2} \equiv 1\ (4)$

se tiene $v_2(D) = 0$. En este caso, $s_2 = 0$ y $\Omega_2 = 4a^3 - 27b^2 \equiv -27b^2 \equiv b^2\ (4)$; ahora bien, $b \equiv 1(2) \Rightarrow b^2 \equiv 1(4)$, luego $\Omega_2 \equiv 1(4)$. Hay, pues, concordancia entre ambos resultados.

Proposición 1.19.: Si $v_2(b) = 1$, $v_2(a) = 0$ y $q \equiv 3(4)$ entonces $(1,\theta^2,\theta_1)$ es minimal en 2 y $v_2(D) = 2$.

Demostración: En este caso no conocemos s_2. Minimizamos, pues, la base $(1,\theta^2,\theta_1)$. Veamos, en primer lugar, que $s_2 \geq 4$.

$b \equiv 0(2)$, $b \not\equiv 0(4) \Rightarrow b \equiv 2(4) \Rightarrow (b/2)^2 \equiv 1(4)$.

$a \equiv 1(2) \Rightarrow a \equiv 1$ ó $3(4)$.

Veamos que $a \equiv 1(4)$ no puede darse:

$a \equiv 1(4) \Rightarrow a^3 - 27(b/2)^2 \equiv 2\ (4) \Rightarrow s_2 = v_2(4a^3 - 27b^2) = 3 \Rightarrow 2 \mid q$ lo cual es absurdo por ser $q \equiv 3(4)$. Por consiguiente, $a \equiv 3(4)$. Así, $a^3 - 27(b/2)^2 \equiv 0(4)$, luego $s_2 \geq 4$ y $4 \mid d$.

Tras estos razonamientos previos, estamos ya en condiciones de aplicar el teorema de Harvey-Cohn a la base $(1,\theta^2,\theta_1)$.

$1/2 \notin R$.

$(s_0 + \theta^2)/2 \notin R$ por ser $v_2(a) = 0$.

$(s_0 + s_1\theta^2 + \theta_1)/2 \notin R$ con $s_0, s_1 \in (0,1)$. De lo contrario, por el lema 1.3. se tendría:

$-3s_0 - 2as_1 \equiv 0(2) \Rightarrow 2 \mid 3s_0 \Rightarrow s_0 = 0$.

$s_1dq - 3aq + a^2s_1^2 \equiv 0(4) \Rightarrow s_1 = 1$.

$-b^2s_1^3 - dq^2 - as_1^2dq + 4a^2s_1q \equiv 0(8)$.

Ahora bien, $q \equiv 3(4)$, $a \equiv 3(4)$, $d \equiv 0(4)$ ==> $-3aq + a^2 + dq \equiv 2(4)$. Luego el sistema de congruencias no tiene solución.

c.q.d.

Proposición 1.20.: Si $v_2(b) = 1$, $v_2(a) = 0$ y $q \equiv 1(4)$ entonces $(1,\theta^2,(\theta^2 + \theta_1)/2)$ es minimal en 2 y $v_2(D) = 0$.

Demostración: Veamos que $(\theta^2 + \theta_1)/2 \in R$. Por el lema 1.3. ello equivale al siguiente sistema de congruencias:

$$-2a \equiv 0(2).$$

$$dq - 3aq + a^2 \equiv 0(4).$$

$$-b^2 - dq^2 - adq + 4a^2q \equiv 0(8).$$

La primera congruencia se verifica trivialmente.

De forma totalmente análoga a la proposición anterior se demuestra que, bajo estas hipótesis, $d \equiv 0(4)$ y $a \equiv 3(4)$. Y, como $q \equiv 1(4)$, entonces la segunda congruencia se verifica.

Estudiamos ahora la última congruencia:

$$d \equiv 0(4) \Rightarrow d \equiv 0(8) \text{ ó } d \equiv 4(8).$$

En el caso $d \equiv 0(8)$ dicha congruencia equivaldría a $-b^2 + 4a^2q \equiv 0(8)$. Por ser $b \equiv 0(2)$ y $b \not\equiv 0(4)$ se tiene $b \equiv 2(4)$, luego $b^2 \equiv 4(8)$. Por otro lado, $a \equiv 3(4)$ ==> $a^2 \equiv 1(8)$; $q \equiv 1\ (4)$ ==> $q \equiv 1(8)$ ó $q \equiv 5(8)$. Para $q \equiv 1(8)$ se tendría $-b^2 + 4a^2q \equiv 0(8)$ y para $q \equiv 5(8)$, $-b^2 + 4a^2q \equiv 0(8)$. Luego el caso $d \equiv 0(8)$ queda terminado.

De forma totalmente análoga se estudia el caso $d \equiv 4(8)$.

Por ser $v_2(\text{disc}(1,\theta^2,(\theta^2 + \theta_1)/2)) = 0$ dicha base es minimal en 2 y $v_2(D) = 0$.

c.q.d.

Nota 2: Los resultados dados en las proposiciones 1.19. y 1.20. sobre v_2 (D) están en concordancia con los dados en el teorema 2 de Pascual LLorente y Enric Nart [L,N]. En efecto,

$d/(2^{v_2(d)}) \equiv 1$ ó 3 (4) $\Longrightarrow$ $(d/2^{v_2(d)})^2 \equiv 1(4)$ $\Longrightarrow$ $\underline{\Omega}_2 = (d/2^{v_2(d)})^2 q \equiv q(4) \Longrightarrow$

$\underline{\Omega}_2 \equiv 3(4)$ sii $q \equiv 3(4)$ y $\underline{\Omega}_2 \equiv 1(4)$ sii $q \equiv 1(4)$. En el caso, $\underline{\Omega}_2 \equiv 3(4)$ y s_2 par el mencionado teorema da $v_2(D) = 2$. Y, en el otro, da $v_2(D) = 0$.

Proposición 1.21.: Si $v_2(b) = 1$, $v_2(a) = 0$ y s_2 es impar entonces $(1,\theta^2,\theta_1)$ es minimal en 2 y $v_2(D) = 3$.

Demostración: Bajo estas hipótesis, $s_2 \geq 3$ y es impar, luego $v_2(q) = 1$, $v_2(d) \geq 1$. Así, $v_2(3^4b^2q) = 3$. Veamos que $(1,\theta^2,\theta_1)$ es minimal en 2.

$1/2 \notin R$.

$(s_0 + \theta^2)/2 \notin R$ con $s_0 \in \{0,1\}$, pues, por lema 1.1. se tendría

$-3s_0 - 2a \equiv 0(2)$ de donde $s_0 = 0$ y $a^2 \equiv 0(4)$, absurdo pues $v_2(a) = 0$.

$(s_0 + s_1\theta^2 + \theta_1)/2 \notin R$, con $s_0, s_1 \in \{0,1\}$. De lo contrario, por el lema 1.3. se tendría en primer lugar $-3s_0 - 2as_1 \equiv 0(2) \Longrightarrow s_0 = 0$. En segundo lugar, $s_1dq - 3aq + a^2s_1^2 \equiv 0\ (4) \Longrightarrow s_1 = 1$, pues $s_1 = 0 \Longrightarrow 4 \mid 3aq \Longrightarrow 2 \mid a$, absurdo. Pero, $dq - 3aq + a^2 \equiv 0(4)$

$\Longrightarrow 2 \mid a^2$ absurdo.

c.q.d.

Proposición 1.22.: Si $v_2(b) = 2$, $v_2(a) = 0$ y $a \equiv 1(4)$ entonces $\{1,\theta,(\theta + \theta^2)/2\}$ y $\{1,\theta^2,(1 + s_1\theta^2 + (\theta^2 + 1)/2)/2\}$ con $s_1 \in \{0,1\}$ son minimales en 2. Además, $v_2(D) = 0$.

Demostración: Se tiene que $s_2 = 2$, luego $v_2(d) = 1$, $v_2(q) = 0$. Por otro lado $(\theta + \theta^2)/2 \in R$. En efecto, por el lema 1.1. ello equivale al siguiente sistema de congruencias:

$-2a \equiv 0(2)$.

$a^2 - a + 3b \equiv 0(4)$.

$-ab + b - b^2 \equiv 0(8)$.

La primera y segunda congruencia se verifican trivialmente. Por ser $v_2(b) = 2$, la tercera congruencia equivale a $-ab + b \equiv 0(8)$, la cual es cierta ya que:

$a \equiv 1(4) \Longrightarrow a \equiv 1(8)$ ó $a \equiv 5(8)$.

$b \equiv 0(4)$, $8 \nmid b \Longrightarrow b \equiv 4(8)$

luego $-ab + b \equiv -4 + 4 \equiv 0(8)$ ó

$-ab + b \equiv -20 + 4 \equiv 0(8)$.

Por consiguiente, $(\theta + \theta^2)/2 \in R$, y $v_2(D) = 0$. Con este resultado, vamos a encontrar una base minimal en 2 a partir de la base $\{1,\theta^2,\theta_1\}$; $v_2(\text{disc}(1,\theta^2,\theta_1)) = 4$.

$1/2 \notin R$.

$(s_0 + \theta^2)/2 \notin R$ con $s_0 \in \{0,1\}$. Pues por el lema 1.1. se tendría $-3s_0 - 2a \equiv 0(2) \Longrightarrow s_0 = 0$; y, de la segunda congruencia de dicho lema se deduciría $a^2 \equiv 0(4)$, absurdo.

Necesariamente, existen s_0, $s_1 \in \{0,1\}$ tales que

$(s_0 + s_1\theta^2 + \theta_1)/2 \in R$. Por el lema 1.3., $-3s_0 - 2as_1 \equiv 0(2)$ ==> $s_0 = 0$; $s_1dq - 3aq + a^2s_1^2 \equiv 0(4)$ ==> $s_1 = 1$. Y no es necesario examinar la tercera congruencia para afirmar que $(\theta^2 + \theta_1)/2 \in R$.

Volvemos a aplicar el teorema de Harvey-Cohn a la base $(1, \theta^2, (\theta^2 + \theta_1)/2)$. Podemos afirmar que existen $s_0, s_1 \in (0,1)$ tales que $(s_0 + s_1\theta^2 + (\theta^2 + \theta_1)/2)/2 \in R$. Aplicando el lema 1.3., de la primera congruencia se deduce que

$-6s_0 - 2a(2s_1 + 1) \equiv 0(4)$, que equivale a $-3s_0 - a \equiv 0(2)$ ==> $s_0 = 1$, y $(1,\theta^2,(1 + s_1\theta^2 + (\theta^2 + \theta_1)/2)/2)$ es minimal en 2.

c.q.d.

Nota 3: El resultado dado en la proposición anterior sobre $v_2(D)$ está en concordancia con el dado en el teorema 2 de Pascual Llorente y Enric Nart [L,N]. Pues, este caso corresponde a s_2 par y $\underline{\Omega}_2 = a^3 - 27(b/2)^2 \equiv 1(4)$ ya que $a \equiv 1(4)$ y $(b/2)^2 \equiv 0(4)$. En esta situación, dicho teorema afirma que $v_2(D) = 0$.

Proposición 1.23.: Si $v_2(b) = 2$, $v_2(a) = 0$ y $a \equiv 3(4)$ entonces $(1,\theta^2,(\theta^2 + \theta_1)/2)$ y $(1,\theta,\theta^2)$ son minimales en 2 y $v_2(D) = 2$.

Demostración: Aplicamos el teorema de Harvey-Cohn a la base $(1,\theta,\theta^2)$. Bajo estas hipótesis, $s_2 = v_2(4a^3 - 27b^2) = 2$ ==> $v_2(d) = 1$, $v_2(q) = 0$.

$1/2 \notin R$.

$(s_0 + \theta)/2 \notin R$ con $s_0 \in (0,1)$, pues, por lema 1.1. se tendría $-3s_0 \equiv 0(2)$, luego $s_0 = 0$. De la segunda congruencia, $a \equiv 0(4)$, absurdo.

$(s_0 + s_1\theta + \theta^2)/2 \notin R$ con $s_0, s_1 \in (0,1)$. Pues, en caso contrario, aplicando el lema 1.1. se tiene:

$-3s_0 - 2a \equiv 0(2)$, luego $s_0 = 0$.

$a^2 - as_1^2 + 3bs_1 \equiv 0(4)$, de donde

$s_1 = 0 \Longrightarrow a^2 \equiv 0(4)$, absurdo.

$s_1 = 1 \Longrightarrow a^2 - a + 3b \equiv 0(4)$, absurdo ya que por hipótesis, $b \equiv 0(4)$, $a \equiv 3(4)$.

Así, $(1,\theta,\theta^2)$ es minimal en 2, y $v_2(D) = 2$. Minimizaremos en 2 la base $(1,\theta^2,\theta_1)$:

$1/2 \notin R$.

$(s_0 + \theta^2)/2 \notin R$ con $s_0 \in (0,1)$, se ve fácilmente aplicando el lema 1.1.

Por ser $v_2(3^4b^2q) = 4$ y $v_2(D) = 2$, necesariamente existen s_0, $s_1 \in (0,1)$ tal que $(s_0 + s_1\theta^2 + \theta_1)/2 \in R$. Aplicando el lema 1.3. se tiene $-3s_0 - 2as_1 \equiv 0(2) \Longrightarrow s_0 = 0$.

$$s_1dq - 3aq + a^2s_1^2 \equiv 0(4) \Longrightarrow s_1 = 1.$$

Y, no hace falta examinar la tercera congruencia para concluir que $(\theta^2 + \theta_1)/2 \in R$.

c.q.d.

Nota 4: También este resultado sobre v_2 (D) está en concordancia con el dado en el teorema 2 de

Pascual Llorente y Enric Nart [L,N] pues, en las hipótesis de esta proposición, s_2 es par y $\Omega_2 = a^3 - 27(b/2)^2 \equiv 3(4)$; en esas condiciones, el mencionado teorema afirma que $v_2(D) = 2$.

Proposición 1.24.: Si $v_2(b) = 2$ y $v_2(a) = 1$ entonces $(1,\theta^2/2,\theta_1)$ y $(1,\theta,\theta^2/2)$ son minimales en 2 y $v_2(D) = 2$.

Demostración: En este caso, $s_2 = v_2(4a^3 - 27b^2) = 4$, luego $v_2(d) = 2$, $v_2(q) = 0$. Por el lema 1.1. tomando $C = -a$, $D = a^2/4$, $E = -b^2/8$ se tiene que $\theta^2/2 \in R$. La base $(1,\theta,\theta^2/2)$ es minimal en 2. En efecto:

$(s_0 + \theta)/2 \notin R$ con $s_0 \in (0,1)$. De lo contrario por el lema 1.1. se tendría que $-s_0 \equiv 0(2)$, luego $s_0 = 0$ y $-a \equiv 0(4)$, absurdo.

$(s_0 + s_1\theta + \theta^2/2)/2 \notin R$ con s_0, $s_1 \in R$. En efecto, de nuevo por el lema 1.1. se tendría $-6s_0 - 2a \equiv 0(4)$, luego $s_0 = 0$; $a^2 - 4as_1^2 + 6bs_1 \equiv 0(16)$, luego $8 \mid a^2$, absurdo.

Por tanto, $v_2(D) = 2$ y $(1,\theta^2/2,\theta_1)$ es minimal en 2.

c.q.d.

Nota 5: El teorema 2 de Pascual Llorente y Enric Nart [L,N] da que, en el caso s_2 par y $\Omega_2 \equiv 3(4)$, $v_2(D) = 2$. En las hipótesis de la proposición anterior, se tiene que $s_2 = v_2(4a^3 - 27b^2) = 4$ que es par; $\Omega_2 = 2(a/2)^3 - 27(b/4)^2$. Pero $b \equiv 0(4)$ y $8 \nmid b \Longrightarrow b \equiv 4(8)$. Por otro lado, $a \equiv 0(2)$ y $4 \nmid a \Longrightarrow a \equiv 2(4) \Longrightarrow a \equiv 2$ ó $6(8)$.

En el caso, $a \equiv 2(8)$, se tendría $\Omega_2 \equiv 2 - 27 \equiv$ $\equiv 3(4)$ y en el caso $a \equiv 6(8)$, $\Omega_2 \equiv 6 - 27 \equiv$ $\equiv 3(4)$. Hay, pues, concordancia entre ambos resultados.

Proposición 1.25.: Si $v_2(b) \geq 3$ y $v_2(a) = 0$ entonces $v_2(D)=0$ ó $v_2(D) = 2$ según que sea $a \equiv 1(4)$ ó $a \equiv 3(4)$, respectivamente. En el caso $a \equiv 1(4)$, $(1,\theta,(\theta + \theta^2)/2)$ es minimal en 2. En el caso $a \equiv 3(4)$, $(1,\theta,\theta^2)$ es minimal en 2.

Demostración: Bajo estas hipótesis $s_2 = v_2(4a^3 - 27b^2) = 2$ y $v_2(d) = 1$, $v_2(q) = 0$. Trabajamos con la base $(1,\theta,\theta^2)$ a la que vamos a aplicar el teorema de Harvey-Cohn.

$1/2 \notin R$.

$(s_0 + \theta)/2 \notin R$ con $s_0 \in (0,1)$, se ve fácilmente aplicando el lema 1.1.

$(s_0 + s_1\theta + \theta^2)/2 \in R$ sii $s_0 = 0$, $s_1 = 1$ y se verifican

$- 2a \equiv 0(2)$.

$a^2 - a + 3b \equiv 0(4)$.

$- ab + b - b^2 \equiv 0(8)$.

La primera y tercera congruencia se verifican. Veamos cuando se verifica la segunda; $a^2 - a + 3b \equiv 0(4)$ sii $a^2 - a \equiv 0(4)$, como $a \not\equiv 0(2)$ se tienen $a \equiv 1$ ó $3(4)$. En el caso $a \equiv 1(4)$, $a^2 - a \equiv 0(4)$ es cierta; en el caso $a \equiv 3(4)$, no lo es.

Quedan, pues, demostrados los resultados enunciados en esta proposición. No vamos a minimizar en 2 la base $(1,\theta^2,\theta_1)$

pues dependerá del valor de $v_2(b)$.

c.q.d.

Nota 6: Referenciando al teorema 2 de Pascual Llorente y Enric Nart [L,N] encontramos que para $v_2(b) > v_2(a)$, s_2 par y $\Omega_2 \equiv 1(4)$ se tiene $v_2(D) = 0$, y para $v_2(b) > v_2(a)$, s_2 par y $\Omega_2 \equiv 3(4)$, $v_2(D) = 2$. En las hipótesis de la proposición 1.25. se tiene $s_2 = v_2(4a^3 - 27b^2) = 2$, que es par. Por otra lado, $b \equiv 0(8) \Rightarrow (b/2)^2 \equiv 0(4)$; $a \equiv 1(4) \Rightarrow a^3 \equiv 1(4)$ y $a \equiv 3(4) \Rightarrow a^3 \equiv 3(4)$. Luego, para $a \equiv 1(4)$ es $\Omega_2 \equiv 1(4)$ y para $a \equiv 3(4)$ es $\Omega_2 \equiv 3(4)$. Ambos resultados son, pues, coherentes entre sí.

Proposición 1.26.: Si $v_2(b) \geq 3$ y $v_2(a) = 1$ entonces $v_2(D)=3$ y $(1,\theta,\theta^2/2)$ es minimal en 2.

Demostración: Bajo estas hipótesis $s_2 = v_2(4a^3 - 27b^2) = 5$. Obviamente, $\theta^2/2 \in R$ (se aplica el lema 1.1. tomando $C = -a$, $D = a^2/4$, $E = -b^2/8$). Una aplicación inmediata del lema 1.1. nos permite afirmar que $1/2 \notin R$, $(s_0 + \theta)/2 \notin R$ con $s_0 \in (0,1)$, $(s_0 + s_1\theta + \theta^2/2)/2 \notin R$ con $s_0, s_1 \in (0,1)$. No vamos a minimizar en 2 la base $(1,\theta^2,\theta_1)$ pues dicho estudio dependerá del valor de $v_2(b)$.

c.q.d.

ESTUDIO DE BASES MINIMALES EN p PRIMO MAYOR QUE TRES.

Lema 1.27.: Sea $p > 3$ un primo tal que $p^2 \mid disc(\theta)$. Entonces $(s_0 + \theta)/p \notin R$, con $s_0 \in \{0,1,\ldots,p-1\}$.

Demostración: Por el lema 1.1., $(s_0 + \theta)/p \in R$ sii $-3s_0 \equiv 0(p)$, $-a + 3s_0^2 \equiv 0(p^2)$ y $b - s_0^3 + as_0 \equiv 0(p^3)$. De la primera congruencia se deduce $s_0 = 0$, luego $-a \equiv 0(p^2)$ y $b \equiv 0(p^3)$, caso que desde un principio ha sido excluido. Por tanto, $(s_0 + \theta)/p \notin R$.

c.q.d.

Proposición 1.28.: Si $1 \leq v_p(b) \leq v_p(a)$ entonces:

o bien $v_p(b) = 1$, en cuyo caso $\{1,\theta^2,\theta_1\}$ y $\{1,\theta,\theta^2\}$ son minimales en p;

o bien $v_p(b) = 2$, en cuyo caso $\{1,\theta^2/p,\theta_1\}$ y $\{1,\theta,\theta^2/p\}$ son minimales en p.

En ambos casos, $v_p(D) = 2$.

Demostración: Supongamos, en primer lugar, $v_p(b) = 1$. Veamos que en este caso, $\{1,\theta,\theta^2\}$ es minimal en p. Aplicando el lema 1.27. sólo tenemos que probar que $(s_0 + s_1\theta + \theta^2)/p \notin R$, con $s_0, s_1 \in \{0,1,\ldots,p-1\}$. En caso contrario, por el lema 1.1. se verificarían

$-3s_0 - 2a \equiv 0(p)$,

$a^2 - as_1^2 + 3s_0^2 + 4as_0 + 3bs_1 \equiv 0(p^2)$, y

$-abs_1 - 2as_0^2 + bs_1^3 - s_0^3 - 3bs_0s_1 - b^2 + as_0s_1^2 - a^2s_0 \equiv 0(p^3)$

Por ser $v_p(a) \geq 1$, de la primera congruencia se deduce $s_0 = 0$. Pero, $s_0 = 0$, $v_p(b) = 1$ y $v_p(a) \geq 1$ implican, por la

tercera congruencia, que $s_1 = 0$; pero, entonces, $p^3 \mid b^2$, absurdo.

En segundo lugar, supongamos $v_p(b) = 2$. Obviamente, por el lema 1.1., $\theta^2/p \in R$. Veamos que $\{1,\theta,\theta^2/p\}$ es minimal en p. Por el lema 1.27., sólo resta ver que $(s_0 + s_1\theta + \theta^2/p)/p \notin R$, con $s_0, s_1 \in \{0,1,\ldots,p-1\}$. En caso contrario, se verificarían

$-3ps_0 - 2a \equiv 0(p^2)$,

$a^2 - ap^2s_1^2 + 3p^2s_0^2 + 4aps_0 + 3bps_1 \equiv 0(p^4)$, y

$- pabs_1 - 2as_0^2p^2 + bp^3s_1^3 - p^3s_0^3 - 3b^2s_0s_1 - b^2 + ap^3s_0s_1^2 - a^2ps_0 \equiv 0(p^6)$.

De dicho sistema de congruencias y de las hipótesis $2 = v_p(b) \leq v_p(a)$ se deduce $s_0 = s_1 = 0$, de donde $p^3 \mid b$, lo cual es absurdo. Así, $v_p(D) = 2$ y $\{1,\theta^2/p,\theta_1\}$ es también minimal en p.

c.q.d.

Proposición 1.29.: Si $v_p(b) = 0$, entonces $\{1,\theta^2,\theta_1\}$ es minimal en p. Además, $v_p(D) = 0$ si $s_p = v_p(4a^3 - 27b^2)$ es par y $v_p(D) = 1$ si s_p es impar.

Demostración: Inmediata. No podemos minimizar en p la base $\{1,\theta,\theta^2\}$ ya que no conocemos s_p.

Proposición 1.30.: Si $v_p(b) = 1$ y $v_p(a) = 0$, entonces $\{1,\theta,\theta^2\}$ y $\{1,\theta^2,(s_0 + s_1\theta^2 + \theta_1)/p\}$ son minimales en p, siendo $s_0, s_1 \in \{1,2,\ldots,p-1\}$ y verificando el siguiente sistema de congruencias:

(1) $- 3s_0 - 2as_1 \equiv 0(p)$,

(2) $s_1dq - 3aq + a^2s_1^2 + 3s_0^2 + 4as_0s_1 \equiv 0(p^2)$,

$$(3) \quad -2as_0^2s_1 - s_0^3 - b^2s_1^3 - a^2s_0s_1^2 - dq^2 - as_1^2dq - dqs_0s_1 + 4a^2s_1q + 3as_0q \equiv 0(p^3).$$

Además, $v_p(D) = 0$.

Demostración: En este caso $s_p = v_p(4a^3 - 27b^2) = 0$, luego $(1,\theta,\theta^2)$ es minimal en p. Por otro lado, $v_p(\text{disc}(1,\theta^2,\theta_1)) = 2$.

$1/p \notin R$.

$(s_0 + \theta^2)/p \notin R$ ya que $(1,\theta,\theta^2)$ es minimal en p.

Necesariamente existe s_0, $s_1 \in \{0,1,\ldots,p-1\}$ verificando el sisteme de congruencias del enunciado (se aplica el lema 1.3.). Además, de la primera y segunda congruencia se deduce $s_0 \not\equiv 0$, $s_1 \not\equiv 0$.

c.q.d.

Proposición 1.31.: Si $v_p(b) = 2$ y $v_p(a) = 0$, entonces $(1,\theta,\theta^2)$ y $(1,\theta^2,(t_0 + t1\theta^2 + (s_0 + s_1\theta^2 + \theta_1)/p)/p)$ son minimales en p, siendo $s_0,s_1,t_0,t1 \in \{0,1,2,\ldots,p-1\}$. Además, $v_p(D) = 0$.

Proposición 1.32.: Si $v_p(b) = 2$ y $v_p(a) = 1$, entonces $\{1,\theta,\theta^2/p\}$ y $\{1,\theta^2/p,\theta_1/p\}$ son minimales en p. Además, $v_p(D) = 1$.

Demostración: En este caso, $s_p = v_p(4a^3 - 27b^2) = 3$, luego $v_p(d) = 1$, $v_p(q) = 1$. Por el lema 1.1., $\theta^2/p \in R$ (se toma $C = -2a/p$, $D = a^2/p^2$, $E = -b^2/p^3$). Por el lema 1.1., tomando $C = 0$, $D = -3aq/p^2$, $E = -dq^2/p^3$, $\theta_1/p \in R$. Y como $v_p(\text{disc}(1,\theta^2/p,\theta_1/p)) = 1$, dicha base es minimal en p. Por ser $\{1,\theta,\theta^2/p\}$ una Q-base de enteros tal que p divide

estrictamente a su discriminante, dicha base es también minimal en p.

c.q.d.

Proposición 1.33.: Si $v_p(b) \geq 3$ y $v_p(a) = 0$, entonces $(1,\theta,\theta^2)$ es minimal en p y $v_p(D) = 0$.

Demostración: Inmediata, pues $s_p = 0$. Además, 1 y θ^2 son elementos de la base minimal en p que se obtiene al aplicar el teorema de Harvey-Cohn a la base $(1,\theta^2,\theta_1)$. El tercer elemento de dicha base depende del valor de $v_p(b)$.

Proposición 1.34.: Si $v_p(b) \geq 3$ y $v_p(a) = 1$, entonces $(1,\theta,\theta^2/p)$ es minimal en p y $v_p(D) = 1$.

Demostración: Tomando $C = -2a/p$, $D = a^2/p^2$ y $E = -b^2/p^3$ en el lema 1.1., $\theta^2/p \in R$. Como $v_p(\text{disc}(1,\theta,\theta^2/p)) = 1$, dicha base es minimal en p y $v_p(D) = 1$. Además, 1 y θ^2/p son elementos de la base minimal en p que se obtiene al aplicar el teorema de Harvey-Cohn a la base $(1,\theta^2,\theta_1)$.

c.q.d.

1.B. CARACTERIZACION DE LA MONOGENEIDAD PARA DIVERSAS FAMILIAS INFINITAS DE CUERPOS CUBICOS.

Como corolario inmediato de los resultados obtenidos en el apartado anterior, 1.A., sobre bases minimales, estudiamos a continuación diversas familias infinitas de cuerpos de números cúbicos. Para los cuerpos de cada una de tales familias la tesis da una base entera, el discriminante y una caracterización de la monogeneidad en términos de la resolución de una ecuación diofántica. En cada caso dicho estudio es realizado en función exclusivamente de los coeficientes de un polinomio de función del cuerpo en cuestión.

Proposición 1.35.: Consideremos la familia infinita de cuerpos cúbicos $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - ax + b$ donde a y b verifican las siguientes condiciones:

(1) ($v_3(b) = 1$, $v_3(a) \geq 2$) ó ($3 \mid a$, $3 \nmid b$, $a \not\equiv 3(9)$ y $b^2 \not\equiv a + 1(9)$) ó ($a \equiv 3(9)$, $b^2 \equiv 4(9)$ y $b^2 \not\equiv a + 1(27)$).

(2) ($1 = v_2(b) \leq v_2(a)$) ó ($v_2(b) = 0$) ó ($v_2(b) = 1$, $v_2(a) = 0$ y $q \equiv 3(4)$) ó ($v_2(b) = 1$, $v_2(a) = 0$ y $s_2 = v_2(4a^3 - 27b^2)$ impar).

(3) Para $p > 3$, primo:

($v_p(b) = 1 \leq v_p(a)$) ó ($v_p(b) = 0$).

Entonces:

(i) $\{1,\theta^2,\theta_1/3\}$ es base entera de K.

(ii) $disc(K) = 3^2b^2q$.

(iii) K es monogénico sii $(d/3)y^3 - ay^2z + (q/3)z^3 = \pm 1$

tiene solución en $y,z \in Z$.

Demostración:

(i) e (ii) como consecuencia del estudio realizado en el apartado 1.A. la base $(1,\theta^2,\theta_1/3)$ es minimal en cada primo. Luego es una base entera de K y disc(K) = $= (\text{disc}(1,\theta^2,\theta_1/3)) = 3^2b^2q$.

(iii) $\alpha \in R \Longrightarrow \alpha = x + y\theta^2 + z(\theta_1/3)$, con $x,y,z \in Z$.

$\beta = \alpha - x$ verifica índice(α) = índice(β). Calculando índice(β) tendremos calculados los posibles índices en R. Por notación, $\alpha \approx \beta$ significa que la diferencia está en Z.

$\beta^2 \approx ((5a/3)y^2 - (q/3)z^2)\theta^2 + ((d/3)y^2 + (2a/3)yz)(\theta_1/3)$.

Luego índice(β) = $|\ (d/3)y^3 + (q/3)z^3 - azy^2\ |$.

Como K monogénico sii existe $\alpha \in R$ tal que índice(α) = 1, tenemos ya demostrado el resultado enunciado.

c.q.d.

Proposición 1.36.: Consideremos la familia infinita de cuerpos cúbicos $K = Q(\theta)$, $\text{Irr}(\theta,Q) = x^3 - ax + b$ donde a y b verifican las siguientes condiciones:

(1) $a \equiv 3(9)$, $3 \nmid b$, $b^2 \not\equiv 4(9)$.

(2) $(2 = v_2(b) \leq v_2(a))$ ó $(v_2(b) = 2\ ,\ v_2(a) = 1)$.

(3) Para $p > 3$, primo:

$(v_p(b) = 1 \leq v_p(a))$ ó $(v_p(b) = 0)$.

Entonces:

(i) $(1,\theta^2/2,\theta_1)$ es base entera de K.

(ii) $\text{disc}(K) = 3^4(b/2)^2q$.

(iii) K es monogénico sii $(d/36)y^3 - (a/2)y^2z + 6qz^3 = \pm 1$ tiene solución en $y,z \in Z$.

Proposición 1.37.: Consideremos la familia infinita de cuerpos cúbicos $K = Q(\theta)$, $\text{Irr}(\theta,Q) = x^3 - ax + b$ donde a y b verifican las siguientes condiciones:

(1) $a \equiv 3(9)$, $3 \nmid b$, $b^2 \not\equiv 4(9)$.

(2) $(1 = v_2(b) \leq v_2(a))$ ó $(v_2(b) = 0)$ ó $(v_2(b) = 1$, $v_2(a) = 0$ y $q \equiv 3(4))$ ó $(v_2(b) = 1$, $v_2(a) = 0$ y $s_2 = v_2(4a^3 - 27b^2)$ impar).

(3) Para un cierto $t > 3$ primo, $v_t(b) = 2$ y $v_t(a) = 1$.

(4) Para $p > 3$, $p \neq t$, primo:
$(v_p(b) = 1 \leq v_p(a))$ ó $(v_p(b) = 0)$.

Entonces:

(i) $\{1,\theta^2/t,\theta_1/t\}$ es base entera de K.

(ii) $\text{disc}(K) = 3^4(b/t^2)^2q$.

(iii) K es monogénico sii $(d/9t)y^3 - (a/t)y^2z + (3q/t)z^3 = \pm 1$ tiene solución en $y,z \in Z$.

Corolario: En las hipótesis de la proposición anterior, si $d = 9t$ entonces K es monogénico siendo $y = 1$, $z = 0$.

Proposición 1.38.: Consideremos la familia infinita de cuerpos cúbicos $K = Q(\theta)$, $\text{Irr}(\theta,Q) = x^3 - ax + b$ donde a y b verifican las siguientes condiciones:

(1) $(v_3(b) = 2, v_3(a) = 3)$ ó $(v_3(b) = v_3(a) = 2)$.

(2) $(1 = v_2(b) \leq v_2(a))$ ó $(v_2(b) = 0)$ ó $(v_2(b) = 1$, $v_2(a) = 0$ y $q \equiv 3(4))$ ó $(v_2(b) = 1$, $v_2(a) = 0$ y

$s_2 = v_2\ (4a^3 - 27b^2)$ impar).

(3) Para $p > 3$, primo:

$v_p(b) = 1 \leq v_p(a))$ ó $(v_p(b) = 0)$.

Entonces:

(i) $\{1,\theta^2/3,\theta_1/3\}$ es base entera de K.

(ii) $disc(K) = b^2q$.

(iii) K es monogénico sii $(d/27)y^3 - (a/3)y^2z + qz^3 = \pm 1$ tiene solución en $y,z \in Z$.

Proposición 1.39.: Consideremos la familia infinita de cuerpos cúbicos $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - ax + b$ donde a y b verifican las siguientes condiciones:

(1) ($v_3(b) = 1$, $v_3(a) \geq 2$) ó ($3 \mid a$, $3 \nmid b$, $a \not\equiv 3(9)$ y $b^2 \not\equiv a + 1(9)$) ó ($a \equiv 3(9)$, $b^2 \equiv 4(9)$ y $b^2 \not\equiv a + 1(27)$).

(2) ($2 = v_2(b) \leq v_2(a)$) ó ($v_2(b) = 2$, $v_2(a) = 1$).

(3) Para $p > 3$, primo:

$(v_p(b) = 1 \leq v_p(a))$ ó $(v_p(b) = 0)$.

Entonces:

(i) $\{1,\theta^2/2,\theta_1/3\}$ es base entera de K.

(ii) $disc(K) = 3^2(b/2)^2q$.

(iii) K es monogénico sii $(d/12)y^3 - (a/2)y^2z + (2q/3)z^3 = \pm 1$ tiene solución en $y,z \in Z$.

Proposición 1.40.: Consideremos la familia infinita de cuerpos cúbicos $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - ax + b$ donde a y b verifican las siguientes condiciones:

(1) $a \equiv 3(9)$, $3 \nmid b$, $b^2 \not\equiv 4(9)$.

(2) ($1 = v_2(b) \leq v_2(a)$) ó ($v_2(b) = 0$) ó ($v_2(b) = 1$, $v_2(a)$

$= 0$ y $q \equiv 3(4)$) ó ($v_2(b) = 1$, $v_2(a) = 0$ y $s_2 = v_2\ (4a^3 - 27b^2)$ impar).

(3) Para $p > 3$, primo:

$(v_p(b) = 1 \leq v_p(a))$ ó $(v_p(b) = 0)$.

Entonces:

(i) $\{1,\theta^2,\theta_1\}$ es base entera de K.

(ii) $disc(K) = 3^4b^2q$.

(iii) K es monogénico sii $(d/9)y^3 - ay^2z + 3qz^3 = \pm 1$ tiene solución en $y,z \in Z$.

CAPITULO II. DESCOMPOSICION EN K DE UN PRIMO p DE Q.

II. DESCOMPOSICION EN K DE UN PRIMO p DE Q.

En este Capítulo, obtenemos la descomposición en K, cuerpo de numeros cúbico, de un primo p de Q. En 1983, Pascual Llorente y Enric Nart [L,N] dan los grados de inercia y los índices de ramificación de dicha descomposición. Con el estudio que vamos a realizar a continuación, completamos dicho estudio dando la descomposición exacta.

Con este fin, en cada caso, aplicamos el lema de Kummer [M,th.27], tras obtener un elemento α de R tal que el primo en cuestión no divida a su índice. Para encontrar dicho elemento utilizamos las bases minimales obtenidas en el Capítulo I.

El buen funcionamiento de este método seguido por la tesis, viene garantizado porque en un cuerpo cúbico sólo 2 puede ser factor común de índices y lo es si y sólo si 2 descompone completamente. En efecto, en 1907, Bauer demostró que si $p < n$ existe un cuerpo de grado n en el cual p es un factor común de índices. Von Zylinsky, en 1913, establece la necesidad de esta condición; o sea, p puede ser un factor común de índices de un cuerpo de grado n sólo si $p < n$. H.T. Engstrom [E] ha investigado que potencias de esos primos pueden ser divisores de los índices de un cuerpo dado. En concreto, para K cuerpo cúbico, H.T. Engstrom demuestra que sólo 2 puede ser factor común de índices y lo es si y solo si

2 descompone completamente. Pascual Llorente y Enric Nart [L,N] han dado un criterio, muy sencillo, que nos permite saber cuando 2 es factor común de índices en términos de los coeficientes a y b de un polinomio $x^3 - ax + b$ definición de K. En concreto, demuestran que 2 es factor común de índices si y solo si a es impar, b par, $s_2 = v_2 (4a^3 - 27b^2)$ par y $\underline{\Omega}_2 \equiv 1(8)$.

Con el fin de facilitar, en algunos casos, la descomposición módulo Z_p [x] de Irr(α,Q) recurrimos al teorema 10.61 de Harvey-Cohn [HC2]. Este teorema establece que si p es un primo de Z y con "e" denotamos al índice de ramificación de un primo de R que yace sobre p, entonces $v_p(D) = - 1 + e + h$ donde $h = 0$ si $p \nmid e$, $h > 0$ si $p \mid e$. Se recuerda que D es el discriminante de K.

Empezamos el estudio de las ramificaciones en R de un primo p de Z. Para dicho estudio distinguimos tres casos: $p = 3$, $p = 2$ y $p > 3$. Es conveniente volver a resaltar que el estudio es realizado en términos exclusivamente de los coeficientes de un polinomio definición de K.

DESCOMPOSICION EN R DEL PRIMO 3 DE Z.

Siguiendo la notación prefijada, $K = Q(\theta)$, $disc(K) = D$, $Irr(\theta,Q) = x^3 - ax + b$, donde se supone que no existe ningún primo p tal que $p^3 \nmid b$ y $p^2 \mid a$.

Por los resultados obtenidos en el Capítulo I, sabemos que $v_3(D) \in \{0,1,3,4,5\}$. Vamos a estudiar por separado cada uno de estos cinco posibles casos.

Caso a): $v_3(D) = 0$

El caso $v_3(D) = 0$ ocurre si y solo si ($3 \nmid a$) ó ($a \equiv 3(9)$, $b^2 \equiv a + 1(27)$ y s_3 par).

Proposición 2.1.: Si $3 \nmid a$ entonces:

(i) $a \equiv -1(3)$, $b \equiv 0(3)$ ==> $3R = (3,\theta)(3,\theta^2 + 1)$.

(ii) $a \equiv -1(3)$, $b \equiv 1(3)$ ==> $3R = (3,\theta - 1)(3,\theta^2 + \theta + 2)$.

(iii) $a \equiv -1(3)$, $b \equiv 2(3)$ ==> $3R = (3,\theta - 2)(3,\theta^2 + 2\theta + 2)$.

(iv) $a \equiv 1(3)$, $b \equiv 0(3)$ ==> $3R = (3,\theta)(3,\theta - 1)(3,\theta - 2)$.

(v) $a \equiv 1(3)$, $b \equiv 1(3)$ ==> $3R = (3,\theta^3 - \theta + 1)$.

(vi) $a \equiv 1(3)$, $b \equiv 2(3)$ ==> $3R = (3,\theta^3 - \theta + 2)$.

Demostración: $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - ax + b$, $disc(\theta) = 4a^3 - 27b^2 = d^2q$ (q libre de cuadrados).

$3 \nmid a$ ==> $3 \nmid disc(\theta)$ ==> $3 \nmid$ índice (θ).

Podemos pues aplicar el lema de Kummer [M,th.27], a dicho elemento.

Si $a \equiv -1(3)$:

$Irr(\theta,Q) = x^3 - ax + b \equiv x(x^2 + 1)$ si $b \equiv 0(3)$.

$\equiv (x - 1)(x^2 + x + 2)$ si $b \equiv 1(3)$.

$\equiv (x - 2)(x^2 + 2x + 2)$ si $b \equiv 2(3)$.

(módulo $Z_3[x]$).

Si $a \equiv 1(3)$:

$Irr(\theta,Q) = x^3 - ax + b \equiv x(x - 1)(x - 2)$ si $b \equiv 0(3)$.

$\equiv x^3 - x + 1$ si $b \equiv 1(3)$.

$\equiv x^3 - x + 2$ si $b \equiv 2(3)$.

(módulo $Z_3[x]$).

c.q.d.

<u>Proposición 2.2.</u>: Si $a \equiv 3(9)$, $b^2 \equiv a + 1(27)$ y $s_3 = v_3 (4a^3 - 27b^2)$ es par, entonces:

(i) $q \equiv -1(3)$ ==>

$3R = (3,\theta_1/3)(3,(\theta_1/3)^2 + 1)$ si $d/27 \equiv 0(3)$.

$3R = (3,(\theta_1/3) + 1)(3,(\theta_1/3)^2 - (\theta_1/3) - 1)$ si $d/27 \equiv 1(3)$.

$3R \equiv (3,(\theta_1/3) - 1)(3,(\theta_1/3)^2 + (\theta_1/3) - 1)$ si $d/27 \equiv 2(3)$.

(ii) $q \equiv 1(3)$ ==>

$3R = (3,\theta_1/3)(3,(\theta_1/3) - 1)(3,(\theta_1/3) + 1)$ si $d/27 \equiv 0(3)$.

$3R \equiv (3,(\theta_1/3)^3 - (\theta_1/3) + 2)$ si $d/27 \equiv 1(3)$.

$3R \equiv (3,(\theta_1/3)^3 - (\theta_1/3) + 1)$ si $d/27 \equiv 2(3)$.

($\theta_1 = (4a^2 - 9b\theta - 6a\theta^2)/d$).

<u>Demostración</u>: Bajo estas hipótesis, $\theta_1/3 \in R$, $3 \nmid q$, $27 \mid d$ (véase proposición 1.11.); $disc(\theta_1/3) = b^2q^3$.

$b^2 \equiv a + 1(3)$, $a \equiv 0(3)$ ==> $b \not\equiv 0(3)$.

Luego, $3 \nmid disc(\theta_1/3)$ ==> $3 \nmid índice(\theta_1/3)$.

Por otra lado, $a \equiv 3(9)$ ==> $a/3 \equiv 1(3)$; por tanto

$Irr(\theta_1/3,Q) = x^3 - (a/3)qx - (d/27)q^2 \equiv x^3 - qx - (d/27)q^2$

$(Z_3[x])$.

Si $q \equiv -1(3)$, $Irr(\theta_1/3,Q) \equiv x^3 + x - (d/27) \equiv$

$$\begin{cases} \equiv x(x^2+1) & \text{si } d/27 \equiv 0(3). \\ \equiv (x+1)(x^2-x-1) & \text{si } d/27 \equiv 1(3). \\ \equiv (x-1)(x^2+x-1) & \text{si } d/27 \equiv 2(3). \end{cases}$$

Si $q \equiv 1(3)$, $Irr(\theta_1/3,Q) \equiv x^3 + x - (d/27) \equiv$

$$\begin{cases} \equiv x(x-1)(x+1) & \text{si } d/27 \equiv 0(3). \\ \equiv x^3 - x + 2 & \text{si } d/27 \equiv 1(3). \\ \equiv x^3 - x + 1) & \text{si } d/27 \equiv 2(3). \end{cases}$$

c.q.d.

Caso b): $v_3(D) = 1$.

El caso $v_3(D) = 1$ ocurre si y solo si ($1 = v_3(a) < v_3(b)$) ó ($3 \mid a$, $a \not\equiv 3(9)$, $b^2 \equiv a + 1(9)$) ó ($a \equiv 3(9)$, $b^2 \equiv a + 1(27)$ y s_3 impar).

Proposición 2.3.: Si $1 = v_3(a) < v_3(b)$ entonces:

(i) $1 = v_3(a) < v_3(b) = 2$ ==>

$3R = (3,\theta^2/3)(3,(\theta^2/3) - (a/3))^2$.

(ii) $1 = v_3(a) < 3 \leq v_3(b)$ ==>

$3R = (3,2\theta + (\theta^2/3))(3,2\theta + (\theta^2/3) + 1)^2$ si $a \equiv 6(9)$.

$3R = (3,2\theta + (\theta^2/3))(3,2\theta + (\theta^2/3) - 1)^2$ si $a \equiv 3(9)$.

Demostración: Bajo estas hipótesis, por la proposición 1.13., $\theta^2/3 \in R$.

(i) Supongamos $1 = v_3(a) < v_3(b) = 2$.

$disc(\theta^2/3) = 3(b/9)^2((d^2q)/27)$.

$v_3(\ disc(\theta^2/3)\ ) = 1 = v_3(D) \Longrightarrow 3 \nmid$ índice $(\theta^2/3)$.

$Irr(\theta^2/3,Q) = x^3 - (2a/3)x^2 + (\ a^2/9)x - (b^2/27) \equiv$

$\equiv x^3 - (2a/3)x^2 + (\ a^2/9)x \equiv x(x - (a/3))^2$.

$(Z_3[x])$.

(ii) Supongamos ahora $1 \equiv v_3(a) < 3 \leq v_3(b)$.

$2\theta + (\theta^2/3) \in R$;

$disc(2\theta + (\theta^2/3)) \equiv 3((\ 2^3 3^3 + b - 6a\ )/9)^2\ ((d^2q)/27)$.

Pero, $2^3 3^3 + b - 6a \equiv -6a(27)$, y como $-6a \not\equiv 0(27)$ se tiene $v_3(disc(2\theta + (\theta^2/3))) = 1 \equiv v_3(D) \Longrightarrow$

$\Longrightarrow 3 \nmid$ índice $(2\theta + (\theta^2/3))$.

$Irr\ (\ 2\theta + (\theta^2/3),Q) = x^3 - (2a/3)x^2 + ((\ a^2 - 36a +$

$+ 18b)/9)x + (\ 6ab + 6^3 b - b^2)/27 \equiv$

$\equiv x(x^2 - (2a/3)x + (a^2 - 36a)/9)\ (Z_3[x])$.

Ahora bien, $a \equiv 0(3)$, $a \not\equiv 0(9) \Longrightarrow a \equiv 3$ ó $6(9)$.

Si $a \equiv 6(9)$, $Irr\ (\ 2\theta + (\theta^2/3),Q) \equiv x(x + 1)^2\ (Z_3[x])$.

Si $a \equiv 3(9)$, $Irr\ (\ 2\theta + (\theta^2/3),Q) \equiv x(x - 1)^2\ (Z_3[x])$.

c.q.d.

Dentro del caso $3 \mid a$, $a \not\equiv 3(9)$, $b^2 \equiv a + 1(9)$, vamos a considerar los dos posibles subcasos $a \equiv 0(9)$ y $a \equiv 6(9)$.

Proposición 2.4.: Si $a \equiv 0(9)$, $b^2 \equiv a + 1(9)$, entonces:

(i) Si $b \equiv 1(9)$, $a + b \not\equiv 1(27)$,

$3R = (3,(\theta^2 - \theta + 1)/3)^2(3,(\theta^2 - \theta + 1)/3 - 1)$.

(ii) Si $b \equiv 1(9)$, $a + b \equiv 1(27)$,

$3R = (3,\theta + (\theta^2 - \theta + 1)/3)(3,\theta + (\theta^2 - \theta + 1)/3 - 2)^2$

(iii) Si $b \equiv 8(9)$, $a - b \not\equiv 1(27)$,

$3R = (3,(\theta^2 + \theta + 1)/3)^2(3,(\theta^2 + \theta + 1)/3 - 1)$.

(iv) Si $b \equiv 8(9)$, $a - b \equiv 1(27)$,

$3R=(3,\theta+(\theta^2 + \theta + 1)/3 - 1)^2(3,\theta + (\theta^2 + \theta + 1)/3 + 1)$.

Demostración: (i) e (ii): $a \equiv 0(9)$, $b \equiv 1(9)$ ==>

==> $(\theta^2 - \theta + 1)/3 \in R$ (véase proposición 1.15.).

índice $((\theta^2 - \theta + 1)/3)$ = índice $((\theta^2 - \theta)/3)$;

$disc((\theta^2 - \theta)/3) = ((a + b - 1)/9)^2((d^2q)/27)3$.

Si $a + b \not\equiv 1(27)$ entonces $3 \nmid$ índice $((\theta^2 - \theta + 1)/3)$.

$Irr((\theta^2 - \theta + 1)/3,Q) \equiv x^3 - (1 + 2a/3)x^2 + ((a^2 + 3a - 3b +$

$+ 3)/9)x + (ab - a + 2b - b^2 - a^2 - 1)/27 \equiv$

$\equiv x^3 - x^2 + (ab - a + 2b - b^2 - 1)/27(Z_3[x])$.

Ahora bien, $3 \mid disc(K)$ ==> 3 ramificado en K ==> existe un primo de R cuyo grado de inercia sobre 3, e, es mayor que uno. Por el teorema 10.61. de Harvey-Cohn [HC2], $v_3(D) = 1 = - 1 + e + h$ siendo $e = 2$ ó 3 y $h \equiv 0$ si $3 \nmid e$, y $h > 0$ si $3 \mid e$. Si fuera $e = 3$, sería $1 = 2 + h$ con $h > 0$, absurdo. Luego $e = 2$ y $3R = P^2Q$. Necesariamente $(ab - a + 2b - b^2 - 1)/27 \equiv 0(3)$ e $Irr((\theta^2 - \theta + 1)/3,Q) \equiv$ $\equiv x^2(x - 1)$ $(Z_3[x])$.

Supongamos ahora $a + b \equiv 1(27)$; $\theta + ((\theta^2 - \theta + 1)/3) \in R$.

$disc(\theta + ((\theta^2 - \theta + 1)/3)) = 3((8 - 2a + b)/9)^2((d^2q)/27)$.

$a + b \equiv 1(27)$ ==> $8 - 2a + b \not\equiv 0(27)$; de lo contrario,

$1 - a - 2a + 8 \equiv 0(27) \Longrightarrow a \equiv 3(9)$, absurdo.

Luego $3 \nmid$ índice $(\theta + ((\theta^2 - \theta + 1)/3))$.

$\text{Irr}\,(\theta + (\theta^2 - \theta + 1)/3, Q) = x^3 - (1 + 2a/3)x^2 + ((a^2 + 6b + 3)/9)x + (-2ab + 2a + 2b - b^2 - a^2 - 1)/27 \equiv$

$\equiv x^3 - x^2 + x + (-2ab + 2a + 2b - b^2 - 1)/27$ $(Z_3[x])$.

Y, como $3R = P^2Q$, necesariamente $\text{Irr}\,(\theta + (\theta^2 - \theta + 1)/3, Q) \equiv$

$\equiv x(x - 2)^2$ $(Z_3[x])$.

(iii) e (iv): $a \equiv 0(9)$, $b \equiv 8(9) \Longrightarrow$ $(\theta^2 + \theta + 1)/3 \in R$ (véase proposición 1.15.).

índice $((\theta^2 + \theta + 1)/3) =$ índice $((\theta^2 + \theta)/3)$;

$\text{disc}\,((\theta^2 + \theta)/3) = 3((-a + b + 1)/9)^2((d^2q)/27)$.

Si $a - b \not\equiv 1(27)$ entonces $3 \nmid$ índice $((\theta^2 + \theta + 1)/3)$.

$\text{Irr}\,((\theta^2 + \theta + 1)/3, Q) = x^3 - (1 + 2a/3)x^2 + ((a^2 + 3a + 3b + 3)/9)x + (-ab - a - 2b - b^2 - a^2 - 1)/27 \equiv$

$\equiv x^3 - x^2 - (ab + a + 2b + b^2 + a^2 + 1)/27 \equiv$

$\equiv x^3 - x^2$ (ya que $3R = P^2Q$) $\equiv x^2(x - 1)$ $(Z_3[x])$.

Supongamos ahora $a - b \equiv 1(27)$; consideramos en este caso $\theta + ((\theta^2 + \theta + 1)/3) \in R$.

$\text{disc}\,(\theta + ((\theta^2 + \theta + 1)/3)) = 3((64 - 4a + b)/9)^2((d^2q)/27)$.

$64 - 4a + b \not\equiv 0(27)$; de lo contrario, $63 \equiv 3a(27) \Longrightarrow$ $a \equiv 3(9)$, absurdo.

Luego $3 \nmid$ índice $(\theta + ((\theta^2 + \theta + 1)/3))$.

$\text{Irr}\,(\theta + (\theta^2 + \theta + 1)/3, Q) = x^3 - (1 + 2a/3)x^2 + ((a^2 + 12b - 12a + 3)/9)x + (-4ab + 14a + 52b - b^2 - a^2 - 1)/27 \equiv$

$\equiv x^3 - x^2 + 2x + (-4ab + 14a + 52b - b^2 - a^2 - 1)/27 \equiv$

$\equiv x^3 - x^2 + 2x + 1$ (pues $3R = P^2Q$) $\equiv (x-1)^2(x+1)$ $(Z_3[x])$.

c.q.d.

Proposición 2.5.: Si $a \equiv 6(9)$, $b^2 \equiv a + 1(9)$, entonces:

(i) Si $b \equiv 4(9)$, $a + b \not\equiv 1(27)$,

$3R = (3, -2 + (\theta^2 - \theta + 1)/3)^2(3, 2 + (\theta^2 - \theta + 1)/3)$.

(ii) Si $b \equiv 4(9)$, $a + b \equiv 1(27)$,

$3R = (3,\theta + (\theta^2 - \theta + 1)/3)(3,\theta + (\theta^2 - \theta + 1)/3 - 1)^2$.

(iii) Si $b \equiv 5(9)$, $a - b \not\equiv 1(27)$,

$3R = (3, -2 + (\theta^2 + \theta + 1)/3)^2(3,(\theta^2 + \theta + 1)/3 + 2)$.

(iv) Si $b \equiv 5(9)$, $a - b \equiv 1(27)$,

$3R = (3,\theta+(\theta^2 + \theta + 1)/3)^2(3,\theta + (\theta^2 + \theta + 1)/3 - 2)$.

Demostración: Por la proposición 1.15., si $a \equiv 6(9)$, $b \equiv 4(9)$ entonces $(\theta^2 - \theta + 1)/3 \in R$. Y si $a \equiv 6(9)$, $b \equiv 5(9)$ entonces $(\theta^2 + \theta + 1)/3 \in R$.

La misma demostración que en la proposición anterior nos permite concluir que si $a \equiv 6(9)$:

$$b \equiv 4(9) \begin{cases} / \; a + b \not\equiv 1(27),\ 3 \nmid \text{indice } ((\theta^2 - \theta + 1)/3) \\ \backslash \; a + b \equiv 1(27),\ 3 \nmid \text{índice } (\theta + (\theta^2 - \theta + 1)/3) \end{cases}$$

$$b \equiv 5(9) \begin{cases} / \; a - b \not\equiv 1(27),\ 3 \nmid \text{índice } ((\theta^2 + \theta + 1)/3) \\ \backslash \; a - b \equiv 1(27),\ 3 \nmid \text{índice } (\theta + (\theta^2 + \theta + 1)/3) \end{cases}$$

Con el fin de aplicar el lema de Kummer [M,th.27]

necesitamos conocer el irreducible sobre Q de cada uno de estos elementos. Dichos polinomios han sido dados en la demostración de la proposición anterior. Pasamos a estudiar la descomposición módulo $Z_3[x]$ de cada uno de esos polinomios. Recurrimos al teorema 10.61. de Harvey-Cohn [HC2] para afirmar que $3R = P^2Q$.

En el caso $a \equiv 6(9)$, $b \equiv 4(9)$ y $a + b \not\equiv 1(27)$,

$$\text{Irr}\,((\theta^2 - \theta + 1)/3, Q) = x^3 - (1 + 2a/3)x^2 + ((a^2 + 3a - 3b + 3)/9)x + (ab - a + 2b - b^2 - a^2 - 1)/27 \equiv$$
$$\equiv x^3 - 2x^2 + 2x + 2 \equiv (x - 2)^2(x + 2) \quad (Z_3[x]),$$

pues $1 + 2a/3 \equiv 2(3)$, $(a^2 + 3a - 3b + 3)/9 \equiv 2(3)$ y $3R = P^2Q$.

En el caso $a \equiv 6(9)$, $b \equiv 4(9)$ y $a + b \equiv 1(27)$,

$$\text{Irr}\,(\theta + (\theta^2 - \theta + 1)/3, Q) = x^3 - (1 + 2a/3)x^2 + ((a^2 + 6b + 3)/9)x + (-2ab + 2a + 2b - b^2 - a^2 - 1)/27 \equiv$$
$$\equiv x^3 - 2x^2 + x \equiv x(x - 1)^2 \quad (Z_3[x]),$$

pues $1 + 2a/3 \equiv 2(3)$, $(a^2 + 6b + 3)/9 \equiv 1(3)$ y $3R = P^2Q$.

Para $a \equiv 6(9)$, $b \equiv 5(9)$ y $a - b \not\equiv 1(27)$,

$$\text{Irr}\,((\theta^2 + \theta + 1)/3, Q) = x^3 - (1 + 2a/3)x^2 + ((a^2 + 3a + 3b + 3)/9)x + (-ab - a - 2b - b^2 - a^2 - 1)/27 \equiv$$
$$\equiv x^3 - 2x^2 + 2x + 2 \equiv (x - 2)^2(x + 2) \quad (Z_3[x]),$$

pues $1 + 2a/3 \equiv 2(3)$, $(a^2 + 3a + 3b + 3)/9 \equiv 2(3)$ y $3R = P^2Q$.

Y, por último, si $a \equiv 6(9)$, $b \equiv 5(9)$ y $a - b \equiv 1(27)$,

$$\text{Irr}\,(\theta + (\theta^2 + \theta + 1)/3, Q) = x^3 - (1 + 2a/3)x^2 + ((a^2 + 12b - 9)/9)x + (-4ab + 14a + 52b - b^2 - a^2 - 1)/27 \equiv$$
$$\equiv x^3 - 2x^2 \equiv x^2(x - 2) \quad (Z_3[x]).$$

pues $1 + 2a/3 \equiv 2(3)$, $(a^2 - 12a + 12b + 3)/9 \equiv$
$\equiv 0(3)$ y $3R = P^2Q$.

c.q.d.

Proposición 2.6.: Si $a \equiv 3(9)$, $b^2 \equiv a + 1(27)$ y $s_3 = v_3(4a^3 - 27b^2)$ impar entonces:

(i) Para $s_3 \geq 9$,

Si $a \equiv 3(27)$ ==>

$3R = (3,(-1 + \theta^2)/3 + \theta_1/3 - 1)(3,(-1 + \theta^2)/3 + \theta_1/3)^2$

Si $a \equiv 12(27)$ ==>

$3R = (3,(-1 + \theta^2)/3 + \theta_1/3 - 2)(3,(-1 + \theta^2)/3 + \theta_1/3 - 1)^2$

Si $a \equiv 21(27)$ ==>

$3R = (3,(-1 + \theta^2)/3 + \theta_1/3)(3,(-1 + \theta^2)/3 + \theta_1/3 - 2)^2$

(ii) Para $s_3 = 7$,

Si $a \equiv 3(27)$ ==>

$3R = (3,(-1 + \theta^2)/3 - 1)(3,(-1 + \theta^2)/3)^2$

Si $a \equiv 12(27)$ ==>

$3R = (3,(-1 + \theta^2)/3 - 2)(3,(-1 + \theta^2)/3 - 1)^2$

Si $a \equiv 21(27)$ ==>

$3R = (3,(-1 + \theta^2)/3)(3,(-1 + \theta^2)/3 - 2)^2$

($\theta_1 = (4a^2 - 9b\theta - 6a\theta^2)/d$; $4a^3 - 27b^2 = d^2q$).

Nota: Bajo las hipótesis de esta proposición, necesariamente $s_3 = v_3(4a^3 - 27b^2) \geq 7$. En efecto:

$a \equiv 3(9)$ ==> $a = 3 + 9r$ con $r \in Z$ ==> $(a/3)^3 = 1 +$
$+ 27r^3 + 9r + 27r^2$ ==> $4(a/3)^3 - b^2 \equiv 4(a/3)^3 - (a + 1)$
$\equiv 4 + 36r - 3 - 9r - 1 \equiv 27r \equiv 0(27)$.

Demostración:

(i) En este caso, $(-1 + \theta^2)/3 + \theta_1/3 \in R$.

$\text{disc}((-1 + \theta^2)/3 + \theta_1/3) = ((d - 9a + 27q)/27)^2 b^2 q$; como $d - 9a + 27q \equiv -9a(3^4)$ y $-9a \not\equiv 0(3^4)$ entonces tenemos 3 $\not|$ índice $((-1 + \theta^2)/3 + \theta_1/3)$.

$$\text{Irr}((-1 + \theta^2)/3 + \theta_1/3, Q) =$$
$$= x^3 + ((3 - 2a)/3)x^2 +$$
$$+ ((dq - 3aq + a^2 + 3 - 4a)/9)x +$$
$$+ (-2a + 1 - b^2 + a^2 - dq^2 - adq + dq + 4a^2q - 3aq)/27.$$

Por otro lado, $a \equiv 3(9) \Longrightarrow a \equiv 3, 12$ ó $21\ (27)$.

Supongamos en primer lugar, $a \equiv 3(27)$:

$(dq - 3aq + a^2 + 3 - 4a)/9 \equiv (a^2 + 3 - 4a)/9\ (3)$, pero

$a \equiv 3(27) \Longrightarrow a^2 + 3 - 4a = (a - 3)^2 - 6 + 2a \equiv 2a - 6 \equiv$
$\equiv 0(27)$.

Luego, $(a^2 + 3 - 4a)/9 \equiv 0(3)$.

$(3 - 2a)/3 = (-2\ (a - 3) - 3)/3 \equiv -3/3 \equiv -1(3)$.

Y no hace falta encontrar el representante módulo 3 de la clase del término independiente del polinomio en cuestión ya que $\text{Irr}((-1 + \theta^2)/3 + \theta_1/3, Q) \equiv$

$$\equiv x^3 - x^2 \equiv x^2(x - 1), \text{ ó}$$
$$\equiv x^3 - x^2 + 1, \text{ ó}$$
$$\equiv x^3 - x^2 - 1 \equiv (x - 2)(x^2 + x + 2)$$
$$(Z_3[x]).$$

Pero $v_3(D) = 1$, luego 3 es ramificado en K. Y, necesariamente, $\text{Irr}((-1 + \theta^2)/3 + \theta_1/3, Q) \equiv x^2(x - 1)$
$(Z_3[x])$.

Supongamos en segundo lugar, $a \equiv 12(27)$:

$(dq - 3aq + a^2 + 3 - 4a)/9 \equiv (a^2 + 3 - 4a)/9\ (3)$, pero

$a \equiv 12(27) \Longrightarrow a^2 + 3 - 4a = (a - 3)^2 - 6 + 2a \equiv 2a - 6 \equiv$
$\equiv 18(27)$.

Luego, $(a^2 + 3 - 4a)/9 \equiv 2(3)$.

$(3 - 2a)/3 = (-2\,(a - 3) - 3)/3 \equiv -3/3 \equiv -1(3)$.

Y no hace falta encontrar el representante módulo 3 de la clase del término independiente del polinomio en cuestión ya que $\mathrm{Irr}\,((-1 + \theta^2)/3 + \theta_1/3, Q) \equiv$

$$\equiv x^3 - x^2 - x + 1 \equiv (x - 2)(x - 1)^2, \text{ ó}$$
$$\equiv x^3 - x^2 - x - 1, \text{ ó}$$
$$\equiv x^3 - x^2 - x \equiv x(x^2 - x - 1)$$

$(Z_3[x])$.

Pero $v_3(D) = 1$, luego 3 es ramificado en K. Y, necesariamente, $\mathrm{Irr}\,((-1 + \theta^2)/3 + \theta_1/3, Q) \equiv (x - 2)(x - 1)^2$, $(Z_3[x])$.

Supongamos en tercer lugar, $a \equiv 21(27)$:

$(dq - 3aq + a^2 + 3 - 4a)/9 \equiv (a^2 + 3 - 4a)/9\ (3)$, pero

$a \equiv 21(27) \Longrightarrow a^2 + 3 - 4a = (a - 21)^2 - 438 + 38a$;

Luego, $(a^2 + 3 - 4a)/9 \equiv (38(a - 21) + 360)/9 \equiv 360/9 \equiv 1(3)$.

$(3 - 2a)/3 \equiv -1(3)$.

No hace falta encontrar el representante módulo 3 de la clase del término independiente del polinomio en cuestión ya que $\mathrm{Irr}\,((-1 + \theta^2)/3 + \theta_1/3, Q) \equiv$

$$\equiv x^3 - x^2 + x + 1\ , \text{ ó}$$
$$\equiv x^3 - x^2 + x - 1 \equiv (x - 1)(x^2 + 1), \text{ ó}$$
$$\equiv x^3 - x^2 + x \equiv x(x - 2)^2$$

$(Z_3[x])$.

Pero 3 es ramificado en K. Y, necesariamente, $\mathrm{Irr}\,((-1 + \theta^2)/3 + \theta_1/3, Q) \equiv x(x - 2)^2$, $(Z_3[x])$.

(ii) En este caso, $(-1 + \theta^2)/3 \in R$.

disc $((-1 + \theta^2)/3) = (d/27)^2 b^2 q$; $v_3(\text{disc}((-1 + \theta^2)/3)) = 1 = v_3(D)$, $3 \nmid$ índice $((-1 + \theta^2)/3)$.

Irr $((-1 + \theta^2)/3, Q) =$

$= x^3 + ((3 - 2a)/3)x^2 +$

$+ ((a^2 + 3 - 4a)/9)x +$

$+ (-2a + 1 - b^2 + a^2)/27$, polinomio que es congruente módulo $Z_3[x]$ con el polinomio del apartado anterior. Se distinguen, pues, los mismos casos que en el apartado (i) y se tiene demostrada la proposición.

c.q.d.

Caso c): $v_3(D) = 3$

El caso $v_3(D) = 3$ ocurre si y solo si $(v_3(a) = v_3(b) = 1)$ ó $(3 \mid a, 3 \nmid b, a \not\equiv 3(9), b^2 \not\equiv a + 1(9))$ ó $(a \equiv 3(9), b^2 \equiv 4(9), b^2 \not\equiv a + 1(27))$.

Vamos a analizar cada subcaso por separado.

Proposición 2.7.: Si $v_3(a) = v_3(b) = 1$, entonces $3R = (3,\theta)^3$.

Demostración: En este caso, $v_3(\text{disc}(\theta)) = v_3(4a^3 - 27b^2) = 3 = v_3(D)$, luego $3 \nmid$ índice(θ).

Irr $(\theta, Q) = x^3 - ax + b \equiv x^3$ $(Z_3[x])$.

c.q.d.

Proposición 2.8.: Si $3 \mid a$, $3 \nmid b$, $a \not\equiv 3(9)$, $b^2 \not\equiv a + 1(9)$ entonces: (i) $3R = (3,\theta - 2)^3$ si $b \equiv 1(3)$.

(ii) $3R = (3,\theta - 1)^3$ si $b \equiv 2(3)$.

Demostración: $s_3 = v_3(4a^3 - 27b^2) = 3$ (véase la demostración

de la proposición 1.10.) = $v_3(D)$ ==> 3 $\nmid$ índice(θ).

Irr (θ,Q) = $x^3 - ax + b \equiv (x - 2)^3$ si $b \equiv 1(3)$

$\equiv (x - 1)^3$ si $b \equiv 2(3)$,

($Z_3[x]$).

c.q.d.

Proposición 2.9.: Si $a \equiv 3(9)$, $b^2 \equiv 4(9)$, $b^2 \not\equiv a + 1(27)$, entonces $3R = (3,\theta_1/3)^3$.

Demostración: Bajo estas hipótesis $\theta_1/3 \in R$; $disc(\theta_1/3) = b^2q^3$ ==> $v_3(disc(\theta_1/3)) = 3 = v_3(D)$ ==> 3 $\nmid$ índice(θ/3).

Irr (θ/3,Q) = $x^3 - (qa/3)x - (dq^2)/27 \equiv x^3$ ($Z_3[x]$), ya que bajo las condiciones enunciadas en la proposición 9 | d, 3 || q.

c.q.d.

Caso d): $v_3(D) = 4$.

El caso $v_3(D) = 4$ ocurre si y solo si ($v_3(a) = v_3(b) = 2$) ó ($a \equiv 3(9)$, 3 $\nmid$ b, $b^2 \not\equiv 4(9)$).

Vamos a analizar cada subcaso por separado.

Proposición 2.10.: Si $v_3(a) = v_3(b) = 2$, entonces $3R = (3,\theta^2/3)^3$.

Demostración: En este caso, $\theta^2/3 \in R$; $disc(\theta^2/3) = b^2((d^2q)/3^6)$; por ser $v_3(d^2q) = 6$, $v_3(disc(\theta^2/3)) = 4 = v_3(D)$, luego 3 $\nmid$ índice(θ^2/3).

Irr (θ^2/3,Q) = $x^3 - (2a/3)x^2 + (a^2/9)x - (b^2/27) \equiv x^3$,($Z_3[x]$).

Proposición 2.11.: Si $a \equiv 3(9)$, $3 \nmid b$, $b^2 \not\equiv 4(9)$ entonces:

(i) $3R = (3,\theta - 2)^3$ si $b \equiv 1(3)$.

(ii) $3R = (3,\theta - 1)^3$ si $b \equiv 2(3)$.

Demostración: $s_3 = v_3(4a^3 - 27b^2) = 4$ (véase la demostración de la proposición 1.9.) $= v_3(D) \Longrightarrow 3 \nmid$ índice(θ).

Irr $(\theta,Q) = x^3 - ax + b \equiv (x - 2)^3$ si $b \equiv 1(3)$

$\equiv (x - 1)^3$ si $b \equiv 2(3)$,

$(Z_3[x])$.

c.q.d.

Caso e): $v_3(D) = 5$.

El caso $v_3(D) = 5$ ocurre si y solo si $1 \leq v_3(b) < v_3(a)$.

Vamos a considerar los dos posibles subcasos:

$(1 = v_3(b) < v_3(a))$, $(2 = v_3(b) < v_3(a))$.

(Desde un principio se acordó que puede suponerse que no existe un primo p tal que $p^3 \mid b$ y $p^2 \mid a$).

Proposición 2.12.: $1 = v_3(b) < v_3(a) \Longrightarrow 3R = (3,\theta)^3$.

Demostración: Trivial.

Proposición 2.13.: $2 = v_3(b) < v_3(a) \Longrightarrow 3R = (3,\theta^2/3)^3$.

Demostración: $\theta^2/3 \in R$; $\text{disc}(\theta^2/3) = (b^2d^2q)/3^6$; $v_3(\text{disc}(\theta^2/3)) = 5 = v_3(D)$, luego $3 \nmid$ índice$(\theta^2/3)$.

Irr $(\theta^2/3,Q) = x^3 - (2a/3)x^2 + (a^2/9)x - (b^2/27) \equiv x^3$,

$(Z_3[x])$.

c.q.d.

DESCOMPOSICION EN R DEL PRIMO 2 DE Z.

De los estudios realizados en el Capítulo I sobre bases minimales en 2 podemos afirmar que $v_2(D) \in (3, 2, 0)$. Vamos a estudiar cada uno de esos posibles tres casos por separado.

Caso a) : $v_2(D) = 3$.

$v_2(D) = 3$ si y sólo si ($v_2(b) = 1$, $v_2(a) = 0$, $s_2 = v_2(4a^3 - 27b^2)$ es impar) ó ($v_2(b) \geq 3$, $v_2(a) = 1$). Analizamos, a su vez, cada uno de estos subcasos por separado.

Proposición 2.14.: Si $v_2(b) = 1$, $v_2(a) = 0$ y s_2 es impar ===> $2R = (2, \theta^2 + \theta_1)(2, \theta^2 + \theta_1 + 1)^2$.
($\theta_1 = (4a^2 - 9b\theta - 6a\theta^2)/d$).
Demostración : Bajo estas hipótesis, $2 \nmid$ indice$(\theta^2 + \theta_1)$. En efecto, disc$(\theta^2 + \theta_1) = (27q - 9a + d)^2 b^2 q$. Pero $v_2(d^2q) \geq 2$, s_2 impar, q libre de cuadrados ===> $2 \,||\, q$, $2 \mid d$. Y como $v_2(a) = 0$ entonces $v_2(27q - 9a + d) = 0$. Luego $v_2(\text{disc}(\theta^2+\theta_1)) = 3 = v_2(D)$ ===> $2 \nmid$ índice$(\theta^2 + \theta_1)$. $\text{Irr}(\theta^2 + \theta_1, Q) = x^3 - 2ax^2 + (dq - 3aq + a^2)x + (-b^2 - dq^2 - adq + 4a^2q) \equiv x^3 + x \equiv x(x + 1)^2$ $(Z_2[x])$.

c.q.d.

Proposición 2.15. : Si $v_2(b) \geq 3$, $v_2(a) = 1$ ===> ==> $2R = (2, \theta^2/2 + \theta)(2, \theta^2/2 + \theta + 1)^2$.

Demostración : Bajo estas hipótesis vimos en la proposición 1.26 que $\theta^2/2 \in R$;$disc(\theta^2/2 + \theta) = ((-2a + b + 8)/4)^2(d/2)^2q$. Luego, como $v_2(d) = 2$, $2 \mid\mid q$, $v_2(a) = 1$ entonces $v_2(disc(\theta^2/2 + \theta)) = 3 = v_2(D)$ ===> $2 \nmid$ índice$(\theta^2/2 + \theta)$. $Irr(\theta^2/2 + \theta, Q) = x^3 - ax^2 + ((-4a + a^2 + 6b)/4)x + (-b^2 - 2ab + 8b)/8 \equiv x^3 + x \equiv x(x + 1)^2$ $(Z_2[x])$.

c.q.d.

Caso b) : $v_2(D) = 2$.

$v_2(D) = 2$ si y sólo si ($1 \leq v_2(b) \leq v_2(a)$) ó ($s_2 = v_2(4a^3 - 27b^2)$ es par y $\Omega_2 \equiv 3$ (4)). Analizamos, a su vez, cada uno de estos subcasos por separado.

Proposición 2.16. : Si $1 \leq v_2(b) \leq v_2(a)$ ===>

(i) $1 = v_2(b) \leq v_2(a)$ ===> $2R = (2, \theta)^3$.

(ii) $2 = v_2(b) \leq v_2(a)$ ===> $2R = (2, \theta^2/2)^3$.

Demostración:

(i) $1 = v_2(b) \leq v_2(a)$ ===> $s_2 = v_2(4a^3 - 27b^2) = 2 = v_2(D)$ ===> $2 \nmid$ índice(θ). $Irr(\theta, Q) = x^3 - ax + b \equiv x^3$ ($Z_2[x]$).

(ii) Supongamos ahora $2 = v_2(b) \leq v_2(a)$. Bajo estas hipótesis vimos en la proposición 1.17 que $\theta^2/2 \in R$; $disc(\theta^2/2) = (b^2d^2q)/2^6$. Por ser $v_2(disc(\theta^2/2)) = 2 = v_2(D)$ ===> $2 \nmid$ índice$(\theta^2/2)$. $Irr(\theta^2/2, Q) = x^3 - ax^2 + (a^2/4)x - b^2/8 \equiv x^3$ $(Z_2[x])$.

c.q.d.

Proposición 2.17. : Si s_2 es par y $\Omega_2 \equiv 3\ (4)$ ===>

(i) $2 \leq v_2(b)$, $v_2(a) = 0$, $a \equiv 3(4)$ ==>

$$2R \simeq (2,\theta)(2,\theta + 1)^2.$$

(ii) $2 = v_2(b)$, $v_2(a) = 1$ ==>

$$2R \simeq (2,\ \theta^2/2)(2,\ 1 + \theta^2/2)^2.$$

(iii) $1 = v_2(b)$, $v_2(a) = 0$, $q \equiv 3(4)$ ==>

$$2R \simeq (2,\theta_1)(2,\theta_1 + 1)^2.$$

$(\theta_1 = (4a^2 - 9b\theta - 6a\theta^2)/d)$.

Demostración:

(i) Bajo estas hipótesis, $s_2 = v_2(4a^3 - 27b^2) = 2 = v_2(D)$ ===> $2 \nmid$ índice(θ). $Irr(\theta,Q) = x^3 - ax + b \equiv x^3 - x \equiv$

$$\equiv x(x + 1)^2 \ (\ Z_2[x]\ ).$$

(ii) En este caso, por la proposición 1.24., $\theta^2/2 \in R$; $disc(\theta^2/2) = (b^2d^2q)/2^6$. Por ser $v_2(disc(\theta^2/2)) = 2 = v_2(D)$ ===> $2 \nmid$ índice$(\theta^2/2)$. $Irr(\theta^2/2,Q) \simeq x^3 - ax^2 + (a^2/4)x -$ $- b^2/8 \equiv x^3 + x \equiv x(x + 1)^2$ $(Z_2[x])$.

(iii) $\theta_1 \in R$ por el lema 1.2.; $disc(\theta_1) = 3^6b^2q^3$; $v_2(3^6b^2q^3) = 2 = v_2(D)$ ===> $2 \nmid$ índice(θ_1). $Irr(\theta_1,Q) = x^3 -$ $= 3aq\ x - dq^2 \equiv x^3 - x \equiv x(x + 1)^2$ $(Z_2[x])$.

c.q.d.

Caso c) : $v_2(D) = 0$.

$v_2(D) = 0$ si y sólo si ($v_2(b) = 0$) ó ($v_2(b) = 1$, $v_2(a) = 0$, $q \equiv 1(4)$) ó ($v_2(b) = 2$, $v_2(a) = 0$, $a \equiv 1(4)$) ó ($v_2(b) \geq 3$, $v_2(a) = 0$, $a \equiv 1(4)$). Analizamos, a su vez, cada uno de estos

subcasos por separado.

Proposición 2.18. : Si $v_2(b) = 0$ ===>

(i) $1 \leq v_2(a)$ ===> $2R = (2, \theta - 1)(2, \theta^2 + \theta + 1)$.

(ii) $v_2(a) = 0$ ===> $2R = (2, \theta^3 + \theta + 1)$.

Demostración: Inmediata.

Proposición 2.19. : Si $v_2(b) = 1$, $v_2(a) = 0$, $q \equiv 1(4)$ ===> (i) $q \equiv 1(8)$ ==> $2R = PQR$.

(ii) $q \equiv 5(8)$ ==>

$$2R = (2, (\theta^2+\theta_1)/2)(2, ((\theta^2+\theta_1)/2)^2+(\theta^2 + \theta_1)/2+1).$$

Demostración:

(i) Bajo estas hipótesis, Pascual Llorente y Enric Nart [L,N] demuestran que 2 es factor común de índices. Y, según Engstrom [E], 2 descompone completamente.

(ii)Veamos en primer lugar que $s_2 = v_2(4a^3 - 27b^2) \geq 4$. Por ser $q \equiv 5(8)$ s_2 es obviamente par; $v_2(b) = 1$ ===> $s_2 \geq 2$. Ahora bien, $a^3 - 27(b/2)^2 \equiv 0$ (2), ya que $a \equiv 1$ (2) ===> $a^3 \equiv 1(2)$, $b \equiv 2$ (4) ===> $b/2 \equiv 1$ (2) ===> $(b/2)^2 \equiv 1(2)$. Luego $s_2 \geq 3$ y como s_2 es par, se tiene $s_2 \geq 4$. Por tanto, $d \equiv 0$ (4).

Si $d \equiv 0$ (8), necesariamente $a \equiv 3$ (8). En efecto,

$b \equiv 2$ (4) ===> $b/2 \equiv 1$ ó 3 (4) ===> $(b/2)^2 \equiv 1$ (8); pero

$a^3 - 27(b/2)^2 \equiv 0$ (8) ===> $a^3 \equiv 3$ (8) ===> $a \equiv 3$ (8).

Si $d \equiv 4$ (8), necesariamente $a \equiv 7$ (8). En efecto,

$a^3 - 27(b/2)^2 \equiv 4$ (8) ===> $a^3 \equiv 7$ (8) ===> $a \equiv 7$ (8).

Por otro lado, por la proposición 1.20. se tiene que

$(\theta^2+\theta_1)/2 \in R$; $disc((\theta^2+\theta_1)/2) = ((27q - 9a + d)/4)^2(b/2)^2q$. Pero $v_2(27q - 9a + d) = 0$ ya que $27q - 9a + d \equiv 4$ (8) tanto si $d \equiv 0$ (8) como si $d \equiv 4$ (8). Luego $2 \nmid$ índice$((\theta^2+\theta_1)/2)$. $Irr((\theta^2 + \theta_1)/2,Q) = x^3 - ax^2 + (dq - 3aq + a^2)/4\ x + (-b^2 -$ $- dq^2 - adq + 4a^2q)/8 \equiv x^3 + x^2 + x + 1$ ó $x^3 + x^2 + x$ $(Z_2[x])$, ya que $dq - 3aq + a^2 \equiv 4$ (8). Como $v_2(D) = 0$ entonces 2 es no ramificado en K; necesariamente $Irr((\theta^2 + \theta_1)/2,Q) \equiv x^3 + x^2+ + x \equiv x\ (x^2 + x + 1)$ $(Z_2[x])$.

c.q.d.

Proposición 2.20. : Si $v_2(b) = 2$, $v_2(a) = 0$, $a \equiv 1$ (4) ===> (i) $a \equiv 5(8)$ ==> $2R = PQR$.

(ii) $a \equiv 1(8)$ ==>

$$2R = (2,(\theta^2+ \theta)/2)(2,((\theta^2+ \theta)/2)^2-(\theta^2+ \theta)/2 + 1).$$

Demostración:

(i) Bajo estas hipótesis, Pascual Llorente y Enric Nart [L,N] demuestran que 2 es factor común de índices. Y, según Engstrom [E], 2 descompone completamente.

(ii) Por la proposición 1.22. se tiene que $(\theta^2+ \theta)/2 \in R$; $disc\ ((\theta^2+\theta)/2) = (\ (-a + b + 1)\ /\ 4\ )^2(\ d/2\ )^2q$. Y como $-a + b + 1 \equiv 4$ (8) y $v_2(d^2q) = 2$, se tiene $2 \nmid$ índice$((\theta^2 + \theta)/2)$. $Irr\ ((\theta^2 + \theta)/2, Q) = x^3 - a\ x^2 +$ $+ (\ 3b - a + a^2\ )/4\ x + (-b^2 + b - ab)/8 \equiv x^3 + x^2 + x$ $(Z_2[x])$, ya que $3b - a + a^2 \equiv 4$ (8) y $-b^2 + b - ab \equiv -ab + b$ $= b(1 - a) \equiv 0$ (16). Luego $Irr((\theta^2 + \theta)/2,Q) \equiv x\ (x^2 + x + 1)$ $(Z_2[x])$.

c.q.d.

Proposición 2.21. : Si $v_2(b) \geq 3$, $v_2(a) = 0$, $a \equiv 1$ (4) ===> (i) $a \equiv 1(8)$ ==> $2R = PQR$.

(ii) $a \equiv 5(8)$ ==>

$$2R = (2,(\theta^2+\theta)/2)(2,((\theta^2+\theta)/2)^2-(\theta^2+\theta)/2+1).$$

Demostración: En este caso el estudio es totalmente paralelo al caso anterior.

(i) Bajo estas hipótesis, Pascual Llorente y Enric Nart [L,N] demuestran que 2 es factor común de índices. Y, según Engstrom [E], 2 descompone completamente $2R = PQR$.

(ii) Por la proposición 1.25. se tiene que $(\theta^2+\theta)/2 \in R$; $\text{disc}((\theta^2+\theta)/2) = ((-a+b+1)/4)^2(d/2)^2q$. Y como $-a+b+1 \equiv -4$ (8) y $v_2(d^2q) = 2$, se tiene $2 \nmid \text{índice}((\theta^2+\theta)/2)$. $\text{Irr}((\theta^2+\theta)/2, Q) = x^3 - a x^2 + (3b - a + a^2)/4\, x + (-b^2 + b - ab)/8 \equiv x^3 + x^2 + x$ $(Z_2[x])$, ya que $3b - a + a^2 \equiv 4$ (8) y $-b^2 + b - ab \equiv -ab + b = b(1-a) \equiv 0$ (16). Luego $\text{Irr}((\theta^2+\theta)/2, Q) \equiv x(x^2+x+1)$ $(Z_2[x])$.

c.q.d.

DESCOMPOSICION EN R DE UN PRIMO p > 3 DE Z.

De los estudios realizados en el Capítulo I sobre bases minimales en p > 3 primo podemos afirmar que $v_p(D) \in (2,1,0)$. Vamos a estudiar cada uno de esos posibles tres casos por separado. En este apartado p denota a un primo mayor que 3.

Caso a) : $v_p(D) = 2$.

$v_p(D) = 2$ si y sólo si $1 \leq v_p(b) \leq v_p(a)$.

Proposición 2.22. : Si $1 \leq v_p(b) \leq v_p(a)$ ===>

(i) $1 = v_p(b) \leq v_p(a)$ ===> $pR = (p, \theta)^3$.

(ii) $2 = v_p(b) \leq v_p(a)$ ===> $pR = (p, \theta^2/p)^3$.

Demostración:

(i) $1 = v_p(b) \leq v_p(a)$ ===> $s_p = v_p(4a^3 - 27b^2) = 2 = v_p(D)$ ===> $p \nmid$ índice(θ). $Irr(\theta,Q) = x^3 - ax + b \equiv x^3$ ($Z_p[x]$).

(ii) Supongamos ahora $2 = v_p(b) \leq v_p(a)$. Bajo estas hipótesis vimos en la proposición 1.28 que $\theta^2/p \in R$; $disc(\theta^2/p) = (b/p^2)^2((d^2q)/p^4)p^2$. Por ser $v_p(disc(\theta^2/p)) = 2 = v_p(D)$ ==> $p \nmid$ índice(θ^2/p). $Irr(\theta^2/p,Q) = x^3 - (2a/p)x^2 + (a^2/p^2)x - (b^2/p^3) \equiv x^3$ ($Z_p[x]$).

c.q.d.

Caso b) : $v_p(D) = 1$.

$v_p(D) = 1$ si y sólo si ($v_p(b) = 0$, $v_p(q) = 1$) ó ($v_p(b) = 2$,

$v_p(a) = 1$) ó ($v_p(b) \geq 3$, $v_p(a) = 1$). Analizamos, a su vez, cada uno de estos subcasos por separado.

En este caso, $v_p(D) = 1$ ==> p ramificado en K ==> existe P < R ideal primo de R tal que $e(P/p) = e = 2$ ó 3. Pero, por el teorema 10.61 de Harvey - Cohn [HC2], $v_p(D) = 1 = -1 + e +$ + h siendo en este caso $h = 0$ pues $p \nmid e$. Luego $e = 2$ y $pR =$ $= P^2Q$.

Proposición 2.23.: Si $v_p(b) = 0$ y $v_p(q) = 1$ entonces

(i) $v_p(d) \geq 1$ ==>

$$pR = (p, \theta^2 + \theta_1 - (a/3)^*)^2(p, \theta^2 + \theta_1 - (4a/3)^*).$$

(ii) $v_p(d) = 0$ ==>

$$pR = (p, \theta - (3b/2a)^*)^2(p, \theta + (3b/a)^*).$$

($\theta_1 = (4a^2 - 9b\theta - 6a\theta^2)/d$). Con $(m/n)^*$ denotamos a un representante en Z de la clase, en Z_p, de m dividida entre la clase de n. Por ser p un primo Z_p es un cuerpo y dicho cociente existe siempre que la clase de m no sea la clase del cero.

Demostración:

(i) En este caso, $p \nmid$ índice$(\theta^2 + \theta_1)$. En efecto, $disc(\theta^2 + \theta_1) = (27q - 9a + d)^2b^2q$. Pero $v_p(d) \geq 1$, $v_p(q) = 1$ y $v_p(a) = 0$ entonces $v_p(27q - 9a + d) = 0$. Luego $v_p(disc(\theta^2 + \theta_1)) = 1 = v_p(D)$ ==> $p \nmid$ índice$(\theta^2 + \theta_1)$. $Irr(\theta^2 + \theta_1, Q) = x^3 - 2ax^2 + (dq - 3aq + a^2)x + (-b^2 - dq^2 - adq + 4a^2q) = x^3 - 2ax^2 + a^2x - b^2$ $(Z_p[x])$. Como ya hemos razonado al principio de este caso b) $pR = P^2Q$ luego, necesariamente, dicho polinomio tiene en Z_p una raíz doble y una simple. La raíz doble tiene que ser raíz de su polinomio

derivado $3x^2 - 4ax + a^2$, cuyas raíces en Z_p son $a + pZ$ y $(a + pZ)/(3 + pZ)$. Se tiene:

$$((a + pZ)/(3 + pZ))^3$$
$$- 2a((a + pZ)/(3 + pZ))^2$$
$$+ a^2((a + pZ)/(3 + pZ))$$
$$- b^2 \equiv (4a^3 - 27b^2)/27 \equiv 0 \ (pZ).$$

Por tanto, $(a + pZ)/(3 + pZ)$ es raíz doble de $Irr(\theta^2 + \theta_1, Q)$ (en Z_p). Y la descomposición en irreducibles de $Z_p[x]$ de dicho polinomio es $Irr(\theta^2 + \theta_1, Q) =$

$$= (x - ((a + pZ)/(3 + pZ)))^2(x - 4(a + pZ)/(3 + pZ)).$$

(ii) Si $v_p(d) = 0$, como s_p es impar entonces $s_p = 1 = v_p(D)$ luego $p \nmid$ índice(θ). Tenemos que descomponer en irreducibles $x^3 - ax + b \in Z_p\,x$. Como $pR = P^2Q$ necesariamente dicho polinomio tiene una raíz doble y una raíz simple en Z_p. La raíz doble tiene que ser raíz del polinomio derivado. Luego $(a + pZ)/(3 + pZ)$ debe ser un cuadrado en Z_p. En efecto, $4a^3 - 27b^2 \equiv 0\ (p) \Longrightarrow (4 + pZ)((a + pZ)/(3 + pZ))^3 = (b + pZ)^2 \Longrightarrow (a + pZ)/(3 + pZ) = ((3b + pZ)/(2a + pZ))^2$. Luego $\pm (3b + pZ)/(2a + pZ)$ son las posibles raíces dobles en Z_p de $x^3 - ax + b$. Pero,

$$((3b + pZ)/(2a + pZ))^3$$
$$- (a + pZ)((3b + pZ)/(2a + pZ))$$
$$+ (b + pZ) = (-4a^3b + 27b^3)/(8a^3 + pZ) =$$
$$= 0 + pZ,$$

entonces $x^3 - ax + b \equiv (x - (3b/2a)^*)^2(x + (3b/a)^*)$, $(Z_p[x])$.

c.q.d.

Proposición 2.24. : Si $v_p(b) = 2$, $v_p(a) = 1$ ===> ===> $pR = (p, \theta^2/p)(p, \theta^2/p - a/p)^2$.

Demostración:

Bajo estas hipótesis vimos en la proposición 1.32. que $\theta^2/p \in R$; $disc(\theta^2/p) = (b^2/p^3)((d^2q)/p^3)$. Por ser $v_p(disc(\theta^2/p)) = 1 = v_p(D)$ ==> $p \nmid indice(\theta^2/p)$. $Irr(\theta^2/p, Q) = x^3 - (2a/p)x^2 + (a^2/p^2)x - (b^2/p^3) = x^3 - (2a/p)x^2 + (a^2/p^2)x = x(x - a/p)^2$, $(Z_p[x])$.

c.q.d.

Proposición 2.25. : Si $v_p(b) \geq 3$, $v_p(a) = 1$ ===> ==> $pR = (p, \theta^2/p + \theta)(p, \theta^2/p + \theta - a/p)^2$.

Demostración : Bajo estas hipótesis vimos en la proposición 1.34 que $\theta^2/p \in R$;

$disc(\theta^2/p + \theta) = ((-pa + b + p^3)/p^2)^2(d/p)^2q$. Luego, como $v_p(d) = 1$, $p \mid\mid q$, $v_p(a) = 1$ y $-pa + b + p^3 \not\equiv 0 \ (p^3)$, entonces $v_p(disc(\theta^2/p + \theta)) = 1 = v_p(D)$ ===> $p \nmid indice(\theta^2/p + \theta)$.

$Irr(\theta^2/p + \theta, Q) = x^3 - (2a/p)x^2 + ((-p^2a + a^2 + 3pb)/p^2)x + (-b^2 - pab + p^3b)/p^3 = x^3 - (2a/p)x^2 + (a^2/p^2)x = x(x - a/p)^2$ $(Z_p[x])$.

c.q.d.

Caso c) : $v_p(D) = 0$.

$v_p(D) = 0$ si y sólo si ($v_p(b) \geq 1$, $v_p(a) = 0$) ó ($v_p(b) = 0$, s_p par). Analizamos, a su vez, cada uno de estos subcasos por separado.

Proposición 2.26.: Si $v_p(b) \geq 1$, $v_p(a) = 0$ entonces:

(i) $pR = (p,\theta)(p,\theta + ((a + pZ)^{1/2})^*)(p,\theta - ((a + pZ)^{1/2})^*)$ si $a + pZ \in Z_p^{\,2}$, siendo $((a + pZ)^{1/2})^*$ un representante en Z de la clase de $(a + pZ)^{1/2}$.

(ii) $pR = (p,\theta)(p,\theta^2 - a)$ si $a + pZ \notin Z_p^{\,2}$.

Demostración: Inmediata.

Proposición 2.27.: Si $v_p(b) = 0$ y s_p es par entonces:

(i) $v_p(a) \geq 1$ ===>

$pR = (p,\theta^2 - ((b + pZ)^{1/3})^*)\theta + (b + pZ)^{2/3})$
$(p,\theta + ((b + pZ)^{1/3})^*)$ si $b \in Z_p^{\,3}$ y $p \equiv -1$ (3).

$pR = (p,\theta - (((b + pZ)^{1/3} - ((b + pZ)^{1/3}(-3 + pZ)^{1/2})/2)^*)$
$(p,\theta - (((b + pZ)^{1/3} + ((b + pZ)^{1/3}(-3 + pZ)^{1/2})/2)^*)$
$(p,\theta + ((b + pZ)^{1/3})^*)$ si $b \in Z_p^{\,3}$ y $p \equiv 1$ (3).

$pR = (p,\theta^3 + b)$ si $b + pZ \notin Z_p^{\,3}$.

(ii) $v_p(a) = 0$, $s_p \geq 1$ ===>

$pR = (p,\theta_1)(p,\theta_1^{\,2} - 3aq)$ si $q \notin Z_p^{\,2}$.

$pR = (p,\theta_1 - (9b(q + pZ)^{1/2}/(2a + pZ))^*)$
$(p,\theta_1 + (9b(q + pZ)^{1/2}/(2a + pZ))^*)$
(p,θ_1) si $q \in Z_p^{\,2}$.

(iii) $v_p(a) = 0$, $s_p = 0$ ===>

la descomposición en R de pR depende de la descomposición en $Z_p[x]$ de $Irr(\theta,Q)$; (información sobre este tema la tenemos en el artículo de P. Llorente [L2]).

Demostración:

(i) en este caso, $p \nmid$ índice(θ). $Irr(\theta,Q) = x^3 - ax + b \equiv$
$\equiv x^3 + b$ $(Z_p[x])$.

Si $b + pZ \notin Z_p^{\,3}$, dicho polinomio es irreducible en $Z_p[x]$. En

caso contrario, $x^3 + b \equiv (x^2 - (b + pZ)^{1/3}x + (b + pZ)^{2/3})$

$(x + (b + pZ)^{1/3})$ $(Z_p[x])$.

A su vez, el primer factor de dicha descomposición es irreducible en $Z_p[x]$ sii $-3 + pZ \notin Z_p^2$ sii $p \equiv -1$ (3).

(ii) $disc(\theta_1) = 3^6b^2q^3$ y $p \nmid 3bq$ se tiene que $p \nmid$ 'indice(θ_1)

$Irr(\theta_1,Q) = x^3 - 3aqx - dq^2 \equiv x^3 - 3aqx \equiv x(x^2 - 3aq)$

$(Z_p[x])$.

Pero, $4a^3 - 27b^2 \equiv 0$ (p) ===>

$a + pZ = (3 + pZ)((3b + pZ)/(2a + pZ))^2$. Luego $3aq + pZ \in Z_p^2$ si y sólo si $q \in Z_p^2$.

c.q.d.

Cuadro de la descomposición en K del primo 3 de Q.

$a \equiv$	$b \equiv$	Otras condiciones	$3R =$
2(3)	0(3)		$(3,\theta)(3,\theta^2+1)$
2(3)	1(3)		$(3,\theta-1)(3,\theta^2+\theta+2)$
2(3)	2(3)		$(3,\theta-2)(3,\theta^2+2\theta+2)$
1(3)	0(3)		$(3,\theta)(3,\theta-1)(3,\theta-2)$
1(3)	1(3)		$(3,\theta^3-\theta+1)$
1(3)	2(3)		$(3,\theta^3-\theta+2)$
0(27)	0(9)	$b \not\equiv 0(27)$	$(3,\theta^2/3)^3$
0(9)	0(9)	$b \not\equiv 0(27)$ $a \not\equiv 0(27)$	$(3,\theta^2/3)^3$
0(9)	0(3)	$b \not\equiv 0(9)$	$(3,\theta)^3$
0(9)	1(9)	$a+b \not\equiv 1(27)$	$(3,(\theta^2-\theta+1)/3-1)(3,(\theta^2-\theta+1)/3)^2$
0(9)	1(9)	$a+b \equiv 1(27)$	$(3,\theta+(\theta^2-\theta+1)/3)(3,\theta+(\theta^2-\theta+1)/3-2)^2$
0(9)	8(9)	$a-b \not\equiv 1(27)$	$(3,(\theta^2+\theta+1)/3-1)(3,(\theta^2+\theta+1)/3)^2$
0(9)	8(9)	$a-b \equiv 1(27)$	$(3,\theta+(\theta^2+\theta+1)/3+1)(3,\theta+(\theta^2+\theta+1)/3-1)^2$
0(3)	0(9)	$a \not\equiv 0(9)$ y $b \not\equiv 0(27)$	$(3,\theta^2/3)(3,(\theta^2/3)-(a/3))^2$
0(3)	1(3)	$b^2 \not\equiv a+1(9)$ y $a \not\equiv 3(9)$	$(3,\theta-2)^3$
0(3)	2(3)	$b^2 \not\equiv a+1(9)$ y $a \not\equiv 3(9)$	$(3,\theta-1)^3$
3(9)	0(27)		$(3,2\theta+\theta^2/3)(3,2\theta+(\theta^2/3)-1)^2$
3(9)		$b^2 \equiv a+1(27)$, $q \equiv -1(3)$ y $d/27 \equiv 0(3)$	$(3,\theta_1/3)(3,(\theta_1/3)^2+1)$
3(9)		$b^2 \equiv a+1(27)$, $q \equiv -1(3)$ y $d/27 \equiv 1(3)$	$(3,(\theta_1/3)+1)(3,(\theta_1/3)^2-(\theta_1/3)-1)$

a ≡	b ≡	Otras condiciones	3R =
3(9)		$b^2 \equiv a + 1(27)$, $q \equiv -1(3)$ y $d/27 \equiv 2(3)$	$(3,(\theta_1/3) - 1)(3,(\theta_1/3)^2 + (\theta_1/3) - 1)$
3(9)		$b^2 \equiv a + 1(27)$ $q \equiv 1(3)$ y $d/27 \equiv 0(3)$	$(3,\theta_1/3)(3,(\theta_1/3) - 1)(3, (\theta_1/3) + 1)$
3(9)		$b^2 \equiv a + 1(27)$, $q \equiv 1(3)$ y $d/27 \equiv 1(3)$	$(3,(\theta_1/3)^3 - (\theta_1/3) + 2)$
3(9)		$b^2 \equiv a + 1(27)$, $q \equiv 1(3)$ y $d/27 \equiv 2(3)$	$(3,(\theta_1/3)^3 - (\theta_1/3) + 1)$
3(27)		$b^2 \equiv a + 1(27)$, s_3 impar y $s_3 \geq 9$	$(3,(\theta^2-1)/3 +\theta_1/3 -1)(3,(\theta^2-1)/3 +\theta_1/3)^2$
12(27)		$b^2 \equiv a + 1(27)$, s_3 impar y $s_3 \geq 9$	$(3,(\theta^2 - 1)/3 + \theta_1/3 -2)$ $(3,(\theta^2 - 1)/3 + \theta_1/3 - 1)^2$
21(27)		$b^2 \equiv a + 1(27)$, s_3 impar y $s_3 \geq 9$	$(3,(\theta^2-1)/3 +\theta_1/3)(3,(\theta^2-1)/3 +\theta_1/3 -2)^2$
3(27)		$b^2 \equiv a + 1(27)$, $s_3 = 7$	$(3,(\theta^2-1)/3 -1)(3,(\theta^2-1)/3)^2$
12(27)		$b^2 \equiv a + 1(27)$, $s_3 = 7$	$(3,(\theta^2-1)/3 -2)(3,(\theta^2-1)/3 -1)^2$
21(27)		$b^2 \equiv a + 1(27)$, $s_3 = 7$	$(3,(\theta^2-1)/3)(3,(\theta^2-1)/3 -2)^2$
3(9)		$b^2 \equiv 4(9)$ $b^2 \not\equiv a + 1(27)$	$(3,\theta_1/3)^3$
3(9)	1(3)	$b^2 \not\equiv 4(9)$	$(3,\theta - 2)^3$
3(9)	2(3)	$b^2 \not\equiv 4(9)$	$(3,\theta - 1)^3$
6(9)	0(27)		$(3,2\theta + \theta^2/3)(3,2\theta + (\theta^2/3) + 1)^2$
6(9)	4(9)	$a + b \not\equiv 1(27)$	$(3,(\theta^2 -\theta +1)/3 +2)(3,(\theta^2 -\theta +1)/3 -2)^2$
6(9)	4(9)	$a + b \equiv 1(27)$	$(3,\theta +(\theta^2-\theta +1)/3)(3,\theta +(\theta^2-\theta+1)/3 -1)^2$

a ≡	b ≡	Otras condiciones	3R =
6(9)	5(9)	$a - b \not\equiv 1(27)$	$(3,(\theta^2+\theta+1)/3+2)(3,(\theta^2+\theta+1)/3-2)^2$
6(9)	5(9)	$a - b \equiv 1(27)$	$(3,\theta+(\theta^2+\theta+1)/3-2)(3,\theta+(\theta^2-\theta+1)/3)^2$

Cuadro de la descomposición en K del primo 2 de Q.

a ≡	b ≡	Otras condiciones	2R =
0(4)	0(4)	$b \not\equiv 0(8)$	$(2,\theta^2/2)^3$
0(2)	0(2)	$b \not\equiv 0(4)$	$(2,\theta)^3$
0(2)	0(8)	$a \not\equiv 0(4)$	$(2,\theta + \theta^2/2)(2,\theta + \theta^2/2 + 1)^2$
0(2)	0(4)	$a \not\equiv 0(4)$ $b \not\equiv 0(8)$	$(2,\theta^2/2)(2,\theta^2/2 + 1)^2$
0(2)	1(2)		$(2,\theta - 1)(2,\theta^2 + \theta + 1)$
1(8)	0(4)	$b \not\equiv 0(8)$	$(2,(\theta + \theta^2)/2)$ $(2,((\theta + \theta^2)/2)^2 - (\theta + \theta^2)/2) + 1)$
5(8)	0(8)		$(2,(\theta + \theta^2)/2)$ $(2,((\theta + \theta^2)/2)^2 + (\theta + \theta^2)/2) + 1)$
3(4)	0(8)		$(2,\theta)(2,\theta + 1)^2$
3(4)	0(4)	$b \not\equiv 0(8)$	$(2,\theta)(2,\theta + 1)^2$
1(2)	0(2)	$q \equiv 1(2)$ $\Omega_2 \equiv 1(8)$	PQR
1(2)	0(2)	$b \not\equiv 0(4)$ $q \equiv 5(8)$	$(2,(\theta_1 + \theta^2)/2)$ $(2,((\theta_1 + \theta^2)/2)^2 + (\theta_1 + \theta^2)/2) + 1)$
1(2)	0(2)	$b \not\equiv 0(4)$ s_2 impar	$(2,\theta_1 + \theta^2)(2,1 + \theta_1 + \theta^2)^2$
1(2)	0(2)	$b \not\equiv 0(4)$ $q \equiv 3(4)$	$(2,\theta_1)(2,1 + \theta_1)^2$
1(2)	1(2)		$(2,\theta^3 + \theta + 1)$

Cuadro de la descomposición en K de un primo $p > 3$.

$a \equiv$	$b \equiv$	Otras condiciones	$pR =$
$0(p^2)$	$0(p^2)$	$b \not\equiv 0(p^3)$	$(p,\theta^2/p)^3$
$0(p)$	$0(p^3)$	$a \not\equiv 0(p^2)$	$(p, \theta^2/p + \theta)(p, \theta^2/p + \theta - a/p)^2$
$0(p)$	$0(p^2)$	$a \not\equiv 0(p^2)$ $b \not\equiv 0(p^3)$	$(p, \theta^2/p)(p, \theta^2/p - a/p)^2$
$0(p)$	$0(p)$	$b \not\equiv 0(p^2)$	$(p, \theta)^3$
$0(p)$		$b \in Z_p^3$ $b \not\equiv 0(p)$ $p \equiv 1(3)$	$(p,\theta-(((b+pZ)^{1/3}-((b+pZ)^{1/3}(-3+pZ)^{1/2})/2)^*)$ $(p,\theta-(((b+pZ)^{1/3}+((b+pZ)^{1/3}(-3+pZ)^{1/2})/2)^*)$ $(p,\theta + ((b + pZ)^{1/3})^*)$
$0(p)$		$b \in Z_p^3$ $b \not\equiv 0(p)$ $p \equiv 2(3)$	$(p,\theta^2 - ((b + pZ)^{1/3})^*)\theta + (b + pZ)^{2/3})$ $(p,\theta + ((b + pZ)^{1/3})^*)$
$0(p)$		$b \notin Z_p^3$ $b \not\equiv 0(p)$	$(p,\theta^3 + b)$
	$0(p)$	$a \in Z_p^2$ $a \not\equiv 0(p)$	$(p,\theta)(p,\theta + ((a + pZ)^{1/2})^*)$ $(p,\theta - ((a + pZ)^{1/2})^*)$
	$0(p)$	$a \notin Z_p^2$ $a \not\equiv 0(p)$	$(p,\theta)(p,\theta^2 - a)$
		$b \not\equiv 0(p)$ $d \equiv 0(p)$ $q \equiv 0(p)$	$(p,\theta^2 + \theta_1 - (a/3)^*)^2(p,\theta^2 + \theta_1 - (4a/3)^*)$
		$bd \not\equiv 0(p)$ $q \equiv 0(p)$	$(p, \theta - (3b/2a)^*)^2(p, \theta + (3b/a)^*)$
		$q \in Z_p^2$ $d \equiv 0(p)$ $abq \not\equiv 0(p)$	$(p,\theta_1 - (9b(q + pZ)^{1/2}/(2a + pZ))^*)$ $(p,\theta_1 + (9b(q + pZ)^{1/2}/(2a + pZ))^*)$ (p,θ_1)
		$q \notin Z_p^2$ $d \equiv 0(p)$ $abq \not\equiv 0(p)$	$(p,\theta_1)(p,\theta_1^2 - 3aq)$
		$abdq \not\equiv 0(p)$	Depende de la descomposición en $Z_p[x]$ de $Irr(\theta,Q) = x^3 - ax + b$.

CAPITULO III. CUERPOS DE NUMEROS CUBICOS CICLICOS.

3.A. Discriminante de un cuerpo cúbico cíclico. Algoritmo de construcción de todos los cuerpos cúbicos cíclicos de discriminante dado.

3.B. Tabla de unidades fundamentales.

3.C. Análisis de la tabla de unidades fundamentales.

CAPITULO III: CUERPOS DE NUMEROS CUBICOS CICLICOS

Este Capítulo centra su estudio en los cuerpos de números cúbicos cíclicos. En concreto, el estudio que realizamos para K cúbico cíclico viene recogido en los siguientes puntos :

1) Discriminante de K.
2) Algoritmo de construcción de todos los cuerpos cúbicos cíclicos de discriminante dado.
3) Tabla de unidades fundamentales .
4) Análisis de dicha tabla, que nos permite obtener un sistema fundamental de unidades para tres familias infinitas de cuerpos cúbicos cíclicos U, V y W. Dicho sistema de unidades fundamentales es obtenido en términos de los coeficientes de un polinomio definición del cuerpo cúbico cíclico en cuestión.
5) Teorema sobre la paridad del número de clase para los cuerpos cúbicos cíclicos pertenecientes a las familias V y W anteriores.
6) Comportamiento del número de clase cuando el discriminante converge hacia $+\infty$ para cuerpos cúbicos cíclicos de la familia V y para los de la familia W.

En los puntos 1), 2) y 3) utilizaremos nuestros resultados del Capítulo I y en el punto 5) los del Capítulo II.

3.A. DISCRIMINANTE DE UN CUERPO DE NUMEROS CUBICO CICLICO. ALGORITMO DE CONSTRUCCION DE TODOS LOS CUERPOS CUBICOS CICLICOS DE DISCRMINANTE DADO.

El discriminante de un cuerpo de números dado es un invariante de gran importancia. Contiene entre sus factores primos a todos los que son ramificados. También nos permite conocer el índice de un elemento dado y ya hemos visto la importancia que ello tiene al estudiar la descomposición en R de un primo de Z. Otra aplicación del discriminante es la identificación de bases enteras.

En el Capítulo I hemos obtenido el discriminante de un cuerpo de números cúbico en términos exclusivamente de los coeficientes de un polinomio definición del mismo.

En este apartado A de este tercer Capítulo vamos a estudiar, en primer lugar, cómo tiene que ser el discriminante de un cuerpo de números cúbico cíclico. Y, en segundo lugar, vamos a encontrar todos los cuerpos cúbicos cíclicos de discriminante dado, obteniendo para cada uno de ellos un polinomio definición.

El conocer a priori el discriminante lo vamos a utilizar, en el apartado B, como criterio de identificación de bases enteras.

Suponemos conocido que si K es un cuerpo de números cúbico cíclico entonces su discriminante es un cuadrado $D = p^2$ (véase [L], páginas 237-238). Nuestro propósito es demostrar que p es, necesariamente, de la forma $p = 3^{\delta} p_1 \dots p_r$, $\delta \in \{ 0, 2 \}$, $p_i \equiv 1 \ (3)$ primo para $1 \leq i \leq r$ y distintos dos a dos.

En el Capítulo I hemos dado $v_q(D)$ (máxima potencia de q que divide a D), para cada q primo, en términos exclusivamente de los coeficientes de un polinomio definición de K. En virtud de dichos resultados, en el caso K cuerpo de números cúbico cíclico de discriminante $D = p^2$ podemos afirmar que $v_3(D) \in \{0,4\}$ y $v_t(D) \in \{0,2\}$ para $t \neq 3$ primo. Demostraremos, por reducción al absurdo, que para t primo, $t \equiv 2(3)$ entonces $v_t(D) \neq 2$. De donde p es, necesariamente, de la forma $p = 3^{\delta} p_1 \dots p_r$, $\delta \in \{ 0, 2 \}$, $p_i \equiv 1 \ (3)$ primo para $1 \leq i \leq r$ y distintos dos a dos.

Enunciamos este resultado y detallamos su demostración en la siguiente proposición 3.1.

Proposición 3.1. : Sea K cúbico cíclico. El discriminante de K es, necesariamente, de la forma p^2 siendo $p = 3^{\delta} p_1 \dots p_r$ $\delta \in \{ 0, 2 \}$, $p_i \equiv 1 \ (3)$ primo para $1 \leq i \leq r$ y distintos

dos a dos.

Demostración: De los resultados obtenidos en el Capítulo I sobre bases minimales y discriminante para un cuerpo cúbico se deduce que :

v_2 (D) $\in$ { 0,2,3 },

v_3 (D) $\in$ { 0,1,3,4,5 },

v_t (D) $\in$ { 0,1,2 } para t > 3 primo.

Por ser K cúbico cíclico su discriminante es un cuadrado. Por consiguiente :

v_2 (D) $\in$ { 0,2 },

v_3 (D) $\in$ { 0,4 },

v_t (D) $\in$ { 0,2 } para t > 3 primo.

Además, v_2 (D) = 2 sii $1 \leq v_2$ (b) $\leq v_2$ (a) y para t > 3 primo, v_t (D) = 2 sii $1 \leq v_t$ (b) $\leq v_t$ (a).

Veamos, en primer lugar, que v_2 (D) = 2 no puede darse. En efecto, supongamos v_2 (D) = 2. Entonces, $1 \leq v_2$ (b) $\leq v_2$(a). Ahora bien, $4a^3 - 27b^2 = d^2$ y $v_2(b) = v_2(d)$. Dividimos ambos miembros de dicha igualdad entre: $2^{2v_2(b)}$ resultando

$$(4a^3)/2^{2v_2(b)} - 27(b/2^{v_2(b)})^2 = (d/2^{v_2(b)})^2$$

Pero, $2 + 3v_2(a) \geq 2 + 3v_2(b) = (2 + v_2(b)) + 2v_2(b)$ y como $2 + v_2(b) \geq 3$ entonces

$$(4a^3)/2^{2v_2(b)} \equiv 0 \ (8).$$

Por otro lado:

$$b/2^{v_2(b)} \quad \text{y} \quad d/2^{v_2(b)}$$

son congruentes con 1, 3, 5 ó 7 módulo 8; luego su cuadrado

es congruente con 1 módulo 8. Y se tendría $-27 \equiv 1\ (8)$, absurdo. Por consiguiente, $v_2(D) = 0$.

Tendremos demostrada la proposición si vemos que, para $t > 3$ primo verificando $v_t(D) = 2$, entonces $t \equiv 1\ (3)$. Supongamos $t \equiv 2\ (3)$. Necesariamente, $1 \leq v_t(b) \leq v_t(a)$. Y como $4a^3 - 27b^2 = d^2$ entonces $v_t(b) = v_t(d)$. Dividimos ambos miembros de dicha igualdad entre

$t^{2v_t(b)}$ resultando

$$(4a^3)/t^{2v_t(b)} - 27(b/t^{v_t(b)})^2 = (d/t^{v_t(b)})^2$$

Ahora bien, $3v_t(a) \geq 3v_t(b) = 2v_t(b) + v_t(b)$ siendo $v_t(b) > 0$. Luego

$(4a^3)/t^{2v_t(b)} \equiv 0\ (t)$ y -27 es un cuadrado en Z_t. Ahora bien,

$-27 \in Z_t^2 \iff -3 \in Z_t^2$;

$t > 3$ primo, $t \equiv 2(3) \Rightarrow t \equiv 1(4) \Rightarrow -1 \in Z_t^2,\ 3 \notin Z_t^2 \Rightarrow$

$\Rightarrow -27 \notin Z_t^2$. Absurdo.

ó $t \equiv 3(4) \Rightarrow -1 \notin Z_t^2,\ 3 \in Z_t^2 \Rightarrow$

$\Rightarrow -27 \notin Z_t^2$. Absurdo.

c.q.d.

Nuestro propósito ahora es dar un algoritmo de construcción de todos los cuerpos cúbicos cíclicos de discriminante dado. Vamos a obtener un sencillo polinomio definición de K cuerpo de números cúbico cíclico; con este polinomio trabajaremos en los próximos apartados 3.B. y 3.C.

En el capítulo I hemos estudiado el discriminante D de K

cuerpo de números cúbico en términos de los coeficientes a y b de un polinomio $x^3 - ax + b$ definición de K. El camino que vamos a recorrer ahora es el inverso. Dado K cuerpo de números cúbico cíclico de discriminante $D = p^2$, ($p = 3^{\delta}p_1 \dots p_r$, $\delta \in \{ 0, 2 \}$, $p_i \equiv 1$ (3) primo para $1 \leq i \leq r$ y distintos dos a dos), ¿ cómo podemos tomar a y b para que $x^3 - ax + b$ defina a K ?.

En principio, podemos tomar $a \leq 3p$, $b \geq 0$ y suponer que no existe ningún primo t tal que $t^3 \mid b$ y $t^2 \mid a$; esto lo justificaremos con el lema 3.2.

Supongamos, por ejemplo, $\delta = 0$ (el caso $\delta = 2$ se razona de forma análoga). Para $1 \leq i \leq r$, $v_{p_i}(D) = 2$, siendo $p_i > 3$ primo, y ello equivale a $1 \leq v_{p_i}(b) \leq v_{p_i}(a)$ (véase proposiciones 1.28. a 1.34.). Luego $p \mid a$ y como $a \leq 3p$ entonces $a = p$, $a = 2p$ ó $a = 3p$. Necesariamente, $p \,||\, b$ (p divide a b y p^2 no divide a b). Lo que vamos a demostrar, en la proposición 3.3., es que tomando $a = p$, $b = pq$ siendo $4p - 27q^2 \in Z^2$, $(p,q) = 1$, $q \in Z^+$ obtenemos todos los cuerpo de números cúbicos cíclicos de discriminante p^2. Además, si tomamos $q' \neq q$ en las hipótesis anteriores, $x^3 - px + pq$ y $x^3 - px + pq'$ definen cuerpos cúbicos cíclicos distintos. La demostración de nuestra proposición 3.3. descansa en el conocimiento del entero θ_1 obtenido en nuestro Capítulo I.

Vamos a suponer conocida la correspondencia biyectiva que a cada cuerpo de números cúbico cíclico de discriminante

p^2 le hace corresponder un único par $(r,q) \in Z^2$ verificando $p = (r^2 + 27q^2)/4$ siendo $q > 0$ y $r \equiv 1(3)$ si $p \equiv 1(3)$ y $r = 3r'$ con $r' \equiv 1(3)$, $q \not\equiv 0(3)$ si $p \equiv 0(3)$ (véase [G1]). Además, el cuerpo de números K cúbico cíclico que se le asocia al par (r,q) es $K = Q(\alpha)$ con:

$Irr(\alpha,Q) = x^3 + x^2 + ((1 - p) / 3)x - (p(3 + r) -1)/ 27$ si 3 es no ramificado en K, e

$Irr(\alpha,Q) = x^3 - (p / 3)x - (rp) / 27$ si 3 es ramificado en K.

Lema 3.2.: Un cuerpo de números cúbico real de discriminante D y sus conjugados son generados por los ceros de un polinomio $f(x) = x^3 - ax + b$ donde $a \leq 3\ D^{1/2}$, $b \geq 0$; se puede, además suponer que no existe un primo t tal que $t^3 \mid b$ y $t^2 \mid a$.

Demostración: H.J. Godwin [Go] demuestra que un cuerpo de números K cúbico real de discriminante D y sus conjugados son generados por los ceros de un polinomio $f(x) = x^3 - dx^2 + ex - f$ donde

$$d^2 - 3e \leq D^{1/2},$$
$$d < 3 + 2D^{1/2},$$
$$f \leq (9ed - 2d^3)/27.$$

Si efectuamos el cambio $x \dashrightarrow x + d/3$ tendremos $x^3 - (d^2 - 3e)/3\ x + (9ed - 2d^3 - 27f)/27$. Las raíces de este polinomio son elementos primitivos de K y sus conjugados. Multiplicando por 27 con el fin de que los coeficiente estén en Z y haciendo el cambio $y = 3x$, nos queda :

$y^3 - (d^2 - 3e)3\ y + (9ed - 2d^3 - 27f)$. También las raíces de este polinomio son elementos primitivos de K y sus

conjugados. Además: $a = (d^2 - 3e)3 \leq 3D^{1/2}$,

$$b = 9ed - 2d^3 - 27f \geq 0.$$

Podemos también suponer que suponer que no existe un primo t tal que $t^3 \mid b$ y $t^2 \mid a$. De lo contrario, el polinomio $x^3 - ax + b$ se sustituye por $x^3 - a / p^2 \; x + b/p^3$.

c.q.d.

Proposición 3.3.: Sea K cuerpo de números cúbico cíclico de discriminante p^2 entonces existe un único $q \in Z^+ - (0)$, $(p,q) = 1$ tal que $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$.

Demostración: Al cuerpo de números K cúbico cíclico de discriminante p^2 le hacemos corresponder, de forma única, el par (r,q) verificando $p = (r^2 + 27q^2)/4$ siendo $q > 0$ y $r \equiv 1(3)$ si $p \equiv 1(3)$ y $r = 3r'$ con $r' \equiv 1(3)$, $q \not\equiv 0(3)$ si $p \equiv 0(3)$ (véase [G1]).

A partir del par (p,q) vamos a definir un cuerpo de números cúbico cíclico L de discriminante p^2 que veremos que coincide con K.

Sea $f(x) = x^3 - px + pq$; f es irreducible sobre Q. En efecto, de la condición $4p - 27q^2 = r^2$, y teniendo en cuenta que $p = 3^{\delta}p_1 \ldots p_r$, $\delta \in \{ 0, 2 \}$, $p_i \equiv 1 \; (3)$ primo para $1 \leq i \leq r$ y distintos dos a dos se deduce que $(p,q) = 1$. En efecto, si $\delta = 0$ entonces $(p,q) = 1$, pues de lo contrario p no sería libre de cuadrados; y si $\delta = 2$ entonces 9 es el único posible factor común de p y q, pero en este caso $r = 3r'$ con $r' \equiv 1(3)$, $q \not\equiv 0(3)$. Luego, en cualquier caso,

$(p,q) = 1$. Por tanto, cualquier p_i divisor primo de p verifica que divide a todos los coeficientes de f(x) salvo al coeficiente principal y su cuadrado no divide al término independiente. Por el criterio de Eisenstein, f(x) es irreducible sobre Q. Si θ es una raiz de f(x) entonces $L = Q(\theta)$ es un cuerpo de números cúbico.

Sea D' el discriminante de L. Para $1 \leq i \leq r$, $v_{pi}(D') = 2$ (proposición 1.28.). Si $3 \nmid p$ entonces $v_3(D') = 0$ (proposición 1.12.) y si $3 \mid p$ entonces $v_3(D') = 4$ (proposición 1.7.). Se tiene que $v_2(D') = 0$ (proposiciones 1.18., 1.20., 1.22. y 1.25.). Y, por último, para $t > 3$ primo, $t \neq p_i$, $1 \leq i \leq r$, se tiene $v_t(D') = 0$ (proposiciones 1.29., 1.30., 1.31. y 1.33.). Por tanto, el discriminante de L es $D' = p^2$.

Por otro lado, $\theta 1 = (4p - 9q\theta - 6\theta^2)/(4p - 27q^2)^{1/2}$ es un entero algebraico de L (véase el lema 1.2.). Luego $L = Q(\theta 1)$. Además, $Irr(\theta 1,Q) = x^3 - 3px - p(4p - 27q^2)^{1/2}$.

Vamos a demostrar que $K = Q(\theta 1)$, con lo que tendremos demostrado que $K = Q(\theta)$ con $Irr(\theta,Q) = x^3 - px + pq$.

Sabemos que, por ser K el cuerpo cúbico cíclico asociado al par (r,q) entonces $K = Q(\alpha)$ con:

$Irr(\alpha,Q) = x^3 + x^2 + ((1 - p) / 3)x - (p(3 + r) -1)/ 27$ si 3 es no ramificado en K, e

$Irr(\alpha,Q) = x^3 - (p / 3)x - (rp) / 27$ si 3 es ramificado en K.

En la demostración del lema 3.2. vemos que si $x^3 - dx^2 + ex - f$ es un polinomio definición de un cuerpo cúbico entonces $x^3 - 3(d^2 - 3e)x + (9ed - 2d^3 - 27f)$ es un polinomio definición del mismo cuerpo cúbico. En nuestro caso:

si 3 es no ramificado en K, tenemos $d = -1$, $e = (1 - p) / 3$, $f = (p(3 + r) - 1)/ 27$ y entonces $3(d^2 - 3e) = 3p$; $(9ed - 2d^3 - 27f) = -pr = -p(4p - 27q^2)^{1/2}$. Luego $x^3 - 3px - p(4p - 27q^2)^{1/2}$ es un polinomio definición de K y $K = Q(\theta 1)$.

si 3 es ramificado en K, tenemos $d = 0$, $e = - p / 3$, $f = rp / 27$ y entonces $3(d^2 - 3e) = 3p$; $(9ed - 2d^3 - 27f) = -pr = -p(4p - 27q^2)^{1/2}$. Luego también en este caso $x^3 - 3px - p(4p - 27q^2)^{1/2}$ es un polinomio definición de K y $K = Q(\theta 1)$.

c.q.d.

Por tanto, en virtud de la proposición 3.3, para obtener todos los cuerpos cúbicos cíclicos de discriminante p^2, evitando repeticiones, tenemos que encontrar todos los $q \in Z^+$ tales que $(p,q) = 1$ y $4p - 27q^2 \in Z^2$. En cada caso, $K = Q(\theta)$ con $\theta^3 - p\theta + pq = 0$ es cíclico de discriminante p^2, y todos son obtenidos así.

3.B. TABLA DE UNIDADES FUNDAMENTALES.

Nuestro objetivo en este segundo apartado de este tercer Capitulo es deducir del teorema de Godwin [Go1] un método de obtención de sistemas de unidades fundamentales en cuerpos de números cúbicos cíclicos. Como un cuerpo de números K cúbico cíclico está contenido en el cuerpo de los números reales, las raíces de la unidad en K son ±1. Luego, por el teorema de las unidades de Dirichlet, tendremos perfectamente determinado el grupo de unidades de R anillo de enteros de K si damos un sistema fundamental de unidades de K que, en este caso, tiene rango r + s - 1 = 2. Si (μ_1,μ_2) es un sistema fundamental de unidades de K toda unidad u de R es de la forma $u = \pm\mu_1^{v}\mu_2^{w}$ con $v,w \in \mathbb{Z}$.

El método de obtención de sistemas fundamentales que deducimos lo aplicaremos a la construcción de una tabla de unidades fundamentales para los cuerpos cúbicos cíclicos de discriminante p^2 menor que $16\cdot10^6$.

En 1960, H.J. Godwin [Go1] da una conjetura sobre las unidades de cuerpos cúbicos totalmente reales. Para K cuerpo cúbico totalmente real define $S(\alpha) = (1/2)[(\alpha - \alpha')^2 + (\alpha - \alpha'')^2 + (\alpha' - \alpha'')^2]$ para $\alpha \in R - \{ 0 \}$. E denota al grupo de las unidades de norma uno de K. H.J. Godwin anuncia la siguiente conjetura : sea $\mu \in E - \{ 1 \}$ tal que $S(\mu)$ sea

mínimo, y sea $\tau \in E - \{ \mu^n : n \in Z \}$ tal que $S(\tau)$ sea mínima; entonces, si $S(\mu) > 9$, (μ,τ) forma un sistema fundamental de unidades de K. En 1980, M.N. Gras [G3] demuestra dicha conjetura en el caso particular de K cúbico cíclico. Ennola Veikko [Ve] prueba recientemente la conjetura de Godwin salvo, a lo sumo, un número finito de casos que pueden ser listados explícitamente de la demostración.

Vamos a realizar dos observaciones de gran interés:

1) Es la primera vez que el teorema de Godwin es estudiado hasta conseguir deducir un algoritmo de cálculo de unidades fundamentales.

2) Ninguna de las tablas conocidas hasta el momento ha permitido sacar consecuencias. No ocurre esto con la nuestra, como veremos en el apartado 3C.

Con el fin de hacer computable el teorema de Godwin, efectuamos a continuación un estudio detallado de la ya definida función S. En lo sucesivo, K va a denotar a un cuerpo cúbico cíclico de discriminante p^2. Por tanto, por el estudio realizado en el apartado 3.A., $p = 3^{\delta}p_1 \ldots p_r$ siendo $\delta \in (0,2)$, $p_i \equiv 1 \ (3)$ primo, $1 \leq i \leq r$, y distintos dos a dos. Además, $K = Q(\theta)$ con $Irr(\theta,Q) = x^3 - px + pq$, $q \in Z^+ - \{ 0 \}$, $(p,q) = 1$. Conocemos, pues, un polinomio definición de K y su discriminante. El conocimiento del discriminante de K lo vamos a utilizar a continuación como criterio de identificación de bases enteras.

Obviamente, $4p - 27q^2 \in Z^2$. Supongamos q impar. Entonces, $m = [(4p - 27q^2)^{1/2} - 3\ ]/2 \in Z$. En el caso q par, $m \notin Z$. Veremos al final de este apartado cómo tenemos que modificar la definición de m en el caso q par para conseguir un estudio paralelo al que vamos a efectuar en el caso q impar.

Por el lema 1.2., y siguiendo la notación prefijada en el Capitulo I, se tiene que $\theta_1 = (4p - 9q\theta - 6\theta^2)/(4p - 27q^2)^{1/2} \in R$. Veamos ahora que $\sigma = (m + \theta_1) / 3 \in R$.

Lema 3.4.: En las condiciones anteriores:

(i) $\sigma = (m + \theta_1) / 3 \in R$.

(ii) $disc(\sigma) = p^2q^2$.

Demostración : Por el lema 1.3., $\sigma \in R$ sii se satisface el siguiente sistema de congruencias :

$$-3m \equiv 0 \ (3).$$

$$-3p + 3m^2 \equiv 0 \ (9).$$

$$-m^3 - p(4p - 27q^2)^{1/2} + 3pm \equiv 0 \ (27).$$

Ahora bien, teniendo en cuenta la definición de m, se tiene :

$m^2 = [\ 4p - 27q^2 + 9 - 6\ (4p - 27q^2)^{1/2}]/4.$

$m^3 = [\ (4p - 27q^2 + 27)\ (4p - 27q^2)^{1/2} - 9(4p - 27q^2) - 27]/8$

Razonamos ya sobre el sistema de congruencias. La primera congruencia se verifica trivialmente. La segunda congruencia equivale a $m^2 - p \equiv 0 \ (3)$. Pero,

$$m^2 - p = [-27q^2 + 9 - 6(4p - 27q^2)^{1/2}] / 4 \equiv 0 \ (3) \ .$$

En cuanto a la tercera congruencia,

$$-m^3 - p(4p - 27q^2)^{1/2} + 3pm = [(27q^2 - 27)(4p - 27q^2)^{1/2} -$$

$$-q^2(5^5 + 27\ )/8 \equiv 0 \ (27);$$

luego también se verifica. Queda, pues demostrado el apartado (i). Por otro lado, $disc(\theta_1) = 3^6p^2q^2$, luego $disc(\sigma) = p^2q^2$.

c.q.d.

Con el fin de obtener una base entera de K, aplicaremos el teorema de Harvey - Cohn [HC2,th.9.28] a la Q-base de enteros $\{ 1,\sigma,\sigma^2 \}$. Tenemos que minimizar dicha base en los primos divisores de q.

Lema 3.5. : $(s_0 + \sigma)/q \notin R$ para $s_0 \in \{ 0,1,\ldots,q-1 \}$.

Demostración : Si fuera $(s_0 + \sigma) / q \in R$ con $s_0 \in \{0,1,\ldots,q-1\}$ por el lema 1.3., tomando $A = 3s_0 + m$, $B = 0$, $r = 3q$, se verificaría $(3s_0 + m) \equiv 0 \ (q)$ y $-p + (3s_0 + m)^2 \equiv 0 \ (q^2)$. Luego, $p \equiv 0 \ (q^2)$, absurdo pues $(p,q) = 1$.

c.q.d.

Podemos, pues, concluir que existen s_0, $s_1 \in \{0,\ldots,q-1\}$ tales que $(1,\sigma,(s_0 + s_1\sigma + \sigma^2)/q)$ es una base entera de R anillo de enteros de K. De momento, no nos preocupamos de obtener s_0, s_1. Tras el estudio de la función S de Godwin, obtendremos información sobre ellos.

Antes de dar el teorema principal de este apartado, vamos a dar un lema, el lema 3.6., con el que se demuestran ciertas congruencias que serán de gran utilidad al calcular la norma de un elemento de K. El lema 3.7. es un lema técnico de gran interés tanto a la hora de determinar si un elemento es o no

de R, como a la hora de calcular para un elemento de R su norma, su traza o la suma del producto de cada dos de sus conjugados.

Lema 3.6. : Sea K cúbico cíclico de discriminante p^2; K=Q(θ) con Irr(θ,Q) = $x^3 - px + pq$ y suponemos q impar. Se verifican las siguientes congruencias :

(a) $(d + m^3)/3 - pm \equiv 0$ (9).

(b) $(2dm - m^4)/3 - p^2 \equiv 0$ (9).

siendo $m = [(4p - 27q^2)^{1/2} - 3] / 2$, $d = p(4p - 27q^2)^{1/2}$.

Demostración : Veamos, en primer lugar, que los primeros miembros de ambas congruencias son de Z. En efecto, $d = p(4p - 27q^2)^{1/2}$.

$m \equiv 0(3) \Rightarrow (4p - 27q^2)^{1/2} = 2m + 3 \equiv 0(3) \Rightarrow d + m^3 \equiv 0(3)$

$m \equiv 1(3) \Rightarrow (4p - 27q^2)^{1/2} = 2m + 3 \equiv 2(3) \Rightarrow d + m^3 \equiv 0(3)$

$m \equiv 2(3) \Rightarrow (4p - 27q^2)^{1/2} = 2m + 3 \equiv 1(3) \Rightarrow d + m^3 \equiv 0(3)$

Luego $(d + m^3)/3 - pm \in Z$. Y como $2d - m^3 \equiv -d - m^3$ (3) $\equiv$ $\equiv 0(3)$, también $(2dm - m^4)/3 - p^2 \in Z$.

Teniendo en cuenta la definición de m, se tiene :

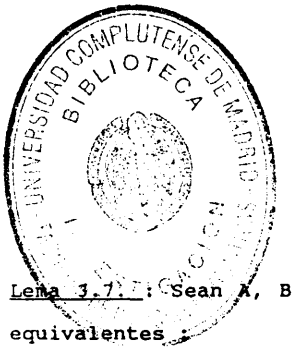
$$m^2 = [(4p - 27q^2 + 9) - 6 (4p - 27q^2)^{1/2}]/4.$$

$$m^3 = [(4p - 27q^2 + 27) (4p - 27q^2)^{1/2} - 9(4p - 27q^2) - 27] / 8.$$

$$m^4 = [(16p^2 - 2^3 3^3pq^2 + 2^3 3^3p - 2\cdot3^6q^2 + 3^6q^4 + 3^4) + (-48p + 4\cdot3^4 q^2 - 4\cdot3^3) (4p - 27 q^2)^{1/2}]/16$$. Sustituyendo y haciendo operaciones :

$$(d + m^3)/3 - pm = [9(1 - q^2)(4p - 27q^2)^{1/2} + 9(9q^2 - 1)]/8 \equiv 0 (9).$$

$$(2dm - m^4)/3 - p^2 = [-72pq^2 - 72 p + 2\cdot3^5q^2 - 3^5q^4 - 3^3$$



$- 4\cdot 3^3q^2(4p - 27q^2)^{1/2} + 4\cdot 3^2(4p - 27q^2)^{1/2}] / 2^4 \equiv 0$ (9).

c.q.d.

Lema 3.7. : Sean A, B, C, r elementos arbitrarios de Z. Son equivalentes :

(i) $(A + B\,\theta_1 + C\,\theta_1^2)/r \in R$.

(ii) $-3A - 6pC \equiv 0$ (r).

$9p^2C^2 - 3pB^2 + 3A^2 + 12pAC - 3dBC \equiv 0(r^2)$.

$3pdBC^2 - 6pA^2C - dB^3 - A^3 + 3dABC - d^2C^3 + 3pAB^2 - 9p^2AC^2 \equiv 0\ (r^3)$

(siguiendo la notación prefijada,

$$\theta_1 = (4p - 9q\theta - 6\theta^2)/(4p - 27q^2)^{1/2}).$$

Demostración : Es una aplicación inmediata del lema 1.1.

Enunciamos y demostramos a continuación el teorema principal de este apartado. Este teorema es un minucioso estudio de la función S de Godwin que permite, además, calcular una base entera de R en términos de p y de q. Este teorema estudia el caso q impar. El teorema 3.13 es un teorema análogo para el caso q par.

Teorema 3.8. : Sea K cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos q impar. Sea $S(\alpha) = (1/2)\,[(\alpha - \alpha')^2 + (\alpha - \alpha'')^2 + (\alpha'' - \alpha')^2]$ definida para $\alpha \in K$. Entonces :

(i) $S(\alpha) \in p\,Z^+$, para todo $\alpha \in R$.

(ii) $4(S(\alpha)/p) = [\,2u + ((2m + 1 + 2s_1)/q)\,v]^2 + 3v^2$

siendo $\alpha = t + u\,\sigma + v\,((s_0 + s_1\,\sigma + \sigma^2)/q)$ con $t, u, v \in Z$.

(iii) $(2m + 1 + 2s_1) / q \in Z$.

(iv) $\{1, \sigma, (s_0 + s_1\,\sigma + \sigma^2) / q\}$ es base entera de K, siendo s_1 el único elemento de $\{0, 1, \ldots, q-1\}$ tal que $2m + 1 + 2s_1 \equiv 0\ (q)$.

Si $3 \nmid q$, s_0 es el único elemento de $(0, 1, \ldots, q-1)$ tal que $9\,s_0 + 3\,s_1\,m + m^2 + 2p \equiv 0\ (q)$.

Si $3 \mid q$ pero $9 \nmid q$ (o sea, $v_3(q) = 1$), entonces para $m \equiv 1(3)$ es $s_0 = -1 + 3t_0$ siendo t_0 único tal que $3\,t_0 + t_1\,m + ((m^2 + 2p) / 3 - 3) / 3 \equiv 0\ (q/3)$; para $m \equiv 2(3)$ es $s_0 = 3t_0$ siendo t_0 único tal que $3\,t_0 + t_1\,m + ((m^2 + 2p) / 3 - m) / 3 \equiv 0\ (q/3)$.

Y, en general, si $r = v_3(q) \geq 1$ entonces en primer lugar minimizamos en 3 la base $(1, \sigma, \sigma^2)$ para de este modo obtener s_0 a partir de t_0 solución única de una congruencia módulo $q / 3^r$.

$(\sigma = (m + \theta_1) / 3\ ,\ m = [\,(4p - 27q^2)^{1/2} - 3\,] / 2)$.

<u>Demostración</u> : (i) Obviamente, $S(\sigma) \in Z$ ya que $S(\alpha) = Tr^K_Q(\alpha^2) - (\alpha\,\alpha' + \alpha'\,\alpha'' + \alpha\,\alpha'') \in Z$.

$\alpha \in R \Longrightarrow \alpha = t + u\,\sigma + v\,((s_0 + s_1\,\sigma + \sigma^2)/q)$;

$t, u, v \in Z$; $s_0, s_1 \in \{0, 1, \ldots, q-1\}$.

Así, $S(\alpha) = S(((q\,u + s_1\,v)\,\sigma + v\,\sigma^2) / q)$. Por notación, sea $\beta = ((qu + s_1\,v)\,\sigma + v\,\sigma^2) / q$. Por ser $\sigma = (m + \theta_1)/3$ y $\theta_1^3 = 3p\theta_1 + p\,(4p - 27q^2)^{1/2}$, se tiene que $\beta^2 = (A + B\,\theta_1 + C\,\theta_1^2) / (3^4\,q^2)$ siendo

$A = (3(qu + s_1v)m + vm^2)^2 + 2\,(3(qu + s_1v) + 2mv)vd$.

$C = (3(qu + s_1v) + 2mv)^2 + 3pv^2 + 2v(3(qu + s_1v)m + m^2v)$.

Como la traza de θ_1 es cero y la de θ_1^2 es 6p entonces $Tr^K_Q(\beta^2) = (A + 2pC)/(3^3 q^2)$.

Por otro lado, aplicando el lema 3.7. ,

$\beta\beta' + \beta\beta'' + \beta'\beta'' = (3p^2v^2 - (3(qu + s_1v) + 2mv)^2p + (3(qu +$
$+ s_1v)\, m + vm^2)^2 + 4p\,(\,3m\,(qu + s_1v) +$
$+ vm^2)v - dv(3(qu + s_1v) + 2mv))/(27q^2)$.

Por tanto, $S(\alpha) = S(\beta) = Tr^K_Q(\beta^2) - (\beta\beta' + \beta\beta'' + \beta'\beta'') =$

$= (p(4p - 27q^2)^{1/2}v(3(qu + s_1v) + 2mv) + p(3(qu + s_1v) +$
$+ 2mv)^2 + p^2v^2)\ /\ (9q^2)$.

Si $(p,3) = 1$ como también $(p,q) = 1$ y $S(\alpha) \in Z^+$ entonces $S(\alpha)$ pertenece a pZ^+.

Si $(p,3) = 3$ entonces $m = ((4p - 27q^2)^{1/2} - 3)/2 \equiv 0\ (3)$, y el numerador de $S(\alpha)$ es un múltiplo de 9p. Por ser $S(\alpha) \in Z^+$ y $(p,q) = 1$, se tiene que $S(\alpha)$ pertenece a pZ^+.

(ii) Dividiendo entre p la expresión de $S(\alpha)$ obtenida en el apartado anterior y efectuando las simplificaciones adecuadas

$S(\alpha)/p = u^2 + ((8m^2 + (6 + 18s_1)m + 9s_1 + p +$
$+ 9s_1^2)/(9q^2))v^2 + ((2m + 1 + 2s_1)/q)uv = u^2 +$
$+ ev^2 + fuv$ (por notación);

forma cuadrática en u y en v pertenecientes a Z con coeficientes también en Z. Su discriminante es -3. En efecto,

$f^2 - 4e = ((2m + 3)^2 - 4p)/(9q^2) = (-27q^2)/(9q^2) = -3$.

Luego $4(S(\alpha)/p) = (2u + ((2m + 1 + 2s_1)/q)v)^2 + 3v^2$.

(iii) y (iv) Como $4(S(\alpha)/p) \in Z$, para todo $u,v \in Z$, en particular, tomando $u = 0, v = 1$ se tiene que $(2m + 1 + 2s_1)/q$

pertenece a Z. Por tanto, s_1 es el único elemento perteneciente a $\{ 0,1,\ldots,q-1 \}$ tal que $2m + 1 + 2s_1 \equiv 0\ (q)$; por ser q impar s_1 existe y es único.

Si $3 \nmid q$, imponiendo la condición $Tr^K_Q((s_0 + s_1\,\sigma + \sigma^2)/q) \in Z$ y teniendo en cuenta que la traza de σ es m y la de σ^2 es $(m^2 + 2p)/3$, se tiene que s_0 es el único elemento de $\{ 0, 1,\ldots,q-1 \}$ tal que $9s_0 + 3s_1m + m^2 + 2p \equiv 0\ (q)$. El caso $3 \mid q$ debe ser considerado aparte, ya que en este caso la última congruencia no tiene solución única.

Si $3 \mid q$ entonces $v_3(p) = 0$, luego $v_3(m) = 0$.

Si $m \equiv 1(3)$

entonces, por el lema 3.7. y teniendo en cuenta la definición de m, $(\sigma^2 - 1) / 3 \in R$. Luego existen t_0, $t_1 \in \{0,1,\ldots,q/3 - 1\}$ tales que $(t_0 + t_1\sigma + (\sigma^2 - 1)/3)/(q/3) \in R$. Imponiendo que la traza de dicho elemento esté en Z, nos queda $3\,t_0 + t_1\,m + ((m^2 + 2p) / 3 -3)/3 \equiv 0\ (q/3)$. Si $9 \nmid q$ entonces t_0 es único módulo q / 3 verificando esta congruencia. Y $s_0 = 3t_0 - 1$.

Si $m \equiv 2(3)$

entonces, por el lema 3.7. y teniendo en cuenta la definición de m, $(\sigma^2 - \sigma) / 3 \in R$. Luego existen t_0, $t_1 \in \{0,1,\ldots,q/3 - 1\}$ tales que $(t_0 + t_1\sigma + (\sigma^2 - \sigma)/3)/(q/3) \in R$. Imponiendo que la traza de dicho elemento esté en Z, nos queda $3\,t_0 + t_1\,m + ((m^2 + 2p) / 3 -m)/3 \equiv 0\ (q/3)$. Si $9 \nmid q$ entonces t_0 es único módulo q / 3 verificando esta congruencia. Y $s_0 = 3t_0$.

En general, si $r = v_3(q) \geq 1$ entonces en primer lugar minimizamos en 3 la base $(1,\sigma,\sigma^2)$ para de este modo

obtener s_0 a partir de t_0 solución única de una congruencia módulo $q / 3^r$.

c.q.d.

En el primer paso del teorema de Godwin para encontrar un par de unidades fundamentales, en el caso de un cuerpo cúbico totalmente real, hay que minimizar S en el conjunto de las unidades de R distintas de ± 1. Necesitamos, pues, imponer la condición norma de un elemento de R igual a ± 1. Dicha condición es estudiada en la siguiente proposición.

Proposición 3.9. : Sea K cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos q impar. Sean s, e, c ϵ Z. La condición $N^K_Q((s + e\sigma + c\sigma^2)/q) = \pm 1$ equivale a :

$-s^3 -$

$-s^2(em + c((m^2 + 2p)/3)) +$

$+s(c^2 (((2dm - m^4)/3 - p^2)/9) + e^2((p - m^2)/3) + ec((d - - 2m^3)/9))+$

$+(-c^3((((d + m^3)/3 - pm)/9)^2) - e^3(((d + m^3)/3 - pm)/9) +$

$+ec^2(((d + m^3)/3 - pm)/9) ((p - m^2)/3) - e^2c(((d + m^3)/3 - - pm)/9)m \pm q^3) = 0.$

($\sigma = (m + \theta_1) / 3$, $m = [(4p - 27q^2)^{1/2} - 3] / 2$).

Demostración : Imponer la condición $N^K_Q((s + e\sigma + c\sigma^2)/q) = = \pm 1$ equivale a igualar a $\pm 3^6q^3$ el primer miembro de la tercera congruencia del lema 3.7., tomando $A = 9s + 3em + + cm^2$, $B = 3e + 2cm$, $C = c$ y $r = 9q$. Ahora bien, utilizando las congruencias del lema 3.6. , dividimos ambos miembros de

dicha igualdad entre 3^6, resultando la condición dada en el enunciado de la proposición.

c.q.d.

Por tanto, imponer la condición $N^K_Q((s + e\sigma + c\sigma^2)/q) = \pm 1$ una vez que tengamos fijados e,c equivale a estudiar la existencia de una raíz en Z del polinomio $P(s) \in Z[x]$ que hemos enunciado en la proposición anterior. Para la obtención de las raíces en Z del polinomio P(s), utilizamos el método aproximado de Newton o de las tangentes para obtener, en primer lugar, sus raíces reales. A continuación, tomamos el entero más próximo a cada una de las raíces reales y vemos si es o no raíz de P(s).

Una vez obtenida una unidad fundamental σ_1 aplicando el teorema de Godwin, la segunda unidad fundamental se obtiene minimizando S en el conjunto de las unidades de R distintas de $\pm \sigma_1^n$, $n \in Z$. En nuestro caso, K es cúbico cíclico; por tanto, $\sigma_2 = \sigma_1'$ (conjugado de σ_1) es una unidad de R. Veamos a continuación que $\sigma_2 = \sigma_1' \neq \pm \sigma_1^n$. Así, como $S(\sigma_1') = S(\sigma_1)$, entonces (σ_1, σ_1') es un sistema fundamental de unidades de K.

Proposición 3.10.: Sea K cúbico cíclico. Sea u una unidad de R, $u \neq \pm 1$. Si u' es un conjugado de u entonces $u' \neq \pm u^r$ con $r \in Z$.

Demostración : Por ser K cúbico cíclico, Gal(K/Q) (grupo de Galois de K sobre Q) = $(1, \Phi, \Phi^2)$. Supongamos $u' = \pm u^r$ con

$r \in Z$; entonces

$\Phi(u) = u' = \pm u^r$, (obviamente, podemos suponer $\Phi(u) = u'$).

$\Phi^2(u) = \Phi(\pm u^r) = \pm (\pm u^r)^r = u''$.

Pero, por ser u unidad de R, $uu'u'' = \pm 1$ luego $uu^r(u^r)^r = \pm 1$ Y, como $u \neq \pm 1$, necesariamente $r^2 + r + 1 = 0$ con $r \in Z$, absurdo.

c.q.d.

Como ya hemos comentado, el caso q par tiene que ser considerado aparte. En este caso, la definición de m que tenemos que dar es $m = (p - 27(q/2)^2)^{1/2}$ resultando un estudio paralelo al ya efectuado para q impar.

Lema 3.11 .: Sea K cuerpo de números cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos q par. Entonces:

(i) $\sigma = (m + \theta_1) / 3 \in R$.

(ii) $disc(\sigma) = p^2q^2$.

($m = (p - 27(q/2)^2)^{1/2}$,

$\theta_1=(2p - 9(q/2)\theta - 3\theta^2)/(p - 27(q/2)^2)^{1/2}$).

Demostración : es análoga a la del lema 3.4.

De forma análoga a como se demuestra en el caso q impar también en el caso q par existen s_0, $s_1 \in \{0,\ldots,q-1\}$ tales que $\{1,\sigma,(s_0 + s_1\sigma + \sigma^2)/q\}$ es una base entera de R anillo de enteros de K. De momento, no nos preocupamos de obtener s_0, s_1. Tras el estudio de la función S de Godwin, obtendremos información sobre ellos.

También en este caso q par vamos a tener un lema, el lema 3.12., análogo al 3.6. y que nos será de gran utilidad al estudiar la norma de un elemento de R.

Lema 3.12. : Sea K cúbico cíclico de discriminante p^2; K=Q(θ) con Irr(θ,Q) = $x^3 - px + pq$ y suponemos q par. Se verifican las siguientes congruencias :

(a) $(d + m^3)/3 - pm \equiv 0 \ (9)$.

(b) $(2dm - m^4)/3 - p^2 \equiv 0 \ (9)$.

siendo $m = (p - 27(q/2)^2)^{1/2}$, $d = 2pm$.

Demostración :

$(d + m^3)/3 - pm = -9(q/2)^2 m \equiv 0 \ (9)$.

$(2dm - m^4)/3 - p^2 = -9(q/2)^2(2p + 27(q/2)^2) \equiv 0(9)$.

c.q.d.

Y ya estamos en condiciones de enunciar el teorema 3.13. que no es sino un minucioso estudio de la función S de Godwin en el caso q par y su aplicación a la determinación definitiva de la base entera $\{1,\sigma,(s_0 + s_1\sigma + \sigma^2)/q\}$.

Teorema 3.13. : Sea K cúbico cíclico de discriminante p^2. K = Q(θ), Irr(θ,Q) = $x^3 - px + pq$ y supongamos q par. Sea $S(\alpha) = (1/2)\ [(\alpha - \alpha')^2 + (\alpha - \alpha'')^2 + (\alpha'' - \alpha')^2]$ definida para $\alpha \in K$. Entonces :

(i) $S(\alpha) \in p\ Z^+$, para todo $\alpha \in R$.

(ii) $4(S(\alpha)/p) = [\ 2u + ((2m + 2s_1)/q)\ v]^2 + 3v^2$

siendo $\alpha = t + u\,\sigma + v\,((s_0 + s_1\,\sigma + \sigma^2)/q)$ con $t, u, v \in Z$.

(iii) $(2m + 2s_1) / q \in Z$.

(iv) $\{1, \sigma, (s_0 + s_1\,\sigma + \sigma^2) / q\}$ es base entera de K, siendo s_1 igual a 1 si $q = 2$ y, en caso contrario, s_1 es el único elemento de $\{0, 1, \ldots, q-1\}$ tal que $m + s_1 \equiv 0\ (q/2)$, y $(m + s_1)/(q/2) \equiv 1(2)$.

Si $3 \nmid q$, s_0 es el único elemento de $\{0, 1, \ldots, q-1\}$ tal que $9\,s_0 + 3\,s_1\,m + m^2 + 2p \equiv 0\ (q)$.

Y, en general, si $r = v_3(q) \geq 1$ entonces en primer lugar minimizamos en 3 la base $(1, \sigma, \sigma^2)$ para de este modo obtener s_0 a partir de t_0 solución única de una congruencia módulo $q / 3^r$.

$(\sigma = (m + \theta_1) / 3\ ,\ m = (p - 27(q/2)^2)^{1/2})$.

Demostración: es totalmente paralela a la del teorema 3.8. y no la vamos a detallar.

La condición norma de un elemento de R igual a ±1 en el caso q par viene estudiada en la siguiente proposición 3.14., que es totalmente análoga a la proposición 3.9., en virtud básicamente del lema 3.12.

Proposición 3.14. : Sea K cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta, Q) = x^3 - px + pq$ y supongamos q par. Sean s, e, $c \in Z$. La condición $N^K_Q((s + e\sigma + c\sigma^2)/q) = \pm 1$ equivale a :

$$-s^3 -$$

$$-s^2(em + c((m^2 + 2p)/3)) +$$

$$+s(c^2\ (((2dm - m^4)/3 - p^2)/9) + e^2((p - m^2)/3) + ec((d - - 2m^3)/9))+$$

$$+(-c^3((((d + m^3)/3 - pm)/9)^2) - e^3(((d + m^3)/3 - pm)/9) +$$

$$+ec^2(((d + m^3)/3 - pm)/9)\ ((p - m^2)/3) - e^2c(((d + m^3)/3 - - pm)/9)m \pm q^3) = 0.$$

$$(\ \sigma = (m + \theta_1)\ /\ 3\ ,\ \ m = (p - 27(q/2)^2)^{1/2}\ ).$$

Después de este minucioso estudio teórico de la función S de Godwin, del teorema de Godwin deducimos el siguiente algoritmo de cálculo de unidades fundamentales para K cúbico cíclico:

Sea K cuerpo de números cúbico cíclico de discriminante p^2; $K = Q(\theta)$ con $Irr(\theta,Q) = x^3 - px + pq$, $q \in Z^+ - \{ 0 \}$. Y suponemos, por ejemplo, q impar.

(1) Fijados (p,q) el primer paso es calcular s_1 el único elemento de $\{ 0, 1,..., q-1 \}$ tal que $2m + 1 + 2s_1 \equiv 0 \ (q)$.
Si $3 \nmid q$, s_0 es el único elemento de $\{0, 1,...,q-1\}$ tal que $9\ s_0 + 3\ s_1\ m + m^2 + 2p \equiv 0\ (q)$.
Si $3 \mid q$ pero $9 \nmid q$ (o sea, $v_3(q) = 1$), entonces
para $m \equiv 1(3)$ es $s_0 = -1 + 3t_0$ siendo t_0 único tal que $3\ t_0 + t_1\ m + ((m^2 + 2p)\ /\ 3 -3)\ /\ 3 \equiv 0\ (q/3)$;
para $m \equiv 2(3)$ es $s_0 = 3t_0$ siendo t_0 único tal que $3\ t_0 +$

$t_1 m + ((m^2 + 2p) / 3 - m) / 3 \equiv 0 \quad (q/3)$.

Y, en general, si $r = v_3(q) \geq 1$ entonces en primer lugar minimizamos en 3 la base $(1,\sigma,\sigma^2)$ para de este modo obtener s_0 a partir de t_0 solución única de una congruencia módulo $q / 3^r$.

Computamos también el valor de $m = [(4p - 27q^2)^{1/2} - 3] / 2$, $d = p(4p - 27q^2)^{1/2}$.

(2) A continuación, tomamos el primer múltiplo de 4, llamémosle j, que se pueda poner de la forma $a^2 + 3b^2$ con $a, b \in Z$. Y calculamos todos los $u, v \in Z$ tales que $j = [2u + ((2m + 1 + 2s_1)/q)\ v]^2 + 3v^2$.

(3) Para cada par (u, v) obtenido y a partir de los valores ya calculados para s_0, s_1, d, m tomamos $e = qu + s_1v$, $c = v$ y sustituimos dichos valores en el primer miembro de la igualdad dada en el enunciado de la proposición 3.9., obteniendo un polinomio P(s) de grado 3 en s con coeficientes en Z. Con el método aproximado de Newton obtenemos las raíces reales de dicho polinomio. Tomamos el entero más próximo a cada una de las raíces reales obtenidas y vemos si es o no raíz de P(s). En caso de encontrar un $s \in Z$ raíz de P(s), vemos si se verifica o no la condición $s \equiv s_0v(q)$. En caso afirmativo, tomamos $t = (s - s_0v) / q \in Z$ y (t, u, v) dan las coordenadas respecto de la base $(1, \sigma, (s_0 + s_1 \sigma + \sigma^2)/q)$ de una unidad fundamental de K. Y esto se repite para cada par (u, v) que definen el mismo j múltiplo de 4 de la forma $a^2 + + 3b^2$.

(4) En caso de no encontrar s raíz entera de P(s) verificando $s \equiv s_0 v(q)$, repetimos el paso (3) para el siguiente múltiplo de 4 que sea expresable en la forma $a^2 + 3b^2$ con a, b ϵ Z. En un número finito de pasos el proceso termina.

(5) Finalizado el paso 4 tendremos, para cada cuerpo cúbico cíclico asociado al par (p, q), computadas todas las unidades de R en las que se alcanza el mínimo de $4(S(\alpha)/p)$. Calculamos a continuación la traza de cada una de ellas. Un par formado por dos de dichas unidades que tengan en valor absoluto la misma traza son, salvo un signo, conjugadas y, por el teorema de Godwin forman un sistema fundamental de unidades de K.

En el caso q par el algoritmo que obtenemos es totalmente similar al detallado en el caso q impar, efectuando los cambios adecuados según el estudio realizado.

El teorema de Godwin ya computable es programado en lenguaje Fortran 77 y ejecutado en un VAX VMS. La única limitación en su ejecución es la precisión del lenguaje utilizado. Dicho programa tiene como entrada la raíz p del discriminante de K y el valor de q asociado a K . Dichos datos de entrada son, a su vez, datos de salida de la ejecución de otro programa Fortran que calcula todos los cuerpos cúbicos cíclicos de discriminante dado. Los datos de salida del programa principal son:

m : $m = ((4p - 27q^2)^{1/2} - 3)/2$ en el caso q impar,
$m = (p - 27(q/2)^2)^{1/2}$ si q es par.

s_0, s_1 : elementos del conjunto $\{0,1,\ldots,q-1\}$ tales que $\{1, \sigma, (s_0 + s_1\sigma + \sigma^2)/q\}$ es base entera de K.
$(\sigma = (m + \theta_1)/3,$
$\theta_1 = (4p - 9q\theta - 6\theta^2)/(4p - 27q^2)^{1/2})$.

t,u,v : coordenadas de una unidad fundamental δ de K respecto de la base entera anterior.

Traza(δ) : traza de δ.

4(S(δ)/p): valor del mínimo de 4(S(δ)/p) en el conjunto de las unidades de R distintas de ± 1.

Para cada cuerpo K la tabla obtiene todas las unidades de R en las que se alcanza el mínimo de 4(S(δ)/p). Se calcula la traza de cada una de ellas; un par formado por dos de dichas unidades que tengan en valor absoluto la misma traza forman un sistema fundamental de unidades de K.

En el posterior análisis de la tabla y en la obtención de consecuencias, el haber computado todas las unidades de R en las que se alcanza el mínimo de 4(S(α)/p) jugará un papel decisivo.

En cada caso encontramos una unidad fundamental cuya traza coincide en valor absoluto con las tabuladas por M.N. Gras [G2]; dicha tabulación fue completada por Godwin [Go2] en los casos en que la precisión del ordenador utilizado por Gras fue insuficiente.

Reproducimos a continuación los datos de la tabla de unidades fundamentales que construimos. En el apartado 3.C. haremos un análisis de la misma.

Vamos a poner un ejemplo con el fin de facilitar la lectura de la tabla de unidades fundamentales.

El único cuerpo cúbico cíclico de discriminante 19^2 es $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - 19x + 19$. En este caso $s_0 = s_1 = 0$, o sea $\{1,\sigma,\sigma^2\}$ es base entera de K. El mínimo de $4(S(\alpha)/p)$ en el conjunto de las unidades de R distintas de ± 1 es igual a 4. Dicho mínimo se alcanza en las siguientes unidades de R, de coordenadas (t,u,v) respecto de la base $\{1,\sigma,\sigma^2\}$:

C_1 = { (1,1,0), (-5,-2,1),(-1,-3,1) } de traza en valor absoluto 5 .

C_2 = { (0,1,0), (-4,-2,1),(-2,-3,1) } de traza en valor absoluto 2.

Hemos agrupado las unidades con igual traza en valor absoluto. Dos unidades cualesquiera y distintas tomadas del mismo conjunto C_i, $1 \leq i \leq 2$, forman un sistema fundamental de unidades de K. En este caso, pues, hemos obtenido 6 sistemas fundamentales de unidades de K.

Nota:

En el teorema de Godwin hay una condición adicional y es $S(\mu) > 0$. Dado que nosotros demostramos que $S(\alpha)$ es un múltiplo de p, siendo p^2 el discriminante del cuerpo, para cada $\alpha \in B$, los únicos casos, en principio, a los que no podemos aplicar el teorema de Godwin son $p = 7, 9$. Estos casos están dentro de la que llamaremos familia U, y el sistema fundamental de unidades que damos para los cuerpos cúbicos ciclicos de esta familia es también válido en estos casos, según demuestra Thomas [T].

TABLA DE UNIDADES FUNDAMENTALES DE K CUERPO CUBICO CICLICO DE DISCRIMINANTE $p^2 < 16.10^6$

p	m	q	sø	s1	t	u	v	traza(δ)*	4S(δ)/p
7	-1	1	0	0	1	1	0	2	4
7	-1	1	0	0	2	1	0	5	4
7	-1	1	0	0	0	1	0	-1*	4
7	-1	1	0	0	-1	1	0	-4	4
7	-1	1	0	0	-3	1	1	-5	4
7	-1	1	0	0	0	1	1	4	4
7	-1	1	0	0	-1	1	1	1*	4
7	-1	1	0	0	-2	1	1	-2	4
7	-1	1	0	0	-1	0	1	2	4
7	-1	1	0	0	0	0	1	5	4
7	-1	1	0	0	-2	0	1	-1*	4
7	-1	1	0	0	-3	0	1	-4	4
9	0	1	0	0	-2	1	0	-6	4
9	0	1	0	0	1	1	0	3	4
9	0	1	0	0	0	1	0	0*	4
9	0	1	0	0	-2	0	1	0*	4
9	0	1	0	0	0	0	1	6	4
9	0	1	0	0	-3	0	1	-3	4
9	0	1	0	0	-4	-1	1	-6	4
9	0	1	0	0	-1	-1	1	3	4
9	0	1	0	0	-2	-1	1	0*	4
13	1	1	0	0	1	1	0	4	4
13	1	1	0	0	0	1	0	1*	4
13	1	1	0	0	-3	-1	1	-1*	4
13	1	1	0	0	-4	-1	1	-4	4
13	1	1	0	0	-1	-2	1	4	4
13	1	1	0	0	-2	-2	1	1*	4
19	2	1	0	0	1	1	0	5	4
19	2	1	0	0	0	1	0	2*	4
19	2	1	0	0	-4	-2	1	-2*	4
19	2	1	0	0	-5	-2	1	-5	4
19	2	1	0	0	-1	-3	1	5	4
19	2	1	0	0	-2	-3	1	2*	4
31	2	2	0	1	-3	0	2	15*	48
31	2	2	0	1	1	-6	2	15*	48
31	2	2	0	1	-17	-6	4	-15*	48

*En cada caso, hay tres unidades fundamentales cuyas trazas coinciden, salvo el signo, con las calculadas por Gras[G2]. A modo de ejemplo, señalamos con un * las que coinciden en los casos de esta primera página de la tabla.

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
37	4	1	0	0	1	1	0	7	4
37	4	1	0	0	0	1	0	4	4
37	4	1	0	0	-6	-4	1	-4	4
37	4	1	0	0	-7	-4	1	-7	4
37	4	1	0	0	-1	-5	1	7	4
37	4	1	0	0	-2	-5	1	4	4
43	4	2	0	1	11	-2	0	25	16
43	4	2	0	1	1	-4	2	25	16
43	4	2	0	1	-13	-6	2	-25	16
61	-1	3	0	2	2	3	3	42	108
61	-1	3	0	2	1	3	3	39	108
61	-1	3	0	2	-1	-6	3	42	108
61	-1	3	0	2	-2	-6	3	39	108
61	-1	3	0	2	-40	-3	6	-39	108
61	-1	3	0	2	-41	-3	6	-42	108
63	6	1	0	0	1	1	0	9	4
63	6	1	0	0	0	1	0	6	4
63	6	1	0	0	-8	-6	1	-6	4
63	6	1	0	0	-9	-6	1	-9	4
63	6	1	0	0	-1	-7	1	9	4
63	6	1	0	0	-2	-7	1	6	4
63	6	2	0	1	1	-2	0	-9	16
63	6	2	0	1	-11	-6	2	-9	16
63	6	2	0	1	-1	-8	2	9	16
67	1	3	2	0	0	3	1	20	52
67	1	3	2	0	-9	-4	3	20	52
67	1	3	2	0	-29	-1	4	-20	52
73	2	3	0	2	3	2	2	49	112
73	2	3	0	2	-1	-10	4	49	112
73	2	3	0	2	-47	-8	6	-49	112
79	7	1	0	0	1	1	0	10	4
79	7	1	0	0	0	1	0	7	4
79	7	1	0	0	-9	-7	1	-7	4
79	7	1	0	0	-10	-7	1	-10	4
79	7	1	0	0	-1	-8	1	10	4
79	7	1	0	0	-2	-8	1	7	4
91	8	2	0	1	-3	-2	0	-25	16
91	8	2	0	1	-17	-8	2	-25	16
91	8	2	0	1	5	-10	2	25	16
91	4	3	2	0	0	1	0	4	4
91	4	3	2	0	-8	-1	1	-4	4
91	4	3	2	0	-4	-2	1	4	4

p	m	q	sØ	s1	t	u	v	traza(δ)	4S(δ)/p
97	8	1	0	0	1	1	0	11	4
97	8	1	0	0	0	1	0	8	4
97	8	1	0	0	-10	-8	1	-8	4
97	8	1	0	0	-11	-8	1	-11	4
97	8	1	0	0	-1	-9	1	11	4
97	8	1	0	0	-2	-9	1	8	4
103	5	3	0	2	-6	-1	2	35	76
103	5	3	0	2	1	-11	3	35	76
103	5	3	0	2	-40	-12	5	-35	76
109	1	4	2	1	-47	78	70	1337	65776
109	1	4	2	1	-25	-148	78	1337	65776
109	1	4	2	1	-1409	-70	148	-1337	65776
117	9	1	0	0	1	1	0	12	4
117	9	1	0	0	0	1	0	9	4
117	9	1	0	0	-11	-9	1	-9	4
117	9	1	0	0	-12	-9	1	-12	4
117	9	1	0	0	-1	-10	1	12	4
117	9	1	0	0	-2	-10	1	9	4
117	3	4	2	3	-7	2	6	129	592
117	3	4	2	3	1	-22	8	129	592
117	3	4	2	3	-135	-20	14	-129	592
127	10	2	0	1	-87	-58	18	311	7696
127	10	2	0	1	121	-210	32	311	7696
127	10	2	0	1	-277	-268	50	-311	7696
133	7	3	2	0	3	1	0	16	4
133	7	3	2	0	-13	-2	1	-16	4
133	7	3	2	0	0	-3	1	16	4
133	5	4	2	1	-7	6	8	225	1488
133	5	4	2	1	9	-36	14	225	1488
133	5	4	2	1	-223	-30	22	-225	1488
139	10	1	0	0	1	1	0	13	4
139	10	1	0	0	0	1	0	10	4
139	10	1	0	0	-12	-10	1	-10	4
139	10	1	0	0	-13	-10	1	-13	4
139	10	1	0	0	-1	-11	1	13	4
139	10	1	0	0	-2	-11	1	10	4
151	8	3	0	2	19	-6	1	55	28
151	8	3	0	2	1	-5	2	55	28
151	8	3	0	2	-35	-11	3	-55	28
157	7	4	2	3	-319	16	270	9145	2128624
157	7	4	2	3	713	-1938	556	9145	2128624
157	7	4	2	3	-8751	-1922	826	-9145	2128624

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
163	11	1	0	0	1	1	0	14	4
163	11	1	0	0	0	1	0	11	4
163	11	1	0	0	-13	-11	1	-11	4
163	11	1	0	0	-14	-11	1	-14	4
163	11	1	0	0	-1	-12	1	14	4
163	11	1	0	0	-2	-12	1	11	4
171	12	2	0	1	-1	-2	4	321	2352
171	12	2	0	1	101	-158	22	321	2352
171	12	2	0	1	-221	-160	26	-321	2352
171	0	5	2	2	0	1	1	24	12
171	0	5	2	2	-1	1	1	21	12
171	0	5	2	2	0	-2	1	24	12
171	0	5	2	2	-1	-2	1	21	12
171	0	5	2	2	-23	-1	2	-21	12
171	0	5	2	2	-24	-1	2	-24	12
181	2	5	1	0	-1	-5	2	37	76
181	2	5	1	0	-14	2	3	37	76
181	2	5	1	0	-52	-3	5	-37	76
193	10	3	2	0	-8	8	7	448	4372
193	10	3	2	0	18	-123	29	448	4372
193	10	3	2	0	-438	-115	36	-448	4372
199	4	5	0	3	-3	2	4	119	304
199	4	5	0	3	1	-16	6	119	304
199	4	5	0	3	-121	-14	10	-119	304
211	5	5	2	2	-1	3	1	45	84
211	5	5	2	2	-14	-9	4	45	84
211	5	5	2	2	-60	-6	5	-45	84
217	13	1	0	0	1	1	0	16	4
217	13	1	0	0	0	1	0	13	4
217	13	1	0	0	-15	-13	1	-13	4
217	13	1	0	0	-16	-13	1	-16	4
217	13	1	0	0	-1	-14	1	16	4
217	13	1	0	0	-2	-14	1	13	4
217	11	3	0	2	-1	0	3	204	756
217	11	3	0	2	-2	0	3	201	756
217	11	3	0	2	23	-63	12	204	756
217	11	3	0	2	22	-63	12	201	756
217	11	3	0	2	-181	-63	15	-201	756
217	11	3	0	2	-182	-63	15	-204	756
223	14	2	0	1	-753	-350	1568	171593	528128272
223	14	2	0	1	57431	-86576	10626	171593	528128272
223	14	2	0	1	-114915	-86926	12194	-171593	528128272

p	m	q	sØ	sl	t	u	v	traza(δ)	4S(δ)/p
229	11	4	2	3	-511	-58	374	19521	6679632
229	11	4	2	3	2913	-4630	1064	19521	6679632
229	11	4	2	3	-17119	-4688	1438	-19521	6679632
241	7	5	1	0	-4	7	7	289	1372
241	7	5	1	0	-5	7	7	286	1372
241	7	5	1	0	10	-35	14	289	1372
241	7	5	1	0	9	-35	14	286	1372
241	7	5	1	0	-282	-28	21	-286	1372
241	7	5	1	0	-283	-28	21	-289	1372
247	14	1	0	0	1	1	0	17	4
247	14	1	0	0	0	1	0	14	4
247	14	1	0	0	-16	-14	1	-14	4
247	14	1	0	0	-17	-14	1	-17	4
247	14	1	0	0	-1	-15	1	17	4
247	14	1	0	0	-2	-15	1	14	4
259	8	5	3	4	-1	0	1	44	28
259	8	5	3	4	-2	0	1	41	28
259	8	5	3	4	2	-7	2	44	28
259	8	5	3	4	1	-7	2	41	28
259	8	5	3	4	-42	-7	3	-41	28
259	8	5	3	4	-43	-7	3	-44	28
271	13	3	2	0	-98	-27	9	84	972
271	13	3	2	0	19	-54	9	84	972
271	13	3	2	0	-163	-81	18	-84	972
277	13	4	2	1	-11	-2	2	71	112
277	13	4	2	1	15	-18	4	71	112
277	13	4	2	1	-67	-20	6	-71	112
279	15	1	0	0	1	1	0	18	4
279	15	1	0	0	0	1	0	15	4
279	15	1	0	0	-17	-15	1	-15	4
279	15	1	0	0	-18	-15	1	-18	4
279	15	1	0	0	-1	-16	1	18	4
279	15	1	0	0	-2	-16	1	15	4
279	9	5	0	3	-1	2	0	15	16
279	9	5	0	3	-25	-4	2	-15	16
279	9	5	0	3	-9	-6	2	15	16
283	16	2	0	1	-163	-88	338	47113	31367632
283	16	2	0	1	16635	-23882	2616	47113	31367632
283	16	2	0	1	-30641	-23970	2954	-47113	31367632
301	14	3	0	2	-1	2	0	25	16
301	14	3	0	2	-27	-10	2	-25	16
301	14	3	0	2	-1	-12	2	25	16

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
301	10	5	2	2	5	1	0	25	4
301	10	5	2	2	-19	-2	1	-25	4
301	10	5	2	2	1	-3	1	25	4
313	16	1	0	0	1	1	0	19	4
313	16	1	0	0	0	1	0	16	4
313	16	1	0	0	-18	-16	1	-16	4
313	16	1	0	0	-19	-16	1	-19	4
313	16	1	0	0	-1	-17	1	19	4
313	16	1	0	0	-2	-17	1	16	4
331	-1	7	0	4	2	3	3	96	108
331	-1	7	0	4	1	3	3	93	108
331	-1	7	0	4	-1	-6	3	96	108
331	-1	7	0	4	-2	-6	3	93	108
331	-1	7	0	4	-94	-3	6	-93	108
331	-1	7	0	4	-95	-3	6	-96	108
333	15	4	2	3	-23	-36	38	2697	77232
333	15	4	2	3	625	-618	116	2697	77232
333	15	4	2	3	-2095	-654	154	-2697	77232
333	0	7	3	3	0	1	1	33	12
333	0	7	3	3	-1	1	1	30	12
333	0	7	3	3	0	-2	1	33	12
333	0	7	3	3	-1	-2	1	30	12
333	0	7	3	3	-32	-1	2	-30	12
333	0	7	3	3	-33	-1	2	-33	12
337	1	7	6	2	-5	17	11	387	2388
337	1	7	6	2	-60	-28	17	387	2388
337	1	7	6	2	-452	-11	28	-387	2388
349	17	1	0	0	1	1	0	20	4
349	17	1	0	0	0	1	0	17	4
349	17	1	0	0	-19	-17	1	-17	4
349	17	1	0	0	-20	-17	1	-20	4
349	17	1	0	0	-1	-18	1	20	4
349	17	1	0	0	-2	-18	1	17	4
367	16	3	2	0	-333	208	285	34249	12853276
367	16	3	2	0	4227	-10083	1633	34249	12853276
367	16	3	2	0	-30355	-9875	1918	-34249	12853276
373	5	7	4	5	-30	19	38	1601	27436
373	5	7	4	5	-31	19	38	1598	27436
373	5	7	4	5	-11	-152	57	1601	27436
373	5	7	4	5	-12	-152	57	1598	27436
373	5	7	4	5	-1641	-133	95	-1598	27436
373	5	7	4	5	-1642	-133	95	-1601	27436

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
379	13	5	3	4	-16	0	13	914	8788
379	13	5	3	4	-17	0	13	911	8788
379	13	5	3	4	75	-169	39	914	8788
379	13	5	3	4	74	-169	39	911	8788
379	13	5	3	4	-854	-169	52	-911	8788
379	13	5	3	4	-855	-169	52	-914	8788
387	18	1	0	0	1	1	0	21	4
387	18	1	0	0	0	1	0	18	4
387	18	1	0	0	-20	-18	1	-18	4
387	18	1	0	0	-21	-18	1	-21	4
387	18	1	0	0	-1	-19	1	21	4
387	18	1	0	0	-2	-19	1	18	4
387	6	7	0	4	1	-4	1	21	28
387	6	7	0	4	-19	-1	2	21	28
387	6	7	0	4	-39	-5	3	-21	28
397	17	4	2	1	5	-6	2	105	48
397	17	4	2	1	39	-12	2	105	48
397	17	4	2	1	-61	-18	4	-105	48
403	17	3	0	2	5	2	0	49	16
403	17	3	0	2	-37	-12	2	-49	16
403	17	3	0	2	7	-14	2	49	16
403	7	7	3	3	-1	1	1	49	28
403	7	7	3	3	-2	-5	2	49	28
403	7	7	3	3	-52	-4	3	-49	28
409	14	5	0	3	-23	1	19	1389	19308
409	14	5	0	3	165	-251	58	1389	19308
409	14	5	0	3	-1247	-250	77	-1389	19308
421	8	7	6	2	-21	5	8	361	1348
421	8	7	6	2	3	-34	13	361	1348
421	8	7	6	2	-379	-29	21	-361	1348
427	19	1	0	0	1	1	0	22	4
427	19	1	0	0	0	1	0	19	4
427	19	1	0	0	-21	-19	1	-19	4
427	19	1	0	0	-22	-19	1	-22	4
427	19	1	0	0	-1	-20	1	22	4
427	19	1	0	0	-2	-20	1	19	4
427	20	2	0	1	-39	-28	42	8521	687568
427	20	2	0	1	3251	-4354	392	8521	687568
427	20	2	0	1	-5309	-4382	434	-8521	687568
433	1	8	4	3	-5319	8514	8054	298609	823707472
433	1	8	4	3	-2785	-16568	8514	298609	823707472

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
433	1	8	4	3	-306713	-8054	16568	-298609	823707472
463	10	7	5	0	-9	7	7	400	1372
463	10	7	5	0	-10	7	7	397	1372
463	10	7	5	0	12	-35	14	400	1372
463	10	7	5	0	11	-35	14	397	1372
463	10	7	5	0	-396	-28	21	-397	1372
463	10	7	5	0	-397	-28	21	-400	1372
469	20	1	0	0	1	1	0	23	4
469	20	1	0	0	0	1	0	20	4
469	20	1	0	0	-22	-20	1	-20	4
469	20	1	0	0	-23	-20	1	-23	4
469	20	1	0	0	-1	-21	1	23	4
469	20	1	0	0	-2	-21	1	20	4
469	19	4	2	3	33	-46	14	961	4432
469	19	4	2	3	329	-158	24	961	4432
469	19	4	2	3	-599	-204	38	-961	4432
469	19	4	2	3	33	-46	14	961	4432
469	19	4	2	3	329	-158	24	961	4432
469	19	4	2	3	-599	-204	38	-961	4432
481	19	3	2	0	-2	2	1	181	292
481	19	3	2	0	24	-57	8	181	292
481	19	3	2	0	-159	-55	9	-181	292
481	7	8	4	5	-403	134	290	13649	1547344
481	7	8	4	5	421	-1138	424	13649	1547344
481	7	8	4	5	-13631	-1004	714	-13649	1547344
487	11	7	1	6	-130	13	142	8557	602188
487	11	7	1	6	502	-1033	297	8557	602188
487	11	7	1	6	-8185	-1020	439	-8557	602188
511	22	2	0	1	-25	-16	54	13721	1472848
511	22	2	0	1	5355	-6990	578	13721	1472848
511	22	2	0	1	-8391	-7006	632	-13721	1472848
511	17	5	1	0	-4	0	1	76	52
511	17	5	1	0	11	-13	3	76	52
511	17	5	1	0	-69	-13	4	-76	52
523	20	3	0	2	-163	-22	325	55621	23655436
523	20	3	0	2	10193	-18349	2253	55621	23655436
523	20	3	0	2	-45591	-18371	2578	-55621	23655436
541	13	7	0	4	-3	2	2	151	208
541	13	7	0	4	3	-20	6	151	208
541	13	7	0	4	-151	-18	8	-151	208

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
547	-1	9	0	5	2	3	3	123	108
547	-1	9	0	5	1	3	3	120	108
547	-1	9	0	5	-1	-6	3	123	108
547	-1	9	0	5	-2	-6	3	120	108
547	-1	9	0	5	-121	-3	6	-120	108
547	-1	9	0	5	-122	-3	6	-123	108
549	18	5	3	4	-6	-1	2	186	268
549	18	5	3	4	25	-37	7	186	268
549	18	5	3	4	-167	-38	9	-186	268
549	21	4	2	1	89	62	48	8049	432016
549	21	4	2	1	2113	-1860	302	8049	432016
549	21	4	2	1	-5847	-1798	350	-8049	432016
553	11	8	4	1	-541	252	318	18321	2429136
553	11	8	4	1	1193	-1458	570	18321	2429136
553	11	8	4	1	-17669	-1206	888	-18321	2429136
553	1	9	8	3	-15	32	27	1175	10468
553	1	9	8	3	-58	-59	32	1175	10468
553	1	9	8	3	-1248	-27	59	-1175	10468
559	22	1	0	0	1	1	0	25	4
559	22	1	0	0	0	1	0	22	4
559	22	1	0	0	-24	-22	1	-22	4
559	22	1	0	0	-25	-22	1	-25	4
559	22	1	0	0	-1	-23	1	25	4
559	22	1	0	0	-2	-23	1	22	4
559	2	9	3	2	2	29	24	1096	8452
559	2	9	3	2	-15	-53	29	1096	8452
559	2	9	3	2	-1109	-24	53	-1096	8452
571	14	7	3	3	1	2	3	244	388
571	14	7	3	3	18	-27	8	244	388
571	14	7	3	3	-225	-25	11	-244	388
577	4	9	2	0	-180	665	504	24296	4125604
577	4	9	2	0	-96	-1169	665	24296	4125604
577	4	9	2	0	-24572	-504	1169	-24296	4125604
589	19	5	0	3	-1	1	0	16	4
589	19	5	0	3	-18	-4	1	-16	4
589	19	5	0	3	-1	-5	1	16	4
589	5	9	6	8	-13	5	14	700	3292
589	5	9	6	8	-3	-52	19	700	3292
589	5	9	6	8	-716	-47	33	-700	3292
603	24	2	0	1	-55	-36	110	32961	7207984
603	24	2	0	1	13151	-16802	1284	32961	7207984

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
603	24	2	0	1	-19865	-16838	1394	-32961	7207984
603	15	7	6	2	-7	3	5	399	1036
603	15	7	6	2	28	-44	13	399	1036
603	15	7	6	2	-378	-41	18	-399	1036
607	23	1	0	0	1	1	0	26	4
607	23	1	0	0	0	1	0	23	4
607	23	1	0	0	-25	-23	1	-23	4
607	23	1	0	0	-26	-23	1	-26	4
607	23	1	0	0	-1	-24	1	26	4
607	23	1	0	0	-2	-24	1	23	4
613	22	3	2	0	-151	67	133	26557	4585708
613	22	3	2	0	4505	-8117	998	26557	4585708
613	22	3	2	0	-22203	-8050	1131	-26557	4585708
631	20	5	2	2	-17	-3	2	129	156
631	20	5	2	2	23	-27	5	129	156
631	20	5	2	2	-123	-30	7	-129	156
657	24	1	0	0	1	1	0	27	4
657	24	1	0	0	0	1	0	24	4
657	24	1	0	0	-26	-24	1	-24	4
657	24	1	0	0	-27	-24	1	-27	4
657	24	1	0	0	-1	-25	1	27	4
657	24	1	0	0	-2	-25	1	24	4
657	15	8	4	5	-75	4	34	2385	35152
657	15	8	4	5	245	-250	72	2385	35152
657	15	8	4	5	-2215	-246	106	-2385	35152
661	23	3	0	2	-1280	-237	2379	516468	1614499884
661	23	3	0	2	102685	-171534	18795	516468	1614499884
661	23	3	0	2	-415063	-171771	21174	-516468	1614499884
673	17	7	5	0	-8	7	0	95	196
673	17	7	5	0	-139	-14	7	-95	196
673	17	7	5	0	-36	-21	7	95	196
679	10	9	8	3	-25	10	14	865	4432
679	10	9	8	3	15	-62	24	865	4432
679	10	9	8	3	-875	-52	38	-865	4432
679	2	10	0	3	-1	20	18	865	4336
679	2	10	0	3	7	-38	20	865	4336
679	2	10	0	3	-859	-18	38	-865	4336
703	26	2	0	1	-25	-14	96	34121	6601744
703	26	2	0	1	13851	-17372	1234	34121	6601744
703	26	2	0	1	-20295	-17386	1330	-34121	6601744

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
703	11	9	3	2	10	1	0	41	4
703	11	9	3	2	-30	-1	1	-41	4
703	11	9	3	2	1	-2	1	41	4
709	25	1	0	0	1	1	0	28	4
709	25	1	0	0	0	1	0	25	4
709	25	1	0	0	-27	-25	1	-25	4
709	25	1	0	0	-28	-25	1	-28	4
709	25	1	0	0	-1	-26	1	28	4
709	25	1	0	0	-2	-26	1	25	4
711	18	7	1	6	-6	5	0	72	100
711	18	7	1	6	-99	-15	5	-72	100
711	18	7	1	6	-21	-20	5	72	100
711	6	10	0	4	-23	22	28	1491	12352
711	6	10	0	4	49	-82	36	1491	12352
711	6	10	0	4	-1465	-60	64	-1491	12352
721	22	5	1	0	-2	1	2	274	412
721	22	5	1	0	-3	1	2	271	412
721	22	5	1	0	49	-47	9	274	412
721	22	5	1	0	48	-47	9	271	412
721	22	5	1	0	-226	-46	11	-271	412
721	22	5	1	0	-227	-46	11	-274	412
721	17	8	4	3	213	98	112	11265	609168
721	17	8	4	3	1277	-1078	322	11265	609168
721	17	8	4	3	-9775	-980	434	-11265	609168
751	19	7	4	5	-22	0	13	1286	8788
751	19	7	4	5	-23	0	13	1283	8788
751	19	7	4	5	147	-169	39	1286	8788
751	19	7	4	5	146	-169	39	1283	8788
751	19	7	4	5	-1160	-169	52	-1283	8788
751	19	7	4	5	-1161	-169	52	-1286	8788
757	13	9	2	0	-762	586	611	43825	10149988
757	13	9	2	0	2493	-3005	1197	43825	10149988
757	13	9	2	0	-42094	-2419	1808	-43825	10149988
763	26	1	0	0	1	1	0	29	4
763	26	1	0	0	0	1	0	26	4
763	26	1	0	0	-28	-26	1	-26	4
763	26	1	0	0	-29	-26	1	-29	4
763	26	1	0	0	-1	-27	1	29	4
763	26	1	0	0	-2	-27	1	26	4
763	25	3	2	0	-7	3	6	1500	11772
763	25	3	2	0	-8	3	6	1497	11772
763	25	3	2	0	278	-465	51	1500	11772
763	25	3	2	0	277	-465	51	1497	11772

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
763	25	3	2	0	-1228	-462	57	-1497	11772
763	25	3	2	0	-1229	-462	57	-1500	11772
769	23	5	3	4	-235	-31	153	22756	2697868
769	23	5	3	4	3865	-4557	734	22756	2697868
769	23	5	3	4	-19126	-4588	887	-22756	2697868
787	14	9	6	8	-1037	24	590	44425	10032304
787	14	9	6	8	2311	-4202	1204	44425	10032304
787	14	9	6	8	-43151	-4178	1794	-44425	10032304
793	20	7	0	4	-1	0	1	103	52
793	20	7	0	4	-2	0	1	100	52
793	20	7	0	4	15	-13	3	103	52
793	20	7	0	4	14	-13	3	100	52
793	20	7	0	4	-88	-13	4	-100	52
793	20	7	0	4	-89	-13	4	-103	52
793	19	8	4	1	-765	206	374	33409	5627152
793	19	8	4	1	4601	-3236	954	33409	5627152
793	19	8	4	1	-29573	-3030	1328	-33409	5627152
817	26	3	0	2	-53	-14	77	20575	2077012
817	26	3	0	2	4357	-6867	679	20575	2077012
817	26	3	0	2	-16271	-6881	756	-20575	2077012
817	-1	11	0	6	2	3	3	150	108
817	-1	11	0	6	1	3	3	147	108
817	-1	11	0	6	-1	-6	3	150	108
817	-1	11	0	6	-2	-6	3	147	108
817	-1	11	0	6	-148	-3	6	-147	108
817	-1	11	0	6	-149	-3	6	-150	108
819	27	1	0	0	1	1	0	30	4
819	27	1	0	0	0	1	0	27	4
819	27	1	0	0	-29	-27	1	-27	4
819	27	1	0	0	-30	-27	1	-30	4
819	27	1	0	0	-1	-28	1	30	4
819	27	1	0	0	-2	-28	1	27	4
819	24	5	0	3	4	1	0	36	4
819	24	5	0	3	-26	-5	1	-36	4
819	24	5	0	3	6	-6	1	36	4
819	12	10	0	3	-73	54	76	5217	130224
819	12	10	0	3	353	-336	130	5217	130224
819	12	10	0	3	-4937	-282	206	-5217	130224
819	0	11	5	5	0	1	1	51	12
819	0	11	5	5	-1	1	1	48	12
819	0	11	5	5	0	-2	1	51	12
819	0	11	5	5	-1	-2	1	48	12

p	m	q	sβ	sl	t	u	v	traza(δ)	4S(δ)/p
819	0	11	5	5	-50	-1	2	-48	12
819	0	11	5	5	-51	-1	2	-51	12
823	1	11	10	4	-402	759	686	35911	6269404
823	1	11	10	4	-957	-1445	759	35911	6269404
823	1	11	10	4	-37270	-686	1445	-35911	6269404
829	2	11	4	3	-42	257	223	11984	692356
829	2	11	4	3	-140	-480	257	11984	692356
829	2	11	4	3	-12166	-223	480	-11984	692356
853	16	9	5	6	-15	-14	21	1516	7252
853	16	9	5	6	272	-105	28	1516	7252
853	16	9	5	6	-1259	-119	49	-1516	7252
859	5	11	8	0	-2	6	1	79	172
859	5	11	8	0	-72	-7	6	79	172
859	5	11	8	0	-153	-1	7	-79	172
871	25	5	2	2	6	-7	2	181	76
871	25	5	2	2	58	-20	3	181	76
871	25	5	2	2	-117	-27	5	-181	76
873	6	11	2	10	3	-14	3	105	388
873	6	11	2	10	-115	-5	8	105	388
873	6	11	2	10	-217	-19	11	-105	388
877	28	1	0	0	1	1	0	31	4
877	28	1	0	0	0	1	0	28	4
877	28	1	0	0	-30	-28	1	-28	4
877	28	1	0	0	-31	-28	1	-31	4
877	28	1	0	0	-1	-29	1	31	4
877	28	1	0	0	-2	-29	1	28	4
883	22	7	6	2	-29	13	7	1011	5772
883	22	7	6	2	71	-143	34	1011	5772
883	22	7	6	2	-969	-130	41	-1011	5772
889	17	9	0	5	-16	3	11	949	4084
889	17	9	0	5	87	-86	25	949	4084
889	17	9	0	5	-878	-83	36	-949	4084
889	7	11	7	9	-1	0	1	60	12
889	7	11	7	9	6	-3	1	60	12
889	7	11	7	9	-55	-3	2	-60	12
907	8	11	1	8	-22	4	11	659	2044
907	8	11	1	8	14	-41	15	659	2044
907	8	11	1	8	-667	-37	26	-659	2044
927	9	11	6	7	-14	2	5	306	436
927	9	11	6	7	5	-19	7	306	436

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
927	9	11	6	7	-315	-17	12	-306	436
937	29	1	0	0	1	1	0	32	4
937	29	1	0	0	0	1	0	29	4
937	29	1	0	0	-31	-29	1	-29	4
937	29	1	0	0	-32	-29	1	-32	4
937	29	1	0	0	-1	-30	1	32	4
937	29	1	0	0	-2	-30	1	29	4
949	29	4	2	1	-3	2	0	49	16
949	29	4	2	1	-39	-14	2	-49	16
949	29	4	2	1	13	-16	2	49	16
949	10	11	0	6	13	1	0	49	4
949	10	11	0	6	-35	-1	1	-49	4
949	10	11	0	6	1	-2	1	49	4
967	19	9	8	3	-9381	2055	4303	415384	712188052
967	19	9	8	3	34228	-36286	10661	415384	712188052
967	19	9	8	3	-390537	-34231	14964	-415384	712188052
973	11	11	5	5	-6	3	4	291	372
973	11	11	5	5	2	-18	7	291	372
973	11	11	5	5	-295	-15	11	-291	372
981	27	5	1	0	-134	-31	4	-519	372
981	27	5	1	0	-314	-31	7	-519	372
981	27	5	1	0	71	-62	11	519	372
981	24	7	5	0	-17	1	4	465	948
981	24	7	5	0	70	-56	13	465	948
981	24	7	5	0	-412	-55	17	-465	948
991	29	3	0	2	101	63	189	65067	16876188
991	29	3	0	2	14402	-21672	1953	65067	16876188
991	29	3	0	2	-50564	-21609	2142	-65067	16876188
1009	20	9	3	2	-14	4	9	893	3052
1009	20	9	3	2	101	-75	22	893	3052
1009	20	9	3	2	-806	-71	31	-893	3052
1027	13	11	4	3	-1	1	0	10	4
1027	13	11	4	3	-23	-1	1	-10	4
1027	13	11	4	3	-12	-2	1	10	4
1033	25	7	1	6	41	7	1	448	532
1033	25	7	1	6	66	-56	11	448	532
1033	25	7	1	6	-341	-49	12	-448	532
1039	28	5	3	4	-41	-1	22	4579	82108
1039	28	5	3	4	902	-939	131	4579	82108

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
1039	28	5	3	4	-3718	-940	153	-4579	82108
1057	14	11	9	2	-10	4	5	401	604
1057	14	11	9	2	-11	4	5	398	604
1057	14	11	9	2	16	-23	9	401	604
1057	14	11	9	2	15	-23	9	398	604
1057	14	11	9	2	-394	-19	14	-398	604
1057	14	11	9	2	-395	-19	14	-401	604
1063	31	1	0	0	1	1	0	34	4
1063	31	1	0	0	0	1	0	31	4
1063	31	1	0	0	-33	-31	1	-31	4
1063	31	1	0	0	-34	-31	1	-34	4
1063	31	1	0	0	-1	-32	1	34	4
1063	31	1	0	0	-2	-32	1	31	4
1099	29	5	0	3	-2	-1	3	625	1396
1099	29	5	0	3	141	-122	17	625	1396
1099	29	5	0	3	-486	-123	20	-625	1396
1099	22	9	2	0	-211	93	124	13813	695764
1099	22	9	2	0	1649	-1147	341	13813	695764
1099	22	9	2	0	-12375	-1054	465	-13813	695764
1123	16	11	8	0	-2961	739	885	71971	19431364
1123	16	11	8	0	3809	-4133	1624	71971	19431364
1123	16	11	8	0	-71123	-3394	2509	-71971	19431364
1129	32	1	0	0	1	1	0	35	4
1129	32	1	0	0	0	1	0	32	4
1129	32	1	0	0	-34	-32	1	-32	4
1129	32	1	0	0	-35	-32	1	-35	4
1129	32	1	0	0	-1	-33	1	35	4
1129	32	1	0	0	-2	-33	1	32	4
1141	-1	13	0	7	2	3	3	177	108
1141	-1	13	0	7	1	3	3	174	108
1141	-1	13	0	7	-1	-6	3	177	108
1141	-1	13	0	7	-2	-6	3	174	108
1141	-1	13	0	7	-175	-3	6	-174	108
1141	-1	13	0	7	-176	-3	6	-177	108
1143	27	7	0	4	-9	0	7	1086	4116
1143	27	7	0	4	-10	0	7	1083	4116
1143	27	7	0	4	201	-147	28	1086	4116
1143	27	7	0	4	200	-147	28	1083	4116
1143	27	7	0	4	-893	-147	35	-1083	4116
1143	27	7	0	4	-894	-147	35	-1086	4116
1143	0	13	6	6	0	1	1	60	12
1143	0	13	6	6	-1	1	1	57	12
1143	0	13	6	6	0	-2	1	60	12

p	m	q	sØ	s1	t	u	v	traza(δ)	4S(δ)/p
1143	0	13	6	6	-1	-2	1	57	12
1143	0	13	6	6	-59	-1	2	-57	12
1143	0	13	6	6	-60	-1	2	-60	12
1147	23	9	6	8	-9	-1	1	77	28
1147	23	9	6	8	10	-9	2	77	28
1147	23	9	6	8	-76	-10	3	-77	28
1147	1	13	12	5	-1	19	17	1070	3892
1147	1	13	12	5	-24	-36	19	1070	3892
1147	1	13	12	5	-1095	-17	36	-1070	3892
1153	2	13	5	4	-221	1094	971	60756	12807804
1153	2	13	5	4	-616	-2065	1094	60756	12807804
1153	2	13	5	4	-61593	-971	2065	-60756	12807804
1159	17	11	2	10	-11	0	7	632	1372
1159	17	11	2	10	-12	0	7	629	1372
1159	17	11	2	10	45	-49	14	632	1372
1159	17	11	2	10	44	-49	14	629	1372
1159	17	11	2	10	-597	-49	21	-629	1372
1159	17	11	2	10	-598	-49	21	-632	1372
1171	4	13	4	2	-32	87	70	4592	74236
1171	4	13	4	2	-58	-157	87	4592	74236
1171	4	13	4	2	-4682	-70	157	-4592	74236
1197	33	1	0	0	1	1	0	36	4
1197	33	1	0	0	0	1	0	33	4
1197	33	1	0	0	-35	-33	1	-33	4
1197	33	1	0	0	-36	-33	1	-36	4
1197	33	1	0	0	-1	-34	1	36	4
1197	33	1	0	0	-2	-34	1	33	4
1197	33	4	2	1	5	2	0	81	16
1197	33	4	2	1	-51	-16	2	-81	16
1197	33	4	2	1	25	-18	2	81	16
1197	18	11	7	9	-2	0	1	93	28
1197	18	11	7	9	-3	0	1	90	28
1197	18	11	7	9	7	-7	2	93	28
1197	18	11	7	9	6	-7	2	90	28
1197	18	11	7	9	-87	-7	3	-90	28
1197	18	11	7	9	-88	-7	3	-93	28
1197	6	13	3	0	-2	4	3	207	148
1197	6	13	3	0	-1	-7	4	207	148
1197	6	13	3	0	-210	-3	7	-207	148
1201	28	7	3	3	-212	10	129	20929	1444684
1201	28	7	3	3	3797	-2759	526	20929	1444684

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
1201	28	7	3	3	-17344	-2749	655	-20929	1444684
1213	7	13	9	12	-137	37	111	7840	202612
1213	7	13	9	12	-138	37	111	7837	202612
1213	7	13	9	12	11	-407	148	7840	202612
1213	7	13	9	12	10	-407	148	7837	202612
1213	7	13	9	12	-7965	-370	259	-7837	202612
1213	7	13	9	12	-7966	-370	259	-7840	202612
1231	8	13	2	11	-31	3	47	3315	28236
1231	8	13	2	11	297	-147	50	3315	28236
1231	8	13	2	11	-3049	-144	97	-3315	28236
1237	19	11	1	8	-94	7	60	5851	109396
1237	19	11	1	8	510	-441	127	5851	109396
1237	19	11	1	8	-5435	-434	187	-5851	109396
1249	25	9	5	6	-3791	42	1790	229537	168725296
1249	25	9	5	6	30093	-23438	5412	229537	168725296
1249	25	9	5	6	-203235	-23396	7202	-229537	168725296
1251	9	13	8	10	-49	2	0	-129	16
1251	9	13	8	10	-1	-2	2	129	16
1251	9	13	8	10	-81	-4	2	-129	16
1261	29	7	6	2	-19	2	8	1369	5968
1261	29	7	6	2	239	-178	34	1369	5968
1261	29	7	6	2	-1149	-176	42	-1369	5968
1267	34	1	0	0	1	1	0	37	4
1267	34	1	0	0	0	1	0	34	4
1267	34	1	0	0	-36	-34	1	-34	4
1267	34	1	0	0	-37	-34	1	-37	4
1267	34	1	0	0	-1	-35	1	37	4
1267	34	1	0	0	-2	-35	1	34	4
1273	10	13	1	9	-1	1	2	157	76
1273	10	13	1	9	-2	1	2	154	76
1273	10	13	1	9	4	-8	3	157	76
1273	10	13	1	9	3	-8	3	154	76
1273	10	13	1	9	-153	-7	5	-154	76
1273	10	13	1	9	-154	-7	5	-157	76
1279	20	11	6	7	-16	9	1	236	532
1279	20	11	6	7	-76	-34	11	236	532
1279	20	11	6	7	-328	-25	12	-236	532
1291	32	5	1	0	7	18	20	5417	88816
1291	32	5	1	0	1237	-986	138	5417	88816
1291	32	5	1	0	-4173	-968	158	-5417	88816
1297	11	13	7	8	-205	122	93	7981	299476

p	m	q	sØ	s1	t	u	v	traza(δ)	4S(δ)/p
1297	11	13	7	8	-1012	-523	215	7981	299476
1297	11	13	7	8	-9198	-401	308	-7981	299476
1333	35	4	2	3	-141	-48	94	30985	2882608
1333	35	4	2	3	10893	-8074	798	30985	2882608
1333	35	4	2	3	-20233	-8122	892	-30985	2882608
1339	35	1	0	0	1	1	0	38	4
1339	35	1	0	0	0	1	0	35	4
1339	35	1	0	0	-37	-35	1	-35	4
1339	35	1	0	0	-38	-35	1	-38	4
1339	35	1	0	0	-1	-36	1	38	4
1339	35	1	0	0	-2	-36	1	35	4
1351	13	13	6	6	-19	6	10	831	2064
1351	13	13	6	6	27	-42	16	831	2064
1351	13	13	6	6	-823	-36	26	-831	2064
1359	33	5	3	4	-32	-7	14	3621	39004
1359	33	5	3	4	815	-742	91	3621	39004
1359	33	5	3	4	-2838	-749	105	-3621	39004
1381	14	13	12	5	-324	98	147	12748	470596
1381	14	13	12	5	-325	98	147	12745	470596
1381	14	13	12	5	362	-637	245	12748	470596
1381	14	13	12	5	361	-637	245	12745	470596
1381	14	13	12	5	-12709	-539	392	-12745	470596
1381	14	13	12	5	-12710	-539	392	-12748	470596
1387	31	7	5	0	-34	11	13	2579	19828
1387	31	7	5	0	469	-328	63	2579	19828
1387	31	7	5	0	-2144	-317	76	-2579	19828
1393	35	3	0	2	-2	-2	5	2269	14716
1393	35	3	0	2	544	-759	58	2269	14716
1393	35	3	0	2	-1727	-761	63	-2269	14716
1413	36	1	0	0	1	1	0	39	4
1413	36	1	0	0	0	1	0	36	4
1413	36	1	0	0	-38	-36	1	-36	4
1413	36	1	0	0	-39	-36	1	-39	4
1413	36	1	0	0	-1	-37	1	39	4
1413	36	1	0	0	-2	-37	1	36	4
1413	15	13	5	4	4	-4	1	36	28
1413	15	13	5	4	-39	-1	2	36	28
1413	15	13	5	4	-71	-5	3	-36	28
1417	28	9	8	3	-27	3	11	1609	7252
1417	28	9	8	3	231	-155	36	1609	7252
1417	28	9	8	3	-1405	-152	47	-1609	7252

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
1417	23	11	10	4	-11	2	4	465	624
1417	23	11	10	4	39	-34	10	465	624
1417	23	11	10	4	-437	-32	14	-465	624
1429	34	5	0	3	-106	-14	105	29446	2426284
1429	34	5	0	3	7160	-5873	721	29446	2426284
1429	34	5	0	3	-22392	-5887	826	-29446	2426284
1447	16	13	11	3	25623	-2351	589	90496	9654988
1447	16	13	11	3	-737	-584	1173	90496	9654988
1447	16	13	11	3	-65610	-2935	1762	-90496	9654988
1453	32	7	1	6	-9	-8	11	2082	11388
1453	32	7	1	6	451	-293	47	2082	11388
1453	32	7	1	6	-1640	-301	58	-2082	11388
1459	28	10	0	2	-79	20	28	3935	45616
1459	28	10	0	2	643	-343	90	3935	45616
1459	28	10	0	2	-3371	-323	118	-3935	45616
1467	24	11	4	3	-55	13	26	3111	26364
1467	24	11	4	3	-56	13	26	3108	26364
1467	24	11	4	3	335	-221	65	3111	26364
1467	24	11	4	3	334	-221	65	3108	26364
1467	24	11	4	3	-2830	-208	91	-3108	26364
1467	24	11	4	3	-2831	-208	91	-3111	26364
1477	29	9	3	2	-248	-9	35	4175	55204
1477	29	9	3	2	706	-419	96	4175	55204
1477	29	9	3	2	-3717	-428	131	-4175	55204
1483	17	13	4	2	-29	14	14	1369	5488
1483	17	13	4	2	41	-70	28	1369	5488
1483	17	13	4	2	-1357	-56	42	-1369	5488
1489	37	1	0	0	1	1	0	40	4
1489	37	1	0	0	0	1	0	37	4
1489	37	1	0	0	-39	-37	1	-37	4
1489	37	1	0	0	-40	-37	1	-40	4
1489	37	1	0	0	-1	-38	1	40	4
1489	37	1	0	0	-2	-38	1	37	4
1501	35	5	2	2	-4	0	3	879	2052
1501	35	5	2	2	-5	0	3	876	2052
1501	35	5	2	2	209	-171	21	879	2052
1501	35	5	2	2	208	-171	21	876	2052
1501	35	5	2	2	-673	-171	24	-876	2052
1501	35	5	2	2	-674	-171	24	-879	2052
1561	19	13	3	0	-1	1	1	106	28
1561	19	13	3	0	-2	1	1	103	28
1561	19	13	3	0	7	-5	2	106	28

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
1561	19	13	3	0	6	-5	2	103	28
1561	19	13	3	0	-99	-4	3	-103	28
1561	19	13	3	0	-100	-4	3	-106	28
1561	5	15	12	2	-21	24	19	1444	5572
1561	5	15	12	2	-31	-43	24	1444	5572
1561	5	15	12	2	-1496	-19	43	-1444	5572
1567	38	1	0	0	1	1	0	41	4
1567	38	1	0	0	0	1	0	38	4
1567	38	1	0	0	-40	-38	1	-38	4
1567	38	1	0	0	-41	-38	1	-41	4
1567	38	1	0	0	-1	-39	1	41	4
1567	38	1	0	0	-2	-39	1	38	4
1591	34	7	0	4	-30	-1	21	4622	53764
1591	34	7	0	4	1016	-645	104	4622	53764
1591	34	7	0	4	-3636	-646	125	-4622	53764
1591	7	15	11	0	-3784	654	627	39624	4923612
1591	7	15	11	0	65	-1281	654	39624	4923612
1591	7	15	11	0	-43343	-627	1281	-39624	4923612
1603	31	9	2	0	-11562	86	57	-23185	335788
1603	31	9	2	0	-9795	-1085	257	-23185	335788
1603	31	9	2	0	1828	-999	314	23185	335788
1603	20	13	9	12	-16	0	7	743	1372
1603	20	13	9	12	-17	0	7	740	1372
1603	20	13	9	12	47	-49	14	743	1372
1603	20	13	9	12	46	-49	14	740	1372
1603	20	13	9	12	-711	-49	21	-740	1372
1603	20	13	9	12	-712	-49	21	-743	1372
1629	27	11	8	0	-18	5	7	942	2172
1629	27	11	8	0	-19	5	7	939	2172
1629	27	11	8	0	111	-64	19	942	2172
1629	27	11	8	0	110	-64	19	939	2172
1629	27	11	8	0	-848	-59	26	-939	2172
1629	27	11	8	0	-849	-59	26	-942	2172
1651	37	5	1	0	154	-114	11	-324	4332
1651	37	5	1	0	-703	-171	26	-324	4332
1651	37	5	1	0	-225	-285	37	324	4332
1651	10	15	2	12	-810	277	786	66364	10333132
1651	10	15	2	12	2064	-2912	1063	66364	10333132
1651	10	15	2	12	-65110	-2635	1849	-66364	10333132
1669	32	9	6	8	4022	545	138	56002	5495356
1669	32	9	6	8	8438	-5623	1097	56002	5495356
1669	32	9	6	8	-43542	-5078	1235	-56002	5495356

p	m	q	sØ	s1	t	u	v	traza(δ)	4S(δ)/p
1687	28	11	2	10	-5	0	2	289	208
1687	28	11	2	10	35	-26	6	289	208
1687	28	11	2	10	-259	-26	8	-289	208
1693	22	13	8	10	-53	18	9	1299	6804
1693	22	13	8	10	-125	-117	36	1299	6804
1693	22	13	8	10	-1477	-99	45	-1299	6804
1729	40	1	0	0	1	1	0	43	4
1729	40	1	0	0	0	1	0	40	4
1729	40	1	0	0	-42	-40	1	-40	4
1729	40	1	0	0	-43	-40	1	-43	4
1729	40	1	0	0	-1	-41	1	43	4
1729	40	1	0	0	-2	-41	1	40	4
1729	38	5	3	4	-4	-1	1	309	228
1729	38	5	3	4	76	-64	7	309	228
1729	38	5	3	4	-237	-65	8	-309	228
1729	13	15	8	9	-22	8	11	1028	2764
1729	13	15	8	9	-15	-49	19	1028	2764
1729	13	15	8	9	-1065	-41	30	-1028	2764
1729	1	16	8	7	-633	10	8	-1297	976
1729	1	16	8	7	-673	-18	10	-1297	976
1729	1	16	8	7	-9	-8	18	1297	976
1737	36	7	6	2	-383	-57	23	2319	20908
1737	36	7	6	2	585	-371	58	2319	20908
1737	36	7	6	2	-2117	-428	81	-2319	20908
1747	29	11	7	9	-37	0	27	4128	37908
1747	29	11	7	9	530	-351	81	4128	37908
1747	29	11	7	9	-3635	-351	108	-4128	37908
1777	7	16	8	1	5	-8	2	113	208
1777	7	16	8	1	-121	2	6	113	208
1777	7	16	8	1	-229	-6	8	-113	208
1791	24	13	7	8	-16	0	3	321	252
1791	24	13	7	8	29	-21	6	321	252
1791	24	13	7	8	-308	-21	9	-321	252
1807	34	9	5	6	-444	-19	189	36011	2872732
1807	34	9	5	6	6530	-3874	737	36011	2872732
1807	34	9	5	6	-29925	-3893	926	-36011	2872732
1843	25	13	0	7	-4	1	3	385	316
1843	25	13	0	7	39	-24	7	385	316
1843	25	13	0	7	-350	-23	10	-385	316
1879	35	9	0	5	-37	0	21	4173	37044

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
1879	35	9	0	5	-38	0	21	4170	37044
1879	35	9	0	5	824	-441	84	4173	37044
1879	35	9	0	5	823	-441	84	4170	37044
1879	35	9	0	5	-3385	-441	105	-4170	37044
1879	35	9	0	5	-3386	-441	105	-4173	37044
1891	40	5	2	2	-49	2	33	12341	322492
1891	40	5	2	2	3135	-2427	266	12341	322492
1891	40	5	2	2	-9255	-2425	299	-12341	322492
1891	38	7	5	0	-7	3	1	344	292
1891	38	7	5	0	66	-49	8	344	292
1891	38	7	5	0	-285	-46	9	-344	292
1897	26	13	6	6	-217	33	93	12111	307908
1897	26	13	6	6	1193	-750	219	12111	307908
1897	26	13	6	6	-11135	-717	312	-12111	307908
1899	42	1	0	0	1	1	0	45	4
1899	42	1	0	0	0	1	0	42	4
1899	42	1	0	0	-44	-42	1	-42	4
1899	42	1	0	0	-45	-42	1	-45	4
1899	42	1	0	0	-1	-43	1	45	4
1899	42	1	0	0	-2	-43	1	42	4
1939	32	11	0	6	-31	-1	7	1037	2356
1939	32	11	0	6	167	-87	20	1037	2356
1939	32	11	0	6	-901	-88	27	-1037	2356
1939	19	15	5	3	-11922	4100	5283	565151	662084668
1939	19	15	5	3	31055	-24049	9383	565151	662084668
1939	19	15	5	3	-546018	-19949	14666	-565151	662084668
1951	-1	17	0	9	2	3	3	231	108
1951	-1	17	0	9	1	3	3	228	108
1951	-1	17	0	9	-1	-6	3	231	108
1951	-1	17	0	9	-2	-6	3	228	108
1951	-1	17	0	9	-229	-3	6	-228	108
1951	-1	17	0	9	-230	-3	6	-231	108
1953	27	13	12	5	-8	0	1	108	28
1953	27	13	12	5	11	-7	2	108	28
1953	27	13	12	5	-105	-7	3	-108	28
1953	15	16	8	9	-1159	698	24	9297	2156752
1953	15	16	8	9	-12665	-1468	722	9297	2156752
1953	15	16	8	9	-23121	-770	746	-9297	2156752
1953	0	17	8	8	0	1	1	78	12
1953	0	17	8	8	-1	1	1	75	12
1953	0	17	8	8	0	-2	1	78	12
1953	0	17	8	8	-1	-2	1	75	12

p	m	q	sØ	s1	t	u	v	traza(δ)	4S(δ)/p
1953	0	17	8	8	-77	-1	2	-75	12
1953	0	17	8	8	-78	-1	2	-78	12
1957	43	4	2	3	-67	-28	2	-377	112
1957	43	4	2	3	-209	-42	4	-377	112
1957	43	4	2	3	101	-70	6	377	112
1957	1	17	16	7	-1	7	3	244	316
1957	1	17	16	7	-102	-10	7	244	316
1957	1	17	16	7	-347	-3	10	-244	316
1963	2	17	7	6	-5	22	20	1609	5296
1963	2	17	7	6	-15	-42	22	1609	5296
1963	2	17	7	6	-1629	-20	42	-1609	5296
1981	20	15	12	2	-6437	295	696	57581	8624932
1981	20	15	12	2	3353	-2678	991	57581	8624932
1981	20	15	12	2	-60665	-2383	1687	-57581	8624932
1981	4	17	6	4	0	-7	2	132	156
1981	4	17	6	4	-92	2	5	132	156
1981	4	17	6	4	-224	-5	7	-132	156
1987	43	1	0	0	1	1	0	46	4
1987	43	1	0	0	0	1	0	43	4
1987	43	1	0	0	-45	-43	1	-43	4
1987	43	1	0	0	-46	-43	1	-46	4
1987	43	1	0	0	-1	-44	1	46	4
1987	43	1	0	0	-2	-44	1	43	4
2007	33	11	5	5	-93	6	35	5904	69724
2007	33	11	5	5	910	-479	111	5904	69724
2007	33	11	5	5	-5087	-473	146	-5904	69724
2007	6	17	5	2	-26	55	45	3897	30100
2007	6	17	5	2	14	-100	55	3897	30100
2007	6	17	5	2	-3909	-45	100	-3897	30100
2011	28	13	5	4	-1145	214	460	63737	8076784
2011	28	13	5	4	7017	-3862	1134	63737	8076784
2011	28	13	5	4	-57865	-3648	1594	-63737	8076784
2041	43	3	2	0	-68	23	56	37801	2798308
2041	43	3	2	0	9099	-12161	807	37801	2798308
2041	43	3	2	0	-28770	-12138	863	-37801	2798308
2041	8	17	4	0	-12	14	11	978	1884
2041	8	17	4	0	10	-25	14	978	1884
2041	8	17	4	0	-980	-11	25	-978	1884
2053	40	7	4	5	-2739	-302	1320	378343	279328336
2053	40	7	4	5	87849	-54646	7618	378343	279328336

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
2053	40	7	4	5	-293233	-54948	8938	-378343	279328336
2061	42	5	1	0	-176	60	139	56619	6223252
2061	42	5	1	0	14959	-10687	1172	56619	6223252
2061	42	5	1	0	-41836	-10627	1311	-56619	6223252
2061	9	17	12	16	-104	1	15	1092	2884
2061	9	17	12	16	9	-47	16	1092	2884
2061	9	17	12	16	-1187	-46	31	-1092	2884
2071	29	13	11	3	-10	2	3	439	388
2071	29	13	11	3	42	-27	8	439	388
2071	29	13	11	3	-407	-25	11	-439	388
2077	44	1	0	0	1	1	0	47	4
2077	44	1	0	0	0	1	0	44	4
2077	44	1	0	0	-46	-44	1	-44	4
2077	44	1	0	0	-47	-44	1	-47	4
2077	44	1	0	0	-1	-45	1	47	4
2077	44	1	0	0	-2	-45	1	44	4
2077	34	11	10	4	22	-11	2	44	76
2077	34	11	10	4	-82	-7	3	44	76
2077	34	11	10	4	-104	-18	5	-44	76
2083	10	17	3	15	-131	27	83	7596	112476
2083	10	17	3	15	132	-303	110	7596	112476
2083	10	17	3	15	-7595	-276	193	-7596	112476
2119	38	10	0	2	-29	9	2	649	1168
2119	38	10	0	2	103	-74	16	649	1168
2119	38	10	0	2	-575	-65	18	-649	1168
2131	44	3	0	2	-830	-284	1397	988060	1832476948
2131	44	3	0	2	253378	-332133	20671	988060	1832476948
2131	44	3	0	2	-735512	-332417	22068	-988060	1832476948
2149	43	5	3	4	-54	-15	1	-361	124
2149	43	5	3	4	-233	-44	5	-361	124
2149	43	5	3	4	74	-59	6	361	124
2149	35	11	4	3	-9	3	1	256	172
2149	35	11	4	3	21	-25	6	256	172
2149	35	11	4	3	-244	-22	7	-256	172
2161	13	17	10	12	-89	56	21	2540	31948
2161	13	17	10	12	-936	-175	77	2540	31948
2161	13	17	10	12	-3565	-119	98	-2540	31948
2169	45	1	0	0	1	1	0	48	4
2169	45	1	0	0	0	1	0	45	4
2169	45	1	0	0	-47	-45	1	-45	4

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
2169	45	1	0	0	-48	-45	1	-48	4
2169	45	1	0	0	-1	-46	1	48	4
2169	45	1	0	0	-2	-46	1	45	4
2191	14	17	1	11	-5	2	3	310	196
2191	14	17	1	11	-1	-13	5	310	196
2191	14	17	1	11	-316	-11	8	-310	196
2223	42	7	3	3	-2	1	0	36	4
2223	42	7	3	3	-33	-6	1	-36	4
2223	42	7	3	3	5	-7	1	36	4
2223	36	11	9	2	-9	2	4	777	1072
2223	36	11	9	2	125	-60	14	777	1072
2223	36	11	9	2	-661	-58	18	-777	1072
2223	15	17	9	10	-4	1	2	207	76
2223	15	17	9	10	-5	1	2	204	76
2223	15	17	9	10	7	-8	3	207	76
2223	15	17	9	10	6	-8	3	204	76
2223	15	17	9	10	-203	-7	5	-204	76
2223	15	17	9	10	-204	-7	5	-207	76
2257	16	17	0	9	1784	123	52	12624	169716
2257	16	17	0	9	402	-402	175	12624	169716
2257	16	17	0	9	-10438	-279	227	-12624	169716
2263	46	1	0	0	1	1	0	49	4
2263	46	1	0	0	0	1	0	46	4
2263	46	1	0	0	-48	-46	1	-46	4
2263	46	1	0	0	-49	-46	1	-49	4
2263	46	1	0	0	-1	-47	1	49	4
2263	46	1	0	0	-2	-47	1	46	4
2263	32	13	3	0	5	-2	0	-49	16
2263	32	13	3	0	-69	-4	2	-49	16
2263	32	13	3	0	-15	-6	2	49	16
2293	17	17	8	8	-191	51	91	9849	165468
2293	17	17	8	8	438	-375	142	9849	165468
2293	17	17	8	8	-9602	-324	233	-9849	165468
2311	43	7	6	2	-32	-5	2	335	268
2311	43	7	6	2	89	-51	7	335	268
2311	43	7	6	2	-278	-56	9	-335	268
2317	46	3	2	0	-5262	-1243	1116	766268	1034788468
2317	46	3	2	0	189884	-249068	15497	766268	1034788468
2317	46	3	2	0	-581646	-250311	16613	-766268	1034788468
2317	47	4	2	3	64289	-42618	2932	-30455	168257968
2317	47	4	2	3	-120615	-51092	4502	-30455	168257968

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
2317	47	4	2	3	-25871	-93710	7434	30455	168257968
2331	45	5	2	2	-3	2	0	81	16
2331	45	5	2	2	-67	-18	2	-81	16
2331	45	5	2	2	17	-20	2	81	16
2331	33	13	9	12	-1	-1	1	144	28
2331	33	13	9	12	27	-9	2	144	28
2331	33	13	9	12	-118	-10	3	-144	28
2331	18	17	16	7	-5	1	2	219	76
2331	18	17	16	7	13	-8	3	219	76
2331	18	17	16	7	-211	-7	5	-219	76
2353	41	9	6	8	-32	-5	19	4924	40684
2353	41	9	6	8	1031	-559	90	4924	40684
2353	41	9	6	8	-3925	-564	109	-4924	40684
2359	47	1	0	0	1	1	0	50	4
2359	47	1	0	0	0	1	0	47	4
2359	47	1	0	0	-49	-47	1	-47	4
2359	47	1	0	0	-50	-47	1	-50	4
2359	47	1	0	0	-1	-48	1	50	4
2359	47	1	0	0	-2	-48	1	47	4
2371	19	17	7	6	-11292	3368	4981	568064	544410124
2371	19	17	7	6	26091	-21679	8349	568064	544410124
2371	19	17	7	6	-553265	-18311	13330	-568064	544410124
2377	38	11	8	0	-255	50	93	18805	589948
2377	38	11	8	0	3279	-1409	329	18805	589948
2377	38	11	8	0	-15781	-1359	422	-18805	589948
2413	47	3	0	2	-25	-10	43	34414	1962748
2413	47	3	0	2	8981	-11569	678	34414	1962748
2413	47	3	0	2	-25458	-11579	721	-34414	1962748
2413	20	17	15	5	-71	17	24	2791	12964
2413	20	17	15	5	120	-106	41	2791	12964
2413	20	17	15	5	-2742	-89	65	-2791	12964
2437	-1	19	0	10	2	3	3	258	108
2437	-1	19	0	10	1	3	3	255	108
2437	-1	19	0	10	-1	-6	3	258	108
2437	-1	19	0	10	-2	-6	3	255	108
2437	-1	19	0	10	-256	-3	6	-255	108
2437	-1	19	0	10	-257	-3	6	-258	108
2439	0	19	9	9	0	1	1	87	12
2439	0	19	9	9	-1	1	1	84	12
2439	0	19	9	9	0	-2	1	87	12
2439	0	19	9	9	-1	-2	1	84	12

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
2439	0	19	9	9	-86	-1	2	-84	12
2439	0	19	9	9	-87	-1	2	-87	12
2443	1	19	18	8	-27	38	36	3161	16432
2443	1	19	18	8	-49	-74	38	3161	16432
2443	1	19	18	8	-3237	-36	74	-3161	16432
2449	2	19	8	7	-8	34	31	2772	12684
2449	2	19	8	7	-30	-65	34	2772	12684
2449	2	19	8	7	-2810	-31	65	-2772	12684
2479	5	19	16	4	35	-3	1	181	28
2479	5	19	16	4	-2	1	2	181	28
2479	5	19	16	4	-148	-2	3	-181	28
2493	45	7	5	0	-514	101	232	80955	10516996
2493	45	7	5	0	20014	-10683	1493	80955	10516996
2493	45	7	5	0	-61455	-10582	1725	-80955	10516996
2493	6	19	6	3	-1113	1736	1458	138297	30682192
2493	6	19	6	3	407	-3194	1736	138297	30682192
2493	6	19	6	3	-139003	-1458	3194	-138297	30682192
2503	22	17	14	3	-446	123	152	18696	562116
2503	22	17	14	3	930	-702	275	18696	562116
2503	22	17	14	3	-18212	-579	427	-18696	562116
2509	7	19	15	2	-3	3	2	196	76
2509	7	19	15	2	-15	-5	3	196	76
2509	7	19	15	2	-214	-2	5	-196	76
2521	47	5	1	0	17045	5065	313	440682	258763836
2521	47	5	1	0	115015	-79133	7882	440682	258763836
2521	47	5	1	0	-308622	-74068	8195	-440682	258763836
2539	40	11	7	9	-3390	-301	1204	263138	109083604
2539	40	11	7	9	-3391	-301	1204	263135	109083604
2539	40	11	7	9	48081	-23779	4515	263138	109083604
2539	40	11	7	9	48080	-23779	4515	263135	109083604
2539	40	11	7	9	-218446	-24080	5719	-263135	109083604
2539	40	11	7	9	-218447	-24080	5719	-263138	109083604
2547	36	13	1	9	-2187	-24	889	160596	40501588
2547	36	13	1	9	24555	-11461	2643	160596	40501588
2547	36	13	1	9	-138228	-11485	3532	-160596	40501588
2547	9	19	14	0	45	-146	66	4959	64144
2547	9	19	14	0	-1025	66	80	4959	64144
2547	9	19	14	0	-5939	-80	146	-4959	64144
2557	49	1	0	0	1	1	0	52	4
2557	49	1	0	0	0	1	0	49	4

p	m	q	sØ	s1	t	u	v	traza(δ)	4S(δ)/p
2557	49	1	0	0	-51	-49	1	-49	4
2557	49	1	0	0	-52	-49	1	-52	4
2557	49	1	0	0	-1	-50	1	52	4
2557	49	1	0	0	-2	-50	1	49	4
2569	10	19	4	18	-21	10	14	1465	4432
2569	10	19	4	18	-121	-62	24	1465	4432
2569	10	19	4	18	-1607	-52	38	-1465	4432
2587	46	7	1	6	-3	-1	2	719	796
2587	46	7	1	6	-4	-1	2	716	796
2587	46	7	1	6	188	-106	13	719	796
2587	46	7	1	6	187	-106	13	716	796
2587	46	7	1	6	-533	-107	15	-716	796
2587	46	7	1	6	-534	-107	15	-719	796
2623	41	11	1	8	-109	37	3	1910	10228
2623	41	11	1	8	106	-248	49	1910	10228
2623	41	11	1	8	-1913	-211	52	-1910	10228
2623	37	13	7	8	-371	4	123	22897	800548
2623	37	13	7	8	3430	-1615	373	22897	800548
2623	37	13	7	8	-19838	-1611	496	-22897	800548
2641	47	8	4	5	-4757	-814	464	106623	20041104
2641	47	8	4	5	33617	-14254	1970	106623	20041104
2641	47	8	4	5	-77763	-15068	2434	-106623	20041104
2647	13	19	12	15	-877	207	509	55032	4544724
2647	13	19	12	15	979	-1941	716	55032	4544724
2647	13	19	12	15	-54930	-1734	1225	-55032	4544724
2653	25	17	4	0	-118	43	47	6220	58156
2653	25	17	4	0	455	-227	90	6220	58156
2653	25	17	4	0	-5883	-184	137	-6220	58156
2659	50	1	0	0	1	1	0	53	4
2659	50	1	0	0	0	1	0	50	4
2659	50	1	0	0	-52	-50	1	-50	4
2659	50	1	0	0	-53	-50	1	-53	4
2659	50	1	0	0	-1	-51	1	53	4
2659	50	1	0	0	-2	-51	1	50	4
2677	14	19	2	14	-658	168	397	43254	2804556
2677	14	19	2	14	1204	-1527	565	43254	2804556
2677	14	19	2	14	-42708	-1359	962	-43254	2804556
2701	38	13	0	7	-22	-1	3	484	388
2701	38	13	0	7	82	-35	8	484	388
2701	38	13	0	7	-424	-36	11	-484	388
2709	51	4	2	3	-5	0	2	1401	2928

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
2709	51	4	2	3	553	-366	26	1401	2928
2709	51	4	2	3	-853	-366	28	-1401	2928
2709	42	11	6	7	-2	0	1	240	84
2709	42	11	6	7	-3	0	1	237	84
2709	42	11	6	7	46	-21	4	240	84
2709	42	11	6	7	45	-21	4	237	84
2709	42	11	6	7	-195	-21	5	-237	84
2709	42	11	6	7	-196	-21	5	-240	84
2709	15	19	11	13	-32	7	15	1674	4156
2709	15	19	11	13	39	-59	22	1674	4156
2709	15	19	11	13	-1667	-52	37	-1674	4156
2743	16	19	1	12	168	-125	4	-1052	56692
2743	16	19	1	12	-4077	-113	117	-1052	56692
2743	16	19	1	12	-2857	-238	121	1052	56692
2763	51	1	0	0	1	1	0	54	4
2763	51	1	0	0	0	1	0	51	4
2763	51	1	0	0	-53	-51	1	-51	4
2763	51	1	0	0	-54	-51	1	-54	4
2763	51	1	0	0	-1	-52	1	54	4
2763	51	1	0	0	-2	-52	1	51	4
2763	27	17	3	15	-18	0	7	975	1372
2763	27	17	3	15	-19	0	7	972	1372
2763	27	17	3	15	80	-49	14	975	1372
2763	27	17	3	15	79	-49	14	972	1372
2763	27	17	3	15	-912	-49	21	-972	1372
2763	27	17	3	15	-913	-49	21	-975	1372
2779	17	19	10	11	-20	6	11	1296	2388
2779	17	19	10	11	41	-45	17	1296	2388
2779	17	19	10	11	-1275	-39	28	-1296	2388
2797	43	11	0	6	-46	0	21	5091	37044
2797	43	11	0	6	-47	0	21	5088	37044
2797	43	11	0	6	1046	-441	84	5091	37044
2797	43	11	0	6	1045	-441	84	5088	37044
2797	43	11	0	6	-4090	-441	105	-5088	37044
2797	43	11	0	6	-4091	-441	105	-5091	37044
2817	33	16	8	7	-5	0	2	297	112
2817	33	16	8	7	45	-14	4	297	112
2817	33	16	8	7	-257	-14	6	-297	112
2817	18	19	0	10	-23	14	1	297	964
2817	18	19	0	10	-285	-31	15	297	964
2817	18	19	0	10	-605	-17	16	-297	964

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
2821	50	5	2	2	7	2	0	121	16
2821	50	5	2	2	-83	-20	2	-121	16
2821	50	5	2	2	31	-22	2	121	16
2821	28	17	11	14	-3	0	1	142	28
2821	28	17	11	14	-4	0	1	139	28
2821	28	17	11	14	12	-7	2	142	28
2821	28	17	11	14	11	-7	2	139	28
2821	28	17	11	14	-132	-7	3	-139	28
2821	28	17	11	14	-133	-7	3	-142	28
2857	19	19	9	9	-175	54	60	7521	93744
2857	19	19	9	9	-115	-288	114	7521	93744
2857	19	19	9	9	-7811	-234	174	-7521	93744
2863	40	13	12	5	-14	2	3	656	652
2863	40	13	12	5	90	-47	11	656	652
2863	40	13	12	5	-580	-45	14	-656	652
2869	52	1	0	0	1	1	0	55	4
2869	52	1	0	0	0	1	0	52	4
2869	52	1	0	0	-54	-52	1	-52	4
2869	52	1	0	0	-55	-52	1	-55	4
2869	52	1	0	0	-1	-53	1	55	4
2869	52	1	0	0	-2	-53	1	52	4
2869	13	20	10	17	-9125	46	974	81337	11930224
2869	13	20	10	17	2433	-3014	1020	81337	11930224
2869	13	20	10	17	-88029	-2968	1994	-81337	11930224
2881	49	7	3	3	5	1	0	64	4
2881	49	7	3	3	-44	-7	1	-64	4
2881	49	7	3	3	15	-8	1	64	4
2881	29	17	2	13	-51	2	20	2945	12016
2881	29	17	2	13	265	-146	42	2945	12016
2881	29	17	2	13	-2731	-144	62	-2945	12016
2887	44	11	5	5	-112402	-10771	5544	602590	896157124
2887	44	11	5	5	149117	-62569	11405	602590	896157124
2887	44	11	5	5	-565875	-73340	16949	-602590	896157124
2899	47	9	3	2	-13	17	33	10924	160876
2899	47	9	3	2	2581	-1125	182	10924	160876
2899	47	9	3	2	-8356	-1108	215	-10924	160876
2899	20	19	18	8	-67	16	25	3119	13324
2899	20	19	18	8	113	-107	41	3119	13324
2899	20	19	18	8	-3073	-91	66	-3119	13324
2923	52	3	2	0	-147	-45	22	18163	463852
2923	52	3	2	0	4681	-5944	329	18163	463852

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
2923	52	3	2	0	-13629	-5989	351	-18163	463852
2923	40	14	0	2	-1069	166	368	70777	6857872
2923	40	14	0	2	12933	-4169	1086	70777	6857872
2923	40	14	0	2	-58913	-4003	1454	-70777	6857872
2947	41	13	5	4	-3	2	4	905	1072
2947	41	13	5	4	151	-60	14	905	1072
2947	41	13	5	4	-757	-58	18	-905	1072
2977	53	1	0	0	1	1	0	56	4
2977	53	1	0	0	0	1	0	53	4
2977	53	1	0	0	-55	-53	1	-53	4
2977	53	1	0	0	-56	-53	1	-56	4
2977	53	1	0	0	-1	-54	1	56	4
2977	53	1	0	0	-2	-54	1	53	4
2979	45	11	10	4	-267	14	84	21753	635824
2979	45	11	10	4	4311	-1834	350	21753	635824
2979	45	11	10	4	-17709	-1820	434	-21753	635824
2983	50	7	6	2	15	-9	2	435	156
2983	50	7	6	2	145	-42	5	435	156
2983	50	7	6	2	-275	-51	7	-435	156
3007	31	17	1	11	-353	27	128	19874	530788
3007	31	17	1	11	1910	-977	283	19874	530788
3007	31	17	1	11	-18317	-950	411	-19874	530788
3031	52	5	1	0	-80	23	61	36641	1772092
3031	52	5	1	0	10528	-7024	633	36641	1772092
3031	52	5	1	0	-26193	-7001	694	-36641	1772092
3033	42	13	11	3	-288	32	85	18585	455956
3033	42	13	11	3	3080	-1233	287	18585	455956
3033	42	13	11	3	-15793	-1201	372	-18585	455956
3037	23	19	7	5	-17	5	6	802	892
3037	23	19	7	5	31	-28	11	802	892
3037	23	19	7	5	-788	-23	17	-802	892
3073	46	11	4	3	-254	-18	21	3954	24732
3073	46	11	4	3	892	-351	66	3954	24732
3073	46	11	4	3	-3316	-369	87	-3954	24732
3073	32	17	9	10	-5	-1	3	436	196
3073	32	17	9	10	69	-18	5	436	196
3073	32	17	9	10	-372	-19	8	-436	196
3097	49	9	2	0	1737	-704	99	2296	131164
3097	49	9	2	0	-3565	-451	110	2296	131164
3097	49	9	2	0	-4124	-1155	209	-2296	131164

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
3097	37	16	8	3	12803	-3998	478	-30169	32112688
3097	37	16	8	3	-94581	-4650	2564	-30169	32112688
3097	37	16	8	3	-51609	-8648	3042	30169	32112688
3121	43	13	4	2	-3599	375	1007	221833	63866548
3121	43	13	4	2	39702	-14591	3396	221833	63866548
3121	43	13	4	2	-185730	-14216	4403	-221833	63866548
3139	53	5	3	4	-138	-39	11	4669	30988
3139	53	5	3	4	1368	-995	82	4669	30988
3139	53	5	3	4	-3439	-1034	93	-4669	30988
3139	25	19	6	3	-27	9	11	1530	2964
3139	25	19	6	3	95	-51	20	1530	2964
3139	25	19	6	3	-1462	-42	31	-1530	2964
3141	33	17	0	9	133	-55	11	366	3388
3141	33	17	0	9	-703	-33	22	366	3388
3141	33	17	0	9	-936	-88	33	-366	3388
3169	47	11	9	2	-1590	362	247	78934	8867836
3169	47	11	9	2	14431	-6997	1350	78934	8867836
3169	47	11	9	2	-66093	-6635	1597	-78934	8867836
3193	52	7	5	0	-31	6	13	5874	43356
3193	52	7	5	0	1569	-789	97	5874	43356
3193	52	7	5	0	-4336	-783	110	-5874	43356
3193	26	19	15	2	-44	1	0	-106	4
3193	26	19	15	2	1	-1	1	106	4
3193	26	19	15	2	-61	-2	1	-106	4
3241	53	8	4	7	-2707	-654	1120	444417	243765264
3241	53	8	4	7	141577	-58608	7186	444417	243765264
3241	53	8	4	7	-305547	-59262	8306	-444417	243765264
3303	45	13	3	0	-74	9	19	4401	23884
3303	45	13	3	0	828	-283	66	4401	23884
3303	45	13	3	0	-3647	-274	85	-4401	23884
3303	6	22	0	5	-2329	2860	2534	268641	87391984
3303	6	22	0	5	3095	-5394	2860	268641	87391984
3303	6	22	0	5	-267875	-2534	5394	-268641	87391984
3307	28	19	14	0	-821	249	190	29589	1248924
3307	28	19	14	0	515	-1068	439	29589	1248924
3307	28	19	14	0	-29895	-819	629	-29589	1248924
3313	56	1	0	0	1	1	0	59	4
3313	56	1	0	0	0	1	0	56	4
3313	56	1	0	0	-58	-56	1	-56	4
3313	56	1	0	0	-59	-56	1	-59	4

p	m	q	sØ	s1	t	u	v	traza(δ)	4S(δ)/p
3313	56	1	0	0	-1	-57	1	59	4
3313	56	1	0	0	-2	-57	1	56	4
3357	36	17	7	6	-31	3	8	1383	2308
3357	36	17	7	6	158	-65	19	1383	2308
3357	36	17	7	6	-1256	-62	27	-1383	2308
3367	56	3	0	2	227	-279	12	-1335	8532
3367	56	3	0	2	-1579	-729	39	-1335	8532
3367	56	3	0	2	-17	-1008	51	1335	8532
3367	49	11	8	0	-3	1	0	40	4
3367	49	11	8	0	-41	-4	1	-40	4
3367	49	11	8	0	2	-5	1	40	4
3367	29	19	4	18	-2	0	1	155	28
3367	29	19	4	18	-3	0	1	152	28
3367	29	19	4	18	12	-7	2	155	28
3367	29	19	4	18	11	-7	2	152	28
3367	29	19	4	18	-144	-7	3	-152	28
3367	29	19	4	18	-145	-7	3	-155	28
3397	46	13	9	12	-1411	-148	425	104984	12995716
3397	46	13	9	12	19266	-8185	1552	104984	12995716
3397	46	13	9	12	-87129	-8333	1977	-104984	12995716
3409	41	16	8	15	-393	-30	56	9743	119632
3409	41	16	8	15	1575	-608	138	9743	119632
3409	41	16	8	15	-8561	-638	194	-9743	119632
3411	54	7	4	5	-2182	-337	1033	495888	288372036
3411	54	7	4	5	136328	-72376	7927	495888	288372036
3411	54	7	4	5	-361742	-72713	8960	-495888	288372036
3469	50	11	2	10	3007	-1141	119	-8521	989212
3469	50	11	2	10	-16495	-2016	427	-8521	989212
3469	50	11	2	10	-4967	-3157	546	8521	989212
3493	47	13	2	11	-69	-5	23	5906	40396
3493	47	13	2	11	1140	-458	87	5906	40396
3493	47	13	2	11	-4835	-463	110	-5906	40396
3493	31	19	3	16	-24799	272	8429	1333249	2035494844
3493	31	19	3	16	114686	-59819	17130	1333249	2035494844
3493	31	19	3	16	-1243362	-59547	25559	-1333249	2035494844
3517	53	9	0	5	176	-109	51	14845	205828
3517	53	9	0	5	4339	-1430	197	14845	205828
3517	53	9	0	5	-10330	-1539	248	-14845	205828
3523	55	7	0	4	-53	-7	35	17341	341236
3523	55	7	0	4	4966	-2492	273	17341	341236

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
3523	55	7	0	4	-12428	-2499	308	-17341	341236
3547	58	1	0	0	1	1	0	61	4
3547	58	1	0	0	0	1	0	58	4
3547	58	1	0	0	-60	-58	1	-58	4
3547	58	1	0	0	-61	-58	1	-61	4
3547	58	1	0	0	-1	-59	1	61	4
3547	58	1	0	0	-2	-59	1	58	4
3571	-1	23	0	12	2	3	3	312	108
3571	-1	23	0	12	1	3	3	309	108
3571	-1	23	0	12	-1	-6	3	312	108
3571	-1	23	0	12	-2	-6	3	309	108
3571	-1	23	0	12	-310	-3	6	-309	108
3571	-1	23	0	12	-311	-3	6	-312	108
3573	0	23	11	11	0	1	1	105	12
3573	0	23	11	11	-1	1	1	102	12
3573	0	23	11	11	0	-2	1	105	12
3573	0	23	11	11	-1	-2	1	102	12
3573	0	23	11	11	-104	-1	2	-102	12
3573	0	23	11	11	-105	-1	2	-105	12
3601	4	23	9	7	-29	59	53	5820	37668
3601	4	23	9	7	-15	-112	59	5820	37668
3601	4	23	9	7	-5864	-53	112	-5820	37668
3613	5	23	20	6	-4534	4362	3849	427749	202524732
3613	5	23	20	6	-2218	-8211	4362	427749	202524732
3613	5	23	20	6	-434501	-3849	8211	-427749	202524732
3627	33	19	2	14	19	1	0	90	4
3627	33	19	2	14	-65	-2	1	-90	4
3627	33	19	2	14	6	-3	1	90	4
3627	6	23	8	5	-53	68	59	6621	48468
3627	6	23	8	5	13	-127	68	6621	48468
3627	6	23	8	5	-6661	-59	127	-6621	48468
3643	7	23	19	4	-3020	1833	1577	177241	34949836
3643	7	23	19	4	-173	-3410	1833	177241	34949836
3643	7	23	19	4	-180434	-1577	3410	-177241	34949836
3661	8	23	7	3	-68	78	65	7505	61516
3661	8	23	7	3	-69	78	65	7502	61516
3661	8	23	7	3	49	-143	78	7505	61516
3661	8	23	7	3	48	-143	78	7502	61516
3661	8	23	7	3	-7523	-65	143	-7502	61516
3661	8	23	7	3	-7524	-65	143	-7505	61516
3667	59	1	0	0	1	1	0	62	4
3667	59	1	0	0	0	1	0	59	4
3667	59	1	0	0	-61	-59	1	-59	4

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
3667	59	1	0	0	-62	-59	1	-62	4
3667	59	1	0	0	-1	-60	1	62	4
3667	59	1	0	0	-2	-60	1	59	4
3673	40	17	5	2	-2416	442	735	143467	22405156
3673	40	17	5	2	18745	-6471	1912	143467	22405156
3673	40	17	5	2	-127138	-6029	2647	-143467	22405156
3679	52	11	1	8	12	-7	3	701	388
3679	52	11	1	8	203	-51	8	701	388
3679	52	11	1	8	-486	-58	11	-701	388
3681	9	23	18	2	-516	332	273	31743	1101556
3681	9	23	18	2	112	-605	332	31743	1101556
3681	9	23	18	2	-32147	-273	605	-31743	1101556
3691	49	13	1	9	-1562	-79	566	152753	25325164
3691	49	13	1	9	31029	-11491	2185	152753	25325164
3691	49	13	1	9	-123286	-11570	2751	-152753	25325164
3727	11	23	17	0	-6	6	1	160	172
3727	11	23	17	0	-145	-7	6	160	172
3727	11	23	17	0	-311	-1	7	-160	172
3769	35	19	1	12	-21539	1350	7072	1227305	1598603152
3769	35	19	1	12	124917	-53554	15494	1227305	1598603152
3769	35	19	1	12	-1123927	-52204	22566	-1227305	1598603152
3781	13	23	16	21	-66	20	57	7244	54268
3781	13	23	16	21	95	-211	77	7244	54268
3781	13	23	16	21	-7215	-191	134	-7244	54268
3787	53	11	6	7	-718	-42	249	82770	7235028
3787	53	11	6	7	19157	-7467	1203	82770	7235028
3787	53	11	6	7	-64331	-7509	1452	-82770	7235028
3789	60	1	0	0	1	1	0	63	4
3789	60	1	0	0	0	1	0	60	4
3789	60	1	0	0	-62	-60	1	-60	4
3789	60	1	0	0	-63	-60	1	-63	4
3789	60	1	0	0	-1	-61	1	63	4
3789	60	1	0	0	-2	-61	1	60	4
3793	50	13	7	8	-1287	283	97	38516	2098948
3793	50	13	7	8	5285	-3452	671	38516	2098948
3793	50	13	7	8	-34518	-3169	768	-38516	2098948
3811	14	23	4	20	-5	1	3	377	148
3811	14	23	4	20	-6	1	3	374	148
3811	14	23	4	20	9	-11	4	377	148
3811	14	23	4	20	8	-11	4	374	148
3811	14	23	4	20	-372	-10	7	-374	148
3811	14	23	4	20	-373	-10	7	-377	148

p	m	q	sø	s1	t	u	v	traza(δ)	4S(δ)/p
3843	42	17	4	0	-14	0	1	144	28
3843	42	17	4	0	22	-7	2	144	28
3843	42	17	4	0	-136	-7	3	-144	28
3843	36	19	10	11	-29	2	8	1425	2128
3843	36	19	10	11	139	-62	18	1425	2128
3843	36	19	10	11	-1315	-60	26	-1425	2128
3843	15	23	15	19	-85	2	0	-225	16
3843	15	23	15	19	-1	-2	2	225	16
3843	15	23	15	19	-141	-4	2	-225	16
3897	54	11	0	6	-159	-13	31	9795	102108
3897	54	11	0	6	2403	-883	142	9795	102108
3897	54	11	0	6	-7551	-896	173	-9795	102108
3897	51	13	0	7	-18	0	7	2004	4116
3897	51	13	0	7	-19	0	7	2001	4116
3897	51	13	0	7	423	-147	28	2004	4116
3897	51	13	0	7	422	-147	28	2001	4116
3897	51	13	0	7	-1598	-147	35	-2001	4116
3897	51	13	0	7	-1599	-147	35	-2004	4116
3913	61	1	0	0	1	1	0	64	4
3913	61	1	0	0	0	1	0	61	4
3913	61	1	0	0	-63	-61	1	-61	4
3913	61	1	0	0	-64	-61	1	-64	4
3913	61	1	0	0	-1	-62	1	64	4
3913	61	1	0	0	-2	-62	1	61	4
3913	59	8	4	1	-37	-6	2	495	336
3913	59	8	4	1	183	-66	8	495	336
3913	59	8	4	1	-349	-72	10	-495	336
3913	17	23	14	17	-3	2	0	25	16
3913	17	23	14	17	-85	-2	2	-25	16
3913	17	23	14	17	-57	-4	2	25	16
3931	43	17	12	16	-6041	-400	1543	324196	107162548
3931	43	17	12	16	44192	-18459	4229	324196	107162548
3931	43	17	12	16	-286045	-18859	5772	-324196	107162548
3937	47	16	8	9	-12145	56	3162	718753	524879248
3937	47	16	8	9	130089	-41330	9542	718753	524879248
3937	47	16	8	9	-600809	-41274	12704	-718753	524879248
3951	60	5	2	2	-2225	-44	1515	1190565	1434743044
3951	60	5	2	2	354611	-237283	18136	1190565	1434743044
3951	60	5	2	2	-838179	-237327	19651	-1190565	1434743044
3951	18	23	2	16	54	-46	15	1314	2884
3951	18	23	2	16	-260	-1	16	1314	2884

p	m	q	sø	sl	t	u	v	traza(δ)	4S(δ)/p
3951	18	23	2	16	-1520	-47	31	-1314	2884
3991	59	7	5	0	-147	25	63	35558	1268548
3991	59	7	5	0	10094	-4824	529	35558	1268548
3991	59	7	5	0	-25611	-4799	592	-35558	1268548
3991	19	23	13	15	107	-5	1	361	52
3991	19	23	13	15	-2	-2	3	361	52
3991	19	23	13	15	-256	-7	4	-361	52
3997	38	19	9	9	169	-13	3	568	148
3997	38	19	9	9	6	-5	4	568	148
3997	38	19	9	9	-393	-18	7	-568	148

3.C. ANALISIS DE LA TABLA DE UNIDADES FUNDAMENTALES.

El estudio de un sistema fundamental de unidades es considerado, en general, un problema computacional; es decir, parece claro que no se puede determinar sistemas de unidades fundamentales en función de los coeficientes de un polinomio de definición. Ahora bien, un análisis minucioso de la tabla de unidades fundamentales dada por la tesis en el apartado anterior, nos lleva a considerar las siguientes familias infinitas de cuerpos cúbicos cíclicos :

U = ($K = Q(\theta)$: $Irr(\theta, Q) = x^3 - px + p$ siendo $p = 3^{\delta} p_1 \cdots p_r$ con $p_i \equiv 1 \ (3)$ primo distintos dos a dos, $\delta \in (0, 2)$, $4p - 27 \in Z^2$),

V = ($K = Q(\theta)$: $Irr(\theta, Q) = x^3 - px + pq$ siendo $p = p_1 \cdots p_r, p_i \equiv 1 \ (3)$ primo y distintos dos a dos, $q > 2$, $4p - 27q^2 = 1$),

W = ($K = Q(\theta)$: $Irr(\theta, Q) = x^3 - px + pq$ siendo $p = 9\, p_1 \cdots p_r$, $p_i \equiv 1 \ (3)$ primo y distintos dos a dos, $q > 2$, $4p - 27q^2 = 9$, $3 \nmid q$).

Nosotros obtenemos un sistema fundamental de unidades para los cuerpos cúbicos cíclicos pertenecientes a dichas familias. El sistema fundamental de unidades obtenido es

sugerido tras el análisis de la tabla de unidades fundamentales. La demostración de que en realidad es un sistema fundamental de unidades es realizada utilizando el teorema de Godwin. El haber computado todas las unidades de R distintas de ± 1 en las que se alcanza el mínimo de la función S de Godwin ha sido decisivo a la hora de analizar la tabla y obtener consecuencias.

Las buenas propiedades de los sistemas fundamentales de unidades que obtenemos para las familias V y W nos van a permitir dar un sencillo criterio sobre la paridad del número de clase. Dichos sistemas de unidades fundamentales también los utilizaremos al final del capítulo para estudiar el comportamiento del número de clase, de los cuerpos cúbicos cíclicos de las familias V y W, cuando el discriminante converge a $+\infty$.

De la bibliografía consultada, se desprende que la tabla que nosotros presentamos es la única que permite deducir consecuencias y abstraer resultados generales para determinadas familias infinitas.

Más aún, "traduciendo" a nuestro lenguaje la tabla de Gras, hemos observado determinadas relaciones generales en su tabla que él mismo parece haber sido incapaz de establecer. De hecho, su tabla 4 sólo se explica por este desconocimiento. En los comentarios a los teoremas 3.13, 3.14 y 3.15 estableceremos dichas relaciones.

Teorema 3.13. : Sea K cúbico cíclico de discriminante p^2. Supongamos q = 1,o sea,K = Q(θ) siendo Irr(θ,Q) = $x^3 - px + p$ Entonces :

(i) K es monogénico siendo $(1, \sigma, \sigma^2)$ base entera de K. ($\sigma = (m + \theta 1)/3$, $\theta 1 = (4p - 9\theta - 6\theta^2)/(4p - 27)^{1/2}$, $m = ((4p - 27)^{1/2} - 3)/2$).

(ii) (σ,σ') es un sistema fundamental de unidades de K (σ' es un conjugado de σ).

Demostración :

(i) Por el lema 3.4., $\sigma \in R$ y $disc(\sigma) = p^2 = disc(K)$. Por tanto, $(1, \sigma, \sigma^2)$ es base entera de K y K es monogénico. Además, $Irr(\sigma,Q) = x^3 - mx^2 + ((m^2 - p)/3)x + (3pm - m^3 - p(4p - 27)^{1/2})/27 = x^3 - mx^2 - (m + 3)x - 1$. Por tanto, σ es una unidad de R.

(ii) En este caso, y siguiendo la notación prefijada en el apartado anterior, se tiene $s\emptyset = s1 = 0$. Aplicando el apartado (ii) del teorema 3.8., tomando u = 1 y v = 0 se tiene que $4(S(\sigma)/p) = 4$. Luego $S(\sigma) = p$. Ahora bien, $S(\alpha) \in pZ^+$ para todo $\alpha \in R$ y $S(\beta) \neq 0$ si β es una unidad de R distinta de ± 1. Entonces, aplicando el teorema de Godwin, (σ,σ') es un sistema fundamental de unidades de K si p > 9. Y también lo es en los casos p = 7, 9 según lo demuestra E. Thomas [T].

c.q.d.

Ejemplos : p = 7, 9, 13, 19, 37, 63, 79, 97, 117, 139, 163, 217, 247, 279, 313, 349, 387, 427, 469, 559, 607, 657, 709,

763, 819, 877, 937, 1063, 1129, 1197, 1267, 1339, 1413, 1489, 1567, 1729, 1899, 1987, 2077, 2169, 2263, 2263, 2359, 2557, 2659, 2763, 2869, 2977, 3199, 3313, 3547, 3667, 3789, 3913.

La familia anterior U de cuerpos cúbicos cíclicos ha sido considerada, entre otros, por Harvey-Cohn [HC1], K. Uchida [U], E. Thomas [T], M.N. Gras [G3] y M. Watabe [Wi], siendo $i = 1,\ldots,6$. Dicha familia tiene las siguientes buenas propiedades : existe una unidad fundamental monogénica y que no es totalmente positiva. Hecho de gran importancia a la hora de formular teoremas sobre la paridad del número de clase, [HC1],[Wi] con $i = 4,5$.

Nota: Para los cuerpos cúbicos cíclicos de discriminante p^2 tales que $4p - 27 \in Z^2$ las trazas que M.N. Gras [G2] calcula son iguales a $((4p - 27)^{1/2} - 3)/2$ (véase su tabla 4).

Teorema 3.14. : Sea K cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos $q > 2$, $4p - 27q^2 = 1$. Entonces :

(i) K es monogénico y $(1, \theta, \theta^2)$ es base entera de K.

(ii) $\mu = 2 + 3\sigma + 3((\sigma^2 + ((q + 1)/2)\sigma)/q$ es una unidad de R. $(\sigma = (-1 + \theta 1)/3, \theta 1 = 4p - 9q\theta - 6\theta^2)$.

(iii) (μ,μ') es un sistema fundamental de unidades de K; $\mu' = -1 - 6\sigma + 3((\sigma^2 + ((q + 1)/2)\sigma)/q)$ es un conjugado de μ.

(iv) $Irr(\mu,Q) = x^3 - 3((1 + 9q)/2)x^2 + ((27q - 3)/2)x + 1$

(v) μ no es totalmente positiva.

Demostración :

(i) $disc(\theta) = 4p^3 - 27p^2q^2 = p^2(4p - 27q^2) = p^2 = disc(K)$.

Luego $(1, \theta, \theta^2)$ es base entera y K es monogénico.

(ii) $\mu = 2 + 3\sigma + 3((\sigma^2 + ((q + 1)/2)\sigma)/q) =$

$= ((3q - 1) + (9q - 1)\theta 1 + 2\theta 1^2) / 6q.$

Por el lema 3.7. tomando $A = 3q - 1$, $B = 9q - 1$, $C = 2$, $r = 6q$ y teniendo en cuenta que $4p - 27q^2 = 1$,

$-(6q)^3 N^K_Q(\mu) = 16p^2 - 8p + 36pq - 108pq^2 - 9q + (27q^2 + 1) -$

$- 27q^3 = 4p(4p - 27q^2) - 8p + 9q(4p - 1) + 4p - 27q^3 =$

$= 9q27q^2 - 27q^3 = 216q^3$.

Luego $N^K_Q(\mu) = -1$. Para ver que $\mu \in R$ vamos a expresar μ como combinación, con coeficientes en Z, de 1, θ y θ^2. Utilizando que $\theta^3 = p\theta - pq$ y $4p - 27q^2 = 1$, se tiene que $\theta 1 = 4p - 9q\,\theta - 6\,\theta^2$, $\theta 1^2 = 4p - 3\theta^2$. Por tanto $\mu = (6p + ((1 + 9q) / 2)) + ((3 - 27q)/2)\theta - 9\theta^2$; como $1 + 9q \equiv 0\ (2)$, $3 - 27q \equiv 0\ (2)$, esos coeficientes están en Z y $\mu \in R$. Estamos, pues, en condiciones de afirmar que μ es una unidad de R.

(iv) Vamos a encontrar la expresión de $Irr(\mu,Q)$. Por ser $Tr^K_Q(\theta) = 0$ y $Tr^K_Q(\theta^2) = 2p$, $Tr^K_Q(\mu) = 3((1 + 9q)/2)$. Por el lema 1.1., el coeficiente en x del $Irr(\mu,Q)$ es

$81p^2 - p((3 - 27q)/2)^2 + 3(6p + ((1 + 9q)/2))^2 - 36p(6p +$

$+ ((1 + 9q)/2)) - 27pq((3 - 27q)/2)$, que, operando y teniendo en cuenta que $4p - 27q^2 = 1$, es igual a $(27q - 3)/2$.

Así, $Irr(\mu,Q) = x^3 - 3((1 + 9q)/2)x^2 + 3((9q - 1)/2)x + 1 =$

$= h(x)$, por notación.

(v) Estudiamos ahora la situación de las raíces de $Irr(\mu,Q)$ obtenido en el párrafo anterior. Dicho polinomio tiene tres

raíces reales que las denotamos como μ_1, μ_2, μ_3. Veamos que :

$$0 < \mu_1 < 1,$$

$$-1 < \mu_2 < 0,$$

$$-1 + 3((1 + 9q)/2) < \mu_3 < 3((1 + 9q)/2).$$

En efecto, $h(0) = 1 > 0$, $h(1) = -1 < 0$, $h(-1) = -27q < 0$,

$$h(3((1+9q)/2)) = 9\ ((81q^2 - 1)/4\ ) + 1 > 0,$$

$$h(-1 + 3((1 + 9q)/2)) = -27q < 0.$$

Por tanto, μ no es totalmente positiva.

(iv) Por el apartado (i), $(1, \theta, \theta^2)$ es una base entera de K. Vamos a obtener S(r) para $r = \alpha\theta + \beta\theta^2$ con $\alpha, \beta \in Z$.

$S(r) = Tr^K_Q(r^2) - (rr' + rr'' + r'r'')$.

Por el lema 1.1.,

$rr' + rr'' + r'r'' = p^2\beta^2 - p\alpha^2 + 3pq\alpha\beta$.

Por otro lado, $\mu^2 = (\alpha^2 + p\beta^2)\theta^2 + (-pq\beta^2 + 2\alpha\beta p)\theta - 2\alpha\beta pq$.

Y, otra vez por el lema 1.1.,

$Tr^K_Q(r^2) = (\alpha^2 + p\beta^2)2p - 6\alpha\beta pq$.

Luego, $S(r) = p(3\alpha^2 + p\beta^2 - 9\alpha\beta q) \in pZ^+$. En particular, tomando $\alpha = (3 - 27q)/2$, $\beta = -9$ tenemos que :

$$(S(\mu))/p = 3((3 - 27q)/2)^2 + 81p + 81q((3 - 27q)/2) =$$

$$= (27 + 4\ 81p - 81 + 324p - 9\ 486q^2)/4 =$$

$$= (27 - 81 + 2\ 81)/4 = 27 \text{ (hemos aplicado que } 4p - 27q^2 = 1).$$

Ahora bien, no existe r unidad de R distinta de $\pm$ 1 verificando $S(r) < 27p$. En efecto, la inecuación $S(r) < 27p$ equivale a $3\alpha^2 + p\beta^2 - 9\alpha\beta q < 27$ para $\alpha, \beta \in Z$; multiplicando por 4 y completando cuadrados equivale a $3(2\alpha - 3q\beta)^2 + \beta^2 < 108$. Hay, pues, que demostrar que no existe $r = \Gamma + \alpha\theta + \beta\theta^2$ distinto de $\pm$ 1 con $\alpha, \beta, \Gamma \in Z$ tal que

$N^K_Q(r) = \pm 1$ y verificando $3(2\alpha - 3q\beta)^2 + \beta^2 < 108$. Sólo hay un número finito de valores para α, $\beta \in \mathbb{Z}$ verificando dicha inecuación; en concreto, dichos valores son :

$\alpha = (3q\beta)/2$, $\beta \in \{2, 4, 6, 8\}$,

$\alpha = (\pm 1 + 3q\beta)/2$, $\beta \in \{1, 3, 5, 7, 9\}$,

$\alpha = (\pm 2 + 3q\beta)/2$, $\beta \in \{2, 4, 6, 8\}$,

$\alpha = (\pm 3 + 3q\beta)/2$, $\beta \in \{1, 3, 5, 7\}$,

$\alpha = (\pm 4 + 3q\beta)/2$, $\beta \in \{2, 4, 6\}$,

$\alpha = (\pm 5 + 3q\beta)/2$, $\beta \in \{1,3,5\}$.

Para cada uno de estos posibles valores de α y β, la ecuación $N^K_Q(r) = \pm 1$, que, por el lema 1.1., equivale a

$\Gamma^3 + 2p\beta\ \Gamma^2 + (3pq\alpha\beta - p\alpha^2 + p^2\beta^2)\ \Gamma + (-p^2q\alpha\beta^2 - pq\alpha^3 + p^2q^2\beta^3 \pm 1) = 0$,

no tiene solución en $\Gamma \in \mathbb{Z}$ (se aplica el teorema de Bolzano al polinomio en Γ que resulta al fijar α y β). Por el teorema de Godwin, podemos concluir que (μ,μ') es un sistema fundamental de unidades de K.

La expresión de μ' (un conjugado de μ), dada en el enunciado del teorema,viene también sugerida por la lectura de la tabla de unidades fundamentales obtenida en el apartado anterior. La demostración de que, en efecto, es un conjugado de μ se hace aplicando el lema 1.1., viendo que tienen el mismo polinomio irreducible sobre Q.

c.q.d.

<u>Ejemplos</u> : p = 61, 331, 547, 817, 1141, 1951, 2437, 2977, 3571, 4219, 4921, 5677, 6487, 7351, 8269, 9241, 10267, 11347, 12481, 13669, 14911, 16207, 17557, 18961.

Nota: Para los cuerpos cúbicos cíclicos de discriminante p^2 tales que $4p - 27q^2 = 1$, $q > 2$ las trazas que M.N. Gras [G2] calcula son iguales a $(27q - 3)/2$ (véase su tabla 4).

Teorema 3.15. : Sea K cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos $q > 2$, $4p - 27q^2 = 9$, $3 \nmid q$. Entonces :

(i) $\{1, \theta, \theta^2/3\}$ y $\{1, \sigma, (((q - 1)/2) + ((q - 1)/2)\sigma + \sigma^2)/q\}$ son bases enteras de K.
$(\sigma = \theta 1/3, \theta 1 = 4(p/3) - 3q\theta - 2\theta^2)$.

(ii) $\mu = (9(q - 1) + 3(3q - 1)\theta 1 + 2\theta 1^2)/(18q)$ es una unidad de R.

(iii) (μ,μ') es un sistema fundamental de unidades de K; μ' es un conjugado de μ,
$\mu' = (9(q - 1) - 3(3q + 1)\theta 1 + 2\theta 1^2)/(18q)$.

(iv) $Irr(\mu,Q) = x^3 - ((3 + 9q)/2)x^2 + ((9q - 3)/2)x + 1$.

(v) μ no es totalmente positiva, (él y sus conjugados no son todos positivos).

Demostración:

(ii) y (iv) Aplicando el lema 3.7., tomando $A = 9(q - 1)$, $B = 3(3q - 1)$, $C = 2$, $r = 18q$, y teniendo en cuenta que $4p - 27q^2 = 9$, se tiene que:

$N^K_Q(\mu) = -1$, $Tr^K_Q(\mu) = (3 + 9q)/2$, $\mu\mu' + \mu\mu'' + \mu'\mu'' = (9q - 3)/2$.

Por tanto, $Irr(\mu,Q) = x^3 - ((3 + 9q)/2)x^2 + ((9q - 3)/2)x + 1$ que pertenece a $Z[x]$, luego μ es una unidad de R.

(i) Por el lema 1.1., $\theta^2/3 \in R$; $disc(\theta) = 9p^2$, luego

$disc(\{1,\theta,\theta^2/3\}) = p^2 = disc(K)$, y dicha base es una base entera de K.

Por otro lado, $(((q - 1)/2) + ((q - 1)/2)\sigma + \sigma^2)/q = = \mu - (\theta 1/3) \in R$ ya que μ, $\theta 1/3 \in R$. Por tanto, $\{1,\sigma,(((q - 1)/2) + ((q - 1)/2)\sigma + \sigma^2)/q\}$ es una Q-base de enteros cuyo discriminante es p^2; es, pues, una base entera de K.

(v) Por notación, $h(x) = Irr(\mu,Q)$. Para ver que μ no es totalmente positiva, vamos a estudiar la situación de las raíces de h(x), (que denotamos como μ_1, μ_2, μ_3).

$h(0) = 1 > 0$,

$h(1) = -1 < 0$,

$h(-1) = -9q < 0$,

$h((3 + 9q)/2) = 1+ ((9q + 3)(9q - 3))/4 > 0$,

$h(-1 + (3 + 9q)/2) = -9q < 0$.

Por tanto, $0 < \mu_1 < 1$,

$-1 < \mu_2 < 0$,

$-1 + (3 + 9q)/2 < \mu_3 < (3 + 9q)/2$, y μ no es totalmente positiva.

(iii) Utilizando el teorema de Godwin demostramos a continuación que $\{\mu,\mu'\}$ es un sistema fundamental de unidades de K. Por el apartado (ii) del teorema 3.8. tomando u = v = = 1, se tiene que $S(\mu) = 3p$. Dado que 8 no se puede poner como 3 por un cuadrado más otro cuadrado, sólo hay que demostrar que $S(\alpha) \neq p$ para toda α unidad de R distinta de $\pm$ 1. En concreto, hay que demostrar que para (u = 1, v = 0), (u = 0, v = 1) y (u = -1, v = 1) no existe $t \in Z$ tal que $\alpha = t + u\sigma + v((((q -1)/2) + ((q - 1)/2)\sigma + \sigma^2)/q)$ es una unidad de R.

Veamos, por ejemplo, el caso u = 1, v = 0; los demás casos son totalmente análogos.

Si u = 1, v = 0 entonces $\alpha = t + (\theta 1/3)$; tenemos, pues, que demostrar que no existe $t \in Z$ tal que $N^K_Q(\alpha) = \pm 1$. Por la proposición 3.9. $N^K_Q(\alpha) = \pm 1$ equivale a $p(3t - 1) - 9t^3 = \pm 9$ O sea, $P(t) = t^3 - 3(p/9)t + ((p/9) \pm 1) = 0$ no debe tener raíces en Z. En efecto, $P(0) = (p/9) \pm 1$; por ser $4p - 27q^2 = 9$

con $q > 2 \Longrightarrow p > 9 \Longrightarrow P(0) > 0$.

$P(1) = -2(p/9)+2$ ó $-2(p/9) \Longrightarrow P(1) < 0$

Luego P(t) tiene una raíz δ tal que $0 < \delta < 1$. Dividiendo P(t) entre $t - \delta$ nos queda $t^2 + \delta t + \delta^2 - (p/3)$.

Las raíces de dicho polinomio de segundo grado son, $(-\delta \pm (-3\delta^2 + (4p/3))^{1/2})/2 = (-\delta \pm (-3\delta^2 + 3 + 9q^2)^{1/2})/2$.

Veamos a continuación que dichas raíces no son de Z. En efecto:

$0 < \delta < 1 \Longrightarrow ((9q^2 + 3(1 - \delta^2))^{1/2})/2 < ((9q^2 + 3)^{1/2})/2 < (1 + 3q)/2$;

luego $(-\delta - (-3\delta^2 + 3 + 9q^2)^{1/2})/2 > (-3q - 2)/2$.

Por otro lado, $(-3\delta^2 + 3 + 9q^2)^{1/2})/2 > (3q/2)$, por tanto, $(-\delta - (-3\delta^2 + 3 + 9q^2)^{1/2})/2 < (-3q)/2$. Pero, el único elemento de Z entre $-3q/2$ y $-1 - (3q/2)$ es $-q - ((q + 1)/2)$ que no es raíz de P(t). Análogamente, $(3q - 1)/2 < (-\delta + (-3\delta^2 + 3 + 9q^2)^{1/2})/2 < (3q + 1)/2$.

Así, P(t) no tiene raíces en Z.

Por el teorema de Godwin, μ es una unidad fundamental de K y (μ,μ') es un sistema fundamental de unidades de K. La expresión de μ' (conjugado de μ) dada en el enunciado del teorema, viene también sugerida tras la lectura de la tabla

de unidades fundamentales. La demostración de que es un conjugado se hace aplicando el lema 3.7., tomando A = 9(q - 1), B = -3(3q + 1), C = 2, r = 18q, y viendo que $Irr(\mu',Q) = Irr(\mu,Q)$; también tenemos que aplicar que $4p - 27q^2 = 9$.
c.q.d.

Ejemplos: p = 171, 333, 819, 1143, 2439, 3573, 4221, 5679, 6489, 8271, 9243, 11349, 12483, 14913, 16209.

Nota: Para los cuerpos cúbicos cíclicos de discriminante p^2 tales que $4p - 27q^2 = 9$, $q > 2$, $3 \nmid q$ las trazas que M.N. Gras [G2] calcula son iguales a (9q - 3)/2 (véase su tabla 4).

Centramos ahora nuestro estudio en las familias de cuerpos cúbicos cíclicos V y W. Nos proponemos dar resultados relativos al número de clase para cada una de tales familias. En concreto, estudiamos:

1) Teoremas sobre la paridad del número de clase.
2) Comportamiento del número de clase cuando el discriminante tiende hacia infinito.

El primer punto ha sido tratado para la familia U por Harvey-Cohn [HC1] y M. Watabe[Wi], i = 4, 5. El segundo punto para la familia U ha sido estudiado por M. Watabe [W2].

1) Teoremas sobre la paridad del número de clase para las familias V y W. Tanto para la familia V como para la familia W se da la circunstancia de que la unidad fundamental μ que la tesis obtiene es no totalmente positiva. Por tanto, toda unidad de R totalmente positiva tiene que ser un cuadrado en R . La tesis lo que hace es encontrar, para cada una de las familias V y W, un elemento $\alpha \in R$ totalmente positivo y tal que el ideal que engendra es un cuadrado J^2. En las hipótesis del teorema sobre la paridad del número de clase, que a continuación enunciamos, lo que hacemos es imponer una condición suficiente para poder asegurar que dicho elemento α no es un cuadrado en R. De donde, la clase del ideal J es un elemento de orden dos en el grupo de clases de K y el número de clase de K es par.

Teorema 3.16 .: Sea K cuerpo de números cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos $4p - 27q^2 = 1$, $q > 2$. Si q es un cuadrado (en Z) y $(1 + 3q)/2$ no es un cuadrado en Z_{qi} para al menos un qi divisor primo de q, entonces el número de clase de K es par.

Demostración: Los primos divisores de p son los únicos que ramifican en K. Por ser $(p,q) = 1$, entonces los primos divisores de q son no ramificados en K. Veamos que todo divisor primo de q descompone completamente en K. Sea q_j primo divisor de q; $disc(\theta) = disc(K) \Longrightarrow q_j \nmid$ índice(θ).

$$x^3 - px + pq \equiv x(x - ((1 + 3q)/2))(x + ((1 + 3q)/2)), \quad (Z_{qj}[x])$$

ya que $4p - 27q^2 = 1$.

Luego $q_jR = (q_j,\theta)(q_j,\theta - ((1 + 3q)/2))(q_j,\theta + ((1 + 3q)/2))$.
Por notación, $Q_{j1} = (q_j,\theta)$, $Q_{j2} = (q_j,\theta - ((1 + 3q)/2))$, $Q_{j3} = (q_j,\theta + ((1 + 3q)/2))$.
Sea $\alpha = -\theta + ((1 + 3q)/2) \in R$. Veamos, en primer lugar, que α es totalmente positivo (él y sus conjugados son positivos). Para ello, tenemos que ver que las raíces de $f(x) = x^3 - px + pq$ son menores que $(1 + 3q)/2$. Ahora bien, los extremos relativos de $f(x)$ se alcanzan en $\pm(p/3)^{1/2}$. Como $f((p/3)^{1/2}) = p(q - (2/3)(p/3)^{1/2}) < 0$, $f(-(p/3)^{1/2}) = p(q + (2/3)(p/3)^{1/2}) > 0$; y $\lim_{x \to \pm\infty} f(x) = \pm\infty$ respectivamente, es suficiente ver que $f((1 + 3q)/2) > 0$ (nótese que $(1 + 3q)/2 > (p/3)^{1/2}$). En efecto,

$$f((1 + 3q)/2) = (1 + 27q^3 + 27q^2 + 9q - 4p - 4pq)/8 =$$
$$= (4p + 4pq - q + 9q - 4p - 4pq)/8 = q > 0.$$

Por consiguiente, $\alpha = -\theta + ((1 + 3q)/2)$ es totalmente positivo.
En segundo lugar, el ideal (α) es necesariamente el cuadrado de un ideal de R. En efecto, $N^K_Q(-\theta + ((1 + 3q)/2)) = f((1 + 3q)/2) = q$, que, por hipótesis, es un cuadrado en Z. Ahora bien, $\alpha = -\theta + ((1 + 3q)/2) \in Q_{j2}$ pero $\alpha \notin Q_{j1}, Q_{j3}$. Necesariamente, $(\alpha) = J^2$, J es un ideal de R.
Y, en tercer lugar, de la hipótesis $(1 + 3q)/2$ no es un cuadrado en Z_{qi}, para al menos un q_i divisor primo de q, vamos a deducir que $\alpha = -\theta + ((1 + 3q)/2)$ no es un cuadrado en R. Supongamos $\alpha = \beta^2$ con $\beta \in R$. Entonces, $(1 + 3q)/2 \equiv \beta^2 (Q_{i1})$. Pero, el grupo de Galois de K sobre Q actúa transitivamente sobre los primos de K que yacen sobre un mismo primo de Z

(véase [M,th. 23]). Luego (1 + 3q)/2 ≡ β'^2 (Q_{i2}), (1 + 3q)/2 ≡ β''^2(Q_{i3}). Ahora bien , por ser $q_iR = Q_{i1}Q_{i2}Q_{i3}$ tenemos el siguiente isomorfismo

$$R/q_i \longleftrightarrow R/Q_{i1} \times R/Q_{i2} \times R/Q_{i3}$$
$$s \longmapsto (s + Q_{i1}, s + Q_{i2}, s + Q_{i3}).$$

Existe, pues, un único $r \in R$ / $r + Q_{i1} = \beta + Q_{i1}$,
$r + Q_{i2} = \beta' + Q_{i2}$,
$r + Q_{i3} = \beta'' + Q_{i3}$.

De donde, $(1 + 3q)/2 \equiv r^2 (q_iR)$. Por el teorema 3.14. , $(1,\theta,\theta^2)$ es base entera de K. Luego $r = A + B\theta + C\theta^2$ con $A,B,C \in Z$. Así, $(1 + 3q)/2 = (A + B\theta + C\theta^2)^2 + q_i(D + E\theta + F\theta^2)$; siendo $D,E,F \in Z$. Teniendo en cuenta que $\theta^3 = p\theta - pq$,

$$(1 + 3q)/2 = (A^2 - 2BCpq + q_iD) + (2AB + 2BCp - pqC^2 + Eq_i)\theta + (b^2 + pC^2 + 2AC + Fq_i)\theta^2.$$

Luego $(1 + 3q)/2 = A^2 - 2BCpq + q_iD \equiv A^2(q_i)$, absurdo por hipótesis.

Resumiendo,hemos encontrado un elemento $\alpha = -\theta + ((1 + 3q)/2)$ de R tal que es totalmente positivo, no es un cuadrado en R y el ideal (α) es el cuadrado de un ideal de R. Terminamos la demostración del teorema razonando de la siguiente manera: tenemos $(\alpha) = J^2$; veamos que J no es un ideal principal de R. Razonamos por reducción al absurdo. Supongamos $J = (r)$ con $r \in R \Longrightarrow (\alpha) \equiv (r^2) \Longrightarrow \alpha = ur^2$ siendo u una unidad de R. Por ser α y r^2 totalmente positivos, u también es totalmente positivo. Ahora bien, por el teorema 3.14. , (μ,μ') es un sistema fundamental de unidades de K siendo μ no totalmente positiva. Como ninguna de μ, μ', $\mu\mu'$ es totalmente positiva, u es necesariamente un cuadrado de R. De donde $\alpha = ur^2 \in R^2$,

absurdo. Así, J no es un ideal principal y el orden de J en el grupo de clases de K es 2.

c.q.d.

Ejemplos:

1) p= 547, q = 9.

   5 no es un cuadrado en Z_3, luego el número de clase h de K es par.

2) p = 4219, q = 25.

   8 no es un cuadrado en Z_5, luego h es par.

Teorema 3.17 .: Sea K cuerpo de números cúbico cíclico de discriminante p^2. K = Q(θ), Irr(θ,Q) = x^3 - px + pq y supongamos $4p - 27q^2 = 9$, q > 2, 3 ∤ q. Si q es un cuadrado (en Z) y (3 + 3q)/2 no es un cuadrado en Z_{qi} para al menos un qi divisor primo de q, entonces el número de clase de K es par.

Demostración: Los primos divisores de p son los únicos que ramifican en K. Por ser (p,q) = 1, entonces los primos divisores de q son no ramificados en K. Veamos que todo divisor primo de q descompone completamente en K. Sea q_j primo divisor de q; disc(θ) = $9p^2$, $3 \nmid q$ ==> $q_j \nmid$ índice(θ).
$x^3 - px + pq = x\,(x - ((3 + 3q)/2))\,(x + ((3 + 3q)/2))$, $(Z_{qj}[x])$ ya que $4p - 27q^2 = 9$.
Luego $q_jR = (q_j,\theta)(q_j,\theta - ((3 + 3q)/2))(q_j,\theta + ((3 + 3q)/2))$.
Por notación, $Q_{j1} = (q_j,\theta)$, $Q_{j2} = (q_j,\theta - ((3 + 3q)/2))$, $Q_{j3} = (q_j,\theta + ((3 + 3q)/2))$.
Sea $\alpha = -\theta + ((3 + 3q)/2) \in R$. Veamos, en primer lugar, que α

es totalmente positivo. Para ello, tenemos que ver que las raíces de $f(x) = x^3 - px + pq$ son menores que $(3 + 3q)/2$. Ahora bien, los extremos relativos de $f(x)$ se alcanzan en $\pm(p/3)^{1/2}$. Como $f((p/3)^{1/2}) = p\,(q - (2/3)(p/3)^{1/2}) < 0$, $f(-(p/3)^{1/2}) = p(q + (2/3)(p/3)^{1/2}) > 0$; y $\lim_{x \to \pm\infty} f(x) = \pm\infty$ es suficiente ver que $f((3 + 3q)/2) > 0$ (nótese que $(3 + + 3q)/2 > (p/3)^{1/2}$). En efecto,

$$f((3 + 3q)/2) = (27 + 27q^3 + 81q^2 + 81q - 12p - 4pq)/8 =$$
$$= (-9q - 27q^3 - 27 - 81q^2 + 81q)/8 = 9q > 0.$$

Por consiguiente, $\alpha = -\theta + ((3 + 3q)/2)$ es totalmente positivo.

En segundo lugar, el ideal (α) es necesariamente el cuadrado de un ideal de R. En efecto, $N^K_Q(-\theta + ((3 + 3q)/2)) = f((3 + 3q)/2) = 9q$, que es un cuadrado en Z, ya que, por hipótesis, $q \in Z^2$. Ahora bien, $\alpha = -\theta + ((3 + 3q)/2) \in Q_{j2}$ pero $\alpha \notin Q_{j1}, Q_{j3}$. Necesariamente, $(\alpha) = J^2$, J es un ideal de R.

Y en tercer lugar, de la hipótesis $(3 + 3q)/2$ no es un cuadrado en Z se deduce de forma totalmente análoga a como se hace en el teorema anterior que $\alpha = -\theta + ((3 + 3q)/2)$ no es un cuadrado en R.

Resumiendo, hemos encontrado un elemento $\alpha = -\theta + ((3 + 3q)/2)$ de R tal que es totalmente positivo, no es un cuadrado en R y el ideal (α) es el cuadrado de un ideal de R. Terminamos la demostración del teorema razonando de la misma forma que en el teorema anterior :

tenemos $(\alpha) = J^2$; veamos que J no es un ideal principal de R. Razonamos por reducción al absurdo. Supongamos $J = (\tau)$ con

$r \in R \Longrightarrow (\alpha) = (r^2) \Longrightarrow \alpha = ur^2$ siendo u una unidad de R. Por ser α y r^2 totalmente positivos, u también es totalmente positivo. Ahora bien, por el teorema 3.15. , (μ,μ') es un sistema fundamental de unidades de K siendo μ no totalmente positiva. Como ninguna de μ, μ', $\mu\mu'$ es totalmente positiva, u es necesariamente un cuadrado de R. De donde $\alpha = ur^2 \in R^2$, absurdo. Así, J no es un ideal principal y el orden de J en el grupo de clases de K es 2.

c.q.d.

Ejemplo:

1) p= 16209, q = 49.

   12 no es un cuadrado en Z_7, luego el número de clase h de K es par.

2) Comportamiento del número de clase cuando el discriminante tiende hacia infinito para las familias V y W.

La tesis demuestra que el número de clase de los cuerpos cúbicos cíclicos de la familia V y de la familia W tiende a infinito cuando el discriminante tiende a infinito. Con este fin utilizaremos la fórmula

$$\lim_{|D|\to\infty} (\log(h_K R_K)/\log((|D_K|)^{1/2})) = 1$$

(h_K es el número de clase de K, R_K es el regulador de K y D es el discriminante de K). Dicha fórmula fue establecida por Siegel para cuerpos cuadráticos y Brauer [B] para cuerpos de números algebraicos generales (fijado el grado).

Para la familia de cuerpos cúbicos cíclicos U ya tenemos el estudio que, en 1983, realiza M. Watabe [W2].

Teorema 3.18 .: Sea K cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos $q > 2$, $4p - 27q^2 = 1$. Entonces $\lim_{p\to+\infty} h_K = +\infty$.

Demostración:

Por el teorema 3.14., (μ,μ') es un sistema fundamental de unidades de K, siendo $Irr(\mu,Q) = x^3 - 3((1 + 9q)/2)x^2 + ((27q - 3)/2)x + 1$, (= h(x) por notación). Además, en la demostración del citado teorema se demuestra que las raíces μ_1, μ_2 y μ_3 de h(x) verifican:

$$-1 < \mu_1 < 0,$$

$$0 < \mu_2 < 1,$$

$$-1 + 3((1 + 9q)/2) < \mu_3 < 3((1 + 9q)/2).$$

Nuestro primer objetivo es demostrar que

$\lim_{p\to\infty} (\log(R_K)/\log(p))$ es igual a cero. Una vez que demostremos esto, el enunciado del teorema se sigue de forma inmediata aplicando la ya mencionada fórmula $\lim_{p\to\infty} (\log(h_K R_K)/\log(p)) = 1$.

Por definición, $R_K = \text{abs}(\log(|\mu_1|)\log(\mu_3) - (\log(\mu_2))^2)$.

Pero, se tiene $\log(|\mu_1|) < 0$, $\log(\mu_3) > 0$, luego $R_K = -\log(|\mu_1|)\log(\mu_3) + (\log(\mu_2))^2)$.

Vamos a obtener, en primer lugar, mejores cotas para las raíces μ_i, $i = 1,2,3$ de $Irr(\mu,Q)$.

$h(-2/(3(1 + 9q))) =$

$= (1/(1 + 9q))(-8/(27(1 + 9q)^2) - 2/3 - 9q + 1) + 1.$

Ahora bien, $1 > (1/(1 + 9q))(8/(27(1 + 9q)^2) + 2/3 + 9q - 1)$ ya que ello equivale a

$3^3(1 + 9q)^3 > 8 + 18(1 + 9q)^2 + (9q - 1)(1 + 9q)^2 27,$

y denotando $r = 1 + 9q$,

$$27r^3 > 8 + 18r^2 + 27(r - 2)r^2 = -36r^2 + 27r^3 + 8$$

y como $r > 19$, esa inecuación se verifica trivialmente. Luego $h(-2/(3(1 + 9q))) > 0$.

Por otro lado,

$h(-1/(1 + 9q)) =$

$= (1/(1 + 9q))(-1/(1 + 9q)^2 - 3/2 - ((27q - 3)/2)) + 1.$

Pero, $h(-1/(1 + 9q)) < 0$ ya que ello equivale a

$$2(1 + 9q)^3 < 2 + 3(1 + 9q)^2 + (27q - 3)(1 + 9q)^2;$$

denotando $r = 1 + 9q$ nos queda:

$2r^3 < 2 + 3r^2 + (3r - 6)r^2$, que equivale a

$0 < r^3 - 3r^2 + 2$, que es cierta ya que $r > 19$.

Por tanto, $-1/(1 + 9q) < \mu_1 < -2/(3(1 + 9q))$, de donde

$$-\log(|\mu_1|) < \log(3(1 + 9q)/2).$$

A continuación, veamos que $2/(1 + 27q) < \mu_2 < 1$. La segunda desigualdad ya se demostró en el teorema 3.14.; para demostrar la primera, vamos a comprobar que el signo de $h(2/(1 + 27q))$ es positivo. En efecto:

$h(2/(1 + 27q)) =$

$= (2/(1 + 27q))((1 - 27q)/(1 + 27q)^2) + ((27q - 3)/2)) + 1.$

Se tiene que $(27q - 3)/2 > (- 1 + 27q)/(1 + 27q)^2$, pues ello equivale a $(27q - 3)(1 + 27q)^2 > 54q - 2$ <===>

$(r - 2)(r + 2)^2 > 2r,$ siendo por notación $r = 27q - 1 > 53.$

Queda, pues, demostrado que $2/(1 + 27q) < \mu_2 < 1$ ====>

===> $\log(2/(1 + 27q)) < \log(\mu_2) < 0$ ===>

$(\log(\mu_2))^2 < (\log((1 + 27q)/2))^2 < (\log((3 + 27q)/2))^2$

Por otro lado, obviamente , $\log(\mu_3) < \log((3 + 27q)/2)$. Por tanto,

$R_K = -\log(|\mu_1|)\log(\mu_3) + (\log(\mu_2))^2 < 2(\log((3 + 27q)/2))^2$

Pero, para q suficientemente grande, $R_K \geq 1$. Efectivamente,

$-1/(1 + 9q) < \mu_1 < -2/(3(1 + 9q))$ ==>

===> $\lim_{q\to+\infty} \mu_1 = 0$ ==> $\lim_{q\to+\infty} (\log|\mu_1|) = -\infty$.

$-1 + 3((1 + 9q)/2) < \mu_3 < 3((1 + 9q)/2)$ ==>

===> $\lim_{q\to+\infty} \mu_3 = +\infty$ ==> $\lim_{q\to+\infty} (\log(\mu_3)) = +\infty$.

Luego, $\lim_{q\to+\infty} (-\log(|\mu_1|)\log(\mu_3)) = +\infty$. Y, en particular, $R_K \geq 1$ si $q \geq q_0$ para un cierto $q_0 \in N$.

Tenemos, pues, $1 \leq R_K < 2(\log((3 + 27q)/2))^2$ para $q \geq q_0$. Tomamos logaritmos en dichas desigualdades y dividimos entre $\log(p)$:

$0 \leq \log(R_K)/\log p < \log 2/\log p + (2\log(\log((3 + 27q)/2)))/\log p <$

$< \log 2/\log p + (2\log(\log((3 + 27q)/2)))/\log((3 + 27q)/2))$

por ser $p = (1 + 27q^2)/4 > (3 + 27q)/2$; para $q \geq q_0$.
Ahora bien, el segundo miembro de la última desigualdad tiende a 0 cuando q --> +∞ (o,de forma equivalente p --> +∞).
Por tanto, $\lim_{q\to+\infty} (\log(R_K)/\log(p)) = 0$ luego
$\lim_{p\to+\infty} (\log(h_K)/\log p) = 1$
ya que $\lim_{p\to+\infty} (\log(h_K R_K)/\log p) = 1$, [B]. Y, necesariamente, $\lim_{p\to+\infty} h_K = +\infty$.

c.q.d.

Teorema 3.19.: Sea K cúbico cíclico de discriminante p^2. $K = Q(\theta)$, $Irr(\theta,Q) = x^3 - px + pq$ y supongamos $q > 2$, $4p - 27q^2 = 9$, $3 \nmid q$. Entonces $\lim_{p\to+\infty} h_K = +\infty$.

Demostración :

Por el teorema 3.15., (μ,μ') es un sistema fundamental de unidades de K, siendo $Irr(\mu,Q) = x^3 - 3((1 + 3q)/2)x^2 + ((9q - 3)/2)x + 1$, (= h(x) por notación). Además, en la demostración del citado teorema se demuestra que las raíces μ_1, μ_2 y μ_3 de h(x) verifican:

$$-1 < \mu_1 < 0,$$

$$0 < \mu_2 < 1,$$

$$-1 + 3((1 + 3q)/2) < \mu_3 < 3((1 + 3q)/2).$$

Veamos, en primer lugar que: $\lim_{p\to+\infty} (\log(R_K)/\log(p)) = 0$.
Por definición, $R_K = abs(\log(|\mu_1|)\log(\mu_3) - (\log(\mu_2))^2)$.
Pero, se tiene $\log(|\mu_1|) < 0$, $\log(\mu_3) > 0$, luego $R_K = -\log(|\mu_1|)\log(\mu_3) + (\log(\mu_2))^2)$.
Vamos a obtener mejores cotas para las raíces de $Irr(\mu, Q)$.
$h(-2/(3(1 + 3q))) = (1/(1 + 3q))(-8/(27(1 + 3q)^2) - 2/3 - 3q + 1) + 1.$
Ahora bien, $1 > (1/(1 + 3q))(8/(27(1 + 3q)^2) + 2/3 + 3q - 1)$

ya que ello equivale a $3^3(1 + 3q)^3 > 8 + 18(1 + 3q)^2 + (3q - -1)(1 + 3q)^2 27$,

y denotando $r = 1 + 3q$,

$$27r^3 > 8 + 18r^2 + 27(r - 2)r^2 = -36r^2 + 27r^3 + 8$$

y como $r > 7$, esa inecuación se verifica trivialmente. Luego $h(-2/(3(1 + 3q))) > 0$.

Por otro lado,

$h(-1/(1 + 3q)) = (1/(1 + 3q))(-1/(1 + 3q)^2 - 3/2 - ((9q - - 3)/2)) + 1.$

Pero, $h(-1/(1 + 3q)) < 0$ ya que ello equivale a

$$2(1 + 3q)^3 < 2 + 3(1 + 3q)^2 + (9q - 3)(1 + 3q)^2;$$

denotando $r = 1 + 3q$ nos queda:

$2r^3 < 2 + 3r^2 + (3r - 6)r^2$, que equivale a

$0 < r^3 - 3r^2 + 2$, que es cierta ya que $r > 7$.

Por tanto, $-1/(1 + 3q) < \mu_1 < -2/(3(1 + 3q))$, de donde

$$-\log(|\mu_1|) < \log(3(1 + 3q)/2).$$

A continuación, veamos que $2/(1 + 9q) < \mu_2 < 1$. La segunda desigualdad ya se demostró en el teorema 3.15.; para demostrar la primera, vamos a comprobar que $h(2/(1 + 9q)) > 0$. En efecto $h(2/(1 + 9q)) =$

$= (2/(1 + 9q))((1 - 9q)/(1 + 9q)^2) + ((9q - 3)/2)) + 1.$

Se tiene que $(9q - 3)/2 > (- 1 + 9q)/(1 + 9q)^2$, pues ello equivale a:

$(9q - 3)(1 + 9q)^2 > 18q - 2 \Longleftrightarrow (r - 3)(r + 1)^2 > 2(r - 1)$,

siendo por notación $r = 9q > 18$.

Queda, pues, demostrado que $2/(1 + 9q) < \mu_2 < 1 \Longrightarrow$

$\Longrightarrow \log(2/(1 + 9q)) < \log(\mu_2) < 0 \Longrightarrow$

$$(\log(\mu_2))^2 < (\log((1 + 9q)/2))^2 < (\log((3 + 9q)/2))^2$$

Por otro lado, obviamente , $\log(\mu_3) < \log((3 + 9q)/2)$.

Por tanto,

$R_K = -\log(|\mu_1|)\log(\mu_3) + (\log(\mu_2))^2 < 2(\log((3 + 9q)/2))^2$

Pero, para q suficientemente grande, $R_K \geq 1$. Efectivamente,

$-1/(1 + 3q) < \mu_1 < -2/(3(1 + 3q)) \Longrightarrow$

$\Longrightarrow \lim_{q\to+\infty} \mu_1 = 0 \Longrightarrow \lim_{q\to+\infty} (\log|\mu_1|) = -\infty.$

$-1 + 3((1 + 3q)/2) < \mu_3 < 3((1 + 3q)/2) \Longrightarrow$

$\Longrightarrow \lim_{q\to+\infty} \mu_3 = +\infty \Longrightarrow \lim_{q\to+\infty} (\log(\mu_3)) = +\infty.$

Luego, $\lim_{q\to+\infty} (-\log(|\mu_1|)\log(\mu_3)) = +\infty$. Y, en particular, $R_K \geq 1$ si $q \geq q_0$ para un cierto $q_0 \in N$.

Tenemos, pues, $1 \leq R_K < 2(\log((3 + 9q)/2))^2$ para $q \geq q_0$.

Tomamos logaritmos en dichas desigualdades y dividimos entre log(p):

$0 \leq \log(R_K)/\log p < \log 2/\log p + (2\log(\log((3 + 9q)/2)))/\log p <$

$< \log 2/\log p + (2\log(\log((3 + 9q)/2)))/\log((3 + 9q)/2))$ por ser $p = (9 + 27q^2)/4 > (3 + 9q)/2$; para $q \geq q_0$.

Ahora bien, el segundo miembro de la última desigualdad tiende a 0 cuando $q \to +\infty$ (o,de forma equivalente $p \to +\infty$).

Por tanto, $\lim_{q\to\infty} (\log(R_K)/\log(p)) = 0$, luego $\lim_{p\to\infty} (\log(h_K)/\log p) = 1$ ya que

$$\lim_{p\to\infty} (\log(h_K R_K)/\log p) = 1, \quad [B].$$

Y, necesariamente, $\lim_{p\to+\infty} h_K = +\infty$.

c.q.d.

BIBLIOGRAFIA

BIBLIOGRAFIA

[A] A.A. Albert. A determination of the integers of all cubic fields. Ann. of Math., 31 (1930), 550-566.

[Ak] A. Akritas. Elements of computer algebra with applications. J. Wiley, cop.1989.

[B] R. Brauer. On the zeta-functions of algebraic numbers fields. Amer. J. Math., 69, 243-250 (1947).

[Be] L. Berstein. On units and fundamental units. Journal fur die reine und angew. Math., Band 257, 1972, pp. 129-145.

[Be1] W.E.H. Berwick. Algebraic number-fields with two independent units. Proc. London Math. Soc. (2) 34 (1932), 360-378.

[Be2] W.E.H. Berwick. Integral Bases. Stechert-Hafner service agency. New York and London, 1964.

[Bi] K.K. Billevich. On the units of algebraic fields of the third and fourth degrees,(in Russian). Mat. Sb., v.40, 1956, pp. 123-136, and v. 48, 1959, p.256.

[B,S] E. Bombieri and W.M. Schmidt. On Thue's equation. Invent. Math. 88, 69-81 (1987).

[C1] T.W.Cusick. Finding fundamental units in cubic fields. Math. Proc. Camb. Phil. Soc. (1982), 92, 385-389.

[C2] T.W.Cusick. Finding fundamental units in totally real fields. Math. Proc. Camb. Phil. Soc. (1984), 96, 191- - 194.

[C,L] T.W. Cusick and Lowell Schoenfeld. A Table of Fundamental Pairs of Units in Totally Real Cubic Fields. Math. Comp., vol. 48, num. 177, (1987), p. 147-158.

[D1] J.R. Delgado. Some questions concerning the cubic number field Q(θ) generated by a root of $x^3 + abx + b =$ $= 0$. Extracta Mathematicae, vol. 1, n. 3, 142-144 (1986).

[D2] J.R.Delgado. Ramification and units of the cubic number field Q(θ) generated by a root of $x^3 + abx + b = 0$. Extracta Mathematicae, vol. 2, n. 2, 53-55 (1987).

[D,F] B. N. Delone and D. K. Faddeev. The theory of irrationalities of the third degree. Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R.I., 1964.

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

[G1] M.N. Gras. Nombre de classes, unites et bases d'entiers des extensions cubiques cycliques de Q. Journées arithmétiques. Bull.Soc.Math. France, Mémoire 37, 1974, p. 101-106.

[G2] M.N.Gras. Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de Q. J.Reine Angew. Math. ,277 (1975), 89-116.

[G3] M.N.Gras. Note a propos d'une conjecture de H.J.Godwin. Sur les unités des corps cubiques. Ann. Inst. Fourier, Grenoble 30, 4 (1980), 1-6.

[Go] H.J. Godwin. On totally complex quartic fields with small discriminants. Proc. Cambridge Philos. Soc., 53 (1957), 1-4.

[Go,S] H.J. Godwin and P.A. Samet. A table of real cubic fields. Journal London Math. Soc. 34 (1959), 108-110.

[Go1] H.J.Godwin. The determination of units in totally real cubic fields. Proc. Cambridge Philos. Soc. 56 (1960), 318-321.

[Go2] H.J.Godwin. The calculation of large units in cyclic cubic fields. J.Reine Angew. Math., v.338, 1983, pp.216-220.

[Go3] H.J. Godwin. A note on Cusick's theorem on units in totally real cubic fields. Math. Proc. Camb. Phil. Soc. (1984), 95, 1.

[H] M.Hall. Indices in cubic fields. Bull Amer. Math. Soc. 43 (1937), 104-108.

[Ha] H. Hasse. Aritmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Math. Z. 31 (1930), 565-582.

[HC1] Harvey-Cohn. A device for generating fields of even class number. Proc. Amer. Math. Soc.,7, 595-598 (1956).

[HC2] Harvey-Cohn. A classical invitation to algebraic numbers and class fields. Springer-Verlag, Berlin-New York, 1978.

[He] H. Heilbronn. On Euclid's Algorithm in cubic self-conjugate fields. Proc. Cambridge Philos. Soc., 46 (1950), 377-382.

[J] G.J. Janusz. Algebraic Number Fields. Academic Press. New York and London 1973.

[L] S. Lang. Algebra. Aguilar, Spain 1971.

[L1] P.Llorente. Algunos problemas en la Teoría de Números Algebraicos. Pub. Mat. UAB. N 23, Febrer 1981.

[L,N] P.Llorente and E.Nart. Effective determination of the descomposition of the rational primes in a cubic field. Proc. of the Am. Math. Soc. vol 87, N.4, April 1983.

[L2] P.Llorente. Cubic Irreducible Polynomials in Z_p [x] and the descomposition of primes in a cubic field. Pub. Mat. UAB. vol 27 N.3 Dec 1983.

[M] D.A. Marcus. Number Fields, Springer-Verlag, New York, 1977.

[Ma] G.B. Mathews. On the Algebraical integers derived from an irreducible cubic equation. Proc. London Math. Soc. (1) 24 (1893), 327-336 [1].

[M,P] J. Martinet and J.J. Payan. Sur les extensions cubiques non-Galoisiennes des rationnels et leur clôture Galoisienne. J. Reine Angew. Math. 228 (1967), 15-37.

[P,Z] M. Pohst & H. Zassenhaus. Algorithmic Algebraic Number Theory. Cambridge University Press, 1989.

[S] M.Scarowsky. On units of certain cubic fields and the diophantine equation $x^3 + y^3 + z^3 = 3$. Proc. Amer. Math. Soc.91(3), 1984, 351-356.

[Sa] P. Samuel. Théorie algébrique des nombres, Hermann, 1967.

[Sch] W.M.Schmidt. Thue equations with few coefficients. Trans. of the Amer. Math. Soc., vol 303, N.1, 1987.

[St] R.J. Stroeker. How to solve a diophantine equation - a number-theoretic excursion. Amer. Math. Monthly 91(1984), no 7, 385-392.

[S,R] R. Steiner & R. Rudman. On an algorithm of Billevich for finding units in algebraic number fields. Math. Comp., v.30, 1976, pp.598-609.

[T] E.Thomas. Fundamental units for orders in certain cubic number fields. J.Reine Angew. Math., 310, 33-55 (1979).

[To] L. Tornheim. Minimal basis and inessential discriminant divisors for a cubic field. Pacific J. Math. 5 (1955), 623-631.

[U] K.Uchida. On a cubic cyclic field with discriminant 163^2. Journal of Number Theory, 8, 346-349 (1976).

[V] G.T. Woronoj. The complex integers derived from an irreducible cubic equation. (Translation of Russian title). Petersburg (1894), 1-173 [1,80].

[Ve] E. Veikko. On a conjecture of H.J. Godwin on cubic units. Ann. Acad. Sci. Fenn. Ser. A I Math. 12 (1987), no2, 319-328.

[W1] M.Watabe. On Certain Cubic Fields. I. Proc. Japan Acad., 59, Ser.A (1983), 66-69.

[W2] M.Watabe. On Certain Cubic Fields. II. Proc. Japan Acad., 59, Ser.A (1983), 107-108.

[W3] M.Watabe. On Certain Cubic Fields. III. Proc. Japan Acad., 59, Ser.A (1983), 260-262.

[W4] M.Watabe. On Certain Cubic Fields. IV. Proc. Japan Acad., 59, Ser.A (1983), 387-389.

[W5] M.Watabe. On Certain Cubic Fields. V. Proc. Japan Acad. 60, Ser.A(1984), 302-305.

[W6] M.Watabe. On Certain Cubic Fields.VI.Proc. Japan Acad., 60, Ser.A(1984), 331-332.

[W,Z] H.C. Williams & C.R. Zarnke. Computer Calculation of Units in Cubic Fields. Proc. Second Manitoba Conf. Numer. Math., 1972, pp. 433-468.

Título: Cuerpos de números cúbicos.
Cálculo de unidades fundamentales.

Autor : Francisca Cánovas Orvay.

Director : Juan Ramón Delgado Pérez.

Fé de erratas.

Página	Línea	Dice	Debe decir
3	17	$f(P_i/Z) = [R/P_i]$	$f(P_i/Z) = [R/P_i : Z/pZ]$
14	7	si es no	si 3 es no
33	6	bases enteras de K	bases de enteros de K
36	27	$v_p(disc(K)) = -1+e_i+h_i$	$v_p(disc(K)) = \sum_{i=1}^{s} (-1+e_i+h_i)f_i$
79	14	$v_p(D) = -1 + e + h$	para $e > 1$, $v_p(D) = -1 + e + h$
128	10	siendo t_0	siendo $t_1 = s_1/3$ y t_0
128	12	siendo t_0	siendo $t_1=(1 + s_1)/3$ y t_0
184	14	$\rho^2 =$	$r^2 =$