UNIVERSIDAD AUTÓNOMA METROPOLITANA – IZTAPALAPA
DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

RAMIFICACIÒN EN GRUPOS DE GALOIS DE POLINOMIOS DE LA FORMA x^4+px^2+p

Tesis que presenta
Julio Pérez Hernández
Para obtener el grado de
Doctor en Ciencias (Matemáticas)

Asesor: Dr. Mario Pineda Ruelas

Jurado Calificador:

Presidente: Dr. Florian Luca

Secretario: Dra. Rita Esther Zuazua Vega

Vocal: Dr. Timothy Mooney Gendron Thornton

Vocal: Dr. Horacio Tapia Recillas

México, D.F. 29 de septiembre 2022

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Iztapalapa

Departamento de Matemáticas

RAMIFICACIÓN EN GRUPOS DE GALOIS DE POLINOMIOS DE LA FORMA $x^4 + px^2 + p$

Presenta:
M. en C. JULIO PÉREZ HERNÁNDEZ

para la obtención del grado
DOCTOR EN CIENCIAS (MATEMÁTICAS)

Asesor: Dr. Mario Pineda Ruelas

México
29 de septiembre del 2022

Dedicatoria

Dedico este trabajo a mi hermano Antonio Pérez Hernández.

Contenido

Introducción

El Teorema Fundamental de la Aritmética establece que cada número natural > 1 se puede expresar en forma única como un producto de ciertas potencias de números primos. En anillos de enteros, esta propiedad no se cumple y el ejemplo clásico es $\mathbb{Z}[\sqrt{-5}]$. A nivel de ideales no cero, cualquier ideal es producto de ideales primos en forma única. Dedekind, en su famosa memoria de 1877 [**8**], pp 53-61, propone estudiar leyes generales de la división que gobiernan a los anillos de enteros. Un año después, publica su célebre Teorema 1.52, en donde describe la factorización de un ideal no cero, como producto de ideales primos, solo que, en las hipótesis aparece una condición sobre el índice del generador del campo. En su teorema, Dedekind da generadores de los ideales primos factores. Como sabemos, si p es un primo racional y $L = \mathbb{Q}(\theta)$ es un campo de números de grado n y $\mathcal{O}_L$ es su anillo de enteros, entonces, teóricamente es posible factorizar

$$p\mathcal{O}_L = P_1^{e_1} \cdots P_g^{e_g},$$

donde los P_i son ideales primos de $\mathcal{O}_L$. El problema de encontrar la factorización anterior ha merecido la atención de matemáticos interesados en el tema. Por ejemplo, Llorente-Nart [**26**] han dado la factorización de cualquier primo racional en un campo cúbico, pero no proporcionan generadores para cada factor ideal primo; S. Alaca *et al* [**1**] dan la factorización explícita de $2\mathcal{O}_L$ en un campo cúbico de índice 2; Guardia *et al* [**27**] han construido un algoritmo para obtener los generadores de los P_i y el discriminante del campo. Este algoritmo es la factorización p-ádica basada en la teoría de los polígonos de Newton de orden superior. Aguilar-Pineda [**3**] dan la ramificación de $2\mathcal{O}_L$ en ciertas extensiones de grado 8.

Bien, pues este trabajo trata de eso; factorizar explícitamente ideales en el anillo de enteros de un campo de números generado por un polinomio de la forma $x^4 + px^2 + p$, en donde p es un primo racional positivo e impar. La importancia de este polinomio radica en que podemos calcular fácilmente sus raíces para obtener el campo de descomposición del polinomio, en donde el grupo de Galois resultante es C_4 o D_8. La importancia de esta investigación, tal como lo planteó Dedekind, consiste en hacer aritmetica explícita para factorizar ideales y dar generadores de ellos en extensiones descritas anteriormente.

En el capítulo 1 damos cuenta de los antecedentes necesarios, destacando el cálculo del grupo de Galois del polinomio $x^4 + px^2 + p$: si $p = 4 + n^2$, entonces el grupo de Galois es C_4, el grupo cíclico de orden 4 y si p no es de la forma $4 + n^2$, entonces el grupo de Galois es el grupo dihédrico de orden 8.

En el capítulo 2 trabajamos el caso cíclico. Sea K el campo de descomposición del polinomio $f(x) = x^4 + px^2 + p$ con $p = 4 + n^2$ un primo racional. Entonces $K/\mathbb{Q}$ es una extensión cíclica de grado 4 cuyo discriminante es p^3, así, el único primo ramificado es p. Damos explícitamente la ramificación del ideal $q\mathcal{O}_K$ y proporcionamos generadores de sus factores primos. Adicionalmente damos la descomposición de manera explícita de los

primos no ramificados . Para esto, usamos el Teorema de Dedekind para cualquier primo racional $q \neq 3$. Para descomponer el ideal $3\mathcal{O}_K$, planteamos como estrategia buscar otro generador adecuado para K y es aquí en donde estudiamos el índice del campo. En el camino pudimos encontrar bases enteras de algunas familias de ideales, lo cual considero que es un problema importante en la teoría de números algebraicos pues en el caso particular del anillo de enteros (que es un ideal), conociendo una base entera, solo es cosa de calcular un determinante para conocer el discriminante del campo, el cual tiene codificada la información de qué primos se ramifican. En el estudio del índice de K queremos resaltar lo siguiente que nos parece importante. De acuerdo a Lavalle *et al* en [**25**] y hasta donde tenemos conocimiento, no se sabe si existe una infinidad de campos cuárticos cíclicos monogénicos; un caso conocido es el campo ciclotómico con $p = 5 = 4 + 1^2$ ver [**28**], Proposition 3.1, el cual coincide con la clase de primos que nos interesa estudiar. Al principio del capítulo 2 presentamos una tabla con los 36 primeros primos racionales de la forma $4 + n^2$, los cuales son fáciles de generar con SAGE. De estos 36 primos, 22 de ellos son de la forma $3k + 2$ y son precisamente estos primos con los que producimos extensiones cíclicas y coincidentemente monogénicas cuando el índice del generador es 1. Aunque está fuera del objetivo de este trabajo, creemos que podemos construir extensiones cíclicas monogénicas cuarticas con primos de la forma $p = 4 + n^2 = 3k + 2$.

En el capítulo 3 estudiamos el caso diédrico. Primero calculamos el discriminante δ_L de la extensión $L/\mathbb{Q}$ sin hacer uso de una base entera del anillo de enteros $\mathcal{O}_L$. Este dato es muy importante porque δ_L es un entero > 1 y en su factorización como producto de primos, aparecen exactamente los primos racionales que son ramificados. En el momento de escribir esta introducción, aún desconocemos una base entera de $L/\mathbb{Q}$. Debemos destacar que para estudiar la ramificación en L, fue de gran ayuda estudiar la ramificación en el campo intermedio $K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4})$ el cual es una extensión de grado 4 sobre $\mathbb{Q}$ y $[L : K] = 2$. En los Teoremas 3.9 y 3.33 obtuvimos que si $p \equiv 3 \pmod 4$, entonces

$$\delta_K = 2^4(p-4)^2p^2 \quad \text{y} \quad \delta_L = 2^{12}(p-4)^4p^6,$$

y si $p \equiv 1 \pmod 4$, entonces

$$\delta_K = (p-4)^2p^2 \quad \text{y} \quad \delta_L = (p-4)^4p^6.$$

Como era de esperarse, en cualquiera de los dos casos $\delta_K \mid \delta_L$. Esta es la razón por la cual primero estudiamos la ramificación en K y después subimos al campo L. Aún cuando no conocemos la factorización de $p-4$, sabemos que los únicos primos ramificados de $\mathbb{Q}$ a L son $2, p$ y los factores primos $q \mid p-4$ si $p \equiv 3 \pmod 4$ y cuando $p \equiv 1 \pmod 4$, solo los primos ramificados son los primos q tal que $q \mid p-4$ y p. El camino que seguimos fue el siguiente: primero estudiamos la ramificación de los primos racionales $q > 3$ tales que $q \mid p-4$, a continuación damos la ramificación de $q = 3$ y por último damos la ramificación de los primos 2 y p.

Capítulo 1

Antecedentes

En este capítulo los resultados que establecemos son válidos en característica cero y algunos son válidos en cualquier característica, lo cual indicaremos en cada caso. Nuestro interés son los campos de números, es decir, extensiones finitas de $\mathbb{Q}$.

1.1. La norma, la traza y el discriminante

Sean L/K una extensión de campos de números con $[L:K]=n$ y $\mathcal{B}=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ una base de L como K-espacio vectorial. Para $\alpha\in L$ definimos la transformación lineal $T_\alpha: L\to L$ como:

$$T_\alpha(\alpha_i)=\alpha\alpha_i=\sum_{j=1}^{n}a_{ji}\alpha_j,$$

donde a_{ji} son los coeficientes de $\alpha\alpha_i$ con respecto a la base $\mathcal{B}$. Denotaremos por (a_{ij}) a la matriz cuyas entradas son los coeficientes a_{ij}. Usando lo anterior definiremos dos funciones que serán muy importantes a lo largo de este trabajo.

Definición 1.1. *La norma de $\alpha\in L$ es $N(\alpha)=\det(a_{ij})$ y la traza de α es $tr(\alpha)=\sum_{i=1}^{n}a_{ii}$.*

La siguiente proposición nos muestra que la norma y la traza de un elemento en L no dependen de la base que elijamos.

Proposición 1.2. *Sean $\{\alpha_1,\ldots,\alpha_n\}$, $\{\beta_1,\ldots,\beta_n\}$ bases de L/K y $\alpha\in L$. Si A es la matriz asociada a T_α con respecto a la base $\{\alpha_1,\ldots,\alpha_n\}$ y B la matriz asociada a T_α con respecto a la base $\{\beta_1,\ldots,\beta_n\}$, entonces $\det(A)=\det(B)$ y $tr(A)=tr(B)$.*

Demostración. Si N es la matriz combio de base, entonces $A=N^{-1}BN$ y

$$\det(A)=\det(N^{-1}BN)=\det(N)^{-1}\det(B)\det(N)=\det(B)$$

y

$$tr(A)=tr(N^{-1}BN)=tr(NN^{-1}B)=tr(IB)=tr(B).$$

□

El resultado que a continuación presentamos, da una forma más sencilla de cómo calcular la norma y la traza de un elemento.

Proposición 1.3. *Sea L/K una estensión de Galois de campos de números con $[L:K]=n$ y $G=Gal(L/K)=\{\sigma_1,\ldots,\sigma_n\}$. Si $\alpha\in L$, entonces*

$$N(\alpha)=\prod_{i=1}^{n}\sigma_i(\alpha)\quad y\quad tr(\alpha)=\sum_{i=1}^{n}\sigma_i(\alpha).$$

Demostración. Esta demostración la haremos en dos partes la primera consiste en demostrar la proposición suponiendo que α es un elmento primitivo y luego demostraremos el caso general.

Si α es un elemento primitivo, entones $L = K(\alpha)$ y $\{1, \alpha \ldots, \alpha^{n-1}\}$ es una base de la extensión. Supongamos que

$$Irr(\alpha, K) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n.$$

Se conocen las siguientes relaciones entre las raíces de un polinomio y sus coeficientes

$$a_0 = (-1)^n \prod_{i=1}^{n} \beta_i, \quad a_{n-1} = \sum_{i=1}^{n} (-1)^n \beta_i$$

donde $\beta_i (1 \leq i \leq n)$ son las distintas raíces del polinomio. Por lo anterior

$$a_0 = (-1)^n \prod_{i=1}^{n} \alpha^{(i)}, \quad a_{n-1} = \sum_{i=1}^{n} (-1)^n \alpha^{(i)}$$

Ahora, como

$\alpha \cdot 1 = 0 \cdot 1 + 1 \cdot \alpha + 0 \cdot \alpha^2 + \cdots + 0 \cdot \alpha^{n-1}$
$\alpha \cdot \alpha = 0 \cdot 1 + 0 \cdot \alpha + 1 \cdot \alpha^2 + \cdots + 0 \cdot \alpha^{n-1}$
$\vdots$
$\alpha \cdot \alpha^{n-2} = 0 \cdot 1 + 0 \cdot \alpha + 0 \cdot \alpha^2 + \cdots + 1 \cdot \alpha^{n-1}$
y además
$\alpha \cdot \alpha^{n-1} = -a_0 \cdot 1 - a_1 \cdot \alpha - a_2 \cdot \alpha^2 - \cdots - a_{n-1} \cdot \alpha^{n-1}$
por lo tanto

$$(a_{ij}) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

El determinante y la traza de esta matríz son

$$det(a_{ij}) = (-1)^n a_0 \quad \text{y} \quad tr(a_{ij}) = -a_{n-1}.$$

De esto se sigue que

$$N(\alpha) = (-1)^n a_0 = (-1)^{2n} \prod_{i=1}^{n} \alpha^{(i)} = \prod_{i=1}^{n} \alpha^{(i)},$$

$$tr(\alpha) = -a_{n-1} = -\sum_{i=1}^{n} (-1)\alpha^{(i)} = \sum_{i=1}^{n} \alpha^{(i)},$$

lo que demuestra el resultado cuando α es un elemento primitivo.

Ahora sea $\alpha \in L$,no necesariamente primitivo. La extensión L/K se puede dividir en dos partes, la primera $K(\alpha)/K$ y la segunda $L/K(\alpha)$. Se observa que si $[K(\alpha) : K] = d$ y $[L : K] = n$, entonces $[L : K(\alpha)] = \dfrac{n}{d} = r$.

Ahora si $\{1, \alpha, \cdots, \alpha^{d-1}\}$ es una base de $K(\alpha)/K$ y $\{\beta_1, \cdots, \beta_r\}$ es una base de la extensión $L/K(\alpha)$, entonces

$$\{\beta_k \alpha^j | 1 \leq k \leq r, 0 \leq j \leq d-1\}$$

es una base de L/K, la cual se puede escribir como una unión de subconjuntos de la siguiente manera

$$\{\beta_k\alpha^j\} = \{\beta_1\alpha^j | 0 \leq j \leq d-1\} \cup \cdots \cup \{\beta_r\alpha^j | 0 \leq j \leq d-1\}.$$

Observemos que $\alpha(\beta_k\alpha^j) = \beta_k(\alpha\alpha^j)$. Además, las entradas de la matríz (a_{ij}) con respecto a $K(\alpha)/K$ se encuentran tomando en cuenta que

$$\alpha\alpha^j = \sum_{i=0}^{d-1} a_{(i+1)(j+1)}\alpha^j.$$

Así,

$$\alpha(\beta_k\alpha^j) = \sum_{i=0}^{d-1} a_{(i+1)(j+1)}\beta_k\alpha^j.$$

Sea $\gamma_l = \beta_k\alpha^j$. Entonces $\alpha\gamma_l = \sum_{i=0}^{d-1} a_{(i+1)(j+1)}\beta_k\alpha^j$ y $\beta_k\alpha^j = \gamma_{dk+j}$. Sea $c_{lm} = a_{ij}$ con $l \equiv i \pmod{d}$ y $m \equiv j \pmod{d}$ con $kd \leq l, m < (k+1)d$. Se puede observar que

$$(c_{ij}) = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}$$

es la matríz asociada a la transformación T_α con respecto a la base $\{\beta_k\alpha^j\}$, donde A es la matíz de T_α con la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ con respecto a la extensión de campos $K(\alpha)/K$.

Así que

$$tr_{L/K}(\alpha) = r \cdot tr(A) \quad \text{y} \quad N_{L/K}(\alpha) = (det(A))^r.$$

Los automorfismos de $K(\alpha)/K$ se pueden extender a L/K r veces cada uno de ellos. Así que si tomamos un automorfismo de $K(\alpha)/K$, digamos $\sigma_i(x)$, existen r automorfismos de L/K, digamos $\sigma_{ij}(x)$ con $1 \leq j \leq r$, tales que al restringirlos a $K(\alpha)$

$$\sigma_{ij}(x)|_{K(\alpha)} = \sigma_i(x).$$

Utilizando esta característica de los automorfismos se puede calcular la traza y la norma de α de la siguiente manera

$$tr_{L/K}(\alpha) = r \cdot tr(A) = r \cdot tr_{K(\alpha)/K}(\alpha) = r \cdot \sum_{i=1}^{d} \sigma_i(\alpha) = \sum_{1\leq i\leq d} \sum_{1\leq j\leq r} \sigma_{ij}(\alpha)$$

$$N_{L/K}(\alpha) = (det(A))^r = (N_{K(\alpha)/K}(\alpha))^r = (\prod_{i=1}^{d} \sigma_i(\alpha))^r = \prod_{1\leq i\leq d} \prod_{1\leq j\leq r} \sigma_{ij}(\alpha)$$

que es el resultado que se buscaba. □

El siguiente resultado nos proporsiona algunas de las propiedades fundamentales de $N(\alpha)$ y $tr(\alpha)$.

Teorema 1.4. *Sea L/K una extensión de campos de números de grado n. Si $\alpha, \beta \in L$ y $a \in K$, entonces:*

(i) $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$.

(ii) $tr(a\alpha) = a \cdot tr(\alpha)$.
(iii) $N(a\alpha) = a^n \cdot N(\alpha)$.
(iv) $N(\alpha\beta) = N(\alpha)N(\beta)$.
(v) *Si* $\alpha \neq 0$*, entonces* $N(\alpha^{-1}) = N(\alpha)^{-1}$.
(vi) $N(a) = a^n$.
(vii) $tr(a) = n \cdot a$.

Demostración. Se sigue inmediatamente de la definición de norma y traza. □

De (i) y (ii) del Teorema 1.4 podemos deducir que la traza es lineal.

Definición 1.5. *Sea L/K una extensión de campos de números de grado n y $\{\alpha_1, \ldots, \alpha_n\}$ un subcoonjunto de L. Definimos el discriminante de $\{\alpha_1, \ldots, \alpha_n\}$ como:*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(tr(\alpha_i\alpha_j))$$

Proposición 1.6. *Sea L/K una extensión finita de grado n. Entonces*

(i) *Si $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base de L sobre K.*
(ii) *En cualquier característica, si L/K es separable y $\{\alpha_1, \ldots, \alpha_n\}$ es una base de L sobre K, entonces $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.*

Demostración. (i) Si $\alpha_1, \ldots, \alpha_n$ son linealmente dependientes, entonces para algún $a_i \neq 0$ tenemos

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = 0.$$

Si multiplicamos esta ecuación por α_j tenemos

$$a_1\alpha_1\alpha_j + a_2\alpha_2\alpha_j + \ldots + a_n\alpha_n\alpha_j = 0.$$

Por lo tanto, para $j = 1, \ldots, n$ tenemos

$$tr(a_1\alpha_1\alpha_j + a_2\alpha_2\alpha_j + \ldots + a_n\alpha_n\alpha_j) = \sum_{i=1}^{n} a_i tr(\alpha_i\alpha_j) = tr(0) = 0$$

Lo anterior significa que $a_1, \ldots, a_n$ es una solución no trivial del sistema

$$\begin{aligned} tr(\alpha_1\alpha_1)x_1 + \cdots + tr(\alpha_n\alpha_1)x_n &= 0 \\ tr(\alpha_1\alpha_2)x_1 + \cdots + tr(\alpha_n\alpha_2)x_n &= 0 \\ &\vdots \\ tr(\alpha_1\alpha_n)x_1 + \cdots + tr(\alpha_n\alpha_n)x_n &= 0 \end{aligned}$$

Si $A = (tr(\alpha_i\alpha_j))$, tenemos $\det(A) = 0 = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

(ii) Si L/K es separable, $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ y $\{\alpha_1, \ldots, \alpha_n\}$ es base de L/K, entonces el sistema

$$\sum_{i=1}^{n} x_i tr(\alpha_i\alpha_j) = 0$$

tiene al menos una solución no trivial $(a_1, \ldots, a_n)$, donde $a_i \neq 0$ para algún i. Consideramos $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \neq 0$. Dado que la traza es lineal, tenemos

$$tr(\alpha\alpha_j) = \sum_{i=1}^{n} a_i tr(\alpha_i\alpha_j) = 0.$$

Sea $\beta = \sum_{i=1}^{n} b_i\alpha_i \in L$. Entonces $\alpha\beta = \sum_{i=1}^{n} b_i\alpha\alpha_i$. Por tanto

$$tr(\alpha\beta) = \sum_{i=1}^{n} b_i tr(\alpha\alpha_i) = \sum_{i=1}^{n} b_i \cdot 0 = 0.$$

En particular, si $\beta = \dfrac{1}{\alpha}$ tenemos $0 = tr(\alpha\beta) = tr(\alpha\frac{1}{\alpha}) = tr(1) = [L : K] = n$, lo cual no puede ser porque la extensión es separable. □

Las siguientes proposiciones nos dan las propiedades más importantes del discriminante de una base.

Proposición 1.7. *Sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ bases de una extensión finita L/K. Entonces*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2\Delta(\beta_1, \ldots, \beta_n),$$

donde (a_{ij}) es la matriz cambio de base.

Demostración. Notemos que $\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i$ y $\alpha_k = \sum_{l=1}^{n} a_{lk}\beta_l$ por tanto:

$$\alpha_j\alpha_k = \sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{lk}\beta_i\beta_l.$$

Al tomar la traza en ambos lados:

$$tr(\alpha_j\alpha_k) = \sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{lk}tr(\beta_i\beta_l).$$

Sean $A = (tr(\alpha_j\alpha_k))$, $B = (tr(\beta_i\beta_l))$ y $C = (a_{ij})$; obsevemos que $A = CBC^T$. Finalmente, usando propiedades del determinante,

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2\Delta(\beta_1, \ldots, \beta_n).$$

□

Proposición 1.8. *Sea L/K separable de grado n. Si $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$, entonces*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\alpha_i^{(j)})^2$$

donde $\alpha_i^{(j)} = \sigma_j(\alpha_i)$ y $\{\sigma_1, \ldots, \sigma_n\}$ son los K-isomorfismos distintos de L a una cerradura algebraica de K.

Demostración. Ver [**21**], Proposición 12.1.3, pág. 173. □

1.2. Anillo de enteros asociado a un campo de números

En esta sección veremos qué es el anillo de enteros de un campo de números y cuáles son las propiedades que cumple dicho anillo.

Definición 1.9. *Sea A un anillo conmutativo y B subanillo de A. El elemento $u \in A$ es entero sobre B si existe $f(x) \in B[x]$ mónico tal que $f(u) = 0$.*

El caso particular que $A = \mathbb{C}$ y $B = \mathbb{Z}$, el conjunto de números complejos enteros sobre $\mathbb{Z}$ es nuestro objeto principal de estudio en este trabajo. Así tenemos nuestra definición particular:

Definición 1.10. *$z \in \mathbb{C}$ es un entero algebraico si z es raíz de algún polinomio mónico con coeficientes enteros. Definimos*

$$\Omega = \{z \in \mathbb{C} : z \text{ es un entero algebraico}\}.$$

Proposición 1.11. *Sean $R \subseteq T$ anillos conumutativos y u un elemento de un anillo que contiene a T. Supongamos que u es entero sobre T y T es entero sobre R. Entonces u es entero sobre R.*

Demostración. Ver [**4**], Corolario 5.4. pág. 67. □

Definición 1.12. *Un $\mathbb{Z}$-módulo finitamente generado, es un subconjunto no vacío $W \subseteq \mathbb{C}$ tal que:*

i) *Si $a \in \mathbb{Z}$ y $\gamma \in W$, entonces $a\gamma \in W$.*
ii) *Si $\gamma_1, \gamma_2 \in W$, entonces $\gamma_1 + \gamma_2 \in W$.*
iii) *Existen $\gamma_1, \gamma_2, \ldots, \gamma_n \in W$ tales que $W = \gamma_1\mathbb{Z} + \gamma_2\mathbb{Z} + \cdots + \gamma_n\mathbb{Z}$.*

A los números $\gamma_1, \ldots, \gamma_n$ de iii) les llamaremos generadores de W.

Proposición 1.13. *Sean W un $\mathbb{Z}$-módulo finitamente generado, con $W \neq \{0\}$ y $\omega \in \mathbb{C}$ tal que $\omega\gamma \in W$ para todo $\gamma \in W$. Entonces $\omega \in \Omega$.*

Demostración. Sean $\gamma_1, \ldots, \gamma_n$ una base de W. Por hipótesis, $\omega\gamma_i \in W$ para $1 \leq i \leq n$. Lo que implica

$$\omega\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j \tag{1}$$

con $a_{ij} \in \mathbb{Z}$. Sea δ_{ij} la función delta de Kronecker. Entonces

$$\omega\gamma_i = \delta_{ii}\omega\gamma_i = \sum_{j=1}^{n} \delta_{ij}\omega\gamma_j. \tag{2}$$

De las ecuaciones (1) y (2)

$$0 = \sum_{j=1}^{n} \delta_{ij}\omega\gamma_j - \sum_{j=1}^{n} a_{ij}\gamma_j = \sum_{j=1}^{n} (\delta_{ij}\omega - a_{ij})\gamma_j.$$

Si $A = (\delta_{ij}\omega - a_{ij})$, observamos que $\det(A) = 0$ y $\det(\delta_{ij}x - a_{ij})$ es un polinomio mónico de grado n con coeficientes enteros del cual ω es raíz. Por lo tanto $\omega \in \Omega$.

□

Proposición 1.14. *Ω es un anillo conmutativo con identidad que contiene a los enteros racionales como subanillo.*

Demostración. Ver [**36**], Theorem 2.9, pág. 43.

□

Definición 1.15. *Sea K un subcampo de $\mathbb{C}$. Diremos que K es un campo de números si $[K:\mathbb{Q}] < \infty$. El anillo de enteros de un campo de números K es el conjunto*

$$\mathcal{O}_K = \{\alpha \in K : \alpha \textit{ es un entero algebraico}\}.$$

El conjunto $\mathcal{O}_K$ tiene estructura de anillo pues claramente $\mathcal{O}_K = K \cap \Omega$.

Lema 1.16. *Sea $\beta \in K$. Existe $b \in \mathbb{Z} \setminus \{0\}$ tal que $b\beta \in \mathcal{O}_K$.*

Demostración. Como $\beta \in K$, entonces $f(\beta) = b_0 + b_1\beta + \cdots + b_n\beta^n = 0$ en donde $f(x) = b_0 + b_1x + \cdots + b_nx^n \in \mathbb{Z}[x]$. Por tanto

$$\begin{aligned} 0 &= b_0b_n^{n-1} + b_1b_n^{n-1}\beta + \cdots + b_nb_n^{n-1}\beta^n \\ &= b_0b_n^{n-1} + b_1b_n^{n-2}(b_n\beta) + b_2b_n^{n-3}(b_n\beta)^2 + \cdots + (b_n\beta)^n. \end{aligned}$$

Si $h(x) = b_0b_n^{n-1} + b_1b_n^{n-2}x + b_2b_n^{n-3}x^2 + \cdots + x^n$, entonces $h(b_n\beta) = 0$ y $b_n\beta \in \mathcal{O}_K$. □

Corolario 1.17. *Sean $\beta_1, \beta_2, \ldots, \beta_r \in K$. Existe $b \in \mathbb{Z} \setminus \{0\}$ tal que*

$$b\beta_1, b\beta_2, \ldots, b\beta_r \in \mathcal{O}_K.$$

Demostración. Sea $b_i \in \mathbb{Z} \setminus \{0\}$ tal que $b_i\beta_i \in \mathcal{O}_K$. Si $b = mcm(b_1, \ldots, b_r)$, entonces $b_i \mid b$ de donde $b = b_it_i$, para algún $t_i \in \mathbb{Z}$. Como $b_i\beta_i \in \mathcal{O}_K$, tenemos $b_it_i\beta_i \in \mathcal{O}_K$ y por el Lema 1.16, $b\beta_i = b_it_i\beta_i \in \mathcal{O}_K$. □

Proposición 1.18. *Sea $I \neq 0$ un ideal de $\mathcal{O}_K$. Entonces I contiene una base de K.*

Demostración. Sea $\{\beta_1, \ldots, \beta_n\}$ base de $K/\mathbb{Q}$ y $b \in \mathbb{Z} \setminus \{0\}$ tal que para $l \in I \setminus \{0\}$, $lb\beta_1, lb\beta_2, \ldots, lb\beta_n$ es base. □

Lema 1.19. *Un número racional $\alpha \in \mathbb{Q}$ es un entero algebraico si y solo si $\alpha \in \mathbb{Z}$.*

Demostración. Si $\alpha \in \mathbb{Q}$ es un entero algebraico, α satisface un polinomio mónico con coeficientes enteros, digamos $f(x) = b_0 + b_1x + \cdots + x^n$, con $b_i \in \mathbb{Z}$. Sea $\alpha = \dfrac{c}{d}$, con $c, d \in \mathbb{Z}$ y $mcd(c,d) = 1$. Por tanto

$$b_0 + b_1\left(\frac{c}{d}\right) + \cdots + \left(\frac{c}{d}\right)^n = 0$$

Multiplicamos por d^n la ecuación anterior,

$$\begin{aligned} c^n &= -(b_0d^n + b_1cd^{n-1} + \cdots + b_{n-1}c^{n-1}d) \\ &= -d(b_0d^{n-1} + b_1cd^{n-2} + \cdots + b_{n-1}c^{n-1}) \end{aligned}$$

y tenemos $d \mid c^n$. Dado que $mcd(c,d) = 1$, se tiene $mcd(c^n, d) = 1$. Así, $d \mid 1$. Por lo tanto, $d = \pm 1$, es decir $\alpha \in \mathbb{Z}$.

Ahora si $\alpha \in \mathbb{Z}$, él satisface al polinomio $f(x) = x - \alpha \in \mathbb{Z}[x]$, se concluye que α es un entero algebraico. □

A partir de ahora, diremos que un elemento en $\mathbb{Z}$ es un entero racional para no confundirlos con los enteros algebraicos.

Proposición 1.20. *Sea $\alpha \in \mathcal{O}_K$. Entonces $N(\alpha)$, $tr(\alpha) \in \mathbb{Z}$.*

Demostración. Si $\alpha \in \mathcal{O}_K$, α satisface un polinomio mónico con coeficientes enteros $f(x) = a_0 + a_1x + \cdots + x^n$, de donde $0 = a_0 + a_1\alpha + \cdots + \alpha^n$. Sea $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$. Entonces

$$0 = \sigma(a_0 + a_1\alpha + \cdots + \alpha^n) = a_0 + a_1\sigma(\alpha) + \cdots + \sigma(\alpha)^n,$$

es decir, $\sigma(\alpha) \in \mathcal{O}_K$ y dado que $N(\alpha) = \prod_{\sigma\in\mathrm{Aut}(K/\mathbb{Q})} \sigma(\alpha)$ y $tr(\alpha) = \sum_{\sigma\in\mathrm{Aut}(K/\mathbb{Q})} \sigma(\alpha)$ tenemos $N(\alpha), tr(\alpha) \in \mathcal{O}_K$.

Por otro lado $N(\alpha), tr(\alpha) \in \mathbb{Q}$. Por lo tanto, por el lema anterior, $N(\alpha), tr(\alpha) \in \mathbb{Z}$. □

Corolario 1.21. *Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathcal{O}_K$ una base de K sobre $\mathbb{Q}$. Entonces,*

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}.$$

Demostración. Sabemos que $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(tr(\alpha_i\alpha_j))$ y por la Proposición 1.20, $tr(\alpha_i\alpha_j) \in \mathbb{Z}$. Por lo tanto, $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$. □

Teorema 1.22. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_K$ y $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq I$ una base de $K/\mathbb{Q}$ de tal forma que $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ es mínimo. Entonces, $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\,\alpha_n$.*[1]

Demostración. Como $\alpha_i \in I$ e I es un ideal, $\mathbb{Z}\alpha_i \subseteq I$. Entonces, $I \supseteq \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. Inversamente, si $\alpha \in I$, escribimos $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, con $a_i \in \mathbb{Q}$. Probaremos que $a_i \in \mathbb{Z}$. Supongamos que $a_i \notin \mathbb{Z}$ para algún $i = 1, \ldots, n$. Sin pérdida de generalidad, supongamos que $a_1 \notin \mathbb{Z}$, es decir $a_1 = m + \theta$, donde $m \in \mathbb{Z}$ y $\theta \in (0, 1)$. Sean

$$\beta_1 = \alpha - m\alpha_1, \quad \beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n.$$

Como $m \in \mathcal{O}_K$ e I es un ideal de $\mathcal{O}_K$, tenemos $m\alpha_1 \in I$ y, por tanto, $\alpha - m\alpha_1 \in I$, es decir, $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\} \subseteq I$. Veremos que $\mathcal{B}$ es una base para $K/\mathbb{Q}$. Supongamos que $0 = q_1\beta_1 + q_2\beta_2 + \cdots + q_n\beta_n$, con $q_i \in \mathbb{Q}$, para $i = 1, \ldots, n$. Así,

$$\begin{aligned} 0 &= q_1(\alpha - m\alpha_1) + q_2\alpha_2 + \cdots + q_n\alpha_n \\ &= q_1(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) - q_1m\alpha_1 + q_2\alpha_2 + \cdots + q_n\alpha_n \\ &= (q_1a_1 - q_1m)\alpha_1 + (q_1a_2 + q_2)\alpha_2 + \cdots + (q_1a_n + q_n)\alpha_n \end{aligned}$$

y dado que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de $K/\mathbb{Q}$, tenemos $q_1a_1 - q_1m = 0$ y $q_1a_j + q_j = 0$ para $j = 2, \ldots, n$. Por tanto, $q_j = 0$ para cada $j = 1, \ldots, n$ y, como $[K : \mathbb{Q}] = n$, tenemos $\mathcal{B}$ es una base para $K/\mathbb{Q}$.

Por otro lado, la matriz cambio de base de $\{\beta_1, \beta_2, \ldots, \beta_n\}$ a $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es

$$A = \begin{pmatrix} \theta & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Dado que $\det(A) = \theta$, por la Proposición 1.7, $|\Delta(\beta_1, \beta_2, \ldots, \beta_n)| = \theta^2|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ y $\theta \in (0, 1)$. De lo anterior,

$$|\Delta(\beta_1, \beta_2, \ldots, \beta_n)| < |\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|,$$

[1]Notemos que $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\,\alpha_n$ es una suma directa, ya que $\{\alpha_1, \ldots, \alpha_n\}$ es una base.

lo cual es una contradicción al hecho de que $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ es mínimo. Entonces, tenemos $a_i \in \mathbb{Z}$ para $i = 1, \ldots, n$. Así, $I \subseteq \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. Por lo tanto, $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. □

Definición 1.23. *Si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq I$ es una base de $K/\mathbb{Q}$ tal que $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ es mínimo, entonces llamaremos a $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base entera de I.*

Observemos que $\mathcal{O}_K$ es un ideal de sí mismo, por lo tanto $\mathcal{O}_K$ contiene una base entera, la cual se llama base entera de $K/\mathbb{Q}$.

Proposición 1.24. *Sea $\{\alpha_1, \ldots, \alpha_n\} \subseteq I$ una $\mathbb{Q}$-base de K tal que $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de I.*

Demostración. Sea $\{\beta_1, \ldots, \beta_n\} \subseteq I$ una $\mathbb{Q}$-base cualquiera de K. Veremos que

$$|\Delta(\alpha_1, \ldots, \alpha_n)| \leq |\Delta(\beta_1, \ldots, \beta_n)|.$$

Notemos que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, con $a_{ij} \in \mathbb{Z}$, entonces

$$\Delta(\beta_1, \ldots, \beta_n) = (\det(a_{ij}))^2 \Delta(\alpha_1, \ldots, \alpha_n)$$

y como $a_{ij} \in \mathbb{Z}$, tenemos $(\det(a_{ij}))^2 \geq 1$. Así, $\Delta(\beta_1, \ldots, \beta_n) \geq \Delta(\alpha_1, \ldots, \alpha_n)$ y por tanto $|\Delta(\alpha_1, \ldots, \alpha_n)| \leq |\Delta(\beta_1, \ldots, \beta_n)|$. □

Con el Teorema 1.22 y la proposición anterior tenemos que $\{\alpha_1, \ldots, \alpha_n\} \subseteq I$ es base entera de I si y solo si $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

Definición 1.25. *Sea K un campo de números de grado n. Diremos que K es monogénico si existe algún $\alpha \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\alpha)$ y*

$$\mathcal{O}_K = \mathbb{Z} + \alpha\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z},$$

es decir, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base entera de $\mathcal{O}_K$.

Corolario 1.26. *Sean $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$,$\{\beta_1, \beta_2, \ldots, \beta_n\}$ dos bases enteras de $K/\mathbb{Q}$. Entonces $\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

Demostración. Sean $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, con $a_{ij} \in \mathbb{Z}$, $\beta_j = \sum_{k=1}^{n} b_{jk}\alpha_k$. Por la Proposición 1.7,

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) = (\det(a_{ij}))^2 \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

y

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\det(b_{ij}))^2 \Delta(\beta_1, \beta_2, \ldots, \beta_n).$$

Por tanto $\det((a_{ij})^2(b_{jk})^2) = 1$, de donde $\det(a_{ij}) = \pm 1$. Así

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

□

Definición 1.27. *El discriminante de $K/\mathbb{Q}$ es el discrimininante de una base entera y lo denotaremos por δ_K.*

Lema 1.28. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_K$. Entonces $I \cap \mathbb{Z} \neq \{0\}$.*

Demostración. Si $\alpha \in I \neq \{0\}$, α satisface un polinomio $f(x) = a_0 + a_1x + \cdots + x^n \in \mathbb{Z}[x]$ irreducible. Puesto que $a_0 \neq 0$, tenemos

$$0 = f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n,$$
$$a_0 = -(a_1\alpha + \cdots + a_n\alpha^n) \in I.$$

Por lo tanto, $a_0 \in I \cap \mathbb{Z}$. □

Lema 1.29. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_K$, con $[K : \mathbb{Q}] = n$. Entonces $|\mathcal{O}_K/I|$ es finito.*

Demostración. Por el lema 1.28 existe $a \in I \cap \mathbb{Z}$, con $a > 0$. Sea $\langle a \rangle$ el ideal principal generado por a en $\mathcal{O}_K$, es decir $a\mathcal{O}_K = \langle a \rangle$. Definimos

$$\varphi : \mathcal{O}_K/\langle a \rangle \longrightarrow \mathcal{O}_K/I$$
$$x + \langle a \rangle \mapsto x + I.$$

La función φ está bien definida pues si $x_1 + \langle a \rangle = x_2 + \langle a \rangle$, entonces $x_1 - x_2 \in \langle a \rangle \subseteq I$ y por tanto $x_1 + I = x_2 + I$, es decir $\varphi(x_1 + \langle a \rangle) = \varphi(x_2 + \langle a \rangle)$. Además es claro que φ es una función sobre, por lo que $|\mathcal{O}_K/I| \leq |\mathcal{O}_K/\langle a \rangle|$, así que para probar que $\mathcal{O}_K/I$ es finito basta probar que $\mathcal{O}_K/\langle a \rangle$ lo es.

Sean $\{\omega_1, \ldots, \omega_n\}$ una base entera de $K/\mathbb{Q}$, es decir $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$, con $\omega_i \in \mathcal{O}_K$ y

$$S = \left\{ \sum_{i=1}^{n} \gamma_i\omega_i : 0 \leq \gamma_i < a \right\}.$$

Observemos que S es un conjunto de representantes de $\mathcal{O}_K/\langle a \rangle$ y que $|S| = a^n$. Tomemos $\omega \in \mathcal{O}_K$, $\omega = m_1\omega_1 + \cdots + m_n\omega_n$, con $m_i \in \mathbb{Z}$ para $i = 1, \ldots, n$. Por el algoritmo de la división en $\mathbb{Z}$, $m_i = q_ia + \gamma_i$, con $0 \leq \gamma_i < a$.

$$\begin{aligned} \omega + \langle a \rangle &= (m_1\omega_1 + \cdots + m_n\omega_n) + \langle a \rangle \\ &= (m_1\omega_1 + \langle a \rangle) + \cdots + (m_n\omega_n + \langle a \rangle) \\ &= ((q_1a + \gamma_1)\omega_1 + \langle a \rangle) + \cdots + ((q_na + \gamma_n)\omega_n + \langle a \rangle). \end{aligned}$$

Como $(q_ia + \gamma_i)\omega_i + \langle a \rangle = q_ia\omega_i + \gamma_i\omega_i + \langle a \rangle = \gamma_i\omega_i + \langle a \rangle$, tenemos

$$\omega + \langle a \rangle = (\gamma_1\omega_1 + \langle a \rangle) + \cdots + (\gamma_n\omega_n + \langle a \rangle) = \sum_{i=1}^{n} \gamma_i\omega_i + \langle a \rangle$$

y $\sum_{i=1}^{n} \gamma_i\omega_i \in S$. Por otro lado, si $\sum_{i=1}^{n} \gamma_i\omega_i = \sum_{i=1}^{n} \gamma_i'\omega_i$, con $0 \leq \gamma_i < a$ y $0 \leq \gamma_i' < a$, se cumple $\gamma_i = \gamma_i'$ ya que $\{\omega_1, \ldots, \omega_n\}$ es una base. Por tanto, $|S| = a^n$ y $|\mathcal{O}_K/\langle a \rangle| = |S|$. Así, $|\mathcal{O}_K/I| \leq a^n$. □

Observemos que si $P \neq \{0\}$ es un ideal primo de $\mathcal{O}_K$, entonces $P \cap \mathbb{Z} = p\mathbb{Z}$, con p un primo racional.

Definición 1.30. *Sea I un ideal no cero de $\mathcal{O}_K$. La norma de I es $|\mathcal{O}_K/I|$ y la denotaremos por $N(I)$.*

Teorema 1.31. *Sea I un ideal no cero de $\mathcal{O}_K$. Entonces $N(I) = \sqrt{\dfrac{\Delta(\beta_1, \ldots, \beta_n)}{\delta_K}}$, donde $\{\beta_1, \ldots, \beta_n\}$ es una base entera de I.*

Demostración. Ver [**36**] Theorem 5.9, pág. 114. □

Proposición 1.32. *Sean I, J ideales no cero de $\mathcal{O}_K$. Entonces*

$$N(IJ) = N(I)N(J).$$

Demostración. Ver [**36**] Theorem 5.12, pág. 116. □

Proposición 1.33. *Sea I un ideal no cero de $\mathcal{O}_K$. Entonces $N(I) \in I$.*

Demostración. Ver [**36**] Theorem 5.14 (b), pág. 118. □

Corolario 1.34. *$\mathcal{O}_K$ es un anillo noetheriano.*

Demostración. Sea $I_1 \neq \{0\}$ un ideal de $\mathcal{O}_K$, por el Lema 1.29, $\mathcal{O}_K\ /I_1$ es finito. Consideremos $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ una cadena ascendente de ideales en $\mathcal{O}_K$. Como I_j/I_1 es un ideal de $\mathcal{O}_K/I_1$ y a lo más hay un número finito de subconjuntos de éste, la cadena $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n = I_{n+1} = \cdots$ se detiene en algún $n \in \mathbb{Z}$. Por lo tanto, $\mathcal{O}_K$ es noetheriano. □

Corolario 1.35. *Si $P \neq \{0\}$ es un ideal primo de $\mathcal{O}_K$, entonces P es máximo.*

Demostración. Como P es primo, entonces $\mathcal{O}_K/P$ es un dominio entero finito, de donde $\mathcal{O}_K/P$ es un campo y por tanto P es un ideal máximo. □

Lema 1.36. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_K$. Si $\beta \in K$, con $\beta \neq 0$ es tal que $\beta I \subseteq I$, entonces $\beta \in \mathcal{O}_K$.*

Demostración. Como I es un $\mathbb{Z}$-módulo, por la Proposición 1.13, $\beta \in \mathcal{O}_K$. □

Lema 1.37. *Sean I, J ideales no cero de $\mathcal{O}_K$ tales que $IJ = I$. Entonces $J = \mathcal{O}_K$.*

Demostración. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de I, es decir, $I = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$. Dado que $\alpha_i \in I = IJ$, existen $b_{ij} \in J$ tales que $\alpha_i = \sum_{i=1}^{n} b_{ij}\alpha_j$. Entonces

$$\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

de donde

$$\begin{pmatrix} b_{11}-1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22}-1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn}-1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

es decir, tenemos el siguiente sistema homogéneo

$$\begin{aligned} 0 &= (b_{11}-1)x_1 + b_{12}x_2 + \cdots + b_{1n}x_n \\ 0 &= b_{21}x_1 + (b_{22}-1)x_2 + \cdots + b_{2n}x_n \\ &\vdots \\ 0 &= b_{n1}x_1 + b_{n2}x_2 + \cdots + (b_{nn}-1)x_n, \end{aligned}$$

el cual tiene una solución no trivial, por lo que

$$\det \begin{pmatrix} b_{11}-1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22}-1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn}-1 \end{pmatrix} = 0.$$

Notemos que un sumando del determinate es $\prod_{i=1}^{n}(b_{ii}-1)$ y como las demás entradas de la matriz están en J, entonces el determinante que queremos calcular tiene la forma

$$\prod_{i=1}^{n}(b_{ii}-1)+r=0 \quad \text{para algún } r \in J.$$

Desarrollando el producto obtenemos $(-1)^n + j = 0$ para algún $j \in J$, de donde $\pm 1 \in J$ y por lo tanto, $J = \mathcal{O}_K$. □

Proposición 1.38. *Sean I, J ideales no cero de $\mathcal{O}_K$ y $\gamma \in \mathcal{O}_K$ tales que se cumple $(\gamma\mathcal{O}_K)I = JI$. Entonces, $J = \gamma\mathcal{O}_K$.*

Demostración. Sean $\alpha \in I$ y $\beta \in J$. Entonces $\alpha\beta \in IJ = (\gamma\mathcal{O}_K)I$, de donde $\alpha\beta = \gamma\alpha'$, con $\alpha' \in I$. Se tiene $\alpha\dfrac{\beta}{\gamma} = \alpha' \in I$ y $\dfrac{\beta}{\gamma}I \subseteq I$. Por el Lema 1.13, $\dfrac{\beta}{\gamma} \in \mathcal{O}_K$, lo que implica $\beta \in \gamma\mathcal{O}_K$. Así, $J \subseteq \gamma\mathcal{O}_K$ y $\gamma^{-1}J$ es un ideal de $\mathcal{O}_K$. Dado que $\gamma I = JI$, $I = (\gamma^{-1}J)I$. Usando el lema anterior, $\gamma^{-1}J = \mathcal{O}_K$ y $J = \gamma\mathcal{O}_K = \gamma\mathcal{O}_K$. □

Si $\alpha \in \mathcal{O}_K \setminus \{0\}$, entonces podemos asociar un entero, llamado índice, al entero algebraico α; esto es debido a que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de K contenida en $\mathcal{O}_K$, [**2**] pág. 146.

Definición 1.39. *Sean K un campo de números, $\alpha \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\alpha)$. Entonces el índice de α, escrito como $ind(\alpha)$, es el entero positivo dado por*

$$ind(\alpha) = \sqrt{\frac{\Delta(\alpha)}{\delta_K}},$$

donde $\Delta(\alpha) = \Delta(1, \alpha, \ldots, \alpha^{n-1})$.

Notemos que si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base entera del ideal $\langle\alpha\rangle$, entonces por el Teorema 1.31,

$$N(\langle\alpha\rangle) = \sqrt{\frac{\Delta(\alpha_1 \ldots, \alpha_n)}{\delta_K}}.$$

De acuerdo a la definición anterior, tenemos que $N(\langle\alpha\rangle) = ind(\alpha)$ si y solo si

$$\Delta(\alpha_1 \ldots, \alpha_n) = \Delta(1, \alpha, \ldots, \alpha^{n-1}),$$

si y solo si $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es base entera del ideal $\langle\alpha\rangle$. Esto último, creemos que es un problema importante del cual no tenemos respuesta.

Teorema 1.40. *Sean K un campo de números de grado n, $\alpha \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\alpha)$. Entonces K es monogénico si y solo si existe $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$ y $ind(\theta) = 1$.*

Demostración. Si K es monogénico, entonces existe $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$ y $\{1, \theta, \ldots, \theta^{n-1}\}$ es base entera, es decir, $\Delta(1, \theta, \ldots, \theta^{n-1}) = \delta_K$, así $ind(\theta) = 1$. Sea $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$ y $ind(\theta) = 1$. Entonces $\delta_K = \Delta(1, \theta, \ldots, \theta^{n-1})$, es decir, $\{1, \theta, \ldots, \theta^{n-1}\}$ es base entera de $\mathcal{O}_K$, por tanto K es monogénico. □

Proposición 1.41. *Supongamos que $1, \alpha, \ldots, \alpha^{n-1}$ son $\mathbb{Q}$-linealmente independientes y sea $f(x) = Irr(\alpha, \mathbb{Q})$. Entonces*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N(f'(\alpha)),$$

donde $f'(x)$ es la derivada formal de $f(x)$.

Demostración. Ver [**21**], Proposition 12.1.4, pág. 174. □

1.3. Factorización de ideales en $\mathcal{O}_K$

En esta sección mostraremos que cualquier ideal no cero de $\mathcal{O}_K$ se puede escribir de forma única como producto de ideales primos.

Proposición 1.42. *Sean I, J ideales en $\mathcal{O}_K$ tal que $I \subseteq J$. Entonces existe un ideal M tal que $JM = I$.*

Demostración. Ver Proposition 12.2.7. en [**21**]. □

Definición 1.43. *Si $I \subseteq J$, entonces $I = JM$, para algún M ideal de $\mathcal{O}_K$. En este caso diremos que el ideal J divide al ideal I y lo escribiremos como $J|I$.*

Lema 1.44. *Sea I, J ideales no cero de $\mathcal{O}_K$ tales que $I \subseteq J$ y $N(I) = N(J)$. Entonces $I = J$.*

Demostración. Como $I \subseteq J$, entonces existe J' ideal no cero de $\mathcal{O}_K$ tal que $I = JJ'$. Dado que la norma es multiplicativa,

$$N(I) = N(J)N(J')$$

pero $N(I) = N(J)$, entonces $1 = N(J')$, es decir, $J' = \mathcal{O}_K$ y por tanto $I = J$. □

Proposición 1.45. *Todo ideal no cero de $\mathcal{O}_K$ se puede escribir como producto de un número finito de ideales primos.*

Demostración. Sea I un ideal no cero de $\mathcal{O}_K$. Si I es primo, la afirmación se cumple. Si I no es primo, entonces existe un ideal primo P_1 tal que $I \subseteq P_1$ y por la proposición anterior, $I = P_1 N_1$, para algún ideal N_1 de $\mathcal{O}_K$. Si N_1 es un ideal primo, $P_1 N_1$ es la expresión deseada. Si N_1 no es un ideal primo, repetimos el procedimiento tantas veces como sea posible, de donde tenemos

$$I = P_1 P_2 N_2 = P_1 P_2 P_3 N_3 = \cdots = P_1 P_2 \cdots P_r N_r.$$

Así generamos una cadena ascendente $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq N_r \subseteq \cdots$. Como $\mathcal{O}_K$ es noetheriano, esta cadena no puede ser infinita por lo que para algún r, $N_r = \mathcal{O}_K$. □

Teorema 1.46. *La factorización de un ideal $I \neq \{0\}$ de $\mathcal{O}_K$, como producto de ideales primos es única.*

Demostración. Supongamos que $I = P_1P_2\cdots P_s = Q_1Q_2\cdots Q_t$, con P_i, Q_j ideales primos. Tenemos 3 casos: $s < t$, $s = t$ y $s > t$. Supongamos que $s < t$, entonces $P_1P_2\cdots P_s = Q_1Q_2\cdots Q_sQ_{s+1}\cdots Q_t \subseteq P_1$ y como P_1 es primo, tenemos $Q_j \subseteq P_1$ para algún j. Sin pérdida de generalidad, supongamos que $Q_j = Q_1$, es decir $P_1 = Q_1$, pues Q_j es primo. Por la ley de la cancelación, $P_2P_3\cdots P_s = Q_2Q_3\cdots Q_sQ_{s+1}\cdots Q_t \subseteq P_2$. Repitiendo el mismo razonamiento, tenemos $P_1 = Q_1, P_2 = Q_2, \ldots, P_s = Q_s$, lo cual implica que $\mathcal{O}_K = Q_{s+1}\cdots Q_t$. De lo anterior, $\mathcal{O}_K \subseteq Q_{s+1}$, lo cual es una contradicción ya que Q_{s+1} es máximo. Análogamente $t < s$ no es posible, por lo que $s = t$. □

Lema 1.47. *Sean $I \neq 0$ un ideal de $\mathcal{O}_K$ y P un ideal primo de $\mathcal{O}_K$ tales que $I^2 = P^2$. Entonces $I = P$*

Demostración. Supongamos $I = P_1P_2\cdots P_r$ con P_i ideales primos de $\mathcal{O}_K$, entonces

$$P_1^2P_2^2\cdots P_r^2 = I^2 = PP.$$

Por el Teorema anterior, $P = P_i$ para algún $i \in \{1, \ldots, r\}$, sin pérdida de generalidad supongamos $P = P_1$, de donde $P_2^2\cdots P_r^2 = \mathcal{O}_K$ y así, $P_2\cdots P_r = \mathcal{O}_K$, lo cual no es posible. Por lo tanto $I = P_1 = P$. □

Teorema 1.48. *Sean $[K : \mathbb{Q}] = n,\ p \in \mathbb{N}$ un primo racional. Entonces existen $P_1, P_2, \ldots, P_g$ ideales primos de $\mathcal{O}_K$ tales que*

$$p\mathcal{O}_K = P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}$$

y $e_1f_1 + e_2f_2 + \cdots + e_gf_g = n$, en donde $N(P_i) = |\mathcal{O}_K/P_i| = p^{f_i}$. En paticular, si $K/\mathbb{Q}$ es Galois, entonces $e_1 = \cdots = e_n = e$, $f_1 = \cdots = f_n = f$ y por tanto $efg = n$.

Demostración. Por la Proposición 1.45, tenemos que todo ideal no cero de $\mathcal{O}_K$ es producto de ideales primos y por el Teorema 1.46, dicha factorización es única, en particular $p\mathcal{O}_K$ es un ideal primo no cero, así

$$p\mathcal{O}_K = P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}.$$

Como los f_i satisfacen $N(P_i) = p^{f_i}$, entonces

$$\begin{aligned} p^n &= N(p\mathcal{O}_K) = N(P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}) \\ &= N(P_1)^{e_1}\cdots N(P_g)^{e_g} \\ &= (p^{f_i})^{e_1}\cdots(p^{f_g})^{e_g} \\ &= p^{e_1f_1+e_2f_2+\cdots+e_gf_g}. \end{aligned}$$

Por lo tanto $e_1f_1 + e_2f_2 + \cdots + e_gf_g = n$. Sea $G = \{\sigma_1, \ldots, \sigma_n\}$ el grupo de Galois de $L/\mathbb{Q}$, puesto que $p\mathcal{O}_K = \prod_{i=1}^g$, entonces para todo índice j, $1 \leq j \leq g$, existe $\sigma \in G$ tal que $\sigma(P_1) = P_j$. Así

$p\mathcal{O}_K = \sigma(p\mathcal{O}_K) = \prod_{i=1}^g \sigma(P_i)^{e_i}$, dado que la descomposición como producto de ideales primos es única, $e_j = e_1$ para todo j, $1 \leq j \leq g$. Similarmente, de $\mathcal{O}_K/P_j = \mathcal{O}_K/\sigma(P_1) \approx \mathcal{O}_K/P_1$, se sigue que $f_j = f_1$, para todo j, $1 \leq j \leq g$. □

Definición 1.49. *Supongamos que $p\mathcal{O}_K = P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}$. Si algún $e_i > 1$, diremos que p es ramificado en K. Si $e_i = 1$ para todo i, diremos que p no se ramifica en K. El número e_i se llama el índice de ramificación del primo p en el ideal primo P_i. El número f_i se llama grado de inercia de p en el ideal primo P_i. ,*

Teorema 1.50. *Sea K un campo de números. Entonces el primo racional p se ramifica en $\mathcal{O}_K$ si y solo si $p|\delta_K$.*

Demostración. Ver [**12**], Proposition 5.44, pág. 111. □

Teorema 1.51. *Sean K un campo de números, I un ideal no cero de $\mathcal{O}_K$ tal que $N(I) = p$, para algún p primo racional. Entonces I es un ideal primo.*

Demostración. Ver [**2**], Theorem 10.1.6 pág. 240. □

Sabemos que el encontrar la factorización de los ideales $p\mathcal{O}_K$ es un problema complicado, como también lo es el encontrar los generadores de los ideales primos que factorizan a $p\mathcal{O}_K$. Un resultado muy útil que nos ayuda a resolver estos dos problemas es el siguiente.

Teorema 1.52 (Dedekind)**.** *Sean $K = \mathbb{Q}(\theta)$ un campo de números de grado n, q un primo racional, $f(x) = Irr(\theta, \mathbb{Q}) \in \mathbb{Z}[x]$ y la función $- : \mathbb{Z}[x] \longrightarrow \mathbb{F}_q[x]$ que reduce módulo q los coeficientes de un polinomio. Sea $\overline{f}(x) = g_1(x)^{e_1} \cdots g_r(x)^{e_r}$, donde $g_1(x), \cdots, g_r(x)$ son polinomios mónicos irreducibles distintos en $\mathbb{F}_q[x]$ y $e_1, \cdots, e_r$ son enteros positivos. Para $i = 1, \cdots, r$ sea $f_i(x) \in \mathbb{Z}[x]$ mónico tal que $\overline{f_i}(x) = g_i(x)$. Sea*

$$P_i = \langle q, f_i(\theta) \rangle.$$

Si $ind(\theta) \not\equiv 0 \pmod{q}$, entonces $P_1, \cdots, P_r$ son ideales primos distintos de $\mathcal{O}_K$ con

$$q\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r} \quad y \quad N(P_i) = q^{gr(f_i)}.$$

Demostración. Ver [**2**] Theorem 10.5.1. □

1.4. Grupo de Galois de un polinomio cuártico

Sea L el campo de descomposición de $f(x) \in K[x]$. Escribimos $G_f = Gal(L/K)$ para denotar al grupo de Galois de $f(x)$. Recordemos que si $\sigma \in G_f$ y $\alpha \in L$ es tal que $f(\alpha) = 0$, entonces $f(\sigma(\alpha)) = 0$. También si α y β son raíces de $f(x)$, entonces existe $\sigma \in G_f$ tal que $\sigma(\alpha) = \beta$. Si $G \leq S_n$, diremos que G es un grupo transitivo de grado n o que G actúa transitivamente sobre $I_n = \{1, \ldots, n\}$ si, para cualquier par $i, j \in \{1, 2, \ldots, n\}$, existe $\sigma \in G$ tal que $\sigma(i) = j$. Si numeramos las raíces de $f(x)$ como $\alpha_1, \ldots, \alpha_n$ entonces es claro que G_f actúa transitivamente sobre las raíces de $f(x)$ [**9**].

Teorema 1.53. *Sean K un campo, $f(x) \in K[x]$ separable de grado n y L el campo de descomposición de $f(x)$ sobre K. Entonces $f(x)$ es irreducible en $K[x]$ si y solo si G_f es un subgrupo transitivo de S_n.*

Demostración. Vea [**6**] Theorem 2.9. □

Para el caso particular $n = 4$, los únicos subgrupos transitivos de S_4 son ([**7**], Apendix A):

(i) el 4-grupo de Klein V,
(ii) el grupo cíclico C_4,
(iii) el grupo dihédrico D_8,
(iv) el grupo alternante A_4,
(v) el grupo S_4.

Dados $f(x), g(x) \in K[x]$ de grado n, m respectivamente con raíces $x_1, \ldots, x_n$ y $y_1, \ldots, y_m$ en el campo de descomposición de $f(x)g(x)$. Definimos la rasultante de f y g como

$$R(f,g) = a_n^m b_m^n \prod_{1 \leq i \leq n} (x_i - y_j),$$

donde a_n y b_m son el coeficiente lider de $f(x)$ y $g(x)$ respectivamente. La expresión $R(f,g)$ tiene propiedades interesantes, por ejemplo $R(f,g) = 0$ si y solo si f y g tienen una raíz en común. De particular importancia para nosotros es el caso particular cuando $g = f'$. En tal caso $R(f,f')$ es lo que se conoce como la resultante de f. En el caso de un polinomio de grado 4, en 1989 L. Kappe y B. Warren [**24**], usan la resultante y establecen condiciones necesarias y suficientes para reconocer a G_f [**34**].

Teorema 1.54. *Sean K un campo de característica $\neq 2$, $f(x)$ irreducible sobre K, $r_3(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d + c^2 - 4bd)$ con campo de descomposición E y $D = disc(f)$. Entonces*

(i) *$G_f = S_4$ si y solo si $r_3(x)$ es irreducible sobre K y $D \notin K^2$.*
(ii) *$G_f = A_4$ si y solo si $r_3(x)$ es irreducible sobre K y $D \in K^2$.*
(iii) *$G_f = V$ si y solo si $r_3(x)$ se descompone en factores lineales sobre K.*
(iv) *$G_f = C_4$ si y solo si $r_3(x)$ tiene exactamente una raíz t en K y $g(x) = (x^2 - tx + d)(x^2 + ax + (b - t))$ se descompone sobre $E[x]$.*
(v) *$G_f = D_8$ si y solo si $r_3(x)$ tiene exactamente una raíz t en K y $g(x)$ no se descompone sobre $E[x]$.*

Demostración. Ver [**24**], Theorem 1, pág. 134. □

Teorema 1.55. *Sean K un campo de característica distinta de 2, $f(x) = x^4 + bx^2 + d$ un polinomio irreducible sobre $K[x]$ y $\pm\alpha, \pm\beta$ sus raíces. Entonces*

(i) *$G_f = V$ si y solo si $d \in K^2$ si y solo si $\alpha\beta \in K$.*
(ii) *$G_f = C_4$ si y solo si $d(b^2 - 4d) \in K^2$ si y solo si $K(\alpha\beta) = K(\alpha^2)$.*
(iii) *$G_f = D_8$ si y solo si $d(b^2 - 4d) \notin K^2$ si y solo si $\alpha\beta \notin K(\alpha^2)$.*

Demostración. Ver [**24**], Theorem 3, pág. 135. □

Ejemplo 1.56. *Sea $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, con $m, n \in \mathbb{Z}$ libres de cuadrados. Entonces*

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n}),$$

$f(x) = Irr(\sqrt{m} + \sqrt{n}, \mathbb{Q}) = x^4 - 2(m+n)x^2 + (m-n)^2$ y por el teorema anterior $G_f = V$

Los siguientes resultados nos ayudarán a factorizar ciertos polinomios.

Teorema 1.57 ([**24**], Theorem 2)**.** *Sean $h(x) = x^4 + bx^2 + d \in K[x]$, $car(K) \neq 2$ y $\pm\alpha, \pm\beta$ las raíces de $f(x)$. Entonces las siguientes condiciones son equivalentes.*

(i) *$h(x)$ es irreducible sobre K.*
(ii) *$\alpha^2, \alpha + \beta, \alpha - \beta \notin K$.*
(iii) *$b^2 - 4d, -b + 2\sqrt{d}, -b - 2\sqrt{d} \notin K^2$.*

Demostración. Notemos primero que $h(x)$ no puede tener un factor cúbico irreducible, ya que si a_0 es una raíz, $-a_0$ también es una raíz, por tanto $h(x)$ es reducible sobre K si y solo si al menos una de las siguientes factorizaciones

$$h(x) = (x^2 - \alpha^2)(x^2 - \beta^2),$$

$$h(x) = (x^2 - (\alpha + \beta)x + \alpha\beta)(x^2 + (\alpha + \beta) + \alpha\beta),$$

$$h(x) = (x^2 - (\alpha - \beta)x - \alpha\beta)(x^2 + (\alpha - \beta) - \alpha\beta),$$

tiene todos sus coeficientes en K. Se sigue inmediatamente que (ii) implica (i). Las relaciones entre los coeficientes y las raíces básicamente son: $-b = \alpha^2 + \beta^2$ y $d = \alpha^2\beta^2$. Esto, junto con $(\alpha + \beta)^2 = -b + 2\alpha\beta$ y $(\alpha - \beta)^2 = -b - 2\alpha\beta$ implica que si α^2 ó $\alpha \pm \beta \in K$, entonces β^2 ó $\alpha\beta \in K$ respectivamente. Si $\alpha^2 \in K$, entonces $\beta^2 \in K$, es decir, $h(x)$ se factoriza sobre K. Si $\alpha \pm \beta \in K$, entonces $\alpha\beta \in K$, es decir, $h(x)$ se factoriza sobre K. De lo anterior, (i) implica (ii). Finalmente, obsevemos lo siguiente

$$\begin{aligned}(b + 2\alpha^2)^2 &= (-\alpha^2 - \beta^2 + 2\alpha^2)^2 \\ &= (\alpha^2 - \beta^2)^2 \\ &= (\alpha + \beta)^2(\alpha - \beta)^2 \\ &= (-b + 2\sqrt{d})(-b - 2\sqrt{d}) \\ &= b^2 - 4d\end{aligned}$$

y $(\alpha \pm \beta)^2 = -b \pm 2\sqrt{d}$. Por lo tanto, $\alpha \pm \beta \in K$ si y solo si $-b \pm 2\sqrt{d} \in K^2$ y $\alpha^2 \in K$ si y solo si $b^2 - 4d \in K^2$, es decir, (ii) si y solo si (iii).

□

El siguiente teorema lo podemos encontrar en [**10**] como Theorem 3.

Teorema 1.58. *Si p es un primo impar y si r, s son enteros tales que $s \not\equiv 0 \pmod{p}$ y $r^2 - 4s \not\equiv 0 \pmod{p}$, entonces se dan las siguientes afirmaciones:*

(i) *$f(x) = x^4 + rx^2 + s$ es producto de dos polinomios lineales mónicos distintos y un polinomio cuadrático mónico irreducible módulo p si y solo si*

$$\left(\frac{s}{p}\right) = -1, \quad \left(\frac{r^2 - 4s}{p}\right) = 1.$$

(ii) *$f(x) = x^4 + rx^2 + s$ es producto de cuatro polinomios lineales mónicos distintos módulo p si y solo si*

$$\left(\frac{s}{p}\right) = 1, \quad \left(\frac{r^2 - 4s}{p}\right) = 1, \quad \left(\frac{-r - 2t}{p}\right) = 1,$$

donde t es un entero tal que $s \equiv t^2 \pmod{p}$.

(iii) *$f(x) = x^4 + rx^2 + s$ es producto de dos polinomios cuadráticos mónicos irreducibles distintos módulo p si y solo si*

$$\left(\frac{s}{p}\right) = 1, \quad \left(\frac{r^2 - 4s}{p}\right) = 1, \quad \left(\frac{-r - 2t}{p}\right) = -1,$$

donde t es un entero tal que $s \equiv t^2 \pmod{p}$, ó

$$\left(\frac{s}{p}\right) = 1, \quad \left(\frac{r^2 - 4s}{p}\right) = -1.$$

(iv) $f(x) = x^4 + rx^2 + s$ *es irreducible módulo p si y solo si*

$$\left(\frac{s}{p}\right) = -1, \quad \left(\frac{r^2 - 4s}{p}\right) = -1.$$

1.5. Extensiones Relativas

Sea K un campo de números, L una extensión finita de grado n sobre K y sean $\mathcal{O}_K, \mathcal{O}_L$ los anillos de enteros de K, L respectivamente. Diremos que $L|K$ es una extensión relativa si $K \neq \mathbb{Q}$.

Definición 1.59. *Sea I un ideal de $\mathcal{O}_L$. La traza relativa de I es un ideal de $\mathcal{O}_K$ definido y denotado como*

$$Tr_{L|K}(I) = \{Tr_{L|K}(x) : x \in I\}.$$

Definición 1.60. *Sea Q un ideal primo de $\mathcal{O}_L$, $Q \cap \mathcal{O}_K = P$ y $[\mathcal{O}_L/Q : \mathcal{O}_K/P] = f$.*

(i) *La norma relativa de Q es $N_{L|K}(Q) = P^f$.*

(ii) *Si I es un ideal no cero de $\mathcal{O}_L$ y $I = \prod_{i=1}^{g} Q_i^{e_i}$, donde $Q_1, \ldots, Q_g$ son ideales primos distintos de $\mathcal{O}_L$, entonces la norma relativa de I es $N_{L|K}(I) = \prod_{i=1}^{g} N_{L|K}(Q_i)^{e_i}$.*

Proposición 1.61. *Con las notaciones previas, $[L : K] = n$ e I cualquier ideal no cero de $\mathcal{O}_K$, tenemos*

$$N_{L|K}(I\mathcal{O}_L) = I^n.$$

Demostración. Por la multiplicidad de la norma relativa, es suficiente mostrar la afirmación anterior cuando $I = P$ es un ideal primo de $\mathcal{O}_K$. Sea $P\mathcal{O}_L = \prod_{i=1}^{g} Q_i^{e_i}$, donde $Q_1, \ldots, Q_g$ son ideales primos distintos de $\mathcal{O}_L$, $e_i \geqslant 1$ y $[\mathcal{O}_L/Q_i : \mathcal{O}_K/P] = f_i$ para $i = 1, \ldots, g$. Puesto que $\sum_{i=1}^{g} e_i f_i = n$, tenemos

$$N_{L|K}(P\mathcal{O}_K) = \prod_{i=1}^{g} N_{L|K}(Q_i)^{e_i} = \prod_{i=1}^{g} P^{f_i e_i} = P^n.$$

□

Proposición 1.62. *Sean $K \subseteq L \subseteq L'$ campos de números y J' un ideal no cero de L'. Entonces $N_{L'|K}(J') = N_{L|K}(N_{L'|L}(J'))$.*

Demostración. Por la multiplicidad de la norma relativa, es suficiente mostrar la afirmación anterior cuando $J' = Q'$ es un ideal primo de $\mathcal{O}_{L'}$. Sea $Q' \cap \mathcal{O}_L = Q$, $Q \cap \mathcal{O}_K = P$. Entonces $N_{L'|K}(Q') = f''$ donde $f'' = [\mathcal{O}_{L'}/Q' : \mathcal{O}_K/P]$. Por otro lado, $N_{L'|L}(Q') = Q^{f'}$

donde $f' = [\mathcal{O}_{L'}/Q' : \mathcal{O}_L/Q]$ y $N_{L|K}(Q) = p^f$ donde $f = [\mathcal{O}_L/Q : \mathcal{O}_K/P]$. Así $f'' = ff'$ y por lo tanto

$$N_{L|K}(N_{L'|L}(Q')) = N_{L|K}(Q^{f'}) = P^{ff'} = P^{f''} = N_{L'|K}(Q').$$

□

Definición 1.63. *Sea K un campo de números, L una extensión finita de grado n sobre K y sean $\mathcal{O}_K, \mathcal{O}_L$ los anillos de enteros de K, L respectivamente. El discriminante relativo de $L|K$ es el ideal $\delta_{L|K}$ de $\mathcal{O}_K$ generado por los elementos $\Delta_{L|K}(x_1, \ldots, x_n)$, para todas las posibles bases $\{x_1, \ldots, x_n\}$ de $L|K$ tales que cada $x_i \in \mathcal{O}_L$.*

Proposición 1.64. *Sea $\{x_1, \ldots, x_n\}$ una base de $L|K$ tales que cada $x_i \in \mathcal{O}_L$. Entonces $\delta_{L|K} = \Delta_{L|K}(x_1, \ldots, x_n) \cdot \mathcal{O}_K$ si y solo si $\mathcal{O}_L$ es un $\mathcal{O}_K-$módulo libre y $\{x_1, \ldots, x_n\}$ es una $\mathcal{O}_K-$base de $\mathcal{O}_L$.*

Demostración. Ver [**30**], G, pág. 237. □

Un resultado que nos ayudará a saber qué ideales de K se ramifican en L es el siguiente.

Teorema 1.65. *Sea P un ideal primo de $\mathcal{O}_K$. Entonces P se ramifica en $L|K$ si y solo si $P \mid \delta_{L|K}$.*

Demostración. Ver [**30**], Theorem 1, pág. 238. □

Teorema 1.66. *Sean $K \subseteq L \subseteq L'$ campos de números. Entonces*

$$\delta_{L'|K} = (\delta_{L|K})^{[L':L]} \cdot N_{L|K}(\delta_{L'|L}).$$

Demostración. Ver [**30**], Q, pág. 249. □

Sean p un primo racional, K un campo de números que contiene una raíz $p-$ésima primitiva de la unidad ζ y $\mathcal{O}_K$ el anillo de enteros de K. Sea a un elemento de K que no es una $p-$ésima potencia de un elemento de K y consideramos el polinomio $F = x^p - a \in K[x]$. Sean t una raíz de F, $L = K(t)$ y $\mathcal{O}_L$ su anillo de enteros. A continuación daremos explícitamente la factorización de los ideales primos de $\mathcal{O}_K$ en $\mathcal{O}_L$.

Proposición 1.67. *Sean P un ideal primo de $\mathcal{O}_K$, $a\mathcal{O}_K = P^h J$, donde J es un ideal de $\mathcal{O}_K$ no múltiplo del ideal P y $h > 0$ es un entero racional no múltiplo de p. Entonces*

$$P\mathcal{O}_L = \langle P, t\rangle^p.$$

Demostración. Ver [**30**], J, pág. 320. □

Ahora sea P un ideal primo de $\mathcal{O}_K$ tal que $a\mathcal{O}_K = P^h J$, donde J es un ideal de $\mathcal{O}_K$ no múltiplo de P y p divide al entero $h \geq 0$. Si $h > 0$, entonces $P \mid a\mathcal{O}_K$ y $p \nmid h$ ó $p \mid h$. El caso $p \nmid h$ es la proposición anterior. Si $p \mid h$, podemos elegir a' de tal manera que $x^p - a'$ genera la misma extensión $L|K$ y $P \nmid a'\mathcal{O}_K$. De hecho a' es tal que $a = a'b^h$. Ahora ya estamos en el caso de la siguiente proposición al igual que el caso $h = 0$.

Proposición 1.68. *Supongamos que $P \nmid a\mathcal{O}_K$ y $P \nmid p\mathcal{O}_K$. Entonces*

(i) *Si la congruencia $x^p \equiv a \pmod{P}$ es soluble en $\mathcal{O}_K$, entonces*

$$P\mathcal{O}_L = \langle P, x - t\rangle\langle P, x - \zeta t\rangle \cdots \langle P, x - \zeta^{p-1}t\rangle.$$

(ii) *Si la congruencia $x^p \equiv a \pmod{P}$ no es soluble en $\mathcal{O}_K$, entonces*

$$P\mathcal{O}_L \text{ es un ideal primo.}$$

Demostración. Ver [**30**], K, pág. 321. □

Como caso particular tenemos las extensiones relativas cuadráticas, es decir, $L|K$ con $[L : K] = 2$. Notemos que en este caso, $L|K$ es Galois y $efg = 2$, las únicas formas en la que un ideal primo P de $\mathcal{O}_K$ se puede factorizar en $\mathcal{O}_L$ son: P es totalmente ramificado, P es inerte y P se descompone totalmente. Concretamente:

(i) $e = 2, f = 1, g = 1$, en este caso $P\mathcal{O}_L = \mathcal{P}^2$ con $\mathcal{P}$ un ideal primo de $\mathcal{O}_L$.
(ii) $e = 1, f = 2, g = 1$, en este caso $P\mathcal{O}_L = \mathcal{P}$ con $\mathcal{P}$ un ideal primo de $\mathcal{O}_L$.
(iii) $e = 1, f = 1, g = 2$, en este caso $P\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2$ con $\mathcal{P}_1$ y $\mathcal{P}_2$ ideales primos de $\mathcal{O}_L$.

Capítulo 2

Ramificación en el caso cíclico

Lo primero que vamos a destacar es quién es G_f para $f(x) = x^4 + px^2 + p$. Notemos que $f(x)$ es irreducible en $\mathbb{Q}[x]$ por el criterio de Eisenstein. También, como $\sqrt{p} \notin \mathbb{Q}$, entonces por la afirmación (i) del Teorema 1.55, $G_f = C_4$ ó $G_f = D_8$.

Teorema 2.1. *Sean p un primo racional, $f(x) = x^4 + px^2 + p$. Entonces $G_f = C_4$ si y solo si $p = 4 + n^2$ para alguna $n \in \mathbb{N}$.*

Demostración. Si $G_f = C_4$, entonces por la afirmación (ii) del Teorema 1.55, existe $\dfrac{a}{b} \in \mathbb{Q}$ tal que

$$p^2(p-4) = \frac{a^2}{b^2}.$$

Por lo anterior, $a = pt$ para algún $t \in \mathbb{Z}$ y así $b^2(p-4) = t^2$. Esto último se cumple si y solo si $p - 4 = n^2$ para alguna $n \in \mathbb{N}$. Inversamente, si $p = 4 + n^2$ para alguna $n \in \mathbb{N}$, entonces

$$p(p^2 - 4p) = p^2(p-4) = p^2n^2 \in \mathbb{Q}^2,$$

y la afirmación (ii) del Teorema 1.55 se cumple y por tanto $G_f = C_4$. □

En general, si $f(x) = x^4 + ax^2 + a$ es irreducible con $a = 4 + n^2$, entonces $G_f = C_4$.

Corolario 2.2. *Con las mismas hipótesis del teorema anterior, $G_f = D_8$ si y solo si p no es de la forma $4 + n^2$.*

En el resto de este capítulo el primo racional p es de la forma $4+n^2$ y creemos que hay una infinidad de ellos pero no conocemos una prueba, de hecho, puede ser equivalente a la conjetura que afirma que hay una infinidad de primos de la forma $1 + n^2$. En la siguiente tabla mostramos los primeros 36 primos racionales de la forma $4 + n^2$.

Primos de la forma $4 + n^2$		
$5 = 2^2 + 1^2$	$13 = 2^2 + 3^2$	$29 = 2^2 + 5^2$
$53 = 2^2 + 7^2$	$173 = 2^2 + 13^2$	$229 = 2^2 + (5 \cdot 3)^2$
$293 = 2^2 + 17^2$	$733 = 2^2 + (3 \cdot 3 \cdot 3)^2$	$1093 = 2^2 + (11 \cdot 3)^2$
$1229 = 2^2 + (7 \cdot 5)^2$	$1373 = 2^2 + 37^2$	$2029 = 2^2 + (5 \cdot 3 \cdot 3)^2$
$2213 = 2^2 + 47^2$	$3253 = 2^2 + (19 \cdot 3)^2$	$4229 = 2^2 + (13 \cdot 5)^2$
$4493 = 2^2 + 67^2$	$5333 = 2^2 + 73^2$	$7229 = 2^2 + (17 \cdot 5)^2$
$7573 = 2^2 + (29 \cdot 3)^2$	$9029 = 2^2 + (19 \cdot 5)^2$	$9413 = 2^2 + 97^2$
$10613 = 2^2 + 103^2$	$13229 = 2^2 + (23 \cdot 5)^2$	$13693 = 2^2 + (13 \cdot 3 \cdot 3)^2$
$15629 = 2^2 + (5 \cdot 5 \cdot 5)^2$	$18229 = 2^2 + (5 \cdot 3 \cdot 3 \cdot 3)^2$	$18773 = 2^2 + 137^2$
$21613 = 2^2 + (7 \cdot 7 \cdot 3)^2$	$24029 = 2^2 + (31 \cdot 5)^2$	$26573 = 2^2 + 163^2$
$27893 = 2^2 + 167^2$	$31333 = 2^2 + (59 \cdot 3)^2$	$33493 = 2^2 + (61 \cdot 3)^2$
$37253 = 2^2 + 193^2$	$41213 = 2^2 + (29 \cdot 7)^2$	$42853 = 2^2 + (23 \cdot 3 \cdot 3)^2$

Sea K una extensión cíclica de grado 4 sobre $\mathbb{Q}$. El siguente resultado será de gran utilidad para nuestro estudio de bases enteras e índice en esta clase de extensiones.

Teorema 2.3 (K. Hardy *et al* [**17**])**.** *K se puede expresar en forma única como*

$$\mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right),$$

donde A, B, C, D son enteros tales que A es libre de cuadrados e impar, $D = B^2 + C^2$ es libre de cuadrados, $B > 0, C > 0$ y $mcd(A, D) = 1$.

Demostración. Ver [**17**] Theorem 1. □

En el caso particular de $f(x) = x^4 + px^2 + p$, es claro que las raíces de $f(x)$ son

$$\pm\sqrt{\frac{-1}{2}(p - n\sqrt{p})}, \quad \pm\sqrt{\frac{-1}{2}(p + n\sqrt{p})}.$$

Observemos que si $G_f = C_4$ y $\alpha = \sqrt{\frac{-1}{2}(p - n\sqrt{p})}$, $\beta = \sqrt{\frac{-1}{2}(p + n\sqrt{p})}$, entonces $\beta \in \mathbb{Q}(\alpha)$. También notemos que el polinomio irreducible de $\sqrt{A(D + B\sqrt{D})}$ en el Teorema 2.3 es $f(x) = x^4 - 2ADx^2 + A^2C^2D$, sin embargo, es posible que el polinomio irreducible de algún otro generador del mismo campo tenga término cúbico y lineal. Vea el Lema 2.24.

Teorema 2.4. *Sean $f(x) = x^4 + px^2 + p$ con $p = 4 + n^2$, $\alpha = \sqrt{\frac{-1}{2}(p - n\sqrt{p})}$ y $\alpha' = \sqrt{-(p + 2\sqrt{p})}$. Entonces $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$.*

Demostración. En la siguiente torre de campos

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}(\sqrt{p}) \\ | \\ \mathbb{Q} \end{array}$$

una $\mathbb{Q}$- base de $\mathbb{Q}(\sqrt{p})$ sobre $\mathbb{Q}$ es $\{1, \sqrt{p}\}$ y una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}(\sqrt{p})$ es $\{1, \alpha\}$. Por tanto, una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$ es $\{1, \sqrt{p}, \alpha, \sqrt{p}\alpha\}$. Puesto que

$$\alpha' = \frac{n+2}{2}\alpha + \frac{1}{2}\sqrt{p}\alpha \in \mathbb{Q}(\alpha),$$

entonces $\mathbb{Q}(\alpha') \subseteq \mathbb{Q}(\alpha)$. El polinomio $g(x) = x^4 + 2px^2 + n^2p$ es irreducible en $\mathbb{Q}[x]$ y $g(\alpha') = 0$. Por tanto $[\mathbb{Q}(\alpha' : \mathbb{Q})] = 4$ y $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$. □

Si $\beta' = \sqrt{-(p - 2\sqrt{p})}$, entonces las raíces de $g(x)$ son $\pm\alpha', \pm\beta'$. Notemos que

$$A = -1, \quad B = 2, \quad C = n, \quad D = p,$$

en el Teorema 2.4 nos produce la igualdad

$$\mathbb{Q}(\sqrt{-(p + 2\sqrt{p})}) = \mathbb{Q}(\alpha').$$

Con la representación $K = \mathbb{Q}(\alpha')$ podemos calcular la forma general de la traza de un elemento típico de K. Antes es necesario conocer la acción de G_f sobre las raíces de $g(x)$.

Teorema 2.5. *Sean $K = \mathbb{Q}(\alpha')$, $\pm\alpha', \pm\beta'$ las raíces de $g(x) = x^4 + 2px^2 + n^2p$. Entonces $Gal(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, donde*

$$\sigma_1(\alpha') = \alpha', \quad \sigma_2(\alpha') = -\alpha', \quad \sigma_3(\alpha') = \beta', \quad \sigma_4(\alpha') = -\beta'.$$

Demostración. Sabemos que $\mathbb{Q}(\alpha') = \mathbb{Q}(\beta') = \mathbb{Q}(-\alpha') = \mathbb{Q}(-\beta')$ y es claro que $\sigma_i \in Gal(K/\mathbb{Q})$. Notemos que si $\alpha_1 = \alpha', \alpha_2 = \beta', \alpha_3 = -\alpha'$ y $\alpha_4 = -\beta'$, entonces

$$\sigma_1(-\alpha') = -\alpha', \quad \sigma_1(\beta') = \beta', \quad \sigma_1(-\beta') = -\beta',$$

así, podemos suponer que

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Puesto que $\sigma_2(\alpha') = -\alpha'$, entonces $\sigma_2(-\alpha') = -\sigma_2(\alpha') = \alpha'$, y

$$\begin{aligned} \sigma_2(\beta') &= \sigma_2\left(-\frac{p+4}{2n}\alpha' - \frac{1}{2n}\alpha'^3\right) = -\frac{p+4}{2n}\sigma_2(\alpha') - \frac{1}{2n}\sigma_2(\alpha')^3 \\ &= \frac{p+4}{2n}\alpha' + \frac{1}{2n}\alpha'^3 = -\beta'. \end{aligned}$$

De lo anterior, $\sigma_2(-\beta') = -\sigma_2(\beta') = \beta'$, y por tanto podemos suponer que

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

De manera similar es fácil concluir

$$\begin{gathered} \sigma_3(\alpha') = \beta', \quad \sigma_4(\alpha') = -\beta', \\ \sigma_3(-\alpha') = -\beta', \quad \sigma_4(-\alpha') = \beta', \\ \sigma_3(\beta') = -\alpha', \quad \sigma_4(\beta') = \alpha', \\ \sigma_3(-\beta') = -\alpha', \quad \sigma_4(-\beta') = -\alpha'. \end{gathered}$$

Por lo tanto, podemos suponer que

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Finalmente como $\sigma_3^2 = \sigma_2$, $\sigma_3^3 = \sigma_4$, $\sigma_3^4 = \sigma_1$, concluimos que $Gal(K/\mathbb{Q}) = \langle\sigma_3\rangle$. □

Lema 2.6. *Sea $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p + 2\sqrt{p})}$. Entonces $tr(\alpha'^2) = -4p$ y*

$$tr(\alpha') = tr(\beta') = tr(\sqrt{p}) = tr(\alpha'^3) = 0.$$

Demostración. Para la primera afirmación, y por el teorema anterior

$$\begin{aligned} tr(\alpha'^2) &= \sigma_1(\alpha'^2) + \sigma_2(\alpha'^2) + \sigma_3(\alpha'^2) + \sigma_4(\alpha'^2) \\ &= \alpha'^2 + \alpha'^2 + \beta'^2 + \beta'^2 \\ &= -2(p + 2\sqrt{p}) - 2(p - 2\sqrt{p}) \\ &= -4p \end{aligned}$$

La prueba de las otras afirmaciones es similar . □

Corolario 2.7. *Sea α' como en el lema anterior. Entonces*

(i) $tr(\alpha'^j) = -2p \cdot tr(\alpha'^{j-2}) - n^2 p \cdot tr(\alpha'^{j-4})$ *si* $j \geq 4$ *es par.*
(ii) $tr(\alpha'^j) = 0$ *si* $j \in \mathbb{N}$ *es impar.*

Demostración. Es claro que $\alpha'^4 = -2p\alpha'^2 - n^2 p$. Por tanto, para $t \geq 2$ tenemos

$$\alpha'^{2t} = \alpha'^{2t-4} \cdot \alpha'^4 = -2p\alpha'^{2t-2} - n^2 p\alpha'^{2t-4}.$$

Por la linealidad de la traza tenemos $tr(\alpha'^{2t}) = -2p \cdot tr(\alpha'^{2t-2}) - n^2 p \cdot tr(\alpha'^{2t-4})$. Para la afirmación (ii) tenemos:

$$tr(\alpha'^j) = \sigma_1(\alpha'^j) + \sigma_2(\alpha'^j) + \sigma_3(\alpha'^j) + \sigma_4(\alpha'^j) = \alpha'^j + \beta'^j - \alpha'^j - \beta'^j = 0.$$

□

Lema 2.8. *Sea $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p + 2\sqrt{p})}$. Entonces $N(\alpha') = N(\beta') = n^2 p$.*

Demostración.

$$\begin{aligned} N(\alpha') &= \sigma_1(\alpha')\sigma_2(\alpha')\sigma_3(\alpha')\sigma_4(\alpha') \\ &= \alpha'(-\alpha')\beta'(-\beta') = \alpha'^2\beta'^2 \\ &= (p^2 - 4p) = p(p-4) \\ &= n^2 p. \end{aligned}$$

□

2.1. Base entera

De la teoría clásica sabemos que para calcular δ_K es suficiente conocer una base entera de $K/\mathbb{Q}$. K. Hardy *et al* [**17**] de manera ingeniosa calcularon el discriminante del polinomio irreducible del generador del campo $K = \mathbb{Q}(\alpha')$ y a partir de ahí, obtuvieron el discriminante del campo δ_K, sin necesidad de conocer explícitamente una base entera.

Teorema 2.9. *Sea $K = \mathbb{Q}(\alpha')$, con α', β' como en el Teorema* 2.5. *Entonces:*

Si $n \equiv 3 \pmod 4$, una base entera para $K/\mathbb{Q}$ es

$$\left\{\omega_1 = 1, \omega_2 = \frac{1+\sqrt{p}}{2}, \omega_3 = \frac{1+\sqrt{p}+\alpha'+\beta'}{4}, \omega_4 = \frac{1-\sqrt{p}+\alpha'-\beta'}{4}\right\},$$

si $n \equiv 1 \pmod 4$, una base entera para $K/\mathbb{Q}$ es

$$\left\{\omega_1 = 1, \omega_2 = \frac{1+\sqrt{p}}{2}, \omega_3 = \frac{1+\sqrt{p}+\alpha'-\beta'}{4}, \omega_4 = \frac{1-\sqrt{p}+\alpha'+\beta'}{4}\right\}.$$

Demostración. Se sigue directamente de Theorem en [**20**], pág. 146. □

Lema 2.10. *Sea $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p + 2\sqrt{p})}, \beta' = \sqrt{-(p - 2\sqrt{p})}$. Si $n \equiv 3 \pmod 4$, entonces*

(i) $\alpha' = -1 + 2\omega_3 + 2\omega_4$.
(ii) $\beta' = 1 - 2\omega_2 + 2\omega_3 - 2\omega_4$.
(iii) $\sqrt{p} = -1 + 2\omega_2$.
(iv) $\alpha' + \beta' = -2\omega_2 + 4\omega_3$.
(v) $\alpha' - \beta' = -2 + 2\omega_2 + 4\omega_4$.

(vi) $(\alpha'+\beta')^2 = 2(n-p) - 4n\omega_2$.
(vii) $(\alpha'-\beta')^2 = -2(n+p) + 4n\omega_2$.
(viii) $(\alpha'+\beta')(\alpha'-\beta') = 4 - 8\omega_2$.
(ix) $(1+\sqrt{p})^2 = (p-1) + 4\omega_2$.
(x) $(1-\sqrt{p})^2 = (p+3) - 4\omega_2$.
(xi) $\sqrt{p}\alpha' = (n-2) - 2n\omega_2 + (4+2n)\omega_3 + (4-2n)\omega_4$.
(xii) $\sqrt{p}\beta' = -(n+2) + 4\omega_2 - (4-2n)\omega_3 + (4+2n)\omega_4$.
(xiii) $(1+\sqrt{p})(\alpha'+\beta') = -4 + (2-2n)\omega_2 + (4+4n)\omega_3 + 8\omega_4$.
(xiv) $(1+\sqrt{p})(\alpha'-\beta') = (2n-2) - (2+2n)\omega_2 + 8\omega_3 + (4-4n)\omega_4$.
(xv) $(1-\sqrt{p})(\alpha'+\beta') = 4 + (2n-6)\omega_2 + (4-4n)\omega_3 - 8\omega_4$.
(xvi) $(1-\sqrt{p})(\alpha'-\beta') = -(2+2n) + (2n+6)\omega_2 - 8\omega_3 + (4+4n)\omega_4$.

Si $n \equiv 1 \pmod 4$, *entonces*

(i) $\alpha' = -1 + 2\omega_3 + 2\omega_4$.
(ii) $\beta' = -1 + 2\omega_2 - 2\omega_3 + 2\omega_4$.
(iii) $\sqrt{p} = -1 + 2\omega_2$.
(iv) $\alpha'+\beta' = -2 + 2\omega_2 + 4\omega_4$.
(v) $\alpha'-\beta' = -2\omega_2 + 4\omega_3$.
(vi) $(\alpha'+\beta')^2 = 2(n-p) - 4n\omega_2$.
(vii) $(\alpha'-\beta')^2 = -2(n+p) + 4n\omega_2$.
(viii) $(\alpha'+\beta')(\alpha'-\beta') = 4 - 8\omega_2$.
(ix) $(1+\sqrt{p})^2 = (p-1) + 4\omega_2$.
(x) $(1-\sqrt{p})^2 = (p+3) - 4\omega_2$.
(xi) $\sqrt{p}\alpha' = -(n+2) + 2n\omega_2 + (4-2n)\omega_3 + (4+2n)\omega_4$.
(xii) $\sqrt{p}\beta' = (2-n) - 4\omega_2 + (4+2n)\omega_3 - (4-2n)\omega_4$.
(xiii) $(1+\sqrt{p})(\alpha'+\beta') = -(2+2n) + (2n-2)\omega_2 + 8\omega_3 + (4n+4)\omega_4$.
(xiv) $(1+\sqrt{p})(\alpha'-\beta') = -4 + (2+2n)\omega_2 + (4-4n)\omega_3 + 8\omega_4$.
(xv) $(1-\sqrt{p})(\alpha'+\beta') = (2n-2) + (6-2n)\omega_2 - 8\omega_3 + (4-4n)\omega_4$.
(xvi) $(1-\sqrt{p})(\alpha'-\beta') = 4 - (2n+6)\omega_2 + (4+4n)\omega_3 - 8\omega_4$.

Demostración. Para el caso $n \equiv 3 \pmod 4$, la base entera es

$$\omega_1 = 1, \quad \omega_2 = \frac{1+\sqrt{p}}{2}, \quad \omega_3 = \frac{1+\sqrt{p}+\alpha'+\beta'}{4}, \quad \omega_4 = \frac{1-\sqrt{p}+\alpha'-\beta'}{4}.$$

Así,

$$-1 + 2\omega_3 + 2\omega_4 = -1 + 2\left(\frac{1+\sqrt{p}+\alpha'+\beta'}{4}\right) + 2\left(\frac{1-\sqrt{p}+\alpha'-\beta'}{4}\right) = \alpha'.$$

$$\begin{aligned} 1 - 2\omega_2 + 2\omega_3 - 2\omega_4 &= 1 - 2\left(\frac{1+\sqrt{p}}{2}\right) + 2\left(\frac{1+\sqrt{p}+\alpha'+\beta'}{4}\right) \\ &\quad -2\left(\frac{1-\sqrt{p}+\alpha'-\beta'}{4}\right) = \beta'. \end{aligned}$$

$$-1 + 2\omega_2 = -1 + 2\left(\frac{1+\sqrt{p}}{2}\right) = \sqrt{p}.$$

Los casos (iv)-(x) se deducen de los tres casos anteriores, notando que $\alpha'\beta' = -n\sqrt{p}$.

$$\begin{aligned}
\sqrt{p}\alpha' &= \frac{-p}{2}\alpha' + \frac{p}{2}\alpha' + \sqrt{p}\alpha' = \frac{-p}{2}\alpha' + \frac{1}{2}(p+2\sqrt{p})\alpha' \\
&= 2\alpha' - \frac{p+4}{2}\alpha' - \frac{1}{2}\alpha'^3 = 2\alpha' + n\beta' \\
&= n - 2 - n - n\sqrt{p} + 1 + \sqrt{p} + \alpha' + \beta' + \frac{n}{2} + \frac{n\sqrt{p}}{2} + \frac{n\alpha'}{2} + \frac{n\beta'}{2} \\
&\quad +1 - \sqrt{p} + \alpha' - \beta' - \frac{n}{2} + \frac{n\sqrt{p}}{2} - \frac{n\alpha'}{2} + \frac{n\beta'}{2} \\
&= (n-2) - 2n\left(\frac{1+\sqrt{p}}{2}\right) + (4+2n)\left(\frac{1+\sqrt{p}+\alpha'+\beta'}{4}\right) \\
&\quad +(4-2n)\left(\frac{1-\sqrt{p}+\alpha'-\beta'}{4}\right) \\
&= (n-2) - 2n\omega_2 + (4+2n)\omega_3 + (4-2n)\omega_4.
\end{aligned}$$

$$\begin{aligned}
\sqrt{p}\beta' &= \frac{p}{2}\beta' - \frac{p}{2}\beta' + \sqrt{p}\beta' = \frac{p}{2}\beta' - \frac{1}{2}(p-2\sqrt{p})\beta' \\
&= -2\beta' + \frac{p+4}{2}\beta' + \frac{1}{2}\beta'^3 = -2\beta' + n\alpha' \\
&= -2 - n + 2 + 2\sqrt{p} - 1 - \sqrt{p} - \alpha' - \beta' + \frac{n}{2} + \frac{n\sqrt{p}}{2} + \frac{n\alpha'}{2} + \frac{n\beta'}{2} \\
&\quad +1 - \sqrt{p} + \alpha' - \beta' + \frac{n}{2} - \frac{n\sqrt{p}}{2} + \frac{n\alpha'}{2} - \frac{n\beta'}{2} \\
&= -(2+n) + 4\left(\frac{1+\sqrt{p}}{2}\right) - (4-2n)\left(\frac{1+\sqrt{p}+\alpha'+\beta'}{4}\right) \\
&\quad +(4+2n)\left(\frac{1-\sqrt{p}+\alpha'-\beta'}{4}\right) \\
&= -(2+n) + 4\omega_2 - (4-2n)\omega_3 + (4+2n)\omega_4.
\end{aligned}$$

Los casos (xiii)-(xvi) se deducen fácilmente de lo anterior. El caso $n \equiv 1 \pmod 4$ se demuestra de manera similar.

□

Corolario 2.11. *Sean $\omega_1, \omega_2, \omega_3, \omega_4$ una base entera de K como en el Teorema 2.9. Si $n \equiv 3 \pmod 4$, entonces*

(i) $\omega_2^2 = \dfrac{p-1}{4} + \omega_2.$

(ii) $\omega_2\omega_3 = \dfrac{n^2-1}{8} + \dfrac{3-n}{4}\omega_2 + \dfrac{1+n}{2}\omega_3 + \omega_4.$

(iii) $\omega_2\omega_4 = \dfrac{-p+2n-1}{8} - \dfrac{1+n}{4}\omega_2 + \omega_3 + \dfrac{1-n}{2}\omega_4.$

(iv) $\omega_3\omega_4 = \dfrac{-p+2n+7}{16} - \omega_2 + \dfrac{3-n}{4}\omega_3 - \dfrac{1+n}{4}\omega_4.$

(v) $\omega_3^2 = \dfrac{-p+2n-9}{16} + \dfrac{1-n}{2}\omega_2 + \dfrac{1+n}{2}\omega_3 + \omega_4.$

(vi) $\omega_4^2 = \dfrac{-p-6n-1}{16} + \dfrac{1+n}{2}\omega_2 - \omega_3 + \dfrac{1+n}{2}\omega_4.$

Si $n \equiv 1 \pmod 4$, *entonces*

(i) $\omega_2^2 = \dfrac{p-1}{4} + \omega_2.$

(ii) $\omega_2\omega_3 = \dfrac{n^2-1}{8} + \dfrac{n+3}{4}\omega_2 + \dfrac{1-n}{2}\omega_3 + \omega_4.$

(iii) $\omega_2\omega_4 = \dfrac{-p-2n-1}{8} + \dfrac{n-1}{4}\omega_2 + \omega_3 + \dfrac{1+n}{2}\omega_4.$

(iv) $\omega_3\omega_4 = \dfrac{-p-2n+7}{16} - \omega_2 + \dfrac{3+n}{4}\omega_3 + \dfrac{n-1}{4}\omega_4.$

(v) $\omega_3^2 = \dfrac{-p-2n-9}{16} + \dfrac{1+n}{2}\omega_2 + \dfrac{1-n}{2}\omega_3 + \omega_4.$

(vi) $\omega_4^2 = \dfrac{-p+6n-1}{16} + \dfrac{1-n}{2}\omega_2 - \omega_3 + \dfrac{1-n}{2}\omega_4.$

Demostración. Solo haremos la prueba de los dos primeros casos si $n \equiv 3 \pmod 4$. Por el lema anterior, tenemos

$$\omega_2^2 = \left(\frac{1+\sqrt{p}}{2}\right)^2 = \frac{(1+\sqrt{p})^2}{4} = \frac{p-1+4\omega_2}{4} = \frac{p-1}{4} + \omega_2.$$

$$\begin{aligned}\omega_2\omega_3 &= \frac{1+\sqrt{p}}{2}\cdot\frac{1+\sqrt{p}+\alpha'+\beta'}{4} = \frac{(1+\sqrt{p})^2+(1+\sqrt{p})(\alpha'+\beta')}{8}\\ &= \frac{p-1+4\omega_2-4+(2-2n)\omega_2+(4+4n)\omega_3+8\omega_4}{8}\\ &= \frac{n^2-1}{8} + \frac{3-n}{4}\omega_2 + \frac{1+n}{2}\omega_3 + \omega_4.\end{aligned}$$

Los demás casos se demuestran de manera similar. □

Lema 2.12. *Sea* $K = \mathbb{Q}(\alpha')$ *con* $\alpha' = \sqrt{-(p+2\sqrt{p})}$. *Entonces*

(i) $tr(\omega_2) = 2.$

(ii) $tr(\omega_3) = tr(\omega_4) = 1.$

(iii) $tr(\omega_2^2) = 1+p.$

(iv) $tr(\omega_2\omega_3) = \dfrac{1+p}{2}.$

(v) $tr(\omega_2\omega_4) = \dfrac{1-p}{2}.$

(vi) $tr(\omega_3\omega_4) = tr(\omega_3^2) = tr(\omega_4^2) = \dfrac{1-p}{4}.$

Demostración. Para el caso $n \equiv 3 \pmod 4$, una base entera de K es

$$\omega_1 = 1, \quad \omega_2 = \frac{1+\sqrt{p}}{2}, \quad \omega_3 = \frac{1+\sqrt{p}+\alpha'+\beta'}{4}, \quad \omega_4 = \frac{1-\sqrt{p}+\alpha'-\beta'}{4}.$$

Así, por el Lema 2.6,

$$tr(\omega_2) = tr\left(\frac{1+\sqrt{p}}{2}\right) = \frac{4+tr(\sqrt{p})}{2} = 2.$$

$$tr(\omega_3) = tr\left(\frac{1+\sqrt{p}+\alpha'+\beta'}{4}\right) = \frac{4+tr(\sqrt{p})+tr(\alpha')+tr(\beta')}{4} = 1.$$

$$tr(\omega_4) = tr\left(\frac{1-\sqrt{p}+\alpha'-\beta'}{4}\right) = \frac{4-tr(\sqrt{p})+tr(\alpha')-tr(\beta')}{4} = 1.$$

Ahora por el Corolario 2.11,

$$tr(\omega_2^2) = tr\left(\frac{p-1}{4}+\omega_2\right) = \frac{p-1}{4}4 + tr(\omega_2) = p-1+2 = p+1.$$

$$\begin{aligned} tr(\omega_2\omega_3) &= tr\left(\frac{n^2-1}{8}+\frac{3-n}{4}\omega_2+\frac{1+n}{2}\omega_3+\omega_4\right) \\ &= \frac{n^2-1}{2}+\frac{3-n}{4}tr(\omega_2)+\frac{1+n}{2}tr(\omega_3)+tr(\omega_4) \\ &= \frac{n^2-1}{2}+\frac{3-n}{2}+\frac{1+n}{2}+1 = \frac{1+p}{2}. \end{aligned}$$

$$\begin{aligned} tr(\omega_2\omega_4) &= tr\left(\frac{-p+2n-1}{8}-\frac{1+n}{4}\omega_2+\omega_3+\frac{1-n}{2}\omega_4\right) \\ &= \frac{-p+2n-1}{2}-\frac{1+n}{2}+1+\frac{1-n}{2} = \frac{1-p}{2}. \end{aligned}$$

$$\begin{aligned} tr(\omega_3\omega_4) &= tr\left(\frac{-p+2n+7}{16}-\omega_2+\frac{3-n}{4}\omega_3-\frac{1+n}{4}\omega_4\right) \\ &= \frac{-p+2n+7}{4}-2+\frac{3-n}{4}-\frac{1+n}{4} = \frac{1-p}{4}. \end{aligned}$$

$$\begin{aligned} tr(\omega_3^2) &= tr\left(\frac{-p+2n-9}{16}+\frac{1-n}{2}\omega_2+\frac{1+n}{2}\omega_3+\omega_4\right) \\ &= \frac{-p+2n-9}{4}+1-n+\frac{1+n}{2}+1 = \frac{1-p}{4}. \end{aligned}$$

$$\begin{aligned} tr(\omega_4^2) &= tr\left(-\frac{p+6n+1}{16}+\frac{1+n}{2}\omega_2-\omega_3+\frac{1+n}{2}\omega_4\right) \\ &= -\frac{p+6n+1}{4}+1+n-1+\frac{1+n}{2} = \frac{1-p}{4}. \end{aligned}$$

Para el caso $n \equiv 1 \pmod 4$, la base entera es

$$\omega_1 = 1, \quad \omega_2 = \frac{1+\sqrt{p}}{2}, \quad \omega_3 = \frac{1+\sqrt{p}+\alpha'-\beta'}{4}, \quad \omega_4 = \frac{1-\sqrt{p}+\alpha'+\beta'}{4}.$$

Así, $tr(\omega_2) = 2$ y

$$tr(\omega_3) = tr\left(\frac{1+\sqrt{p}+\alpha'-\beta'}{4}\right) = \frac{4+tr(\sqrt{p})+tr(\alpha')-tr(\beta')}{4} = 1.$$

$$tr(\omega_4) = tr\left(\frac{1-\sqrt{p}+\alpha'+\beta'}{4}\right) = \frac{4-tr(\sqrt{p})+tr(\alpha')+tr(\beta')}{4} = 1.$$

$$tr(\omega_2^2) = tr\left(\frac{p-1}{4} + \omega_2\right) = \frac{p-1}{4}4 + tr(\omega_2) = p - 1 + 2 = p + 1$$

$$\begin{aligned} tr(\omega_2\omega_3) &= tr\left(\frac{n^2-1}{8} + \frac{3+n}{4}\omega_2 + \frac{1-n}{2}\omega_3 + \omega_4\right) \\ &= \frac{n^2-1}{2} + \frac{3+n}{2} + \frac{1-n}{2} + 1 = \frac{1+p}{2} \end{aligned}$$

$$\begin{aligned} tr(\omega_2\omega_4) &= tr\left(\frac{-p-2n-1}{8} + \frac{n-1}{4}\omega_2 + \omega_3 + \frac{1+n}{2}\omega_4\right) \\ &= \frac{-p-2n-1}{2} + \frac{n-1}{2} + 1 + \frac{n+1}{2} = \frac{1-p}{2} \end{aligned}$$

$$\begin{aligned} tr(\omega_3\omega_4) &= tr\left(\frac{-p-2n+7}{16} - \omega_2 + \frac{3+n}{4}\omega_3 + \frac{n-1}{4}\omega_4\right) \\ &= \frac{-p-2n+7}{4} - 2 + \frac{3+n}{4} + \frac{n-1}{4} = \frac{1-p}{4} \end{aligned}$$

$$\begin{aligned} tr(\omega_3^2) &= tr\left(\frac{-p-2n-9}{16} + \frac{1+n}{2}\omega_2 + \frac{1-n}{2}\omega_3 + \omega_4\right) \\ &= \frac{-p-2n-9}{4} + 1 + n + \frac{1-n}{2} + 1 = \frac{1-p}{4} \end{aligned}$$

$$\begin{aligned} tr(\omega_4^2) &= tr\left(\frac{-p+6n-1}{16} + \frac{1-n}{2}\omega_2 - \omega_3 + \frac{1-n}{2}\omega_4\right) \\ &= \frac{-p+6n-1}{4} + 1 - n - 1 + \frac{1-n}{2} = \frac{1-p}{4} \end{aligned}$$

□

Recordemos que en [**17**], los autores calcularon el discriminante de K sin hacer uso de alguna base entera. Nosotros vamos a calcular el discriminante de K haciendo uso de una base entera.

Teorema 2.13. *Sea $K = \mathbb{Q}(\alpha)$ como en el Teorema 2.4. Entonces $\delta_K = p^3$.*

Demostración. Puesto que $\delta_K = \Delta(\omega_1, \omega_2, \omega_3, \omega_4) = det(tr(\omega_i\omega_j))$, entonces por el Lema 2.12,

$$\Delta(\omega_1, \omega_2, \omega_3, \omega_4) = det\begin{pmatrix} 4 & 2 & 1 & 1 \\ 2 & 1+p & \frac{1+p}{2} & \frac{1-p}{2} \\ 1 & \frac{1+p}{2} & \frac{1-p}{4} & \frac{1-p}{4} \\ 1 & \frac{1-p}{2} & \frac{1-p}{4} & \frac{1-p}{4} \end{pmatrix} = p^3. \quad \square$$

2.2. El índice de un campo de números

Sean K un campo de números de grado n, $\theta \in \mathcal{O}_K$ y δ_K el discriminante de K. De la Definición 1.39 sabemos que $\Delta(1, \theta, \ldots, \theta^{n-1}) = ind(\theta)^2 \delta_K$, así, si K es monogénico, entonces de la igualdad anterior, $ind(\theta) = 1$. Para investigar los primos racionales ramificados en un campo de números, es el Teorema 1.52 (Teorema de Dedekind) la herramienta ideal. Antes, necesitamos introducir un objeto aritmético de K conocido como el índice de K definido como

$$ind(K) = mcd\{ind(\alpha) : \alpha \in \mathcal{O}_K \text{ y } K = \mathbb{Q}(\alpha)\}.$$

Puesto que cada campo cuadrático K es monogénico, entonces $ind(K) = 1$. Si K es un campo cúbico, Dedekind [2] fue el primero en encontrar un ejemplo de un campo no monogénico adjuntando una raíz de $x^3 - x^2 - 2x - 8$ a $\mathbb{Q}$. También en el caso cúbico, Engstrom [**11**] mostró que $ind(K) = 1$ ó 2 y Llorente-Nart en [**26**] dieron una condición necesaria y suficiente para que $ind(K) = 2$. Varios autores interesados en el tema han aprovechado el índice para la factorización de ciertos primos racionales; por ejemplo, S. Alaca *et al* en [**1**] dan la factorización explícita de $2\mathcal{O}_K$ en campos cubicos con índice 2. En el caso cuártico, Engstrom [**11**] mostró que $ind(K) = 1, 2, 3, 4, 6$ ó 12 y Spearman-Williams mostraron en [**33**] que todos estos valores se alcanzan en el caso cíclico. Esto no sucede en campos cuárticos puros ($K = \mathbb{Q}(\sqrt[4]{m})$, con m libre de cuartas potencias); en este caso $ind(K) = 1$ ó 2 [**13**].

De acuerdo a las hipótesis del Teorema de Dedekind 1.52, éste será útil para casi todos los primos racionales, excepto aquellos primos q tal que $q \mid ind(\theta)$, en donde $K = \mathbb{Q}(\theta)$, para algún $\theta \in \mathcal{O}_K$; en este caso, algo ingenioso tenemos que hacer para lograr la factorización de $q\mathcal{O}_K$. Escondido en el enunciado del Teorema de Dedekind, se encuentra la ruta a seguir para estudiar la ramificación de éste conjunto finito de primos: buscar un generador de K de tal forma que este generador tenga las propiedades adecuadas para poder aplicar Dedekind.

De acuerdo al Teorema 2.3, cada campo cuártico cíclico K, se puede expresar de forma única como

$$K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right).$$

En nuestro caso, $K = \mathbb{Q}\left(\sqrt{-(p + 2\sqrt{p})}\right)$, de donde

$$A = -1 \equiv 11 \pmod{12}, B = 2 \equiv -1 \pmod{3}, D = p \equiv \pm 1 \pmod{3}.$$

De acuerdo a Theorem A en [**33**] concluimos que $ind(K) = 1$ si $p \equiv 2 \pmod{3}$ e $ind(K) = 3$ si $p \equiv 1 \pmod{3}$. Theorem A en [**33**] da condiciones necesarias y suficientes para que $ind(K)$ sea $1, 2, 3, 4, 6$ ó 12. Por completes enunciamos este teorema tal como aparece en [**33**].

[2] Dedekind publicó los detalles de su ejemplo en *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen,* Gött. Abhandlungen 1878, 1-23. También puede ser encontrado en Dedekind Werke II, 202-223

Theorem A							
$A \equiv$	$B \equiv$	$D \equiv$	$ind(K)$	$A \equiv$	$B \equiv$	$D \equiv$	$ind(K)$
1 (12)	$\pm 1, \pm 2, \pm 5$ (12)		1	5 (12)	$\pm 1, \pm 2, \pm 5$ (12)	1 (3)	3
3 (12)			1	7 (12)	0 (3)		3
5 (12)	$\pm 1, \pm 2, \pm 5$ (12)	2 (3)	1	11 (12)	± 1 (3)	1 (3)	3
5 (12)	$\pm 3, 6$ (12)		1	1 (24)	± 8 (24)		4
7 (12)	± 1 (3)		1	5 (24)	± 4 (24)	2 (3)	4
9(12)	$\pm 1, 2$ (4)		1	5 (24)	12 (24)		4
11 (12)	0 (3)		1	9 (24)	0 (8)		4
11 (12)	± 1 (3)	2 (3)	1	13 (24)	± 4 (24)		4
1 (24)	± 4 (24)		2	17 (24)	0 (24)		4
5 (24)	0 (24)		2	17 (24)	± 8 (24)	2 (3)	4
5 (24)	± 8 (24)	2 (3)	2	21 (24)	4 (8)		4
9 (24)	4 (8)		2	1 (24)	12 (24)		6
13 (24)	± 8 (24)		2	5 (24)	± 8 (24)	1 (3)	6
17 (24)	± 4 (24)	2 (3)	2	13 (24)	0 (24)		6
17 (24)	12 (24)		2	17 (24)	± 4 (24)	1 (3)	6
21 (24)	0 (8)		2	1 (24)	0 (24)		12
1 (12)	$\pm 3, 6$ (12)		3	5 (24)	± 4 (24)	1 (3)	12
				13 (24)	12 (24)		12
				17 (24)	± 8 (24)	1 (3)	12

El siguiente resultado da las condiciones necesarias y suficientes para que $ind(K) = 3$.

Teorema 2.14. *Sea $K = \mathbb{Q}\left(\sqrt{-(p + 2\sqrt{p})}\right)$, con p primo racional de la forma $4 + n^2$. Entonces $ind(K) = 3$ si y solo si $3 \mid n$.*

Demostración. Si $n = 3t$ para algún $t \in \mathbb{Z}$, entonces

$$p = 4 + 9t^2 = 1 + (3 + 9t^2) \equiv 1 \pmod 3.$$

Por Theorem A en [**33**] $ind(K) = 3$. Inversamente, si $ind(K) = 3$, entonces $p \not\equiv 2 \pmod 3$. Como $p = 4 + n^2 > 3$ es primo, entonces $p \equiv 1 \pmod 3$. De lo anterior, $n \equiv 0 \pmod 3$. □

Corolario 2.15. *Sea $K = \mathbb{Q}\left(\sqrt{-(p + 2\sqrt{p})}\right)$, con p primo racional de la forma $4 + n^2$. Entonces $ind(K) = 1$ si y solo si $3 \nmid n$.*

Demostración. Es consecuencia directa del Theorem A en [**33**] y del teorema anterior. □

Ejemplo 2.16. *Sean $K = \mathbb{Q}(\sqrt{-(13 + 2\sqrt{13})})$ y $K' = \mathbb{Q}(\sqrt{-(173 + 2\sqrt{173})})$. Como $13 = 4 + 3^2$, $173 = 4 + 13^2$, por el teorema anterior, $ind(K) = 3$ e $ind(K') = 1$.*

Del teorema anterior concluimos que $q = 3$ es el único primo racional para el cual no podremos aplicar el Teorema de Dedekind, por lo que tendremos que dar la descomposición de $3\mathcal{O}_K$ de otra manera.

En lo que sigue de este capítulo calcularemos la factorización explícita de cualquier primo racional q y dejaremos al final el caso $q = 3$ y $3 \mid n$ por tratarse de un primo especial

pues para la factorización del ideal $3\mathcal{O}_K$ no podemos usar Dedekind; en todos los demás casos se puede utilizar Dedekind.

Sea $K = \mathbb{Q}(\alpha)$, con α raíz de $f(x) = x^4 + px^2 + p$. Puesto que $\delta_K = p^3$, entonces p es el único primo racional que se ramifica en $\mathcal{O}_K$ y el siguiente teorema nos da la forma explícita de dicha ramificación.

Teorema 2.17. *Sea $K = \mathbb{Q}(\alpha)$, con $\alpha = \sqrt{\frac{-1}{2}(p - n\sqrt{p})}$. Entonces $p\mathcal{O}_K = \langle p, \alpha\rangle^4$.*

Demostración. Primero veremos que $N(\sqrt{p}) = p^2$ y $N(\alpha) = p$. Por el Lema 2.8,

$$N(\sqrt{p}) = N\left(\frac{-1}{n}\alpha'\beta'\right) = N\left(\frac{-1}{n}\right)N(\alpha')N(\beta') = \frac{1}{n^4}(n^2p)(n^2p) = p^2.$$

$$N(\alpha) = N\left(\frac{n+2}{2n}\alpha' - \frac{\sqrt{p}}{2n}\alpha'\right) = N\left(\frac{n+2}{2n} - \frac{\sqrt{p}}{2n}\right)N(\alpha') = \frac{1}{n^2}(n^2p) = p.$$

Ahora veamos que $ind(\alpha) = 2^2n^2$. Como $f'(\alpha) = \alpha(4\alpha^2 + 2p)$, entonces

$$N(f'(\alpha)) = N(\alpha \cdot 2n \cdot \sqrt{p}) = N(\alpha)N(2n)N(\sqrt{p}) = p(2n)^4p^2.$$

Por la Proposición 1.41, $\Delta(\alpha) = 2^4n^4p^3$. Así $ind(\alpha) = \sqrt{\frac{2^4n^4p^3}{p^3}} = 2^2n^2$. Finalmente, puesto que $ind(\alpha) \not\equiv 0 \pmod{p}$, entonces por el Teorema de Dedekind, $p\mathcal{O}_K = \langle p, \alpha\rangle^4$. □

Observaciones:

(i) Si $\alpha' = \sqrt{-(p + 2\sqrt{p})}$, entonces $g(x) = Irr(\alpha', \mathbb{Q}) = x^4 + 2px^2 + n^2p$, así que $g'(\alpha') = -8\alpha'\sqrt{p}$ y por tanto

$$N(g'(\alpha')) = N(8)N(\alpha')N(\sqrt{p}) = 8^4n^2p^3.$$

Por lo anterior es claro que entonces $ind(\alpha') = 2^6n$ y $p\mathcal{O}_K = \langle p, \alpha'\rangle^4$.

(ii) Como $\alpha^4 + p\alpha^2 + p = 0$, entonces $p = \alpha(-\alpha^3 - p\alpha)$ y por tanto $\langle p, \alpha\rangle = \langle\alpha\rangle$, es decir, $p\mathcal{O}_K = \langle\alpha\rangle^4$.

2.3. Descomposición de $q\mathcal{O}_K$, $q \nmid n$

Sabemos que p es el único primo racional que se ramifica en $\mathcal{O}_K$, por tanto, cualquier otro primo racional q es no ramificado, es decir, $e = 1$. Así $efg = fg = 4$, de donde

$$g = 1, \quad g = 2, \quad \text{ó} \quad g = 4.$$

Teorema 2.18. *Sean $K = \mathbb{Q}(\alpha)$, con $\alpha = \sqrt{\frac{-1}{2}(p - n\sqrt{p})}$. Para q un primo racional tal que $q \neq 2, p$ y $q \nmid n$ se cumple:*

(i) *Si $\left(\frac{p}{q}\right) = -1$, entonces $q\mathcal{O}_K = \langle q\rangle$ es ideal primo de $\mathcal{O}_K$, es decir, q es inerte en $\mathcal{O}_K$.*

(ii) *Si* $p \equiv t^2 \pmod q$ *para algún* $t \in \mathbb{Z}$ *y* $\left(\dfrac{-p-2t}{q}\right) = -1$*, entonces*

$$q\mathcal{O}_K = \langle q, \alpha^2 + a_1\alpha + a_0\rangle\langle q, \alpha^2 + b_1\alpha + b_0\rangle,$$

donde $a_1, a_0, b_1, b_0 \in \mathbb{Z}$ *satisfacen*

$$x^4 + px^2 + p \equiv (x^2 + a_1x + a_0)(x^2 + b_1x + b_0) \pmod q.$$

(iii) *Si* $p \equiv t^2 \pmod q$ *para algún* $t \in \mathbb{Z}$ *y* $\left(\dfrac{-p-2t}{q}\right) = 1$*, entonces*

$$q\mathcal{O}_K = \langle q, \alpha + a_0\rangle\langle q, \alpha + b_0\rangle\langle q, \alpha + c_0\rangle\langle q, \alpha + d_0\rangle,$$

donde $a_0, b_0, c_0, d_0 \in \mathbb{Z}$ *satisfacen*

$$x^4 + px^2 + p \equiv (x + a_0)(x + b_0)(x + c_0)(x + d_0) \pmod q.$$

Demostración. Por hipótesis, $ind(\alpha) \not\equiv 0 \pmod q$, es decir, podemos usar el Teorema de Dedekind. Notemos que

$$\left(\frac{p^2-4p}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{p-4}{q}\right) = \left(\frac{p}{q}\right).$$

Si $\left(\dfrac{p}{q}\right) = -1$, entonces $\left(\dfrac{p^2-4p}{q}\right) = -1$ y por el Teorema de Carlitz 1.58 parte (iv), $f(x) = x^4 + px^2 + p$ es irreducible en $\mathbb{F}_q[x]$. Por lo tanto $q\mathcal{O}_K = \langle q, \alpha^4 + p\alpha^2 + p\rangle = \langle q\rangle$, es decir, q es inerte en $\mathcal{O}_K$ y más aún, es principal.

Para la afirmación (ii), si $\left(\dfrac{p}{q}\right) = 1$, entonces $\left(\dfrac{p^2-4p}{q}\right) = 1$. Si $\left(\dfrac{-p-2t}{q}\right) = -1$, por el Teorema de Carlitz parte (iii) $f(x) = x^4 + px^2 + p$ es producto de dos polinomios cuadráticos mónicos irreducibles distintos módulo q. Si escribimos

$$x^4 + px^2 + p \equiv (x^2 + a_1x + a_0)(x^2 + b_1x + b_0) \pmod q,$$

y $P_1 = \langle q, \alpha^2 + a_1\alpha + a_0\rangle$, $P_2 = \langle q, \alpha^2 + b_1\alpha + b_0\rangle$, entonces por el Teorema de Dedekind tenemos

$$q\mathcal{O}_K = P_1P_2,$$

con P_1, P_2 ideales primos de O_K.

Para el inciso (iii), si $\left(\dfrac{p}{q}\right) = 1$, entonces

$$\left(\frac{p^2-4p}{q}\right) = \left(\frac{p}{q}\right) = \left(\frac{-p-2t}{q}\right) = 1,$$

y por el Teorema de Carlitz parte (ii), $f(x) = x^4+px^2+p$ es producto de cuatro polinomios lineales mónicos distintos módulo q. Si escribimos

$$x^4 + px^2 + p \equiv (x + a_0)(x + b_0)(x + c_0)(x + d_0) \pmod q$$

y $P_1 = \langle q, \alpha + a_0\rangle$, $P_2 = \langle q, \alpha + b_0\rangle$, $P_3 = \langle q, \alpha + c_0\rangle$, $P_4 = \langle q, \alpha + d_0\rangle$, entonces

$$q\mathcal{O}_K = P_1P_2P_3P_4$$

con P_1, P_2, P_3, P_4 ideales primos de $\mathcal{O}_K$.

□

Corolario 2.19. *Sean K como en el teorema anterior y $q = 3$. Entonces $3\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$.*

Demostración. Como $3 \nmid n$, entonces $n = 3m_0 + t$, con $t = 1, 2$. Por tanto

$$p = 4 + (3m_0 + t)^2 \equiv 2 \pmod 3.$$

Así que, $\left(\frac{p}{3}\right) = -1$ y por el inciso (i) del teorema anterior, $3\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$. □

2.4. Descomposición de $q\mathcal{O}_K,\ q \mid n$ y $q \neq 3$

En el Teorema 2.17 vimos que $ind(\alpha) = 2^2n^2$ y en la observación que sigue a la prueba del mismo teorema mostramos que $ind(\alpha') = 2^6n$. En suma, α y α' no cumplen una de las hipótesis del Teorema de Dedekind para factorizar ideales generados por ciertos primos racionales.

Lema 2.20. *Sean $p = 4 + n^2$ un primo racional y $k \in \mathbb{Z}$. Entonces el polinomio*

$$h(x) = x^4 + 2p(1 + k^2)x^2 + p(4k - n(1 - k^2))^2 \in \mathbb{Z}[x]$$

es irreducible.

Demostración. Sean $b = 2p(1 + k^2)$ y $d = p(4k - n(1 - k^2))^2$ y notemos que

$$\begin{aligned} b^2 - 4d &= 4p^2(1 + k^2)^2 - 4p(4k - n(1 - k^2))^2 \\ &= 4p[(4 + n^2)(1 + 2k^2 + k^4) - (16k^2 - 8kn(1 - k^2) + (1 - k^2)^2n^2)] \\ &= 16p((1 - k^2) + kn)^2. \\ -b + 2\sqrt{d} &= -2p(1 + k^2) + 2(4k - n(1 - k^2))\sqrt{p}. \\ -b - 2\sqrt{d} &= -2p(1 + k^2) - 2(4k - n(1 - k^2))\sqrt{p}. \end{aligned}$$

De lo anterior, $b^2-4d, -b+2\sqrt{d}, -b-2\sqrt{d} \notin \mathbb{Q}^2$. Por el Teorema 1.57, $h(x)$ es irreducible. □

Proposición 2.21. *Sea $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p + 2\sqrt{p})}$ y $\beta' = \sqrt{-(p - 2\sqrt{p})}$. Entonces*

(i) $\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha' + k\beta')$ *para todo* $k \in \mathbb{Z}$.
(ii) $ind(\alpha' + k\beta') = 2^6(4k - n(1 - k^2))(k^2 - 1 - kn)^2$.

Demostración. Para el inciso (i) notemos que $\alpha', \beta' \in \mathbb{Q}(\alpha')$, así $\mathbb{Q}(\alpha' + k\beta') \subseteq \mathbb{Q}(\alpha')$, ahora notemos que si $x = \alpha' + k\beta'$, entonces

$$\begin{aligned} x^2 &= (\alpha' + k\beta')^2 \\ &= \alpha'^2 + 2k\alpha'\beta' + k^2\beta' \\ &= -(p + 2\sqrt{p}) - 2kn\sqrt{p} - k^2(p - 2\sqrt{p}) \end{aligned}$$

Así $x^2 + p(1 + k^2) = (-1 + k^2 - kn)2\sqrt{p}$, si elevamos al cuadrado la igualdad anterior,

$$x^4 + 2p(1 + k^2)x^2 + p^2(1 + k^2)^2 = (1 - 2(k^2 - kn) + (k^2 - kn)^2)4p,$$

de donde $x^4 + 2p(1+k^2)x^2 + p^2(1+k^2)^2 - 4p(1-2(k^2-kn)+(k^2-kn)^2) = 0$ y así $x^4 + 2p(1+k^2)x^2 + p(4k-n(1-k^2))^2 = 0$, es decir $h(\alpha' + k\beta') = 0$ y por el lema anterior, $h(x) = Irr(\alpha' + k\beta', \mathbb{Q})$. Por lo tanto

$$[\mathbb{Q}(\alpha' + k\beta') : \mathbb{Q}] = 4.$$

De lo anterior, $\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha' + k\beta')$. Para la afirmación (ii), sabemos que

$$ind(\alpha' + k\beta') = \sqrt{\frac{D(\alpha' + k\beta')}{\delta_K}} \quad \text{y} \quad D(\alpha' + k\beta') = N(h'(\alpha' + k\beta')),$$

y como

$$h'(\alpha' + k\beta') = 4(\alpha' + k\beta')((\alpha' + k\beta')^2 + p(1+k^2)) = 4(\alpha' + k\beta')(2k^2 - 2 - 2kn)\sqrt{p},$$

entonces

$$\begin{aligned} N(h'(\alpha' + k\beta')) &= N(4)N(\alpha' + k\beta')N(2k^2 - 2 - 2kn)N(\sqrt{p}) \\ &= 4^4 p(4k - n(1-k^2))^2(2k^2 - 2 - 2kn)^4 p^2. \end{aligned}$$

Así

$$\begin{aligned} ind(\alpha' + k\beta') &= \sqrt{\frac{4^4 p^3 (4k - n(1-k^2))^2 (2k^2 - 2 - 2kn)^4}{p^3}} \\ &= 2^6(4k - n(1-k^2))(k^2 - 1 - kn)^2. \end{aligned}$$

□

Sea q un primo racional tal que $q|n$. Es fácil verificar que $q|ind(\alpha' + k\beta')$ si y solo si $q|k-1$ ó $q|k$ ó $q|k+1$.

Proposición 2.22. *Sean $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p + 2\sqrt{p})}$, $\theta_1 = \alpha' + 2\beta'$ y q un primo impar tal que $q \mid n$, $q \neq 3$. Entonces*

(i) $\mathbb{Q}(\alpha') = \mathbb{Q}(\theta_1)$.
(ii) $q \nmid ind(\theta_1)$.

Demostración. La afirmación (i) se cumple por la proposición anterior parte (i) tomando $k = 2$. Para la afirmación (ii), tenemos

$$ind(\theta_1) = 2^6(3n+8)(3-2n)^2.$$

Por lo que

(1) Si $q \mid 3n+8$, entonces $q = 2$, lo cual no es posible, por tanto $q \nmid 3n+8$.
(2) Si $q \mid (3-2n)^2$, entonces $q = 3$, lo cual no puede ser, por tanto $q \nmid (3-2n)^2$.

Por lo tanto $q \nmid ind(\theta_1)$. □

Teorema 2.23. *Sean $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p + 2\sqrt{p})}$ y q primo impar tal que $q \mid n$ y $q \neq 3$.*

(i) *Si $q \equiv 5, 7 \pmod 8$, entonces $q\mathcal{O}_K = \langle q, \theta_1^2 + a_1\theta_1 + a_0\rangle\langle q, \theta_1^2 + b_1\theta_1 + b_0\rangle$ donde $a_1, a_0, b_1, b_0 \in \mathbb{Z}$ satisfacen*

$$x^4 + ax^2 + b \equiv (x^2 + a_1x + a_0)(x^2 + b_1x + b_0) \mod q.$$

(ii) *Si* $q \equiv 1, 3 \pmod 8$, *entonces* $q\mathcal{O}_K = \langle q, \theta_1+a_0\rangle\langle q, \theta_1+b_0\rangle\langle q, \theta_1+c_0\rangle\langle q, \theta_1+d_0\rangle$ *donde* $a_0, b_0, c_0, d_0 \in \mathbb{Z}$ *satisfacen*

$$x^4 + ax^2 + b \equiv (x + a_0)(x + b_0)(x + c_0)(x + d_0) \pmod q.$$

Demostración. Como $K = \mathbb{Q}(\theta_1)$, con $\theta_1 = \alpha' + 2\beta'$ y $ind(\theta_1) \not\equiv 0 \pmod q$, podemos aplicar el Teorema de Dedekind. Recordemos que $Irr(\theta_1, \mathbb{Q}) = x^4 + 10px^2 + p(3n + 8)^2$. Si $q = 5$, la factorización de $Irr(\theta_1, \mathbb{Q})$ en $\mathbb{F}_5[x]$ es

$$x^4 + 10px^2 + p(3n + 8)^2 \equiv x^4 + 1 \equiv (x^2 + 2)(x^2 + 3) \pmod 5,$$

así que

$$5\mathcal{O}_K = \langle 5, \theta_1^2 + 2\rangle\langle 5, \theta_1^2 + 3\rangle.$$

Para $q > 5$

$$x^4 + 10px^2 + p(3n + 8)^2 \equiv x^4 + ax^2 + b \pmod q,$$

con $a \equiv 2^3 \cdot 5 \pmod q$ y $b \equiv (2^4)^2 \pmod q$. Notemos que

$$\left(\frac{b}{q}\right) = 1 \quad \text{y} \quad \left(\frac{a^2 - 4b}{q}\right) = \left(\frac{2^6 \cdot 5^2 - 4 \cdot 2^8}{q}\right) = \left(\frac{3^2}{q}\right) = 1.$$

Si $t = 2^4$ como en el Teorema de Carlitz 1.58, afirmación (ii) ó (iii), tenemos

$$\left(\frac{-a - 2t}{q}\right) = \left(\frac{-2^3 \cdot 5 - 2 \cdot 2^4}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right).$$

Por lo tanto, por las Leyes Suplementarias

$$\left(\frac{-a - 2t}{q}\right) = \begin{cases} 1 & \text{si} \quad q \equiv 1, 3 \pmod 8 \\ -1 & \text{si} \quad q \equiv 5, 7 \pmod 8 \end{cases}.$$

Por lo anterior, si $q \equiv 5, 7 \pmod 8$, por el Teorema de Carlitz parte (iii), $x^4 + ax^2 + b$ es producto de dos polinomios cuadráticos mónicos irreducibles distintos en $\mathbb{F}_q[x]$. Si escribimos $x^4 + ax^2 + b \equiv (x^2 + a_1x + a_0)(x^2 + b_1x + b_0)$ en $\mathbb{F}_q[x]$ y

$$P_1 = \langle q, \theta_1^2 + a_1\theta_1 + a_0\rangle, \quad P_2 = \langle q, \theta_1^2 + b_1\theta_1 + b_0\rangle,$$

entonces

$$q\mathcal{O}_K = P_1P_2$$

con P_1, P_2 ideales primos de $\mathcal{O}_K$. Si $q \equiv 1, 3 \pmod 8$, por el Teorema de Carlitz parte (ii), $x^4 + ax^2 + b$ es producto de cuatro polinomios lineales mónicos distintos en $\mathbb{F}_q[x]$. Si escribimos

$$x^4 + ax^2 + b \equiv (x + a_0)(x + b_0)(x + c_0)(x + d_0) \pmod q,$$

y $P_1 = \langle q, \theta_1 + a_0\rangle, P_2 = \langle q, \theta_1 + b_0\rangle, P_3 = \langle q, \theta_1 + c_0\rangle, P_4 = \langle q, \theta_1 + d_0\rangle$, entonces

$$q\mathcal{O}_K = P_1P_2P_3P_4,$$

con P_1, P_2, P_3, P_4 son ideales primos de $\mathcal{O}_K$. □

2.5. Descomposición de $2\mathcal{O}_K$

Hasta este momento tenemos $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha') = \mathbb{Q}(\theta_1)$ con

$$ind(\alpha) \equiv ind(\alpha') \equiv ind(\theta_1) \equiv 0 \pmod 2,$$

de modo que si queremos utilizar el Teorema de Dedekind, tendremos que encontrar un nuevo generador $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$ e $ind(\theta) \not\equiv 0 \pmod 2$. Sabemos que este nuevo generador existe pues $ind(K) \neq 2$.

Lema 2.24. *Sea* $\theta = \dfrac{1+\alpha'}{2}$, *con* $\alpha' = \sqrt{-(p+2\sqrt{p})}$. *Entonces*

(i) $h(x) = Irr(\theta, \mathbb{Q}) = x^4 - 2x^3 + 2(k+1)x^2 - (2k+1)x + k^2$, *donde* $k \in \mathbb{Z}$ *es tal que* $p = 4k+1$.

(ii) *El polinomio* $r(x) = x^4 + x + 1$ *es irreducible en* $\mathbb{F}_2[x]$.

Demostración. La afirmación (i) se sigue de observar que $h(\theta) = 0$ y $h(x + \dfrac{1}{2})$ es irreducible en $\mathbb{Q}[x]$. Para la afirmación (ii) supongamos que $r(x)$ no es irreducible módulo 2. Entonces algunas de las siguientes factorizaciones se cumple en $\mathbb{F}_2[x]$:

$$x^4 + x + 1 \equiv (x + a_0)(x^3 + b_2x^2 + b_1x + b_0) \pmod 2,$$

$$x^4 + x + 1 \equiv (x^2 + a_1x + a_0)(x^2 + b_1x + b_0) \pmod 2,$$

$$x^4 + x + 1 \equiv (x + a_0)(x + b_0)(x + c_0)(x + d_0) \pmod 2.$$

En el primer caso tenemos las siguientes relaciones entre coeficientes:

$$\begin{cases} b_2 + a_0 \equiv 0 \pmod 2 & (1) \\ b_1 + a_0b_2 \equiv 0 \pmod 2 & (2) \\ b_0 + a_0b_1 \equiv 1 \pmod 2 & (3) \\ a_0b_0 \equiv 1 \pmod 2 & (4) \end{cases}$$

de (4), $a_0 \equiv b_0 \equiv 1 \pmod 2$, ahora por (1), $b_2 \equiv 1 \pmod 2$ y por (2), $b_1 \equiv 1 \pmod 2$. Por tanto (3) no es posible. En los otros dos casos concluimos lo mismo. Por lo tanto $r(x) = x^4 + x + 1$ es irreducible en $\mathbb{F}_2[x]$.

□

De acuerdo a la afirmación (i) del lema anterior, θ es un entero algebraico y

$$tr(\theta^j) = \frac{1}{2^j} \sum_{k=0}^{j} \binom{j}{k} tr(\alpha'^{j-k}).$$

Lema 2.25. *Sean* $\alpha = \sqrt{\frac{-1}{2}(p - n\sqrt{p})}$, $\alpha' = \sqrt{-(p+2\sqrt{p})}$ *y* $\theta = \dfrac{1+\alpha'}{2}$. *Entonces*

(i) $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$.

(ii) $ind(\theta) = n$.

Demostración. El Teorema 2.4 nos asegura que $\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha)$, así que $\theta = \dfrac{1+\alpha'}{2} \in \mathbb{Q}(\alpha)$. Por tanto $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha)$. Por la afirmación (i) del lema anterior, $[\mathbb{Q}(\theta) : \mathbb{Q}] = 4$ y

por tanto $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$. Para la afirmación (ii) primero vamos a calcular las entradas de la matriz $(tr(\theta^i))$:

$$tr(\theta) = \frac{1}{2}tr(1+\alpha') = \frac{1}{2}(4+0) = 2,$$
$$tr(\theta^2) = \frac{1}{4}tr((1+\alpha')^2) = \frac{1}{4}(4-4p) = 1-p,$$
$$tr(\theta^3) = \frac{1}{8}tr((1+\alpha')^3) = \frac{1}{8}(4-12p) = \frac{1-3p}{2},$$
$$tr(\theta^4) = \frac{1}{16}tr((1+\alpha')^4) = \frac{1}{16}(4-24p+4p(p+4)) = \frac{(p-1)^2}{4},$$
$$tr(\theta^5) = \frac{1}{32}tr((1+\alpha')^5) = \frac{1}{32}(4-40p+20p(p+4)) = \frac{1+10p+5p^2}{8},$$
$$tr(\theta^6) = \frac{1}{64}tr((1+\alpha')^6) = \frac{1}{64}(4-60p+60p(p+4)-4p^2(p+12)) = \frac{1+45p+3p^2-p^3}{16}.$$

Por lo tanto

$$\Delta(1,\theta,\theta^2,\theta^3) = det\begin{pmatrix} 4 & 2 & 1-p & \frac{1-3p}{2} \\ 2 & 1-p & \frac{1-3p}{2} & \frac{(p-1)^2}{4} \\ 1-p & \frac{1-3p}{2} & \frac{(p-1)^2}{4} & \frac{1+10p+5p^2}{8} \\ \frac{1-3p}{2} & \frac{(p-1)^2}{4} & \frac{1+10p+5p^2}{8} & \frac{1+45p+3p^2-p^3}{16} \end{pmatrix} = n^2p^3.$$

Así obtenemos $ind(\theta) = \sqrt{\frac{n^2p^3}{p^3}} = n$. □

Teorema 2.26. *Sea $K = \mathbb{Q}(\alpha)$ con $\alpha = \sqrt{\frac{-1}{2}(p - n\sqrt{p})}$. Entonces $2\mathcal{O}_K$ es un ideal primo principal de $\mathcal{O}_K$.*

Demostración. Por el lema anterior, $K = \mathbb{Q}(\theta)$ con $ind(\theta) = n$ y n impar, es decir, $ind(\theta) \not\equiv 0 \pmod 2$. Por tanto podemos usar el Teorema de Dedekind.

Sabemos que $Irr(\theta, \mathbb{Q}) = x^4 - 2x^3 + 2(k+1)x^2 - (2k+1)x + k^2$. Por otro lado, $p = 4 + n^2$, con $n = 2l + 1$ para algún $l \in \mathbb{Z}$. Entonces $p = 4k + 1 = 4l^2 + 4l + 5$, de donde $k = l^2 + l + 1$. Así,

$$x^4 - 2x^3 + 2(k+1)x^2 - (2k+1)x + k^2 \equiv x^4 + x + 1 \pmod 2,$$

el cual, por el Lema 2.24 parte (ii), es irreducible en $\mathbb{F}_2[x]$. Por lo tanto,

$$2\mathcal{O}_K = \langle 2, \theta^4 + \theta + 1\rangle.$$

Finalmente observemos que $N(\langle 2, \theta^4 + \theta + 1\rangle) = 2^4$, $N(\langle 2\rangle) = N(2) = 2^4$ y $\langle 2\rangle \subseteq \langle 2, \theta^4 + \theta + 1\rangle$, así $\langle 2, \theta^4 + \theta + 1\rangle = \langle 2\rangle$.

□

2.6. Descomposición de $3\mathcal{O}_K$, con $3 \mid n$

En el Corolario 2.19 probamos que si $3 \nmid n$, entonces $3\mathcal{O}_K$ es un ideal primo en $\mathcal{O}_K$. En el caso en que $3|n$ no podremos utilizar el Teorema de Dedekind pues en este caso

$ind(K) = 3$ lo que nos dice es que no existe un generador $\gamma \in \mathcal{O}_K$ tal que $3 \nmid ind(\gamma)$. De modo que tendremos que factorizar $3\mathcal{O}_K$ con una estrategia diferente.

Lema 2.27. *Sean $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p+2\sqrt{p})}$ y $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ la base entera de $\mathcal{O}_K$ que aparece en el Teorema 2.9. Entonces*

(i) $\dfrac{3+\alpha'}{2} = 1 + \omega_3 + \omega_4.$
(ii) $\dfrac{5-\alpha'}{2} = 3 - \omega_3 - \omega_4.$
(iii) $\dfrac{5+\alpha'}{2} = 2 + \omega_3 + \omega_4.$

Demostración. Si $n \equiv 3 \pmod 4$, entonces

$$\omega_1 = 1, \quad \omega_2 = \frac{1+\sqrt{p}}{2}, \quad \omega_3 = \frac{1+\sqrt{p}+\alpha'+\beta'}{4}, \quad \omega_4 = \frac{1-\sqrt{p}+\alpha'-\beta'}{4}$$

es una base entera de $\mathcal{O}_K$. Así

$$\begin{aligned} 1 + \omega_3 + \omega_4 &= 1 + \frac{1+\sqrt{p}+\alpha'+\beta'}{4} + \frac{1-\sqrt{p}+\alpha'-\beta'}{4} \\ &= \frac{4+1+\sqrt{p}+\alpha'+\beta'+1-\sqrt{p}+\alpha'-\beta'}{4} \\ &= \frac{3+\alpha'}{2}. \end{aligned}$$

Las afirmaciones (ii) y (iii) se justifican de manera similar. El caso $n \equiv 1 \pmod 4$ es idéntico.

□

Proposición 2.28. *Sea $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p+2\sqrt{p})}$. Consideremos los ideales*

$$M = \left\langle 3, \frac{3+\alpha'}{2} \right\rangle, \quad P_1 = \left\langle 3, \frac{5-\alpha'}{2} \right\rangle, \quad P_2 = \left\langle 3, \frac{5+\alpha'}{2} \right\rangle.$$

Entonces

(i) $M = 3\mathbb{Z} + (3+3\omega_3)\mathbb{Z} + (-4+\omega_2-3\omega_3)\mathbb{Z} + (1+\omega_3+\omega_4)\mathbb{Z}$.
(ii) $P_1 = 3\mathbb{Z} + (-17+\omega_3)\mathbb{Z} + (-8+\omega_2+\omega_3)\mathbb{Z} + (-3+\omega_3+\omega_4)\mathbb{Z}$.
(iii) $P_2 = 3\mathbb{Z} + (-1+\omega_3)\mathbb{Z} + (\omega_2+3\omega_3)\mathbb{Z} + (2+\omega_3+\omega_4)\mathbb{Z}$.

Demostración. Primero analizemos el caso $n \equiv 3 \pmod 4$. Para $\gamma \in M$, tenemos que $\gamma = 3\gamma_1 + \left(\frac{3+\alpha'}{2}\right)\gamma_2$, para ciertos $\gamma_1, \gamma_2 \in \mathcal{O}_K$. Así

$$\begin{aligned}
\gamma &= 3\gamma_1 + \left(\frac{3+\alpha'}{2}\right)\gamma_2 \\
&= 3(a_1 + a_2\omega_2 + a_3\omega_3 + a_4\omega_4) + (1 + \omega_3 + \omega_4)(b_1 + b_2\omega_2 + b_3\omega_3 + b_4\omega_4) \\
&= \left[3a_1 + b_1 + \frac{n-3}{4}b_2 + \frac{-p+2n-1}{8}b_3 + \frac{-p-2n+3}{8}b_4\right] \\
&\quad + \left[3a_2 - \frac{n-3}{2}b_2 - \frac{n+1}{2}b_3 + \frac{n-1}{2}b_4\right]\omega_2 \\
&\quad + \left[3a_3 + b_1 + \frac{n+3}{2}b_2 + \frac{n+9}{4}b_3 - \frac{n+1}{4}b_4\right]\omega_3 \\
&\quad + \left[3a_4 + b_1 + \frac{3-n}{2}b_2 + \frac{3-n}{4}b_3 + \frac{n+5}{4}b_4\right]\omega_4.
\end{aligned}$$

Si escribimos $n = 4l + 3$ para algún $l \in \mathbb{Z}$, entonces

$$\begin{aligned}
\gamma &= \left[3a_1 + b_1 + lb_2 - (2l^2 + 2l + 1)b_3 - (2l^2 + 4l + 2)b_4\right] \\
&\quad + \left[3a_2 - 2lb_2 - (2l + 2)b_3 + (2l + 1)b_4\right]\omega_2 \\
&\quad + \left[3a_3 + b_1 + (2l + 3)b_2 + (l + 3)b_3 - (l + 1)b_4\right]\omega_3 \\
&\quad + \left[3a_4 + b_1 - 2lb_2 - lb_3 + (l + 2)b_4\right]\omega_4.
\end{aligned}$$

Sea $x = 3a_4 + b_1 - 2lb_2 - lb_3 + (l + 2)b_4$. Entonces $b_1 = x - 3a_4 + 2lb_2 + lb_3 - (l + 2)b_4$. Así

$$\begin{aligned}
\gamma &= \left[3a_1 - 3a_4 + 3lb_2 - (2l^2 + l + 1)b_3 - (2l^2 + 5l + 4)b_4\right] \\
&\quad + \left[3a_2 - 2lb_2 - (2l + 2)b_3 + (2l + 1)b_4\right]\omega_2 \\
&\quad + \left[3a_3 - 3a_4 + (4l + 3)b_2 + (2l + 3)b_3 - (2l + 3)b_4\right]\omega_3 + (1 + \omega_3 + \omega_4)x.
\end{aligned}$$

Si $y = 3a_2 - 2lb_2 - (2l+2)b_3 + (2l+1)b_4$, entonces $(2l+1)b_4 = y - 3a_2 + 2lb_2 + (2l+2)b_3$. Así que

$$\begin{aligned}
\gamma &= \left[3a_1 + 12a_2 - 3a_4 - 5lb_2 - (2l^2 + 9l + 9)b_3 - (2l^2 - 3l)b_4\right] \\
&\quad + \left[3a_3 + 9a_2 - 3a_4 + (-2l + 3)b_2 - (4l + 3)b_3 + 4lb_4\right]\omega_3 \\
&\quad + (-4 + \omega_2 - 3\omega_3)y + (1 + \omega_3 + \omega_4)x.
\end{aligned}$$

Como $3 \mid n$ y $n = 4l + 3$, tenemos $l = 3t$, para algún $t \in \mathbb{Z}$. Por tanto

$$\begin{aligned}
\gamma &= \left[3a_1 + 12a_2 - 3a_4 - 5lb_2 - (2l^2 + 9l + 9)b_3 - (2l^2 - 3l)b_4\right] \\
&\quad + 3\left[a_3 + 3a_2 - a_4 + (-2t + 1)b_2 - (4t+)b_3 + 4tb_4\right]\omega_3 \\
&\quad + (-4 + \omega_2 - 3\omega_3)y + (1 + \omega_3 + \omega_4)x.
\end{aligned}$$

Sea $z = a_3 + 3a_2 - a_4 + (-2t + 1)b_2 - (4t + 1)b_3 + 4tb_4$. Entonces $a_4 = -z + a_3 + 3a_2 + (-2t + 1)b_2 - (4t+)b_3 + 4tb_4$.

$$\begin{aligned}\gamma &= 3\left[a_1+a_2-a_3-(1+3t)b_2-(6t^2+13t+4)b_3-(6t^2+t)b_4\right]\\ &\quad +(3+3\omega_3)z+(-4+\omega_2-3\omega_3)y+(1+\omega_3+\omega_4)x.\end{aligned}$$

Por lo tanto, $M = 3\mathbb{Z}+(3+3\omega_3)\mathbb{Z}+(-4+\omega_2-3\omega_3)\mathbb{Z}+(1+\omega_3+\omega_4)\mathbb{Z}$.
Para $\delta \in P_1$, $\delta = 3\delta_1 + \left(\dfrac{5-\alpha'}{2}\right)\delta_2$, con $\delta_1, \delta_2 \in \mathcal{O}_K$. Entonces

$$\begin{aligned}\delta &= 3\delta_1+\left(\frac{5-\alpha'}{2}\right)\delta_2\\ &= 3(c_1+c_2\omega_2+c_3\omega_3+c_4\omega_4)+(3-\omega_3-\omega_4)(d_1+d_2\omega_2+d_3\omega_3+d_4\omega_4)\\ &= \left[3c_1+3d_1-ld_2+(2l^2+2l+1)d_3+2(l+1)^2d_4\right]\\ &\quad +\left[3c_2+(2l+4)d_2+(2l+2)d_3-(2l+1)d_4\right]\omega_2\\ &\quad +\left[3c_3-d_1-(2l+3)d_2+(1-l)d_3+(l+1)d_4\right]\omega_3\\ &\quad +\left[3c_4-d_1+2ld_2+ld_3+(2-l)d_4\right]\omega_4.\end{aligned}$$

Sea $x = 3c_4-d_1+2ld_2+ld_3+(2-l)d_4$. Entonces $d_1 = -x+3c_4+2ld_2+ld_3+(2-l)d_4$. Así

$$\begin{aligned}\delta &= \left[3c_1+9c_4+5ld_2+(2l^2+5l+1)d_3+(2l^2+l+8)d_4\right]\\ &\quad +\left[3c_2+(2l+4)d_2+(2l+2)d_3-(2l+1)d_4\right]\omega_2\\ &\quad +\left[3c_3-3c_4-(4l+3)d_2+(1-2l)d_3+(2l-1)d_4\right]\omega_3+(-3+\omega_3+\omega_4)x.\end{aligned}$$

Sea $y = 3c_2+(2l+4)d_2+(2l+2)d_3-(2l+1)d_4$. Entonces $-(2l+1)d_4 = y-3c_2-(2l+4)d_2-(2l+2)d_3$. Así que

$$\begin{aligned}\delta &= \left[3c_1+24c_2+9c_4+(21l+32)d_2+(2l^2+21l+17)d_3+(2l^2-15l)d_4\right]\\ &\quad +\left[3c_3-3c_2-3c_4-(4l+7)d_2-(4l+1)d_3+4ld_4\right]\omega_3\\ &\quad +(-8+\omega_2+\omega_3)y+(-3+\omega_3+\omega_4)x.\end{aligned}$$

Sea $z = 3c_3-3c_2-3c_4-(4l+7)d_2-(4l+1)d_3+4ld_4$. Entonces $-(4l+1)d_3 = z-3c_3+3c_2+3c_4+(4l+7)d_2-4ld_4$. Por lo tanto

$$\begin{aligned}\delta &= 3\left[c_1-9c_2+17c_3-14c_4-(47t+29)d_2+(6t^2-47t)d_3+(6t^2+53t)d_4\right]\\ &\quad +(-17+\omega_3)z+(-8+\omega_2+\omega_3)y+(-3+\omega_3+\omega_4)x.\end{aligned}$$

Por lo anterior, $P_1 = 3\mathbb{Z}+(-17+\omega_3)\mathbb{Z}+(-8+\omega_2+\omega_3)\mathbb{Z}+(-3+\omega_3+\omega_4)\mathbb{Z}$.

Para $\mu \in P_2$, $\delta = 3\mu_1 + \left(\frac{5+\alpha'}{2}\right)\mu_2$, con $\mu_1, \mu_2 \in \mathcal{O}_K$. Así tenemos

$$\begin{aligned}
\mu &= 3\mu_1 + \left(\frac{5+\alpha'}{2}\right)\mu_2 \\
&= 3(e_1 + e_2\omega_2 + e_3\omega_3 + e_4\omega_4) + (2 + \omega_3 + \omega_4)(f_1 + f_2\omega_2 + f_3\omega_3 + f_4\omega_4) \\
&= \left[3e_1 + 2f_1 + lf_2 - (2l^2 + 2l + 1)f_3 - 2(l+1)^2 f_4\right] \\
&\quad + \left[3e_2 + (1-2l)f_2 - (2l+2)f_3 + (2l+1)f_4\right]\omega_2 \\
&\quad + \left[3e_3 + f_1 + (2l+3)f_2 + (l+4)f_3(l+1)f_4\right]\omega_3 \\
&\quad + \left[3e_4 + f_1 - 2lf_2 - lf_3 + (l+3)f_4\right]\omega_4.
\end{aligned}$$

Sea $x = 3e_4 + f_1 - 2lf_2 - lf_3 + (l+3)f_4$. Entonces $f_1 = x - 3e_4 + 2lf_2 + lf_3 - (l+3)f_4$ y así

$$\begin{aligned}
\mu &= \left[3e_1 - 6e_4 + 5lf_2 - (2l^2 + 4l + 1)f_3 + (-2l^2 - 6l - 8)f_4\right] \\
&\quad + \left[3e_2 + (1-2l)f_2 - (2l+2)f_3 + (2l+1)f_4\right]\omega_2 \\
&\quad + \left[3e_3 - 3e_4 + (4l+3)f_2 + (2l+4)f_3 - (2l+4)f_4\right]\omega_3 + (2 + \omega_3 + \omega_4)x.
\end{aligned}$$

Sea $y = 3e_2 + (1-2l)f_2 - (2l+2)f_3 + (2l+1)f_4$. Entonces $(1-2l)f_2 = y - 3e_2 + (2l+2)f_3 - (2l+1)f_4$. Por lo tanto

$$\begin{aligned}
\mu &= \left[3e_1 - 6e_4 + 5lf_2 - (2l^2 + 4l + 1)f_3 + (-2l^2 - 6l - 8)f_4\right] \\
&\quad + \left[3e_3 - 3e_4 + 10lf_2 - 9e_2 + (8l+10)f_3 - (8l+7)f_4\right]\omega_3 \\
&\quad + (\omega_2 + 3\omega_3)y + (2 + \omega_3 + \omega_4)x.
\end{aligned}$$

Sea $z = 3e_3 - 3e_4 + 10lf_2 - 9e_2 + (8l+10)f_3 - (8l+7)f_4$. Entonces $(8l+7)f_4 = -z + 3e_3 - 3e_4 + 10lf_2 - 9e_2 + (8l+10)f_3$. Así que

$$\begin{aligned}
\mu &= 3\left[e_1 - 3e_2 + e_3 - 3e_4 + 5lf_2 + (-6t^2 + 4t + 3)f_3 - (6t^2 + 14t + 5)f_4\right] \\
&\quad + (-1 + \omega_3)z + (\omega_2 + 3\omega_3)y + (2 + \omega_3 + \omega_4)x.
\end{aligned}$$

Por lo anterior, es claro que $P_2 = 3\mathbb{Z} + (-1+\omega_3)\mathbb{Z} + (\omega_2 + 3\omega_3)\mathbb{Z} + (2 + \omega_3 + \omega_4)\mathbb{Z}$.

El caso $n \equiv 1 \pmod 4$ es similar. □

Corolario 2.29. *Sean $K = \mathbb{Q}(\alpha')$, M, P_1 y P_2 como en la proposición anterior. Entonces $N(M) = 9$, $N(P_1) = N(P_2) = 3$.*

Demostración. De acuerdo a la proposición anterior, una base entera para M es:

$$3, \quad 3 + 3\omega_3, \quad -4 + \omega_2 - 3\omega_3, \quad 1 + \omega_3 + \omega_4.$$

Para calcular el discriminante de la base entera anterior necesitamos lo siguiente:

$$\begin{aligned}
&tr(9) = 36, \\
&tr(3(3 + 3\omega_3)) = 9tr(1 + \omega_3) = 9(4+1) = 45, \\
&tr(3(-4 + \omega_2 - 3\omega_3)) = 3tr(-4 + \omega_2 - 3\omega_3) = 3(-16 + 2 - 3) = -51, \\
&tr(3(1 + \omega_3 + \omega_4)) = 3tr(1 + \omega_3 + \omega_4) = 3(4 + 1 + 1) = 18,
\end{aligned}$$

$$tr((3+3\omega_3)^2) = 9tr(1+2\omega_3+\omega_3^2) = 9\left(4+2+\frac{1-p}{4}\right),$$

$$tr((3+3\omega_3)(-4+\omega_2-3\omega_3)) = 3tr(-4+\omega_2-7\omega_3+\omega_2\omega_3-3\omega_3^2) = 3\left(-16+2-7+\frac{1+p}{2}-3\frac{1-p}{4}\right) = 15\left(\frac{p-17}{4}\right),$$

$$tr((3+3\omega_3)(1+\omega_3+\omega_4)) = 3tr((1+\omega_3)^2+\omega_4+\omega_3\omega_4) = 3\left(\frac{25-p}{4}+1+\frac{1-p}{4}\right) = 3\left(\frac{15-p}{2}\right),$$

$$tr((-4+\omega_2-3\omega_3)^2) = tr(16-8(\omega_2-3\omega_3)+(\omega_2-3\omega_3)^2) = 16(4)-8(-1)+\frac{1-17p}{4} = \frac{289-17p}{4},$$

$$tr((-4+\omega_2-3\omega_3)(1+\omega_3+\omega_4)) = \frac{-51+3p}{4},$$

$tr((1+\omega_3+\omega_4)^2) = tr(1+2(\omega_3+\omega_4)+(\omega_3+\omega_4)^2) = 4+4+1-p = 9-p.$
Finalmente, puesto que

$$\Delta(3,3+3\omega_3,-4+\omega_2-3\omega_3,1+\omega_3+\omega_4) = det\begin{pmatrix} 36 & 45 & -51 & 18 \\ 45 & \frac{225-9p}{4} & \frac{15p-255}{4} & \frac{45-3p}{2} \\ -51 & \frac{15p-255}{4} & \frac{289-17p}{4} & \frac{3p-51}{2} \\ 18 & \frac{45-3p}{2} & \frac{3p-51}{2} & 9-p \end{pmatrix},$$

tenemos $\Delta(3,3+3\omega_3,-4+\omega_2-3\omega_3,1+\omega_3+\omega_4) = 3^4p^3$. Por el Teorema 1.31 concluimos que

$$N(M) = \sqrt{\frac{3^4p^3}{p^3}} = 3^2.$$

Siguiendo las mismas ideas, podemos comprobar fácilmente que $N(P_1) = N(P_2) = 3$. □

Del corolario anterior, la afirmación $N(P_1) = N(P_2) = 3$ implica que P_1 y P_2 son ideales primos de $\mathcal{O}_K$ y $P_1 \cap \mathbb{Z} = P_2 \cap \mathbb{Z} = 3\mathbb{Z}$. También notemos que $3\mathcal{O}_K \subset MP_1P_2$. El objetivo es mostrar la igualdad $3\mathcal{O}_K = MP_1P_2$.

Recordemos que p es un primo racional de la forma $4+n^2$, para alguna $n \in \mathbb{N}$ y por tanto p es de la forma $4m+1$ para algún $m \in \mathbb{N}$.

Lema 2.30. *Sea* $K = \mathbb{Q}(\alpha')$, *con* $\alpha' = \sqrt{-(p+2\sqrt{p})}$ *y* $p = 4+n^2 = 4m+1$. *Entonces*

(i) $m = 3k$ *para algún* $k \in \mathbb{Z}$.

(ii) $\dfrac{3+\alpha'}{2} \cdot \dfrac{\alpha'^2+(p-2)}{4} \in 3\mathcal{O}_K$.

Demostración. (i) Si $n = 4l+3$, tenemos $m = 4l^2+6l+3$ y como $3 \mid n$, entonces $l = 3t$, para algún $t \in \mathbb{Z}$. Por lo tanto, $m = 3(12t^2+6t+1)$. Si $n = 4l+1$, entonces $m = 4l^2+2l+1$ y como $3 \mid n$, obtenemos $3t = 4l+1$, para algún $t \in \mathbb{Z}$. De lo anterior, $l+1 = 3(t-l)$ y así $m = 4l^2+2l+1 = 3l^2+(l+1)^2 = 3(l^2+3(t-l)^2)$.

Para la afirmación (ii) aplicamos el Lema 2.27. Si $n \equiv 3 \pmod 4$, entonces

$$\begin{aligned}\frac{3+\alpha'}{2}\cdot\frac{\alpha'^2+(p-2)}{4} &= (1+\omega_3+\omega_4)(-\omega_2)\\ &= -\omega_2-\omega_2\omega_3-\omega_2\omega_4\\ &= -\omega_2-\left(\frac{n^2-1}{8}+\frac{3-n}{4}\omega_2+\frac{1+n}{2}\omega_3+\omega_4\right)\\ &\quad -\left(\frac{-p+2n-1}{8}-\frac{1+n}{4}\omega_2+\omega_3+\frac{1-n}{2}\omega_4\right)\\ &= \frac{3-n}{4}-\frac{3-n}{2}\omega_2-\frac{3+n}{2}\omega_3-\frac{3-n}{2}\omega_4.\end{aligned}$$

Puesto que $n = 4l+3$, con $l = 3t$, tenemos

$$\frac{3+\alpha'}{2}\cdot\frac{\alpha'^2+(p-2)}{4} = -3t+6t\omega_2-3(2t+1)\omega_3+6t\omega_4 \in 3\mathcal{O}_K.$$

El caso $n \equiv 1 \pmod 4$ se justifica de manera similar.

□

Teorema 2.31. *Sea $K = \mathbb{Q}(\alpha')$, con $\alpha' = \sqrt{-(p+2\sqrt{p})}$. Consideremos los ideales*

$$M = \left\langle 3, \frac{3+\alpha'}{2}\right\rangle, \quad P_1 = \left\langle 3, \frac{5-\alpha'}{2}\right\rangle, \quad P_2 = \left\langle 3, \frac{5+\alpha'}{2}\right\rangle.$$

Entonces

$$3\mathcal{O}_K = MP_1P_2.$$

Demostración. Primero vamos a probar

$$P_1P_2 = \left\langle 3, \frac{5-\alpha'}{2}\right\rangle\left\langle 3, \frac{5+\alpha'}{2}\right\rangle = \langle 3, -\omega_2\rangle,$$

es decir, queremos probar

$$\left\langle 9, 3\left(\frac{5+\alpha'}{2}\right), 3\left(\frac{5-\alpha'}{2}\right), \frac{25+p+2\sqrt{p}}{4}\right\rangle = \langle 3, -\omega_2\rangle.$$

Observemos que, sin importar $n \equiv 3 \pmod 4$ ó $n \equiv 1 \pmod 4$, de acuerdo al Lema 2.27 es fácil ver que el ideal $\left\langle 9, 3\left(\frac{5+\alpha'}{2}\right), 3\left(\frac{5-\alpha'}{2}\right), \frac{25+p+2\sqrt{p}}{4}\right\rangle$ lo podemos escribir como:

$$\left\langle 9, 6+3\omega_3+3\omega_4, 9-3\omega_3-3\omega_4, \frac{23+p}{4}+\omega_2\right\rangle.$$

En seguida vamos a mostrar que

$$\left\langle 9, 6+3\omega_3+3\omega_4, 9-3\omega_3-3\omega_4, \frac{23+p}{4}+\omega_2\right\rangle = \langle 3, -\omega_2\rangle.$$

Primero observemos lo siguiente:

$$9, \quad 6+3\omega_3+3\omega_4, \quad 9-3\omega_3-3\omega_4 \in \langle 3, -\omega_2\rangle.$$

Siguiendo la notación del Lema 2.27 y la afirmación (i) del mismo, tenemos que

$$\frac{23+p}{4}+\omega_2 = 6+m+\omega_2 = 3(2+k)+\omega_2 \in \langle 3, -\omega_2\rangle.$$

Por lo tanto, $\left\langle 9, 6+3\omega_3+3\omega_4, 9-3\omega_3-3\omega_4, \dfrac{23+p}{4}+\omega_2 \right\rangle \subseteq \langle 3, -\omega_2\rangle$. Puesto que

$$3 = 2(9) - 3\left(\frac{5+\alpha'}{2}\right) - 3\left(\frac{5-\alpha'}{2}\right), \quad \omega_2 = \left(\frac{23+p}{4}+\omega_2\right) - \left(\frac{23+p}{4}\right) \in P_1P_2,$$

tenemos $\langle 3, -\omega_2\rangle \subseteq P_1P_2$ y así $P_1P_2 = \langle 3, -\omega_2\rangle$. Finalmente, como $-\omega_2 = \dfrac{\alpha'^2+(p-2)}{4}$, entonces

$$MP_1P_2 = \left\langle 3, \frac{3+\alpha'}{2} \right\rangle \langle 3, -\omega_2\rangle = \left\langle 9, 3\frac{3+\alpha'}{2}, 3\frac{\alpha'^2+(p-2)}{4}, \frac{3+\alpha'}{2}\cdot\frac{\alpha'^2+(p-2)}{4} \right\rangle,$$

y ya tenemos todo para mostrar $MP_1P_2 = 3\mathcal{O}_k$. Primero notemos que

$$9, \quad 3\frac{\alpha'^2+(p-2)}{4} = -3\omega_2, \quad 3\frac{3+\alpha'}{2} = 3+3\omega_3+3\omega_4 \in 3\mathcal{O}_K,$$

por la parte (ii) del lema anterior, $\dfrac{3+\alpha'}{2}\cdot\dfrac{\alpha'^2+(p-2)}{4} \in 3\mathcal{O}_K$, es decir,

$$\left\langle 3, \frac{3+\alpha'}{2} \right\rangle \left\langle 3, \frac{\alpha'^2+(p-2)}{4} \right\rangle \subseteq 3\mathcal{O}_K.$$

Puesto que $N\left(\left\langle 3, \dfrac{3+\alpha'}{2} \right\rangle \left\langle 3, \dfrac{\alpha'^2+(p-2)}{4} \right\rangle\right) = N(3\mathcal{O}_K)$, entonces por el Lema 1.44,

$$MP_1P_2 = \left\langle 3, \frac{3+\alpha'}{2} \right\rangle \left\langle 3, \frac{\alpha'^2+(p-2)}{4} \right\rangle = 3\mathcal{O}_K.$$

□

Por las observaciones hechas al principio de la sección 2.3 con $q = 3$, el ideal $3\mathcal{O}_K$ no puede ser producto de tres ideales primos, y como P_1, P_2 son ideales primos, entonces M no es un ideal primo. Enseguida vamos a dar la factorización de M.

Proposición 2.32. *Sea K como en el teorema anterior. Si $n \equiv 3 \pmod 4$ consideremos los ideales $Q_1 = \langle 3, \omega_2-\omega_3\rangle$, $Q_2 = \langle 3, -\omega_3\rangle$. Si $n \equiv 1 \pmod 4$, consideremos los ideales $Q_1' = \langle 3, -1-\omega_4\rangle$, $Q_2' = \langle 3, 2-\omega_2-\omega_4\rangle$. Entonces*

(i) $Q_1 = 3\mathbb{Z} + (1-\omega_3)\mathbb{Z} + (\omega_2-\omega_3)\mathbb{Z} + (1+\omega_2+\omega_4)\mathbb{Z}$.
(ii) $Q_2 = 3\mathbb{Z} + (2+\omega_2-\omega_3)\mathbb{Z} + (\omega_2+\omega_4)\mathbb{Z} - \omega_3\mathbb{Z}$.
(iii) $Q_1' = 3\mathbb{Z} + (-1-\omega_4)\mathbb{Z} + \omega_3\mathbb{Z} + (3-\omega_2-\omega_4)\mathbb{Z}$.
(iv) $Q_2' = 3\mathbb{Z} + (1-\omega_4)\mathbb{Z} + (2+\omega_3)\mathbb{Z} + (-2+\omega_2+\omega_4)\mathbb{Z}$.

Demostración. Primero analizemos el caso $n \equiv 3 \pmod 4$, en el cual, una base entera está dada en el Teorema 2.9. Concretamente:

$$\omega_1 = 1, \quad \omega_2 = \frac{1+\sqrt{p}}{2}, \quad \omega_3 = \frac{1+\sqrt{p}+\alpha'+\beta'}{4}, \quad \omega_4 = \frac{1-\sqrt{p}+\alpha'-\beta'}{4}.$$

Para $\gamma \in Q_1$, tenemos que $\gamma = 3\gamma_1 + (\omega_2 - \omega_3)\gamma_2$, con $\gamma_1, \gamma_2 \in \mathcal{O}_K$. Así

$$\begin{aligned}
\gamma &= 3\gamma_1 + (\omega_2 - \omega_3)\gamma_2 \\
&= 3(a_1 + a_2\omega_2 + a_3\omega_3 + a_4\omega_4) + (\omega_2 - \omega_3)(b_1 + b_2\omega_2 + b_3\omega_3 + b_4\omega_4) \\
&= \left[3a_1 + \frac{p+3}{8}b_2 + \frac{3n^2 - 2n + 11}{16}b_3 + \frac{-p + 2n - 9}{16}b_4\right] + \\
&\quad \left[3a_2 + b_1 + \frac{1+n}{4}b_2 + \frac{1+n}{4}b_3 + \frac{3-n}{4}b_4\right]\omega_2 + \\
&\quad \left[3a_3 - b_1 - \frac{1+n}{2}b_2 + \frac{1+n}{4}b_4\right]\omega_3 + \left[3a_4 - b_2 + \frac{3-n}{4}b_4\right]\omega_4.
\end{aligned}$$

Si escribimos $n = 4l + 3$ para algún $l \in \mathbb{Z}$, entonces

$$\begin{aligned}
\gamma &= \left[3a_1 + (2l^2 + 3l + 2)b_2 + (3l^2 + 4l + 2)b_3 - (l^2 + l + 1)b_4\right] \\
&\quad + \left[3a_2 + b_1 + (l+1)b_2 + (l+1)b_3 - lb_4\right]\omega_2 \\
&\quad + \left[3a_3 - b_1 - (2l+2)b_2 + (l+1)b_4\right]\omega_3 \\
&\quad + \left[3a_4 - b_2 - lb_4\right]\omega_4.
\end{aligned}$$

Si $x = 3a_4 - b_2 - lb_4$, entonces $-b_2 = x - 3a_4 + lb_4$ y por tanto

$$\begin{aligned}
\gamma &= \left[3a_1 - 3a_4 + (2l^2 + 3l + 3)b_2 + (3l^2 + 4l + 2)b_3 - (l^2 + 1)b_4\right] \\
&\quad + \left[3a_2 - 3a_4 + b_1 + (l+2)b_2 + (l+1)b_3\right]\omega_2 \\
&\quad + \left[3a_3 - b_1 - (2l+2)b_2 + (l+1)b_4\right]\omega_3 + (1 + \omega_2 + \omega_4)x.
\end{aligned}$$

Si $y = 3a_2 - 3a_4 + b_1 + (l+2)b_2 + (l+1)b_3$, entonces $b_1 = y - 3a_2 + 3a_4 - (l+2)b_2 - (l+1)b_3$. Así que

$$\begin{aligned}
\gamma &= \left[3a_1 - 3a_4 + (2l^2 + 3l + 3)b_2 + (3l^2 + 4l + 2)b_3 - (l^2 + 1)b_4\right] \\
&\quad + \left[3a_3 + 3a_2 - 3a_4 - lb_2 + (l+1)b_3 + (l+1)b_4\right]\omega_3 \\
&\quad + (\omega_2 - \omega_3)y + (1 + \omega_2 + \omega_4)x.
\end{aligned}$$

Sea $-z = 3a_3 + 3a_2 - 3a_4 - lb_2 + (l+1)b_3 + (l+1)b_4$. Entonces $lb_2 = z + 3a_3 + 3a_2 - 3a_4 + (l+1)b_3 + (l+1)b_4$. Así

$$\begin{aligned}
\gamma &= \left[3a_1 + 3a_2 + 3a_3 - 6a_4 + (2l^2 + 2l + 3)b_2 + (3l^2 + 5l + 3)b_3 - (l^2 - l)b_4\right] \\
&\quad + (1 - \omega_3)z + (\omega_2 - \omega_3)y + (1 + \omega_2 + \omega_4)x.
\end{aligned}$$

Como $3 \mid n$ y $n = 4l + 3$, tenemos $l = 3t$, para algún $t \in \mathbb{Z}$. Por tanto

$$\begin{aligned}
\gamma &= 3\left[a_1 + a_2 + a_3 - 2a_4 + (6t^2 + 2t + 1)b_2 + (9t^2 + 5t + 1)b_3 - (3t^2 - t)b_4\right] \\
&\quad + (1 - \omega_3)z + (\omega_2 - \omega_3)y + (1 + \omega_2 + \omega_4)x.
\end{aligned}$$

Por lo tanto, $Q_1 = 3\mathbb{Z} + (1 - \omega_3)\mathbb{Z} + (\omega_2 - \omega_3)\mathbb{Z} + (1 + \omega_2 + \omega_4)\mathbb{Z}$.

Para los ideales Q_2, Q_1', Q_2' la prueba es similar.

□

Corolario 2.33. *Sea $K = \mathbb{Q}(\alpha')$. Entonces Q_1, Q_2, Q_1' y Q_2' son ideales primos de $\mathcal{O}_K$.*

Demostración. La idea de la demostración consiste en mostrar que

$$N(Q_1) = N(Q_2) = N(Q_1') = N(Q_2') = 3.$$

De acuerdo a la proposición anterior una base para el ideal Q_1 es:

$$3, \quad 1-\omega_3, \quad \omega_2-\omega_3, \quad 1+\omega_2+\omega_4.$$

Para calcular el discriminante de la base entera anterior, usamos el Lema 2.12:

$tr(9) = 36,$

$tr(3(1-\omega_3)) = 3tr(1-\omega_3) = 9,$

$tr(3(\omega_2-\omega_3)) = 3tr(\omega_2-\omega_3) = 3,$

$tr(3(1+\omega_2+\omega_4)) = 3tr(1+\omega_2+\omega_4) = 21,$

$tr((1-\omega_3)^2) = tr(1-2\omega_3+\omega_3^2) = \dfrac{9-p}{4},$

$tr((1-\omega_3)(\omega_2-\omega_3)) = tr(\omega_2-\omega_3-\omega_2\omega_3-\omega_3^2) = \dfrac{3-3p}{4},$

$tr((1-\omega_3)(1+\omega_2+\omega_4)) = tr(1+\omega_2+\omega_4-\omega_3-\omega_2\omega_3-\omega_3\omega_4) = \dfrac{21-p}{4},$

$tr((\omega_2-\omega_3)^2) = tr(\omega_2^2-2(\omega_2\omega_3)+\omega_3^2) = \dfrac{1-p}{4},$

$tr((\omega_2-\omega_3)(1+\omega_2+\omega_4)) = tr(\omega_2+\omega_2^2+\omega_2\omega_4-\omega_3-\omega_2\omega_3-\omega_3\omega_4) = \dfrac{7+p}{4},$

$tr((1+\omega_2+\omega_4)^2) = tr(1+2(\omega_2+\omega_4)+(\omega_2+\omega_4)^2) = \dfrac{49-p}{4}.$

De lo anterior,

$$\Delta(3, 1-\omega_3, \omega_2-\omega_3, 1+\omega_2+\omega_4) = det\begin{pmatrix} 36 & 9 & 3 & 21 \\ 9 & \frac{9-p}{4} & \frac{3-3p}{4} & \frac{21-p}{4} \\ 3 & \frac{3-3p}{4} & \frac{1-p}{4} & \frac{7+p}{4} \\ 21 & \frac{21-p}{4} & \frac{7+p}{4} & \frac{49-p}{4} \end{pmatrix},$$

es decir, $\Delta(3, 1-\omega_3, \omega_2-\omega_3, 1+\omega_2+\omega_4) = 3^2p^3$. De acuerdo al Teorema 1.31

$$N(Q_1) = \sqrt{\frac{3^2p^3}{p^3}} = 3.$$

La norma de Q_2, Q_1', Q_2' se calcula de manera similar. □

Teorema 2.34. *Sean $K = \mathbb{Q}(\alpha')$ con $\alpha' = \sqrt{-(p+2\sqrt{p})}$ y Q_1, Q_2, Q_1', Q_2' como en la Proposición 2.32. Entonces*

$$M = \begin{cases} Q_1Q_2 & si \quad n \equiv 3 \pmod 4, \\ Q_1'Q_2' & si \quad n \equiv 1 \pmod 4. \end{cases}$$

Demostración. Si $n \equiv 3 \pmod 4$, entonces

$$Q_1Q_2 = \langle 3, \omega_2 - \omega_3\rangle\langle 3, -\omega_3\rangle = \langle 3, 1 + \omega_3 + \omega_4\rangle = M$$

si y solo si

$$\langle 9, -3\omega_3, 3\omega_2 - 3\omega_3, -\omega_3(\omega_2 - \omega_3)\rangle = \langle 3, 1 + \omega_3 + \omega_4\rangle.$$

Notemos que $9, -3\omega_3, 3\omega_2 - 3\omega_3 \in \langle 3, 1 + \omega_3 + \omega_4\rangle$. Puesto que $n = 4l + 3$ tenemos

$$-\omega_3(\omega_2 - \omega_3) = (-3l^2 - 4l - 2) - (1 + l)\omega_2.$$

De acuerdo a la Proposición 2.28, $\{3, 3 + 3\omega_3, -4 + \omega_2 - 3\omega_3, 1 + \omega_3 + \omega_4\}$ es una base entera de M y

$$(-3l^2 - 4l - 2) - (1 + l)\omega_2 =$$

$$3\left(\frac{-3l^2 - 5l - 3}{3}\right) + (3 + 3\omega_3)(-l - 1) + (-4 + \omega_2 - 3\omega_3)(-l - 1) + (1 + \omega_3 + \omega_4) \cdot 0.$$

Por lo anterior $-\omega_3(\omega_2 - \omega_3) \in M$ y así $Q_1Q_2 \subseteq M$. Puesto que $N(Q_1Q_2) = N(M) = 9$, por el Lema 1.44 concluimos que $Q_1Q_2 = M$.

La factorización $M = Q_1'Q_2'$ en el caso $n \equiv 1 \pmod 4$ es similar.

□

Capítulo 3

Ramificación diédrica

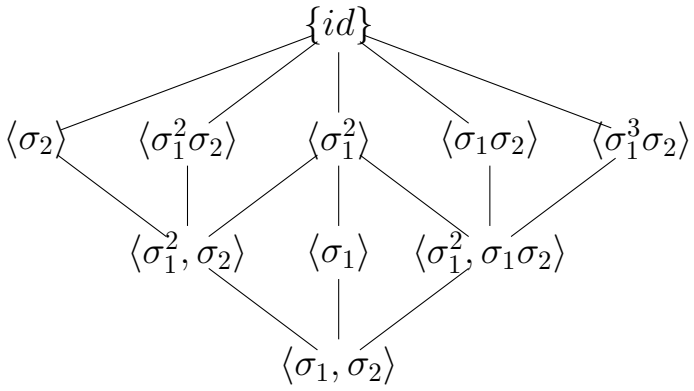
En todo este capítulo asumiremos que p es un primo positivo impar y $p \neq 4 + n^2$. El campo de descomposición de $f(x) = x^4 + px^2 + p$ sobre $\mathbb{Q}$ es $L = \mathbb{Q}(\alpha_1, \alpha_3)$. Más adelante diremos quiénes son α_1, α_3. Por el Corolario 2.2

$$G_f = D_8 = \{\sigma_1, \sigma_2 : \sigma_1^4 = \sigma_2^2 = id\},$$

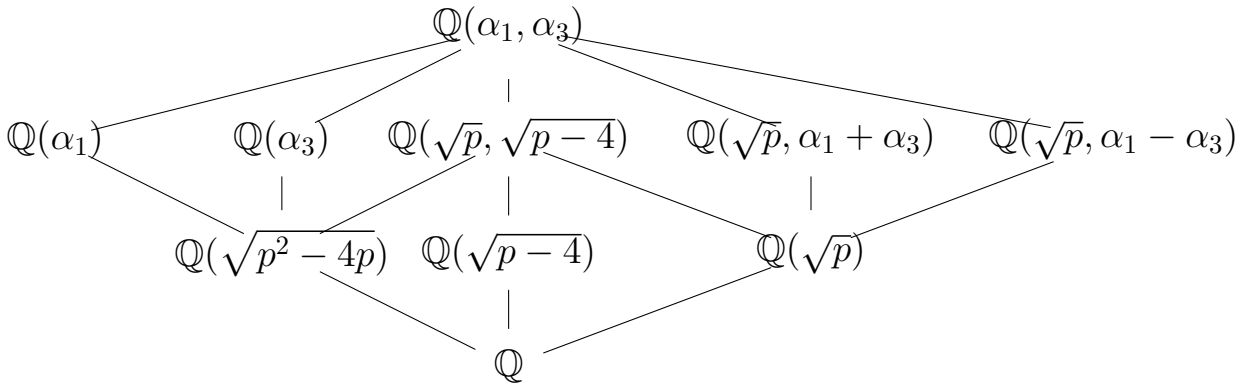
en donde

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

La red de subgrupos de D_8 es la siguiente:



y la red de subcampos es:



en donde $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ son las raíces del polinomio $f(x) = x^4 + px^2 + p$ dadas por

$$\alpha_1 = \sqrt{\frac{-p + \sqrt{p^2 - 4p}}{2}}, \quad \alpha_2 = -\alpha_1, \quad \alpha_3 = \sqrt{\frac{-p - \sqrt{p^2 - 4p}}{2}}, \quad \alpha_4 = -\alpha_3.$$

Ahora nos fijamos en la siguiente torre de campos

$$\begin{array}{c} L = \mathbb{Q}(\alpha_1, \alpha_3) \\ | \\ K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4}) \\ | \\ \mathbb{Q} \end{array}$$

Encontraremos un elemento primitivo apropiado para $L/\mathbb{Q}$, con dos expresiones distintas. La primera expresión nos facilita el cálculo del discriminante de $\alpha_1 + 2\alpha_3$ lo cual es útil para estimar $ind(\alpha_1 + 2\alpha_3)$. La segunda

Lema 3.1. *Sean* $\alpha_1 = \sqrt{\dfrac{-p + \sqrt{p^2 - 4p}}{2}}$, $\alpha_3 = \sqrt{\dfrac{-p - \sqrt{p^2 - 4p}}{2}}$ *y* $p \neq 4 + n^2$. *Entonces*

(i) $\alpha_1 + 2\alpha_3 = \sqrt{-\dfrac{5}{2}p - \sqrt{\left(\dfrac{9}{4}p^2 + 7p\right) + 12p\sqrt{p-4}}}$.

(ii) $\alpha_1 + 2\alpha_3 = \sqrt{-\left(\dfrac{3}{2}\sqrt{p-4} + 4\right)\sqrt{p} - \dfrac{5}{2}p}$.

Demostración. Es un cálculo directo. □

Proposición 3.2. *Sea* $L = \mathbb{Q}(\alpha_1, \alpha_3)$ *con* α_1, α_3 *como en el lema anterior. Entonces* $L = \mathbb{Q}(\alpha_1 + 2\alpha_3)$.

Demostración. Notemos que $\mathbb{Q}(\alpha_1 + 2\alpha_3) \subset \mathbb{Q}(\alpha_1, \alpha_3)$. Por otro lado, de la parte (i) del lema anterior, $\sqrt{p-4} \in \mathbb{Q}(\alpha_1 + 2\alpha_3)$ y de la parte (ii), $\sqrt{p} \in \mathbb{Q}(\alpha_1 + 2\alpha_3)$ de donde $\sqrt{p^2 - 4p} \in \mathbb{Q}(\alpha_1 + 2\alpha_3)$ y por tanto $\alpha_1^2, \alpha_3^2 \in \mathbb{Q}(\alpha_1 + 2\alpha_3)$. Como $\alpha_1\alpha_3 = -\sqrt{p} \in \mathbb{Q}(\alpha_1 + 2\alpha_3)$, entonces

$$\alpha_3(\alpha_1^2 - 4\alpha_3^2) = [\alpha_1\alpha_3(\alpha_1 + 2\alpha_3)] - [2\alpha_3^2(\alpha_1 + 2\alpha_3)] \in \mathbb{Q}(\alpha_1 + 2\alpha_3),$$

de donde $\alpha_3 \in \mathbb{Q}(\alpha_1 + 2\alpha_3)$ y en consecuencia $\alpha_1 \in \mathbb{Q}(\alpha_1 + 2\alpha_3)$. Por lo tanto

$$\mathbb{Q}(\alpha_1 + 2\alpha_3) = \mathbb{Q}(\alpha_1, \alpha_3).$$

□

Lema 3.3. *Sea* $\theta = \alpha_1 + 2\alpha_3$. *Entonces*

$$Irr(\theta, \mathbb{Q}) = \rho(x) = x^8 + 10px^6 + p(33p - 14)x^4 + 10p^2(4p - 7)x^2 + p^2(4p - 25)^2.$$

Demostración. Es fácil probar que $\rho(\theta) = 0$. Por la Proposición 3.2,

$$\mathbb{Q}(\alpha_1, \alpha_3) = \mathbb{Q}(\alpha_1 + 2\alpha_3) = \mathbb{Q}(\theta).$$

Puesto que $[\mathbb{Q}(\alpha_1, \alpha_3) : \mathbb{Q}] = 8$, entonces $[\mathbb{Q}(\theta) : \mathbb{Q}] = 8$ y así $\rho(x)$ es irreducible. □

Proposición 3.4. *Sea* $L = \mathbb{Q}(\theta)$. *Entonces*

$$D(\theta) = 2^{32}3^8p^{14}(p-4)^4(9p-100)^4(4p-25)^2$$

Demostración. Las raíces de $\rho(x)$ son:

$$\theta_1 = \sqrt{-\frac{5}{2}p + \sqrt{\left(\frac{9}{4}p^2 + 7p\right) + 12p\sqrt{p-4}}},$$

$$\theta_2 = \theta = \sqrt{-\frac{5}{2}p - \sqrt{\left(\frac{9}{4}p^2 + 7p\right) + 12p\sqrt{p-4}}},$$

$$\theta_3 = \sqrt{-\frac{5}{2}p + \sqrt{\left(\frac{9}{4}p^2 + 7p\right) - 12p\sqrt{p-4}}},$$

$$\theta_4 = \sqrt{-\frac{5}{2}p - \sqrt{\left(\frac{9}{4}p^2 + 7p\right) - 12p\sqrt{p-4}}},$$

así como $-\theta_1, -\theta_2, -\theta_3$ y $-\theta_4$. Por tanto

$$D(\theta) = \prod_{i<j}(\theta_i - \theta_j)^2 = 2^{32}3^8p^{14}(p-4)^4(9p-100)^4(4p-25)^2.$$

□

El siguiente lema nos da otra forma de las raíces de $\rho(x)$, la cual nos será de ayuda para encontrar la acción de cada $\sigma_i \in G_f$ sobre las raíces de $\rho(x)$.

Lema 3.5. *Sea $L = \mathbb{Q}(\theta)$. Entonces otra expresión para los θ_i de la proposición anterior es:*

$$\theta_1 = \sqrt{\left(\frac{3}{2}\sqrt{p-4} + 4\right)\sqrt{p} - \frac{5}{2}p}, \quad \theta_2 = \theta,$$

$$\theta_3 = \sqrt{\left(\frac{3}{2}\sqrt{p-4} - 4\right)\sqrt{p} - \frac{5}{2}p} \quad , \qquad \theta_4 = \sqrt{-\left(\frac{3}{2}\sqrt{p-4} - 4\right)\sqrt{p} - \frac{5}{2}p}\ .$$

Demostración. La demostración es inmediata. □

Lo que haremos a continuación es ver cómo actúa G_f sobre las raíces de $\rho(x)$. Recordemos que $G_f = D_8 = \{\sigma_1, \sigma_2 : \sigma_1^4 = \sigma_2^2 = id\}$ con

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

Los otros elementos son $\sigma_0 = id$, $\sigma_3 = \sigma_1^2$, $\sigma_4 = \sigma_1^3$, $\sigma_5 = \sigma_1\sigma_2$, $\sigma_6 = \sigma_1^2\sigma_2$, $\sigma_7 = \sigma_1^3\sigma_2$.

Proposición 3.6. *Sean θ_j como en el lema anterior y $\sigma_i \in G_f$. Entonces la acción de $\sigma_i(\theta_j)$ está descrita en la siguiente tabla:*

	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7
θ_1	θ_1	$-\theta_2$	$-\theta_3$	$-\theta_1$	θ_2	θ_4	θ_3	$-\theta_4$
θ_2	θ_2	θ_1	θ_4	$-\theta_2$	$-\theta_1$	θ_3	$-\theta_4$	$-\theta_3$
θ_3	θ_3	$-\theta_4$	$-\theta_1$	$-\theta_3$	θ_4	θ_2	θ_1	$-\theta_2$
θ_4	θ_4	θ_3	θ_2	$-\theta_4$	$-\theta_3$	θ_1	$-\theta_2$	$-\theta_1$
θ_5	θ_5	θ_2	θ_3	θ_1	$-\theta_2$	$-\theta_4$	$-\theta_3$	θ_4
θ_6	θ_6	$-\theta_1$	$-\theta_4$	θ_2	θ_1	$-\theta_3$	θ_4	θ_3
θ_7	θ_7	θ_4	θ_1	θ_3	$-\theta_4$	$-\theta_2$	$-\theta_1$	θ_2
θ_8	θ_8	$-\theta_3$	$-\theta_2$	θ_4	θ_3	$-\theta_1$	θ_2	θ_1

Demostración. Sabemos que G_f actúa directamente sobre las raíces de $f(x) = x^4+px^2+p$, las cuales son α_1, $\alpha_2 = -\alpha_1$, α_3 y $\alpha_4 = -\alpha_3$. A su vez las raíces de $\rho(x)$ están ralacionadas con las raíces de $f(x)$ de la siguiente manera

$\theta_1 = \alpha_3 - 2\alpha_1$, $\theta_2 = \alpha_1 + 2\alpha_3$, $\theta_3 = \alpha_3 + 2\alpha_1$, $\theta_4 = \alpha_1 - 2\alpha_3$.

Sólo veremos cómo actúa G_f sobre θ_1:

$\sigma_0(\theta_1) = \sigma_0(\alpha_3) - 2\sigma_0(\alpha_1) = \alpha_3 - 2\alpha_1 = \theta_1$
$\sigma_1(\theta_1) = \sigma_1(\alpha_3) - 2\sigma_1(\alpha_1) = \alpha_2 - 2\alpha_3 = -\alpha_1 - 2\alpha_3 = -\theta_2$
$\sigma_2(\theta_1) = \sigma_2(\alpha_3) - 2\sigma_2(\alpha_1) = \alpha_4 - 2\alpha_1 = -\alpha_3 - 2\alpha_1 = -\theta_3$
$\sigma_3(\theta_1) = \sigma_3(\alpha_3) - 2\sigma_3(\alpha_1) = \alpha_4 - 2\alpha_2 = -\alpha_3 + 2\alpha_1 = -\theta_1$
$\sigma_4(\theta_1) = \sigma_4(\alpha_3) - 2\sigma_4(\alpha_1) = \alpha_1 - 2\alpha_4 = \alpha_1 + 2\alpha_3 = \theta_2$
$\sigma_5(\theta_1) = \sigma_5(\alpha_3) - 2\sigma_5(\alpha_1) = \alpha_1 - 2\alpha_3 = \theta_4$
$\sigma_6(\theta_1) = \sigma_6(\alpha_3) - 2\sigma_6(\alpha_1) = \alpha_3 - 2\alpha_2 = \alpha_3 + 2\alpha_1 = \theta_3$
$\sigma_7(\theta_1) = \sigma_7(\alpha_3) - 2\sigma_7(\alpha_1) = \alpha_2 - 2\alpha_4 = -\alpha_1 + 2\alpha_3 = -\theta_4$

La acción de G_f sobre las otras raíces de $\rho(x)$ es similar. □

Lema 3.7. *Sea $L = \mathbb{Q}(\theta)$. Entonces*

	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7
$\sqrt{p}$	$\sqrt{p}$	$-\sqrt{p}$	$-\sqrt{p}$	$\sqrt{p}$	$-\sqrt{p}$	$\sqrt{p}$	$-\sqrt{p}$	$\sqrt{p}$
$\sqrt{p-4}$	$\sqrt{p-4}$	$\sqrt{p-4}$	$-\sqrt{p-4}$	$\sqrt{p-4}$	$\sqrt{p-4}$	$-\sqrt{p-4}$	$-\sqrt{p-4}$	$-\sqrt{p-4}$

Demostración. Sólo probaremos que $\sigma_1(\sqrt{p}) = -\sqrt{p}$ y $\sigma_1(\sqrt{p-4}) = \sqrt{p-4}$, los otros casos son similares. Notemos que si θ_2, θ_3 son como en el Lema 3.5, entonces

$$\sqrt{p} = -\frac{1}{8}(5p + \theta_2^2 + \theta_3^2),$$

si θ_2 es como en la Proposición 3.4, entonces

$$\sqrt{p-4} = \frac{1}{12p}(4p^2 - 7p + 5p\theta_2^2 + \theta_2^4).$$

Así

$$\begin{aligned}
\sigma_1(\sqrt{p}) &= -\frac{1}{8}\sigma_1(5p + \theta_2^2 + \theta_3^2) = -\frac{1}{8}(5p + \theta_1^2 + \theta_4^2) \\
&= -\frac{1}{8}\left(5p + \left(\frac{3}{2}\sqrt{p-4} + 4\right)\sqrt{p} - \frac{5}{2}p - \left(\frac{3}{2}\sqrt{p-4} - 4\right)\sqrt{p} - \frac{5}{2}p\right) \\
&= -\frac{1}{8}(8\sqrt{p}) = -\sqrt{p}.
\end{aligned}$$

$$\begin{aligned}\sigma_1(\sqrt{p-4}) &= \frac{1}{12p}\sigma_1(4p^2 - 7p + 5p\theta_2^2 + \theta_2^4) = \frac{1}{12p}(4p^2 - 7p + 5p\theta_1^2 + \theta_1^4) \\ &= \frac{1}{12p}\left(4p^2 - 7p - \frac{25}{2}p^2 + \frac{9}{4}p^2 - 9p + 12p\sqrt{p-4} + 16p + \frac{25}{4}p^2\right) \\ &= \frac{1}{12p}(12p\sqrt{p-4}) = \sqrt{p-4}.\end{aligned}$$

□

3.1. Ramificación en $K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4})$

En esta sección daremos la factorización en $\mathcal{O}_K$ de los ideales $q\mathcal{O}_K$ con q un primo racional. La expresión de θ que aparece en (ii) en el Lema 3.1 es la que utilizaremos en el resto del capítulo.

Teorema 3.8. *Sea $K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4})$. Entonces una base entera para $\mathcal{O}_K$ es*

(i) $\left\{1, \sqrt{p}, \frac{\sqrt{p} + \sqrt{p-4}}{2}, \frac{1 + \sqrt{p^2 - 4p}}{2}\right\}$ *si* $p \equiv 3 \pmod 4$.

(ii) $\left\{1, \frac{1+\sqrt{p}}{2}, \frac{1+\sqrt{p-4}}{2}, \frac{1 + \sqrt{p} + \sqrt{p-4} + \sqrt{p^2-4p}}{4}\right\}$ *si* $p \equiv 1 \pmod 4$.

Demostración. Ver [**37**], Theorem 2. □

Teorema 3.9. *Sea $K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4})$. Entonces δ_K es*

(i) $2^4(p-4)^2p^2$ *si* $p \equiv 3 \pmod 4$.

(ii) $(p-4)^2p^2$ *si* $p \equiv 1 \pmod 4$.

Demostración. Ver [**37**], Theorem 3. □

Lema 3.10. *Sea* $\mu = -\left(\frac{3}{2}\sqrt{p-4} + 4\right)\sqrt{p} - \frac{5}{2}p$. *Entonces*

$$\mu\mathcal{O}_K = \langle\sqrt{p}\rangle\langle -\sqrt{p} - \sqrt{p-4} - 1\rangle^2.$$

Demostración. Como $\mu = \sqrt{p}\left(\frac{-\sqrt{p} + \sqrt{p-4}}{2}\right)(-\sqrt{p} - \sqrt{p-4} - 1)^2$ y $\left(\frac{-\sqrt{p} + \sqrt{p-4}}{2}\right)\left(\frac{\sqrt{p} + \sqrt{p-4}}{2}\right) = -1$, entonces

$$\begin{aligned}\mu\mathcal{O}_K &= \langle\sqrt{p}\rangle\left\langle\frac{-\sqrt{p} + \sqrt{p-4}}{2}\right\rangle\langle -\sqrt{p} - \sqrt{p-4} - 1\rangle^2. \\ &= \langle\sqrt{p}\rangle\langle -\sqrt{p} - \sqrt{p-4} - 1\rangle^2.\end{aligned}$$

□

Notemos que los ideales que aparecen en la factorización de $\mu\mathcal{O}_K$ no necesariamente son ideales primos. Observemos que

$$K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4}) = \mathbb{Q}(\sqrt{p} + \sqrt{p-4}) = \mathbb{Q}\left(\frac{\sqrt{p} + \sqrt{p-4}}{2}\right).$$

Proposición 3.11. *El índice del generador* $\dfrac{\sqrt{p}+\sqrt{p-4}}{2}$ *es*

(i) $ind\left(\dfrac{\sqrt{p}+\sqrt{p-4}}{2}\right) = 1$ *si* $p \equiv 3 \pmod 4$.

(ii) $ind\left(\dfrac{\sqrt{p}+\sqrt{p-4}}{2}\right) = 2^2$ *si* $p \equiv 1 \pmod 4$.

Demostración. De la Proposición 1.41 tenemos que

$$\Delta\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) = N\left(f'\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)\right)$$

donde $f(x) = Irr\left(\dfrac{\sqrt{p}+\sqrt{p-4}}{2}, \mathbb{Q}\right) = x^4 + (2-p)x^2 + 1$ y $f'(x) = 2x(2x^2+2-p)$.
Así

$$\Delta\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) = N(2)N\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)N(\sqrt{p-4})N(\sqrt{p}) = 2^4(p-4)^2p^2.$$

De acuerdo a la Definición 1.39,

$$ind\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) = \begin{cases} \sqrt{\dfrac{2^4(p-4)^2p^2}{2^4(p-4)^2p^2}} = 1 & \text{si} \quad p \equiv 3 \pmod 4 \\ \sqrt{\dfrac{2^4(p-4)^2p^2}{(p-4)^2p^2}} = 2^2 & \text{si} \quad p \equiv 1 \pmod 4 \end{cases}$$

□

Si $p \equiv 3 \pmod 4$, por la proposición anterior, podemos utilizar el Teorema de Dedekind para factorizar cualquier primo racional. Del Teorema 3.9 parte (i), los únicos primos que se ramifican en $\mathcal{O}_K$ son $2, p$ y los factores primos de $p-4$. A continuación damos su ramificación en el caso $p \equiv 3 \pmod 4$.

Proposición 3.12. *Sea* $K = \mathbb{Q}\left(\dfrac{\sqrt{p}+\sqrt{p-4}}{2}\right)$. *Entonces*

(i) $p\mathcal{O}_K = \left\langle p, \dfrac{p+\sqrt{p^2-4p}}{2}\right\rangle^2$.

(ii) $2\mathcal{O}_K = \left\langle 2, \dfrac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2}\right\rangle^2$.

Demostración. Como

$$x^4 + (2-p)x^2 + 1 \equiv (x^2+1)^2 \pmod p, \text{ con } x^2+1 \text{ irreducible en } \mathbb{F}_p[x]$$

y

$$x^4 + (2-p)x^2 + 1 \equiv (x^2+x+1)^2 \pmod 2, \text{ con } x^2+x+1 \text{ irreducible en } \mathbb{F}_2[x],$$

entonces

$$p\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + 1\right\rangle^2 = \left\langle p, \frac{p+\sqrt{p^2-4p}}{2}\right\rangle^2,$$

y

$$\begin{aligned} 2\mathcal{O}_K &= \left\langle 2, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + 1 \right\rangle^2 \\ &= \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle^2. \end{aligned}$$

□

Corolario 3.13. $\sqrt{p}\mathcal{O}_K = \left\langle p, \frac{p+\sqrt{p^2-4p}}{2} \right\rangle$ *es un ideal primo de* $\mathcal{O}_K$.

Demostración. Notemos que $(\sqrt{p})^2 = p$, entonces $(\sqrt{p}\mathcal{O}_K)^2 = p\mathcal{O}_K$. Por otro lado, por la proposición anterior (i), $p\mathcal{O}_K = \left\langle p, \frac{p+\sqrt{p^2-4p}}{2} \right\rangle^2$. Así por el Lema 1.47, $\sqrt{p}\mathcal{O}_K = \left\langle p, \frac{p+\sqrt{p^2-4p}}{2} \right\rangle$. □

Proposición 3.14. *Sea* q *un primo racional tal que* $q \mid p-4$*. Entonces*

$$q\mathcal{O}_K = \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1 \right\rangle^2 \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1 \right\rangle^2.$$

Demostración. Notemos que $x^4 + (2-p)x^2 + 1 \equiv (x^2 + \frac{1}{2}(2-p))^2 \pmod{q}$, donde $\frac{1}{2}$ representa al inverso multiplicativo de 2 módulo q. Como $q \mid p-4$, entonces $p-2 = ql+2$, para algún $l \in \mathbb{Z}$ y

$$x^2 + \frac{1}{2}(2-p) = x^2 - \frac{1}{2}(p-2) = x^2 - \frac{1}{2}(ql+2) \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod{q},$$

así $x^4 + (2-p)x^2 + 1 \equiv (x-1)^2(x+1)^2 \pmod{q}$. Por lo tanto, por el Teorema de Dedekind,

$$q\mathcal{O}_K = \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1 \right\rangle^2 \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1 \right\rangle^2.$$ □

Ahora veremos la factorización de los primos racionales q tal que $q \nmid \delta_K$, los cuales no son ramificados en $\mathcal{O}_K$.

Proposición 3.15. *Sea* q *un primo racional tal que* $q \nmid \delta_K$*. Entonces*

(i) *Si* $\left(\frac{p-4}{q}\right) = 1$ *y* $\left(\frac{p}{q}\right) = 1$*, entonces*

$$q\mathcal{O}_K = \prod_{i=1}^{4} \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} + a_i \right\rangle,$$

donde los $a_i \in \mathbb{Z}$ *son tales que*

$$x^4 + (2-p)x^2 + 1 \equiv (x+a_1)(x+a_2)(x+a_3)(x+a_4) \pmod{q}.$$

(ii) *Si* $\left(\frac{p-4}{q}\right) = -1$ *y* $\left(\frac{p}{q}\right) = -1$ *ó* $\left(\frac{p^2-4p}{q}\right) = -1$, *entonces* $q\mathcal{O}_K = Q_1Q_2$ *donde*

$$Q_1 = \left\langle q, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + a_1\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + a_2 \right\rangle$$

y

$$Q_2 = \left\langle q, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + b_1\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b_2 \right\rangle,$$

donde $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ *son tales que*

$$x^4 + (2-p)x^2 + 1 \equiv (x^2 + a_1x + a_2)(x^2 + b_1x + b_2) \pmod{q}.$$

Demostración. Si $\left(\frac{p-4}{q}\right) = 1$ y $\left(\frac{p}{q}\right) = 1$, entonces por el Teorema 1.58 parte (ii),

$x^4 + (2-p)x^2 + 1 \equiv (x+a_1)(x+a_2)(x+a_3)(x+a_4) \pmod{q}$ con $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. Por lo tanto

$$q\mathcal{O}_K = \prod_{i=1}^{4} \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} + a_i \right\rangle.$$

Ahora, si $\left(\frac{p-4}{q}\right) = -1$ y $\left(\frac{p}{q}\right) = -1$ ó $\left(\frac{p^2-4p}{q}\right) = -1$, entonces por el Teorema 1.58 parte (iii),

$x^4 + (2-p)x^2 + 1 \equiv (x^2 + a_1x + a_2)(x^2 + b_1x + b_2) \pmod{q}$ con $a_1, a_2, b_1b_2 \in \mathbb{Z}$. Por lo tanto $q\mathcal{O}_K = Q_1Q_2$ donde

$$Q_1 = \left\langle q, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + a_1\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + a_2 \right\rangle,$$

y

$$Q_2 = \left\langle q, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + b_1\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b_2 \right\rangle.$$

□

Si $p \equiv 1 \pmod 4$, entonces $ind\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) = 2^2$ y por tanto, podemos utilizar el Teorema de Dedekind para factorizar cualquier ideal $q\mathcal{O}_K$ con $q \neq 2$. En lo que resta de esta sección $p \equiv 1 \pmod 4$.

Proposición 3.16. *Sea* $K = \mathbb{Q}\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)$. *Entonces*

$$p\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle^2 \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b \right\rangle^2$$

donde $b^2 \equiv -1 \pmod p$.

Demostración. Recordemos que

$$x^4 + (2-p)x^2 + 1 \equiv (x^2+1)^2 \pmod{p} \equiv (x-b)^2(x+b)^2 \pmod{p},$$

donde $b^2 \equiv -1 \pmod{p}$. Así

$$p\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle^2 \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b \right\rangle^2.$$

□

Corolario 3.17. $\sqrt{p}\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b \right\rangle$, *donde* $b^2 \equiv -1 \pmod{p}$.

Demostración. Notemos que $(\sqrt{p})^2 = p$, entonces $(\sqrt{p}\mathcal{O}_K)^2 = p\mathcal{O}_K$. Por otro lado, por la proposición anterior,

$$p\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle^2 \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b \right\rangle^2.$$

Así por el Lema 1.47, tenemos

$$\sqrt{p}\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b \right\rangle.$$

□

Proposición 3.18. *Sea q un primo racional tal que $q \mid p-4$. Entonces*

$$q\mathcal{O}_K = \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1 \right\rangle^2 \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1 \right\rangle^2.$$

Demostración. La demostración es idéntica a la demostración de la Proposición 3.14. □

Ahora veremos la factorización de los primos racionales q tal que $q \nmid \delta_K$, los cuales no son ramificados.

Proposición 3.19. *Sea q un primo racional tal que $q \nmid \delta_K$. Entonces*

(i) *Si* $\left(\frac{p-4}{q}\right) = 1$ *y* $\left(\frac{p}{q}\right) = 1$, *entonces*

$$q\mathcal{O}_K = \prod_{i=1}^{4} \left\langle q, \frac{\sqrt{p}+\sqrt{p-4}}{2} + a_i \right\rangle,$$

donde los $a_i \in \mathbb{Z}$ son tales que

$$x^4 + (2-p)x^2 + 1 \equiv (x+a_1)(x+a_2)(x+a_3)(x+a_4) \pmod{q}.$$

(ii) *Si* $\left(\frac{p-4}{q}\right) = -1$ *y* $\left(\frac{p}{q}\right) = -1$ *ó* $\left(\frac{p^2-4p}{q}\right) = -1$, *entonces* $q\mathcal{O}_K = Q_1Q_2$

$$Q_1 = \left\langle q, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + a_1\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + a_2 \right\rangle$$

y

$$Q_2 = \left\langle q, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 + b_1\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b_2 \right\rangle,$$

donde $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ *son tales que*

$$x^4 + (2-p)x^2 + 1 \equiv (x^2 + a_1x + a_2)(x^2 + b_1x + b_2) \pmod{q}.$$

Demostración. La demostración es idéntica a la demostración de la Proposición 3.15 □

Como $p = 4k+1$, por el Teorema 4 en [**14**], tenemos $ind(K) = 2$, es decir, no existe un generador $\gamma \in \mathcal{O}_K$ tal que $2 \nmid ind(\gamma)$ y como consecuencia no podemos utilizar el Teorema de Dedekind para factorizar $2\mathcal{O}_K$. Lo haremos de otra manera. Sabemos que $2 \nmid \delta_K$, entonces $2\mathcal{O}_K$ no es ramificado. A continuación damos su factorización, pero antes proporcionamos bases enteras de los siguientes ideales.

Lema 3.20. *Sea* $K = \mathbb{Q}\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)$. *Si* $k = 2t$, *consideremos los ideales*

$$Q_1 = \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle, \; Q_2 = \left\langle 2, \frac{3+\sqrt{p}}{2} \right\rangle,$$

y si $k = 2t+1$, *consideremos los ideales*

$$Q_1' = \left\langle 2, \frac{-1-\sqrt{p-4}}{2} \right\rangle, \; Q_2' = \left\langle 2, \frac{1-\sqrt{p-4}}{2} \right\rangle.$$

Entonces

$$\text{(i) } Q_1 = 2\mathbb{Z} + \left(\frac{1+\sqrt{p}}{2}\right)\mathbb{Z} + \left(-1-\sqrt{p-4}\right)\mathbb{Z} + \left(\frac{-1-\sqrt{p}-\sqrt{p-4}-\sqrt{p^2-4p}}{4}\right)\mathbb{Z}.$$

$$\text{(ii) } Q_2 = 2\mathbb{Z} + \left(\frac{3+\sqrt{p}}{2}\right)\mathbb{Z} + \left(-1-\sqrt{p-4}\right)\mathbb{Z} + \left(\frac{-1+\sqrt{p}-\sqrt{p-4}+\sqrt{p^2-4p}}{4}\right)\mathbb{Z}.$$

$$\text{(iii) } Q_1' = 2\mathbb{Z} + \left(\frac{-1-\sqrt{p-4}}{2}\right)\mathbb{Z} + (1+\sqrt{p})\,\mathbb{Z} + \left(\frac{-1+\sqrt{p}-\sqrt{p-4}+\sqrt{p^2-4p}}{4}\right)\mathbb{Z},$$

$$\text{(iv) } Q_2' = 2\mathbb{Z} + \left(\frac{1-\sqrt{p-4}}{2}\right)\mathbb{Z} + (1+\sqrt{p})\,\mathbb{Z} + \left(\frac{-7-\sqrt{p}-\sqrt{p-4}+\sqrt{p^2-4p}}{4}\right)\mathbb{Z}.$$

Demostración. Sólo probaremos el caso (i), los otros casos son similares. Notemos que

(i) $2, \dfrac{1+\sqrt{p}}{2} \in Q_1$.

(ii) $-1-\sqrt{p-4} \in Q_1$ porque $-1-\sqrt{p-4} = -2\left(\dfrac{1+\sqrt{p-4}}{2}\right)$.

(iii) $\left(\dfrac{-1-\sqrt{p}-\sqrt{p-4}-\sqrt{p^2-4p}}{4}\right) \in Q_1$ porque

$$\left(\frac{-1-\sqrt{p}-\sqrt{p-4}-\sqrt{p^2-4p}}{4}\right) = -\left(\frac{1+\sqrt{p}}{2}\right)\left(\frac{1+\sqrt{p-4}}{2}\right).$$

Por lo anterior

$$2\mathbb{Z}+\left(\frac{1+\sqrt{p}}{2}\right)\mathbb{Z}+\left(-1-\sqrt{p-4}\right)\mathbb{Z}+\left(\frac{-1-\sqrt{p}-\sqrt{p-4}-\sqrt{p^2-4p}}{4}\right)\mathbb{Z} \subset Q_1.$$

Para la otra contención, si $\gamma \in \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle$, entonces existen $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Z}$ tales que

$$\begin{aligned}
\gamma &= \left[2a_1 + \left(\frac{p-1}{4}\right)b_2\right] + [2a_2 + b_1 + b_2]\left(\frac{1+\sqrt{p}}{2}\right) \\
&\quad + \left[2a_3 + \left(\frac{p-1}{4}\right)b_4\right]\left(\frac{1+\sqrt{p-4}}{2}\right) \\
&\quad + [2a_4 + b_3 + b_4]\left(\frac{1+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{4}\right) \\
&= 2(a_1 + tb_2) + \left(\frac{1+\sqrt{p}}{2}\right)(2a_2 + b_1 + b_2) + (-1-\sqrt{p-4})(-a_3 - tb_4) \\
&\quad + \left(\frac{-1-\sqrt{p}-\sqrt{p-4}-\sqrt{p^2-4p}}{4}\right)(-2a_4 - b_3 - b_4).
\end{aligned}$$

Por lo tanto

$$Q_1 = 2\mathbb{Z}+\left(\frac{1+\sqrt{p}}{2}\right)\mathbb{Z}+\left(-1-\sqrt{p-4}\right)\mathbb{Z}+\left(\frac{-1-\sqrt{p}-\sqrt{p-4}-\sqrt{p^2-4p}}{4}\right)\mathbb{Z}.$$

□

Corolario 3.21. *Sean Q_1, Q_2, Q_1' y Q_2' ideales de $\mathcal{O}_K$ como en el lema anterior. Entonces $N(Q_1) = N(Q_2) = N(Q_1') = N(Q_2') = 4$.*

Demostración. Sólo probaremos que $N(Q_1) = 4$, los otros casos son similares. Puesto que la norma de cualquier ideal I es $N(I) = \sqrt{\frac{D(I)}{\delta_K}}$, por el lema anterior,

$$\begin{aligned}
D(Q_1) &= \Delta\left(2, \frac{1+\sqrt{p}}{2}, -1-\sqrt{p-4}, \frac{-1-\sqrt{p}-\sqrt{p-4}-\sqrt{p^2-4p}}{4}\right) \\
&= 2^4(p-4)^2p^2.
\end{aligned}$$

Por lo tanto $N(Q_1) = 4$. □

Lema 3.22. *Sean Q_1, Q_2, Q_1' y Q_2' como en el Lema 3.20. Entonces Q_1, Q_2, Q_1' y Q_2' son ideales primos de $\mathcal{O}_K$.*

Demostración. Sólo probaremos que el ideal Q_1 es un ideal primo de $\mathcal{O}_K$, los otros casos son similares. Primero veremos que

$$\mathcal{O}_K/Q_1 = \left\{Q_1, 1+Q_1, \frac{1+\sqrt{p-4}}{2}+Q_1, \left(\frac{p-5}{4}+\frac{1+\sqrt{p-4}}{2}\right)+Q_1\right\} \quad (3)$$

Como $\left\{Q_1, 1+Q_1, \frac{1+\sqrt{p-4}}{2}+Q_1, \left(\frac{p-5}{4}+\frac{1+\sqrt{p-4}}{2}\right)+Q_1\right\} \subset \mathcal{O}_K/Q_1$; y todas las clases son distintas pues

$$1-\frac{1+\sqrt{p-4}}{2}, 1-\left(\frac{p-5}{4}+\frac{1+\sqrt{p-4}}{2}\right), \frac{1+\sqrt{p-4}}{2}-\left(\frac{p-5}{4}+\frac{1+\sqrt{p-4}}{2}\right) \notin Q_1$$

y dado que $N(Q_1)=4$, entonces se cumple (3). Por otro lado, $(1+Q_1)(1+Q_1) = 1+Q_1$ y

$$\left(\frac{1+\sqrt{p-4}}{2}+Q_1\right)\left(\left(\frac{p-5}{4}+\frac{1+\sqrt{p-4}}{2}\right)+Q_1\right) = 1+Q_1,$$

es decir, todo elemento no cero tiene inverso multiplicativo. Así, $\mathcal{O}_K/Q_1$ es un campo y por tanto Q_1 es un ideal primo de $\mathcal{O}_K$. □

Teorema 3.23. *Sea* $K = \mathbb{Q}\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)$ *con* $p = 4k+1$. *Entonces*

(i) $2\mathcal{O}_K = \left\langle 2, \frac{1+\sqrt{p}}{2}\right\rangle\left\langle 2, \frac{3+\sqrt{p}}{2}\right\rangle$ *si* k *es par.*

(ii) $2\mathcal{O}_K = \left\langle 2, \frac{-1-\sqrt{p-4}}{2}\right\rangle\left\langle 2, \frac{1-\sqrt{p-4}}{2}\right\rangle$ *si* k *es impar.*

Demostración. Para (i)

$$\begin{aligned}\left\langle 2, \frac{1+\sqrt{p}}{2}\right\rangle\left\langle 2, \frac{3+\sqrt{p}}{2}\right\rangle &= \left\langle 4, 2\frac{3+\sqrt{p}}{2}, 2\frac{1+\sqrt{p}}{2}, \frac{p+3+4\sqrt{p}}{4}\right\rangle \\ &= \langle 2\rangle\left\langle 2, \frac{3+\sqrt{p}}{2}, \frac{1+\sqrt{p}}{2}, \frac{p+3+4\sqrt{p}}{8}\right\rangle.\end{aligned}$$

Notemos que

$$\frac{p+3+4\sqrt{p}}{8} = \frac{k}{2}+\left(\frac{1+\sqrt{p}}{2}\right) \in \mathcal{O}_K \text{ y } 1 = \left(\frac{3+\sqrt{p}}{2}\right)-\left(\frac{1+\sqrt{p}}{2}\right).$$

Así $\left\langle 2, \frac{3+\sqrt{p}}{2}, \frac{1+\sqrt{p}}{2}, \frac{p+3+4\sqrt{p}}{8}\right\rangle = \mathcal{O}_K$. Por lo tanto

$$2\mathcal{O}_K = \left\langle 2, \frac{1+\sqrt{p}}{2}\right\rangle\left\langle 2, \frac{3+\sqrt{p}}{2}\right\rangle.$$

Para (ii)

$$\begin{aligned}\left\langle 2, \frac{-1-\sqrt{p-4}}{2}\right\rangle\left\langle 2, \frac{1-\sqrt{p-4}}{2}\right\rangle &= \left\langle 4, 2\frac{1-\sqrt{p-4}}{2}, 2\frac{-1-\sqrt{p-4}}{2}, \frac{p-5}{4}\right\rangle \\ &= \langle 2\rangle\left\langle 2, \frac{1-\sqrt{p-4}}{2}, \frac{-1-\sqrt{p-4}}{2}, \frac{p-5}{8}\right\rangle.\end{aligned}$$

Notemos que

$$\frac{p-5}{8} = \frac{k-1}{2} \in \mathcal{O}_K \quad \text{y} \quad 1 = \left(\frac{1-\sqrt{p-4}}{2}\right) - \left(\frac{-1-\sqrt{p-4}}{2}\right).$$

Así

$$\left\langle 2, \frac{1-\sqrt{p-4}}{2}, \frac{-1-\sqrt{p-4}}{2}, \frac{p-5}{8} \right\rangle = \mathcal{O}_K.$$

Por lo tanto $2\mathcal{O}_K = \left\langle 2, \frac{-1-\sqrt{p-4}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{p-4}}{2} \right\rangle$. □

3.2. Discriminate de L

Sabemos que una base entera y el discriminante de un campo son conceptos que están ligados, es decir, si uno conoce una base entera, entonces uno puede calcular el discriminante del campo y si tenemos el discriminante del campo, entonces podemos decidir si una n-áda de elementos del campo es o no una base entera. En [**17**] los autores calculan el discriminante de cierto campo sin tener base entera. En esta sección nosotros tambien calcularemos δ_L sin tener ninguna base entera de L.

Para enteros (o ideales) A y B, escribimos $A \mid B$ para indicar que A divide a B y $A^m \parallel B$ indicará que $A^m \mid B$ y $A^{m+1} \nmid B$.

Teorema 3.24. *Sean K un campo de números, $\mu \in \mathcal{O}_K \setminus \mathcal{O}_K^2$, $L = K(\sqrt{\mu})$ tal que $[L:K] = 2$ y P un ideal primo de $\mathcal{O}_K$. Definimos los enteros no negativos l_P, m_P y w_P como*

$$P^{l_P} \parallel 2, \ P^{m_P} \parallel \mu, \ P^{w_P} \parallel \delta_{L/K}.$$

Entonces w_P es el entero no negativo más chico h con $h \equiv m_P \pmod 2$, para el cual la congruencia

$$\alpha^2 \equiv \mu \pmod{P^{2l_P+m_P-h}} \tag{4}$$

es soluble para cierto $\alpha \in \mathcal{O}_K$.

Demostración. Ver [**15**] Lemma 2. □

Escribiremos l, m y w en vez de l_P, m_P y w_P cuando no haya confusión del ideal primo P.

Corolario 3.25. *Con las mismas hipótesis del teorema anterior.*

(i) *Si $m \equiv 1 \pmod 2$, entonces $1 \leq w \leq 2l+1$ y $w \equiv 1 \pmod 2$.*
(ii) *Si $m \equiv 0 \pmod 2$, entonces $0 \leq w \leq 2l$ y $w \equiv 0 \pmod 2$.*
(iii) *Si $l = 0$ (esto es $P \nmid 2$), entonces*

$$w = \begin{cases} 0 & \textit{si} \quad m \equiv 0 \pmod 2 \\ 1 & \textit{si} \quad m \equiv 1 \pmod 2. \end{cases}$$

Demostración. Si $m \equiv 1 \pmod 2$, entonces por el teorema anterior, $h \equiv 1 \pmod 2$. Notemos que h puede tomar cualquiera de los siguientes valores $h = 1, 3, \ldots, 2l-1, 2l+1, 2l+3, \ldots$ Si $h = 2l+1$, entonces (4) es soluble con $\alpha = 0$. Por tanto $1 \leq w \leq 2l+1$ y $w \equiv 1 \pmod 2$.

Si $m \equiv 0 \pmod 2$, entonces por el teorema anterior, $h \equiv 0 \pmod 2$. Notemos que h puede tomar cualquiera de los siguientes valores $h = 0, 2, \ldots, 2l-2, 2l, 2l+2, \ldots$ Si $h = 2l$, entonces (4) es soluble con $\alpha = 0$. Por tanto $0 \leq w \leq 2l$ y $w \equiv 0 \pmod 2$.

El caso (iii) se deduce fácilmemte de los casos anteriores. □

Corolario 3.26. *Sean P un ideal primo de $\mathcal{O}_K$ tal que $P \nmid 2\mathcal{O}_K$, $\mu\mathcal{O}_K = RS^2$ con R libre de cuadrados y μ como en el Teorema 3.24. Entonces $P \parallel \delta_{L/K}$ si y solo si $P \parallel R$.*

Demostración. Como R es libre de cuadrados, entonces

$$\begin{aligned} P \parallel R &\Leftrightarrow m \text{ es impar} \\ &\Leftrightarrow w = 1 \text{ por el corolario anterior parte (iii)} \\ &\Leftrightarrow P \parallel \delta_{L/K}. \end{aligned}$$

□

Lema 3.27. *Sean $p \equiv 3 \pmod 4$, $\mu = -\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p} - \frac{5}{2}p$ y $K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4})$. Entonces $2\mathcal{O}_K \nmid \mu\mathcal{O}_K$.*

Demostración. Observamos que $\mu = -\left(\frac{5p-3}{2}\right) - 4\sqrt{p} - 3\left(\frac{1+\sqrt{p^2-4p}}{2}\right)$. Ahora supongamos que $2\mathcal{O}_K \mid \mu\mathcal{O}_K$. Entonces $\mu\mathcal{O}_K \subset 2\mathcal{O}_K$, de donde $\mu \in 2\mathcal{O}_K$. Así, existen enteros a_1, a_2, a_3, a_4 tales que

$$\mu = 2a_1 + 2a_2\sqrt{p} + 2a_3\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + 2a_4\left(\frac{1+\sqrt{p^2-4p}}{2}\right).$$

Tenemos el siguiente sistema

$$\begin{aligned} 2a_1 &= -\left(\frac{5p-3}{2}\right) \\ 2a_2 &= -4 \\ 2a_3 &= 0 \\ 2a_4 &= -3, \end{aligned}$$

de lo anterior tenemos que $a_4 = \frac{-3}{2}$, lo cual no puede ser. Por lo tanto, $2\mathcal{O}_K \nmid \mu\mathcal{O}_K$. □

Lema 3.28. *Con las mismas hipótesis del lema anterior, sea*

$$P_1 = \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle.$$

Entonces $P_1 \nmid \mu\mathcal{O}_K$.

Demostración. Si $P_1 \mid \mu\mathcal{O}_K$, entonces $P_1 \mid \langle\sqrt{p}\rangle$ o $P_1 \mid \langle -\sqrt{p}-\sqrt{p-4}-1\rangle$. Puesto que $P_1 \nmid \langle\sqrt{p}\rangle$, tenemos $P_1 \mid \langle -\sqrt{p}-\sqrt{p-4}-1\rangle$, es decir, $-\sqrt{p}-\sqrt{p-4}-1 \in P_1$, de donde $(-\sqrt{p}-\sqrt{p-4}-1)(-\sqrt{p}-\sqrt{p-4}+1) = 2p+2\sqrt{p^2-4p}-5 \in P_1$. Así $5 \in P_1$, lo cual no puede ser. □

Lema 3.29. *Con las mismas hipótesis del Lema 3.27. Tenemos $x^2 \equiv \mu \pmod{P_1^4}$ no es soluble en $\mathcal{O}_K$ y $x^2 \equiv \mu \pmod{P_1^2}$ es soluble en $\mathcal{O}_K$.*

Demostración. De la Proposición 3.12 tenemos que $P_1^4 = 4\mathcal{O}_K$ y $P_1^2 = 2\mathcal{O}_K$.

Sea $\alpha = a_1 + a_2\sqrt{p} + a_3\dfrac{\sqrt{p}+\sqrt{p-4}}{2} + a_4\dfrac{1+\sqrt{p^2-4p}}{2} \in \mathcal{O}_K$. Entonces

$$\begin{aligned}\alpha^2 - \mu \;=\; & \left[a_1^2 + a_2^2 p + (p-1)a_2a_3 + \left(\frac{p-3}{2}\right)a_3^2 + \left(\frac{p^2-4p-1}{4}\right)a_4^2 + \left(\frac{5p-3}{2}\right)\right] \\ & +[2a_1a_2 + (1-p)a_2a_4 - 2a_3a_4 + 4]\sqrt{p} \\ & +[2a_1a_3 + 2pa_2a_4 + (1+p)a_3a_4]\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) \\ & +[2a_1a_4 + 2a_2a_3 + a_3^2 + a_4^2 + 3]\left(\frac{1+\sqrt{p^2-4p}}{2}\right)\end{aligned}$$

con $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. Notemos que $\alpha^2 - \mu \in 4\mathcal{O}_K$ si y solo si todos los coeficientes de $\alpha^2 - \mu$ son múltiplos enteros de 4. Dado que los a_i son pares ó impares tenemos los siguientes casos

	a_1	a_2	a_3	a_4
1	par	par	par	par
2	par	par	par	impar
3	par	par	impar	par
4	par	par	impar	impar
5	par	impar	par	par
6	par	impar	par	impar
7	par	impar	impar	par
8	par	impar	impar	impar
9	impar	par	par	par
10	impar	par	par	impar
11	impar	par	impar	par
12	impar	par	impar	impar
13	impar	impar	par	par
14	impar	impar	par	impar
15	impar	impar	impar	par
16	impar	impar	impar	impar

Si $p = 4t + 3$, entonces

$$\frac{p-3}{2} = 2t, \quad \frac{p^2-4p-1}{4} = 2(2t^2+t) - 1, \quad \frac{5p-3}{2} = 2(5t+3).$$

El caso 1 no puede ser ya que el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 2 no puede ser ya que $\left(\dfrac{p^2-4p-1}{4}\right)a_4^2 + \left(\dfrac{5p-3}{2}\right)$ sería impar y por lo tanto el primer coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 3 no puede ser ya que

$$\left(\frac{p-3}{2}\right)a_3^2 + \left(\frac{5p-3}{2}\right) = 2t(2m+1) + 2(5t+3) = 2(2(tm+3t+1)+1) \neq 4d$$

y por lo tanto el primer coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 4 no puede ser ya que el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 5 no puede ser ya que el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 6 no puede ser ya que $2pa_2a_4$ no sería múltiplo de 4 y por lo tanto el tercer coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 7 no puede ser ya que $2a_2a_3$ no sería múltiplo de 4 y por lo tanto el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 8 no puede ser ya que $2a_2a_3 + a_3^2$ no sería múltiplo de 4 y por lo tanto el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 9 no puede ser ya que el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 10 no puede ser ya que $2a_1a_4$ no sería múltiplo de 4 y por lo tanto el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 11 no puede ser ya que $2a_1a_3$ no sería múltiplo de 4 y por lo tanto el tercer coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 12 no puede ser ya que $2a_1a_4 + a_4^2$ no sería múltiplo de 4 y por lo tanto el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 13 no puede ser ya que el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 14 no puede ser ya que $2a_1a_4$ no sería múltiplo de 4 y por lo tanto el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 15 no puede ser ya que $2a_1a_3$ no sería múltiplo de 4 y por lo tanto el tercer coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

El caso 16 no puede ser ya que a_3^2 no sería múltiplo de 4 y por lo tanto el último coeficiente de $\alpha^2 - \mu$ no sería múltiplo de 4.

De lo anterior, podemos concluir que $x^2 \equiv \mu \pmod{P_1^4}$ no es soluble en $\mathcal{O}_K$.

Ahora sea $\alpha = 1 + \left(\dfrac{1+\sqrt{p^2-4p}}{2}\right)$, observemos que,

$$\alpha^2 - \mu = 2(2t^2+6t+3) + 4\sqrt{p} + 0\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + 6\left(\frac{1+\sqrt{p^2-4p}}{2}\right),$$

es decir, $\alpha^2 - \mu \in 2\mathcal{O}_K = P_1^2$. Por lo tanto $x^2 \equiv \mu \pmod{P_1^2}$ es soluble en $\mathcal{O}_K$. □

Ahora veamos que pasa si $p \equiv 1 \pmod 4$.

Lema 3.30. *Si* $\mu = -\left(\dfrac{3}{2}\sqrt{p-4}+4\right)\sqrt{p} - \dfrac{5}{2}p$ *y* $K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4})$, *entonces*

$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle \nmid 2\mathcal{O}_K \quad y \quad \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b\right\rangle \nmid 2\mathcal{O}_K$$

en donde $b^2 \equiv -1 \pmod p$.

Demostración. De acuerdo al Teorema 3.23

$$2\mathcal{O}_K = \begin{cases} Q_1Q_2, & \text{si} \quad k \text{ es par} \\ Q_1'Q_2', & \text{si} \quad k \text{ es impar} \end{cases}$$

donde

$$Q_1 = \left\langle 2, \frac{1+\sqrt{p}}{2}\right\rangle, \; Q_2 = \left\langle 2, \frac{3+\sqrt{p}}{2}\right\rangle,$$

$$Q_1' = \left\langle 2, \frac{-1-\sqrt{p-4}}{2} \right\rangle, Q_2' = \left\langle 2, \frac{1-\sqrt{p-4}}{2} \right\rangle$$

son los ideales primos que aparecen en el Lema 3.22. Entonces

$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \nmid 2\mathcal{O}_K \text{ si y solo si } \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \nmid Q_i \text{ y } Q_i',$$

con $i \in \{1,2\}$. Sólo probaremos que $\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \nmid Q_1$, los otros casos son similares. Supongamos que $\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \mid Q_1$. Como ambos ideales son primos, entonces

$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle = \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle,$$

y por tanto

$$p \in \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle.$$

Por otro lado, como $1+p$ es par, entonces $1+p \in \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle$. Así

$$1 = (1+p) - p \in \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle,$$

lo cual no puede ser. Por lo anterior $\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \nmid Q_1$. De manera similar se prueba que $\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b \right\rangle \nmid 2\mathcal{O}_K$. □

Lema 3.31. *Con las mismas hipótesis del lema anterior, se cumple*

$$Q_1 \nmid \mu\mathcal{O}_K,\ Q_2 \nmid \mu\mathcal{O}_K,\ Q_1' \nmid \mu\mathcal{O}_K,\ y\ Q_2' \nmid \mu\mathcal{O}_K.$$

Demostración. Sólo probaremos que $Q_1 \nmid \mu\mathcal{O}_K$, los otros casos son similares. Supongamos que $Q_1 \mid \mu\mathcal{O}_K$. De acuerdo al Lema 3.10 y Corolario 3.17

$$\mu\mathcal{O}_K = \langle\sqrt{p}\rangle\langle -\sqrt{p}-\sqrt{p-4}-1\rangle^2 =$$
$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b \right\rangle \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b \right\rangle \langle -\sqrt{p}-\sqrt{p-4}-1\rangle^2,$$

entonces $Q_1 \mid \mu\mathcal{O}_K$ si y solo si $Q_1 \mid \langle -\sqrt{p}-\sqrt{p-4}-1\rangle$. Si $Q_1 \mid \langle -\sqrt{p}-\sqrt{p-4}-1\rangle$, entonces $\langle -\sqrt{p}-\sqrt{p-4}-1\rangle \subset \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle$ de donde $1+\sqrt{p}+\sqrt{p-4} \in \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle$. De la igualdad

$$1 + 2\frac{\sqrt{p}+\sqrt{p-4}}{2} = 1+\sqrt{p}+\sqrt{p-4} \in \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle,$$

se sigue que $1 \in \left\langle 2, \frac{1+\sqrt{p}}{2} \right\rangle$, lo cual no puede ser. Así, $Q_1 \nmid \langle -\sqrt{p}-\sqrt{p-4}-1\rangle$ y por lo tanto $Q_1 \nmid \mu\mathcal{O}_K$. □

Teorema 3.32. *Sean* $K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4})$, $\mu = -\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p} - \frac{5}{2}p$ *y* $L = K(\sqrt{\mu})$. *Entonces*

$$\delta_{L/K} = \begin{cases} \langle 2\rangle\langle\sqrt{p}\rangle & \textit{si} \quad p \equiv 3 \pmod 4, \\ \langle\sqrt{p}\rangle & \textit{si} \quad p \equiv 1 \pmod 4. \end{cases}$$

Demostración. Por el Lema 3.10 $\mu\mathcal{O}_K = \langle\sqrt{p}\rangle\langle -\sqrt{p} - \sqrt{p-4} - 1\rangle^2$, con $\langle\sqrt{p}\rangle$ libre de cuadrados. Primero veremos el caso $p \equiv 3 \pmod 4$. Por la Proposición 3.12, (ii) $2\mathcal{O}_K = P_1^2$ con $P_1 = \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2}\right\rangle$ un ideal primo de $\mathcal{O}_K$ y $\langle\sqrt{p}\rangle$ es un ideal primo de $\mathcal{O}_K$. Notemos que $\langle\sqrt{p}\rangle$ es el único ideal primo de $\mathcal{O}_K$ que divide a la parte libre de cuadrados de $\mu\mathcal{O}_K$. Como $\langle\sqrt{p}\rangle \nmid 2\mathcal{O}_K$, por el Corolario 3.26, tenemos que $\langle\sqrt{p}\rangle \parallel \delta_{L/K}$. Por el Lema 3.28, $m_{P_1} = 0$ y como $l_{P_1} = 2$, por el Corolario 3.25 parte (ii), $0 \leq w_{P_1} \leq 4$ y $w_{P_1} \equiv 0 \pmod 2$. Por el Lema 3.29, tenemos $w_{P_1} = 2$. De lo anterior, concluimos que $\delta_{L/K} = \langle 2\rangle\langle\sqrt{p}\rangle$.

Para el caso $p = 4k+1$, por el Teorema 3.23

$$2\mathcal{O}_K = \begin{cases} Q_1Q_2 & \text{si} \quad k \text{ es par} \\ Q_1'Q_2' & \text{si} \quad k \text{ es impar} \end{cases}$$

con

$$Q_1 = \left\langle 2, \frac{1+\sqrt{p}}{2}\right\rangle, \quad Q_2 = \left\langle 2, \frac{3+\sqrt{p}}{2}\right\rangle,$$

$$Q_1' = \left\langle 2, \frac{-1-\sqrt{p-4}}{2}\right\rangle, \quad Q_2' = \left\langle 2, \frac{1-\sqrt{p-4}}{2}\right\rangle,$$

ideales primos de $\mathcal{O}_K$ y por el Corolario 3.17, $\langle\sqrt{p}\rangle = R_1R_2$ con

$$R_1 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle, \; R_2 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b\right\rangle$$

ideales primos de $\mathcal{O}_K$. Notemos que R_1 y R_2 son los únicos ideales primos de $\mathcal{O}_K$ que dividen a la parte libre de cuadrados de $\mu\mathcal{O}_K$. Por el Lema 3.30, tenemos $R_1 \nmid 2\mathcal{O}_K$ y $R_2 \nmid 2\mathcal{O}_K$, por el Corolario 3.26, tenemos que $R_1 \parallel \delta_{L/K}$ y $R_2 \parallel \delta_{L/K}$.

De acuerdo a la factorización de $2\mathcal{O}_K$ vemos que $l_{Q_1} = l_{Q_2} = l_{Q_1'} = l_{Q_2'} = 1$ y por el Lema 3.31 tenemos $m_{Q_1} = m_{Q_2} = m_{Q_1'} = m_{Q_2'} = 0$. Por el Corolario 3.25 (ii), concluimos

$$0 \leq w_{Q_1}, w_{Q_2}, w_{Q_1'}, w_{Q_2'} \leq 2 \quad \text{y} \quad w_{Q_1} \equiv w_{Q_2} \equiv w_{Q_1'} \equiv w_{Q_2'} \equiv 0 \pmod 2.$$

Observe que $Q_1^2 = \left\langle 4, 2\left(\frac{1+\sqrt{p}}{2}\right), \left(\frac{1+\sqrt{p}}{2}\right)^2\right\rangle$. Si $\alpha_1 = \frac{1-\sqrt{p-4}}{2}$, entonces $\alpha_1^2 = \frac{p-1}{4} - \frac{1+\sqrt{p-4}}{2}$. Así que $\alpha_1^2 - \mu \in Q_1^2$. Análogamente si

$$\alpha_2 = \frac{1+\sqrt{p-4}}{2}, \quad \alpha_3 = \frac{1-\sqrt{p}}{2}, \quad \alpha_4 = \frac{1+\sqrt{p}}{2},$$

entonces

$$\alpha_2^2 \equiv \mu \pmod{Q_2^2}, \quad \alpha_3^2 \equiv \mu \pmod{Q_1'^2}, \quad \alpha_4^2 \equiv \mu \pmod{Q_2'^2}.$$

Por el Teorema 3.24 obtenemos

$$w_{Q_1} = w_{Q_2} = w_{Q_1'} = w_{Q_2'} = 0.$$

Por lo anterior, concluimos que $\delta_{L/K} = \langle\sqrt{p}\rangle$. □

Teorema 3.33. *Sean* $L = \mathbb{Q}(\sqrt{\mu})$, $\mu = -\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p} - \frac{5}{2}p$. *Entonces*

$$\delta_L = \begin{cases} 2^{12}(p-4)^4p^6 & \textit{si} \quad p \equiv 3 \pmod 4 \\ (p-4)^4p^6 & \textit{si} \quad p \equiv 1 \pmod 4. \end{cases}$$

Demostración. Observemos la siguiente torre de campos

$$\begin{array}{c} L = \mathbb{Q}(\alpha_1, \alpha_3) \\ | \\ K = \mathbb{Q}(\sqrt{p}, \sqrt{p-4}) \\ | \\ \mathbb{Q} \end{array}$$

Por el Teorema 1.66, tenemos

$$\delta_L = (\delta_K)^2 N_K(\delta_{L/K}).$$

Si $p \equiv 3 \pmod 4$, por el Teorema 3.9 (i) $\delta_K = 2^4(p-4)^2p^2$ y por el teorema anterior $\delta_{L/K} = \langle 2\rangle\langle\sqrt{p}\rangle$, con $N_K(\langle 2\rangle) = 2^4$ y $N_K(\langle\sqrt{p}\rangle) = p^2$. Por lo tanto $\delta_L = 2^{12}(p-4)^4p^6$. Si $p \equiv 1 \pmod 4$, entonces $\delta_K = (p-4)^2p^2$ y $\delta_{L/K} = \langle\sqrt{p}\rangle$, con $N_K(\langle\sqrt{p}\rangle) = p^2$. Por lo tanto $\delta_L = (p-4)^4p^6$. □

El siguiente resultado nos ayudará a decidir para qué primos racionales podemos usar el Teorema de Dedekind y para cuáles no.

Corolario 3.34. *Sea* $L = \mathbb{Q}(\theta)$, *con* $\theta = \sqrt{\mu}$. *Entonces*

$$ind(\theta) = \begin{cases} 2^{10}3^4p^4(9p-100)^2(4p-25) & \textit{si} \quad p \equiv 3 \pmod 4, \\ 2^{16}3^4p^4(9p-100)^2(4p-25) & \textit{si} \quad p \equiv 1 \pmod 4. \end{cases}$$

Demostración. Por la Proposición 3.4, $D(\theta) = 2^{32}3^8p^{14}(p-4)^4(9p-100)^4(4p-25)^2$. Por el teorema anterior, si $p \equiv 3 \pmod 4$, entonces

$$ind(\theta) = \sqrt{\frac{2^{32}3^8p^{14}(p-4)^4(9p-100)^4(4p-25)^2}{2^{12}(p-4)^4p^6}} = 2^{10}3^4p^4(9p-100)^2(4p-25),$$

y si $p \equiv 1 \pmod 4$,

$$ind(\theta) = \sqrt{\frac{2^{32}3^8p^{14}(p-4)^4(9p-100)^4(4p-25)^2}{(p-4)^4p^6}} = 2^{16}3^4p^4(9p-100)^2(4p-25).$$

□

3.3. Ramificación en L

De acuerdo al Teorema 3.33, los únicos primos racionales que se ramifican en $\mathcal{O}_L$ son: $2, p$ y los factores primos de $p-4$ si $p \equiv 3 \pmod 4$; si $p \equiv 1 \pmod 4$, los únicos primos racionales que se ramifican son p y los factores primos de $p-4$. En esta sección estudiaremos la ramificación de dichos primos racionales en $\mathcal{O}_L$, aún sin conocer la factorización de $p-4$.

Iniciamos el estudio de la ramificación de los primos q tales que $q|p-4$ sin importar si $p \equiv 1, 3 \pmod 4$. Este caso es relativamente fácil porque con dichos primos podemos utilizar el Teorema de Dedekind.

Lema 3.35. *Sea $L = \mathbb{Q}(\theta)$, con $\theta = \sqrt{\mu}$, μ como en el Teorema 3.33 y $q > 3$ un primo racional tal que $q \mid p-4$. Entonces $q \nmid ind(\theta)$.*

Demostración. Notemos que $q \nmid 9p-100$ y $q \nmid 4p-25$, ya que si $q \mid 9p-100$ ó $q \mid 4p-25$ y dado que

$$9p - 100 = 9(p-4) - 2^6 \quad \text{y} \quad 4p - 25 = 4(p-4) - 3^2,$$

entonces $q = 2$ ó $q = 3$ lo cual no puede ser. De lo anterior concluimos que $q \nmid ind(\theta)$. □

Proposición 3.36. *Sean L, θ, μ como en el lema anterior, $q > 3$ un primo racional tal que $q \mid p-4$ y*

$$\rho(x) = x^8 + 10px^6 + (33p^2 - 14p)x^4 + 5p(8p^2 - 14p)x^2 + p^2(4p-25)^2 = Irr(\theta, \mathbb{Z}).$$

Entonces

$$\rho(x) \equiv \begin{cases} (x^2+2)^2(x^2+18)^2 \pmod q & \text{si } q \equiv 5, 7 \pmod 8 \\ (x-a_1)^2(x+a_1)^2(x-a_2)^2(x+a_2)^2 \pmod q & \text{si } q \equiv 1, 3 \pmod 8, \end{cases}$$

donde $a_1^2 \equiv -2 \pmod q$ y $a_2^2 \equiv -18 \pmod q$.

Demostración. Como $q \mid p-4$, entonces $p \equiv 4 \mod q$. Así

$$\begin{aligned} \rho(x) &= x^8 + 10px^6 + (33p^2 - 14p)x^4 + 5p(8p^2 - 14p)x^2 + p^2(4p-25)^2 \\ &\equiv x^8 + 2^3 5x^6 + 2^3(59)x^4 + 2^5 3^2 5x^2 + 2^4 3^4 \pmod q \\ &\equiv (x^2 - (-2))^2(x^2 - (-18))^2 \pmod q. \end{aligned}$$

Si $q \equiv 5, 7 \pmod 8$, entonces $q \equiv 1, 3 \pmod 4$ respectivamente, en este caso tenemos

$$\left(\frac{-2}{q}\right) = \left(\frac{-18}{q}\right) = -1,$$

es decir, los polinomios $x^2 - (-2)$ y $x^2 - (-18)$ son irreducibles en $\mathbb{F}_q[x]$. Así

$$\rho(x) \equiv (x^2+2)^2(x^2+18)^2 \pmod q.$$

Si $q \equiv 1, 3 \pmod 8$, entonces $q \equiv 1, 3 \pmod 4$ respectivamente, en este caso tenemos

$$\left(\frac{-2}{q}\right) = \left(\frac{-18}{q}\right) = 1,$$

es decir, $x^2 - (-2) \equiv (x-a_1)(x+a_1)$ y $x^2 - (-18) \equiv (x-a_2)(x+a_2)$ en $\mathbb{F}_q[x]$. Así $\rho(x) \equiv (x-a_1)^2(x+a_1)^2(x-a_2)^2(x+a_2)^2 \pmod q$, donde $a_1^2 \equiv -2 \pmod q$ y $a_2^2 \equiv -18 \pmod q$. □

El siguiente resultado nos da la ramificación de los factores primos de $p-4$.

Teorema 3.37. *Sea $L = \mathbb{Q}(\theta)$ y $q > 3$ un primo racional tal que $q \mid p-4$. Entonces*

$$q\mathcal{O}_L = \begin{cases} \langle q, \theta^2+2\rangle^2\langle q, \theta^2+18\rangle^2 & \textit{si} \quad q \equiv 5,7 \pmod 8 \\ \langle q, \theta-a_1\rangle^2\langle q, \theta+a_1\rangle^2\langle q, \theta-a_2\rangle^2\langle q, \theta+a_2\rangle^2 & \textit{si} \quad q \equiv 1,3 \pmod 8, \end{cases}$$

donde $a_1^2 \equiv -2 \pmod q$ y $a_2^2 \equiv -18 \pmod q$.

Demostración. Sea $q \neq 3$ un primo racional tal que $q \mid p-4$- Entonces por el Lema 3.35, tenemos $q \nmid ind(\theta)$ y por tanto, podemos usar el Teorema de Dedekind. Por la proposición anterior,

$$\rho(x) \equiv \begin{cases} (x^2+2)^2(x^2+18)^2 \pmod q & \text{si} \quad q \equiv 5,7 \pmod 8, \\ (x-a_1)^2(x+a_1)^2(x-a_2)^2(x+a_2)^2 \pmod q & \text{si} \quad q \equiv 1,3 \pmod 8. \end{cases}$$

Por lo tanto,

$$q\mathcal{O}_L = \begin{cases} \langle q, \theta^2+2\rangle^2\langle q, \theta^2+18\rangle^2 & \text{si} \quad q \equiv 5,7 \pmod 8 \\ \langle q, \theta-a_1\rangle^2\langle q, \theta+a_1\rangle^2\langle q, \theta-a_2\rangle^2\langle q, \theta+a_2\rangle^2 & \text{si} \quad q \equiv 1,3 \pmod 8, \end{cases}$$

□

Como acabamos de ver, la ramificación de los factores primos $\neq 3$ de $p-4$ es la misma sin importar $p \equiv 1,3 \pmod 4$. Ahora veremos cuál es la ramificación de $3\mathcal{O}_L$ si $3 \mid p-4$. Por la Proposición 3.14, tenemos

$$3\mathcal{O}_K = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle^2 \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle^2,$$

en donde

$$\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle \quad \text{y} \quad \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle$$

son ideales primos de $\mathcal{O}_K$.

Lema 3.38. *Los ideales $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle$ y $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle$ satisfacen*

$$\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle \nmid \delta_{L/K}, \quad \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle \nmid \delta_{L/K}.$$

Demostración. Si $p \equiv 3 \pmod 4$, entonces por el Teorema 3.32,

$$\delta_{L/K} = \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle^2 \langle\sqrt{p}\rangle.$$

Supongamos que $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle \mid \delta_{L/K}$, entonces

$$\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle \mid \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle$$

ó

$$\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle \mid \langle\sqrt{p}\rangle.$$

Si $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle \mid \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle$, se tiene que

$$1 \in \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle,$$

lo cual no puede ser. Por la misma razón $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle \nmid \langle\sqrt{p}\rangle$. De manera similar se prueba que $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle \nmid \delta_{L/K}$. El caso $p \equiv 1 \pmod 4$ es similar. □

De la proposición anterior, $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle$ y $\left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle$ no se ramifican en $\mathcal{O}_L$, de hecho como veremos a continuación, dichos ideales se descomponen totalmente en $\mathcal{O}_L$.

Lema 3.39. *Sea* $P_1 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1 \right\rangle$. *La congruencia* $x^2 \equiv \mu \pmod{P_1}$ *es soluble.*

Demostración. Notemos que

$$\begin{aligned} 1-\mu &= 1+\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p}+\frac{5}{2}p \\ &= 3\left[\frac{7+2p}{3}+2\sqrt{p}+\frac{4-p}{3}\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)\right] \\ &\quad +\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}+1\right)\left[-6+\frac{\sqrt{p}+\sqrt{p-4}}{2}+2\frac{1+\sqrt{p^2-4p}}{2}\right]. \end{aligned}$$

Así, $1-\mu \in P_1$, es decir, la congruencia $x^2 \equiv \mu \pmod{P_1}$ es soluble con $x=1$. □

Lema 3.40. *Sea* $\nu = \frac{-p+\sqrt{p^2-4p}}{2}$. *Entonces*

(i) $K(\sqrt{\mu}) = K(\sqrt{\nu})$.

(ii) $\nu \notin \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle$.

Demostración. Para (i) sólo notemos que $\mu = \left(\frac{-p+\sqrt{p^2-4p}}{2}\right)(-\sqrt{p}-\sqrt{p-4}-1)^2$.

Para (ii), si $\frac{-p+\sqrt{p^2-4p}}{2} \in \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle$, entonces

$$-p = \left(\frac{-p+\sqrt{p^2-4p}}{2}\right)\left(\frac{p+\sqrt{p^2-4p}}{2}\right) \in \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1 \right\rangle,$$

lo cuál no puede ser. □

Lema 3.41. *Sea* $P_2 = \left\langle 3, \dfrac{\sqrt{p}+\sqrt{p-4}}{2} - 1 \right\rangle$. *La congruencia* $x^2 \equiv \nu \pmod{P_2}$ *es soluble.*

Demostración. Sea $x = \dfrac{\sqrt{p}+\sqrt{p-4}}{2}$. Entonces

$$\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)^2 - \left(\frac{-p+\sqrt{p^2-4p}}{2}\right) = p-1 \in P_2. \quad \square$$

Proposición 3.42. *La factorización en* $\mathcal{O}_L$ *de los ideales* $P_1 = \left\langle 3, \dfrac{\sqrt{p}+\sqrt{p-4}}{2} + 1 \right\rangle$ *y* $P_2 = \left\langle 3, \dfrac{\sqrt{p}+\sqrt{p-4}}{2} - 1 \right\rangle$ *con* $3 \mid p-4$ *es la siguiente.*

$$P_1\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2 \quad y \quad P_2\mathcal{O}_L = \mathcal{P}_3\mathcal{P}_4,$$

donde

$$\mathcal{P}_1 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1, 1 - \sqrt{\mu} \right\rangle, \quad \mathcal{P}_2 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1, 1 + \sqrt{\mu} \right\rangle,$$

$$\mathcal{P}_3 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1, \frac{\sqrt{p}+\sqrt{p-4}}{2} - \sqrt{\nu} \right\rangle,$$

y

$$\mathcal{P}_4 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1, \frac{\sqrt{p}+\sqrt{p-4}}{2} + \sqrt{\nu} \right\rangle.$$

Demostración. Por el Lema 3.39, tenemos que la congruencia $x^2 \equiv \mu \pmod{P_1}$ es soluble en $\mathcal{O}_K$, con $x = 1$. Por lo tanto, por la Proposición 1.68 (i),

$$P_1\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2,$$

con

$$\mathcal{P}_1 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1, 1 - \sqrt{\mu} \right\rangle, \quad \mathcal{P}_2 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1, 1 + \sqrt{\mu} \right\rangle.$$

Dado que $\mu \in P_2$, el Lema 3.40 nos proporciona un nuevo generador ν tal que $\nu \notin P_2$ y por el Lema 3.41, la congruencia $x^2 \equiv \nu \pmod{P_2}$ es soluble con $x = \dfrac{\sqrt{p}+\sqrt{p-4}}{2}$. Así por la Proposición 1.68 (i),

$$P_2\mathcal{O}_L = \mathcal{P}_3\mathcal{P}_4,$$

con

$$\mathcal{P}_3 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1, \frac{\sqrt{p}+\sqrt{p-4}}{2} - \sqrt{\nu} \right\rangle$$

y

$$\mathcal{P}_4 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1, \frac{\sqrt{p}+\sqrt{p-4}}{2} + \sqrt{\nu} \right\rangle.$$

$\square$

Ahora veremos cuál es la ramificación de $3\mathcal{O}_L$ con $3 \mid p-4$.

Teorema 3.43. *Sea $L = \mathbb{Q}(\theta)$ con $\theta = \sqrt{\mu}$ y $3 \mid p-4$. Entonces*

$$3\mathcal{O}_L = \mathcal{P}_1^2\mathcal{P}_2^2\mathcal{P}_3^2\mathcal{P}_4^2$$

donde

$$\mathcal{P}_1 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1, 1 - \sqrt{\mu} \right\rangle, \quad \mathcal{P}_2 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} + 1, 1 + \sqrt{\mu} \right\rangle,$$

$$\mathcal{P}_3 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1, \frac{\sqrt{p}+\sqrt{p-4}}{2} - \sqrt{\nu} \right\rangle,$$

y

$$\mathcal{P}_4 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2} - 1, \frac{\sqrt{p}+\sqrt{p-4}}{2} + \sqrt{\nu} \right\rangle.$$

Demostración.

$$\begin{aligned} 3\mathcal{O}_L &= (3\mathcal{O}_K)\mathcal{O}_L \\ &= (P_1^2P_2^2)\mathcal{O}_L \\ &= (P_1\mathcal{O}_L)^2(P_2\mathcal{O}_L)^2 \\ &= \mathcal{P}_1^2\mathcal{P}_2^2\mathcal{P}_3^2\mathcal{P}_4^2. \end{aligned}$$

□

Lo que sigue a continuación es dar la ramificación de los primos 2 y p cuando $p \equiv 3 \pmod 4$. Para dichos primos no podremos usar el Teorema de Dedekind, por lo menos, no con el generador θ. Lo que haremos es usar la teoría de las extensiones relativas.

Teorema 3.44. *Sea $L = \mathbb{Q}(\theta)$ con $\theta = \sqrt{\mu}$ y μ como en el Teorema 3.33. Entonces*

(i) $2\mathcal{O}_L = \mathcal{Q}^4$ *con $\mathcal{Q}$ un ideal primo de $\mathcal{O}_L$.*
(ii) $p\mathcal{O}_L = \mathcal{P}^4$ *con $\mathcal{P}$ un ideal primo de $\mathcal{O}_L$.*

Demostración. Si $p \equiv 3 \pmod 4$, por el Teorema 3.32 entonces

$$\delta_{L/K} = \langle 2 \rangle \langle \sqrt{p} \rangle,$$

y como $2\mathcal{O}_K = \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle^2$, los únicos ideales primos de $\mathcal{O}_K$ que se ramifican en $\mathcal{O}_L$ son $\langle\sqrt{p}\rangle$ y $\left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle$, es decir, $e > 1$ y como $efg = 2$ dado que la extensión $L|K$ es Galois, podemos concluir que $e = 2, f = 1$ y $g = 1$. De lo anterior tenemos que

$$\langle\sqrt{p}\rangle\mathcal{O}_L = \mathcal{P}^2 \quad \text{y} \quad \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle \mathcal{O}_L = \mathcal{Q}^2,$$

con $\mathcal{P}$ y $\mathcal{Q}$ ideales primos de $\mathcal{O}_L$. Así para el caso (i) tenemos que

$$\begin{aligned} 2\mathcal{O}_L &= (2\mathcal{O}_K)\mathcal{O}_L \\ &= \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle^2 \mathcal{O}_L \\ &= \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle \mathcal{O}_L \cdot \left\langle 2, \frac{p+\sqrt{p}+\sqrt{p-4}+\sqrt{p^2-4p}}{2} \right\rangle \mathcal{O}_L \\ &= \mathcal{Q}^2 \cdot \mathcal{Q}^2 = \mathcal{Q}^4. \end{aligned}$$

y para el caso (ii) tenemos que

$$p\mathcal{O}_L = (p\mathcal{O}_K)\mathcal{O}_L = \langle\sqrt{p}\rangle^2\mathcal{O}_L = \langle\sqrt{p}\rangle\mathcal{O}_L\langle\sqrt{p}\rangle\mathcal{O}_L = \mathcal{P}^2 \cdot \mathcal{P}^2 = \mathcal{P}^4.$$

□

A continuación damos los generadores de $\mathcal{Q}$ y $\mathcal{P}$.

Lema 3.45. *Sean* $L = \mathbb{Q}(\theta)$ *y* $\eta = \left(\frac{1+\sqrt{p}}{2}\right)\left(\frac{\sqrt{p}-\sqrt{p-4}}{2} - 1 - \theta\right)$. *Entonces*

$$\eta, \frac{\eta^4}{2} \in \mathcal{O}_L.$$

Demostración. Primero veremos que η es entero algebraico. Notemos que η es raíz de

$$\begin{aligned} h(x) &= x^2 - (1+\sqrt{p})\left(\frac{\sqrt{p}-\sqrt{p-4}}{2} - 1\right)x \\ &\quad + \left(\frac{p+1}{2} + \sqrt{p}\right)\left(\frac{3p-1}{2} + \frac{1+\sqrt{p^2-4p}}{2} - \frac{\sqrt{p}-\sqrt{p-4}}{2} + 2\sqrt{p}\right), \end{aligned}$$

y $h(x) \in \mathcal{O}_K[x]$, es decir, η es entero sobre $\mathcal{O}_K$ y como $\mathcal{O}_K$ es entero sobre $\mathbb{Z}$, por la Proposición 1.11, η es entero sobre $\mathbb{Z}$. Por lo tanto $\eta \in \mathcal{O}_L$.

Ahora veremos que $\dfrac{\eta^4}{2}$ es entero algebraico. Notemos que

$$\eta^2 = \left(\frac{p+1}{2} + \sqrt{p}\right)\left(-p - \sqrt{p^2-4p} - 2\sqrt{p} - \left(\frac{\sqrt{p}-\sqrt{p-4}}{2}\right)(1+\theta) + \theta\right).$$

Como $p = 4t + 3$, tenemos

$$\begin{aligned}
\frac{\eta^4}{2} &= p^2\left(\frac{p+1}{2}+\sqrt{p}\right)^2 + p\left(\sqrt{p^2-4p}+2\sqrt{p}\right)\left(\frac{p+1}{2}+\sqrt{p}\right)^2 \\
&+\left(p+\sqrt{p^2-4p}+2\sqrt{p}\right)\left(\left(\frac{\sqrt{p}-\sqrt{p-4}}{2}\right)(1+\theta)-\theta\right)\left(\frac{p+1}{2}+\sqrt{p}\right)^2 \\
&+2p\sqrt{p-4}\left(\frac{p+1}{2}+\sqrt{p}\right)^2 + \theta\left(\frac{p-2-\sqrt{p^2-4p}}{2}\right)\left(\frac{p+1}{2}+\sqrt{p}\right)^2 \\
&-\left(\frac{\sqrt{p}-\sqrt{p-4}}{2}\right)(1+\theta)\theta\left(\frac{p+1}{2}+\sqrt{p}\right)^2 - (6t+5)\left(\frac{p+1}{2}+\sqrt{p}\right)^2 \\
&-(2t+1)\left(\frac{p+1}{2}\right)\left(\frac{p+1}{2}+\sqrt{p}\right)^2 - 2\sqrt{p}\left(\frac{p+1}{2}+\sqrt{p}\right)^2 \\
&+(2t+1)\left(\frac{1+\sqrt{p^2-4p}}{2}\right)\left(\frac{p+1}{2}+\sqrt{p}\right)^2 \\
&-2\sqrt{p}\left(\frac{p-2-\sqrt{p^2-4p}}{2}\right)\left(\frac{p+1}{2}+\sqrt{p}\right)^2.
\end{aligned}$$

Dado que $\frac{\eta^4}{2}$ es suma y producto de enteros algebraicos de $\mathcal{O}_L$, tenemos que $\frac{\eta^4}{2} \in \mathcal{O}_L$. $\square$

Lema 3.46. *Sean* $L = \mathbb{Q}(\theta)$ *y* $\eta = \left(\frac{1+\sqrt{p}}{2}\right)\left(\frac{\sqrt{p}-\sqrt{p-4}}{2} - 1 - \theta\right)$. *Entonces*

$$\left\langle 8, 4\eta, 2\eta^2, \eta^3, \frac{\eta^4}{2}\right\rangle = \mathcal{O}_L.$$

Demostración. Lo que haremos es calcular la norma de $\frac{\eta^4}{2}$, para ello necesitamos la norma de η.

$$\begin{aligned}
N(\eta) &= \sigma_0(\eta)\sigma_1(\eta)\sigma_2(\eta)\sigma_3(\eta)\sigma_4(\eta)\sigma_5(\eta)\sigma_6(\eta)\sigma_7(\eta)\\
&= \left(\frac{1+\sqrt{p}}{2}\right)\left(\frac{\sqrt{p}-\sqrt{p-4}}{2}-1-\theta_2\right)\left(\frac{1-\sqrt{p}}{2}\right)\left(\frac{-\sqrt{p}-\sqrt{p-4}}{2}-1-\theta_1\right)\\
&\quad \left(\frac{1-\sqrt{p}}{2}\right)\left(\frac{-\sqrt{p}+\sqrt{p-4}}{2}-1-\theta_4\right)\left(\frac{1+\sqrt{p}}{2}\right)\left(\frac{\sqrt{p}-\sqrt{p-4}}{2}-1+\theta_2\right)\\
&\quad \left(\frac{1-\sqrt{p}}{2}\right)\left(\frac{-\sqrt{p}-\sqrt{p-4}}{2}-1+\theta_1\right)\left(\frac{1+\sqrt{p}}{2}\right)\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}-1-\theta_3\right)\\
&\quad \left(\frac{1-\sqrt{p}}{2}\right)\left(\frac{-\sqrt{p}+\sqrt{p-4}}{2}-1+\theta_4\right)\left(\frac{1+\sqrt{p}}{2}\right)\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}-1+\theta_3\right)\\
&= \left(\frac{p-1}{4}\right)^4\left[\left(\frac{\sqrt{p}-\sqrt{p-4}}{2}-1\right)^2-\theta_2^2\right]\left[\left(\frac{-\sqrt{p}-\sqrt{p-4}}{2}-1\right)^2-\theta_1^2\right]\\
&\quad \left[\left(\frac{-\sqrt{p}+\sqrt{p-4}}{2}-1\right)^2-\theta_4^2\right]\left[\left(\frac{\sqrt{p}+\sqrt{p-4}}{2}-1\right)^2-\theta_3^2\right].
\end{aligned}$$

Del Lema3.5 tenemos

$$\theta_1=\sqrt{\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p}-\frac{5}{2}p},\quad \theta_2=\sqrt{-\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p}-\frac{5}{2}p},$$

$$\theta_3=\sqrt{\left(\frac{3}{2}\sqrt{p-4}-4\right)\sqrt{p}-\frac{5}{2}p},\quad \theta_4=\sqrt{-\left(\frac{3}{2}\sqrt{p-4}-4\right)\sqrt{p}-\frac{5}{2}p}.$$

Así

$$\begin{aligned}
N(\eta) &= \left(\frac{p-1}{4}\right)^4(4p^4-4p^3-3p^2+2p+1)\\
&= 2^2\left(\frac{p-1}{2}\right)^6(2p+1)^2.
\end{aligned}$$

De lo anterior, $N\left(\frac{\eta^4}{2}\right)=\left(\frac{p-1}{2}\right)^{24}(2p+1)^8$. Como $N\left(\frac{\eta^4}{2}\right)\in\left\langle 8,4\eta,2\eta^2,\eta^3,\frac{\eta^4}{2}\right\rangle$, concluimos que $\left\langle 8,4\eta,2\eta^2,\eta^3,\frac{\eta^4}{2}\right\rangle=\mathcal{O}_L$. □

Proposición 3.47. *Sea $L=\mathbb{Q}(\theta)$. Entonces*

$$2\mathcal{O}_L=\langle 2,\eta\rangle^4.$$

Demostración.

$$\begin{aligned}
\langle 2,\eta\rangle^4 &= \langle 16,8\eta,4\eta^2,2\eta^3,\eta^4\rangle\\
&= \langle 2\rangle\left\langle 8,4\eta,2\eta^2,\eta^3,\frac{\eta^4}{2}\right\rangle.
\end{aligned}$$

Del lema anterior, $\left\langle 8, 4\eta, 2\eta^2, \eta^3, \frac{\eta^4}{2} \right\rangle = \mathcal{O}_L$, entonces $\langle 2, \eta\rangle^4 = \langle 2\rangle = 2\mathcal{O}_L$. □

Lema 3.48. *Sea $\mathcal{Q}$ el ideal primo del Teorema 3.44. Entonces $\mathcal{Q} = \langle 2, \eta\rangle$.*

Demostración. Supongamos que $\langle 2, \eta\rangle$ no es ideal primo. Sea $\mathcal{Q}_1$ un ideal máximo tal que $\langle 2, \eta\rangle \subset \mathcal{Q}_1$. Entonces por la Proposición 1.42 existe un ideal R tal que

$$\langle 2, \eta\rangle = \mathcal{Q}_1 R.$$

Así

$$\langle 2, \eta\rangle^4 = \mathcal{Q}_1^4 R^4 = 2\mathcal{O}_L = \mathcal{Q}^4.$$

Como $\mathcal{Q}$ y $\mathcal{Q}_1$ son ideales primos, por factorización única tenemos $R^4 = \mathcal{O}_L$, de donde $\mathcal{Q}_1 = \mathcal{Q}$ y por tanto $\mathcal{Q} = \langle 2, \eta\rangle$. □

Lema 3.49. *Sean $L = \mathbb{Q}(\theta)$ y $T = \left\langle p\sqrt{p}, \frac{5}{2}\sqrt{p} + \frac{3}{2}\sqrt{p-4} + 4 \right\rangle$ un ideal de $\mathcal{O}_L$. Entonces $1 \in T$.*

Demostración. Notemos que $p^2 \in T$ y

$$\frac{5}{2}\sqrt{p} + \frac{3}{2}\sqrt{p-4} + 4 = \left(\frac{\sqrt{p} - \sqrt{p-4}}{2}\right)(\sqrt{p} + \sqrt{p-4} + 1)^2 \in T$$

y como $\left(\frac{\sqrt{p} - \sqrt{p-4}}{2}\right)$ es unidad de $\mathcal{O}_L$, entonces $(\sqrt{p} + \sqrt{p-4} + 1)^2 \in T$. Así

$$(5 + 2\sqrt{p})^2 = (\sqrt{p} + \sqrt{p-4} + 1)^2(\sqrt{p} - \sqrt{p-4} + 1)^2 \in T.$$

De lo anterior, $(25 + 20\sqrt{p} + 4p)p \in T$, de donde $25p \in T$. Por otro lado,

$$5^4 - 8(25p) + 16p^2 = (5 + 2\sqrt{p})^2(5 - 2\sqrt{p})^2 \in T$$

y así $5^4 \in T$. Dado que $p \geq 7$, entonces $mcd(p^2, 5^4) = 1$. Por lo tanto, $1 \in T$. □

Proposición 3.50. *Sea $L = \mathbb{Q}(\theta)$. Entonces $\langle p, \theta\rangle^4 = p\mathcal{O}_L$.*

Demostración. Notemos

$$\begin{aligned} \langle p, \theta\rangle^2 &= \langle p^2, p\theta, p\theta, \mu\rangle \\ &= \langle p^2, p\theta, \mu\rangle \\ &= \langle \sqrt{p}\rangle \left\langle p\sqrt{p}, \sqrt{p}\theta, -\frac{5}{2}\sqrt{p} - \frac{3}{2}\sqrt{p-4} - 4 \right\rangle. \end{aligned}$$

Sea T como en el lema anterior. Observemos que

$$T \subseteq \left\langle p\sqrt{p}, \sqrt{p}\theta, -\frac{5}{2}\sqrt{p} - \frac{3}{2}\sqrt{p-4} - 4 \right\rangle,$$

por tanto

$$\left\langle p\sqrt{p}, \sqrt{p}\theta, -\frac{5}{2}\sqrt{p} - \frac{3}{2}\sqrt{p-4} - 4 \right\rangle = \mathcal{O}_L.$$

Así $\langle p, \theta\rangle^4 = p\mathcal{O}_L$. □

Lema 3.51. *Sea $\mathcal{P}$ el ideal primo del Teorema 3.44* (ii)*. Entonces $\mathcal{P} = \langle p, \theta\rangle$.*

Demostración. La demostración es idéntica a la demostración de Lema 3.48 □

Por último daremos la ramificación de p en $\mathcal{O}_L$ con $p \equiv 1 \pmod 4$ y de nuevo usaremos la teoría de extensiones relativas. Recordemos que la ramificación de p en el caso $p \equiv 3 \pmod 4$ la hemos estudiado en el Teorema 3.44 y en la Proposición 3.50.

Teorema 3.52. *Sea $L = \mathbb{Q}(\theta)$ con $p \equiv 1 \pmod 4$. Entonces*

$$p\mathcal{O}_L = \mathcal{P}_1^4\mathcal{P}_2^4,$$

con $\mathcal{P}_1$ y $\mathcal{P}_2$ ideales primos de $\mathcal{O}_L$.

Demostración. En este caso, $\delta_{L/K} = \langle\sqrt{p}\rangle$ y por el Corolario 3.17, tenemos

$$\sqrt{p}\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b\right\rangle,$$

donde $b^2 \equiv -1 \pmod p$. Los únicos ideales primos de $\mathcal{O}_K$ que se ramifican en $\mathcal{O}_L$ son

$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle \quad \text{y} \quad \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b\right\rangle.$$

De igual manera tenemos que $efg = 2$ con $e = 2$, $f = g = 1$. Así

$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle \mathcal{O}_L = \mathcal{P}_1^2, \quad \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b\right\rangle \mathcal{O}_L = \mathcal{P}_2^2,$$

con $\mathcal{P}_1$ y $\mathcal{P}_2$ ideales primos de $\mathcal{O}_L$. De lo anterior,

$$\begin{aligned} p\mathcal{O}_L &= (p\mathcal{O}_K)\mathcal{O}_L \\ &= \left(\langle\sqrt{p}\rangle\mathcal{O}_L\right)^2 \\ &= \left(\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle \mathcal{O}_L\right)^2 \left(\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b\right\rangle \mathcal{O}_L\right)^2 \\ &= \mathcal{P}_1^4 \cdot \mathcal{P}_2^4. \end{aligned}$$

□

Lo que sigue a continuación es dar los generadores de $\mathcal{P}_1$ y $\mathcal{P}_2$.

Proposición 3.53. *Con las mismas hipótesis del teorema anterior tenemos:*

$$\mathcal{P}_1 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b, \theta\right\rangle \quad y \quad \mathcal{P}_2 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b, \theta\right\rangle.$$

Demostración. Por el Lema 3.10 $\mu\mathcal{O}_K = \langle\sqrt{p}\rangle\langle-\sqrt{p}-\sqrt{p-4}-1\rangle^2$ y el Corolario 3.17, tenemos

$$\sqrt{p}\mathcal{O}_K = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b\right\rangle,$$

entonces por la Proposición 1.67, con $t = \theta$ y $h = 2$, se cumple

$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b\right\rangle \mathcal{O}_L = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b, \theta\right\rangle^2$$

y

$$\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)+b\right\rangle \mathcal{O}_L = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)+b, \theta\right\rangle^2,$$

con $\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)-b, \theta\right\rangle$ y $\left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)+b, \theta\right\rangle$ ideales primos de $\mathcal{O}_L$. Así tenemos que

$$p\mathcal{O}_L = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)-b, \theta\right\rangle^4 \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)+b, \theta\right\rangle^4.$$

Por tanto, por la factorización única de ideales

$$\mathcal{P}_1 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)-b, \theta\right\rangle \quad \text{y} \quad \mathcal{P}_2 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right)+b, \theta\right\rangle.$$

□

En los próximos dos teoremas resumimos la factorización de los primos racionales ramificados en $\mathcal{O}_L$

Teorema 3.54. *Sea* $L = \mathbb{Q}(\theta)$ *con* $\theta = \sqrt{-\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p}-\frac{5}{2}p}$ *y* $p \equiv 3 \pmod 4$.

Entonces

(i) $\delta_L = 2^{12}(p-4)^4p^6$. *Ver Teorema 3.33.*

(ii) *Si* $q \geq 7$ *es un primo racional tal que* $q \mid p-4$, *entonces*

$$q\mathcal{O}_L = \begin{cases} \langle q, \theta^2+2\rangle^2\langle q, \theta^2+18\rangle^2 & \textit{si} \quad q \equiv 5,7 \pmod 8 \\ \langle q, \theta-a_1\rangle^2\langle q, \theta+a_1\rangle^2\langle q, \theta-a_2\rangle^2\langle q, \theta+a_2\rangle^2 & \textit{si} \quad q \equiv 1,3 \pmod 8, \end{cases}$$

donde $a_1^2 \equiv -2 \pmod q$ *y* $a_2^2 \equiv -18 \pmod q$. *Ver Teorema 3.37.*

(iii) *Si* $3 \mid p-4$ *y* $\nu = \dfrac{-p+\sqrt{p^2-4p}}{2}$, *entonces*

$$3\mathcal{O}_L = \mathcal{P}_1^2\mathcal{P}_2^2\mathcal{P}_3^2\mathcal{P}_4^2$$

donde

$$\mathcal{P}_1 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1, 1-\theta\right\rangle, \quad \mathcal{P}_2 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1, 1+\theta\right\rangle,$$

$$\mathcal{P}_3 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1, \frac{\sqrt{p}+\sqrt{p-4}}{2}-\sqrt{\nu}\right\rangle$$

y

$$\mathcal{P}_4 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1, \frac{\sqrt{p}+\sqrt{p-4}}{2}+\sqrt{\nu}\right\rangle.$$

Ver Teorema 3.43.

(iv) $2\mathcal{O}_L = \mathcal{Q}^4$ *con* $\mathcal{Q} = \langle 2, \eta\rangle$ *un ideal primo de* $\mathcal{O}_L$. *Ver Teorema 3.44 (i) y Lema 3.48.*

(v) $p\mathcal{O}_L = \mathcal{P}^4$ *con* $\mathcal{P} = \langle p, \theta\rangle$ *un ideal primo de* $\mathcal{O}_L$. *Ver Teorema 3.44 (ii) y Lema 3.51.*

Teorema 3.55. *Sea* $L = \mathbb{Q}(\theta)$ *con* $\theta = \sqrt{-\left(\frac{3}{2}\sqrt{p-4}+4\right)\sqrt{p} - \frac{5}{2}p}$ *y* $p \equiv 1 \pmod 4$.

Entonces

(i) $\delta_L = (p-4)^4 p^6$. *Ver Teorema 3.33.*

(ii) *Si* $q \geq 7$ *es un primo racional tal que* $q \mid p-4$, *entonces*

$$q\mathcal{O}_L = \begin{cases} \langle q, \theta^2+2\rangle^2\langle q, \theta^2+18\rangle^2 & \text{si} \quad q \equiv 5,7 \pmod 8 \\ \langle q, \theta-a_1\rangle^2\langle q, \theta+a_1\rangle^2\langle q, \theta-a_2\rangle^2\langle q, \theta+a_2\rangle^2 & \text{si} \quad q \equiv 1,3 \pmod 8, \end{cases}$$

donde $a_1^2 \equiv -2 \pmod q$ *y* $a_2^2 \equiv -18 \pmod q$. *Ver Teorema 3.37.*

(iii) *Si* $3 \mid p-4$ *y* $\nu = \dfrac{-p+\sqrt{p^2-4p}}{2}$, *entonces*

$$3\mathcal{O}_L = \mathcal{P}_1^2\mathcal{P}_2^2\mathcal{P}_3^2\mathcal{P}_4^2$$

donde

$$\mathcal{P}_1 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1, 1-\theta \right\rangle, \quad \mathcal{P}_2 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}+1, 1+\theta \right\rangle,$$

$$\mathcal{P}_3 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1, \frac{\sqrt{p}+\sqrt{p-4}}{2}-\sqrt{\nu} \right\rangle$$

y

$$\mathcal{P}_4 = \left\langle 3, \frac{\sqrt{p}+\sqrt{p-4}}{2}-1, \frac{\sqrt{p}+\sqrt{p-4}}{2}+\sqrt{\nu} \right\rangle.$$

Ver Teorema 3.43.

(iv) $p\mathcal{O}_L = \mathcal{P}_1^4\mathcal{P}_2^4$ *con*

$$\mathcal{P}_1 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) - b, \theta \right\rangle, \quad \mathcal{P}_2 = \left\langle p, \left(\frac{\sqrt{p}+\sqrt{p-4}}{2}\right) + b, \theta \right\rangle$$

ideales primos de $\mathcal{O}_L$ *y* $b^2 \equiv -1 \pmod p$. *Ver Teorema 3.52 y Proposición 3.53.*

Conclusiones generales

Se cumplieron todos los objetivos planteados en el proyecto:

(i) Dar la factorización de cualquier primo racional q en $\mathcal{O}_K$ cuando $G_f = C_4$ para $f(x) = x^4 + px^2 + p$.
(ii) Dar la ramificación ($e > 1$) en $\mathcal{O}_L$ de los primos racionales q cuando $G_f = D_8$ para $f(x) = x^4 + px^2 + p$.
(iii) Dar generadores de todos los ideales primos que aparecen en la ramificación y factorización de los primos racionales q.

Trabajo inmediato

(i) Creemos que podemos construir extensiones cíclicas monogénicas cuarticas con primos de la forma $p = 4 + n^2 = 3k + 2$. (ver Teorema 2.14).
(ii) Dar la descomposición de primos racionales no ramificados en $\mathcal{O}_L$ en el caso diédrico.
(iii) Encontrar una base entera para $\mathcal{O}_L$ en donde $L|\mathbb{Q}$ es una extensión de Galois diédrica de grado 8.
(iv) Encontrar una base entera de una extensión de campos de números $L|K$ dada una base entera de $\mathcal{O}_K$.

Índice alfabético

Bibliografía

[1] Alaca S, Spearman B.K. and Williams K. The Factorization of 2 in Cubic Fields with Index 2. Far East J. Math. Sci. pp. 273-282, 2004.

[2] Alaca S. and Williams K. *Introductory Algebraic Number Theory*, Cambridge University Press, 2004.

[3] Aguilar-Zavoznik A. and Pineda-Ruelas M. Ramification of 2 in Quadratic Extensions over Some Pure Quartic Fields. International Journal of Algebra, vol. 7, no. 10, pp. 487-508, 2013.

[4] Atiyah M.F. and Macdonald I.G. *Introducción al álgebra conmutativa*. Reverté, 1973.

[5] Conrad Keith. Factoring after Dedekind. https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf.

[6] Conrad Keith, Galois group and permutations groups, https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf

[7] Conway J.H. Hulpke A., McKay J. On transitive permutation groups, LMS J. Comput. Math. pp 1-8, 1998.

[8] Dedekind R. *Theory of algebraic integers.* Cambridge Mathematical Library. Translated from the 1877 French original and with an introduction by John Stillwell, 1997.

[9] Dixon J., Mortimer B. *Permutation Groups*. Springer Verlag GTM 163, New York, 1986.

[10] Driver E., Leonard P.A. and Williams K.S. Irreducible Quartic Polynomials with Factorizations modulo p, The Mathematical Association of America, American Mathematical Monthly 112, pp. 876-890, December 2005 .

[11] Engstrom H.T. On the common index divisors of an algebraic field. Trans. Amer. Math. Soc. 32, pp. 223-237, 1921.

[12] Frazer J. *Algebraic Number Theory*. Springer-Verlag UTM, 2014.

[13] Funakura T. On integral bases of pure quartic fields, Math. J. Okayama Univ. No. 26, pp. 27-41, 1984 .

[14] Gaal I., Petho A., Pohst M. On the indices of biquadratic number fields having Galois group V4 , Arch. Math. vol. 57, pp. 357-361, 1991.

[15] Godwin H. J. On Relations Between Cubic and Quartic Fields, Quart. J. Math. Oxford (2), 13, pp 206-212, 1962.

[16] Hardy H., Hudson R.H., Richman D. and Williams K.S. Determination of all imaginary cyclic quartic fields with class number 2. Transaction of the American Mathematical Society, vol. 311, No. 1, 1989.

[17] Hardy H., Hudson R.H., Richman D., Williams K.S. and Holtz N.M. Calculation of the Class Numbers of Imaginary Cyclic Quartic Fields. Mathematics of Computation, Vol. 49, No. 180, pp 615-620, 1987.

[18] Huard J.G., Sperman B.K. and Williams K.S. Integral bases for quartic fields with quadratic subfields. Carleton University Centre for Research in Algebra and Number Theory Mathematical Research Series No. 4, June 1991.

[19] Huard J.G., Sperman B.K. and Williams K.S. Integral bases for quartic fields with quadratic subfields. Journal Number Theory, **51**, pp 87-102, 1995.

[20] Hudson R.H. and Williams K.S. The Integers of a Cyclic Quartic Field. Rocky Mountain Journal of Mathematics, vol. 20, pp. 145-150, 1990.

[21] Ireland K. and Rosen M. *A Classical Introduction to Modern Number Theory,* Springer-Verlag GTM 84, New York, 1982.

[22] Kaplansky I. *Commutative Rings*, The University Chicago Press, 1974.

[23] Kaplansky I. *Fields and Rings*, Chicago Lectures in Mathematics, The University Chicago Press, 1972.

[24] Kappe L.C. and Warren B. An Elementary Test for the Galois Group of a Quartic Polynomial, American Mathematical Montly, vol. 96, No. 2, pp. 133-137, 1989.

[25] Lavallee M.J., Spearman B. K., Williams K.S. and Yang Q. Dihedral quintic fields with a power basis, Math. J. Okayama Univ. **47**, pp. 75-79, 2005.

[26] Llorente P. and Nart E. Effective determination of the decomposition of the rational primes in a cubic field , Proceedings of the AMS, vol. 87, No. 4, April 1983.
[27] Guardia J., Montes J., Nart E. Higher Newton polygons in the computation of discriminants and prime ideals decomposition in number fields. J. Théor. Nombres Bordx. 23, pp. 667-696, 2011.
[28] Nakahara T. On cyclic biquadratic fields related to a problem of Hasse. Mh. Math., 94, pp. 125-132, 1982.
[29] Neukirch J. *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.
[30] Ribenboim P. *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.
[31] Robertson Ashford S. Dyadic Ramification and Quartic Number Field, Journal of Number Theory, No. 45, pp. 68-91, 1993.
[32] Spearman B.K. and Williams K.S. The Conductor of a Cyclic Quartic Field Using Gauss Sums, Czechoslovak Mathematical Journal, vol. 47, No. 3, pp. 453-462, 1997.
[33] Spearman B.K. and Williams K.S. The Index of a Cyclic Quartic Field, Monatsh. Math. 140, pp. 19-70, 2003.
[34] Uspensky J.V. *Teoría de Ecuaciones.* LIMUSA, 1987.
[35] Stein Williams A. *Sage Mathematics Software (Version 8.1)*, The Sage Development Team, http://www.sagemath.org, 2017.
[36] Stewart I., Tall D. *Algebraic Number Theory and Fermat's Last Theorem.* Chapman and Hall, John Wiley and Sons, New York, 1979.
[37] Williams K.S. Integers of biquadratic fields , Canad. Math. Bull., vol. 13, pp. 519-526, 1970.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE DISERTACIÓN PÚBLICA

No. 00079
Matrícula: 2142800095

RAMIFICACIÓN EN GRUPOS DE GALOIS DE POLINOMIOS DE LA FORMA x^4+px^2+p

En la Ciudad de México, se presentaron a las 14:00 horas del día 29 del mes de septiembre del año 2022 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. FLORIAN LUCA
DR. MARIO PINEDA RUELAS
DR. TIMOTHY MOONY GENDRON THORNTON
DR. HORACIO TAPIA RECILLAS
DRA. RITA ESTHER ZUAZUA VEGA

Bajo la Presidencia del primero y con carácter de Secretaria la última, se reunieron a la presentación de la Disertación Pública cuya denominación aparece al margen, para la obtención del grado de:

DOCTOR EN CIENCIAS (MATEMATICAS)

DE: JULIO PEREZ HERNANDEZ

y de acuerdo con el artículo 78 fracción IV del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

JULIO PEREZ HERNANDEZ
ALUMNO

REVISÓ

MTRA. ROSALÍA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

Román Linares Romero

DR. ROMAN LINARES ROMERO

PRESIDENTE

DR. FLORIAN LUCA

VOCAL

DR. MARIO PINEDA RUELAS

VOCAL

DR. TIMOTHY MOONY GENDRON THORNTON

VOCAL

DR. HORACIO TAPIA RECILLAS

SECRETARIA

DRA. RITA ESTHER ZUAZUA VEGA