UNIVERSIDAD AUTÓNOMA METROPOLITANA

UNIDAD IZTAPALAPA

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

EL 2-GRUPO DE CLASES DE UN CAMPO CUADRÁTICO Y UNA FAMILIA DE CAMPOS CUÁRTICOS CON 2-GRUPO DE CLASES DE ORDEN 2

Tesis que presenta

Alejandro Aguilar Zavoznik

para obtener el grado de

Doctor en Ciencias (Matemáticas)

Asesor: Dr. Mario Pineda Ruelas.

Jurado:

Presidente: Dr. Gabriel Daniel Villa Salvador.
Secretario: Dr. Mario Pineda Ruelas.
Vocal: Dr. Pedro Luis del Ángel Rodríguez.
Vocal: Dr. Rogelio Fernández-Alonso González.
Vocal: Dr. Florian Luca.

México

13 de julio de 2012

Índice general

Introducción

El concepto de ideal surgió de forma paralela en la teoría de los números y la geometría algebraica. En el primer caso, el objetivo de usar ideales era recuperar la factorización única cuando un anillo no la tiene. El concepto actual de ideal, que fue definido por Dedekind, está basado en los números ideales de Kummer, los cuales surgieron en el estudio de los campos ciclotómicos. Consideremos el anillo $\mathbb{Z} + \sqrt{10}\,\mathbb{Z} = \{a_1 + a_2\sqrt{10} : a_1, a_2 \in \mathbb{Z}\}$. Este anillo no es de factorización única, pues

$$10 = (2)(5) = \sqrt{10}^2 \tag{1}$$

tiene dos factorizaciones que son esencialmente distintas, es decir, 2 y 5 no son asociados de $\sqrt{10}$. Si ahora consideramos el monoide $(\mathbb{Z} + \sqrt{10}\,\mathbb{Z}) \cup (\sqrt{2}\mathbb{Z} + \sqrt{5}\,\mathbb{Z})$, tenemos que

$$2 = (\sqrt{2})^2, \quad 5 = (\sqrt{5})^2 \quad \text{y} \quad \sqrt{10} = \sqrt{2}\sqrt{5}.$$

Así, las dos factorizaciones en (1) se convierten en:

$$10 = (\sqrt{2})^2(\sqrt{5})^2 = (\sqrt{2}\,\sqrt{5})^2.$$

Lo que hicimos fue agregar los elementos ideales o necesarios al anillo original para que, en la nueva estructura haya factorización única.

El objetivo de los ideales en la teoría de los números algebraicos es el mismo que tenían en un principio los números ideales que se agregaban a una estructura algebraica para procurar la factorización única. Ahora ya no es necesario buscar qué elementos nos servirán como números ideales, pues en este caso, los ideales son subconjuntos del mismo anillo que estamos estudiando. Consideremos el mismo ejemplo, pero ahora tomando la factorización de ideales:

$$\langle 10\rangle = \langle 2\rangle\,\langle 5\rangle = \left\langle \sqrt{10}\right\rangle^2.$$

En $\mathbb{Z} + \sqrt{10}\,\mathbb{Z}$ tenemos

$$\langle 2\rangle = \left\langle 2, \sqrt{10}\right\rangle^2, \quad \langle 5\rangle = \left\langle 5, \sqrt{10}\right\rangle^2 \quad \text{y} \quad \left\langle \sqrt{10}\right\rangle = \left\langle 2, \sqrt{10}\right\rangle \left\langle 5, \sqrt{10}\right\rangle.$$

Así que:

$$\langle 10\rangle = \left\langle 2, \sqrt{10}\right\rangle^2 \left\langle 5, \sqrt{10}\right\rangle^2 = \left(\left\langle 2, \sqrt{10}\right\rangle \left\langle 5, \sqrt{10}\right\rangle\right)^2.$$

De nueva cuenta, volvemos a convertir dos factorizaciones distintas de ideales principales en una misma factorización de ideales que no necesariamente son principales, de esta forma podemos ver que los ideales no principales están tomando el mismo papel que tenían originalmente los números ideales. En lugar de agregar las combinaciones de los elementos $\sqrt{2}$ y $\sqrt{5}$ agregamos los ideales no principales.

Muchos conceptos que nos proporcionan herramientas para estudiar la factorización de ideales han surgido desde entonces. Uno de los más importantes es el grupo de clases

de ideales, que, entre otras cosas, facilita el trabajo de identificar cuándo un producto de ideales es principal y cuándo no lo es. Una herramienta fundamental para estudiar este grupo es el comportamiento de la ramificación de los ideales primos. Un primer objetivo de este trabajo es estudiar el 2-subgupo de Sylow del grupo de clases de ideales de un campo cuadrático, concentrando nuestra atención en el caso en que el exponente del grupo es 2. Como aplicación de los resultados obtenidos encontramos un criterio para distinguir ideales principales de los no principales, dando como consecuencia la clasificación de primos e irreducibles en una familia de anillos de enteros cuadráticos que no es de factorización única. Para continuar con nuestra línea de investigación, es decir, el estudio del 2-grupo de clases en extensiones de grado mayor que 2, un elemento fundamental es la ramificación del primo 2. Mostramos que en extensiones de la forma $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ primo racional, el número de clases $h_{\mathbb{K}}$ es par. De esta forma tenemos una familia de anillos de enteros que no son de factorización única en los cuales toma sentido nuestra investigación. La ramificación de 2 en campos de números suele ser un problema complicado. Se conoce la ramificación de 2 en algunas extensiones de grado 4 (ver [**27**]). Por tal motivo, nosotros nos interesamos en extensiones cuadráticas de $\mathbb{K}$ y logramos distinguir el comportamiento de la ramificación de 2 en esta clase de extensiones. Finalizamos demostrando que el 2-grupo de clases de ideales de $\mathbb{K}$ tiene orden 2.

En el primer capítulo proporcionamos los fundamentos básicos para el desarrollo de este trabajo. En el segundo capítulo estudiamos el 2-subgrupo de Sylow del grupo de clases de ideales de campos cuadráticos. Proporcionamos dos métodos que nos ayudan a decidir si un ideal es o no principal. El primer método es una aplicación de los resultados que obtuvimos en el estudio del 2-subgupo de Sylow del grupo de clases de ideales. En el segundo método estudiamos ecuaciones diofantinas de la forma:

$$d_1\, b_1^2 - d_2\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{I})$$

donde $\mathfrak{I}$ es un ideal no trivial del anillo de enteros de una extensión cuadrática $\mathbb{F}$ de la forma $\mathbb{Q}(\sqrt{d})$ y $d = d_1\, d_2$. Dependiendo de la solubilidad o no solubilidad de ésta se puede decidir si $\mathfrak{I}$ es principal o no lo es. Finalizamos este capítulo proporcionando un criterio para clasificar elementos primos, irreducibles o compuestos en un anillo de enteros de una extensión cuadrática de $\mathbb{Q}$ que no es de factorización única. Comenzamos el tercer capítulo estudiando al grupo de unidades de $\mathbb{Q}(\sqrt{p})$ y los elementos de norma par con $p \equiv 7 \pmod{16}$. Aprovechamos lo anterior para describir ahora al grupo de unidades $\mathcal{U}_{\mathbb{K}}$, donde $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$. Al estudiar los elementos de norma par en el anillo de enteros $\mathbb{K}$ observamos que la ecuación $N_{\mathbb{K}/\mathbb{Q}}\,(\alpha) = \pm 2$ no es soluble, esto nos permite concluir que 2 se ramifica totalmente en $\mathbb{K}$, pero el único ideal con norma 2 no es principal. En la parte final de este capítulo, si $\alpha \in \mathbb{K}$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$, donde α es libre de cuadrados en todas sus factorizaciones, clasificamos las extensiones $\mathbb{L}$ en las cuales 2 se ramifica totalmente o no. Por supuesto que esto va a depender de la elección de α. En algunos casos será fundamental encontrar una base entera de $\mathbb{L}$ para justificar que 2 no se ramifica. Usaremos las herramientas desarrolladas en el tercer capítulo para demostrar que el 2-grupo de clases de ideales es isomorfo a $\mathbb{Z}/2\mathbb{Z}$, para esto, demostramos que solamente existe una extensión cuadrática no ramificada de $\mathbb{K}$ y que el subgrupo cíclico de $Cl_{\mathbb{K}}$ generado por la única clase de orden 2 de $Cl_{\mathbb{K}}$ es maximal en el conjunto de los subgrupos cíclicos de $Cl_{\mathbb{K}}$.

Capítulo 1

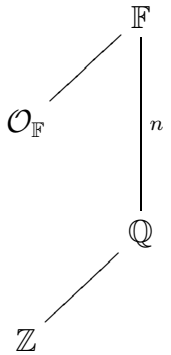
Antecedentes

En este capítulo expondremos sin demostración la teoría necesaria que soportará los siguientes capítulos. Principalmente utilizaremos el libro de Ribenboim [**26**] debido a que ahí podemos encontrar la mayoría de los enunciados que presentamos a continuación. El libro de Ireland y Rosen [**18**] incluye una breve pero muy buena introducción a la teoría de los números algebraicos en el capítulo 12. También vale la pena mencionar el texto de Stewart y Tall [**31**].

A través de este trabajo usaremos las siguientes notaciones: $\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$, $\mathbb{Z}$ denota al anillo de los enteros y $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a los campos de los números racionales, reales y complejos respectivamente. $\left(\frac{a}{p}\right)$ es el símbolo de Legendre de a módulo p, donde $\left(\frac{a}{p}\right) = 0$ si $p \mid a$. Escribiremos $a^n \mid\mid b$ para indicar que $a^n \mid b$ y $a^{n+1} \nmid b$. También $\mathrm{ord}_b\,(a) = n$ indicará que $a^n \mid\mid b$.

1.1. Campos de números

Un elemento $\alpha \in \mathbb{C}$ es un número algebraico si α es raíz de algún $f(x) \in \mathbb{Z}[x]$ y $\mathrm{gr}(f(x)) \geq 1$, donde $\mathrm{gr}(f(x))$ indica el grado de $f(x)$. Si $f(x)$ es mónico, diremos que α es un entero algebraico. Si un campo $\mathbb{F} \subseteq \mathbb{C}$ es tal que $[\mathbb{F} : \mathbb{Q}] = n < \infty$, entonces diremos que $\mathbb{F}$ es un campo de números. En particular, si $\alpha \in \mathbb{F}$, entonces α es un número algebraico. Es fácil probar que el conjunto $\Omega = \{\alpha \in \mathbb{C} : \alpha \text{ es un entero algebraico}\}$ es un anillo. Al anillo $\mathcal{O}_{\mathbb{F}} = \mathbb{F} \cap \Omega$ lo llamaremos el anillo de enteros de $\mathbb{F}$.



Si $\frac{a}{b} \in \mathbb{Q}$ y $f(x) = bx - a$, entonces $f\left(\frac{a}{b}\right) = 0$ y así todo racional es un ńumero algebraico, pero no todo racional es un entero algebraico. Los racionales que son raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$ son precisamente los elementos de $\mathbb{Z}$: el anillo de enteros de $\mathbb{Q}$ es $\mathbb{Z}$. En general, el anillo de enteros de un campo de números juega un papel parecido al que tiene $\mathbb{Z}$ en $\mathbb{Q}$. Estudiaremos en $\mathcal{O}_{\mathbb{F}}$ problemas similares a los que

tenemos en $\mathbb{Z}$: factorización, ideales principales y no principales, unidades y en general, la aritmética del anillo $\mathcal{O}_{\mathbb{F}}$. Para distinguir a los enteros ordinarios de los enteros algebraicos, usaremos la frase "entero racional" para referirnos a los elementos de $\mathbb{Z}$. De la misma forma, un "primo racional" es un elemento primo de $\mathbb{Z}$.

Sean $\mathbb{F}$ un campo de números tal que $[\mathbb{F} : \mathbb{Q}] = n$ y $\mathcal{O}$ un $\mathbb{Z}$-submódulo de $\mathcal{O}_{\mathbb{F}}$. Diremos que $\mathcal{O}$ es un módulo completo si el rango de $\mathcal{O}$ es n. Un módulo completo $\mathcal{O} \subseteq \mathcal{O}_{\mathbb{F}}$ es un orden de $\mathbb{F}$ si además $1 \in \mathcal{O}$.

Si $[\mathbb{F} : \mathbb{Q}] = 2$ diremos que $\mathbb{F}$ es un campo cuadrático. Todo campo cuadrático es de la forma $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, donde d es un entero racional libre de cuadrados. Si $d > 0$, diremos que $\mathbb{F}$ es un campo cuadrático real y si $d < 0$, diremos que $\mathbb{F}$ es un campo cuadrático imaginario.

Proposición 1.1. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d \in \mathbb{Z}$ libre de cuadrados y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros. Entonces*

$$\mathcal{O}_{\mathbb{F}} = \begin{cases} \mathbb{Z} + \sqrt{d}\,\mathbb{Z} & \text{si } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z} + \dfrac{1+\sqrt{d}}{2}\,\mathbb{Z} & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

DEMOSTRACIÓN. Ver [**26**], pag. 97, **V**. □

La proposición anterior nos indica que, si $d \equiv 2, 3 \pmod 4$, entonces los elementos de $\mathcal{O}_{\mathbb{F}}$ son de la forma $a_1 + a_2\sqrt{d}$ con $a_1, a_2 \in \mathbb{Z}$. Por ejemplo, si $d = 3$, entonces $4 - 5\sqrt{3} \in \mathcal{O}_{\mathbb{F}}$, pero $\dfrac{3+\sqrt{3}}{2}$ no es un entero algebraico. Por otro lado, si $d \equiv 1 \pmod 4$, los enteros algebraicos son los elementos de la forma $\dfrac{a_1 + a_2\sqrt{d}}{2}$, tales que $a_1, a_2 \in \mathbb{Z}$ tienen la misma paridad. Observemos que si a_1, a_2 son pares, tenemos los elementos de la forma $a_1 + a_2\sqrt{d}$ con $a_1, a_2 \in \mathbb{Z}$. Como ejemplos, $\dfrac{3+7\sqrt{-5}}{2}$ y $2 + 3\sqrt{-5}$ son enteros algebraicos, pero $\dfrac{1+\sqrt{-5}}{3}$ y $\dfrac{1+2\sqrt{-5}}{2}$ no son enteros algebraicos.

Cuando $d \equiv 1 \pmod 4$, tenemos que $\mathbb{Z} + \sqrt{d}\,\mathbb{Z} \subsetneq \mathcal{O}_{\mathbb{F}}$. De esta forma $\mathbb{Z} + \sqrt{d}\,\mathbb{Z}$ es un orden de $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ pero no es el anillo de enteros. Observemos también que $\mathbb{Z}$ y $\sqrt{d}\,\mathbb{Z}$ no son órdenes de $\mathbb{F}$ pues son $\mathbb{Z}$-módulos de rango 1.

El siguiente resultado resume las principales propiedades de un campo de números y su anillo de enteros:

Proposición 1.2. *Sea $\mathbb{F}$ un campo de números y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros.*

1. *$\mathbb{F}$ es el campo de cocientes de $\mathcal{O}_{\mathbb{F}}$.*
2. *$\mathcal{O}_{\mathbb{F}}$ es un anillo Noetheriano.*
3. *$\mathcal{O}_{\mathbb{F}}$ es un anillo íntegramente cerrado.*
4. *$\mathcal{O}_{\mathbb{F}}$ es un dominio Dedekind.*
5. *Todo ideal distinto de $\langle 0 \rangle$ de $\mathcal{O}_{\mathbb{F}}$ contiene una base de $\mathbb{F}$ como $\mathbb{Q}$ espacio vectorial.*
6. *Para cualquier ideal $\mathfrak{I} \neq \langle 0 \rangle$ de $\mathcal{O}_{\mathbb{F}}$, el anillo $\mathcal{O}_{\mathbb{F}}/\mathfrak{I}$ es finito.*
7. *Todo ideal primo $\mathfrak{p} \neq \langle 0 \rangle$ de $\mathcal{O}_{\mathbb{F}}$ es maximal.*
8. *Todo ideal de $\mathcal{O}_{\mathbb{F}}$ distinto de $\langle 0 \rangle$ se factoriza de forma única como producto de ideales primos.*

9. *Si $\mathfrak{I}$, $\mathfrak{J}$ y $\mathfrak{J}'$ son ideales $\neq \langle 0\rangle$ de $\mathcal{O}_{\mathbb{F}}$, entonces $\mathfrak{I}\,\mathfrak{J} = \mathfrak{I}\,\mathfrak{J}'$ implica $\mathfrak{J} = \mathfrak{J}'$.*
10. *Si $\mathfrak{I}, \mathfrak{J}$ son dos ideales de $\mathcal{O}_{\mathbb{F}}$, entonces $\mathfrak{J} \supseteq \mathfrak{I}$ si y sólo si existe un ideal $\mathfrak{d}$ tal que $\mathfrak{I} = \mathfrak{J}\,\mathfrak{d}$.*

DEMOSTRACIÓN. Ver Capítulo 12 de [**18**]. □

La afirmación 8 de la proposición anterior es una herramienta fundamental en nuestra investigación. Es posible que $\mathcal{O}_{\mathbb{F}}$ no sea un anillo de factorización única, por ejemplo, si $\mathbb{F} = \mathbb{Q}(\sqrt{10})$, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \sqrt{10}\,\mathbb{Z}$. En $\mathcal{O}_{\mathbb{F}}$, 10 se puede factorizar como

$$10 = (2)(5) = \left(\sqrt{10}\right)^2, \tag{2}$$

en donde $2, 5, \sqrt{10}$ son irreducibles no asociados. Esto muestra que $\mathcal{O}_{\mathbb{F}}$ no es un dominio de factorización única. Sin embargo, si en lugar de factorizar los elementos, factorizamos los ideales generados por esos números, siempre obtendremos la misma factorización. Consideremos el ideal $\langle 10\rangle$ y los ideales primos $\mathfrak{p}_2 = \left\langle 2, \sqrt{10}\right\rangle$ y $\mathfrak{p}_5 = \left\langle 5, \sqrt{10}\right\rangle$. Tenemos que

$$\langle 10\rangle = \mathfrak{p}_2^2\,\mathfrak{p}_5^2, \quad \langle 2\rangle = \mathfrak{p}_2^2, \quad \langle 5\rangle = \mathfrak{p}_5^2, \quad \left\langle \sqrt{10}\right\rangle = \mathfrak{p}_2\mathfrak{p}_5.$$

Podemos ver que al considerar los elementos como ideales, las dos factorizaciones de (2) se vuelven una misma:

$$\langle 10\rangle = \mathfrak{p}_2^2\,\mathfrak{p}_5^2 = (\mathfrak{p}_2\,\mathfrak{p}_5)^2.$$

Ésta es una buena razón por la que los ideales son muy importantes para trabajar problemas de factorización en anillos de enteros.

La noción de divisibilidad en $\mathbb{Z}$ la extendemos a ideales de la siguiente forma. Si $\mathfrak{I}, \mathfrak{J}$ son ideales de $\mathcal{O}_{\mathbb{F}}$, diremos que $\mathfrak{J}$ divide a $\mathfrak{I}$ si existe un ideal $\mathfrak{d}$ tal que $\mathfrak{I} = \mathfrak{J}\,\mathfrak{d}$. El inciso 10 de la Proposición 1.2 nos afirma que dividir y contener es lo mismo, es decir, $\mathfrak{J} \mid \mathfrak{I}$ si y sólo si $\mathfrak{J} \supseteq \mathfrak{I}$. El inciso 9 de la Proposición 1.2 es la ley de la cancelación para el producto de ideales.

1.2. Bases enteras

Sea $\mathcal{B} = \{B_1, \ldots, B_n\}$ una base de $\mathbb{F}$ como $\mathbb{Q}$-espacio vectorial. De acuerdo a la Proposición 1.2, todo ideal $\mathfrak{I} \neq \langle 0\rangle$ de $\mathcal{O}_{\mathbb{F}}$ contiene una base de $\mathbb{F}/\mathbb{Q}$, en particular, si $\mathfrak{I} = \mathcal{O}_{\mathbb{F}}$. Por lo anterior, podemos suponer que $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{F}}$. Consideremos la matriz $M = (t(B_i\,B_j))$, donde

$$t(A) = \sum_{i=1}^{n} \sigma_i(A)$$

y σ_i son las distintas inmersiones de $\mathbb{F}$ en $\mathbb{C}$. Definimos el discriminante de una base como $\Delta(\mathcal{B}) = \det(M)$. Si $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{F}}$, entonces $\Delta(\mathcal{B}) \in \mathbb{Z}$. Si $\mathcal{B}$ es una base tal que $|\Delta(\mathcal{B})|$ es mínimo, diremos que $\mathcal{B}$ es un a base entera de $\mathbb{F}$. La propiedad más importante de una base entera es la siguiente:

Teorema 1.3. *Si $\mathcal{B} = \{B_1, \ldots, B_n\}$ es una base entera de $\mathbb{F}$, entonces*

$$\mathcal{O}_{\mathbb{F}} = B_1\,\mathbb{Z} + \cdots + B_n\,\mathbb{Z}.$$

DEMOSTRACIÓN. Ver [**18**], Proposition 12.2.2, pp. 175. □

En el caso de los campos cuadráticos, por la Proposición 1.1 tenemos:

Corolario 1.4. *Sea* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$.

1. *Si* $d \equiv 1 \pmod 4$, *entonces* $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ *es una base entera de* $\mathbb{F}$.
2. *Si* $d \equiv 2, 3 \pmod 4$, *entonces* $\{1, \sqrt{d}\}$ *es una base entera de* $\mathbb{F}$. □

El siguiente resultado nos ayudará a trabajar con bases enteras. La demostración es elemental.

Proposición 1.5. *Sean* $\mathcal{M}$ *un* $\mathbb{Z}$*-módulo libre,* $\mathcal{M}_1$, $\mathcal{M}_2$ *dos* $\mathbb{Z}$*-submódulos de* $\mathcal{M}$ *con bases* $\mathcal{B}_1 = \{B_1, \ldots, B_{n-1}, C_1\}$ *y* $\mathcal{B}_2 = \{B_1, \ldots, B_{n-1}, C_2\}$ *respectivamente. Si* $C_1 - C_2 \in \mathcal{M}_1 \cap \mathcal{M}_2$, *entonces* $\mathcal{M}_1 = \mathcal{M}_2$. □

Lo anterior nos dice que podemos cambiar un generador C_1 de la base $\mathcal{B}_1$ por otro de la forma $C_2 = C_1 + \sum_{i=1}^{n-1} b_i\, B_i$, con $b_i \in \mathbb{Z}$ para todo i. Otro cambio que se puede hacer sin afectar al $\mathbb{Z}$-módulo es cambiarle el signo a un generador.

Ejemplo 1.6. *Consideremos* $\mathcal{M} = \mathbb{Z} + \sqrt[3]{5}\,\mathbb{Z} + \sqrt[3]{25}\,\mathbb{Z}$,

$$\mathcal{M}_1 = (6 + 6\sqrt[3]{5} + 4\sqrt[3]{25})\,\mathbb{Z} + (4 + 9\sqrt[3]{5} + 8\sqrt[3]{25})\,\mathbb{Z} + (8 + 12\sqrt[3]{5} + 10\sqrt[3]{25})\,\mathbb{Z},$$

$$\mathcal{M}_2 = (6 + 6\sqrt[3]{5} + 4\sqrt[3]{25})\,\mathbb{Z} + (4 + 9\sqrt[3]{5} + 8\sqrt[3]{25})\,\mathbb{Z} + (8 - 3\sqrt[3]{5} - 6\sqrt[3]{25})\,\mathbb{Z}.$$

En este ejemplo, $C_1 = 8 + 12\sqrt[3]{5} + 10\sqrt[3]{25}$, $C_2 = 8 - 3\sqrt[3]{5} - 6\sqrt[3]{25}$ *y así tenemos*

$$C_1 - C_2 = 15\sqrt[3]{5} + 16\sqrt[3]{25} = 3(4 + 9\sqrt[3]{5} + 8\sqrt[3]{25}) - 2(6 + 6\sqrt[3]{5} + 4\sqrt[3]{25}) \in \mathcal{M}_1 \cap \mathcal{M}_2.$$

Por lo anterior, $\mathcal{M}_1 = \mathcal{M}_2$.

Continuando con el mismo ejemplo, simplificaremos la representación del $\mathbb{Z}$*-módulo* $\mathcal{M}_1 = \mathcal{M}_2$. *Para esto, usaremos la notación* (a_1, a_2, a_3) *para representar al elemento* $a_1 + a_2\sqrt[3]{5} + a_3\sqrt[3]{25}$. *En el lado derecho de cada renglón vamos a indicar (con números romanos) qué generador estamos cambiando y por cuál:*

$$\begin{array}{rcll}
\mathcal{M}_1 & = & (6,6,4)\,\mathbb{Z} + (4,9,8)\,\mathbb{Z} + (8,12,10)\,\mathbb{Z} & \\
& = & (6,6,4)\,\mathbb{Z} + (4,9,8)\,\mathbb{Z} + (0,-6,-6)\,\mathbb{Z} & \text{III} \to \text{III} - 2\text{II} \\
& = & (2,-3,-4)\,\mathbb{Z} + (4,9,8)\,\mathbb{Z} + (0,6,6)\,\mathbb{Z} & \text{III} \to -\text{III}, \text{I} \to \text{I} - \text{II} \\
& = & (2,-3,-4)\,\mathbb{Z} + (0,15,16)\,\mathbb{Z} + (0,6,6)\,\mathbb{Z} & \text{II} \to \text{II} - 2\text{I} \\
& = & (2,-3,-4)\,\mathbb{Z} + (0,3,4)\,\mathbb{Z} + (0,6,6)\,\mathbb{Z} & \text{II} \to \text{II} - 2\text{III} \\
& = & (2,-3,-4)\,\mathbb{Z} + (0,3,4)\,\mathbb{Z} + (0,0,-2)\,\mathbb{Z} & \text{III} \to \text{III} - 2\text{II} \\
& = & (2,-3,-4)\,\mathbb{Z} + (0,3,0)\,\mathbb{Z} + (0,0,-2)\,\mathbb{Z} & \text{II} \to \text{II} + 2\text{III} \\
& = & (2,0,0)\,\mathbb{Z} + (0,3,0)\,\mathbb{Z} + (0,0,-2)\,\mathbb{Z} & \text{I} \to \text{I} + \text{III} - 2\text{III} \\
& = & (2,0,0)\,\mathbb{Z} + (0,3,0)\,\mathbb{Z} + (0,0,2)\,\mathbb{Z} & \text{III} \to -\text{III},
\end{array}$$

Así que $\mathcal{M}_1 = \mathcal{M}_2 = 2\,\mathbb{Z} + (3\sqrt[3]{5})\,\mathbb{Z} + (2\sqrt[3]{25})\,\mathbb{Z}$.

Los campos de la forma $\mathbb{Q}(\sqrt[n]{d})$ se conocen como campos puros de grado n. De forma más general, las extensiones $\mathbb{K}/\mathbb{F}$ tales que $\mathbb{K} = \mathbb{F}(\sqrt[n_1]{D_1}, \ldots, \sqrt[n_g]{D_g})$ con $D_1, \ldots, D_g \in \mathcal{O}_\mathbb{F}$ se llaman extensiones radicales, en particular, los campos puros sobre $\mathbb{Q}$ son extensiones radicales. De particular interés para nosotros son extensiones de la forma $\mathbb{Q}(\sqrt[4]{d})/\mathbb{Q}$.

Proposición 1.7. *Sean d un entero libre de cuadrados y $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$.*

1. *Si $d \equiv 1 \pmod 8$, entonces $\left\{1, \sqrt[4]{d}, \dfrac{1+\sqrt{d}}{2}, \dfrac{1+\sqrt[4]{d}+\sqrt{d}+\sqrt[4]{d^3}}{4}\right\}$ es una base entera de $\mathbb{K}$.*
2. *Si $d \equiv 5 \pmod 8$, entonces $\left\{1, \sqrt[4]{d}, \dfrac{1+\sqrt{d}}{2}, \dfrac{\sqrt[4]{d}+\sqrt[4]{d^3}}{2}\right\}$ es una base entera de $\mathbb{K}$.*
3. *Si $d \equiv 2, 3 \pmod 4$, entonces una base entera de $\mathbb{K}$ es $\left\{1, \sqrt[4]{d}, \sqrt{d}, \sqrt[4]{d^3}\right\}$.*

DEMOSTRACIÓN. [**10**] Theorem 1, pp. 28. □

1.3. Ideales y ramificación

Los ideales $\neq \langle 0\rangle$ de un anillo de enteros tienen propiedades importantes, por ejemplo la factorización única como producto de ideales primos. Con respecto al número de generadores tenemos que, si $\mathfrak{I}$ es ideal de $\mathcal{O}_\mathbb{F}$ y $\{B_1, \ldots, B_n\} \subseteq \mathfrak{I}$ es tal que $\mathfrak{I} = B_1\,\mathbb{Z} + \cdots + B_n\,\mathbb{Z}$, entonces $\mathfrak{I} = \langle B_1, \ldots, B_n\rangle$. Sin embargo, n no necesariamente es el número óptimo de generadores de $\mathfrak{I}$. Así, tenemos el siguiente resultado:

Teorema 1.8. *Sea $\mathfrak{I} \neq \langle 0\rangle$ ideal de $\mathcal{O}_\mathbb{F}$ y $B \in \mathfrak{I} - \{0\}$. Existe $A \in \mathfrak{I}$ tal que $\mathfrak{I} = \langle A, B\rangle$.*

DEMOSTRACIÓN. Ver [**31**], Theorem 5.20 pp. 121 □

El análogo a la Proposición 1.5 para ideales es el siguiente: si $A_1, A_2, C \in \mathcal{O}_\mathbb{F}$, entonces:

$$\langle A_1, A_2\rangle = \langle A_1, A_2 + C\,A_1\rangle\,.$$

Sea $\mathbb{K}/\mathbb{F}$ una extensión de campos de números. Si $\mathfrak{I}_\mathbb{F}$ es un ideal de $\mathcal{O}_\mathbb{F}$, denotaremos $\langle\mathfrak{I}_\mathbb{F}\rangle_\mathbb{K}$ al ideal $\mathfrak{I}_\mathbb{F}\mathcal{O}_\mathbb{K}$ de $\mathcal{O}_\mathbb{K}$. Si $A_1, A_2 \in \mathcal{O}_\mathbb{F}$, el ideal de $\mathcal{O}_\mathbb{F}$ generado por A_1 y A_2 lo escribiremos como $\langle A_1, A_2\rangle_\mathbb{F}$, mientras que $\langle A_1, A_2\rangle_\mathbb{K}$ representa al ideal de $\mathcal{O}_\mathbb{K}$ generado por los mismos elementos. Al ideal $\langle\mathfrak{I}_\mathbb{F}\rangle_\mathbb{K}$ le llamaremos la extensión de $\mathfrak{I}_\mathbb{F}$ a $\mathcal{O}_\mathbb{K}$ y al ideal $\mathfrak{I}_\mathbb{K} \cap \mathcal{O}_\mathbb{F}$ le llamaremos la restricción de $\mathfrak{I}_\mathbb{K}$ a $\mathcal{O}_\mathbb{F}$. Como es usual, en una extensión de la forma $\mathbb{F}/\mathbb{Q}$, escribiremos $\langle A_1, A_2\rangle$ sin hacer referencia al campo $\mathbb{F}$.

Proposición 1.9. *Sea $\mathbb{F} \subseteq \mathbb{K}$ una extensión de campos de números. Si $\mathfrak{I}_\mathbb{F}$ es un ideal de $\mathcal{O}_\mathbb{F}$, entonces $\langle\mathfrak{I}_\mathbb{F}\rangle_\mathbb{K} \cap \mathcal{O}_\mathbb{F} = \mathfrak{I}_\mathbb{F}$.*

DEMOSTRACIÓN. Ver [**26**], pp. 189, **A**. □

Inversamente, si $\mathfrak{I}_\mathbb{K}$ es un ideal de $\mathcal{O}_\mathbb{K}$, entonces no necesariamente $\langle\mathfrak{I}_\mathbb{K} \cap \mathcal{O}_\mathbb{F}\rangle_\mathbb{K} = \mathfrak{I}_\mathbb{K}$, por ejemplo, si $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ y $\mathbb{F} = \mathbb{Q}$, el ideal $\mathfrak{I}_\mathbb{K} = \langle\sqrt{2}\rangle_\mathbb{K}$ satisface $\mathfrak{I}_\mathbb{F} = \mathfrak{I}_\mathbb{K} \cap \mathcal{O}_\mathbb{F} = \langle 2\rangle_\mathbb{F}$ y $\langle\mathfrak{I}_\mathbb{F}\rangle_\mathbb{K} = \langle 2\rangle_\mathbb{K} \neq \mathfrak{I}_\mathbb{K}$.

Proposición 1.10. *Sean $\mathbb{F} \subseteq \mathbb{K}$ dos campos de números, $\mathcal{O}_\mathbb{F}, \mathcal{O}_\mathbb{K}$ sus anillos de enteros y $\mathfrak{I}_\mathbb{F} = \langle A_1, A_2 \rangle_\mathbb{F}$ un ideal de $\mathcal{O}_\mathbb{F}$ con $A_1, A_2 \in \mathcal{O}_\mathbb{F}$. Entonces $\langle \mathfrak{I}_\mathbb{F} \rangle_\mathbb{K} = \langle A_1, A_2 \rangle_\mathbb{K}$.*

DEMOSTRACIÓN. Tomemos $\alpha \in \langle \mathfrak{I}_\mathbb{F} \rangle_\mathbb{K}$. Entonces,

$$\alpha = \sum_{i=1}^{k} (A_1\beta_{1i} + A_2\beta_{2i})\gamma_i = A_1 \left(\sum_{i=1}^{k} \beta_{1i}\gamma_i \right) + A_2 \left(\sum_{i=1}^{k} \beta_{2i}\gamma_i \right) \in \langle A_1, A_2 \rangle_\mathbb{K}.$$

Así $\langle \mathfrak{I}_\mathbb{K} \rangle_\mathbb{K} \subseteq \langle A_1, A_2 \rangle_\mathbb{K}$. La otra contención se sigue de que $A_1, A_2 \in \langle \mathfrak{I}_\mathbb{F} \rangle_\mathbb{K}$. □

Corolario 1.11. *Sean $\mathbb{F} \subseteq \mathbb{K}$ dos campos de números, $\mathcal{O}_\mathbb{F}, \mathcal{O}_\mathbb{K}$ sus anillos de enteros y $\mathfrak{I}_\mathbb{K}$ un ideal de $\mathcal{O}_\mathbb{K}$ con $\mathfrak{I}_\mathbb{K} = \langle A_1, A_2 \rangle_\mathbb{K}$, donde $A_1, A_2 \in \mathcal{O}_\mathbb{F}$. Entonces $\mathfrak{I}_\mathbb{K} \cap \mathcal{O}_\mathbb{F} = \langle A_1, A_2 \rangle_\mathbb{F}$.*

DEMOSTRACIÓN. Sea $\mathfrak{I}_\mathbb{F} = \langle A_1, A_2 \rangle_\mathbb{F}$. Por la proposición anterior, $\langle \mathfrak{I}_\mathbb{F} \rangle_\mathbb{K} = \mathfrak{I}_\mathbb{K}$ y como $\langle \mathfrak{I}_\mathbb{F} \rangle_\mathbb{K} \cap \mathcal{O}_\mathbb{F} = \mathfrak{I}_\mathbb{F}$, entonces el resultado es cierto. □

1.3.1. Grupo de clases de ideales

Sea $\mathbb{F}$ un campo de números y $\mathcal{O}_\mathbb{F}$ su anillo de enteros. Consideremos el conjunto

$$\{\mathfrak{I} \subseteq \mathcal{O}_\mathbb{F} : \mathfrak{I} \text{ es ideal de } \mathcal{O}_\mathbb{F}, \mathfrak{I} \neq \langle 0 \rangle\}.$$

Los ideales $0 \neq \mathfrak{I}, \mathfrak{J} \subseteq \mathcal{O}_\mathbb{F}$ están relacionados ($\sim$) si existen $A, B \in \mathcal{O}_\mathbb{F} - \{0\}$ tales que $A\,\mathfrak{I} = B\,\mathfrak{J}$. Esta relación es de equivalencia. Denotaremos como $Cl_\mathbb{F}$ al conjunto de las clases de equivalencia de ideales $\neq \langle 0 \rangle$ de $\mathcal{O}_\mathbb{F}$. El conjunto $\overline{\mathfrak{I}} = \{\mathfrak{J} : \mathfrak{J} \sim \mathfrak{I}\}$ es la clase equivalencia de $\mathfrak{I}$. Si $\overline{\mathfrak{I}}, \overline{\mathfrak{J}}$ son dos clases, definimos el producto de forma natural: $\overline{\mathfrak{I}}\,\overline{\mathfrak{J}} = \overline{\mathfrak{I}\,\mathfrak{J}}$. Esta operación está bien definida y $Cl_\mathbb{F}$ es un grupo abeliano finito conocido como el grupo de clases de ideales de $\mathbb{F}$. El neutro del grupo $Cl_\mathbb{F}$ es $\overline{\mathcal{O}_\mathbb{F}} = \{\mathfrak{I} \subseteq \mathcal{O}_\mathbb{F} : \mathfrak{I} \text{ es un ideal principal}\}$. La cardinalidad de $Cl_\mathbb{F}$ se conoce como el número de clases de $\mathbb{F}$ y lo denotaremos como $h_\mathbb{F}$.

Teorema 1.12. *Sea $\mathbb{F}$ un campo de números. El anillo $\mathcal{O}_\mathbb{F}$ es de factorización única si y sólo si $h_\mathbb{F} = 1$.*

DEMOSTRACIÓN. Ver [**31**], pp. 153, Theorem 9.1. □

Ejemplo 1.13. *Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$. Entonces $\mathcal{O}_\mathbb{F} = \mathbb{Z} + \sqrt{10}\,\mathbb{Z}$. Consideremos el ideal*

$$\langle 30 \rangle = \mathfrak{p}_2^2\,\mathfrak{p}_5^2\,\mathfrak{p}_3\,\mathfrak{p}_3',$$

donde $\mathfrak{p}_2 = \langle 2, \sqrt{10} \rangle$, $\mathfrak{p}_5 = \langle 5, \sqrt{10} \rangle$, $\mathfrak{p}_3 = \langle 3, 1 + \sqrt{10} \rangle$ y $\mathfrak{p}_3' = \langle 3, 1 - \sqrt{10} \rangle$. El grupo de clases de ideales de $\mathbb{F}$ es $Cl_\mathbb{F} = \{\overline{\mathcal{O}_\mathbb{F}}, \overline{\mathfrak{p}_2}\} \cong \mathbb{Z}/2\mathbb{Z}$, donde $\overline{\mathcal{O}_\mathbb{F}} = \{\mathfrak{I} \subseteq \mathcal{O}_\mathbb{F} : \mathfrak{I}$ es un ideal principal $\neq \langle 0 \rangle\}$ y $\overline{\mathfrak{p}_2} = \{\mathfrak{I} \subseteq \mathcal{O}_\mathbb{F} : \mathfrak{I}$ es un ideal no principal$\}$. Lo anterior nos indica que el producto de dos ideales no principales es un ideal principal. Usaremos esta información para encontrar todas las posibles factorizaciones de 30. El ideal $\langle 30 \rangle$ tiene seis divisores primos, todos ellos son no principales. Así, para encontrar todas las factorizaciones de 30 debemos separar los factores en parejas. En la siguiente tabla proporcionamos todas las posibilidades. Las primeras tres columnas muestran las parejas y las últimas tres columnas contienen un generador de cada uno de los ideales de las primeras columnas, tal que al multiplicarlos dan las seis factorizaciones distintas en irreducibles de 30.

$\mathfrak{p}_2^2$	$\mathfrak{p}_5^2$	$\mathfrak{p}_3\,\mathfrak{p}_3'$	2	5	3
$\mathfrak{p}_2^2$	$\mathfrak{p}_5\,\mathfrak{p}_3$	$\mathfrak{p}_5\,\mathfrak{p}_3'$	2	$-5+\sqrt{10}$	$-5-\sqrt{10}$
$\mathfrak{p}_2\,\mathfrak{p}_5$	$\mathfrak{p}_2\,\mathfrak{p}_5$	$\mathfrak{p}_3\,\mathfrak{p}_3'$	$\sqrt{10}$	$\sqrt{10}$	3
$\mathfrak{p}_2\,\mathfrak{p}_5$	$\mathfrak{p}_2\,\mathfrak{p}_3$	$\mathfrak{p}_5\,\mathfrak{p}_3'$	$\sqrt{10}$	$2-\sqrt{10}$	$-5-\sqrt{10}$
$\mathfrak{p}_2\,\mathfrak{p}_5$	$\mathfrak{p}_2\,\mathfrak{p}_3'$	$\mathfrak{p}_5\,\mathfrak{p}_3$	$\sqrt{10}$	$-2-\sqrt{10}$	$-5+\sqrt{10}$
$\mathfrak{p}_2\,\mathfrak{p}_3$	$\mathfrak{p}_2\,\mathfrak{p}_3'$	$\mathfrak{p}_5^2$	$2-\sqrt{10}$	$-2-\sqrt{10}$	5

Por ejemplo, del primer renglón tenemos $(\mathfrak{p}_2^2)(\mathfrak{p}_5^2)(\mathfrak{p}_3\,\mathfrak{p}_3') = \langle 2\rangle\,\langle 5\rangle\,\langle 3\rangle$. *Así que:*

$$\begin{aligned} 30 &= (2)(5)(3) \\ &= (2)(-5+\sqrt{10})(-5-\sqrt{10}) \\ &= (\sqrt{10})^2(3) \\ &= (\sqrt{10})(2-\sqrt{10})(-5-\sqrt{10}) \\ &= (\sqrt{10})(-2-\sqrt{10})(-5+\sqrt{10}) \\ &= (2-\sqrt{10})(-2-\sqrt{10})(5) \end{aligned}$$

1.3.2. Ramificación

Sea $\mathbb{K}/\mathbb{F}$ una extensión de campos de números. Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_\mathbb{F}$, el ideal $\langle\mathfrak{p}\rangle_\mathbb{K}$ se factoriza como producto de ideales primos de $\mathcal{O}_\mathbb{K}$, digamos:

$$\langle\mathfrak{p}\rangle_\mathbb{K} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}, \tag{3}$$

donde cada $\mathfrak{q}_i$ es un ideal primo de $\mathcal{O}_\mathbb{K}$ y $e_i \in \mathbb{N}$. Un ideal primo $\mathfrak{q} \subseteq \mathcal{O}_\mathbb{K}$ cumple $\mathfrak{q}\cap\mathcal{O}_\mathbb{F} = \mathfrak{p}$ si y sólo si $\mathfrak{q} = \mathfrak{q}_i$ para algún $1 \leq i \leq g$. El valor e_i se llama el índice de ramificación de $\mathfrak{q}_i$ en $\mathbb{K}/\mathbb{F}$, o bien, el índice de ramificación de $\mathfrak{q}_i$ sobre $\mathfrak{p}$. Sabemos que $\mathcal{O}_\mathbb{K}/\mathfrak{q}_i$ y $\mathcal{O}_\mathbb{F}/\mathfrak{p}$ son campos finitos, de hecho, existe un monomorfismo de campos $\mathcal{O}_\mathbb{F}/\mathfrak{p} \hookrightarrow \mathcal{O}_\mathbb{K}/\mathfrak{q}_i$ y el número $f_i = [\mathcal{O}_\mathbb{K}/\mathfrak{q}_i : \mathcal{O}_\mathbb{F}/\mathfrak{p}]$ lo llamaremos el grado de inercia de $\mathfrak{q}_i$ sobre $\mathfrak{p}$. Al número g le llamaremos el grado de descomposición de $\mathfrak{p}$ en $\mathbb{K}/\mathbb{F}$.

Si $n = [\mathbb{K} : \mathbb{F}]$, entonces $n = \sum_{i=1}^{g} e_i f_i$ ([**26**], pp. 193, **G**). Si $\mathbb{K}/\mathbb{F}$ es Galois, entonces $e = e_1 = \cdots = e_g$, $f = f_1 = \cdots = f_g$ y $n = efg$ ([**26**], pp. 192, **F**).

Consideremos la factorización dada en (3). Un ideal $\mathfrak{p} \subseteq \mathcal{O}_\mathbb{F}$ se ramifica si $e_i \neq 1$ para algún $1 \leq i \leq g$ y $\mathfrak{p}$ es no ramificado si $e_1 = \cdots = e_g = 1$. Si $g = 1$ y $e_1 = n$ diremos que el primo $\mathfrak{p}$ se ramifica totalmente, si $g > 1$ entonces $\mathfrak{p}$ se descompone. Si $g = n$ diremos que $\mathfrak{p}$ se descompone totalmente y si $g = 1$ y $e_1 = 1$ entonces diremos que $\mathfrak{p}$ es inerte, . En este último caso el primo $\mathfrak{p}$ sigue siendo primo al extenderlo a $\mathcal{O}_\mathbb{K}$.

Ejemplo 1.14. *Sea* $\mathbb{K} = \mathbb{Q}(\sqrt{3},\sqrt{7})$. *Para los siguientes primos racionales, los ideales* $\langle p\rangle_\mathbb{K}$ *de* $\mathcal{O}_\mathbb{K}$ *se factorizan de la forma en que se indica a continuación.*

p	*Factorización*	*Tipo de ramificación*
2	$\mathfrak{p}^2$	*Se ramifica*
3	$\mathfrak{p}_1^2\mathfrak{p}_2^2$	*Se ramifica y se descompone*
5	$\mathfrak{p}_1\mathfrak{p}_2$	*Se descompone*
7	$\mathfrak{p}^2$	*Se ramifica*
37	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	*Se descompone totalmente*

Notemos que ninguno de estos primos se ramifica totalmente.

Ejemplo 1.15. *Ahora consideremos* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{3})$*, en este caso:*

p	*Factorización*	*Tipo de ramificación*
2	$\mathfrak{p}^4$	*Se ramifica totalmente*
3	$\mathfrak{p}^4$	*Se ramifica totalmente*
5	$\mathfrak{p}$	*Es inerte*
7	$\mathfrak{p}_1\mathfrak{p}_2$	*Se descompone*
11	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	*Se descompone*
13	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	*Se descompone totalmente*

Más adelante regresaremos a los dos ejemplos anteriores.

Proposición 1.16. *Sean* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$*,* d *libre de cuadrados y* $p \in \mathbb{Z}$ *un primo impar.*

1. *Si* $p \mid d$*, entonces* $\langle p\rangle = \left\langle p, \sqrt{d}\right\rangle^2$*, con* $\left\langle p, \sqrt{d}\right\rangle$ *un ideal primo.*
2. *Si* $p \nmid d$ *y existe* $a \in \mathbb{Z}$ *tal que* $a^2 \equiv d \pmod{p}$*, entonces*
$$\langle p\rangle = \left\langle p, a + \sqrt{10}\right\rangle \left\langle p, a - \sqrt{10}\right\rangle.$$
Los ideales $\left\langle p, a + \sqrt{10}\right\rangle$ *y* $\left\langle p, a - \sqrt{10}\right\rangle$ *son primos.*
3. *Si* $p \nmid d$ *y no existe* $a \in \mathbb{Z}$ *tal que* $a^2 \equiv d \pmod{p}$*, entonces* p *es inerte y* $\langle p\rangle$ *es primo.*

DEMOSTRACIÓN. Ver [**26**], 199, **K**. □

Resumiendo, si p es un primo impar, entonces: p se ramifica (totalmente) si y sólo si $p \mid d$, p se descompone (totalmente) si $\left(\frac{d}{p}\right) = 1$ y p es inerte si $\left(\frac{d}{p}\right) = -1$.

Proposición 1.17. *Sean* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$*,* d *libre de cuadrados.*

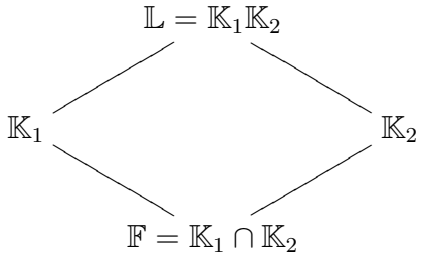
1. $\langle 2\rangle = \left\langle 2, \sqrt{d}\right\rangle^2$ *si* $d \equiv 2 \pmod{4}$.

2. $\langle 2\rangle = \left\langle 2, 1+\sqrt{d}\right\rangle^2$ *si* $d \equiv 3 \pmod 4$.
3. $\langle 2\rangle$ *es primo si* $d \equiv 5 \pmod 8$.
4. $\langle 2\rangle = \left\langle 2, 1+\sqrt{d}\right\rangle \left\langle 2, 1-\sqrt{d}\right\rangle$ *si* $d \equiv 1 \pmod 8$.

DEMOSTRACIÓN. Ver [**26**], pp. 200, **L**. □

El resultado anterior nos indica que 2 se ramifica (totalmente) si $d \equiv 2, 3 \pmod 4$, 2 es inerte si $d \equiv 5 \pmod 8$ y 2 se descompone (totalmente) si $d \equiv 1 \pmod 8$.

Proposición 1.18. *Sean* $\mathbb{L}/\mathbb{F}$, $\mathbb{K}_1/\mathbb{F}$ *y* $\mathbb{K}_2/\mathbb{F}$ *extensiones de Galois de campos de números tales que* $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{F}$ *y* $\mathbb{K}_1\mathbb{K}_2 = \mathbb{L}$. *Sean* $\mathfrak{p}_\mathbb{F}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_\mathbb{L}$ *ideales primos en los anillos de enteros de* $\mathbb{F}, \mathbb{K}_1, \mathbb{K}_2, \mathbb{L}$ *respectivamente, tales que* $\mathfrak{p}_\mathbb{F} = \mathfrak{p}_\mathbb{L} \cap \mathbb{F} = \mathfrak{p}_1 \cap \mathbb{F} = \mathfrak{p}_2 \cap \mathbb{F}$, $\mathfrak{p}_1 = \mathfrak{p}_\mathbb{L} \cap \mathbb{K}_1$ *y* $\mathfrak{p}_2 = \mathfrak{p}_\mathbb{L} \cap \mathbb{K}_2$. *Sean* $\mathfrak{q}_1, \mathfrak{q}_2 \in \{\mathfrak{p}_\mathbb{F}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_\mathbb{L}\}$ *tales que* $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$. *Denotaremos por:* $e(\mathfrak{q}_1/\mathfrak{q}_2)$ *al índice de ramificación de* $\mathfrak{q}_1$ *sobre* $\mathfrak{q}_2$, $f(\mathfrak{q}_1/\mathfrak{q}_2)$ *al grado de inercia de* $\mathfrak{q}_1$ *sobre* $\mathfrak{q}_2$ *y* $g_{\mathbb{K}_1}(\mathfrak{p}_\mathbb{F}), g_{\mathbb{K}_2}(\mathfrak{p}_\mathbb{F}), g_\mathbb{L}(\mathfrak{p}_\mathbb{F})$ *los índices de descomposición de los ideales indicados en el campo dado.*



Entonces:

1. $g_\mathbb{L}(\mathfrak{p}_\mathbb{F}) = g_{\mathbb{K}_1}(\mathfrak{p}_\mathbb{F}) g_{\mathbb{K}_2}(\mathfrak{p}_\mathbb{F})$.
2. $f(\mathfrak{p}_\mathbb{L}/\mathfrak{p}_\mathbb{F}) = f(\mathfrak{p}_{\mathbb{K}_1}/\mathfrak{p}_\mathbb{F}) f(\mathfrak{p}_{\mathbb{K}_2}/\mathfrak{p}_\mathbb{F})$.
3. $e(\mathfrak{p}_\mathbb{L}/\mathfrak{p}_\mathbb{F}) = e(\mathfrak{p}_{\mathbb{K}_1}/\mathfrak{p}_\mathbb{F}) e(\mathfrak{p}_{\mathbb{K}_2}/\mathfrak{p}_\mathbb{F})$.

DEMOSTRACIÓN. Para las afirmaciones 1 y 2, ver [**26**], pp. 263, **E**. La afirmación 3 se sigue de las afirmaciones 1 y 2 y Teoría de Galois. □

La Teoría de Galois nos enseña que dada una extensión de campos de números $\mathbb{K}/\mathbb{F}$ de grado n, existen n inmersiones distintas $\sigma_1, \ldots, \sigma_n$,

$$\sigma_i : \mathbb{K} \hookrightarrow \mathbb{C}$$

tales que $\sigma_i\big|_\mathbb{F} = id_\mathbb{F}$. Convenimos que $\sigma_1 = id_\mathbb{K}$. Si $\sigma(\mathbb{K}) \subseteq \mathbb{R}$, diremos que σ es una inmersión real. Si $\sigma(\mathbb{K}) \not\subseteq \mathbb{R}$, diremos que σ es una inmersión imaginaria. Para $\alpha \in \mathbb{K}$, definimos los conjugados de α como $\sigma_1(\alpha) = \alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$. En particular, si $\mathbb{K}$ es un campo cuadrático y $\mathbb{F} = \mathbb{Q}$, entonces $\sigma_2(a_1 + a_2\sqrt{d}) = a_1 - a_2\sqrt{d}$. En este caso, si $\alpha = a_1 + a_2\sqrt{d} \in \mathbb{K}$, los conjugados de α son α y $a_1 - a_2\sqrt{d}$ y escribiremos $\overline{\alpha} = a_1 - a_2\sqrt{d}$.

Si $\mathbb{K}/\mathbb{F}$ una extensión de campos de números de grado n, a cada inmersión real σ de $\mathbb{K}$ que fija a $\mathbb{F}$ le asociamos un objeto llamado primo al infinito el cual denotaremos como $\mathfrak{p}_\sigma$. Si σ es una inmersión imaginaria, entonces a σ le corresponde una inmersión conjugada $\overline{\sigma}$. Al par $(\sigma, \overline{\sigma})$ le asociamos el primo al infinito $\mathfrak{p}_\sigma$. Recordemos que por cada inmersión $\sigma : \mathbb{F} \hookrightarrow \mathbb{C}$, existen n inmersiones $\sigma_1, \ldots, \sigma_n : \mathbb{K} \hookrightarrow \mathbb{C}$ que extienden a σ. Diremos que $\mathfrak{p}_\sigma$ se ramifica en $\mathbb{K}/\mathbb{F}$ si $\mathfrak{p}_\sigma$ es un primo al infinito real y, para al menos un $1 \leq i \leq n$, $\mathfrak{p}_{\sigma_i}$ es un primo al infinito imaginario. En cualquier otro caso, $\mathfrak{p}_\sigma$ es un primo no ramificado.

Cuando ningún primo, finito o infinito, se ramifica en $\mathbb{K}/\mathbb{F}$, diremos que $\mathbb{K}/\mathbb{F}$ es una extensión no ramificada. Si algún primo, finito o infinito, se ramifica, diremos que $\mathbb{K}/\mathbb{F}$ es una extensión ramificada. Si $\mathbb{F}$ es un campo de números, definimos el campo de clases de Hilbert de $\mathbb{F}$ como la máxima extensión abeliana no ramificada de $\mathbb{F}$ y la denotaremos $\mathbb{H}_{\mathbb{F}}$.

Teorema 1.19. *Sea $\mathbb{F}$ un campo de números y $\mathbb{H}_{\mathbb{F}}$ su campo de clases de Hilbert. Si G es el grupo de Galois de $\mathbb{H}_{\mathbb{F}}/\mathbb{F}$, entonces $G \cong Cl_{\mathbb{F}}$ y $h_{\mathbb{F}} = [\mathbb{H}_{\mathbb{F}} : \mathbb{F}]$.*

DEMOSTRACIÓN. Ver [**7**], pp. 61, 135, Isomorphism Theorem. Otra opción es [**19**], pp. 228, Theorem 12.1. □

Una de las propiedades más importantes del campo de clases de Hilbert es que cualquier ideal $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ al ser extendido al anillo de enteros de $\mathbb{H}_{\mathbb{F}}$, $\langle \mathfrak{I}_{\mathbb{F}} \rangle_{\mathbb{H}_{\mathbb{F}}}$ es principal. A esto se le conoce como capitulación.

Ejemplo 1.20. *Sea $\mathbb{F} = \mathbb{Q}(\sqrt{17}, \sqrt{-1})$. Entonces $\mathbb{H}_{\mathbb{F}} = \mathbb{F}(\sqrt{4+\sqrt{17}})$. Se tiene que $[\mathbb{F} : \mathbb{Q}] = 4$ y $[\mathbb{H}_{\mathbb{F}} : \mathbb{Q}] = 8$, por lo que $h_{\mathbb{F}} = 2$. Sabemos que todo ideal de $\mathcal{O}_{\mathbb{F}}$ extendido a $\mathcal{O}_{\mathbb{H}_{\mathbb{F}}}$ es principal. El ideal*

$$\mathfrak{I}_{\mathbb{F}} = \left\langle 2, \frac{2 - \sqrt{-17} - \sqrt{-1}}{2} \right\rangle_{\mathbb{F}}$$

no es principal, pero

$$\langle \mathfrak{I}_{\mathbb{F}} \rangle_{\mathbb{H}_{\mathbb{F}}} = \left\langle \frac{-3 - \sqrt{17} - 5\sqrt{-1}\sqrt{4+\sqrt{17}} + \sqrt{-17}\sqrt{4+\sqrt{17}}}{4} \right\rangle_{\mathbb{H}_{\mathbb{F}}}.$$

1.4. Norma y traza

Dada una extensión de campos de números $\mathbb{K}/\mathbb{F}$ de grado n y $\alpha \in \mathbb{K}$, la traza relativa de α en $\mathbb{K}/\mathbb{F}$ la definimos como

$$t_{\mathbb{K}/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

donde σ_i son las n inmersiones de $\mathbb{K} \hookrightarrow \mathbb{C}$ que fijan a $\mathbb{F}$ y la norma relativa de α en $\mathbb{K}/\mathbb{F}$ es

$$N_{\mathbb{K}/\mathbb{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Cuando la extensión en la que estemos trabajando sea clara, usaremos los símbolos $t(\alpha)$ y $N(\alpha)$. Si $\mathbb{F} = \mathbb{Q}$, entonces las funciones anteriores se llaman traza absoluta de α en $\mathbb{K}$ y norma absoluta de α en $\mathbb{K}$. La siguiente proposición muestra algunas propiedades importantes de la norma y la traza.

Proposición 1.21. *Sean $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ una torre de campos de números, $n = [\mathbb{K} : \mathbb{F}]$, $\alpha \in \mathbb{L}$, $\beta, \beta_1, \beta_2 \in \mathbb{K}$ y $A \in \mathbb{F}$.*

1. $N_{\mathbb{K}/\mathbb{F}}(\beta), t_{\mathbb{K}/\mathbb{F}}(\beta) \in \mathbb{F}$.
2. *Si* $\beta \in \mathcal{O}_{\mathbb{K}}$, $N_{\mathbb{K}/\mathbb{F}}(\beta), t_{\mathbb{K}/\mathbb{F}}(\beta) \in \mathcal{O}_{\mathbb{F}}$.
3. $N_{\mathbb{K}/\mathbb{F}}(A) = A^n$.
4. $t_{\mathbb{K}/\mathbb{F}}(A) = n\,A$.

5. $N_{\mathbb{K}/\mathbb{F}}(\beta_1\,\beta_2) = N_{\mathbb{K}/\mathbb{F}}(\beta_1)N_{\mathbb{K}/\mathbb{F}}(\beta_2)$.
6. $t_{\mathbb{K}/\mathbb{F}}(\beta_1+\beta_2) = t_{\mathbb{K}/\mathbb{F}}(\beta_1) + t_{\mathbb{K}/\mathbb{F}}(\beta_2)$.
7. $N_{\mathbb{L}/\mathbb{F}}(\alpha) = N_{\mathbb{K}/\mathbb{F}}\big(N_{\mathbb{L}/\mathbb{K}}(\alpha)\big) = N_{\mathbb{K}/\mathbb{F}} \circ N_{\mathbb{L}/\mathbb{K}}(\alpha)$.
8. $t_{\mathbb{L}/\mathbb{F}}(\alpha) = t_{\mathbb{K}/\mathbb{F}}(t_{\mathbb{L}/\mathbb{K}}(\alpha)) = t_{\mathbb{K}/\mathbb{F}} \circ t_{\mathbb{L}/\mathbb{K}}(\alpha)$.

DEMOSTRACIÓN. Ver [**26**], pp. 20 y [**25**], pp. 48, Proposition 2.4. □

Si $\mathbb{F}$ es un campo cuadrático y $A = a_1 + a_2\sqrt{d} \in \mathbb{F}$, entonces

$$N_{\mathbb{F}/\mathbb{Q}}(A) = (a_1 + a_2\sqrt{d})(a_1 - a_2\sqrt{d}) = a_1^2 - d\,a_2^2,$$

$$t_{\mathbb{F}/\mathbb{Q}}A = (a_1 + a_2\sqrt{d}) + (a_1 - a_2\sqrt{d}) = 2\,a_1.$$

De hecho, $f(x) = x^2 - t(A)x + N(A)$ es un polinomio tal que $f(A) = 0$ y, si $a_2 \neq 0$, entonces $f(x) = \mathrm{Irr}(A, \mathbb{Q})$ es el polinomio irreducible de A con coeficientes en $\mathbb{Q}$, más aún, por ser A un entero algebraico, los coeficientes de $f(x)$ están en $\mathbb{Z}$. Por ejemplo, si $A = 4 + 5\sqrt{17} \in \mathbb{Q}(\sqrt{17})$, entonces

$$N_{\mathbb{F}/\mathbb{Q}}(A) = 4^2 - 17(5)^2 = -409, \quad t_{\mathbb{F}/\mathbb{Q}}(A) = 2(4) = 8, \quad \mathrm{Irr}(A, \mathbb{Q}) = x^2 - 8\,x - 409.$$

De acuerdo a la afirmación 6 de la Proposición 1.2, para cualquier ideal $\mathfrak{I}$ de $\mathcal{O}_{\mathbb{F}}$, $|\mathcal{O}_{\mathbb{F}}/\mathfrak{I}| = m < \infty$. Definimos la norma de $\mathfrak{I}$ como $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) = m$. La afirmación 4 de la siguiente proposición es la razón por la que es práctico usar la misma notación para la norma de un número y para la norma de un ideal. La norma de un ideal será útil para estudiar propiedades de divisibilidad.

Proposición 1.22. *Sean $\mathbb{F}$ un campo de números, $A, A_1, A_2 \in \mathcal{O}_{\mathbb{F}}$ y $\mathfrak{I}, \mathfrak{J} \subseteq \mathcal{O}_{\mathbb{F}}$ ideales:*

1. $N_{\mathbb{F}/\mathbb{Q}}(\mathcal{O}_{\mathbb{F}}) = 1$.
2. $N_{\mathbb{F}/\mathbb{Q}}(\langle 0\rangle) = 0$.
3. $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}\,\mathfrak{J}) = N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I})N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{J})$.
4. *Si* $\mathfrak{I} \mid \mathfrak{J}$, *entonces* $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) \mid N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{J})$.
5. $N_{\mathbb{F}/\mathbb{Q}}(\langle A\rangle) = |N_{\mathbb{F}/\mathbb{Q}}(A)|$.
6. *Si* $A \in \mathfrak{I}$, *entonces* $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) \mid N_{\mathbb{F}/\mathbb{Q}}(A)$.
7. *Si* $\mathfrak{I} = \langle A_1, A_2\rangle$, *entonces* $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) \mid \mathrm{m.c.d.}\big(N_{\mathbb{F}/\mathbb{Q}}(A_1), N_{\mathbb{F}/\mathbb{Q}}(A_2)\big)$.

DEMOSTRACIÓN. Las afirmaciones 1 y 2 son consecuencia directa de las definiciones. Para la afirmación 3, ver [**26**], pp. 142, **D**. La afirmación 4 es consecuencia directa de 3. Para la afirmación 5 ver [**31**], pp. 116, Corollary 5.10. La afirmación 6 es consecuencia directa de 5. La afirmación 7 se sigue de las afirmaciones 4, 5 y 6. □

Sean $\mathbb{K}/\mathbb{F}$ una extensión de campos de números, $\mathfrak{q}$ un ideal primo de $\mathcal{O}_{\mathbb{K}}$ y $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_{\mathbb{F}}$. Si $f = [\mathcal{O}_{\mathbb{K}}/\mathfrak{q} : \mathcal{O}_{\mathbb{F}}/\mathfrak{p}]$ es el grado de inercia de $\mathfrak{q}$ sobre $\mathfrak{p}$, definimos el ideal

$$N_{\mathbb{K}/\mathbb{F}}(\mathfrak{q}) = \mathfrak{p}^f.$$

Si $\mathfrak{I}_{\mathbb{K}} = \prod_{i=1}^{k} \mathfrak{q}_i^{e_i}$, entonces $N_{\mathbb{K}/\mathbb{F}}(\mathfrak{I}_{\mathbb{K}}) = \prod_{i=1}^{k} N_{\mathbb{K}/\mathbb{F}}(\mathfrak{q}_i)^{e_i}$ es un ideal en $\mathcal{O}_{\mathbb{F}}$ al cual llamaremos la norma relativa de $\mathfrak{I}_{\mathbb{K}}$ en $\mathbb{K}/\mathbb{F}$. En particular, si $\mathbb{F} = \mathbb{Q}$, lo anterior coincide con la definición de norma de un ideal.

Proposición 1.23. *Sean $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ campos de números con $[\mathbb{K} : \mathbb{F}] = n$, $\mathcal{O}_{\mathbb{F}}, \mathcal{O}_{\mathbb{K}}, \mathcal{O}_{\mathbb{L}}$ sus anillos de enteros.*

1. *Si* $\mathfrak{I}_{\mathbb{F}}$ *es un ideal de* $\mathcal{O}_{\mathbb{F}}$*, entonces* $N_{\mathbb{K}/\mathbb{F}}\left(\langle\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}}\right) = \mathfrak{I}_{\mathbb{F}}{}^{n}$.
2. *Si* $\mathfrak{I}_{\mathbb{L}}$ *es un ideal de* $\mathcal{O}_{\mathbb{L}}$*, entonces* $N_{\mathbb{L}/\mathbb{F}}(\mathfrak{I}_{\mathbb{L}}) = N_{\mathbb{K}/\mathbb{F}}\left(N_{\mathbb{L}/\mathbb{K}}(\mathfrak{I}_{\mathbb{L}})\right)$.
3. $N_{\mathbb{K}/\mathbb{F}}\left(\langle\alpha\rangle_{\mathbb{K}}\right) = \left\langle N_{\mathbb{K}/\mathbb{F}}\left(\alpha\right)\right\rangle_{\mathbb{F}}$.

DEMOSTRACIÓN. Ver [**26**], pp. 235-236, **C**, **D** y **F**. □

1.5. Unidades

Sea $\mathbb{F}$ un campo de números. Escribiremos $\mathcal{U}_{\mathbb{F}}$ para denotar al grupo de unidades del anillo de enteros $\mathcal{O}_{\mathbb{F}}$. El Teorema de las Unidades de Dirichlet describe la estructura de $\mathcal{U}_{\mathbb{F}}$.

Teorema 1.24. (Teorema de las Unidades de Dirichlet) *Sea* $\mathbb{F}$ *un campo de números con* $[\mathbb{F} : \mathbb{Q}] = n = s + 2t$*, donde* s *denota el número de inmersiones reales de* $\mathbb{F}$ *en* $\mathbb{R}$ *y* $2t$ *es el número de inmersiones imaginarias de* $\mathbb{F}$ *en* $\mathbb{C}$*. Entonces*

$$\mathcal{U}_{\mathbb{F}} \cong W \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

donde W *el grupo de las raíces* k*-ésimas de la unidad para algún* $k \in \mathbb{N}$ *y en la descomposición hay* $s + t - 1$ *copias de* $\mathbb{Z}$*.*

DEMOSTRACIÓN. Ver [**31**], pp. 300, Theorem B.6. □

En particular, si $\mathbb{F}$ es un campo cuadrático real, entonces $s = 2$ y $t = 0$. En este caso $\mathcal{U}_{\mathbb{F}} \cong \{1, -1\} \times \mathbb{Z}$. Si $\mathbb{F}$ es un campo cuadrático imaginario, $s = 0, t = 1$ y $\mathcal{U}_{\mathbb{F}} = \{1, -1\}$ a menos que $d = -1$, en cuyo caso $\mathcal{U}_{\mathbb{F}} = \{1, -1, i, -i\}$ y si $d = -3$, entonces $\mathcal{U}_{\mathbb{F}} = \left\{1, -1, \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}\right\}$. Si $\mathbb{F} = \mathbb{Q}(\sqrt[4]{d})$ con $d > 0$, entonces $s = 2, t = 1$ y $\mathcal{U}_{\mathbb{F}} = \{1, -1\} \times \mathbb{Z}^2$.

En el caso cuadrático real, $\mathcal{U}_{\mathbb{F}}$ contiene una elemento de interés particular para nosotros, conocido como la unidad fundamental de $\mathbb{F}$. El siguiente resultado describe algunas de sus propiedades.

Proposición 1.25. *Sea* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *con* $d > 0$ *libre de cuadrados. Existe* $U_{\mathbb{F}} \in \mathcal{U}_{\mathbb{F}}$ *tal que si* $U \in \mathcal{U}_{\mathbb{F}}$*, entonces* $U = \pm U_{\mathbb{F}}^{k}$*, para algún* $k \in \mathbb{Z}$*.* □

Recordemos que si $\langle A\rangle = \langle B\rangle$ son dos ideales principales de un anillo de enteros $\mathcal{O}_{\mathbb{F}}$, entonces $A = u\,B$ para algún $u \in \mathcal{U}_{\mathbb{F}}$ y que, para cualquier $u \in \mathcal{U}_{\mathbb{F}}$, $\langle A\rangle = \langle u\,A\rangle$.

1.6. Discriminante

Sea $\mathbb{F}$ un campo de números, $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros y $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{F}}$ una base de $\mathbb{F}/\mathbb{Q}$. Sabemos que $\mathcal{B}$ es una base entera de $\mathbb{F}$ si $|\Delta(\mathcal{B})|$ es mínimo. Definimos el discriminante de $\mathbb{F}$ como el valor $\delta_{\mathbb{F}} = \Delta(\mathcal{B})$, donde $\mathcal{B}$ es una base entera.

Sea $\mathbb{K}/\mathbb{F}$ una extensión de campos de números y $\mathcal{B}$ una base de $\mathbb{K}$ como $\mathbb{F}$-espacio vectorial. Definimos el discriminante relativo $\delta_{\mathbb{K}/\mathbb{F}}$ de $\mathbb{K}/\mathbb{F}$ como el ideal

$$\delta_{\mathbb{K}/\mathbb{F}} = \left\langle \Delta(\mathcal{B}) : \mathcal{B} \subseteq \mathcal{O}_{\mathbb{K}} \text{ es una base de } \mathbb{K} \text{ como } \mathbb{F}\text{-espacio vectorial}\right\rangle_{\mathbb{F}}.$$

Proposición 1.26. *Sean $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ campos de números. Entonces*

$$\delta_{\mathbb{L}/\mathbb{F}} = (\delta_{\mathbb{K}/\mathbb{F}})^{[\mathbb{L}:\mathbb{K}]} \cdot N_{\mathbb{K}/\mathbb{F}}(\delta_{\mathbb{L}/\mathbb{K}}).$$

DEMOSTRACIÓN. Ver [**26**], pp. 249, **Q**. □

Observemos que en la igualdad de la proposición anterior todos los factores son ideales de $\mathcal{O}_{\mathbb{F}}$, en particular, $N_{\mathbb{K}/\mathbb{F}}(\delta_{\mathbb{L}/\mathbb{K}}) \subseteq \mathcal{O}_{\mathbb{F}}$ pues la norma $N_{\mathbb{K}/\mathbb{F}}$ de un ideal de $\mathcal{O}_{\mathbb{K}}$ está en $\mathcal{O}_{\mathbb{F}}$.

El discriminante es un concepto importante que, entre otras cosas, nos indica cuáles son los ideales que se ramifican en una extensión.

Proposición 1.27. *Sea $\mathbb{K}/\mathbb{F}$ una extensión de campos de números con anillos de enteros $\mathcal{O}_{\mathbb{F}}$ y $\mathcal{O}_{\mathbb{K}}$ respectivamente. Entonces:*

1. *Si $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{K}}$ es una base de $\mathbb{K}/\mathbb{F}$, $\mathcal{B}$ es una base de $\mathcal{O}_{\mathbb{K}}$ como $\mathcal{O}_{\mathbb{F}}$-módulo si y sólo si $\delta_{\mathbb{K}/\mathbb{F}} = \langle \Delta(\mathcal{B}) \rangle_{\mathbb{F}}$.*
2. *Un ideal primo $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{F}}$ se ramifica en $\mathbb{K}/\mathbb{F}$ si y sólo si $\mathfrak{p} \mid \delta_{\mathbb{K}/\mathbb{F}}$.*

DEMOSTRACIÓN. Ver [**26**], pp. 237, **G** y Theorem 1. □

La siguiente proposición nos da el discriminante de una base de potencias, es decir, una base de la forma $\mathcal{B} = \{1, B, B^2, \ldots, B^{n-1}\}$.

Proposición 1.28. *Sean $\mathbb{F}$ un campo de números, $f(x) \in \mathbb{F}[x]$ mónico irreducible con $\mathrm{gr}(f(x)) = n$. Si $B \in \mathcal{O}_{\mathbb{F}}$ es tal que $f(B) = 0$, entonces*

$$\Delta(1, B, \ldots, B^{n-1}) = (-1)^{n(n-1)/2} N_{\mathbb{F}(B)/\mathbb{F}}(f'(B)).$$

DEMOSTRACIÓN. Ver [**26**], pp. 22. □

1.7. Primos e irreducibles

Uno de los problemas que estudiaremos en el Capítulo 2 será clasificar primos e irreducibles en ciertas familias de campos cuadráticos. Sea $\mathbb{F}$ un campo de números y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros. Un elemento P en $\mathcal{O}_{\mathbb{F}}$ es primo si: siempre que $P \mid A\,B$, entonces $P \mid A$ ó $P \mid B$. Diremos que $P \in \mathcal{O}_{\mathbb{F}}$ es irreducible si $P = A\,B$ implica $A \in \mathcal{U}_{\mathbb{F}}$ ó $B \in \mathcal{U}_{\mathbb{F}}$. Si $\mathcal{O}_{\mathbb{F}}$ es un dominio de factorización única (es decir, $h_{\mathbb{F}} = 1$), entonces el concepto de primo e irreducible coinciden. Si $h_{\mathbb{F}} > 1$, entonces todo elemento primo es irreducible y existen irreducibles que no son primos. Por ejemplo, consideremos el número 70 en el anillo de enteros de $\mathbb{F} = \mathbb{Q}(\sqrt{10})$. Observemos que

$$70 = 2 \cdot 5 \cdot 7 = 7(\sqrt{10})^2$$

son sus dos posibles factorizaciones. El elemento 7 es primo en $\mathcal{O}_{\mathbb{F}}$ mientras que $2, 5, \sqrt{10}$ son irreducibles pero no primos. El 7 aparece en todas las factorizaciones, los irreducibles solamente en una de las dos. Esta es una propiedad que tienen todos los primos: si $A \in \mathcal{O}_{\mathbb{F}}$, y P es primo tal que $P \mid A$, entonces P aparece en todas las posibles factorizaciones de A en elementos irreducibles.

El resultado siguiente nos ayuda a clasificar los elementos primos e irreducibles de acuerdo a su factorización en ideales primos.

Proposición 1.29. *Sean $\mathbb{F}$ un campo de números, $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros y $P \in \mathcal{O}_{\mathbb{F}} - \{0\}$. Entonces:*

1. *P es un elemento irreducible si y sólo si el ideal $\langle P\rangle$ es maximal en el conjunto de los ideales propios principales de $\mathcal{O}_{\mathbb{F}}$.*
2. *P es un elemento primo si y sólo si $\langle P\rangle$ es un ideal primo.*

DEMOSTRACIÓN. Probaremos la afirmación 1. Supongamos que P es irreducible y sea $\langle A\rangle$ tal que $\langle A\rangle \supseteq \langle P\rangle$. Entonces, existe $\mathfrak{I}$ tal que $\langle P\rangle = \langle A\rangle\, \mathfrak{I}$. Observemos que $\mathfrak{I}$ debe ser principal porque $\mathfrak{I} \sim \mathcal{O}_{\mathbb{F}}$. Sea $\mathfrak{I} = \langle B\rangle$. Por lo anterior, $A\,B$ es un asociado de P, por lo que $A\,B$ es un irreducible en $\mathcal{O}_{\mathbb{F}}$. Por definición se cumple una de las dos afirmaciones siguientes: $A \in \mathcal{U}_{\mathbb{F}}$ ó $B \in \mathcal{U}_{\mathbb{F}}$. En el primer caso $\langle A\rangle = \mathcal{O}_{\mathbb{F}}$. Si $B \in \mathcal{U}_{\mathbb{F}}$, entonces $\langle P\rangle = \langle A\rangle\,\langle B\rangle = \langle A\rangle$.

Inversamente, supongamos que $\langle P\rangle$ es un ideal maximal en el conjunto de los ideales principales propios de $\mathcal{O}_{\mathbb{F}}$. Sean A, B tales que $P = A\,B$. Entonces $\langle P\rangle = \langle A\rangle\,\langle B\rangle$ y $\langle A\rangle \supseteq \langle P\rangle$. Como $\langle P\rangle$ es maximal en el conjunto de los ideales principales no triviales, entonces $\langle A\rangle = \mathcal{O}_{\mathbb{F}}$ o bien $\langle A\rangle = \langle P\rangle$. En el primer caso, A es una unidad; en el segundo,

$$\langle A\rangle = \langle P\rangle = \langle A\rangle\,\langle B\rangle\,,$$

y por la ley de la cancelación $\mathcal{O}_{\mathbb{F}} = \langle B\rangle$, por lo que B es una unidad. Esto implica que P es un irreducible.

La justificación de la afirmación 2 es similar. □

Capítulo 2

El 2-grupo de clases en campos cuadráticos y aplicaciones

Encontrar el grupo de clases de un campo de números es un problema complicado, incluso la tarea de encontrar el p-subgrupo de Sylow no es sencilla. Algunos algoritmos se han implementado en programas computacionales tales como KANT/KASH o PARI/GP. En el caso de un campo cuadrático, el célebre Teorema de Gauss sobre el 2-rango (Teorema 2.4) da con precisión el rango del 2-subgrupo de Sylow de $Cl_{\mathbb{F}}$ en términos del número de divisores del discriminante del campo. En [**5**], [**6**], [**17**] y [**28**] se dan algoritmos que usan la teoría de las formas cuadráticas para encontrar Cl_2. Dada una clase $\overline{\mathfrak{I}} \in Cl_2$, ellos encuentran diferentes métodos para obtener, de ser posible, otra clase $\overline{\mathfrak{J}}$ tal que $\overline{\mathfrak{J}}^{\,2} = \overline{\mathfrak{I}}$. Es fácil encontrar representantes de cada clase ambigua (i.e. clases de orden 2) y podemos usar cualquiera de los métodos anteriores para construir Cl_2. En este capítulo vamos a dar otro procedimiento para obtener Cl_2, pero en lugar de comenzar con las clases ambiguas, vamos a hallar ideales $\mathfrak{I} \subseteq \mathcal{O}_{\mathbb{F}}$ tales que $\langle\overline{\mathfrak{I}}\rangle$ es maximal en el conjunto de subgrupos cíclicos de Cl_2. Si el exponente de $Cl_{\mathbb{F}}$ es 2, vamos a usar la misma técnica para dar un criterio para decidir si un ideal de $\mathcal{O}_{\mathbb{F}}$ es principal o no. Después relacionaremos este problema con la solubilidad de ciertas ecuaciones diofantinas. Finalmente, usaremos el criterio para distinguir ideales principales y no principales para clasificar los elementos primos, irreducibles y compuestos en algunos anillos de enteros de ciertos campos cuadráticos. Con la ayuda de los programas computacionales KASH3 [**9**] y Sage [**30**] resolveremos algunos ejemplos explícitos.

2.1. Algunas propiedades de los grupos abelianos finitos

Denotaremos con C_n al grupo cíclico de orden n y para $a \in \mathbb{Z}$ escribiremos $\overline{a}$ para representar la clase de a en C_n, donde asumimos que $C_n = \mathbb{Z}/n\mathbb{Z}$. Sea $G = \langle g_1, \ldots, g_r\rangle$ un grupo abeliano finito. Estamos interesados en encontrar generadores $h_1, \ldots, h_k \in G$ tales que

$$G = \langle h_1, \ldots, h_k\rangle \cong \langle h_1\rangle \oplus \cdots \oplus \langle h_k\rangle.$$

Sea $\mathcal{C}_G = \{\langle a\rangle : a \in G\}$. Entonces

Proposición 2.1. *Sea $G = G_1 \oplus \cdots \oplus G_k$ un p-grupo abeliano finito donde cada G_j es un p-grupo cíclico. Si $(\overline{a_1}, \ldots, \overline{a_k}) \in G$, entonces $\langle(\overline{a_1}, \ldots, \overline{a_k})\rangle$ es un elemento maximal de $\mathcal{C}_G$ si y sólo si $\mathrm{m.c.d.}\,(a_i, p) = 1$ para algún i.*

DEMOSTRACIÓN. Supongamos que $\langle(\overline{a_1}, \ldots, \overline{a_k})\rangle$ es maximal en $\mathcal{C}_G$ y que, para todo i, $\mathrm{m.c.d.}\,(a_i, p) = p$. Si $b_i = a_i/p$ tenemos

$$\langle(\overline{a_1}, \ldots, \overline{a_k})\rangle = \langle(\overline{pb_1}, \ldots, \overline{pb_k})\rangle = \langle p(\overline{b_1}, \ldots, \overline{b_k})\rangle.$$

Como

$$o(\langle(\overline{a_1},\ldots,\overline{a_k})\rangle) = \frac{o(\langle(\overline{b_1},\ldots,\overline{b_k})\rangle)}{p},$$

entonces

$$\langle(\overline{a_1},\ldots,\overline{a_k})\rangle \subsetneq \langle(\overline{b_1},\ldots,\overline{b_k})\rangle,$$

así que $\langle(\overline{a_1},\ldots,\overline{a_k})\rangle$ no es un elemento maximal en $\mathcal{C}_G$.

Inversamente, podemos asumir, sin pérdida de generalidad, que $\mathrm{m.c.d.}\,(a_1,p) = 1$. Consideremos $\langle(\overline{c_1},\ldots,\overline{c_k})\rangle \in \mathcal{C}_G$ tal que $\langle(\overline{a_1},\ldots,\overline{a_k})\rangle \subseteq \langle(\overline{c_1},\ldots,\overline{c_k})\rangle$. Sea $n \in \mathbb{Z}$ tal que $\langle(\overline{a_1},\ldots,\overline{a_k})\rangle = \langle n(\overline{c_1},\ldots,\overline{c_k})\rangle$. Tomemos la proyección $\phi : G \to G_1$. Como $\mathrm{m.c.d.}\,(a_1,p) = 1$, entonces $\phi(\langle(\overline{a_1},\ldots,\overline{a_k})\rangle) = G_1$. De la igualdad

$$o((\overline{a_1},\ldots,\overline{a_k})) = \frac{o((\overline{c_1},\ldots,\overline{c_k}))}{\mathrm{m.c.d.}\,(n, o((\overline{c_1},\ldots,\overline{c_k})))}$$

se sigue que, si $\mathrm{m.c.d.}\,(n, o((\overline{c_1},\ldots,\overline{c_k}))) > 1$, entonces $p \mid n$ y $\phi(\langle n(\overline{c_1},\ldots,\overline{c_k})\rangle) \neq G_1$, lo que es imposible. Por tanto $\mathrm{m.c.d.}\,(n, o((\overline{c_1}\ldots\overline{c_k}))) = 1$ y de esto se sigue que $\langle(\overline{a_1},\ldots,\overline{a_k})\rangle$ es un elemento maximal en $\mathcal{C}_G$. □

El siguiente resultado es similar al Teorema Fundamental de los Grupos Abelianos Finitos.

Proposición 2.2. *Sea G un p-grupo abeliano finito, H un subgrupo de G, $g \in G$ tal que $G = \langle H, g\rangle$, $g \notin H$ y $o(g) \leq o(\langle h\rangle)$ para todo $\langle h\rangle$ maximal en $\mathcal{C}_H$. Entonces existe $g' \in G$ tal que $G = \langle H, g'\rangle \cong H \oplus \langle g'\rangle$.*

DEMOSTRACIÓN. Sea $\mu = sp^m$ el mínimo entero positivo tal que $\mathrm{m.c.d.}\,(s,p) = 1$ y $\mu g \in H$. Como $\langle g\rangle = \langle sg\rangle$, podemos suponer que $\mu = p^m$. Ahora consideremos $h \in H$ con $\langle h\rangle$ maximal en $\mathcal{C}_H$, $p^m g \in \langle h\rangle$ y sea $\nu = tp^n$ el menor entero positivo tal que $\mathrm{m.c.d.}\,(t,p) = 1$ y $p^m g = \nu h$. Como antes, podemos reemplazar h por th y suponer que $\nu = p^n$. Es claro que si $o(g) = p^{m+r}$ entonces $o(h) = p^{n+r}$. Si e es el neutro de G entonces:

$$\begin{aligned} e &= p^{m+r}g = p^m p^r g = p^r(p^m g) = (p^r-1)(p^m g) + (p^m g) \\ &= (p^r-1)(p^n h) + (p^m g) = p^m((p^r-1)p^{n-m}h + g). \end{aligned}$$

Sea $g' = (p^r-1)p^{n-m}h + g$. Es claro que $g' \neq e$ y $o(g') \leq p^m$. Supongamos que $o(g') = p^j$ y $1 \leq j < m$. Entonces

$$e = p^j g' = p^j((p^r-1)p^{n-m}h + g) = p^j((p^r-1)p^{n-m}h) + p^j g \in \langle h\rangle.$$

Se sigue que $p^j g \in \langle h\rangle$ lo que es imposible. Por lo tanto $j = m$.

Por lo anterior $g' = (p^r-1)p^{n-m}h + g$ y $G = \langle H, g'\rangle$. La afirmación $\langle H, g'\rangle \cong H \oplus \langle g'\rangle$ es consecuencia de $H \cap \langle g'\rangle = \langle e\rangle$. □

A continuación describiremos un algoritmo que nos ayudará a modificar el conjunto de generadores de un grupo abeliano finito G de tal forma que el nuevo conjunto de generadores descompone a G como una suma directa.

Algoritmo. *Sea $G = \langle g_1,\ldots,g_r\rangle$ un grupo abeliano finito y supongamos que conocemos los valores de $o(g_i)$ para $i = 1,\ldots,r$. Primero estudiaremos el caso donde G es un p-grupo. En el proceso que describimos a continuación, cuando cambiemos un generador (en caso de ser necesario), indexamos los nuevos elementos de tal forma que*

$$o(g_1) \geq o(g_2) \geq \cdots \geq o(g_r).$$

Sea $G' = \langle g_1, g_2\rangle$, $H' = \langle g_1\rangle$ y $g = g_2$ como en la Proposición 2.2. *Si $g_2 \in H'$, entonces $G = \langle g_1, g_3, \ldots, g_r\rangle$. Así que podemos suponer que $g_2 \notin H'$. Usando la* Proposición 2.2, *existe $g_2' \in G'$ tal que*

$$G' = \langle H', g_2'\rangle \cong H' \oplus \langle g_2'\rangle \quad y \quad \langle g_1, g_2, \ldots, g_r\rangle = \langle g_1, g_2', \ldots, g_r\rangle.$$

Es posible que $o(g_2') < o(g_3)$. Si esto ocurre, indexamos y repetimos el proceso hasta que $g_2' = g_2$. Por tanto $G' \cong \langle g_1\rangle \oplus \langle g_2\rangle$. Para el siguiente paso consideramos $G' = \langle g_1, g_2, g_3\rangle$, $H' = \langle g_1, g_2\rangle \cong \langle g_1\rangle \oplus \langle g_2\rangle$ y $g = g_3$ como en la Proposición 2.2. *Podemos suponer $g_3 \notin H'$. Puesto que $o(g_1) \geq o(g_2) \geq o(g_3)$, entonces el orden de cualquier subgrupo cíclico maximal de H' es mayor o igual a $o(g_3)$ por lo que satisface la hipótesis de la* Proposición 2.2. *Sea $g_3' \in G'$ con $G' = \langle g_1\rangle \oplus \langle g_2\rangle \oplus \langle g_3'\rangle$. Si $o(g_3') < o(g_4)$, repetimos el proceso hasta obtener $g_3' = g_3$ y $G' = \langle g_1\rangle \oplus \langle g_2\rangle \oplus \langle g_3\rangle$. Continuamos con este procedimiento para construir explícitamente una base $\{g_1, \ldots, g_t\}$ de G tal que $G \cong \langle g_1\rangle \oplus \cdots \oplus \langle g_t\rangle$.*

En el caso general, si G es un grupo abeliano finito arbitrario, aplicamos el algoritmo a cada p-subgrupo de Sylow de G.

En este capítulo llamaremos el *Algoritmo* al procedimiento que acabamos de describir.

Ejemplo 2.3. *Sea $G = C_{16}\oplus C_8\oplus C_8\oplus C_4$ y $H = \langle g_1, g_2, g_3, g_4, g_5\rangle$ donde $g_1 = (\overline{1}, \overline{1}, \overline{1}, \overline{1})$, $g_2 = (\overline{3}, \overline{1}, \overline{1}, \overline{1})$, $g_3 = (\overline{7}, \overline{3}, \overline{0}, \overline{2})$, $g_4 = (\overline{3}, \overline{0}, \overline{1}, \overline{1})$, $g_5 = (\overline{12}, \overline{6}, \overline{3}, \overline{1}) \in G$. Usaremos el Algoritmo para encontrar una representación de H como la suma directa de subgrupos cíclicos de H. Notemos que*

$$o(g_1) = o(g_2) = o(g_3) = o(g_4) = 16, \quad o(g_5) = 8,$$

entonces los elementos están acomodados correctamente para utilizar el Algoritmo. Aplicamos la Proposición 2.2 *a $G' = \langle g_1, g_2\rangle$, $H' = \langle g_1\rangle$ y $g = g_2$. Los menores enteros positivos μ y ν tales que $\mu g_1 = \nu g_2$ son $\mu = 12$ y $\nu = 4$. Como $12 = 3 \cdot 4$, reemplazamos g_1 por $3g_1$, y una vez más llamamos g_1 al nuevo elemento. Con esta notación tenemos $g_1 = (\overline{3}, \overline{3}, \overline{3}, \overline{3})$. Si $h = g_1$ tenemos $4g \in \langle h\rangle$ y los menores enteros positivos μ y ν tales que $\mu g = \nu h$ son $\mu = \nu = 2^2$. Observemos que $2^{2+2}g = 2^{2+2}h = e$. Entonces, los valores que necesitamos para construir a g' como en la Proposición* 2.2 *son $r = m = n = 2$ y*

$$g' = (2^2 - 1)(2^{2-2})h + g = 3h + g = 3(\overline{3}, \overline{3}, \overline{3}, \overline{3}) + (\overline{3}, \overline{1}, \overline{1}, \overline{1}) = (\overline{12}, \overline{2}, \overline{2}, \overline{2}).$$

Como $o(g') = 4$, reemplazamos g_2 por g' y acomodamos los generadores de tal forma que $o(g_1) \geq \cdots \geq o(g_5)$. Tenemos

$$\begin{array}{rcl} g_1 & = & (\overline{1}, \overline{1}, \overline{1}, \overline{1}), \\ g_2 & = & (\overline{7}, \overline{3}, \overline{0}, \overline{2}), \\ g_3 & = & (\overline{3}, \overline{0}, \overline{1}, \overline{1}), \\ g_4 & = & (\overline{12}, \overline{6}, \overline{3}, \overline{1}), \\ g_5 & = & (\overline{12}, \overline{2}, \overline{2}, \overline{2}). \end{array}$$

Repetimos el proceso con $g = g_2$, $h = g_1$, $8g = 8h$, $16g = 16h = e$, $m = n = 3$, $r = 1$ y

$$g' = (2^1 - 1)(2^0)h + g = (\overline{1}, \overline{1}, \overline{1}, \overline{1}) + (\overline{7}, \overline{3}, \overline{0}, \overline{2}) = (\overline{8}, \overline{4}, \overline{1}, \overline{3}).$$

Reemplazamos g_2 por g' y reordenamos. Así, hemos obtenido una nueva lista de generadores de H:

$$\begin{aligned} g_1 &= (\overline{1},\overline{1},\overline{1},\overline{1}),\\ g_2 &= (\overline{3},\overline{0},\overline{1},\overline{1}),\\ g_3 &= (\overline{12},\overline{6},\overline{3},\overline{1}),\\ g_4 &= (\overline{8},\overline{4},\overline{1},\overline{3}),\\ g_5 &= (\overline{12},\overline{2},\overline{2},\overline{2}). \end{aligned}$$

Repetimos el proceso con los nuevos $g_2 = g$, $H' = \langle g_1\rangle$, $h = g_1$, $8g = 8h$, $16g = 16h = e$, $m = n = 3$, $r = 1$. *Así*

$$g' = (2^1-1)(2^0)h + g = (\overline{1},\overline{1},\overline{1},\overline{1}) + (\overline{3},\overline{0},\overline{1},\overline{1}) = (\overline{4},\overline{1},\overline{2},\overline{2}).$$

Por tanto, tenemos un nuevo conjunto de generadores de H*:*

$$\begin{aligned} g_1 &= (\overline{1},\overline{1},\overline{1},\overline{1}),\\ g_2 &= (\overline{4},\overline{1},\overline{2},\overline{2}),\\ g_3 &= (\overline{12},\overline{6},\overline{3},\overline{1}),\\ g_4 &= (\overline{8},\overline{4},\overline{1},\overline{3}),\\ g_5 &= (\overline{12},\overline{2},\overline{2},\overline{2}). \end{aligned}$$

Notemos que si aplicamos nuevamente el procedimiento no habrá cambios ya que $16g_1 = 8g_2 = e$ *y* $r = 0$. *Continuando con* $g = g_3, H' = \langle g_1, g_2\rangle$ *y* $h = g_1$ *observamos que* $8g = 16h = e$ *y* $r = 0$. *Por tanto, no es necesario modificar* g_3.

En el siguiente paso aplicamos el Algoritmo con $g = g_4$, $H' = \langle g_1, g_2, g_3\rangle$. *En este caso* $g_4 = 12g_1 + 6g_2 + 3g_3 \in H'$. *Entonces:*

$$g_1 = (\overline{1},\overline{1},\overline{1},\overline{1}),\ \ g_2 = (\overline{4},\overline{1},\overline{2},\overline{2}),\ \ g_3 = (\overline{12},\overline{6},\overline{3},\overline{1}),\ \ g_4 = (\overline{12},\overline{2},\overline{2},\overline{2}).$$

Como en el paso anterior $g = g_4 \in H' = \langle g_1, g_2, g_3\rangle$. *Así, los generadores que estamos buscando son* g_1, g_2, g_3 *y*

$$H = \langle (\overline{1},\overline{1},\overline{1},\overline{1}), (\overline{4},\overline{1},\overline{2},\overline{2}), (\overline{12},\overline{6},\overline{3},\overline{1})\rangle \cong C_{16}\oplus C_8\oplus C_8,$$

donde $o(g_1) = 16,\ o(g_2) = o(g_3) = 8$.

2.2. El 2-grupo de clases de campos cuadráticos reales

Como una aplicación del Algoritmo, vamos a construir un conjunto de generadores del 2-subgrupo de Sylow del grupo de clases de ideales de un campo cuadrático real. El siguiente teorema es conocido ([**21**], Theorem 3.70).

Teorema 2.4. (Teorema de Gauss sobre el 2-rango de $Cl_{\mathbb{F}}$) *Sea* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *un campo cuadrático y* t *el número de factores primos distintos de* $\delta_{\mathbb{F}}$. *Si existe un primo* $p \equiv 3 \pmod 4$ *tal que* $p \mid \delta_{\mathbb{F}}$ *y* $d > 0$, *entonces el rango de* Cl_2 *es* $t-2$. *En cualquier otro caso, el rango es* $t-1$. □

Sea $a, b \in \mathbb{Z},\ b > 1$. Usaremos la siguiente notación:

$$\left[\frac{a}{b}\right] = \begin{cases} 1 & \text{si } x^2 \equiv a \pmod b \text{ es soluble,}\\ -1 & \text{si } x^2 \equiv a \pmod b \text{ no es soluble.}\end{cases}$$

Si b es un primo racional y $\text{m.c.d.}\,(a,b) = 1$, entonces $\left[\frac{a}{b}\right]$ es el símbolo de Legendre $\left(\frac{a}{b}\right)$. Como consecuencia del Teorema Chino del Residuo tenemos:

Lema 2.5. *Sean* $a,\ b = b_1 \cdots b_t > 1$ *enteros tales que* $\text{m.c.d.}\,(b_i, b_j) = 1$ *para* $i \neq j$. *Entonces,* $\left[\dfrac{a}{b}\right] = 1$ *si y sólo si* $\left[\dfrac{a}{b_i}\right] = 1$ *para* $i = 1, \ldots, t$. □

Lema 2.6. *Sean* $b_1, \ldots, b_t \in \{-1, 1\},\ a, n, p_1, \ldots, p_t \in \mathbb{N}$ *con* $a < 2^n$ *un número impar y donde* p_i *es un primo racional impar para* $i = 1, \ldots, t$. *Entonces existe un primo racional* q *tal que*

$$q \equiv a \pmod{2^n}, \quad \left(\frac{q}{p_1}\right) = b_1, \ldots, \left(\frac{q}{p_t}\right) = b_t.$$

DEMOSTRACIÓN. Sean $c_1, \ldots, c_t \in \mathbb{Z}$ tales que $\left(\dfrac{c_i}{p_i}\right) = b_i$. Usando el Teorema Chino del Residuo, existe $c \in \mathbb{Z}$ tal que

$$\begin{aligned} c &\equiv a \pmod{2^n} \\ c &\equiv c_1 \pmod{p_1} \\ &\vdots \\ c &\equiv c_t \pmod{p_t}. \end{aligned}$$

Como $p_i \nmid c_i$ entonces $\text{m.c.d.}\,(c, 2^n p_1 \cdots p_t) = 1$ y por el Teorema de Dirichlet existe una infinidad de primos $q \equiv c \pmod{2^n p_1 \cdots p_t}$. □

Lema 2.7. *Sea* $d = p_0 p_1 \cdots p_g$ *un entero positivo libre de cuadrados,* $p_i \equiv 1 \pmod 4$ *para* $0 \leq i \leq g$. *Entonces existen primos racionales* $q_1, \ldots, q_g$ *tales que*

$$\left(\frac{d}{q_i}\right) = 1 \quad y \quad \left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1.$$

DEMOSTRACIÓN. Se sigue del Lema 2.6, la Ley de Reciprocidad Cuadrática y el Lema 2.5. □

De la primera afirmación del Lema 2.6, los primos $q_1, \ldots, q_g$ pueden ser elegidos de tal forma que $q_i \equiv 1 \pmod 4$. Elegir los primos con esta propiedad será relevante en el siguiente lema.

Lema 2.8. *Sea* $d = 2\, p_1 \cdots p_g$ *un entero libre de cuadrados con* $p_i \equiv 1 \pmod 4$ *para* $1 \leq i \leq g$. *Existen* $q_1, \ldots, q_g$ *primos que satisfacen*

$$\left(\frac{4d}{q_i}\right) = 1 \quad y \quad \left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1.$$

DEMOSTRACIÓN. Por el Lema 2.6 y la Ley de Reciprocidad Cuadrática, escogemos $q_1 \equiv 5 \pmod 8$ tales que

$$\left(\frac{p_1}{q_1}\right) = -1 \quad \text{y} \quad \left(\frac{p_j}{q_1}\right) = 1, \quad 2 \leq j \leq g.$$

Entonces

$$\left(\frac{d}{q_1}\right) = \left(\frac{2}{q_1}\right)\left(\frac{p_1}{q_1}\right)\left(\frac{p_2}{q_1}\right) \cdots \left(\frac{p_g}{q_1}\right) = (-1)(-1)(1) \cdots (1) = 1.$$

Finalmente $\left(\frac{4d}{q_1}\right) = \left(\frac{d}{q_1}\right)$. Como en la prueba del lema anterior se sigue

$$\left[\frac{q_1}{d}\right] = \left[\frac{-q_1}{d}\right] = -1.$$

Los primos $q_2, \ldots, q_g$ se obtienen como en el Lema 2.7 con la condición adicional $q_i \equiv 1 \pmod 8$. □

Lema 2.9. *Sea $d = p_0 p_1 \cdots p_g \equiv 1 \pmod 4$ un entero positivo libre de cuadrados con $g \geq 1$ tal que para algún $t \in \{-1, 0, 1, \ldots, g-2\}$*

$$p_0, \ldots, p_t \equiv 1 \pmod 4, \quad p_{t+1}, \ldots, p_g \equiv 3 \pmod 4.$$

Existen primos racionales $q_1, \ldots, q_{g-1}$ tales que $\left(\frac{d}{q_i}\right) = 1$ y $\left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1$.

DEMOSTRACIÓN. Los primeros primos $q_1, \ldots, q_t$ se obtienen como en el Lema 2.7 de tal forma que $q_i \equiv 1 \pmod 4$. Para $t+1 \leq i \leq g-1$, escogemos los primos q_i tales que

$$\left(\frac{p_{i-1}}{q_i}\right) = \left(\frac{p_i}{q_i}\right) = -1, \qquad \left(\frac{p_j}{q_i}\right) = 1, \quad j \neq i-1, i.$$

Así $\left(\frac{d}{q_i}\right) = -1$, $\left[\frac{q_i}{d}\right] = -1$. Finalmente, como $\left(\frac{q_i}{p_g}\right) = 1$, obtenemos $\left(\frac{-q_i}{p_g}\right) = -1$ y $\left[\frac{-q_i}{p_g}\right] = \left[\frac{-q_i}{d}\right] = -1$. □

Lema 2.10. *Sea $d = p_0 p_1 \cdots p_g \equiv 3 \pmod 4$ un entero positivo libre de cuadrados, tal que para algún $t \in \{-1, 0, 1, \ldots, g-1\}$*

$$p_0, \ldots, p_t \equiv 1 \pmod 4, \quad p_{t+1}, \ldots, p_g \equiv 3 \pmod 4.$$

Existen primos $q_1, \ldots, q_g$ con $\left(\frac{4d}{q_i}\right) = 1$ y $\left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1$.

DEMOSTRACIÓN. Los primos $q_1, \ldots, q_t$ se obtienen como en el Lema 2.7. Como $d \equiv 3 \pmod 4$, tenemos un número impar de primos $\equiv 3 \pmod 4$. Primero supongamos que p_g es el único primo tal que $p_g \equiv 3 \pmod 4$. En este caso elegimos un primo $q_g \equiv 1 \pmod 4$ que satisfaga

$$\left(\frac{p_{g-1}}{q_g}\right) = \left(\frac{q_g}{p_{g-1}}\right) = \left(\frac{q_g}{p_g}\right) = -1.$$

Por lo anterior, $\left[\frac{-q_g}{d}\right] = -1$. Finalmente, si más de un primo es $\equiv 3 \pmod 4$, entonces, en lugar de usar p_g como en el Lema 2.9, usamos cualquiera de los primos $p_j \equiv 3 \pmod 4$ tales que $\left(\frac{q_i}{p_j}\right) = 1$. La prueba se sigue como en los lemas anteriores. □

Lema 2.11. *Sea $d = 2\, p_1 \cdots p_g$ un entero positivo libre de cuadrados con $p_1, \ldots, p_t \equiv 1 \pmod 4$ y $p_{t+1}, \ldots, p_g \equiv 3 \pmod 4$ para $0 \leq t \leq g-1$. Existen primos $q_1, \ldots, q_{g-1}$ tales que $\left(\frac{4d}{q_i}\right) = 1$ y $\left[\frac{q_i}{d}\right] = \left[\frac{-q_i}{d}\right] = -1$.*

DEMOSTRACIÓN. Si $t > 0$, entonces $q_1, \ldots, q_t$ se obtienen como en el Lema 2.8 y los otros primos $q_{t+1}, \ldots, q_{g-1}$ como en el Lema 2.9. Si $t = 0$, entonces $p_i \equiv 3 \pmod 4$ para $i = 1, \ldots, g$ y $g \geq 2$. En este caso elegimos $q_1 \equiv 5 \pmod 8$ de tal forma que

$$\left(\frac{p_1}{q_1}\right) = -1, \quad \left(\frac{p_i}{q_1}\right) = 1, \quad i > 1.$$

De lo anterior y $\left(\frac{2}{q_1}\right) = -1$ tenemos

$$\left(\frac{4d}{q_1}\right) = 1, \quad \left[\frac{q_1}{d}\right] = \left[\frac{-q_1}{d}\right] = -1.$$

Los primos $q_2, \ldots, q_{g-1}$ se obtienen como en el Lema 2.9. □

Sea $\mathcal{P} = \{q_1, \ldots, q_t\}$ obtenido como en los Lemas 2.7, 2.8, 2.9, 2.10 ó 2.11. Observemos que existe una infinidad de $a_i \in \mathbb{N}$ tales que $a_i^2 \equiv d \pmod{q_i}$. Fijamos uno de estos y definimos los ideales $\mathfrak{q}_i = \langle q_i, a_i + \sqrt{d}\rangle$. Claramente, $\mathfrak{q}_i$ es un ideal primo, $N(\mathfrak{q}_i) = q_i$ y $\langle q_i\rangle = \mathfrak{q}_i\mathfrak{q}_i'$ donde $\mathfrak{q}_i' = \langle q_i, a_i - \sqrt{d}\rangle$. Dado $\mathcal{P}$ como antes, definimos $\mathcal{I}_\mathcal{P} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$. Escribiremos $\operatorname{ord}_\mathfrak{I}(\mathfrak{J})$ para indicar que $\mathfrak{I}^{\operatorname{ord}_\mathfrak{I}(\mathfrak{J})} \mid \mathfrak{J}$ y $\mathfrak{I}^{\operatorname{ord}_\mathfrak{I}(\mathfrak{J})+1} \nmid \mathfrak{J}$.

Observemos que $N(a_1 + a_2\sqrt{d}) = a_1^2 - da_2^2$, así que, si $\mathfrak{I} = \langle a_1 + a_2\sqrt{d}\rangle$, entonces $N(\mathfrak{I}) \equiv a_1^2 \pmod d$ ó $-N(\mathfrak{I}) \equiv a_1^2 \pmod d$. Por tanto, si $\left[\frac{\pm N(\mathfrak{I})}{d}\right] = -1$ tenemos que $\mathfrak{I}$ es un ideal no principal.

Teorema 2.12. *Sea $d = p_0p_1\cdots p_g$ un entero positivo libre de cuadrados y $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Si $\mathfrak{I} = \prod_{\mathfrak{q}\in\mathcal{I}_\mathcal{P}} \mathfrak{q}^{\operatorname{ord}_\mathfrak{q}(\mathfrak{I})}$ y $\operatorname{ord}_\mathfrak{q}(\mathfrak{I})$ es impar para algún $\mathfrak{q} \in \mathcal{I}_\mathcal{P}$, entonces*

1. $\left[\frac{\pm N(\mathfrak{I})}{d}\right] = -1$ *y por tanto $\mathfrak{I}$ es no principal.*
2. *Si $\overline{\mathfrak{I}} \in Cl_\mathbb{F}$ es la clase del ideal $\mathfrak{I}$, entonces $o(\overline{\mathfrak{I}})$ es par.*
3. *Sea $\mathfrak{J} = \prod_{\mathfrak{q}\in\mathcal{I}_\mathcal{P}} \mathfrak{q}^{\operatorname{ord}_\mathfrak{q}(\mathfrak{J})}$ tal que para algún $\mathfrak{q} \in \mathcal{I}_\mathcal{P}$, $\operatorname{ord}_\mathfrak{q}(\mathfrak{J})$ impar y $\operatorname{ord}_\mathfrak{q}(\mathfrak{I}) \not\equiv \operatorname{ord}_\mathfrak{q}(\mathfrak{J}) \pmod 2$. Entonces $\overline{\mathfrak{I}} \neq \overline{\mathfrak{J}}$.*

DEMOSTRACIÓN. Para la primera afirmación necesitamos que $\left[\frac{N(\mathfrak{I})}{p_1'}\right] = \left[\frac{-N(\mathfrak{I})}{p_2'}\right] = -1$ para ciertos divisores primos p_1', p_2' de d. Sea $j = \max\{i : \operatorname{ord}_{\mathfrak{q}_i}(\mathfrak{I}) \text{ es impar}\}$. Observemos que $j > 0$ y p_j es impar. Sabemos que $\left(\frac{q_j}{p_j}\right) = \left(\frac{q_j^{\operatorname{ord}_{\mathfrak{q}_j}(\mathfrak{I})}}{p_j}\right) = -1$, así, para cualquier $\mathfrak{q}_i \in \mathcal{I}_\mathcal{P}$ se tiene que $i < j$ ó $\operatorname{ord}_{\mathfrak{q}_i}(\mathfrak{I})$ es par. Por construcción, $\left(\frac{q_i^{\operatorname{ord}_{\mathfrak{q}_i}(\mathfrak{I})}}{p_j}\right) = 1$ si $q_i \mid N(\mathfrak{I})$, $q_i \neq q_j$. Por lo tanto $\left(\frac{N(\mathfrak{I})}{p_j}\right) = \left[\frac{N(\mathfrak{I})}{d}\right] = -1$. Si algún divisor primo p de d, $p \equiv 1 \pmod 4$, satisface $\left(\frac{N(\mathfrak{I})}{p}\right) = -1$, entonces $\left(\frac{-N(\mathfrak{I})}{p}\right) = \left[\frac{-N(\mathfrak{I})}{d}\right] = -1$.

Ahora consideremos el caso $\left(\frac{N(\mathfrak{I})}{p}\right) = 1,\ p \equiv 1 \pmod 4$, $p \mid d$. Si $d \equiv 1, 2 \pmod 4$, aplicando los Lemas 2.9 y 2.11 obtenemos, $\left(\frac{N(\mathfrak{I})}{p_g}\right) = 1$. Por tanto

$$\left(\frac{-N(\mathfrak{I})}{p_g}\right) = \left[\frac{-N(\mathfrak{I})}{p_g}\right] = \left[\frac{-N(\mathfrak{I})}{d}\right] = -1.$$

Ahora estudiemos el caso $d \equiv 3 \pmod 4$, $\left(\frac{N(\mathfrak{I})}{p}\right) = 1,\ p \equiv 1 \pmod 4$. Al principio de la prueba vimos que existe un primo $p_j \mid d$ tal que $\left(\frac{N(\mathfrak{I})}{p_j}\right) = -1$. Si $k = \min\{i : \operatorname{ord}_{\mathfrak{q}_i}(\mathfrak{I}) \text{ es impar}\}$, entonces $\left(\frac{N(\mathfrak{I})}{p_{k-1}}\right) = -1$. Como $d \equiv 3 \pmod 4$, d debe tener un número impar de divisores primos de la forma $4x+3$ y puesto que $p_j, p_{k-1} \equiv 3 \pmod 4$, entonces debe haber al menos tres de estos primos. Sea $q_i \in \mathcal{P}$ tal que $\operatorname{ord}_{\mathfrak{q}_i}(\mathfrak{I})$ es impar. Cada uno de estos tiene asociados dos divisores primos $p_{i-1},\ p_i$ de d tales que $\left(\frac{q_i}{p_{i-1}}\right) = \left(\frac{q_i}{p_i}\right) = -1$. Por la anterior, existe un número par de parejas (p_l, q_m) que satisfacen $\left(\frac{q_m}{p_l}\right) = -1$. Así, entre los símbolos $\left(\frac{N(\mathfrak{I})}{p_0}\right), \ldots, \left(\frac{N(\mathfrak{I})}{p_g}\right)$, un número par de ellos toman el valor -1 para ciertos primos $p_i \equiv 3 \pmod 4$. Por tanto, existe un primo $p \equiv 3 \pmod 4$ tal que $\left(\frac{N(\mathfrak{I})}{p}\right) = 1$. Como en el caso $d \equiv 1, 2 \pmod 4$ obtenemos $\left(\frac{-N(\mathfrak{I})}{p}\right) = \left[\frac{-N(\mathfrak{I})}{d}\right] = -1$. Notemos que $o(\overline{\mathfrak{I}})$ es par pues $\mathfrak{I}^a$ es no-principal para algún $a \in \mathbb{N}$ impar.

Finalmente, la clase $\overline{\mathfrak{I}}^{-1}$ tiene un representante

$$\mathfrak{I}' = \prod_{\mathfrak{q} \in \mathcal{I}_{\mathcal{P}}} \mathfrak{q}^{o(\overline{\mathfrak{q}}) - \operatorname{ord}_{\mathfrak{q}}(\mathfrak{I})},$$

donde $\operatorname{ord}_{\mathfrak{q}}(\mathfrak{I}') \equiv \operatorname{ord}_{\mathfrak{q}}(\mathfrak{I}) \pmod 2$. Así $\operatorname{ord}_{\mathfrak{q}}(\mathfrak{I}\mathfrak{I}')$ es impar y $\mathfrak{I}\mathfrak{I}'$ es no principal. Por tanto $\overline{\mathfrak{J}} \neq \overline{\mathfrak{I}'}^{-1}$ y $\overline{\mathfrak{I}} \neq \overline{\mathfrak{J}}$. □

Lema 2.13. *Sea $\mathbb{F}$ como siempre, $\mathfrak{I}, \mathfrak{J}$ ideales de $\mathcal{O}_{\mathbb{F}}$ tales que $\left[\frac{\pm N(\mathfrak{I})}{d}\right] = -1, o(\overline{\mathfrak{I}})$ es par y de forma que para cualquier primo ramificado p, $p \nmid N(\mathfrak{I})$ y $p \nmid N(\mathfrak{J})$. Si $\mathfrak{J} \in \overline{\mathfrak{I}}$ entonces $\left[\frac{\pm N(\mathfrak{J})}{d}\right] = -1$.*

DEMOSTRACIÓN. Sea $\mathfrak{J} \in \overline{\mathfrak{I}}$ tal que $\left[\frac{N(\mathfrak{J})}{d}\right] = 1$ ó $\left[\frac{-N(\mathfrak{J})}{d}\right] = 1$. Como $\overline{\mathfrak{I}}$ tiene orden par, tenemos $\left[\frac{N(\mathfrak{I}^{o(\overline{\mathfrak{I}})})}{d}\right] = 1$. Por la multiplicatividad del Símbolo de Legendre y el Lema 2.5, tenemos $\left[\frac{\pm N(\mathfrak{I}^{o(\overline{\mathfrak{I}})-1})}{d}\right] = -1$. Como $\left[\frac{N(\mathfrak{J})}{d}\right] = 1$ ó $\left[\frac{-N(\mathfrak{J})}{d}\right] = 1$, en

ambos casos tenemos

$$\left[\frac{N(\mathfrak{I}^{o(\overline{\mathfrak{I}})-1}\mathfrak{J})}{d}\right] = \left[\frac{-N(\mathfrak{I}^{o(\overline{\mathfrak{I}})-1}\mathfrak{J})}{d}\right] = -1.$$

De $\overline{\mathfrak{I}^{o(\overline{\mathfrak{I}})-1}} = \overline{\mathfrak{I}}^{\,-1} = \overline{\mathfrak{J}}^{\,-1}$, se sigue que $\mathfrak{I}^{o(\overline{\mathfrak{I}})-1}\mathfrak{J}$ es un ideal principal, lo que es imposible. Por tanto $\left[\frac{\pm N(\mathfrak{J})}{d}\right] = -1$. □

Si $\mathfrak{q}_i \in \mathcal{I}_{\mathcal{P}}$, entonces $o(\overline{\mathfrak{q}_i}) = 2^{k_i}t_i$ para algún $k_i, t_i \in \mathbb{N}$, t_i impar. Para $\mathfrak{q}_i \in \mathcal{I}_{\mathcal{P}}$ definimos

$$\mathfrak{J}_i = \mathfrak{q}_i^{t_i} \quad \text{y} \quad \mathcal{J}_{\mathcal{P}} = \{\mathfrak{J}_1, \ldots, \mathfrak{J}_{|\mathcal{P}|}\}. \tag{4}$$

Observemos que, como $\mathfrak{q}_i \neq \mathfrak{q}_j$ para $i \neq j$, entonces $\mathfrak{J}_i \neq \mathfrak{J}_j$.

Lema 2.14. *Sean $\mathbb{F}$ un campo cuadrático real y $\mathfrak{J}_i$ como antes. Entonces:*

1. $\left[\frac{\pm N(\mathfrak{J}_i)}{d}\right] = -1$ *para* $1 \leq i \leq |\mathcal{P}|$.
2. *Si $\mathfrak{J}_i \in \mathcal{J}_{\mathcal{P}}$, entonces $\overline{\mathfrak{J}_i} \notin \langle \overline{\mathfrak{J}_1}, \ldots, \overline{\mathfrak{J}_{i-1}}, \overline{\mathfrak{J}_{i+1}}, \ldots, \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle$.*
3. *Podemos modificar los elementos de $\mathcal{J}_{\mathcal{P}}$ de tal forma que*

$$\langle \overline{\mathfrak{J}_1}, \ldots, \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle \cong \langle \overline{\mathfrak{J}_1}\rangle \times \cdots \times \langle \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle.$$

DEMOSTRACIÓN. Los ideales que vamos a usar son tales que sus normas y d son primos relativos entre sí, así que podemos usar el Lema 2.13. La afirmación 1 se sigue del Lema 2.5 ya que t_i es impar. Para la afirmación 2 supongamos que $\overline{\mathfrak{J}_i} \in \langle \overline{\mathfrak{J}_1}, \ldots, \overline{\mathfrak{J}_{i-1}}, \overline{\mathfrak{J}_{i+1}}, \ldots, \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle$. Sea $\mathfrak{I} = \prod_{\mathfrak{J}_l \in \mathcal{J}_{\mathcal{P}}} \mathfrak{J}_l^{e_l}$ con $e_i = 0$ y e_j enteros no negativos para $i \neq j$. Es claro que $\overline{\mathfrak{I}} \in \langle \overline{\mathfrak{J}_1}, \ldots, \overline{\mathfrak{J}_{i-1}}, \overline{\mathfrak{J}_{i+1}}, \ldots, \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle$. Si $\mathfrak{I} \in \overline{\mathfrak{J}_i}$, entonces $\left[\frac{\pm N(\mathfrak{I})}{d}\right] = -1$, pues $\left[\frac{\pm N(\mathfrak{J}_i)}{d}\right] = -1$. Por lo tanto algún e_l es impar. Puesto que $e_i = 0$, entonces, por el Teorema 2.12 inciso 3, tenemos $\mathfrak{J}_i = \mathfrak{q}_i^{t_i} \notin \overline{\mathfrak{I}}$. Para la afirmación 3, observamos primero que el rango de $\langle \overline{\mathfrak{J}_1}, \ldots, \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle$ es $|\mathcal{P}|$. Ahora usamos el Algoritmo. □

Teorema 2.15. *Si $\mathbb{F}$ es un campo cuadrático real, entonces $Cl_2 = \langle \overline{\mathfrak{J}_1}, \ldots, \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle$.*

DEMOSTRACIÓN. Por el Lema 2.14 y el Teorema 2.4, sabemos que $G_{\mathcal{J}} = \langle \overline{\mathfrak{J}_1}, \ldots, \overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle$ es un 2-grupo con rango igual al rango de Cl_2. Supongamos que existe un ideal $\mathfrak{I} \subseteq \mathcal{O}_{\mathbb{F}}$ tal que $o(\overline{\mathfrak{I}}) = 2^k$ con $k \in \mathbb{N}$ y $\text{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) = 1$. Como el 2-rango de $Cl_{\mathbb{F}}$ es igual al 2-rango de $G_{\mathcal{J}}$, existen $t, e_1, \ldots, e_{|\mathcal{P}|} \in \mathbb{N}$ tal que

$$\overline{\mathfrak{I}^t} = \overline{\prod_{\mathfrak{J}_i \in \mathcal{J}_{\mathcal{P}}} \mathfrak{J}_i^{e_i}},$$

con $\overline{\mathfrak{I}^t} \neq \overline{\mathcal{O}_{\mathbb{F}}}$. Elegimos el menor entero t que satisface esta condición. Notemos que t es par, si no fuera así $\overline{\mathfrak{I}} \in G_{\mathcal{J}}$. Así $\left[\frac{N(\mathfrak{I}^t)}{d}\right] = 1$. Por otra parte, al menos un e_i es impar, pues de lo contrario t no sería mínimo. Del Teorema 2.12 tenemos $\left[\frac{N(\mathfrak{I}^t)}{d}\right] = -1$. Esto muestra que cualquier ideal $\mathfrak{I} \subseteq \mathcal{O}_{\mathbb{F}}$ con $\text{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) = 1$ satisface $\overline{\mathfrak{I}} \in G_{\mathcal{J}}$. Sea p

un primo ramificado y $\mathfrak{p}$ un ideal primo tal que $N(\mathfrak{p}) = p$. Sabemos que el rango de Cl_2 es igual al rango de $G_{\mathcal{J}}$, así $\langle G_{\mathcal{J}}, \overline{\mathfrak{p}}\rangle$ debe de tener el mismo rango que $G_{\mathcal{J}}$. Esto implica que $\overline{\mathfrak{p}} \in G_{\mathcal{J}}$ o existe un ideal maximal $H \in C_{G_{\mathcal{J}}}$ tal que $H \subseteq \langle\overline{\mathfrak{p}}\rangle$. Si sucede lo segundo, $1 < o(H) \leq o(\overline{\mathfrak{p}}) \leq 2$, así que $H = \langle\overline{\mathfrak{p}}\rangle$, $\overline{\mathfrak{p}} \in G_{\mathcal{J}}$ y $G_{\mathcal{J}} = \langle G_{\mathcal{J}}, \overline{\mathfrak{p}}\rangle$. Aplicamos este argumento a cada primo ramificado y así obtenemos $Cl_2 = G_{\mathcal{J}}$. □

Lema 2.16. *Sea $\mathbb{F}$ un campo cuadrático real. Cada clase de $Cl_{\mathbb{F}}$ tiene un representante $\mathfrak{I}$ tal que* $\mathrm{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) = 1$.

DEMOSTRACIÓN. Sea $\overline{\mathfrak{J}} \in Cl_{\mathbb{F}}$ tal que $\mathfrak{J} = \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{q}_1 \cdots \mathfrak{q}_r$ donde $\mathfrak{p}_i$ es un ideal primo ramificado para $1 \leq i \leq k$ y $\mathfrak{q}_i$ es un ideal primo no ramificado para $1 \leq i \leq r$. Es suficiente probar que cada $\overline{\mathfrak{p}_i}$ tiene un representante que satisface la afirmación.

Primero, probaremos la afirmación para $d \equiv 1, 2 \pmod 4$. En este caso, un primo p se ramifica si y sólo si $p \mid d$, y el ideal con norma p_i es $\mathfrak{p}_i = \langle p_i, \sqrt{d}\rangle = \langle p_i, p_i + \sqrt{d}\rangle$. Así tenemos

$$\langle p_i - \sqrt{d}\rangle \mathfrak{p}_i = \langle p_i(p_i - \sqrt{d}), p_i^2 - d\rangle = \langle p_i\rangle\langle p_i - \sqrt{d}, p_i - d/p_i\rangle,$$

y $\mathfrak{p}_i$ está relacionado con $\mathfrak{p}_i' = \langle p_i - \sqrt{d}, p_i - d/p_i\rangle$. Notemos que $\mathfrak{p}_i'$ no necesariamente es un ideal primo. Observemos que $\mathrm{m.c.d.}\,(p, p_i - d/p_i) = 1$ para todo primo p tal que $p \mid d$. Entonces $p \nmid p_i - d/p_i$ y $p \nmid N(p_i - d/p_i)$. El hecho de que $\mathfrak{p}_i' \mid \langle p_i - d/p_i\rangle$ implica $p \nmid N(\mathfrak{p}_i')$. Por tanto $\mathrm{m.c.d.}\,(d, N(\mathfrak{p}_i')) = 1$. Si cambiamos $\mathfrak{p}_i$ por $\mathfrak{p}_i'$, obtenemos un nuevo ideal $\mathfrak{I}$ relacionado con $\mathfrak{J}$ sin factores primos ramificados.

Ahora supongamos $d \equiv 3 \pmod 4$. Procedemos de forma similar al caso anterior, obteniendo así un ideal $\mathfrak{I} \in \overline{\mathfrak{J}}$ tal que $\mathrm{m.c.d.}\,(N(\mathfrak{I}), d) = 1$. En este caso, 2 es ramificado, pero $2 \nmid d$, así que es posible que $\mathfrak{p} = \langle 2, 1 + \sqrt{d}\rangle \mid \mathfrak{I}$. En este caso, tenemos

$$\mathfrak{p}\langle 1 - \sqrt{d}\rangle = \langle 2(1 - \sqrt{d}), 1 - d\rangle = \langle 2\rangle\langle 1 - \sqrt{d}, (1 - d)/2\rangle,$$

donde $\mathfrak{p}' = \langle 1 - \sqrt{d}, (1 - d)/2\rangle \sim \mathfrak{p}$ y $\dfrac{1 - d}{2} \in \mathbb{Z}$ es impar. En particular $2 \nmid N(\mathfrak{p}')$. Como $\mathrm{m.c.d.}\,(1 - d, d) = 1$ tenemos $\mathrm{m.c.d.}\,(N(\mathfrak{p}'), d) = 1$, así $\mathrm{m.c.d.}\,(N(\mathfrak{p}'), \delta_{\mathbb{F}}) = 1$. Reemplazando $\mathfrak{p}$ por $\mathfrak{p}'$ obtenemos el ideal que queríamos. □

Proposición 2.17. *Sea $\mathbb{F}$ un campo cuadrático real tal que $|Cl_{\mathbb{F}}| = 2^k$ para algún $k \in \mathbb{N}$ y $\overline{\mathfrak{I}} \in Cl_{\mathbb{F}}$ con* $\mathrm{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) = 1$. *Entonces $\langle\overline{\mathfrak{I}}\rangle$ es maximal en $\mathcal{C}_{Cl_{\mathbb{F}}}$ si y sólo si* $\left[\dfrac{\pm N(\mathfrak{I})}{d}\right] = -1$.

DEMOSTRACIÓN. Sabemos que $Cl_{\mathbb{F}} = G_{\mathcal{J}} \cong \langle\overline{\mathfrak{J}_1}\rangle \times \cdots \langle\overline{\mathfrak{J}_{|\mathcal{P}|}}\rangle$. Si $\langle\overline{\mathfrak{I}}\rangle$ es maximal en $\mathcal{C}_{Cl_{\mathbb{F}}}$, entonces $\mathfrak{I}$ está relacionado con algún ideal de la forma

$$\mathfrak{J} = \prod_{\mathfrak{J}_i \in \mathcal{J}_{\mathcal{P}}} \mathfrak{J}_i^{\mathrm{ord}_{\mathfrak{J}_i}(\mathfrak{J})}$$

donde algún $\mathrm{ord}_{\mathfrak{J}_i}(\mathfrak{J})$ es impar. El Teorema 2.12 implica que $\left[\dfrac{\pm N(\mathfrak{I})}{d}\right] = -1$. Inversamente, supongamos que $\langle\overline{\mathfrak{I}}\rangle$ no es maximal. Entonces $\langle\overline{\mathfrak{I}}\rangle \subsetneq \langle\overline{\mathfrak{J}}\rangle$ para una clase $\overline{\mathfrak{J}}$. Podemos

elegir $\mathfrak{J}$ de tal forma que $\mathrm{m.c.d.}\,(N(\mathfrak{J}), \delta_{\mathbb{F}}) = 1$. Así, $\overline{\mathfrak{I}} = \overline{\mathfrak{J}}^t$ para algún $t \in \mathbb{N}$. Como consecuencia de $\overline{\mathfrak{I}} \neq \overline{\mathfrak{J}}$ tenemos que t es par. Por lo tanto, $\left[\dfrac{N(\mathfrak{I})}{d}\right] = \left[\dfrac{N(\mathfrak{J}^t)}{d}\right] = 1.$ □

Ejemplo 2.18. *Sea $\mathbb{F} = \mathbb{Q}(\sqrt{322})$, donde $322 = 2 \cdot 7 \cdot 23$. Del Teorema 2.4 tenemos que el rango de Cl_2 es 1. Aplicamos el Lema 2.11 con $t = 0, g = 2$. Encontraremos un ideal no principal $\mathfrak{q}_1$ cuya clase genera Cl_2. Para esto, necesitamos un primo q_1 tal que*

$$\left(\frac{4 \cdot 322}{q_1}\right) = 1 \quad y \quad \left[\frac{\pm q_1}{322}\right] = -1.$$

Siguiendo la prueba del Lema 2.11, es suficiente con que q_1 satisfaga

$$q_1 \equiv 5 \pmod 8, \quad \left(\frac{q_1}{7}\right) = \left(\frac{7}{q_1}\right) = -1, \quad \left(\frac{q_1}{23}\right) = \left(\frac{23}{q_1}\right) = 1. \tag{5}$$

Del Lema 2.6, tenemos que 325 satisface (5), pero no es primo. Del Teorema de Dirichlet sabemos que existe un primo $q_1 \equiv 325 \pmod{322}$, en este caso $q_1 = 325 + 1288 = 1613$

$$\langle 1613 \rangle = \langle 1613, 100 + \sqrt{322} \rangle \langle 1613, 100 - \sqrt{322} \rangle.$$

Por lo tanto $\overline{\mathfrak{q}_1} = \overline{\langle 1613, 100 + \sqrt{322} \rangle}$ genera Cl_2 y $o(\overline{\mathfrak{q}_1}) = 4$.

Ejemplo 2.19. *Sea $d = 272490 = 2 \cdot 5 \cdot 293 \cdot 3 \cdot 31$ y $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Para encontrar generadores apropiados de Cl_2, usamos el Lema 2.11 con $g = 4, t = 2$. Observemos que el rango de Cl_2 es 3. De acuerdo al Lema 2.8, necesitamos un primo racional q_1 tal que*

$$q_1 \equiv 5 \pmod 8, \quad \left(\frac{q_1}{5}\right) = -1, \quad \left(\frac{q_1}{293}\right) = \left(\frac{q_1}{3}\right) = \left(\frac{q_1}{31}\right) = 1.$$

Es suficiente que q_1 satisfaga

$$\begin{array}{ll} q_1 \equiv 5 & \pmod 8 \\ q_1 \equiv 3 & \pmod 5 \\ q_1 \equiv 1 & \pmod{27249} \end{array} \tag{6}$$

El primo $q_1 = 762973$ resuelve (6) y

$$\mathfrak{q}_1 = \langle 762973, 349636 + \sqrt{272490} \rangle$$

es un ideal primo tal que $N(\mathfrak{q}_1) = q_1$ y $o(\overline{\mathfrak{q}_1}) = 8$. De la misma forma encontramos $q_2 = 1895713$ y el ideal primo $\mathfrak{q}_2 = \langle 1895713, 507828 + \sqrt{272490} \rangle$ que satisfacen $N(\mathfrak{q}_2) = q_2, o(\overline{\mathfrak{q}_2}) = 8$. El primo $q_3 = 5674241$ y el ideal primo $\mathfrak{q}_3 = \langle 5674241, 1813618 + \sqrt{272490} \rangle$ satisfacen $N(\mathfrak{q}_3) = q_3, o(\overline{\mathfrak{q}_3}) = 8$. Por tanto, $Cl_2 = \langle \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_2}, \overline{\mathfrak{q}_3} \rangle$.

Las relaciones mínimas entre $\overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_2}, \overline{\mathfrak{q}_3}$ que aparecen en la Proposición 2.2 son

$$\overline{\mathfrak{q}_1}^{\,4} = \overline{\mathfrak{q}_2}^{\,4}, \qquad \overline{\mathfrak{q}_1}^{\,2} = \overline{\mathfrak{q}_3}^{\,2}, \qquad \overline{\mathfrak{q}_1}^{\,8} = \overline{\mathfrak{q}_2}^{\,8} = \overline{\mathfrak{q}_3}^{\,8} = \overline{\mathcal{O}_{\mathbb{F}}}.$$

Reemplazamos $\overline{\mathfrak{q}_2}$ por $\overline{\mathfrak{q}_1}^{\,(2^1-1)(2^0)}\mathfrak{q}_2 = \overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2}$ y $\overline{\mathfrak{q}_3}$ por $\overline{\mathfrak{q}_1}^{\,(2^2-1)(2^0)}\overline{\mathfrak{q}_3} = \overline{\mathfrak{q}_1}^{\,3}\,\overline{\mathfrak{q}_3}$. Ahora tenemos $Cl_2 = \langle \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2}, \overline{\mathfrak{q}_1}^{\,3}\,\overline{\mathfrak{q}_3} \rangle$, con $o(\overline{\mathfrak{q}_1}) = 8, o(\overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2}) = 4$ y $o(\overline{\mathfrak{q}_1}^{\,3}\,\overline{\mathfrak{q}_3}) = 2$. Continuando con el Algoritmo, verificamos que el conjunto de generadores de Cl_2 ya no se puede simplificar más. Por tanto

$$Cl_2 = \langle \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2}, \overline{\mathfrak{q}_1}^{\,3}\,\overline{\mathfrak{q}_3} \rangle \cong \langle \overline{\mathfrak{q}_1} \rangle \times \langle \overline{\mathfrak{q}_1}\,\overline{\mathfrak{q}_2} \rangle \times \langle \overline{\mathfrak{q}_1}^{\,3}\,\overline{\mathfrak{q}_3} \rangle \cong C_8 \times C_4 \times C_2.$$

2.3. Otros casos

Se pueden obtener resultados similares si $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$, con d entero positivo libre de cuadrados. En este caso, la norma de un elemento en $\mathbb{F}$ es positiva y por tanto usaremos $\left[\frac{N(\mathfrak{I})}{d}\right]$ en lugar de $\left[\frac{\pm N(\mathfrak{I})}{d}\right]$. Para construir $\mathcal{P}, \mathcal{I}_{\mathcal{P}}, \mathcal{J}_{\mathcal{P}}$ necesitaremos encontrar números primos como se indica a continuación:

1. Si $d = p_0 \cdots p_g$ es como en el Lema 2.7, podemos encontrar $g+1$ primos $q_0, \ldots, q_g$ tales que $\left(\frac{p_i}{q_i}\right) = -1$, $\left(\frac{p_j}{q_i}\right) = 1$ para $i \neq j$ y $q_i \equiv 3 \pmod 4$. En este caso $\left(\frac{-1}{d}\right) = -1$ y $\left(\frac{q_i}{p_i}\right) = -1$.
2. Si $d = 2\,p_1 \cdots p_g$ es como en el Lema 2.8 ó $d = p_0 p_1 \cdots p_g \equiv 3 \pmod 4$ como en el Lema 2.10, podemos encontrar g números primos tales que $\left(\frac{\delta_{\mathbb{F}}}{q_i}\right) = 1$ y $\left[\frac{q_i}{d}\right] = -1$. De hecho, podemos usar los mismos q_i's que encontramos en el caso real.
3. Si $d = p_0 p_1 \cdots p_g \equiv 1 \pmod 4$ es como en el Lema 2.9, entonces $-d \equiv 3 \pmod 4$ y $\delta_{\mathbb{F}} = -4d$. En este caso, podemos encontrar $g+1$ primos $q_0, \ldots, q_g$ tales que $\left(\frac{p_i}{q_i}\right) = -1$, $\left(\frac{p_j}{q_i}\right) = 1$ para $i \neq j$ y $q_i \equiv 3 \pmod 4$. Como $g \geq 1$, siempre tendremos un primo p_j tal que $\left(\frac{p_j}{q_i}\right) = 1$ y $\left(\frac{q_i}{p_j}\right) = -1$. Por tanto $\left[\frac{q_i}{d}\right] = -1$.
4. Si $d = 2\,p_1 \cdots p_g \equiv 1 \pmod 4$ es como en el Lema 2.11, existen g primos $q_1, \ldots, q_g$ tales que $\left(\frac{p_i}{q_i}\right) = -1$, $\left(\frac{p_j}{q_i}\right) = 1$ para $i \neq j$ y $q_i \equiv 5 \pmod 8$.

Con estos números primos definimos $\mathcal{P}$, $\mathcal{I}_{\mathcal{P}}$ y $\mathcal{J}_{\mathcal{P}}$ como en el caso real. Los Lemas 2.13, 2.14 y 2.16, Proposición 2.17 y los Teoremas 2.12 y 2.15 pueden ser generalizados quitando el signo menos de $\left[\frac{\pm N(\mathfrak{I})}{d}\right]$. En particular:

Proposición 2.20. *Sea $\mathbb{F}$ un campo cuadrático imaginario tal que $|Cl_{\mathbb{F}}| = 2^k$ para algún $k \in \mathbb{N}$ y $\overline{\mathfrak{I}} \in Cl_{\mathbb{F}}$ con $\text{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) = 1$. Entonces $\langle \overline{\mathfrak{I}} \rangle$ es maximal en $\mathcal{C}_{Cl_{\mathbb{F}}}$ si y sólo si $\left[\frac{N(\mathfrak{I})}{d}\right] = -1$.* □

Un caso particular de lo que hemos estudiado se da cuando el exponente de $Cl_{\mathbb{F}}$ es 2. El siguiente resultado se sigue del Teorema 2.15 y de su versión en campos imaginarios:

Corolario 2.21. *Sea $\mathbb{F}$ un campo cuadrático tal que $Cl_{\mathbb{F}}$ tiene exponente 2. Entonces $Cl_{\mathbb{F}} = \langle \mathcal{J}_{\mathcal{P}} \rangle$ con $\mathcal{J}_{\mathcal{P}}$ como en* (4) *y cada clase tiene un ideal de la forma $\prod_{\mathfrak{J} \in A} \mathfrak{J}$, para algún $A \subseteq \mathcal{J}_{\mathcal{P}}$, donde $\prod_{\mathfrak{J} \in \emptyset} \mathfrak{J} = \mathcal{O}_{\mathbb{F}}$ cuando $A = \emptyset$.* □

El siguiente resultado es muy importante, pues nos permite determinar si un ideal es o no principal en el anillo de enteros de un campo cuadrático real, que es uno de los objetivos principales de este capítulo. Además de la importancia que tiene por si sólo, utilizaremos esta afirmación más adelante para clasificar elementos primos e irreducibles cuando el número de clases es 2.

Teorema 2.22. *Sean $\mathbb{F}$ un campo cuadrático real tal que $Cl_{\mathbb{F}}$ tiene exponente 2 y $\mathfrak{I} \subseteq \mathcal{O}_{\mathbb{F}}$ un ideal tal que $\text{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) = 1$. Entonces $\mathfrak{I}$ no es principal si y sólo si $\left[\dfrac{\pm N(\mathfrak{I})}{d}\right] = -1$.*

DEMOSTRACIÓN. Toda clase tiene un representante de la forma $\mathfrak{I}_A = \prod_{\mathfrak{J}\in A} \mathfrak{J}$, para algún $\emptyset \neq A \subseteq \mathcal{J}_{\mathcal{P}}$. Por la afirmación 1 del Teorema 2.12 tenemos $\left[\dfrac{\pm N(\mathfrak{I}_A)}{d}\right] = -1$. Si un ideal $\mathfrak{I}$ satisface $\left[\dfrac{\pm N(\mathfrak{I})}{d}\right] = -1$, entonces por el Lema 2.13 todo ideal $\mathfrak{J}$ contenido en $\overline{\mathfrak{I}}$ tal que $\text{m.c.d.}\,(N(\mathfrak{J}), \delta_{\mathbb{F}}) = 1$ satisface $\left[\dfrac{\pm N(\mathfrak{J})}{d}\right] = -1$. Por tanto, todo ideal no principal cumple $\left[\dfrac{\pm N(\mathfrak{I})}{d}\right] = -1$. La afirmación inversa es válida en cualquier campo cuadrático real. □

La condición $\text{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) = 1$ es necesaria. Si $\text{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) > 1$, entonces puede existir un ideal no principal $\mathfrak{I}$ tal que $\left[\dfrac{N(\mathfrak{I})}{d}\right] = 1$ ó $\left[\dfrac{-N(\mathfrak{I})}{d}\right] = 1$. Por ejemplo, si $\mathbb{F} = \mathbb{Q}(\sqrt{10})$, entonces $\left[\dfrac{\pm 5}{10}\right] = 1$ pero $\langle 5, \sqrt{10}\rangle$ no es principal. Algo similar sucede en el caso imaginario.

Ejemplo 2.23. *Sea $\mathbb{F} = \mathbb{Q}(\sqrt{-665})$. Vamos a determinar Cl_2 de $\mathbb{F}$. Como $-665 = -(5)(7)(19) \equiv 3 \pmod 4$, entonces $\delta_{\mathbb{F}} = -2660$, $p_0 = 5$, $p_1 = 7$ y $p_2 = 19$. La siguiente tabla muestra los primeros primos $q \equiv 3 \pmod 4$ tales que $\left(\dfrac{\delta_{\mathbb{F}}}{q}\right) = 1$. En ésta podemos observar que $q_0 = 3$, $q_1 = 71$ y $q_2 = 131$ satisfacen las condiciones que necesitamos. En este caso $\mathfrak{p}_1 = \langle 3, 4 + \sqrt{-665}\rangle$, $\mathfrak{p}_2 = \langle 71, 20 + \sqrt{-665}\rangle$ y $\mathfrak{p}_3 = \langle 131, 11 + \sqrt{-665}\rangle$, $o(\mathfrak{p}_1) = o(\mathfrak{p}_2) = o(\mathfrak{p}_3) = 6$, $\mathcal{I}_{\mathcal{P}} = \{\mathfrak{p}_1^3, \mathfrak{p}_2^3, \mathfrak{p}_3^3\}$. Si aplicamos el Algoritmo, encontramos que $\mathcal{I}_{\mathcal{P}} = \mathcal{J}_{\mathcal{P}}$ y $Cl_2 \cong C_2 \times C_2 \times C_2$.*

q	$\left(\frac{\delta_F}{q}\right)$	$\left(\frac{5}{q}\right)$	$\left(\frac{7}{q}\right)$	$\left(\frac{19}{q}\right)$	$\left[\frac{q}{665}\right]$
3	**1**	**−1**	**1**	**1**	**−1**
23	1	−1	−1	−1	−1
43	1	−1	−1	−1	−1
71	**1**	**1**	**−1**	**1**	**−1**
79	1	1	−1	1	−1
103	1	−1	1	1	−1
131	**1**	**1**	**1**	**−1**	**−1**
139	1	1	1	−1	−1
151	1	1	−1	1	−1

Ejemplo 2.24. *Si* $\mathbb{F} = \mathbb{Q}(\sqrt{-21})$*, entonces* $Cl_{\mathbb{F}} \cong C_2 \times C_2$*; así, un ideal* $\mathfrak{I}$ *es principal si y sólo si* $\left[\frac{N(\mathfrak{I})}{21}\right] = 1$*. Por ejemplo,* $\langle 5, 2+\sqrt{-21}\rangle$ *no es un ideal principal pues* $N(\mathfrak{I}) = 5$ *y* $\left[\frac{5}{21}\right] = -1$*. El ideal* $\langle 37, 41+\sqrt{-21}\rangle$ *es principal ya que* $N(\mathfrak{I}) = 37$ *y* $4^2 \equiv 37 \pmod{21}$.

2.4. El campo de clases de Hilbert de algunos campos cuadráticos

En esta sección vamos a encontrar el campo de clases de Hilbert de campos cuadráticos cuyo grupo de clases de ideales tiene exponente 2. En [**8**] Proposition 1.2, H. Cohen y X. Roblot afirman que si $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d > 0$ y $h_{\mathbb{F}} = 2$, entonces existe un divisor d_2 de $\delta_{\mathbb{F}}$ con $1 < d_2 < \delta_{\mathbb{F}}$ y $d_2 \equiv 0, 1 \pmod 4$ tal que $\mathbb{H}_{\mathbb{F}} = \mathbb{F}(\sqrt{d_2})$. El problema es encontrar d_2. Ellos afirman que, usando teoría de géneros o teoría de Kummer, se puede encontrar d_2 en un número finito de pasos. Nosotros daremos una prueba de este resultado en la que hallamos explícitamente d_2. Terminaremos la sección generalizando este resultado cuando el grupo de clases tiene exponente 2 incluyendo el caso imaginario.

Como consecuencia inmediata del Teorema de Gauss sobre el 2-rango de $Cl_{\mathbb{F}}$ (Teorema 2.4) tenemos:

Proposición 2.25. *Sea* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *con* $h_{\mathbb{F}} = 2$*. Entonces, para algunos* p, q, r *primos racionales positivos impares,* d *es de alguna de las siguientes formas:*

1. $d = 2\,p$ *con* $p \equiv 1 \pmod 4$.
2. $d = p\,q$ *con* $p \equiv q \equiv 1 \pmod 4$.
3. $d = p\,q$ *con* $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$.
4. $d = 2\,p\,q$ *con* $p \equiv q \equiv 3 \pmod 4$.
5. $d = 2\,p\,q$ *con* $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$.
6. $d = p\,q\,r$ *con* $p \equiv 1 \pmod 4$, $q \equiv r \equiv 3 \pmod 4$.
7. $d = -p$ *con* $p \equiv 1 \pmod 4$.
8. $d = -2\,p$.
9. $d = -p\,q$ *con* $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$. □

En cada uno de los casos que describe la proposición anterior, sólo hay una manera de factorizar $d = d_1\, d_2$ de tal forma que $d_1, d_2 \neq 1$, $d_2 \equiv 1 \pmod 4$ y donde al menos uno de los factores es positivo:

1. $d_1 = 2$, $d_2 = p$.
2. $d_1 = p$, $d_2 = q$.
3. $d_1 = q$, $d_2 = p$.
4. $d_1 = 2$, $d_2 = p\, q$.
5. $d_1 = 2\, q$, $d_2 = p$.
6. $d_1 = p$, $d_2 = q\, r$.
7. $d_1 = -1$, $d_2 = p$.
8. $d_1 = -2, d_2 = p$ si $p \equiv 1 \pmod 4$ y $d_1 = 2, d_2 = -p$ si $p \equiv 3 \pmod 4$.
9. $d_1 = -q$, $d_2 = p$.

Teorema 2.26. *Sean $d = d_1\, d_2$, $d_2 \equiv 1 \pmod 4$, $d_1, d_2 \neq 1$ y $d_1 > 0$ ó $d_2 > 0$. Si $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $h_{\mathbb{F}} = 2$, entonces $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.*

DEMOSTRACIÓN. Sea $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Notemos que $\left\{1, \dfrac{1+\sqrt{d_2}}{2}\right\}$ y $\{1, \sqrt{d_1}\}$ son bases de $\mathbb{K}/\mathbb{F}$ formadas por enteros algebraicos. Sabemos que $\Delta(\{1, \sqrt{d_1}\}) = 4d_1$ y $\Delta\left(\left\{1, \dfrac{1+\sqrt{d_2}}{2}\right\}\right) = d_2$, más aún $\text{m.c.d.}\,(4d_1, d_2) = \text{m.c.d.}\,(d_1, d_2) = 1$. Entonces, $\delta_{\mathbb{K}/\mathbb{F}} = \mathcal{O}_{\mathbb{F}}$ y $\mathbb{K}/\mathbb{F}$ es una extensión no ramificada, incluyendo los primos al infinito. Por tanto $\mathbb{H}_{\mathbb{F}} = \mathbb{K}$. □

Teorema 2.27. *Sean $d = p_0 \cdots p_g$ un entero racional libre de cuadrados, $p_i > 0$ primo para todo i y $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ tal que $Cl_{\mathbb{F}}$ tiene exponente 2.*

1. *Si $p_i \equiv 1, 2 \pmod 4$ para todo i, entonces $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_g})$.*
2. *Si $p_0 = 2$, $p_1 \equiv 3 \pmod 4$ y $p_i \equiv 1 \pmod 4$ para $i \geq 2$, entonces $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{2\, p_1}, \sqrt{p_2}, \ldots, \sqrt{p_g})$.*
3. *Si $d \equiv 1, 2 \pmod 4$ y para algún $0 \leq t < g$ tenemos que $p_0, \ldots, p_{t-1} \equiv 1, 2 \pmod 4$, $p_t, \ldots, p_g \equiv 3 \pmod 4$, entonces el campo de clases de Hilbert de $\mathbb{F}$ es $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_{t-1}}, \sqrt{p_g p_t}, \sqrt{p_g p_{t+1}}, \ldots, \sqrt{p_g p_{g-1}})$. Observemos que debe haber al menos dos primos congruentes con 3 módulo 4 y el caso $t = 0$ significa que $p_i \equiv 3 \pmod 4$ para $i = 0, \ldots, g$.*
4. *Si $d \equiv 3 \pmod 4$, entonces $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_g})$.*

DEMOSTRACIÓN. Solamente probaremos la primera afirmación. Para $i = 1, \ldots, g$ consideremos los campos $\mathbb{L}_i = \mathbb{F}(\sqrt{p_i})$. Usando las ideas de la prueba del Teorema 2.26, es fácil mostrar que $\mathbb{L}_i/\mathbb{F}$ es una extensión no ramificada. Como $\mathbb{L}_i/\mathbb{F}$ son no ramificadas y $\mathbb{L}_i \cap \mathbb{L}_j = \mathbb{F}$ para $i \neq j$, entonces $\mathbb{L}_1 \cdots \mathbb{L}_g/\mathbb{F}$ es no ramificada como consecuencia de la proposición 1.18. Finalmente, por el Teorema de Gauss del 2-rango de un campo cuadrático, $[\mathbb{L}_1 \cdots \mathbb{L}_g : \mathbb{F}] = 2^{g-1} = o(Cl_{\mathbb{F}})$. Por lo tanto, $\mathbb{H}_{\mathbb{F}} = \mathbb{L}_1 \cdots \mathbb{L}_g$. Las otras afirmaciones se prueban de forma análoga. □

El siguiente resultado es la versión imaginaria del teorema anterior. La prueba es similar a la del caso real.

Teorema 2.28. *Sean $d = -p_0 \cdots p_g$ un entero libre de cuadrados con p_i primos racionales positivos y $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ tal que el exponente de $Cl_{\mathbb{F}}$ es 2:*

1. *Si $d \equiv 1 \pmod 4$, donde $p_0, \ldots, p_{t-1} \equiv 1 \pmod 4$, $p_t, \ldots, p_g \equiv 3 \pmod 4$ para algún $0 \leq t \leq g+1$, entonces $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{p_0}, \ldots, \sqrt{p_{t-1}}, \sqrt{-p_t}, \ldots, \sqrt{-p_g})$. El caso $t = g+1$ significa que no hay primos congruentes con 3 módulo 4.*
2. *Si $d \equiv 2 \pmod 4$, donde $p_0 = 2$, $p_1, \ldots, p_{t-1} \equiv 1 \pmod 4$, $p_t, \ldots, p_g \equiv 3 \pmod 4$ para algún $1 \leq t \leq g+1$, entonces*

$$\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{\pm 2}, \sqrt{p_1}, \ldots, \sqrt{p_{t-1}}, \sqrt{-p_t}, \ldots, \sqrt{-p_g}),$$

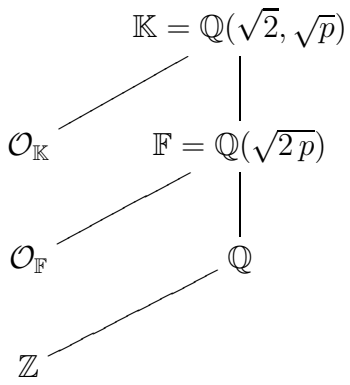
   donde el signo de 2 es $+$ si $d/2 \equiv 1 \pmod 4$ y $-$ si $d/2 \equiv 3 \pmod 4$.
3. *Si $d \equiv 3 \pmod 4$, entonces $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{-1}, \sqrt{p_0}, \ldots, \sqrt{p_g})$.* □

2.5. Ideales principales y ecuaciones diofantinas

A partir de esta sección vamos a demostrar de forma distinta algunos resultados que estudiamos anteriormente. Aunque este método solamente funciona para un número restringido de casos, es interesante pues vamos a obtener relaciones entre la clase de ideales $\overline{\mathfrak{I}}$ y la ecuación diofantina $d_1\, b_1^2 - d_2\, b_2^2 = \pm s^2 N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I})$, donde las variables son b_1 y b_2. En este trabajo, cuando digamos que una ecuación diofantina de la forma $f(b_1, b_2) = \pm c$, es soluble nos referiremos a que tiene solución para al menos uno de los dos signos, en algunos casos la ecuación será soluble para los dos signos y en otras ocasiones solamente para uno de los dos.

Sea $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ un campo cuadrático con $h_{\mathbb{F}} = 2$. Como vimos en la sección anterior, existen $d_1, d_2 \in \mathbb{Z}$ con $d_2 \equiv 1 \pmod 4$ tales que $d = d_1\, d_2$ y al menos uno es positivo. Como todos los primos que dividen a d_1 ó d_2 se ramifican en $\mathbb{F}$, entonces existen $\mathfrak{d}_1, \mathfrak{d}_2$ ideales tales que $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_1) = |d_1|$ y $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_1) = |d_2|$. Es claro que $\mathfrak{d}_1, \mathfrak{d}_2$ son únicos. Como $\mathfrak{d}_1\mathfrak{d}_2 = \left\langle \sqrt{d} \right\rangle_{\mathbb{F}}$, entonces ambos ideales son principales o ambos son no principales. De la igualdad anterior se ve que $\overline{\mathfrak{d}_2} = \overline{\mathfrak{d}_1}^{-1}$ y como $\mathfrak{d}_1^2 = \langle d_1 \rangle_{\mathbb{F}}$, entonces $\overline{\mathfrak{d}_1} = \overline{\mathfrak{d}_1}^{-1}$, por lo tanto $\overline{\mathfrak{d}_1} = \overline{\mathfrak{d}_2}$.

Primero trabajaremos el caso $d = 2\,p$, $0 < p \equiv 5 \pmod 8$ un primo racional, donde se tiene un criterio muy sencillo para identificar ideales principales y no principales. Sean $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$, $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ el campo de clases de Hilbert de $\mathbb{F}$ y $\mathcal{O}_{\mathbb{F}}, \mathcal{O}_{\mathbb{K}}$ los anillos de enteros respectivamente. Es claro que $\mathcal{O}_{\mathbb{F}} = \mathbb{Z} + \sqrt{2\,p}\,\mathbb{Z}$.



Como $2 \mid \delta_{\mathbb{F}}$, entonces $\langle 2\rangle_{\mathbb{F}}$ se ramifica y si $\mathfrak{p}_2 = \left\langle 2, \sqrt{2\,p}\right\rangle_{\mathbb{F}}$, entonces $\langle 2\rangle_{\mathbb{F}} = \mathfrak{p}_2^2$. Tenemos $p \equiv 5 \pmod 8$ así que $\left(\dfrac{2}{p}\right) = \left[\dfrac{2}{p}\right] = \left[\dfrac{2}{2\,p}\right] = -1$, de esto $\mathfrak{p}_2$ es un ideal no principal y, como $\mathfrak{p}_2^2$ es principal, entonces $h_{\mathbb{F}}$ es par. A partir de ahora estudiaremos el caso $h_{\mathbb{F}} = 2$.

Lema 2.29. *Sean* $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ *con* $0 < p \equiv 5 \pmod 8$, $h_{\mathbb{F}} = 2$ *y* $\mathfrak{p}_2 = \left\langle 2, \sqrt{2\,p}\right\rangle_{\mathbb{F}}$.

1. $\langle \mathfrak{p}_2\rangle_{\mathbb{K}} = \left\langle \sqrt{2}\right\rangle_{\mathbb{K}}$.
2. *Si* $\mathfrak{J}_{\mathbb{F}}$ *es un ideal no principal de* $\mathcal{O}_{\mathbb{F}}$, *entonces existe* $B = b_1\sqrt{2} + b_2\sqrt{p} \in \mathcal{O}_{\mathbb{K}}$ *tal que* $b_1, b_2 \in \mathbb{Z}$ *y* $\langle \mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle B\rangle_{\mathbb{K}}$.

DEMOSTRACIÓN. Claramente $\langle \mathfrak{p}_2\rangle_{\mathbb{K}} = \left\langle 2, \sqrt{2\,p}\right\rangle_{\mathbb{K}}$. En $\mathcal{O}_{\mathbb{K}}$, $\sqrt{2} \mid 2$ y $\sqrt{2} \mid \sqrt{2\,p}$, por lo que $\left\langle \sqrt{2}\right\rangle_{\mathbb{K}} \mid \langle \mathfrak{p}_2\rangle_{\mathbb{K}}$. Por un lado, como consecuencia de la Proposición 1.21 tenemos

$$N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{2}\right) = N_{\mathbb{F}/\mathbb{Q}}\left(N_{\mathbb{K}/\mathbb{F}}\left(\sqrt{2}\right)\right) = N_{\mathbb{F}/\mathbb{Q}}\left(-2\right) = 4, \tag{7}$$

mientras que

$$N_{\mathbb{K}/\mathbb{Q}}\left(\langle \mathfrak{p}_2\rangle_{\mathbb{K}}\right) = N_{\mathbb{F}/\mathbb{Q}}\left(N_{\mathbb{K}/\mathbb{F}}\left(\langle \mathfrak{p}_2\rangle_{\mathbb{K}}\right)\right) = N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{p}_2{}^2\right) = N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{p}_2\right)^2 = 4 \tag{8}$$

por la Proposición 1.23. Ahora, la afirmación 1 se sigue de (7) y (8).

Como $h_{\mathbb{F}} = 2$, entonces $\overline{\mathfrak{p}_2} = \overline{\mathfrak{J}_{\mathbb{F}}}$ y el producto $\mathfrak{p}_2\mathfrak{J}_{\mathbb{F}}$ es principal, digamos $\mathfrak{p}_2\mathfrak{J}_{\mathbb{F}} = \langle A\rangle_{\mathbb{F}}$. Si consideramos la igualdad en $\mathbb{K}$ obtenemos

$$\langle A\rangle_{\mathbb{K}} = \langle \mathfrak{p}_2\rangle_{\mathbb{K}}\,\langle \mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \left\langle \sqrt{2}\right\rangle_{\mathbb{K}}\langle \mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}\,.$$

El campo $\mathbb{K}$ es el campo de clases de Hilbert de $\mathbb{F}$, entonces $\langle \mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}$ debe de ser un ideal principal, digamos $\langle \mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle \beta\rangle_{\mathbb{K}}$. Por lo anterior

$$\left\langle \sqrt{2}\right\rangle_{\mathbb{K}}\langle \beta\rangle_{\mathbb{K}} = \left\langle \sqrt{2}\beta\right\rangle_{\mathbb{K}} = \langle A\rangle_{\mathbb{K}}\,,$$

lo que nos indica $\sqrt{2}\,\beta\,\mu = A$ para alguna unidad $\mu \in \mathcal{O}_{\mathbb{K}}$ y $A = a_1 + a_2\sqrt{2\,p}$. Ya que $\langle \beta\rangle_{\mathbb{K}} = \langle \mu\,\beta\rangle_{\mathbb{K}}$ podemos suponer

$$\sqrt{2}\,\beta = A = a_1 + a_2\sqrt{2\,p}.$$

De la igualdad anterior tenemos $\sqrt{2} \mid A$ y, como $\sqrt{2} \mid a_2\sqrt{2\,p}$, entonces $\sqrt{2} \mid a_1$, donde $a_1 \in \mathbb{Z}$ y así a_1 debe ser par. Entonces

$$\sqrt{2}\,\beta = 2\frac{a_1}{2} + a_2\,\sqrt{p}\,\sqrt{2} = \sqrt{2}\left(\frac{a_1}{2}\sqrt{2} + a_2\sqrt{p}\right),$$

donde $\dfrac{a_1}{2}, a_2 \in \mathbb{Z}$. Así, para cada ideal no principal $\mathfrak{J}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ existe un elemento de la forma $b_1\sqrt{2} + b_2\sqrt{p} \in \mathcal{O}_{\mathbb{K}}$ donde $b_1, b_2 \in \mathbb{Z}$ tal que $\langle \mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \left\langle b_1\sqrt{2} + b_2\sqrt{p}\right\rangle_{\mathbb{K}}$. Lo anterior prueba 2. □

Observemos que si $\beta = b_1\sqrt{2} + b_2\sqrt{p}$ y $\mathfrak{J}_{\mathbb{F}}$ es un ideal de $\mathcal{O}_{\mathbb{F}}$ tal que $\langle \mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle \beta\rangle_{\mathbb{K}}$, entonces

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}\left(\beta\right) &= (b_1\sqrt{2} + b_2\sqrt{p})(b_1\sqrt{2} - b_2\sqrt{p})(-b_1\sqrt{2} + b_2\sqrt{p})(-b_1\sqrt{2} - b_2\sqrt{p}) \\ &= (2b_1^2 - pb_2^2)^2. \end{aligned}$$

Por otro lado, $N_{\mathbb{K}/\mathbb{Q}}\left(\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}\right) = \left(N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{J}_{\mathbb{F}}\right)\right)^2$ y así $|2\,b_1^2 - p\,b_2^2| = N_{\mathbb{F}/\mathbb{Q}}\left(\mathfrak{J}_{\mathbb{F}}\right)$. De esto, podemos ver que si $\mathfrak{J}_{\mathbb{F}}$ es un ideal no principal, entonces, $2\,b_1^2 - p\,b_2^2 = \pm N_{\mathbb{F}}(\mathfrak{J}_{\mathbb{F}})$ tiene solución entera en las variables b_1, b_2 para al menos uno de los signos. Además, en cualquier campo cuadrático real $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, si $\mathfrak{J}_{\mathbb{F}}$ es un ideal principal de $\mathcal{O}_{\mathbb{F}}$, entonces una de las ecuaciones $b_1^2 - d\,b_2^2 = \pm N(\mathfrak{J}_{\mathbb{F}})$ debe de tener solución entera.

Proposición 2.30. *Sean $d \equiv 5 \pmod 8$ un entero racional, $c \in \mathbb{N}$ impar y b_1, b_2, b_3, b_4 variables. Consideremos las ecuaciones:*

1. $b_1^2 - 2\,d\,b_2^2 = \pm c$.
2. $2\,b_3^2 - d\,b_4^2 = \pm c$.

No es posible que tanto 1 *como* 2 *sean solubles simultáneamente.*

DEMOSTRACIÓN. Como $d \equiv 5 \pmod 8$, $-2\,d \equiv 6 \pmod 8$. Los cuadrados módulo 8 son $0, 1, 4$, estos valores multiplicados por 6 son $0, 6, 0$ módulo 8. Con esto en mente, los posibles valores impares de $b_1^2 - 2\,d\,b_2^2 \equiv b_1^2 + 6\,b_2^2 \pmod 8$ son ± 1. Haciendo un procedimiento similar, los únicos valores impares que puede tomar $2\,b_3^2 - d\,b_4^2 \equiv 2\,b_3^2 + 3\,b_4^2 \pmod 8$ módulo 8 son ± 3. Por tanto, la proposición es cierta. □

De la prueba anterior se puede concluir que:

Teorema 2.31. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ un campo cuadrático real con número de clases 2 con $p \equiv 5 \pmod 8$ un primo racional y $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros. Si $\mathfrak{J}_{\mathbb{F}}$ es un ideal de $\mathcal{O}_{\mathbb{F}}$ con $N(\mathfrak{J}_{\mathbb{F}})$ impar, entonces:*

1. *$\mathfrak{J}_{\mathbb{F}}$ es principal si y sólo si al menos una de las ecuaciones $b_1^2 - 2\,p\,b_2^2 = \pm N(\mathfrak{J}_{\mathbb{F}})$ tiene solución con $b_1, b_2 \in \mathbb{Z}$.*
2. *$\mathfrak{J}_{\mathbb{F}}$ es un ideal no principal si y sólo si existe una solución de $2\,b_1^2 - p\,b_2^2 = \pm N(\mathfrak{J}_{\mathbb{F}})$ con $b_1, b_2, \in \mathbb{Z}$.*
3. *$\mathfrak{J}_{\mathbb{F}}$ es un ideal principal si y sólo si $N(\mathfrak{J}_{\mathbb{F}}) \equiv \pm 1 \pmod 8$.* □

Si un ideal $\mathfrak{J}_{\mathbb{F}}$ tiene norma par, lo podemos factorizar como $\mathfrak{J}_{\mathbb{F}} = \mathfrak{p}_2^k \mathfrak{J}_{\mathbb{F}}{}'$, donde $\mathfrak{J}_{\mathbb{F}}{}'$ tiene norma impar y $\mathfrak{p}_2$ es el único ideal de $\mathcal{O}_{\mathbb{F}}$ con norma 2. Si k es par, el ideal es principal si y sólo si $\mathfrak{J}_{\mathbb{F}}{}'$ es principal. Si k es impar, entonces $\mathfrak{J}_{\mathbb{F}}$ es principal si y sólo si $\mathfrak{J}_{\mathbb{F}}{}'$ no es principal.

Teorema 2.32. *Sea $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ un campo cuadrático real con $h_{\mathbb{F}} = 2$, $p \equiv 5 \pmod 8$, $\mathcal{O}_{\mathbb{F}}$ su anillo de enteros y $\mathfrak{J}_{\mathbb{F}}$ un ideal de $\mathcal{O}_{\mathbb{F}}$ con $N(\mathfrak{J}_{\mathbb{F}})$ par. Si $\mathfrak{J}_{\mathbb{F}} = \mathfrak{p}_2^k \mathfrak{J}_{\mathbb{F}}{}'$ como antes, entonces $\mathfrak{J}_{\mathbb{F}}$ es principal si y sólo si una de los siguientes afirmaciones es cierta:*

1. *k es par y $N(\mathfrak{J}_{\mathbb{F}}{}') \equiv \pm 1 \pmod 8$.*
2. *k es impar y $N(\mathfrak{J}_{\mathbb{F}}{}') \equiv \pm 3 \pmod 8$.* □

Resumiendo lo anterior, cuando $d = 2\,p > 0$ con $p \equiv 5 \pmod 8$ y $h_{\mathbb{F}} = 2$, si $\mathfrak{J}_{\mathbb{F}}$ un ideal de $\mathcal{O}_{\mathbb{F}}$ es principal con norma impar, entonces $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}$ tiene un generador de la forma $a_1 + a_2\sqrt{d}$, y si el ideal no es principal, éste sera $a_1\sqrt{d_1} + a_2\sqrt{d_2}$. Nos referiremos a los elementos de la forma $a_1 + a_2\sqrt{d}$ como elementos tipo 1 y los elementos tipo 2 serán los que tengan la forma $a_1\sqrt{d_1} + a_2\sqrt{d_2}$. A continuación vamos a ver cuándo se puede

generalizar este resultado y qué sucede en el resto de los casos, para esto es importante ver lo que sucede cuando se multiplican elementos de esta forma, en particular, si $d = d_1\, d_2$:

$$(a_1 + a_2\sqrt{d})(a_3\sqrt{d_1} + a_4\sqrt{d_2}) = (a_1\, a_3 + a_2\, a_4\, d_2)\sqrt{d_1} + (a_1\, a_4 + a_2\, a_3\, d_1)\sqrt{d_2},$$

$$(a_1\sqrt{d_1} + a_2\sqrt{d_2})(a_3\sqrt{d_1} + a_4\sqrt{d_2}) = (a_1\, a_3\, d_1 + a_2\, a_4\, d_2) + (a_1\, a_4 + a_2\, a_3)\sqrt{d},$$

estos productos son congruentes con el hecho de que el producto de un ideal principal por uno no principal es no principal, mientras que el producto de dos ideales no principales da como resultado uno que sí es principal. También observemos que $\mathfrak{d}_1^2 = \langle d_1\rangle_{\mathbb{F}}$ y $\left\langle\sqrt{d_1}\right\rangle_{\mathbb{K}}^2 = \langle d_1\rangle_{\mathbb{K}}$, lo que implica que $\langle\mathfrak{d}_1\rangle_{\mathbb{K}}^2 = \left\langle\sqrt{d_1}\right\rangle_{\mathbb{K}}^2$, por la factorización única de ideales, $\langle\mathfrak{d}_1\rangle_{\mathbb{K}} = \left\langle\sqrt{d_1}\right\rangle_{\mathbb{K}}$. Análogamente, $\langle\mathfrak{d}_2\rangle_{\mathbb{K}} = \left\langle\sqrt{d_2}\right\rangle_{\mathbb{K}}$. Observemos que en algunos casos es posible que $a_1, a_2 \notin \mathbb{Z}$, pero $a_1 + a_2\sqrt{d}$ ó $a_1\sqrt{d_1} + a_2\sqrt{d_2}$ sí sean enteros algebraicos, por ejemplo, si $d \equiv 1 \pmod 4$, entonces $\dfrac{1+\sqrt{d}}{2}$ es un entero algebraico.

Proposición 2.33. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d = d_1\, d_2$ libre de cuadrados, $d_1, d_2 \in \mathbb{Z}$ y $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Si $\mathfrak{I}_{\mathbb{F}}, \mathfrak{J}_{\mathbb{F}}$ son ideales de $\mathcal{O}_{\mathbb{F}}$ tales que $\langle\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ y $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$ con $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ elementos del tipo 2, entonces $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{J}_{\mathbb{F}}}$ en $Cl_{\mathbb{F}}$.*

DEMOSTRACIÓN. Sean $\mathfrak{d}_1, \mathfrak{d}_2$ los únicos ideales de $\mathcal{O}_{\mathbb{F}}$ con normas $|d_1|, |d_2|$ respectivamente. Multipliquemos $\langle\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ y $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$ por $\sqrt{d_1}$. Como α, β y $\sqrt{d_1}$ son elementos del tipo 2, entonces $\alpha\sqrt{d_1}$ y $\beta\sqrt{d_2}$ son elementos del tipo 1, es decir, $\langle\mathfrak{I}_{\mathbb{F}}\mathfrak{d}_1\rangle_{\mathbb{K}}$ y $\langle\mathfrak{J}_{\mathbb{F}}\mathfrak{d}_1\rangle_{\mathbb{K}}$ tienen generadores del tipo 1, lo que indica que $\mathfrak{I}_{\mathbb{F}}\mathfrak{d}_1$ y $\mathfrak{J}_{\mathbb{F}}\mathfrak{d}_1$ son principales en $\mathcal{O}_{\mathbb{F}}$, es decir, están relacionados. Por lo anterior, existen $A, B \in \mathcal{O}_{\mathbb{F}}$ tales que $A\,\mathfrak{I}_{\mathbb{F}}\,\mathfrak{d}_1 = B\,\mathfrak{J}_{\mathbb{F}}\,\mathfrak{d}_1$. Por la ley de la cancelación, $A\,\mathfrak{I}_{\mathbb{F}} = B\,\mathfrak{J}_{\mathbb{F}}$ y $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{J}_{\mathbb{F}}}$. □

Proposición 2.34. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d = d_1\, d_2$ libre de cuadrados, $d_1, d_2 \in \mathbb{Z}$ y $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Si $\mathfrak{I}_{\mathbb{F}}, \mathfrak{J}_{\mathbb{F}}$ son dos ideales de $\mathcal{O}_{\mathbb{F}}$ tales que $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{J}_{\mathbb{F}}}$ en $Cl_{\mathbb{F}}$ y $\langle\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ con $\alpha \in \mathcal{O}_{\mathbb{K}}$ un elementos del tipo 2, entonces existe $\beta \in \mathcal{O}_{\mathbb{K}}$ del tipo 2 tal que $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$.*

DEMOSTRACIÓN. Como $\mathfrak{I}_{\mathbb{F}}$ y $\mathfrak{J}_{\mathbb{F}}$ están relacionados, entonces existen $A, B \in \mathcal{O}_{\mathbb{F}}$ tales que $A\mathfrak{I}_{\mathbb{F}} = B\mathfrak{J}_{\mathbb{F}}$. Así, $\langle A\mathfrak{I}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle A\,\alpha\rangle_{\mathbb{K}} = \langle B\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}$. De la igualdad anterior, $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}}$ debe de ser un ideal principal, digamos $\langle\mathfrak{J}_{\mathbb{F}}\rangle_{\mathbb{K}} = \langle\beta\rangle_{\mathbb{K}}$ para algún $\beta \in \mathcal{O}_{\mathbb{K}}$. Por lo anterior, existe $\mu \in \mathcal{O}_{\mathbb{K}}$ unidad tal que $A\,\alpha = B\,\beta\,\mu$. Podemos suponer que $\beta = \beta\mu$ y $A\,\alpha = B\,\beta$. Despejando,

$$\beta = \frac{A}{B}\alpha,$$

donde $\dfrac{A}{B} \in \mathbb{K}$ es del tipo 1 y α del tipo 2. Aunque uno de los elementos no necesariamente es un entero algebraico, se sigue cumpliendo que el producto de ellos es del tipo 2 y β es el valor que buscamos. □

Como $\langle\mathfrak{d}_1\rangle_{\mathbb{K}} = \left\langle\sqrt{d_1}\right\rangle_{\mathbb{K}}$, entonces siempre existe una clase de $Cl_{\mathbb{F}}$ con un ideal que al extenderlo a $\mathcal{O}_{\mathbb{K}}$ tiene un generador del tipo 2. Por los resultados anteriores, para cada factorización $d = d_1\, d_2$ tenemos una clase relacionada a los elementos del tipo 2 que surgen con estos números. Sin embargo, estas clases no necesariamente son distintas, es

posible que una misma clase de ideales corresponda a los elementos del tipo 2 de dos factorizaciones distintas de d, como de hecho se puede ver en el Corolario 2.36. El siguiente resultado nos muestra que este criterio es más fuerte, no sólo nos ayuda a identificar ideales de $\mathcal{O}_{\mathbb{F}}$ que están relacionados con $\mathfrak{d}_1$ y $\mathfrak{d}_2$, sino que además sirve para clasificar los ideales de $\mathcal{O}_{\mathbb{K}}$ que al bajarlos a $\mathcal{O}_{\mathbb{F}}$ están relacionados con esta pareja de ideales.

Proposición 2.35. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d = d_1\, d_2$ libre de cuadrados, $d_1, d_2 \in \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ y $\mathfrak{d}_1, \mathfrak{d}_2$ los únicos ideales de $\mathcal{O}_{\mathbb{F}}$ con normas $|d_1|, |d_2|$ respectivamente. Si $\mathfrak{I}_{\mathbb{K}} = \langle \alpha \rangle_{\mathbb{K}}$ es un ideal de $\mathcal{O}_{\mathbb{K}}$ con $\alpha = a_1\sqrt{d_1} + a_2\sqrt{d_2}$, $a_1, a_2 \in \mathbb{Q}$, entonces $\mathfrak{I}_{\mathbb{F}} = \mathfrak{I}_{\mathbb{K}} \cap \mathbb{F}$ es un ideal tal que $\overline{\mathfrak{I}_{\mathbb{F}}} = \overline{\mathfrak{d}_1} = \overline{\mathfrak{d}_2}$.*

DEMOSTRACIÓN. Sean $\beta_1 = \alpha\sqrt{d_1}, \beta_2 = \alpha\sqrt{d_2} \in \mathcal{O}_{\mathbb{F}}$. Consideremos el ideal $\mathfrak{J}_{\mathbb{K}} = \langle \beta_1, \beta_2 \rangle_{\mathbb{K}}$. Sabemos que $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{J}_{\mathbb{K}}) \mid \text{m.c.d.}\left(N_{\mathbb{K}/\mathbb{Q}}(\beta_1), N_{\mathbb{K}/\mathbb{Q}}(\beta_2)\right)$. Como d_1 y d_2 son primos relativos, entonces $N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{d_1}\right)$ y $N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{d_2}\right)$ también lo son, por las definiciones de β_1 y β_2. Lo anterior implica que $\text{m.c.d.}\left(N_{\mathbb{K}/\mathbb{Q}}(\beta_1), N_{\mathbb{K}/\mathbb{Q}}(\beta_2)\right) = |N_{\mathbb{K}/\mathbb{Q}}(\alpha)|$ y consecuentemente $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{J}_{\mathbb{K}}) \mid N_{\mathbb{K}/\mathbb{Q}}(\alpha)$. Como además $\alpha \mid \mathfrak{J}_{\mathbb{K}}$, entonces $\mathfrak{I}_{\mathbb{K}} = \mathfrak{J}_{\mathbb{K}}$, es decir $\langle \alpha \rangle_{\mathbb{K}} = \langle \beta_1, \beta_2 \rangle_{\mathbb{K}}$. Sabemos que $\beta_1, \beta_2 \in \mathcal{O}_{\mathbb{F}}$, así que, por el Corolario 1.11, $\mathfrak{I}_{\mathbb{F}} = \mathfrak{I}_{\mathbb{K}} \cap \mathbb{F} = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}}$, que al subirlo a $\mathcal{O}_{\mathbb{K}}$ es $\mathfrak{I}_{\mathbb{K}} = \langle \alpha \rangle_{\mathbb{K}}$, así que, por la Proposición 2.33, $\mathfrak{I}_{\mathbb{F}}$ está relacionado con $\mathfrak{d}_1$ y $\mathfrak{d}_2$. □

Los siguientes corolarios generalizan lo que hallamos para el caso $d = 2\,p$. Observemos que si $d \equiv 1 \pmod 4$, entonces una base entera de $\mathcal{O}_{\mathbb{F}}$ es $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ y como cualquier entero algebraico del tipo 2 multiplicado por $\sqrt{d_1}$ y por $\sqrt{d_2}$ debe de estar en $\mathcal{O}_{\mathbb{F}}$, entonces en este caso puede haber elementos de la forma $\dfrac{a_1\sqrt{d_1} + a_2\sqrt{d_2}}{2}$ con $a_1, a_2 \in \mathbb{Z}$ impares. Por lo anterior, en este caso es necesario incluir un 4 en el lado derecho de las ecuaciones diofantinas que usaremos a continuación.

Corolario 2.36. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d = d_1\, d_2$ libre de cuadrados, $h_{\mathbb{F}} = 2$, $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $\mathfrak{d}_1, \mathfrak{d}_2$ los únicos ideales de $\mathcal{O}_{\mathbb{F}}$ con $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_1) = |d_1|$ y $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_2) = |d_2|$ y $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ un ideal. Si $\mathfrak{d}_1, \mathfrak{d}_2$ son principales, entonces $\mathfrak{I}_{\mathbb{F}}$ es un ideal principal si y sólo si existe una solución de $d_1\, b_1^2 - d_2\, b_2^2 = \pm s^2\, N(\mathfrak{I}_{\mathbb{F}})$ con $b_1, b_2 \in \mathbb{Z}$ donde $s = 1$ si $d \equiv 2, 3 \pmod 4$ ó $s = 2$ si $d \equiv 1 \pmod 4$.* □

Corolario 2.37. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d = d_1\, d_2$ libre de cuadrados, $h_{\mathbb{F}} = 2$, $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $\mathfrak{d}_1, \mathfrak{d}_2$ los únicos ideales de $\mathcal{O}_{\mathbb{F}}$ con $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_1) = |d_1|$ y $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_2) = |d_2|$, $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ un ideal y $s = 1$ si $d \equiv 2, 3 \pmod 4$ ó $s = 2$ si $d \equiv 1 \pmod 4$. Si $\mathfrak{d}_1, \mathfrak{d}_2$ son no principales, entonces:*

1. *$\mathfrak{I}_{\mathbb{F}}$ es principal si y sólo si al menos una de las ecuaciones $b_1^2 - d\, b_2^2 = \pm s^2\, N(\mathfrak{I}_{\mathbb{F}})$ tiene solución con $b_1, b_2 \in \mathbb{Z}$.*
2. *$\mathfrak{I}_{\mathbb{F}}$ es un ideal no principal si y sólo si existe una solución de $d_1\, b_1^2 - d_2\, b_2^2 = \pm s^2\, N(\mathfrak{I}_{\mathbb{F}})$ con $b_1, b_2, \in \mathbb{Z}$.* □

Ejemplo 2.38. *Sea $d = 2 \cdot 3 \cdot 5 \cdot 7$ y $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Tenemos las siguientes posibles factorizaciones de d con d_1, d_2 positivos.*

d_1	d_2
1	210
2	105
3	70
5	42
6	35
7	30
10	21
14	15

Sean $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_7$ los únicos ideales de $\mathcal{O}_\mathbb{F}$ con norma $2, 3, 5, 7$ respectivamente. Como d tiene cuatro factores primos y entre ellos hay algunos congruentes con 3 módulo 4, entonces el 2-rango de $Cl_\mathbb{F}$ es 2, de hecho $Cl_\mathbb{F} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donde $\mathfrak{p}_2\mathfrak{p}_7$ y $\mathfrak{p}_3\mathfrak{p}_5$ son ideales principales, $\mathfrak{p}_2, \mathfrak{p}_7, \mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_7, \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ están en la misma clase, $\mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7, \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$ están en una segunda clase de ideales no principales y $\mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{p}_5, \mathfrak{p}_5\mathfrak{p}_7, \mathfrak{p}_3\mathfrak{p}_7$ están en la última clase. En este caso, un ideal $\mathfrak{I} \subseteq \mathcal{O}_\mathbb{F}$ es principal si y sólo si

$$b_1^2 - 210\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) \quad y \quad 14b_1^2 - 15\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I})$$

son solubles; $\mathfrak{I} \in \overline{\mathfrak{p}_2}$ si y sólo si

$$2\, b_1^2 - 105\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) \quad y \quad 7b_1^2 - 30\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I})$$

son solubles; $\mathfrak{I} \in \overline{\mathfrak{p}_3}$ si y sólo si

$$3\, b_1^2 - 70\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) \quad y \quad 5b_1^2 - 42\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I})$$

son solubles; $\mathfrak{I} \in \overline{\mathfrak{p}_2\mathfrak{p}_3}$ si y sólo si

$$6\, b_1^2 - 35\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}) \quad y \quad 10\, b_1^2 - 21\, b_2^2 = \pm N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I})$$

son solubles.

En el caso $d = 2\,p > 0$ con $p \equiv 5 \pmod 8$ ya vimos que $\mathfrak{d}_1, \mathfrak{d}_2$ son ideales no principales. Vamos a terminar esta sección demostrando que si $p \equiv 1 \pmod 8$ los ideales mencionados sí son principales. El siguiente ejemplo nos servirá de guía.

Ejemplo 2.39. *Sean $d = d_1\, d_2$ con $d_1 = 2$ y $d_2 = 17$, $\mathfrak{d}_1, \mathfrak{d}_2$ los únicos ideales de $\mathcal{O}_\mathbb{F}$ tales que $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_1) = d_1$ y $N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{d}_2) = d_2$. En este caso $\mathfrak{d}_1, \mathfrak{d}_2$ son principales. En efecto, el primo 3 se descompone en $\mathbb{F}$, ya que $34 \equiv 1 \pmod 3$ y*

$$\left(\frac{\delta_\mathbb{F}}{3}\right) = \left(\frac{4 \cdot 34}{3}\right) = \left(\frac{34}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

De hecho,

$$\langle 3 \rangle_\mathbb{F} = \left\langle 3, 1 + \sqrt{34} \right\rangle_\mathbb{F} \left\langle 3, 1 - \sqrt{34} \right\rangle_\mathbb{F}.$$

Ninguno de estos ideales es principal, pues de lo contrario, existiría $\alpha = a_1 + a_2\sqrt{34}$ con $N_{\mathbb{F}/\mathbb{Q}}(\alpha) = 3$. Vamos a probar que α no existe. Si $a_1^2 - 34a_2^2$ es impar, entonces a_1 debe ser impar, así $a_1^2 \equiv 1 \pmod 8$. Si a_2 es par, entonces $34a_2^2 \equiv 0 \pmod 8$ y si a_2 es impar, entonces $34a_2^2 \equiv 2 \pmod 8$. Por tanto $a_1^2 - 34a_2^2 \equiv \pm 1 \pmod 8$. Esto prueba

que no existen elementos con norma ± 3 *modulo* 8*, así,* $\left\langle 3, 1+\sqrt{34}\right\rangle_{\mathbb{F}}$ *y* $\left\langle 3, 1-\sqrt{34}\right\rangle_{\mathbb{F}}$ *son ideales no principales.*

Ahora vamos a probar que $17b_1^2 - 2b_2^2 = \pm 3$ *no tiene soluciones enteras. Una vez más, vamos a considerar la ecuación como una congruencia módulo* 8*. Puesto que* $17b_1^2 \equiv 1 \pmod 8$ *y* $2b_2^2 \equiv 0, 2 \pmod 8$*, entonces* $17b_1^2 - 2b_2^2 \equiv \pm 1 \pmod 8$*. Por tanto, ninguna de las cuatro ecuaciones tiene soluciones enteras. Por la contrapositiva del* Corolario 2.37*, los ideales* $\mathfrak{d}_1$ *y* $\mathfrak{d}_2$ *deben de ser principales.*

El ejemplo anterior se puede generalizar cuando $d = 2\,p$ con $p \equiv 1 \pmod 8$.

Proposición 2.40. *Sea* $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ *con* $p > 0$ *un primo racional y* $p \equiv 1 \pmod 8$*. Entonces, existe un ideal no principal* $\mathfrak{I}_{\mathbb{F}}$ *de* $\mathcal{O}_{\mathbb{F}}$ *tal que* $p\,b_1^2 - 2\,b_2^2 = \pm N(\mathfrak{I}_{\mathbb{F}})$ *no tiene soluciones enteras.*

DEMOSTRACIÓN. En general, si $p \equiv 1 \pmod 8$, entonces $p\,b_1^2 - 2\,b_2^2 \equiv \pm 1 \pmod 8$, así, basta con encontrar un ideal no principal cuya norma sea $\pm 3 \pmod 8$.

Sea $a \in \mathbb{Z}$ tal que $\left(\dfrac{a}{p}\right) = -1$. Como $\text{m.c.d.}\,(p, 8) = 1$, existe $b \in \mathbb{Z}$ tal que $b \equiv a \pmod p$ y $b \equiv 3 \pmod 8$. Usando el Teorema de Dirichlet sobre primos en sucesiones aritméticas, existe una infinidad de primos congruentes con b modulo $8\,p$. Sea q uno de estos primos. Como $q \equiv 3 \pmod 8$ y $q \equiv a \pmod p$ tenemos

$$\left(\frac{2}{q}\right) = -1, \quad \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = -1, \quad \left[\frac{q}{2\,p}\right] = -1, \quad \left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1.$$

De lo anterior, existe un ideal $\mathfrak{q}$ con $N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{q}) = q$ tal que $\mathfrak{q}$ no es principal.

Ahora observemos que $p\,b_1^2 - 2\,b_2^2 \equiv \pm 3 \pmod 8$ no tiene soluciones enteras puesto que $q \equiv 3 \pmod 8$. □

Corolario 2.41. *Sean* $\mathbb{F} = \mathbb{Q}(\sqrt{2\,p})$ *con* $p > 0$ *un primo racional,* $p \equiv 1 \pmod 8$*,* $h_{\mathbb{F}} = 2$ *y* $\mathfrak{d}_1, \mathfrak{d}_2$ *los únicos ideales de* $\mathcal{O}_{\mathbb{F}}$ *tales que* $N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{d}_1) = 2$ *y* $N_{\mathbb{F}/\mathbb{Q}}\,(\mathfrak{d}_2) = p$*. Entonces,* $\mathfrak{d}_1$ *y* $\mathfrak{d}_2$ *son ideales principales.*

DEMOSTRACIÓN. Como $h_{\mathbb{F}} = 2$, solamente hay dos clases de ideales en $\mathcal{O}_{\mathbb{F}}$, la de los ideales principales y la de los que no lo son. Por la Proposición 2.40, existe un ideal no principal $\mathfrak{I}_{\mathbb{F}}$ que no satisface la ecuación $p\,b_1^2 - 2\,b_2^2 = \pm N(\mathfrak{I}_{\mathbb{F}})$. Por la Proposición 2.34, ninguno de los ideales no principales resuelve dicha ecuación, así que la clase que debe de resolver la ecuación es la de los ideales principales. El resultado se sigue de la contrapositiva del Corolario 2.37. □

En el caso imaginario, el siguiente resultado nos afirma que $\mathfrak{d}_1, \mathfrak{d}_2$ nunca van a ser principales a menos que $|d_1| = 1$ ó $|d_2| = 1$. Si esto sucede, debemos de utilizar el Teorema 2.20 para saber si un ideal es principal.

Proposición 2.42. *Sean* $d = d_1\,d_2 < 0$ *un entero racional libre de cuadrados con* $|d_1| \neq 1 \neq |d_2|$*,* $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ *y* $\mathfrak{d}_1, \mathfrak{d}_2$ *los únicos ideales de* $\mathcal{O}_{\mathbb{F}}$ *con norma* $|d_1|, |d_2|$ *respectivamente. Los ideales* $\mathfrak{d}_1, \mathfrak{d}_2$ *no son principales.*

DEMOSTRACIÓN. Sea $A = a_1 + a_2\sqrt{d}$ con $N_{\mathbb{F}/\mathbb{Q}}\,(A) = a_1^2 - d\,a_2^2 = a_1^2 + |d|\,a_2^2$ libre de cuadrados. Por la condición anterior, $a_2 \neq 0$, así que $N_{\mathbb{F}/\mathbb{Q}}\,(A) \geq |d|$. Como d_1, d_2 son

libres de cuadrados y $|d_1| < |d|$, $|d_2| < |d|$, entonces no existe ningún elemento con norma $|d_1|$ ó $|d_2|$, por lo que $\mathfrak{d}_1, \mathfrak{d}_2$ no son principales. □

Corolario 2.43. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d = d_1\, d_2 < 0$, $h_{\mathbb{F}} = 2$, $\mathbb{H}_{\mathbb{F}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $|d_1| \neq 1 \neq |d_2|$, $\mathfrak{I}_{\mathbb{F}}$ un ideal de $\mathcal{O}_{\mathbb{F}}$ y $s = 1$ si $d \equiv 2, 3 \pmod 4$, $s = 2$ si $d \equiv 1 \pmod 4$. Entonces:*

1. *$\mathfrak{I}_{\mathbb{F}}$ es principal si y sólo si al menos una de las ecuaciones $b_1^2 - d\, b_2^2 = s^2\, N(\mathfrak{I}_{\mathbb{F}})$ tiene solución con $b_1, b_2 \in \mathbb{Z}$.*
2. *$\mathfrak{I}_{\mathbb{F}}$ es un ideal no principal si y sólo si existe una solución de $d_1\, b_1^2 - d_2\, b_2^2 = \pm s^2\, N(\mathfrak{I}_{\mathbb{F}})$ con $b_1, b_2, \in \mathbb{Z}$.* □

En [**29**], H. Stark clasificó los campos cuadráticos imaginarios con $h_{\mathbb{F}} = 2$:

Teorema 2.44. *Si $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ es un campo cuadrático imaginario, entonces $h_{\mathbb{F}} = 2$ si y sólo si $d = -5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123, -187, -235, -267, -403, -427$.* □

De estos 18 números, podemos aplicar el corolario en todos menos en $d = -5, -13, -37$, que son los que no cumplen la condición $|d_1| \neq 1 \neq |d_2|$.

2.6. Clasificación de primos e irreducibles en campos cuadráticos con $h_{\mathbb{F}} = 2$

Ahora vamos a estudiar una aplicación del Teorema 2.22, el cual nos proporciona un criterio para saber si un ideal de $\mathcal{O}_{\mathbb{F}}$ es o no principal. Usaremos esta información para clasificar los elementos primos, irreducibles y compuestos del anillo de enteros de un campo cuadrático con $h_{\mathbb{F}} = 2$.

Si $h_{\mathbb{F}} = 2$, entonces el producto de dos ideales no principales es principal. De la proposición 1.29 se sigue que P es irreducible si y sólo si $\langle P \rangle = \mathfrak{pq}$ donde $\mathfrak{p}, \mathfrak{q}$ son ideales primos no principales.

Sea $\mathfrak{I}$ un ideal tal que $\text{m.c.d.}\,(N(\mathfrak{I}), \delta_{\mathbb{F}}) > 1$. Si queremos saber si $\mathfrak{I}$ es principal, factorizamos $\mathfrak{I} = \mathfrak{I}_1\mathfrak{I}_2$ tal que $\text{m.c.d.}\,(N(\mathfrak{I}_1), \delta_{\mathbb{F}}) = 1$ y cada ideal primo que divide a $\mathfrak{I}_2$ se ramifica. Entonces $\mathfrak{I}$ es principal si y sólo si $\overline{\mathfrak{I}_1} = \overline{\mathfrak{I}_2}^{\,-1}$. Si $h_{\mathbb{F}} = 2$, entonces $\mathfrak{I}$ es principal si y sólo si $\mathfrak{I}_1, \mathfrak{I}_2$ son ambos principales o ninguno lo es.

Teorema 2.45. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ un campo cuadrático real, $h_{\mathbb{F}} = 2$ y $P \in \mathcal{O}_{\mathbb{F}}$ tal que $\text{m.c.d.}\,(N(P), \delta_{\mathbb{F}}) = 1$. Entonces P es primo si y sólo si una de las siguientes afirmaciones se cumple:*

1. *$|N(P)| = q$ es un primo racional tal que $\left(\dfrac{\delta_{\mathbb{F}}}{q}\right) = 1$ y $\left[\dfrac{q}{d}\right] = 1$ ó $\left[\dfrac{-q}{d}\right] = 1$.*
2. *$N(P) = q^2$ donde q es un primo racional tal que $\left(\dfrac{\delta_{\mathbb{F}}}{q}\right) = -1$.*

DEMOSTRACIÓN. Es suficiente probar que $|N(P)| = q$ es primo si y sólo si se cumple 1. Recordemos que $N(\mathfrak{I})$ es primo si y sólo si $\mathfrak{I}$ se ramifica o se descompone. Por hipótesis, $\text{m.c.d.}\,(N(P), \delta_{\mathbb{F}}) = 1$, así que $\left(\dfrac{\delta_{\mathbb{F}}}{q}\right) = 1$. Del Teorema 2.22, se sigue que $\mathfrak{I}$ es principal

si y sólo si $\left[\frac{q}{d}\right] = 1$ ó $\left[\frac{-q}{d}\right] = 1$, en particular, si $\mathfrak{I} = \langle P \rangle$ se sigue 1. El caso de la afirmación 2 se obtiene cuando el primo q es inerte. □

Teorema 2.46. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ un campo cuadrático real, $h_{\mathbb{F}} = 2$ y $P \in \mathcal{O}_{\mathbb{F}}$ tal que $\mathrm{m.c.d.}\,(N(P), \delta_{\mathbb{F}}) = 1$. Entonces P es irreducible si y sólo si una de las siguientes afirmaciones se cumple:*

1. *P es primo.*
2. *$|N(P)| = pq,\ p, q$ primos racionales tales que $\left(\frac{\delta_{\mathbb{F}}}{p}\right) = \left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1$ y $\left[\frac{\pm p}{d}\right] = \left[\frac{\pm q}{d}\right] = -1$, para al menos uno de los signos, donde los signos de $\pm p$ y $\pm q$ pueden ser distintos o iguales.*

DEMOSTRACIÓN. Si P es un elemento irreducible no primo, entonces $\langle P \rangle = \mathfrak{pq}$, donde $\mathfrak{p}, \mathfrak{q}$ son ideales primos no principales. La norma de cada uno de estos ideales debe ser un primo, pues de lo contrario $\mathfrak{p}$ y $\mathfrak{q}$ serían ambos principales. Sean $N(\mathfrak{p}) = p$, $N(\mathfrak{q}) = q$. Así $\left(\frac{\delta_{\mathbb{F}}}{p}\right) = \left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1$. La condición $\left[\frac{\pm p}{d}\right] = \left[\frac{\pm q}{d}\right] = -1$ es necesaria para que los ideales sean no principales. □

El caso en que $\mathbb{F}$ es un campo cuadrático imaginario es similar:

Teorema 2.47. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$ un campo cuadrático imaginario, $h_{\mathbb{F}} = 2$ y $P \in \mathcal{O}_{\mathbb{F}}$ tal que $\mathrm{m.c.d.}\,(N(P), \delta_{\mathbb{F}}) = 1$. Entonces P es primo si y sólo si una de las siguientes afirmaciones se cumple:*

1. *$N(P) = q$ es un primo racional tal que $\left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1$ y $\left[\frac{q}{d}\right] = 1$.*
2. *$N(P) = q^2$ donde q es un primo racional tal que $\left(\frac{\delta_{\mathbb{F}}}{q}\right) = -1$.* □

Teorema 2.48. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$ un campo cuadrático imaginario, $h_{\mathbb{F}} = 2$ y $P \in \mathcal{O}_{\mathbb{F}}$ tal que $\mathrm{m.c.d.}\,(N(P), \delta_{\mathbb{F}}) = 1$. Entonces P es irreducible si y sólo si una de las siguientes afirmaciones se cumple:*

1. *P es primo.*
2. *$N(P) = pq,\ p, q$ primos racionales tales que $\left(\frac{\delta_{\mathbb{F}}}{p}\right) = \left(\frac{\delta_{\mathbb{F}}}{q}\right) = 1$ y $\left[\frac{p}{d}\right] = \left[\frac{q}{d}\right] = -1$.* □

Ejemplo 2.49. *Sea $\mathbb{F} = \mathbb{Q}(\sqrt{10})$. En este ejemplo, $Cl_{\mathbb{F}} = \{\overline{1}, \overline{\langle 2, \sqrt{10}\rangle}\}$, así que $h_{\mathbb{F}} = 2$. Los primos ramificados son 2 y 5 y los ideales $\langle 2, \sqrt{10}\rangle$ y $\langle 5, \sqrt{10}\rangle$ son no principales. Un primo p se descompone si $\left(\frac{\delta_{\mathbb{F}}}{p}\right) = 1$, es decir, si $p \equiv 1, 3, 9, 13, 27, 31, 37, 39$*

$(\text{mód } 40)$. *Por otro lado,* $\left[\frac{\pm a}{10}\right] = 1$ *si y sólo si* $a \equiv 0, 1, 4, 5, 6, 9 \pmod{10}$. *Si* $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$*, entonces* p *es inerte. Así, obtenemos:*

1. $P \in \mathcal{O}_{\mathbb{F}}$ *es primo si y sólo si una de las siguientes afirmaciones es cierta:*
   a) $|N(P)| = p$ *para un primo* $p \equiv 1, 9, 31, 39 \pmod{40}$.
   b) $|N(P)| = p^2$*, con* $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \pmod{40}$.
2. $P \in \mathcal{O}_{\mathbb{F}}$ *es irreducible pero no primo si* $|N(P)| = pq$ *con* $p \equiv 2, 3, 5, 13, 27, 37 \pmod{40}$ *y* $q \equiv 2, 3, 5, 13, 27, 37 \pmod{40}$.

Los resultados del ejemplo anterior están escritos utilizando el Teorema 2.22, debido a esto se utiliza como módulo el número 40. También podemos clasificar irreducibles en $\mathbb{Q}(\sqrt{10})$ utilizando el Teorema 2.31: observemos que $1 \equiv 9 \equiv 1 \pmod 8$, $31 \equiv 39 \equiv -1 \pmod 8$, $3 \equiv 27 \equiv 3 \pmod 8$ y $13 \equiv 37 \equiv -3 \pmod 8$, así que en el inciso 1 a) consideramos $p \equiv \pm 1 \pmod 8$ y en el inciso 2, $p \equiv \pm 3 \pmod 8$ ó $p = 2$.

Ejemplo 2.50. *Sea* $\mathbb{F} = \mathbb{Q}(\sqrt{34})$*. Puesto que* $Cl_{\mathbb{F}} = \{\overline{\mathcal{O}_{\mathbb{F}}}, \overline{\mathfrak{p}_3}\}$*, donde* $\mathfrak{p}_3 = \langle 3, 1 + \sqrt{34}\rangle$*, entonces* $h_{\mathbb{F}} = 2$*. De acuerdo al Teorema 2.26, en este caso,* $d_1 = 2$*,* $d_2 = 17 \equiv 1 \pmod 8$ *y por lo tanto* $\mathfrak{d}_1 = \langle 6 + \sqrt{34}\rangle$ *es principal. Lo anterior significa que no es posible dar las soluciones módulo* 8 *como lo hicimos en el caso de* $\mathbb{Q}(\sqrt{10})$*, así que debemos dar los resultados módulo* $(34)(4)$.

1. $P \in \mathcal{O}_{\mathbb{F}}$ *es primo si y sólo si una de las siguientes afirmaciones es cierta:*
   a) $|N(P)| = p$ *para un primo racional* $p \equiv 1, 2, 9, 15, 17, 25, 33, 47, 49, 55, 81, 87, 89, 103, 111, 121, 127, 135 \pmod{136}$.
   b) $|N(P)| = p^2$ *para un primo* $p \equiv 7, 13, 19, 21, 23, 31, 35, 39, 41, 43, 53, 57, 59, 63, 65, 67, 69, 71, 73, 77, 79, 83, 93, 95, 97, 101, 105, 113, 115, 117, 123, 129 \pmod{136}$.
2. $P \in \mathcal{O}_{\mathbb{F}}$ *es irreducible pero no primo si* $|N(P)| = pq$ *con* $p \equiv 3, 5, 11, 27, 29, 37, 45, 61, 75, 91, 99, 107, 109, 125, 131, 133 \pmod{136}$ *y* $q \equiv 3, 5, 11, 27, 29, 37, 45, 61, 75, 91, 99, 107, 109, 125, 131, 133 \pmod{136}$.

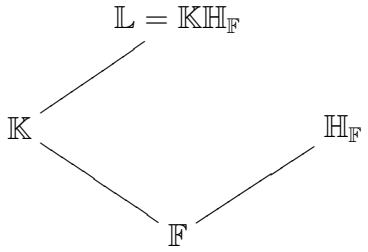
Ejemplo 2.51. *Si* $\mathbb{F} = \mathbb{Q}(\sqrt{-5})$*, entonces* $h_{\mathbb{F}} = 2$*,* $Cl_{\mathbb{F}} = \{\overline{\mathcal{O}_{\mathbb{F}}}, \overline{\langle 2, 1 + \sqrt{-5}\rangle_{\mathbb{F}}}\}$ *y* $\delta_{\mathbb{F}} = -20$*. De acuerdo al Teorema 2.22, un ideal* $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$ *con* $\gcd(N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}}), \delta_{\mathbb{F}}) = 1$ *es principal si y sólo si* $\left[\frac{N_{\mathbb{F}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{F}})}{5}\right] = 1$*. Es claro que* $\langle 2, 1 + \sqrt{-5}\rangle$ *no es principal ya que* $b_1^2 + 5\,b_2^2 = 2$ *no tiene soluciones* $b_1, b_2 \in \mathbb{Z}$ *y el único ideal con norma* 5 *es* $\langle \sqrt{-5}\rangle_{\mathbb{F}}$*. Entonces:*

1. $P \in \mathcal{O}_{\mathbb{F}}$ *es un elemento primo si se cumple una de las siguientes afirmaciones:*
   a) $|N_{\mathbb{F}/\mathbb{Q}}(P)| = p$ *para algún primo* $p \equiv 0, 1, 4 \pmod 5$*. Esto sucede cuando* $p \equiv 1, 5, 9 \pmod{20}$.
   b) $|N_{\mathbb{F}/\mathbb{Q}}(P)| = p^2$*, con* $p \equiv 11, 13, 17, 19 \pmod{136}$ *un primo racional.*
2. $P \in \mathcal{O}_{\mathbb{F}}$ *es irreducible pero no primo si* $|N_{\mathbb{F}/\mathbb{Q}}(P)| = pq$ *con* $p \equiv 2, 3, 7 \pmod{20}$ *y* $q \equiv 2, 3, 7 \pmod{20}$.

Capítulo 3

Una familia de campos cuaŕticos con 2-grupo de clases de orden 2

Sea $\mathbb{K}/\mathbb{F}$ una extensión de campos de números. Un problema interesante es estudiar si existe alguna relación entre la aritmética de $\mathbb{K}$ y la de $\mathbb{F}$. En particular, uno de nuestros objetivos es hallar algún vínculo no conocido entre $Cl_{\mathbb{K}}$ y $Cl_{\mathbb{F}}$. Es posible que $h_{\mathbb{F}} > h_{\mathbb{K}}$, como por ejemplo, si $\mathbb{F} = \mathbb{Q}(\sqrt{10})$ y $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, entonces $h_{\mathbb{F}} = 2$ y $h_{\mathbb{K}} = 1$. También es posible que $h_{\mathbb{F}} = h_{\mathbb{K}}$, por ejemplo si $\mathbb{F} = \mathbb{Q}(\sqrt{10})$ y $\mathbb{K} = \mathbb{Q}(\sqrt[4]{10})$, entonces $h_{\mathbb{F}} = h_{\mathbb{K}} = 2$; incluso es posible que $h_{\mathbb{F}} < h_{\mathbb{K}}$ que es parte de lo que estudiaremos a lo largo de este capítulo. Un caso interesante se da cuando $\mathbb{K}/\mathbb{F}$ es una extensión Galois en la que existe un ideal primo en $\mathcal{O}_{\mathbb{F}}$ que se ramifica totalmente.



Si $\mathbb{L} = \mathbb{K}\mathbb{H}_{\mathbb{F}}$, entonces como consecuencia de la afirmación 3 de la Proposición 1.18, la extensión $\mathbb{L}/\mathbb{K}$ es no ramificada, así que:

Teorema 3.1. *Sea $\mathbb{K}/\mathbb{F}$ una extensión Galois tal que existe un ideal primo de $\mathcal{O}_{\mathbb{F}}$ totalmente ramificado en $\mathbb{K}/\mathbb{F}$. Si $\mathbb{H}_{\mathbb{F}}$ es el campo de clases de Hilbert de $\mathbb{F}$ y $\mathbb{L} = \mathbb{K}\mathbb{H}_{\mathbb{F}}$, entonces $\mathbb{L} \subseteq \mathbb{H}_{\mathbb{K}}$.* □

El teorema anterior nos indica que existe un monomorfismo $Cl_{\mathbb{F}} \hookrightarrow Cl_{\mathbb{K}}$ y además, $h_{\mathbb{F}} \mid h_{\mathbb{K}}$. En particular, si $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ con $d \in \mathbb{Z}$ libre de cuadrados y $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$, cualquier primo p que divide a d se ramifica totalmente en $\mathbb{K}/\mathbb{F}$, de hecho, también se ramifica totalmente en $\mathbb{K}/\mathbb{Q}$, tomando en cuenta que claramente $\langle p \rangle_{\mathbb{K}} = \left\langle p, \sqrt[4]{d} \right\rangle_{\mathbb{K}}^{4}$. Lo anterior nos implica que el 2-rango de $Cl_{\mathbb{F}}$ es menor o igual que el 2-rango de $Cl_{\mathbb{K}}$. De esta forma, el Teorema de Gauss del 2-rango de un campo cuadrático nos da una cota inferior del 2-rango de $Cl_{\mathbb{K}}$.

En este capítulo estudiaremos la familia de extensiones $\mathbb{K}/\mathbb{F}$ donde $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ y $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ con $0 < p \equiv 7 \pmod{16}$ un primo racional, donde $h_{\mathbb{F}}$ es impar y $h_{\mathbb{K}}$ es par, es decir, mostraremos que el 2-rango de $Cl_{\mathbb{K}}$ es estrictamente mayor que el 2-rango de $Cl_{\mathbb{F}}$. En particular, si $h_{\mathbb{K}} = 2$, el campo de clases de Hilbert de $\mathbb{K}$ es $\mathbb{H}_{\mathbb{K}} = \mathbb{K}(\sqrt{U_{\mathbb{F}}})$, donde $U_{\mathbb{F}}$ es la unidad fundamental de $\mathbb{F}$. Continuaremos estudiando la ramificación de 2

en extensiones similares a $\mathbb{H}_{\mathbb{K}}$, es decir, en campos de la forma $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ donde α es libre de cuadrados en todas sus factorizaciones. Usaremos lo anterior para demostrar que el 2-grupo de clases de ideales de $\mathbb{K}$ es isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

3.1. Elementos de $\mathcal{O}_{\mathbb{F}}$

Comenzaremos estudiando algunas propiedades de los elementos de $\mathbb{F} = \mathbb{Q}(\sqrt{p})$. Daremos un criterio para decidir si la raíz cuadrada de un elemento de $\mathcal{O}_{\mathbb{F}}$ también está en $\mathcal{O}_{\mathbb{F}}$, esto nos ayudará a describir la unidad fundamental de $\mathbb{F}$.

Lema 3.2. *Sean $a, b, d \in \mathbb{Z}$ tales que $a^2 \mid d\,b^2$, donde d es libre de cuadrados. Entonces $a \mid b$.*

DEMOSTRACIÓN. Si $a^2 \nmid b^2$, entonces existe $p \in \mathbb{Z}$ un divisor primo de a tal que $\operatorname{ord}_p(a^2) > \operatorname{ord}_p(b^2)$. Como $a^2 \mid d\,b^2$, entonces

$$\operatorname{ord}_p\left(a^2\right) \leq \operatorname{ord}_p\left(d\,b^2\right) \leq \operatorname{ord}_p\left(b^2\right) + 1 < \operatorname{ord}_p\left(a^2\right) + 1.$$

Por esta desigualdad, $\operatorname{ord}_p(a^2) = \operatorname{ord}_p(b^2) + 1$, lo cual no es posible pues $\operatorname{ord}_p(a^2)$ y $\operatorname{ord}_p(b^2)$ son ambos pares. Por lo tanto $a^2 \mid b^2$ y $a \mid b$. □

Proposición 3.3. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ con $p \equiv 3 \pmod 4$ primo racional y $M = m_1 + m_2\sqrt{p} \in \mathcal{O}_{\mathbb{F}}$ tal que m_1 es impar y $N_{\mathbb{F}/\mathbb{Q}}(M) = 1$. Entonces, existe $A \in \mathcal{O}_{\mathbb{F}}$ tal que $A^2 = M$.*

DEMOSTRACIÓN. Si $A = a_1 + a_2\sqrt{p} \in \mathcal{O}_{\mathbb{F}}$ es tal que $A^2 = M$, entonces

$$M = m_1 + m_2\sqrt{p} = a_1^2 + p\,a_2^2 + 2\,a_1\,a_2\,\sqrt{p}.$$

Para encontrar A debemos de resolver el sistema de ecuaciones diofantinas:

$$\begin{cases} m_1 = a_1^2 + p\,a_2^2 \\ m_2 = 2\,a_1\,a_2 \end{cases} \tag{9}$$

Si $a_1 = 0$ entonces $N_{\mathbb{F}/\mathbb{Q}}(M) \neq 1$, así que $a_2 = \dfrac{m_2}{2a_1}$ y tenemos el sistema equivalente:

$$\begin{cases} m_1 = a_1^2 + p\left(\dfrac{m_2}{2\,a_1}\right)^2 \\ a_2 = \dfrac{m_2}{2\,a_1} \end{cases}$$

Primero vamos a ver que la primera ecuación tiene al menos una solución $a_1 \in \mathbb{Z}$. Multiplicamos ambos lados de la igualdad por $4\,a_1^2$ y obtenemos la ecuación:

$$0 = 4\,a_1^4 - 4\,a_1^2 m_1 + p\,m_2^2. \tag{10}$$

Por lo tanto:

$$a_1^2 = \frac{4\,m_1 \pm \sqrt{16\,m_1^2 - 16\,p\,m_2^2}}{8} = \frac{m_1 \pm \sqrt{m_1^2 - p\,m_2^2}}{2}.$$

Como $m_1^2 - p\,m_2^2 = N_{\mathbb{F}/\mathbb{Q}}\left(m_1 + m_2\sqrt{p}\right) = 1$, entonces las cuatro soluciones de (10) son:

$$a_1 = \pm\sqrt{\frac{m_1 \pm 1}{2}}. \tag{11}$$

Vamos a mostrar que una de éstas cumple $a_1 \in \mathbb{Z}$. En efecto, como $(m_1+1)-(m_1-1)=2$ y m_1 es impar, entonces $\text{m.c.d.}\,(m_1+1, m_1-1)=2$, así $\text{m.c.d.}\left(\dfrac{m_1+1}{2}, \dfrac{m_1-1}{2}\right)=1$. Sabemos que

$$p\left(\frac{m_2}{2}\right)^2 = \frac{p\,m_2^2}{4} = \frac{m_1^2-1}{4} = \left(\frac{m_1+1}{2}\right)\left(\frac{m_1-1}{2}\right).$$

Por lo anterior, podemos suponer $\left(\dfrac{m_1 \pm 1}{2}\right) = c_1^2$ y $\left(\dfrac{m_1 \mp 1}{2}\right) = p\,c_2^2$, además para algunos $c_1, c_2 \in \mathbb{Z}$, por lo que una solución de (11) es $a_1 = c_1 \in \mathbb{Z}$.

Ahora vamos a demostrar que $a_2 = \dfrac{m_2}{2\,a_1} \in \mathbb{Z}$. Dependiendo del signo de la solución de (11) con $a_1 \in \mathbb{Z}$, tenemos que $a_1^2 \mid \dfrac{m_1+1}{2}$ ó $a_1^2 \mid \dfrac{m_1-1}{2}$. En cualquiera de los dos casos, $a_1^2 \mid \dfrac{m_1^2-1}{4} = \dfrac{p\,m_2^2}{4}$ ya que $N_{\mathbb{F}/\mathbb{Q}}(M)=1$ y $(2\,a_1)^2 \mid p\,m_2^2$. Usando el Lema 3.2, tenemos que $2\,a_1 \mid m_2$. Por lo anterior, $A = a_1 + a_2\sqrt{p} \in \mathcal{O}_{\mathbb{F}}$ satisface $A^2 = M$. □

Los dos resultados siguientes describen el grupo de unidades de $\mathcal{O}_{\mathbb{F}}$.

Lema 3.4. *Sean $d \equiv 3 \pmod 4$ y $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Entonces, toda unidad de $\mathcal{O}_{\mathbb{F}}$ tiene norma* 1.

DEMOSTRACIÓN. Si $U = u_1 + u_2\sqrt{d}$ es una unidad, entonces $N_{\mathbb{F}/\mathbb{Q}}(U) = u_1^2 - d\,u_2^2 = \pm 1$. Si u_1 es par, entonces $N_{\mathbb{F}/\mathbb{Q}}(U) \equiv 0 - 3(1) \equiv 1 \pmod 4$ por ser u_2 impar. Si u_1 es impar, $N_{\mathbb{F}/\mathbb{Q}}(U) \equiv 1 - 3(0) \equiv 1 \pmod 4$ por ser u_2 par. □

Proposición 3.5. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ con p un primo racional positivo y $U_{\mathbb{F}} = u_1 + u_2\sqrt{p}$ la unidad fundamental de $\mathbb{F}$. Si $p \equiv 3 \pmod 4$, entonces u_1 es par. Más aún, si $p \equiv 3 \pmod 8$, entonces $u_1 \equiv 2 \pmod 4$ y si $p \equiv 7 \pmod 8$, entonces $4 \mid u_1$.*

DEMOSTRACIÓN. Por el Lema 3.4, la unidad fundamental tiene norma 1. El coeficiente u_1 debe de ser par, pues de lo contrario, por la Proposición 3.3, $U_{\mathbb{F}}$ tendría una raíz cuadrada en $\mathcal{O}_{\mathbb{F}}$, por lo que no sería la unidad fundamental. Si $4 \mid u_1$ y $p \equiv 3 \pmod 8$, entonces $u_1^2 - 3\,u_2^2 \equiv 8 - 3(1) \equiv 5 \pmod 8$. Si $u_1 \equiv 2 \pmod 4$ y $p \equiv 7 \pmod 8$, entonces $u_1^2 - 7\,u_2^2 \equiv 4 - 7(1) \equiv 5 \pmod 8$. En ninguno de los dos casos la norma es 1. □

Proposición 3.6. *Si $0 < p \equiv 3 \pmod 4$ es un primo racional y $\mathbb{F} = \mathbb{Q}(\sqrt{p})$, entonces existe un elemento en $\mathcal{O}_{\mathbb{F}}$ con norma 2 cuando $p \equiv 7 \pmod 8$ ó un elemento con norma -2 cuando $p \equiv 3 \pmod 8$.*

DEMOSTRACIÓN. Como $p \equiv 3 \pmod 4$, entonces $\langle 2 \rangle = \mathfrak{p}^2$. Además, p es primo, así que por el Teorema 2.4 el número de clases de $\mathbb{F}$ es impar. Lo anterior implica que $\mathfrak{p}$ debe de ser principal, pues de lo contrario el orden de $\overline{\mathfrak{p}}$ es 2, lo que no es posible. Por lo tanto, existe un elemento con norma 2 ó -2.

Sea $A = a_1 + a_2\sqrt{p} \in \mathcal{O}_{\mathbb{F}}$ tal que $|N_{\mathbb{F}/\mathbb{Q}}(A)| = |a_1^2 - p\,a_2^2| = 2$. Si a_1, a_2 son pares, entonces $N_{\mathbb{F}/\mathbb{Q}}(A) = a_1^2 - pa_2^2 \equiv 0 - 3(0) \equiv 0 \pmod 4$, lo cual es imposible. Si a_1, a_2 tienen paridad distinta, entonces $N_{\mathbb{F}/\mathbb{Q}}(A)$ es impar. Por lo tanto, a_1, a_2 son impares. Si

$p \equiv 3 \pmod 8$, entonces $N_{\mathbb{F}/\mathbb{Q}}(A) = a_1^2 - p\,a_2^2 \equiv 1 - 3(1) \equiv -2 \pmod 8$, así que $N_{\mathbb{F}/\mathbb{Q}}(A) = -2$. Si $p \equiv 7 \pmod 8$, entonces $N_{\mathbb{F}/\mathbb{Q}}(A) \equiv 1 - (7)(1) \equiv 2 \pmod 8$ y $N_{\mathbb{F}/\mathbb{Q}}(A) = 2$. □

Como 2 se ramifica totalmente en $\mathcal{O}_{\mathbb{F}}$, donde $\mathbb{F} = \mathbb{Q}(\sqrt{p})$, entonces existe un único ideal con norma 2, por lo que si $A, B \in \mathcal{O}_{\mathbb{F}}$ son tales que $|N_{\mathbb{F}/\mathbb{Q}}(A)| = |N_{\mathbb{F}/\mathbb{Q}}(B)| = 2$ entonces $\langle A\rangle_{\mathbb{F}} = \langle B\rangle_{\mathbb{F}}$.

Corolario 3.7. *Sea* $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ *con* $0 < p \equiv 3 \pmod 4$ *un primo racional. Existe un elemento* $L_2 \in \mathcal{O}_{\mathbb{F}}$ *tal que* $L_2^2\, U_{\mathbb{F}} = 2$.

DEMOSTRACIÓN. Sabemos que existe un ideal $\mathfrak{p}_2 \subseteq \mathcal{O}_{\mathbb{F}}$ tal que $\mathfrak{p}_2^2 = \langle 2\rangle_{\mathbb{F}}$ y que $\mathfrak{p}_2$ es un ideal principal, digamos $\mathfrak{p}_2 = \langle L_2\rangle_{\mathbb{F}}$. Debe existir una unidad U tal que $L_2^2\, U = 2$, $U = \pm U_{\mathbb{F}}^k$ para algún $k \in \mathbb{Z}$. Como $L_2^2 > 0$ y $2 > 0$, entonces $U = U_{\mathbb{F}}^k$. Escribamos $k = 2\,k_1 + k_2$ con $k_2 \in \{0, 1\}$. Puesto que $\langle L_2\rangle_{\mathbb{F}} = \left\langle L_2\, U_{\mathbb{F}}^{k_1}\right\rangle_{\mathbb{F}}$, podemos suponer que $k_1 = 0$. En el caso en que $k_2 = 0$, $L_2^2 = 2$ con $L_2 = l_1 + l_2\sqrt{p}$. De esto se sigue

$$2 = (l_1 + l_2\sqrt{p})^2 = l_1^2 + p\,l_2^2 + 2\,l_1\,l_2\,\sqrt{p}.$$

Por lo anterior, $l_1 = 0$ ó $l_2 = 0$. En el primer caso $l_2^2\, p = 2$ y en el segundo caso $l_1^2 = 2$, ambos casos son imposibles. Por lo tanto, $L_2^2\, U_{\mathbb{F}} = 2$. □

El elemento L_2 que aparece en la demostración del corolario anterior será importante para estudiar los enteros algebraicos con norma par en algunas extensiones de $\mathbb{F}$.

3.2. Generadores de $\mathcal{U}_{\mathbb{K}}$ y $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = \pm 2$

Sea $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con p un primo racional. En esta sección vamos a describir, en algunos casos, el grupo de unidades de $\mathcal{O}_{\mathbb{K}}$, así como la ramificación de 2 en $\mathbb{K}$. Primero encontraremos una familia de campos $\mathbb{K}$ en los que 2 se ramifica totalmente pero en los que el único ideal con norma 2 de $\mathcal{O}_{\mathbb{K}}$ no es principal.

Sea $\alpha = a_1 + a_2\, d^{1/4} + a_3\, d^{1/2} + a_4\, d^{3/4} \in \mathcal{O}_{\mathbb{K}}$. La norma de α es:

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}(\alpha) &= N_{\mathbb{F}/\mathbb{Q}}\left(N_{\mathbb{K}/\mathbb{F}}(\alpha)\right) \\ &= N_{\mathbb{F}/\mathbb{Q}}\left((\alpha)(a_1 - a_2\, d^{1/4} + a_3\, d^{1/2} - a_4\, d^{3/4})\right) \\ &= N_{\mathbb{F}/\mathbb{Q}}\left(a_1^2 + a_3^2\, d - 2\,a_2\,a_4\,d + \sqrt{d}(-a_2^2 + 2\,a_1\,a_3 - a_4^2\,d)\right) \\ &= (a_1^2 + a_3^2\, d - 2\,a_2\,a_4\,d)^2 - d(-a_2^2 + 2\,a_1\,a_3 - a_4^2\,d)^2 \\ &= a_1^4 - a_2^4\,d + 4\,a_1\,a_2^2\,a_3\,d - 2\,a_1^2\,a_3^2\,d - 4\,a_1^2\,a_2\,a_4\,d + a_3^4\,d^2 \\ &\quad -4\,a_2\,a_3^2\,a_4\,d^2 + 2\,a_2^2\,a_4^2\,d^2 + 4\,a_1\,a_3\,a_4^2\,d^2 - a_4^4\,d^3. \end{aligned}$$

Proposición 3.8. *Sean* $0 < p \equiv 3 \pmod 4$ *un primo racional y* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$. *El primo* 2 *se ramifica totalmente en* $\mathbb{K}$.

DEMOSTRACIÓN. Sea $\mathbb{F} = \mathbb{Q}(\sqrt{p})$. Como $p \equiv 3 \pmod 4$, entonces 2 se ramifica en $\mathcal{O}_{\mathbb{F}}$, $\langle 2\rangle_{\mathbb{F}} = \mathfrak{p}_2^2$, donde $\mathfrak{p}_2$ es el único ideal de $\mathcal{O}_{\mathbb{F}}$ con norma 2. Por la Proposición 3.6, $\mathfrak{p}_2$ es principal. Escribimos $\mathfrak{p}_2 = \langle L_2\rangle_{\mathbb{F}}$.

Consideremos el ideal $\mathfrak{I}_{\mathbb{K}} = \left\langle 2, 1 + \sqrt[4]{p}\right\rangle_{\mathbb{K}}$. Por la Proposición 1.22, $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}}) \mid N_{\mathbb{K}/\mathbb{Q}}(2) = 2^4$ y $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}}) \mid N_{\mathbb{K}/\mathbb{Q}}\left(1 + \sqrt[4]{p}\right) = 1 - p$. Como $p \equiv 3 \pmod 4$, entonces $1 - p \equiv 2 \pmod 4$. Por lo tanto existe $\mathfrak{J}_{\mathbb{K}}$ ideal de $\mathcal{O}_{\mathbb{K}}$ con $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{J}_{\mathbb{K}}) = 2$ y

$\mathfrak{J}_{\mathbb{K}} \supseteq \left\langle 1 + \sqrt[4]{p} \right\rangle_{\mathbb{K}}$. Por lo anterior, $2 \in \mathfrak{J}_{\mathbb{K}}$ y así $\mathfrak{J}_{\mathbb{K}} \mid \langle 2 \rangle_{\mathbb{K}}$. Puesto que $\mathfrak{J}_{\mathbb{K}}$ divide a los generadores de $\mathfrak{I}_{\mathbb{K}}$, entonces $\mathfrak{J}_{\mathbb{K}} \mid \mathfrak{I}_{\mathbb{K}}$. Además, $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}}) \leq \text{m.c.d.}\,(2^4, 1-p) = 2$, por lo que $\mathfrak{J}_{\mathbb{K}} = \mathfrak{I}_{\mathbb{K}}$ y $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}}) = 2$.

Notemos que $N_{\mathbb{K}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{K}}{}^2\right) = N_{\mathbb{K}/\mathbb{Q}}\left(\left\langle 4, 2 + 2\sqrt[4]{p}, (1+\sqrt[4]{p})^2 \right\rangle_{\mathbb{K}}\right) = 4$. Vamos a demostrar que $\mathfrak{I}_{\mathbb{K}}{}^2 = \langle L_2 \rangle_{\mathbb{K}}$. Como $|N_{\mathbb{F}/\mathbb{Q}}(L_2)| = 2$, entonces $L_2 \mid 2$ en $\mathcal{O}_{\mathbb{F}}$ y en $\mathcal{O}_{\mathbb{K}}$. Por esto, L_2 divide a los dos primeros generadores de $\mathfrak{I}_{\mathbb{K}}{}^2$. Veamos que $L_2 \mid (1+\sqrt[4]{p})^2$. En efecto, notamos

$$(1+\sqrt[4]{p})^2 = 1 + \sqrt{p} + 2\sqrt[4]{p} \quad \text{y} \quad N_{\mathbb{F}/\mathbb{Q}}(1+\sqrt{p}) = 1 - p \equiv 2 \pmod 4,$$

por lo que el único ideal con norma 2 de $\mathcal{O}_{\mathbb{F}}$ divide a $1+\sqrt{p}$. Entonces $L_2 \mid 1+\sqrt{p}$ en $\mathcal{O}_{\mathbb{F}}$ y en $\mathcal{O}_{\mathbb{K}}$. Como además $L_2 \mid 2\sqrt[4]{p}$, tenemos $L_2 \mid 1 + \sqrt{p} + 2\sqrt[4]{p}$. Por lo tanto

$$L_2 \mid 4, \quad L_2 \mid 2 + 2\sqrt{p}, \quad L_2 \mid (1+\sqrt[4]{p})^2$$

y así $\langle L_2 \rangle_{\mathbb{K}} \mid \mathfrak{I}_{\mathbb{K}}{}^2$. Para la otra contención, observemos

$$N_{\mathbb{K}/\mathbb{Q}}\left(\langle L_2 \rangle_{\mathbb{K}}\right) = N_{\mathbb{K}/\mathbb{Q}}(L_2) = N_{\mathbb{F}/\mathbb{Q}}\left(L_2^2\right) = N_{\mathbb{F}/\mathbb{Q}}(L_2)^2 = 2^2 = 4$$

y por tanto $\mathfrak{I}_{\mathbb{K}}{}^2 = \langle L_2 \rangle_{\mathbb{K}}$. Finalmente, $\mathfrak{I}_{\mathbb{K}}{}^4 = \langle L_2 \rangle_{\mathbb{K}}^2 = \langle \mathfrak{p}_2 \rangle_{\mathbb{K}}^2 = \langle \mathfrak{p}_2^2 \rangle_{\mathbb{K}} = \langle 2 \rangle_{\mathbb{K}}$, así que 2 se ramifica totalmente en $\mathbb{K}$ y $\mathfrak{I}_{\mathbb{K}}$ es el único ideal en $\mathcal{O}_{\mathbb{K}}$ de norma 2. □

Sea $a \in \mathbb{Z}$. Observemos que:

1. Si $a \equiv 0 \pmod 4$, entonces $a^2 \equiv 0 \pmod{16}$.
2. Si $a \equiv 2 \pmod 4$, entonces $a^2 \equiv 4 \pmod{16}$.
3. Si $a \equiv \pm 1 \pmod 8$, entonces $a^2 \equiv 1 \pmod{16}$.
4. Si $a \equiv \pm 3 \pmod 8$, entonces $a^2 \equiv 9 \pmod{16}$.

Proposición 3.9. *Sean $d \equiv 7 \pmod{16}$ libre de cuadrados, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$ y el ideal $\mathfrak{I}_{\mathbb{K}} = \left\langle 2, 1+\sqrt[4]{d} \right\rangle_{\mathbb{K}}$. Entonces, $\mathfrak{I}_{\mathbb{K}}$ no es principal.*

DEMOSTRACIÓN. Sea $\alpha = a_1 + a_2\sqrt[4]{d} + a_3\sqrt{d} + a_4\sqrt[4]{d^3} \in \mathcal{O}_{\mathbb{K}}$. Vamos a mostrar que $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \neq \pm 2$. Un cálculo elemental nos muestra

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}(\alpha) &\equiv a_1^4 + a_2^4 + a_3^4 + a_4^4 + 2\,a_1^2\,a_3^2 + 2\,a_2^2\,a_4^2 \\ &\equiv (a_1^2 + a_3^2)^2 + (a_2^2 + a_4^2)^2 \pmod 4, \end{aligned} \tag{12}$$

y en general, para que $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ sea par, es necesario que α tenga un número par de coeficientes pares y, por lo mismo, un número par de coeficientes impares. Si todos los a_i's son pares, entonces $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 0 \pmod 4$, así que en este caso $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \neq \pm 2$. Si todos los a_i's son impares, entonces $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 0 \pmod 4$ y $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \neq \pm 2$. Entonces, dos a_i's son pares y dos impares.

Si a_1 y a_3 tienen la misma paridad, entonces a_2 y a_4 tienen la misma paridad con lo cual $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 0 \pmod 4$ y $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \neq \pm 2$. Por lo anterior, $a_1 \not\equiv a_3 \pmod 2$ y $a_2 \not\equiv a_4 \pmod 2$. Nuevamente observemos que

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}(\alpha) &\equiv a_1^4 + 9\,a_2^4 + a_3^4 + 9\,a_4^4 + 2\,a_1^2\,a_3^2 + 2\,a_2^2\,a_4^2 \\ &\quad +12\,a_1\,a_2^2\,a_3 + 4\,a_1^2\,a_2\,a_4 + 12\,a_2\,a_3^2\,a_4 + 4\,a_1\,a_3\,a_4^2 \\ &\equiv (a_1^2 + a_3^2)^2 + 9(a_2^2 + a_4^2)^2 \\ &\quad +4\,a_1\,a_3(3\,a_2^2 + a_4^2) + 4\,a_2\,a_4(a_1^2 + 3a_3^2) \pmod{16}. \end{aligned} \tag{13}$$

Supongamos $a_1 \equiv 0 \pmod 4$. En este caso $a_1^2 \equiv 0 \pmod{16}$ y como a_3 es impar, entonces $a_3^2 \equiv 1, 9 \pmod{16}$. En cualquiera de los dos casos $(a_1^2 + a_3^2)^2 \equiv 1 \pmod{16}$. Además, $4\,a_1 \equiv 0 \pmod{16}$, por lo que $(a_1^2 + a_3^2)^2 + 4\,a_1\,a_3(3\,a_2^2 + a_4^2) \equiv 1 \pmod{16}$. Ahora supongamos $a_1 \equiv 2 \pmod 4$. Como $a_1^2 \equiv 4 \pmod{16}$, entonces $(a_1^2 + a_3^2)^2 \equiv 9 \pmod{16}$. Como a_3 y $(3a_2^2 + a_4^2)$ son impares, entonces $4\,a_1\,a_3(3\,a_2^2 + a_4^2) \equiv 8 \pmod{16}$, por lo que en este caso también $(a_1^2 + a_3^2)^2 + 4\,a_1\,a_3(3\,a_2^2 + a_4^2) \equiv 1 \pmod{16}$. Si a_1 es impar y a_3 es par, sucede algo similar, así que para todas las posibilidades de a_1 y a_3, $(a_1^2 + a_3^2)^2 + 4\,a_1\,a_3(3\,a_2^2 + a_4^2) \equiv 1 \pmod{16}$.

De manera análoga, tenemos $9(a_2^2 + a_4^2)^2 + 4\,a_2\,a_4(a_1^2 + 3a_3^2) \equiv 9 \pmod{16}$, por lo que $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 10 \pmod{16}$ ó $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 0 \pmod 4$. En cualquiera de los dos casos $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \neq \pm 2$. □

Sea $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$ para un valor d libre de cuadrados y $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. A continuación, daremos condiciones para decidir si la raíz cuadrada de un elemento de $\mathcal{O}_\mathbb{K}$ está en $\mathcal{O}_\mathbb{K}$. Este resultado nos servirá para estudiar al grupo $\mathcal{U}_\mathbb{K}$.

Notemos que el polinomio irreducible de α en $\mathcal{O}_\mathbb{F}[x]$ es:

$$f(x) = x^2 - 2(a_1 + a_3\sqrt{d})x + N_{\mathbb{K}/\mathbb{F}}(\alpha).$$

Proposición 3.10. *Sean $d \in \mathbb{Z}$ impar libre de cuadrados, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{d})$, $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, $f(x) = x^2 + A_1x + A_0 \in \mathcal{O}_\mathbb{F}[x]$, $\alpha \in \mathbb{C}$ con $f(\alpha) = 0$ y $\Delta_f = A_1^2 - 4A_0$. Entonces $\alpha \in \mathcal{O}_\mathbb{K}$ si y sólo si existe $C \in \mathcal{O}_\mathbb{F}$ tal que $\Delta_f = C^2$ ó $\Delta_f = C^2\sqrt{d}$. En el primer caso $\alpha \in \mathcal{O}_\mathbb{F}$, en el segundo $\alpha \in \mathcal{O}_\mathbb{K} - \mathcal{O}_\mathbb{F}$.*

DEMOSTRACIÓN. Como f es mónico y sus coeficientes son enteros algebraicos, entonces las raíces de f deben ser enteros algebraicos. Ésta es la razón por la que si $f(\alpha) = 0$ y $\alpha \in \mathbb{K}$, entonces $\alpha \in \mathcal{O}_\mathbb{K}$. En particular, si $\alpha \in \mathcal{O}_\mathbb{F}$ tenemos

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

para algún $\beta \in \mathcal{O}_\mathbb{F}$. Así

$$\begin{aligned} \Delta_f &= (\alpha + \beta)^2 - 4\,\alpha\,\beta = \alpha^2 + 2\,\alpha\,\beta + \beta^2 - 4\,\alpha\,\beta \\ &= \alpha^2 - 2\,\alpha\,\beta + \beta^2 = (\alpha - \beta)^2. \end{aligned}$$

Si $\alpha \in \mathcal{O}_\mathbb{K} - \mathcal{O}_\mathbb{F}$, existen $A_1, A_2 \in \mathbb{F}$ tales que $\alpha = A_1 + A_2\sqrt[4]{d}$. De lo anterior

$$f(x) = x^2 - t_{\mathbb{K}/\mathbb{F}}(\alpha)x + N_{\mathbb{K}/\mathbb{F}}(\alpha) = x^2 - 2\,A_1x + A_1^2 - \sqrt{d}\,A_2^2,$$

y por tanto

$$\Delta_f = (-2A_1)^2 - 4(A_1^2 - \sqrt{d}\,A_2^2) = 4\,A_1^2 - 4\,A_1^2 + \sqrt{d}\,4\,A_2^2 = \sqrt{d}\,4\,A_2^2.$$

Sea $C = 2A_2 \in \mathbb{F}$. Vamos a mostrar que $C \in \mathcal{O}_\mathbb{F}$.

Por la Proposición 1.7, si $d \equiv 1 \pmod 8$, $A_2 = \dfrac{a_1 + a_2\sqrt{d}}{4}$ para algunos $a_1, a_2 \in \mathbb{Z}$ con $a_1 \equiv a_2 \pmod 2$. Así, $C = 2\,A_2 \in \mathcal{O}_\mathbb{F}$. En cualquier otro caso, $2\,A_2 \in \mathbb{Z}[\sqrt{d}]$, por lo que claramente $C \in \mathcal{O}_\mathbb{F}$. La demostración de la suficiencia es directa. □

Sea $f(x) = x^2 - Ax + B^2$ un polinomio con coeficientes en $\mathcal{O}_\mathbb{F}$ cuyas raíces están en $\mathcal{O}_\mathbb{K}$. El resultado anterior nos indica que existe $C \in \mathcal{O}_\mathbb{F}$ tal que $\Delta_f = A^2 - 4B^2 = (A + 2B)(A - 2B) = C^2\sqrt{d}$.

Proposición 3.11. *Sean $\alpha > 0$ un elemento de $\mathcal{O}_{\mathbb{K}} - \mathcal{O}_{\mathbb{F}}$ tal que $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = B^2$ para algún $B \in \mathcal{O}_{\mathbb{F}}$ y $f(x) = \mathrm{Irr}(\alpha, \mathcal{O}_{\mathbb{F}}) = x^2 - Ax + B^2$. Existe $C \in \mathcal{O}_{\mathbb{F}}$ tal que $C^2 = A \pm 2B$ para alguno de los dos signos si y sólo si $\sqrt{\alpha} \in \mathcal{O}_{\mathbb{K}}$.*

DEMOSTRACIÓN. Sea $g(x) = x^2 + Cx \mp B$ y $h(x) = x^2 - Cx \mp B$, donde el signo es el contrario al que aparece en $C^2 = A \pm 2B$.

$$\begin{aligned} g(x)h(x) &= (x^2 + Cx \mp B)(x^2 - Cx \mp B) = x^4 - (C^2 \pm 2\,B)x^2 + B^2 \\ &= x^4 - Ax^2 + B^2. \end{aligned}$$

Observemos que $g(x)h(x) = f(x^2)$ y $f(\sqrt{\alpha}^2) = g(\sqrt{\alpha})h(\sqrt{\alpha}) = f(\alpha) = 0$. Por lo anterior, $g(\sqrt{\alpha}) = 0$ ó $h(\sqrt{\alpha}) = 0$. Esto quiere decir que $\sqrt{\alpha}$ está en una extensión de grado 1 ó 2 sobre $\mathbb{F}$ y además, por cerradura, $\sqrt{\alpha}^2 = \alpha \in \mathbb{F}(\sqrt{\alpha})$. Por otra parte, sabemos que $\mathbb{F}(\alpha) = \mathbb{K}$ es una extensión de grado 2 sobre $\mathbb{F}$, donde $\mathbb{F}(\alpha) \subseteq \mathbb{F}(\sqrt{\alpha})$. Entonces, $\mathbb{K} = \mathbb{F}(\sqrt{\alpha})$ y por lo tanto $\sqrt{\alpha} \in \mathbb{K}$.

Ahora supongamos que $\sqrt{\alpha} \in \mathcal{O}_{\mathbb{K}}$. Como $f(\alpha) = 0$, entonces $\sqrt{\alpha}$ es una raíz de $f(x^2)$. El polinomio irreducible de $\sqrt{\alpha}$ debe dividir a $f(x^2)$ y como α es un elemento de $\mathcal{O}_{\mathbb{K}} - \mathcal{O}_{\mathbb{F}}$, entonces el grado de dicho polinomio debe ser 2. Supongamos que $x^4 - Ax^2 + B^2 = (x^2 + C_1x + C_2)(x^2 + D_1x + D_2)$ para algunos $C_1, C_2, D_1, D_2 \in \mathcal{O}_{\mathbb{F}}$.

$$f(x^2) = x^4 + (C_1 + D_1)x^3 + (C_1D_1 + D_2 + C_2)x^2 + (C_1D_2 + C_2D_1)x + C_2D_2.$$

Por esto, $C_1 + D_1 = 0$, lo que implica que $D_1 = -C_1$. Si $C_1 = 0$, entonces $D_1 = 0$ y $f(x^2) = (x^2 + C_2)(x^2 + D_2)$, de donde $f(x) = (x + C_2)(x + D_2) \neq \mathrm{Irr}(\alpha, \mathcal{O}_{\mathbb{F}})$. Entonces $C_1 \neq 0$. Por lo anterior, $C_1D_2 + C_2D_1 = 0$ y así $D_2 = C_2$. Ahora

$$\begin{aligned} x^4 - Ax^2 + B^2 &= (x^2 + C_1x + C_2)(x^2 - C_1x + C_2) \\ &= x^4 - (C_1^2 - 2C_2)x^2 + C_2^2. \end{aligned}$$

De esta igualdad se observa que $C_2 = \pm B$ y por tanto $C = C_1$ satisface la proposición. □

Usaremos el resultado anterior para mostrar:

Proposición 3.12. *Sean $p \equiv 3 \pmod 4$ un primo racional positivo, $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ y $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$. Si $\alpha \in \mathcal{O}_{\mathbb{K}}$, entonces $N_{\mathbb{K}/\mathbb{F}}(\alpha) \neq -1$.*

DEMOSTRACIÓN. Como $N_{\mathbb{F}/\mathbb{Q}}\left(\sqrt{p}\right) = -p$, entonces $\mathcal{O}_{\mathbb{F}}/\left\langle\sqrt{p}\right\rangle_{\mathbb{F}} \cong \mathbb{Z}/p\mathbb{Z}$. Adicionalmente $a_1 + a_2\sqrt{p} \equiv a_1 \pmod{\left\langle\sqrt{p}\right\rangle_{\mathbb{F}}}$, así que toda clase en $\mathcal{O}_{\mathbb{F}}/\left\langle\sqrt{p}\right\rangle_{\mathbb{F}}$ tiene un representante en $\mathbb{Z}$. La función $\phi : \mathcal{O}_{\mathbb{F}}/\left\langle\sqrt{p}\right\rangle_{\mathbb{F}} \to \mathbb{Z}/p\mathbb{Z}$ definida como $\phi(1 + \left\langle\sqrt{p}\right\rangle_{\mathbb{F}}) = 1 + p\mathbb{Z}$ es un isomorfismo de campos. Puesto que $p \equiv 3 \pmod 4$ y $\left(\dfrac{-1}{p}\right) = -1$, no existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod{\left\langle\sqrt{p}\right\rangle_{\mathbb{F}}}$.

Si $\alpha = A_1 + A_2\sqrt[4]{p}$ con $A_1, A_2 \in \mathcal{O}_{\mathbb{F}}$, entonces $N_{\mathbb{K}/\mathbb{F}}(\alpha) = A_1^2 - A_2^2\sqrt{p}$. Así que $N_{\mathbb{K}/\mathbb{F}}(\alpha)$ es un cuadrado en $\mathcal{O}_{\mathbb{F}}$ módulo $\left\langle\sqrt{p}\right\rangle_{\mathbb{F}}$, por lo que $N_{\mathbb{K}/\mathbb{F}}(\alpha) \not\equiv -1 \pmod{\left\langle\sqrt{p}\right\rangle_{\mathbb{F}}}$. Por lo tanto, $N_{\mathbb{K}/\mathbb{F}}(\alpha) \neq -1$. □

Sea $a_1 + a_2\sqrt{d} \in \mathcal{O}_{\mathbb{F}}$ con $d \equiv 3 \pmod 4$ y $(a_1 + a_2\sqrt{d})^2 = a_1^2 + d\,a_2^2 + 2\,a_1\,a_2\,\sqrt{d}$. Si a_1 y a_2 son pares, entonces $(a_1 + a_2\sqrt{d})^2 \equiv 0 \pmod 4$. Si ambos son impares, entonces $(a_1 + a_2\sqrt{d})^2 \equiv 1 + 3 + 2\sqrt{d} \equiv 2\sqrt{d} \pmod 4$. Si a_1 es par y a_2 impar, tenemos $(a_1 +$

$a_2\sqrt{d})^2 \equiv 4 + 3 + 4\sqrt{d} \equiv 3 \pmod 4$. Finalmente, si a_1 es impar y a_2 par, entonces $(a_1 + a_2\sqrt{d})^2 \equiv 1 \pmod 4$. Así que los cuadrados en $\mathbb{Z}[\sqrt{d}]$ módulo 4 son 0, 1, 3 y $2\sqrt{d}$.

Por la Proposición 1.7, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt[4]{d}]$, así que un elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ es de la forma $A_1 + A_2\sqrt[4]{d}$, donde $A_1, A_2 \in \mathcal{O}_{\mathbb{F}}$ y $N_{\mathbb{K}/\mathbb{F}}(\alpha) = A_1^2 - \sqrt{d}\,A_2^2$. De la observación anterior, sólo hay dos posibilidades para que $N_{\mathbb{K}/\mathbb{F}}(\alpha) = 1$: $A_1^2 \equiv 1 \pmod 4$ y $A_2^2 \equiv 0 \pmod 4$, o bien, $A_1^2 \equiv 3 \pmod 4$ y $A_2^2 \equiv 2\sqrt{d} \pmod 4$. Si $A_1 = a_1 + a_2\sqrt{d}$ y $A_2 = a_3 + a_4\sqrt{d}$ con $a_1, a_2, a_3, a_4 \in \mathbb{Z}$, entonces a_1 es impar y a_2, a_3, a_4 son pares o bien a_1 es par y a_2, a_3, a_4 son impares.

La parte importante del siguiente resultado es la afirmación 4, las tres primeras son el antecedente para demostrarlo.

Proposición 3.13. *Sea $p \equiv 7 \pmod 8$ un primo racional positivo. Si $\mu \in \mathcal{U}_{\mathbb{K}}$ es tal que $\mu = m_1 + m_2\sqrt[4]{p} + m_3\sqrt{p} + m_4\sqrt[4]{p^3}$ y $N_{\mathbb{K}/\mathbb{F}}(\mu) = 1$ con m_1 par, entonces:*

1. *Si $L_2 \in \mathcal{O}_{\mathbb{F}}$ es tal que $L_2^2\,U_{\mathbb{F}} = 2$, entonces, para ambos signos, $L_2 \mid m_1 \pm 1 + m_3\sqrt{p}$ pero $2 \nmid m_1 \pm 1 + m_3\sqrt{p}$ en $\mathcal{O}_{\mathbb{F}}$.*
2. $\left\langle \dfrac{m_1 + 1 + m_3\sqrt{p}}{L_2} \right\rangle + \left\langle \dfrac{m_1 - 1 + m_3\sqrt{p}}{L_2} \right\rangle = \mathcal{O}_{\mathbb{F}}$.
3. *Existe $B \in \mathcal{O}_{\mathbb{F}}$ tal que $\dfrac{m_1 \pm 1 + m_3\sqrt{p}}{L_2} = B^2\,U$ para uno de los dos signos y $U = 1$ ó $U = U_{\mathbb{F}}$.*
4. *Existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $|N_{\mathbb{K}/\mathbb{Q}}(\alpha)| = 2$.*

DEMOSTRACIÓN. Como $m_1 \pm 1$ es impar y m_3 es impar, entonces $(m_1 + 1)^2 - p\,m_3^2 \equiv 1 - 3(1) \equiv 2 \pmod 4$. Por la Proposición 3.6, $\langle L_2\rangle_{\mathbb{F}}$ es el único ideal de $\mathcal{O}_{\mathbb{F}}$ con norma 2 y $\langle 2\rangle_{\mathbb{F}} = \langle L_2\rangle_{\mathbb{F}}^2$, entonces $L_2 \mid m_1 \pm 1 + m_3\sqrt{p}$ en $\mathcal{O}_{\mathbb{F}}$ y $2 \nmid m_1 \pm 1 + m_3\sqrt{p}$.

Notemos que $(m_1 + 1 + m_3\sqrt{p}) - (m_1 - 1 + m_3\sqrt{p}) = 2$, es decir

$$\langle m_1 + 1 + m_3\sqrt{p}\rangle_{\mathbb{F}} + \langle m_1 - 1 + m_3\sqrt{p}\rangle_{\mathbb{F}} \supseteq \langle 2\rangle_{\mathbb{F}},$$

por lo que las opciones para la suma son $\mathcal{O}_{\mathbb{F}}$, $\langle L_2\rangle_{\mathbb{F}}$ y $\langle 2\rangle_{\mathbb{F}}$. Usando 1

$$\langle m_1 + 1 + m_3\sqrt{p}\rangle_{\mathbb{F}} + \langle m_1 - 1 + m_3\sqrt{p}\rangle_{\mathbb{F}} = \langle L_2\rangle_{\mathbb{F}},$$

y por lo tanto la afirmación 2 es válida.

El polinomio irreducible de μ con coeficientes en $\mathcal{O}_{\mathbb{F}}$ es

$$f(x) = \operatorname{Irr}(\mu, \mathcal{O}_{\mathbb{F}}) = x^2 - 2(m_1 + m_3\sqrt{p})\,x + 1.$$

Como las raíces de f están en $\mathcal{O}_{\mathbb{K}}$, entonces, por la Proposición 3.10 tenemos

$$\Delta_f = 4(m_1 + m_3\sqrt{p})^2 - 4 = 4(m_1 + 1 + m_3\sqrt{p})(m_1 - 1 + m_3\sqrt{p}) = C^2\sqrt{p}.$$

Usando lo anterior,

$$\langle 2\,L_2\rangle_{\mathbb{F}}^2 \left\langle \frac{m_1 + 1 + m_3\sqrt{p}}{L_2} \right\rangle_{\mathbb{F}} \left\langle \frac{m_1 - 1 + m_3\sqrt{p}}{L_2} \right\rangle_{\mathbb{F}} = \langle C\rangle_{\mathbb{F}}^2\,\langle\sqrt{p}\rangle_{\mathbb{F}}. \tag{14}$$

Por la factorización única en el conjunto de ideales $\neq \langle 0\rangle_{\mathbb{F}}$ de $\mathcal{O}_{\mathbb{F}}$ y por la afirmación 2 tenemos

$$\langle\sqrt{p}\rangle_{\mathbb{F}} \supseteq \left\langle \frac{m_1 + 1 + m_3\sqrt{p}}{L_2} \right\rangle_{\mathbb{F}} \quad \text{ó} \quad \langle\sqrt{p}\rangle_{\mathbb{F}} \supseteq \left\langle \frac{m_1 - 1 + m_3\sqrt{p}}{L_2} \right\rangle_{\mathbb{F}},$$

pero no ambas. Denotemos por $\mathfrak{I}_{\mathbb{F}}, \mathfrak{I}'_{\mathbb{F}}$ a los ideales de la discusión previa tal que $\left\langle \sqrt{p} \right\rangle_{\mathbb{F}} \nmid \mathfrak{I}_{\mathbb{F}}$ y $\left\langle \sqrt{p} \right\rangle_{\mathbb{F}} \mid \mathfrak{I}'_{\mathbb{F}}$. Podemos dividir entre $\langle 2\, L_2 \rangle_{\mathbb{F}}^2 \left\langle \sqrt{p} \right\rangle_{\mathbb{F}}$ en (14) para obtener

$$\mathfrak{I}_{\mathbb{F}} \left(\frac{\mathfrak{I}'_{\mathbb{F}}}{\left\langle \sqrt{p} \right\rangle_{\mathbb{F}}} \right) = \left(\frac{\langle C \rangle_{\mathbb{F}}}{\langle 2L_2 \rangle_{\mathbb{F}}} \right)^2,$$

donde todos los ideales que aparecen en esta igualdad son ideales enteros. Por 2, $\mathfrak{I}_{\mathbb{F}} + \left(\frac{\mathfrak{I}'_{\mathbb{F}}}{\left\langle \sqrt{p} \right\rangle_{\mathbb{F}}} \right) = \mathcal{O}_{\mathbb{F}}$, así $\mathfrak{I}_{\mathbb{F}} = {\mathfrak{J}_{\mathbb{F}}}^2$, para algún ideal $\mathfrak{J}_{\mathbb{F}}$. Como $h_{\mathbb{F}}$ es impar y $\mathfrak{I}_{\mathbb{F}}$ es principal, entonces $\mathfrak{J}_{\mathbb{F}}$ es principal. Sea $\mathfrak{J}_{\mathbb{F}} = \langle B \rangle_{\mathbb{F}}$. Esto quiere decir que para uno de los dos signos y una unidad U tenemos:

$$\frac{m_1 \pm 1 + m_3\sqrt{p}}{L_2} = B^2 U. \tag{15}$$

Podemos suponer que $U = 1$ ó $U = U_{\mathbb{F}}$ la unidad fundamental de $\mathcal{O}_{\mathbb{F}}$, pues si $U = U_{\mathbb{F}}^{2k_1+k_2}$ con $k_2 \in \{0, 1\}$, entonces $\left\langle B U_{\mathbb{F}}^{k_1} \right\rangle_{\mathbb{F}} = \langle B \rangle_{\mathbb{F}}$, así que en lugar de tomar el generador B tomamos $B U_{\mathbb{F}}^{k_1}$. Con esto hemos demostrado la afirmación 3.

Para la afirmación 4, dividimos la prueba en dos casos. Si $U = U_{\mathbb{F}}$, multiplicamos (15) por $2L_2^2$. Así tenemos

$$2\, L_2\, (m_1 \pm 1 + m_3\sqrt{p}) = 2\, B^2 U_{\mathbb{F}}\, L_2^2.$$

Como $L_2^2\, U_{\mathbb{F}} = 2$ tenemos

$$(2\, B)^2 = 2\, L_2\, (m_1 + m_3\sqrt{p}) \pm 2\, L_2. \tag{16}$$

Puesto que las raíces del polinomio $f(x) = x^2 - 2(m_1 + m_3\sqrt{p})\, x + 1$ tienen norma en $\mathbb{K}/\mathbb{F}$ igual a 1, entonces

$$\begin{aligned} g(x) &= L_2^2\, f\left(\frac{x}{L_2} \right) \\ &= L_2^2 \left(\left(\frac{x}{L_2} \right)^2 - 2(m_1 + m_3\sqrt{p}) \left(\frac{x}{L_2} \right) + 1 \right) \\ &= x^2 - 2\, L_2\, (m_1 + m_3\sqrt{p})\, x + L_2^2 \in \mathcal{O}_{\mathbb{F}}[x]. \end{aligned}$$

Sea $\beta = \mu\, L_2 \in \mathcal{O}_{\mathbb{K}}$. Claramente $g(\beta) = 0$ y

$$N_{\mathbb{K}/\mathbb{Q}}(\beta) = N_{\mathbb{K}/\mathbb{Q}}(\mu) N_{\mathbb{K}/\mathbb{Q}}(L_2) = 4.$$

Por la Proposición 3.11, la definición de $g(x)$ y la ecuación (16), tenemos que $\sqrt{\beta} \in \mathcal{O}_{\mathbb{K}}$ y $N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{\beta}\right) = \pm 2$.

Si $U = 1$, multiplicamos (15) por $2\, L_2^2\, U_{\mathbb{F}}$ y obtenemos

$$2\, L_2\, U_{\mathbb{F}}\, (m_1 \pm 1 + m_3\sqrt{p}) = 2\, B^2 U_{\mathbb{F}}\, L_2^2.$$

Si $g(x) = (L_2\, U_{\mathbb{F}})^2\, f\left(\frac{x}{L_2\, U_{\mathbb{F}}} \right)$ y $\beta = \mu\, L_2\, U_{\mathbb{F}}$, entonces $g(\beta) = 0$, $N_{\mathbb{K}/\mathbb{Q}}(\beta) = 4$. Por tanto, $\sqrt{\beta} \in \mathcal{O}_{\mathbb{K}}$ y $N_{\mathbb{K}/\mathbb{Q}}\left(\sqrt{\beta}\right) = \pm 2$. □

Corolario 3.14. *Sean $p \equiv 7 \pmod{16}$ un primo racional positivo, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ y $\mu = m_1 + m_2\sqrt[4]{p} + m_3\sqrt{p} + m_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ una unidad con $N_{\mathbb{K}/\mathbb{F}}(\mu) = 1$. Entonces, m_1 es impar y m_2, m_3, m_4 son pares.*

DEMOSTRACIÓN. Es consecuencia de la Proposición 3.9 y de la contrapositiva de la afirmación 4 de la Proposición 3.13. □

Sean $\mathcal{U}_{\mathbb{K}}$ y $\mathcal{U}_{\mathbb{F}}$ los grupos de unidades de $\mathbb{K}$ y $\mathbb{F}$ respectivamente. Si $\mu \in \mathcal{U}_{\mathbb{K}}$, entonces $N_{\mathbb{K}/\mathbb{F}}(\mu) \in \mathcal{U}_{\mathbb{F}}$, pues $|N_{\mathbb{F}/\mathbb{Q}}\left(N_{\mathbb{K}/\mathbb{F}}(\mu)\right)| = 1$. Por el Teorema de las Unidades de Dirichlet, $\mathcal{U}_{\mathbb{K}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$. Así que $\mathcal{U}_{\mathbb{K}}$ se puede describir con tres generadores, uno de ellos es -1. Sea $\mathcal{U}_{\mathbb{K}} = \langle -1, \mu_1, \mu_2 \rangle$. Si $U_{\mathbb{F}}$ es la unidad fundamental de $\mathbb{F}$, $N_{\mathbb{K}/\mathbb{F}}(U_{\mathbb{F}}) = U_{\mathbb{F}}^2$. Esto, junto con el hecho de que la norma relativa es una función multiplicativa, nos muestra que no es posible que $N_{\mathbb{K}/\mathbb{F}}(\mu_1) = N_{\mathbb{K}/\mathbb{F}}(\mu_2) = 1$, pues en este caso todos los elementos de $\mathcal{U}_{\mathbb{K}}$ tendrían norma relativa 1.

Supongamos que $N_{\mathbb{K}/\mathbb{F}}(\mu_1) = U_{\mathbb{F}}^{k_1}$ y $N_{\mathbb{K}/\mathbb{F}}(\mu_2) = U_{\mathbb{F}}^{k_2}$ con k_1 y k_2 distintos de cero. Puesto que $\langle -1, \mu_1, \mu_2 \rangle = \left\langle -1, \mu_1^{-1}, \mu_2 \right\rangle$, entonces podemos suponer que $0 < k_1 \leq k_2$. Otra igualdad de grupos que es cierta es

$$\langle -1, \mu_1, \mu_2 \rangle = \left\langle -1, \mu_1, \mu_2\mu_1^k \right\rangle. \tag{17}$$

para cualquier $k \in \mathbb{Z}$. Consideremos los únicos enteros q, r tales que $k_2 = k_1 q + r$ con $0 \leq r < k_1$. Usando $k = -q$ en (17) obtenemos una nueva representación de $\mathcal{U}_{\mathbb{K}}$. En este caso,

$$N_{\mathbb{K}/\mathbb{F}}\left(\mu_2\mu_1^k\right) = N_{\mathbb{K}/\mathbb{F}}(\mu_2)N_{\mathbb{K}/\mathbb{F}}(\mu_1)^k = U_{\mathbb{F}}^{k_2}(U_{\mathbb{F}}^{k_1})^{-q} = U_{\mathbb{F}}^{k_2 - k_1 q} = U_{\mathbb{F}}^r.$$

De esta forma, el nuevo valor de k_2 es más pequeño que el que teníamos anteriormente, pero sigue siendo mayor o igual a cero. Si continuamos con este procedimiento, lo que estamos haciendo es seguir el algoritmo de Euclides para encontrar el máximo común divisor de k_1 y k_2, así que en algún momento $r = 0$ y tendremos un conjunto de generadores en el que $N_{\mathbb{K}/\mathbb{F}}(\mu_1) = U_{\mathbb{F}}^0 = 1$ ó $N_{\mathbb{K}/\mathbb{F}}(\mu_2) = 1$. Por lo anterior, podemos encontrar un conjunto de generadores de

$$\mathcal{U}_{\mathbb{K}} = \langle -1, \mu_1, \mu_2 \rangle$$

con $N_{\mathbb{K}/\mathbb{F}}(\mu_1) = 1$ y $N_{\mathbb{K}/\mathbb{F}}(\mu_2) \neq 1$. Si $N_{\mathbb{K}/\mathbb{F}}(\mu_2) = U_{\mathbb{F}}^{k_2}$, k_2 debe de ser el mínimo entero positivo tal que $U_{\mathbb{F}}^{k_2}$ es una norma relativa. Como $N_{\mathbb{K}/\mathbb{F}}(U_{\mathbb{F}}) = U_{\mathbb{F}}^2$, entonces $k_2 \in \{1, 2\}$.

Proposición 3.15. *Sean $p \equiv 7 \pmod{16}$ un primo positivo, $\mathbb{F} = \mathbb{Q}(\sqrt{p})$, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, $U_{\mathbb{F}}$ la unidad fundamental de $\mathbb{F}$ y $\mathcal{U}_{\mathbb{K}} = \langle -1, \mu_1, \mu_2 \rangle$ el grupo de unidades de $\mathcal{O}_{\mathbb{K}}$ con $N_{\mathbb{K}/\mathbb{F}}(\mu_1) = 1$. Entonces, $\sqrt{\mu_1\, U_{\mathbb{F}}} \in \mathcal{O}_{\mathbb{K}}$.*

DEMOSTRACIÓN. Como $\mu_1 = m_1 + m_2\sqrt[4]{p} + m_3\sqrt{p} + m_4\sqrt[4]{p^3}$ genera todas las unidades con norma relativa 1, entonces μ_1 no puede tener raíz cuadrada en $\mathcal{O}_{\mathbb{K}}$. Sea $f(x) = x^2 - 2(m_1 + m_3\sqrt{p})x + 1$ el polinomio irreducible de μ_1 con coeficientes en $\mathcal{O}_{\mathbb{F}}$. La Proposición 3.11 nos indica que no existe $C \in \mathcal{O}_{\mathbb{F}}$ tal que $C^2 = 2(m_1 \pm 1 + m_3\sqrt{p})$ para ninguno de los dos signos.

Por otro lado, como $\mu_1 \in \mathcal{O}_{\mathbb{K}}$, entonces, por la Proposición 3.10 debe existir $D \in \mathcal{O}_{\mathbb{F}}$ tal que:

$$\begin{aligned} \Delta_f &= 4(m_1 + m_2\sqrt{p})^2 - 4 \\ &= 4(m_1 + 1 + m_2\sqrt{p})(m_1 - 1 + m_2\sqrt{p}) \\ &= D^2\sqrt{p} \end{aligned}$$

Usando las mismas ideas de la demostración de la Proposición 3.13, la igualdad anterior implica que para uno de los dos signos

$$2(m_1 \pm 1 + m_2\sqrt{p}) = B^2\, U, \tag{18}$$

donde $U = 1$ ó $U = U_{\mathbb{F}}$. Por lo anterior, $U \neq 1$ porque $\sqrt{\mu} \notin \mathcal{O}_{\mathbb{K}}$. Multiplicando (18) por $U_{\mathbb{F}}$ en ambos lados de la igualdad tenemos:

$$2(m_1 \pm 1 + m_2\sqrt{p})U_{\mathbb{F}} = (B\, U_{\mathbb{F}})^2. \tag{19}$$

Sea $g(x) = U_{\mathbb{F}}^2\, f\left(\dfrac{x}{U_{\mathbb{F}}}\right) = x^2 - 2(m_1 + m_3\sqrt{p})U_{\mathbb{F}}\, x + U_{\mathbb{F}}^2$. Claramente $g(\mu_1\, U_{\mathbb{F}}) = 0$. Por la Proposicioń 3.11, si $\sqrt{\mu_1 U_{\mathbb{F}}} \in \mathcal{O}_{\mathbb{K}}$, entonces

$$2(m_1 + m_3\sqrt{p})U_{\mathbb{F}} \pm 2\, U_{\mathbb{F}} = 2(m_1 \pm 1 + m_3\sqrt{p})U_{\mathbb{F}}$$

debe ser un cuadrado para alguno de los dos signos. Esta condición se cumple por la ecuación (19). Así que $\sqrt{\mu_1\, U_{\mathbb{F}}} \in \mathcal{O}_{\mathbb{K}}$. □

Como $N_{\mathbb{K}/\mathbb{F}}\left(\sqrt{\mu_1\, U_{\mathbb{F}}}\right)^2 = N_{\mathbb{K}/\mathbb{F}}\left(\mu_1\, U_{\mathbb{F}}\right) = U_{\mathbb{F}}^2$, entonces $N_{\mathbb{K}/\mathbb{F}}\left(\sqrt{\mu_1\, U_{\mathbb{F}}}\right) = \pm U_{\mathbb{F}}$. Por lo tanto

$$\mathcal{U}_{\mathbb{K}} = \langle -1, \mu_1, \mu_2 \rangle,$$

donde $N_{\mathbb{K}/\mathbb{F}}\left(\mu_1\right) = 1$ y $N_{\mathbb{K}/\mathbb{F}}\left(\mu_2\right) = \pm U_{\mathbb{F}}$. Con esto concluimos el objetivo de esta sección.

3.3. Bases enteras

Consideremos los campos $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ para algún α en $\mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones. Vamos a encontrar bases enteras de algunos campos $\mathbb{L}$; para esto, será necesario estudiar propiedades generales de las mismas. Como vimos en el Capítulo 1, las bases enteras nos ayudan a calcular discriminantes y éstos, a su vez, nos sirven para estudiar la ramificación en $\mathbb{L}/\mathbb{K}$.

3.3.1. Generalidades

Sea $\mathbb{F}$ un campo de números y $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$, $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ dos bases de $\mathbb{F}$ como $\mathbb{Q}$-espacio vectorial con $\alpha_i, \beta_i \in \mathcal{O}_{\mathbb{F}}$ para todo i. Sea M la matriz cambio de base entre $\mathcal{A}$ y $\mathcal{B}$. Es conocido que $\Delta(\mathcal{A}) = (\det M)^2\Delta(\mathcal{B})$, sin embargo, $\det M$ nos da más información sobre la relación que hay entre $\mathcal{A}$ y $\mathcal{B}$.

Sea $\delta \in \mathcal{O}_{\mathbb{F}}$. Sabemos que $\delta = \dfrac{a_1}{b_1}\alpha_1 + \ldots + \dfrac{a_n}{b_n}\alpha_n$. Tomemos $m = \text{m.c.m.}\,(b_1, \ldots, b_n)$. Entonces $\delta = \dfrac{m\,\delta}{m}$, donde $m\,\delta \in \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$ y $m \in \mathbb{N}$. Supongamos que $\alpha_1 = \dfrac{\beta_1}{a}$ para algún $a \in \mathbb{Z}$ y $\alpha_i = \beta_i$ para $i > 1$. La matriz cambio de base entre $\mathcal{A}$ y $\mathcal{B}$ es la matriz diagonal:

$$M = \begin{pmatrix} a & 0 & 0 & & & & \\ 0 & 1 & 0 & \cdots & & 0 & \\ 0 & 0 & 1 & & & & \\ & \vdots & & \ddots & & \vdots & \\ & & & & 1 & 0 & 0 \\ & 0 & & \cdots & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{pmatrix}.$$

Puesto que $(\det M)^2 = a^2$, entonces $\Delta(\mathcal{A})$ y $\Delta(\mathcal{B})$ difieren por a^2.

Supongamos que $\det M = p$ un primo y $\mathbb{Z}[\mathcal{A}] \subseteq \mathbb{Z}[\mathcal{B}]$. Encontremos $\gamma_i \in \mathbb{Z}[\mathcal{A}]$ y $c_i \in \mathbb{Z}$ tales que $\beta_i = \dfrac{\gamma_i}{c_i}$.

Lema 3.16. *Sea $\mathbb{F}$ un campo de números, $\mathcal{O}_\mathbb{F}$ su anillo de enteros, $\mathcal{M} = \langle \beta_1, \beta_2 \rangle$ el $\mathbb{Z}$-módulo generado por $\beta_1, \beta_2 \in \mathcal{O}_\mathbb{F}$ y $\gamma_1 = b_1\,\beta_1 + b_2\,\beta_2 \in \mathcal{M}$ con $\mathrm{m.c.d.}\,(b_1, b_2) = 1$. Entonces, existe $\gamma_2 \in \mathcal{M}$ tal que $\mathcal{M} = \langle \gamma_1, \gamma_2 \rangle$.*

DEMOSTRACIÓN. Sean $c_1, c_2 \in \mathbb{Z}$ tales que $b_1\,c_1 + b_2\,c_2 = 1$, $\gamma_2 = c_2\,\beta_1 - c_1\,\beta_2$ y $\mathcal{N} = \langle \gamma_1, \gamma_2 \rangle$. Claramente $\mathcal{N} \subseteq \mathcal{M}$. Por otra parte,

$$\begin{aligned} c_1\,\gamma_1 + b_2\,\gamma_2 &= c_1(b_1\,\beta_1 + b_2\,\beta_2) + b_2(c_2\,\beta_1 - c_1\,\beta_2) \\ &= c_1\,b_1\,\beta_1 + c_1\,b_2\,\beta_2 + b_2\,c_2\,\beta_1 - b_2\,c_1\,\beta_2 \\ &= (b_1\,c_1 + b_2\,c_2)\beta_1 = \beta_1. \end{aligned}$$

$$\begin{aligned} c_2\,\gamma_1 - b_1\,\gamma_2 &= c_2(b_1\,\beta_1 + b_2\,\beta_2) - b_1(c_2\,\beta_1 - c_1\,\beta_2) \\ &= c_2\,b_1\,\beta_1 + c_2\,b_2\,\beta_2 - b_1\,c_2\,\beta_1 + b_1\,c_1\,\beta_2 \\ &= (b_1\,c_1 + b_2\,c_2)\beta_2 = \beta_2. \end{aligned}$$

Por lo tanto $\mathcal{M} = \mathcal{N}$. □

Proposición 3.17. *Sean $\mathbb{F}$ un campo de números, $\mathcal{O}_\mathbb{F}$ su anillo de enteros y una base $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ de $\mathbb{F}$ como $\mathbb{Q}$-espacio vectorial con $\mathcal{A} \subseteq \mathcal{O}_\mathbb{F}$ y $\alpha = a_1\,\alpha_1 + \cdots + a_n\,\alpha_n \in \mathcal{O}_\mathbb{F}$, con $a_1, \ldots, a_n \in \mathbb{Z}$. Si $\mathrm{m.c.d.}\,(a_1, \ldots, a_n) = 1$, entonces existe una base de $\mathbb{Z}[\mathcal{A}]$ como $\mathbb{Z}$-módulo en la que α es uno de los generadores.*

DEMOSTRACIÓN. Supongamos que $\mathcal{A}$ está ordenado de tal forma que para un entero $1 \leq t \leq n$, $a_i \neq 0$ cuando $i \leq t$ y $a_i = 0$ para $i > t$. Usaremos inducción sobre t.

Si $t = 1$, entonces $a_1 \neq 0$ y $a_2 = \cdots = a_n = 0$. En este caso tenemos que $\mathrm{m.c.d.}\,(a_1, \ldots, a_n) = a_1 = 1$. Por lo tanto, $\alpha = \alpha_1$ y $\mathcal{A}$ es la base que buscamos.

Supongamos que el resultado es cierto para $t = r$. Si $t = r + 1$, consideremos $b_1 = a_1$, $b_2 = \mathrm{m.c.d.}\,(a_2, \ldots, a_n)$, $\beta_1 = \alpha_1$, $\beta_2 = \dfrac{\alpha - a_1\,\alpha_1}{b_2}$ y

$$\gamma_1 = \alpha = b_1\,\beta_1 + b_2\,\beta_2 \in \langle \beta_1, \beta_2 \rangle\,.$$

El Lema 3.16 nos dice que existe γ_2 tal que $\langle \beta_1, \beta_2 \rangle = \langle \gamma_1, \gamma_2 \rangle$, donde β_2 tiene a lo más r coeficientes a_i's distintos de 0. Por lo anterior y la hipótesis de inducción, existe una base de $\langle \alpha_2, \ldots, \alpha_n \rangle$ en la que β_2 es un generador. Si ésta es $\{\beta_2, \beta_3, \ldots, \beta_n\}$, entonces $\langle \beta_1, \ldots, \beta_n \rangle = \langle \alpha_1, \ldots, \alpha_n \rangle$. Como $\langle \beta_1, \beta_2 \rangle = \langle \gamma_1, \gamma_2 \rangle$, entonces $\{\gamma_1, \gamma_2, \beta_3, \ldots, \beta_n\}$ es una base de $\mathbb{Z}[\mathcal{A}]$ que tiene a $\gamma_1 = \alpha$ en el conjunto de generadores. □

Proposición 3.18. *Sean $\mathbb{F}$ un campo de números, $\mathcal{O}_\mathbb{F}$ su anillo de enteros y $\mathcal{O}_1 \subsetneq \mathcal{O}_2$ dos órdenes de $\mathcal{O}_\mathbb{F}$, con $\mathcal{O}_1 = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$ y $\mathcal{O}_2 = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$. Si $p^2\,\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\beta_1, \ldots, \beta_n)$, entonces existe una base de $\mathcal{O}_1$, $\gamma_1, \ldots, \gamma_n$, tal que $\mathcal{O}_2 = \dfrac{\gamma_1}{p}\mathbb{Z} + \gamma_2\mathbb{Z} + \cdots + \gamma_n\mathbb{Z}$.*

DEMOSTRACIÓN. Como la contención de los órdenes es estricta, entonces existe un entero algebraico $\kappa \in \mathcal{O}_2 - \mathcal{O}_1$. Si $\kappa = \dfrac{k_1\,\kappa_1}{k_2}$ con $k_1, k_2 \in \mathbb{Z}$ primos relativos y $\kappa_1 \in \mathcal{O}_1$, entonces $k_1 \mid k_2\,\kappa$ y puesto que $\langle k_1\rangle, \langle k_2\rangle$ son ideales primos relativos, entonces $k_1 \mid \kappa$. Por lo anterior, podemos suponer que $\kappa = \dfrac{\kappa_1}{k}$ con $\kappa_1 \in \mathcal{O}_1$, $k \in \mathbb{Z}$ y no existe ningún entero racional que divida a κ. Esto implica que si $\kappa_1 = a_1\,\alpha_1 + \cdots + a_n\,\alpha_n$, entonces $\text{m.c.d.}\,(a_1, \ldots, a_n) = 1$. Por la Proposición 3.17, existe una base de $\mathcal{O}_1$ en la que κ_1 es uno de los generadores, digamos que $\mathcal{O}_1 = \kappa_1\mathbb{Z} + \gamma_2\mathbb{Z} + \cdots + \gamma_n\mathbb{Z}$. Así,

$$\mathcal{O}_1 \subseteq \frac{\kappa_1}{k}\mathbb{Z} + \gamma_2\mathbb{Z} + \cdots + \gamma_n\mathbb{Z} \subseteq \mathcal{O}_2.$$

El discriminante de la base $\dfrac{\kappa_1}{k}, \gamma_2, \ldots, \gamma_n$ satisface:

$$p^2\Delta(\mathcal{O}_2) \leq k^2\Delta(\frac{\kappa_1}{k}, \gamma_2, \ldots, \gamma_n) = \Delta(\kappa_1, \gamma_2, \ldots, \gamma_n) = \Delta(\mathcal{O}_1),$$

por lo que $k = p$ y $\dfrac{\gamma_1}{p} = \dfrac{\kappa_1}{p}$. □

3.3.2. Caso particular

Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ para algún $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ tal que $\sqrt{\alpha} \notin \mathbb{K}$. Una base de $\mathbb{L}$ como $\mathbb{Q}$-espacio vectorial es:

$$\mathcal{B} = \{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \sqrt{\alpha}, \sqrt[4]{p}\,\sqrt{\alpha}, \sqrt{p}\,\sqrt{\alpha}, \sqrt[4]{p^3}\,\sqrt{\alpha}\}. \tag{20}$$

A cada uno de estos elementos lo llamaremos $\beta_1, \ldots, \beta_8$ respectivamente. Vamos a calcular $\Delta(\mathcal{B})$, para lo cual, necesitamos encontrar las inmersiones de $\mathbb{L}$ en $\mathbb{C}$. Sabemos que deben existir ocho de éstas, y para describirlas, basta con decir a dónde manda cada inmersión a los elementos $\sqrt[4]{p}$ y $\sqrt{\alpha}$. En la siguiente tabla vemos la imagen de estos dos elementos y del resto de los generadores de $\mathbb{L}$ bajo cada una de las ocho inmersiones y en el último renglón obtenemos la suma de éstos, que es la traza de β_i:

	1	$\sqrt[4]{p}$	$\sqrt{p}$	$\sqrt[4]{p^3}$	$\sqrt{\alpha}$	$\sqrt[4]{p}\,\sqrt{\alpha}$	$\sqrt{p}\,\sqrt{\alpha}$	$\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_1	1	$\sqrt[4]{p}$	$\sqrt{p}$	$\sqrt[4]{p^3}$	$\sqrt{\alpha}$	$\sqrt[4]{p}\,\sqrt{\alpha}$	$\sqrt{p}\,\sqrt{\alpha}$	$\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_2	1	$i\sqrt[4]{p}$	$-\sqrt{p}$	$-i\sqrt[4]{p^3}$	$\sqrt{\alpha}$	$i\sqrt[4]{p}\,\sqrt{\alpha}$	$-\sqrt{p}\,\sqrt{\alpha}$	$-i\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_3	1	$-\sqrt[4]{p}$	$\sqrt{p}$	$-\sqrt[4]{p^3}$	$\sqrt{\alpha}$	$-\sqrt[4]{p}\,\sqrt{\alpha}$	$\sqrt{p}\,\sqrt{\alpha}$	$-\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_4	1	$-i\sqrt[4]{p}$	$-\sqrt{p}$	$i\sqrt[4]{p^3}$	$\sqrt{\alpha}$	$-i\sqrt[4]{p}\,\sqrt{\alpha}$	$-\sqrt{p}\,\sqrt{\alpha}$	$i\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_5	1	$\sqrt[4]{p}$	$\sqrt{p}$	$\sqrt[4]{p^3}$	$-\sqrt{\alpha}$	$-\sqrt[4]{p}\,\sqrt{\alpha}$	$-\sqrt{p}\,\sqrt{\alpha}$	$-\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_6	1	$i\sqrt[4]{p}$	$-\sqrt{p}$	$-i\sqrt[4]{p^3}$	$-\sqrt{\alpha}$	$-i\sqrt[4]{p}\,\sqrt{\alpha}$	$\sqrt{p}\,\sqrt{\alpha}$	$i\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_7	1	$-\sqrt[4]{p}$	$\sqrt{p}$	$-\sqrt[4]{p^3}$	$-\sqrt{\alpha}$	$\sqrt[4]{p}\,\sqrt{\alpha}$	$-\sqrt{p}\,\sqrt{\alpha}$	$\sqrt[4]{p^3}\,\sqrt{\alpha}$
σ_8	1	$-i\sqrt[4]{p}$	$-\sqrt{p}$	$i\sqrt[4]{p^3}$	$-\sqrt{\alpha}$	$i\sqrt[4]{p}\,\sqrt{\alpha}$	$\sqrt{p}\,\sqrt{\alpha}$	$-i\sqrt[4]{p^3}\,\sqrt{\alpha}$
t	8	0	0	0	0	0	0	0

En esta tabla observamos que el único sumando importante para calcular la traza de un elemento de $\mathbb{L}$ es el que está en $\mathbb{Q}$. Para calcular el discriminante tenemos que encontrar el

determinante de la matriz $M = (t(\beta_i\beta_j))$, donde t es la traza en la extensión $\mathbb{L}/\mathbb{Q}$:

$$M = \left(\begin{array}{cccc|cccc} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 8p & 0 & 0 & 0 & 0 \\ 0 & 0 & 8p & 0 & 0 & 0 & 0 & 0 \\ 0 & 8p & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 0 & & M_1 & & \\ 0 & 0 & 0 & 0 & & & & \end{array}\right)$$

donde M_1 es la matriz:

$$\begin{aligned} M_1 &= \begin{pmatrix} t(\alpha) & t(\alpha\sqrt[4]{p}) & t(\alpha\sqrt{p}) & t(\alpha\sqrt[4]{p^3}) \\ t(\alpha\sqrt[4]{p}) & t(\alpha\sqrt{p}) & t(\alpha\sqrt[4]{p^3}) & t(\alpha\, p) \\ t(\alpha\sqrt{p}) & t(\alpha\sqrt[4]{p^3}) & t(\alpha\, p) & t(\alpha\, p\sqrt[4]{p}) \\ t(\alpha\sqrt[4]{p^3}) & t(\alpha\, p) & t(\alpha\, p\sqrt[4]{p}) & t(\alpha\, p\sqrt{p}) \end{pmatrix} \\ &= \begin{pmatrix} 8\,a_1 & 8\,a_4\,p & 8\,a_3\,p & 8\,a_2\,p \\ 8\,a_4\,p & 8\,a_3\,p & 8\,a_2\,p & 8\,a_1\,p \\ 8\,a_3\,p & 8\,a_2\,p & 8\,a_1\,p & 8\,a_4\,p^2 \\ 8\,a_2\,p & 8\,a_1\,p & 8\,a_4\,p^2 & 8\,a_3\,p^2 \end{pmatrix}. \end{aligned}$$

Por tanto $\Delta(\mathcal{B}) = 2^{12}\,p^3\ \det(M_1)$, donde:

$$\begin{aligned} \det(M_1) &= 2^{12}\,p^3 \det\begin{pmatrix} a_1 & a_4\,p & a_3\,p & a_2\,p \\ a_4 & a_3 & a_2 & a_1 \\ a_3 & a_2 & a_1 & a_4\,p \\ a_2 & a_1 & a_4\,p & a_3\,p \end{pmatrix} \\ &= -2^{12}\,p^3\,N_{\mathbb{K}/\mathbb{Q}}\,(\alpha). \end{aligned}$$

De esta forma

$$\Delta(\mathcal{B}) = \det M = -2^{24}\,p^6\,N_{\mathbb{K}/\mathbb{Q}}\,(\alpha). \tag{21}$$

Por lo anterior $-2^{24}\,p^6\,N_{\mathbb{K}/\mathbb{Q}}\,(\alpha) \in \delta_{\mathbb{L}/\mathbb{Q}}$, y así $\langle 2^{24}\,p^6\,N_{\mathbb{K}/\mathbb{Q}}\,(\alpha)\rangle \subseteq \delta_{\mathbb{L}/\mathbb{Q}}$.

Por otra parte, $\delta_{\mathbb{K}/\mathbb{Q}} = 2^8\,p^3$ y por la Proposición 1.26 tenemos

$$\langle 2^{24}\,p^6\,N_{\mathbb{K}/\mathbb{Q}}\,(\alpha)\rangle \subseteq \delta_{\mathbb{L}/\mathbb{Q}} = \delta^2_{\mathbb{K}/\mathbb{Q}}\,N_{\mathbb{K}/\mathbb{Q}}\left(\delta_{\mathbb{L}/\mathbb{K}}\right) = \langle 2^{16}\,p^6\,N_{\mathbb{K}/\mathbb{Q}}\left(\delta_{\mathbb{L}/\mathbb{K}}\right)\rangle.$$

Usando la factorización única en ideales tenemos

$$\langle 2^8\,N_{\mathbb{K}/\mathbb{Q}}\,(\alpha)\rangle \subseteq \langle N_{\mathbb{K}/\mathbb{Q}}\left(\delta_{\mathbb{L}/\mathbb{K}}\right)\rangle. \tag{22}$$

3.3.3. El caso α unidad y el campo de clases de Hilbert de $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $h_{\mathbb{K}} = 2$

El objetivo de esta sección es encontrar el campo de clases de Hilbert de $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ y $h_{\mathbb{K}} = 2$. Para esto, primero será necesario encontrar una base entera de $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ en el caso en que α es unidad. Como

$$\langle 2^8\rangle \subseteq \langle N_{\mathbb{K}/\mathbb{Q}}\left(\delta_{\mathbb{L}/\mathbb{K}}\right)\rangle, \tag{23}$$

entonces es posible que existan unidades α para las cuales $\mathcal{B}$ no es base entera de $\mathbb{L}$. En caso de que la base entera no sea de esta forma, la Proposición 3.18 nos indica que debe existir un elemento de la forma

$$\alpha = \frac{a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} + \sqrt{\alpha}(a_5 + a_6\sqrt[4]{p} + a_7\sqrt{p} + a_8\sqrt[4]{p^3})}{2}, \tag{24}$$

donde $a_i \in \mathbb{Z}$. Si a_1 es par, digamos $a_1 = 2\,b_1$, entonces $\alpha - b_1$ también es un entero algebraico. Este es el mismo elemento pero intercambiando a_1 por 0. Si $a_1 = 2\,b_1 + 1$, volvemos a tomar $\alpha - b_1$ y en este caso tendremos el mismo elemento pero con 1 en lugar de a_1. Este procedimiento se puede volver a aplicar para cada uno de los a_i's, así que podemos suponer que $a_i \in \{0, 1\}$ para $1 \leq i \leq 8$.

Proposición 3.19. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 3 \pmod 4$ un primo racional, $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ con $\alpha \in \mathcal{U}_{\mathbb{K}}$ tal que $\mathbb{L} \neq \mathbb{K}$ y $\mathcal{B}$ como en* (20)*. Si $\mathcal{B}$ no es una base entera de $\mathbb{L}$ entonces*

$$\frac{1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3}}{2}(1 + \sqrt{\alpha})$$

es un entero algebraico.

DEMOSTRACIÓN. Primero nos concentraremos en los valores de a_1, a_2, a_3, a_4 en (24). Vamos a representar estos valores con el vector (a_1, a_2, a_3, a_4) y diremos que un elemento es de la forma (b_1, b_2, b_3, b_4) si $a_i = b_i$ para $i = 1, 2, 3, 4$, sin importar los valores de a_5, a_6, a_7, a_8. Si existe un entero algebraico de la forma $(1, 0, 0, 0)$ y lo multiplicamos por $\sqrt[4]{p}$ obtenemos un entero algebraico de la forma $(0, 1, 0, 0)$. Si multiplicamos este entero por $\sqrt[4]{p}$ obtenemos uno de la forma $(0, 0, 1, 0)$ y multiplicando de nuevo por $\sqrt[4]{p}$ obtenemos un elemento de la forma $(0, 0, 0, 1)$. Finalmente, si multiplicamos un elemento de la forma $(0, 0, 0, 1)$ por $\sqrt[4]{p}$ obtenemos $(p, 0, 0, 0)$ y como p es impar, entonces tenemos un elemento de la forma $(1, 0, 0, 0)$. Si en lugar de tener un 1 en el vector tenemos dos o tres 1's, se presenta un comportamiento similar.

Supongamos que tenemos un entero algebraico de la forma $(1, 0, 0, 0)$. Como ya vimos, también existen enteros algebraicos de las formas $(0, 1, 0, 0)$, $(0, 0, 1, 0)$ y $(0, 0, 0, 1)$. Sumando estos cuatro elementos queda uno de la forma $(1, 1, 1, 1)$. Si hay un elemento de la forma $(1, 1, 0, 0)$, $(0, 1, 1, 0)$, $(0, 0, 1, 1)$ ó $(1, 0, 0, 1)$, entonces los tenemos todos. Sumando el primero más el tercero obtenemos un entero de la forma $(1, 1, 1, 1)$. Ahora, si existe un entero algebraico de una de las siguientes formas: $(1, 1, 1, 0)$, $(1, 1, 0, 1)$, $(1, 0, 1, 1)$, $(0, 1, 1, 1)$, entonces hay elementos de las cuatro formas. Este caso se reduce al anterior pues $(1, 1, 1, 0) + (1, 1, 0, 1) = (0, 0, 1, 1)$. Finalmente, supongamos que se tiene un entero algebraico de la forma $(1, 0, 1, 0)$ ó $(0, 1, 0, 1)$. Notemos que la existencia de uno garantiza la existencia del otro y la suma de ellos es de la forma $(1, 1, 1, 1)$. Por todo lo anterior, si $\mathcal{B}$ no es base entera de $\mathbb{L}$, entonces existe un elemento como en (24) donde $a_1 = a_2 = a_3 = a_4 = 0$ ó un elemento con $a_1 = a_2 = a_3 = a_4 = 1$.

Usando las mismas ideas, vamos a estudiar el comportamiento de a_5, a_6, a_7, a_8. Escribiremos $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ para representar a los elementos de la forma (24).

Si $(1, 1, 1, 1, 1, 0, 0, 0) \in \mathcal{O}_{\mathbb{L}}$, multiplicamos por $\sqrt[4]{p}$ varias veces para obtener los elementos

$$(1, 1, 1, 1, 0, 1, 0, 0), \quad (1, 1, 1, 1, 0, 0, 1, 0) \quad \text{y} \quad (1, 1, 1, 1, 0, 0, 0, 1).$$

Sumando estos cuatro, tenemos que $(0,0,0,0,1,1,1,1)$ es un entero algebraico. Si tenemos los elementos

$$(1,1,1,1,1,1,0,0), \quad (1,1,1,1,0,1,1,0),$$
$$(1,1,1,1,0,0,1,1), \quad (1,1,1,1,1,0,0,1),$$

entonces sumando los de la izquierda o los de la derecha tenemos que $(0,0,0,0,1,1,1,1)$ es entero algebraico. Si los elementos $(1,1,1,1,1,0,1,0)$ y $(1,1,1,1,1,0,1,0)$ son enteros algebraicos, entonces $(0,0,0,0,1,1,1,1)$ también lo es.

Si $(1,1,1,1,1,1,1,0) \in \mathcal{O}_{\mathbb{L}}$, entonces $(1,1,1,1,0,1,1,1)$ es entero algebraico y $(0,0,0,0,1,0,0,1) \in \mathcal{O}_{\mathbb{L}}$, así que este caso implica que hay un elemento de la forma $(0,0,0,0)$ que vamos a comentar ahora. Cuando estudiamos el comportamiento de a_1, a_2, a_3, a_4 observamos que siempre existe un elemento de la forma $(0,0,0,0)$ o de la forma $(1,1,1,1)$. Usando un análisis similar al anterior, si $a_1 = a_2 = a_3 = a_4 = 0$, entonces $(0,0,0,0,0,0,0,0) \in \mathcal{O}_{\mathbb{L}}$, y por tanto $\alpha = 0$, o bien, $(0,0,0,0,1,1,1,1) \in \mathcal{O}_{\mathbb{L}}$.

En todos los casos anteriores, el elemento $(0,0,0,0,1,1,1,1)$ es entero algebraico. El elemento $(1,1,1,1,1,1,1,1)$ es el único que no cae en los casos anteriores. Resumiendo, si $\mathcal{B}$ no es base entera de $\mathbb{L}$, entonces

$$\frac{1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}}{2}\sqrt{\alpha} \quad \text{ó} \quad \frac{1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}}{2}(1+\sqrt{\alpha})$$

es elemento de $\mathcal{O}_{\mathbb{L}}$. Mostraremos que $\dfrac{1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}}{2}\sqrt{\alpha} \notin \mathcal{O}_{\mathbb{L}}$. Puesto que $1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3} = (1+\sqrt{p})(1+\sqrt[4]{p})$, tenemos:

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}\left((1+\sqrt{p})(1+\sqrt[4]{p})\right) &= N_{\mathbb{K}/\mathbb{Q}}\left(1+\sqrt{p}\right) N_{\mathbb{K}/\mathbb{Q}}\left(1+\sqrt[4]{p}\right) \\ &= (1-p)^2(1-p) = (1-p)^3 \end{aligned}$$

y como $p \equiv 7 \pmod{16}$, entonces $1-p \equiv 2 \pmod 4$, con lo cual obtenemos $\operatorname{ord}_2\left((1-p)^3\right) = 3$. Como consecuencia de esto,

$$\operatorname{ord}_2\left(N_{\mathbb{L}/\mathbb{Q}}\left(1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}\right)\right) = 6, \quad N_{\mathbb{L}/\mathbb{Q}}\left(\sqrt{\alpha}\right) = 1, \quad N_{\mathbb{L}/\mathbb{Q}}\left(2\right) = 2^8,$$

por lo que si α es unidad, $\dfrac{1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}}{2}\sqrt{\alpha}$ no es un entero algebraico. Por lo tanto

$$\frac{1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}}{2}(1+\sqrt{\alpha}) \in \mathcal{O}_{\mathbb{L}}.$$

□

Proposición 3.20. *Sean* $\mathbb{F} = \mathbb{Q}(\sqrt{p})$, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo,* $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ *con* $\alpha \in \mathcal{O}_{\mathbb{K}}$ *libre de cuadrados en todas sus factorizaciones,* $N_{\mathbb{K}/\mathbb{F}}(\alpha) = \pm U_{\mathbb{F}}$ *y* $\mathcal{B}$ *como en* (20)*. Entonces,* $\mathcal{B}$ *es base entera de* $\mathbb{L}$*.*

DEMOSTRACIÓN. De acuerdo a la Proposición 3.19, basta con demostrar que el elemento $\dfrac{1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}}{2}(1+\sqrt{\alpha})$ no es un entero algebraico. Primero observemos que $N_{\mathbb{L}/\mathbb{Q}}(1+\sqrt{\alpha}) = N_{\mathbb{K}/\mathbb{Q}}(1-\alpha)$, y como $N_{\mathbb{K}/\mathbb{F}}(\alpha) = \pm U_{\mathbb{F}}$, el polinomio irreducible de α con coeficientes en $\mathcal{O}_{\mathbb{F}}$ es

$$f(x) = x^2 - 2(a_1 + a_3\sqrt{p})\,x \pm U_{\mathbb{F}},$$

donde $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3}$. El polinomio irreducible de $1-\alpha$ con coeficientes en $\mathcal{O}_{\mathbb{F}}$ es

$$\begin{aligned} g(x) &= f(-x+1) = (-x+1)^2 - 2(a_1 + a_3\sqrt{p})(-x+1) \pm U_{\mathbb{F}} \\ &= x^2 - 2x + 2(a_1 + a_3\sqrt{p})\, x + 1 - 2(a_1 + a_3\sqrt{p}) \pm U_{\mathbb{F}}, \end{aligned}$$

de donde $N_{\mathbb{K}/\mathbb{F}}\,(1-\alpha) = 1 - 2(a_1 + a_3\sqrt{p}) \pm U_{\mathbb{F}}$. Si $U_{\mathbb{F}} = u_1 + u_2\sqrt{p}$, entonces $1 \pm U_{\mathbb{F}} = 1 \pm u_1 \pm u_2\sqrt{p}$ y, por la Proposición 3.5, $1 \pm u_1$ y u_2 son impares. Por lo anterior, $(1 \pm u_1)^2 - p\,u_2^2 \equiv 1 - 3(1) \equiv 2 \pmod 4$, así que $L_2 \mid 1 \pm U_{\mathbb{F}}$ y $2 \nmid 1 \pm U_{\mathbb{F}}$. Por lo anterior, $L_2 \mid N_{\mathbb{K}/\mathbb{F}}\,(1-\alpha)$ y $2 \nmid N_{\mathbb{K}/\mathbb{F}}\,(1-\alpha)$, de donde

$$N_{\mathbb{L}/\mathbb{Q}}\left(1 + \sqrt{\alpha}\right) = N_{\mathbb{K}/\mathbb{Q}}\,(1-\alpha) \equiv 2 \pmod 4.$$

Como $N_{\mathbb{K}/\mathbb{Q}}\left(1 - \sqrt[4]{p}\right) = N_{\mathbb{F}/\mathbb{Q}}\left(1 - \sqrt{p}\right) = 1 - p \equiv 2 \pmod 4$ y $p \equiv 7 \pmod{16}$, entonces $2^2 || N_{\mathbb{L}/\mathbb{Q}}\left(1 - \sqrt[4]{p}\right)$ y $2^4 || N_{\mathbb{L}/\mathbb{Q}}\left(1 - \sqrt{p}\right)$. Ahora es fácil observar que el número $\dfrac{1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3}}{2}(1 + \sqrt{\alpha})$ no es entero algebraico pues

$$N_{\mathbb{L}/\mathbb{Q}}\left((1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3})(1 + \sqrt{\alpha})\right) \equiv 2^7 \pmod{2^8} \quad \text{y} \quad N_{\mathbb{L}/\mathbb{Q}}\,(2) = 2^8.$$

□

Proposición 3.21. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{p})$, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod 8$ un primo racional positivo, $U_{\mathbb{F}} = u_1 + u_2\sqrt{p}$ la unidad fundamental de $\mathcal{O}_{\mathbb{F}}$ y $\mathbb{L} = \mathbb{K}(\sqrt{U_{\mathbb{F}}})$.*

1. *Si $u_2 \equiv 1 \pmod 4$, definimos $\beta = \dfrac{1 + \sqrt{U_{\mathbb{F}}}\,\sqrt[4]{p^3}}{2}$.*
2. *Si $u_2 \equiv 3 \pmod 4$, definimos $\beta = \dfrac{1 + \sqrt{U_{\mathbb{F}}}\,\sqrt[4]{p}}{2}$.*

Entonces, una base entera de $\mathbb{L}$ es:

$$\mathcal{B}_1 = \{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \beta, \beta\sqrt[4]{p}, \beta\sqrt{p}, \beta\sqrt[4]{p^3}\}.$$

DEMOSTRACIÓN. Primero vamos a demostrar que β es un entero algebraico y con esto podemos concluir que todos los elementos de $\mathcal{B}_1$ lo son.

El polinomio irreducible de $\sqrt{U_{\mathbb{F}}}\,\sqrt[4]{p^k}$ en $\mathcal{O}_{\mathbb{F}}[x]$ es $f(x) = x^2 - U_{\mathbb{F}}\sqrt{p^k}$, donde $k = 1, 3$ dependiendo del caso. Sea

$$g(x) = \frac{f(2x-1)}{4} = \frac{(2x-1)^2 - U_{\mathbb{F}}\,\sqrt{p^k}}{4} = x^2 - x + \frac{1 - U_{\mathbb{F}}\sqrt{p^k}}{4}.$$

Entonces $g(x)$ es irreducible en $\mathcal{O}_{\mathbb{F}}[x]$ y $g(\beta) = 0$. Para que β sea un entero algebraico, basta con que $4 \mid 1 - U_{\mathbb{F}}\,\sqrt{p^k}$ en $\mathcal{O}_{\mathbb{F}}$. Notemos que

$$1 - U_{\mathbb{F}}\,\sqrt{p^k} = 1 - u_1\,\sqrt{p^k} - u_2\,p^{(k+1)/2}.$$

Por la Proposición 3.5, $4 \mid u_1$. Por otra parte, si $u_2 \equiv 1 \pmod 4$ y $k = 3$, entonces $1 - u_2p^2 \equiv 1 - 1(3^2) \equiv 0 \pmod 4$. Si $u_2 \equiv 3 \pmod 4$ y $k = 1$, tenemos que $1 - u_2p \equiv 1 - 3(3) \equiv 0 \pmod 4$. Cualquiera que sea el caso, $4 \mid 1 - u_2\,p^{(k+1)/2}$. Por lo tanto, $4 \mid 1 - U_{\mathbb{F}}\,\sqrt{p^k}$ y β es un entero algebraico.

Si $\mathcal{B}$ es como en (20), entonces $\Delta(\mathcal{B}) = -2^{24}\,p^6 N_{\mathbb{K}/\mathbb{Q}}\,(U_{\mathbb{F}}) = -2^{24}\,p^6$. Claramente, $\mathcal{B}_1$ lo obtuvimos sustituyendo cuatro elementos de $\mathcal{B}$ por elementos con denominador 2.

Entonces $\Delta(\mathcal{B}_1) = \dfrac{2^{24}\,p^6}{(2^2)^4} = 2^{16}\,p^6$. Como $\delta_{\mathbb{K}} = 2^8\,p^3$, por la fórmula de la Proposición 1.26 el discriminante de $\mathbb{L}$ no puede ser menor. Por lo tanto, $\mathcal{B}_1$ es una base entera de $\mathbb{L}$. □

Usando los resultados anteriores podemos calcular discriminantes de extensiones $\mathbb{L}/\mathbb{K}$, donde $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ con $\alpha \in \mathcal{U}_{\mathbb{K}}$. Con esto y la Proposición 1.26 tenemos:

Teorema 3.22. *Sean $\mathbb{F} = \mathbb{Q}(\sqrt{p})$, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$, con $\alpha \in \mathbb{K}$. Si $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = U_{\mathbb{F}}$, entonces $\mathbb{K}/\mathbb{F}$ es una extensión ramificada. Si $\alpha = U_{\mathbb{F}}$, entonces $\mathbb{L}/\mathbb{K}$ no se ramifica en ningún primo.* □

Corolario 3.23. *Sea $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo. Entonces $h_{\mathbb{K}}$ es par. En particular, si $h_{\mathbb{K}} = 2$, el campo de clases de Hilbert de $\mathbb{K}$ es $\mathbb{H}_{\mathbb{K}} = \mathbb{K}(\sqrt{U_{\mathbb{F}}})$.* □

3.4. Ramificación de 2 en extensiones cuadráticas sobre $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$

La Proposición 1.17 describe con detalle la ramificación de 2 en campos cuadráticos. La ramificación de 2 en extensiones cuárticas ha sido estudiada por S. Roberson Ashford [**27**] en extensiones cuárticas en términos de los coeficientes de un polinomio de la forma $d + b\,x^2 + x^4$. En esta sección vamos a estudiar la ramificación de 2 en extensiones cuadráticas sobre $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$.

Sea q un primo racional y $\mathbb{F}$ un campo de números con una base entera de potencias. La factorización como producto de ideales primos de $\langle q\rangle_{\mathbb{F}}$ está dada por el célebre Teorema de Dedekind:

Teorema 3.24. *Sean $\mathbb{K} = \mathbb{Q}(\theta)$ un campo de números de grado n con $\theta \in \mathcal{O}_{\mathbb{K}}$, $f(x) = \mathrm{Irr}(\theta, \mathbb{Z})$ y q un primo racional y $ind(\theta)$ el número natural tal que*

$$ind(\theta)^2 \delta_{\mathbb{K}} = \Delta(1, \theta, \ldots, \theta^{n-1}).$$

Si $f(x) \in \mathbb{Z}[x]$, entonces $\overline{f}(x)$ es la proyección natural de $f(x)$ en $\mathbb{Z}/q\mathbb{Z}[x]$. Si

$$\overline{f}(x) = g_1(x)^{e_1} \cdots g_r(x)^{e_r},$$

con $g_i(x) \in \mathbb{Z}/q\mathbb{Z}[x]$ irreducibles y $e_i \in \mathbb{Z}$ para todo i, definamos f_i como cualquier polinomio en $\mathbb{Z}[x]$ tal que $\overline{f_i}(x) = g_i(x)$ y $\mathfrak{q}_i = \langle q, f_i(\theta)\rangle$ para todo i. Si $ind(\theta) \not\equiv 0 \pmod{q}$, entonces

$$\langle q\rangle = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r},$$

donde $\mathfrak{q}_i$ es un ideal primo para todo i.

DEMOSTRACIÓN. Ver [**4**], pp. 257, Theorem 10.5.1. □

Los casos interesantes o difíciles se dan para primos q que dividen a $\Delta(1, \ldots, \theta)$. En particular, si el grado de la extensión es par, es común que el discriminante sea par, por esta razón, la ramificación del primo 2 suele complicarse.

Lema 3.25. *Sean $p \equiv 7 \pmod{16}$ un primo racional positivo, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ para algún $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{L} \neq \mathbb{K}$ y $\mathfrak{I}_{\mathbb{L}} = \langle 2, \beta \rangle_{\mathbb{L}}$ con $\beta \in \mathcal{O}_{\mathbb{L}}$, $N_{\mathbb{L}/\mathbb{Q}}(\beta) \equiv 2 \pmod{4}$.*

1. $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) = 2$.
2. *Si $\beta = \gamma_1 + \gamma_2\sqrt{\alpha}$ con $\gamma_1, \gamma_2 \in \mathbb{K}$, tomemos $\beta' = \gamma_1 - \gamma_2\sqrt{\alpha}$. Si $\langle 2, \beta \rangle_{\mathbb{L}} = \langle 2, \beta' \rangle_{\mathbb{L}}$ entonces 2 se ramifica totalmente en $\mathbb{L}$.*

DEMOSTRACIÓN. Como $N_{\mathbb{L}/\mathbb{Q}}(\beta) \equiv 2 \pmod{4}$, entonces existe un ideal primo $\mathfrak{q}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}$ con $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{q}_{\mathbb{L}}) = 2$. Puesto que $\mathfrak{q}_{\mathbb{L}} \mid 2$, entonces $\mathfrak{q}_{\mathbb{L}} \supseteq \langle 2, \beta \rangle_{\mathbb{L}} = \mathfrak{I}_{\mathbb{L}}$. Por otra parte, $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) \mid N_{\mathbb{L}/\mathbb{Q}}(2)$ y $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) \mid N_{\mathbb{L}/\mathbb{Q}}(\beta)$, así que

$$N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) \mid \text{m.c.d.}\left(N_{\mathbb{L}/\mathbb{Q}}(2), N_{\mathbb{L}/\mathbb{Q}}(\beta)\right) = 2.$$

Por lo anterior,

$$2 = N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{q}_{\mathbb{L}}) \mid N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) \mid 2,$$

y $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) = 2$.

De acuerdo a la Proposición 3.8, el primo 2 se ramifica totalmente en $\mathbb{K}$. Considerando que $\mathfrak{I}_{\mathbb{L}} = \langle 2, \beta \rangle_{\mathbb{L}} = \langle 2, \beta' \rangle_{\mathbb{L}}$, entonces ${\mathfrak{I}_{\mathbb{L}}}^2 = \langle 4, 2\beta, 2\beta', \beta\beta' \rangle_{\mathbb{L}} \supseteq \langle 4, \beta\beta' \rangle_{\mathbb{L}}$. Como $N_{\mathbb{L}/\mathbb{K}}(\beta) = \beta\beta'$, entonces $N_{\mathbb{K}/\mathbb{Q}}(\beta\beta') \equiv 2 \pmod{4}$. De forma análoga a la demostración de la afirmación 1, se tiene que $N_{\mathbb{K}/\mathbb{Q}}(\langle 4, \beta\beta' \rangle_{\mathbb{K}}) = 2$ y $N_{\mathbb{L}/\mathbb{Q}}(\langle 4, \beta\beta' \rangle_{\mathbb{L}}) = 2^2 = 4$. Por lo anterior y $N_{\mathbb{L}/\mathbb{Q}}\left({\mathfrak{I}_{\mathbb{L}}}^2\right) = 4$, obtenemos ${\mathfrak{I}_{\mathbb{L}}}^2 = \langle 4, \beta\beta' \rangle_{\mathbb{L}}$. Además, $\langle 4, \beta\beta' \rangle_{\mathbb{K}}$ es el único ideal de $\mathcal{O}_{\mathbb{K}}$ con norma 2 y $\langle 4, \beta\beta' \rangle_{\mathbb{K}}^4 = \langle 2 \rangle_{\mathbb{K}}$, con lo que concluimos ${\mathfrak{I}_{\mathbb{L}}}^8 = \langle 2 \rangle_{\mathbb{L}}$. □

3.4.1. $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 2 \pmod{4}$ y $8 \mid N_{\mathbb{K}/\mathbb{Q}}(\alpha)$.

Como consecuencia del Lema 3.25 obtenemos de forma inmediata:

Proposición 3.26. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $0 < p \equiv 7 \pmod{16}$ un primo racional, $\alpha \in \mathbb{K}$ libre de cuadrados en todas sus factorizaciones tal que $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 2 \pmod{4}$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. Entonces 2 se ramifica totalmente en $\mathbb{L}$.*

DEMOSTRACIÓN. Sean $\beta = \sqrt{\alpha}$ y $\mathfrak{I}_{\mathbb{L}} = \langle 2, \beta \rangle_{\mathbb{L}}$. Puesto que

$$N_{\mathbb{L}/\mathbb{Q}}(\beta) = N_{\mathbb{K}/\mathbb{Q}}\left(N_{\mathbb{L}/\mathbb{K}}(\beta)\right) = N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 2 \pmod{4},$$

entonces, por el Lema 3.25, $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) = 2$ y como $\beta' = -\beta$, tenemos $\langle 2, \beta \rangle_{\mathbb{L}} = \langle 2, \beta' \rangle_{\mathbb{L}}$, lo que implica que 2 se ramifica totalmente. □

Para el caso en el que $8 \mid N_{\mathbb{K}/\mathbb{Q}}(\alpha)$, podemos suponer que de hecho $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 8 \pmod{16}$ ya que si $16 \mid N_{\mathbb{K}/\mathbb{Q}}(\alpha)$, entonces $2 = U_{\mathbb{F}} L_2^2 \mid \alpha$ y $\mathbb{K}(\sqrt{\alpha}) = \mathbb{K}\left(\dfrac{\sqrt{\alpha}}{L_2}\right) = \mathbb{K}\left(\sqrt{\dfrac{\alpha}{L_2^2}}\right)$, donde $N_{\mathbb{K}/\mathbb{Q}}\left(\dfrac{\alpha}{L_2^2}\right) = \dfrac{N_{\mathbb{K}/\mathbb{Q}}(\alpha)}{16}$. Sea $\mathfrak{p}_{\mathbb{K}} = \left\langle 2, 1 + \sqrt[4]{p} \right\rangle_{\mathbb{K}}$ el único ideal de $\mathcal{O}_{\mathbb{K}}$ con norma 2 tal como lo construimos en la Proposición 3.8. Veamos cómo es la ramificación de $\mathfrak{p}_{\mathbb{K}}$ en $\mathbb{L}$.

Proposición 3.27. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, donde $0 < p \equiv 7 \pmod{16}$ es un primo racional, $\alpha \in \mathbb{K}$ libre de cuadrados en todas sus factorizaciones tal que $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 8 \pmod{16}$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. Si $\langle 2 \rangle_{\mathbb{K}} = \mathfrak{p}_{\mathbb{K}}^4$, entonces $\mathfrak{p}_{\mathbb{K}}$ se ramifica en $\mathbb{L}$.*

DEMOSTRACIÓN. Supongamos que $\mathfrak{p}_{\mathbb{K}}$ es inerte. Como $\mathfrak{p}_{\mathbb{K}}^3 \mid\mid \langle\alpha\rangle_{\mathbb{K}}$, entonces $\langle\mathfrak{p}_{\mathbb{K}}\rangle_{\mathbb{L}}^3 \mid\mid \langle\alpha\rangle_{\mathbb{L}}$. Lo anterior implica que $\langle\alpha\rangle_{\mathbb{L}}$ no puede ser un cuadrado, pues de ser así cada ideal primo que divide a $\langle\alpha\rangle_{\mathbb{L}}$ debería dividir a $\langle\alpha\rangle_{\mathbb{L}}$ un número par de veces. Esto es una contradicción pues $\langle\sqrt{\alpha}\rangle_{\mathbb{L}}^2 = \langle\alpha\rangle_{\mathbb{L}}$.

Si $\mathfrak{p}_{\mathbb{K}}$ se descompone, entonces $\langle\mathfrak{p}_{\mathbb{K}}\rangle_{\mathbb{L}} = \mathfrak{q}_{\mathbb{L}}\,\mathfrak{q}'_{\mathbb{L}}$, donde $\mathfrak{q}_{\mathbb{L}}^3 \mid\mid \langle\alpha\rangle_{\mathbb{L}}$. De la misma forma que en el caso anterior, $\langle\alpha\rangle_{\mathbb{L}}$ no es un cuadrado lo cual es absurdo y $\mathfrak{p}_{\mathbb{K}}$ se ramifica en $\mathbb{L}$. □

Corolario 3.28. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, donde $p \equiv 7 \pmod{16}$ es un primo racional positivo, $\alpha \in \mathbb{K}$ libre de cuadrados en todas sus factorizaciones, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 8 \pmod{16}$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. Entonces 2 se ramifica totalmente en $\mathbb{L}$.* □

3.4.2. $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$

Ahora supongamos que $\alpha = L_2\,\varphi = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3}$ con L_2 el único elemento de $\mathcal{O}_{\mathbb{F}}$ con $N_{\mathbb{F}/\mathbb{Q}}(L_2) = 2$ y algún $\varphi = f_1 + f_2\sqrt[4]{p} + f_3\sqrt{p} + f_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ con $N_{\mathbb{K}/\mathbb{Q}}(\varphi)$ impar. Un cálculo elemental nos muestra

$$\begin{array}{rcl} N_{\mathbb{K}/\mathbb{Q}}(\alpha) & \equiv & a_1^4 + a_2^4 + a_3^4 + a_4^4 + 2\,a_1^2\,a_3^2 + 2\,a_2^2\,a_4^2 \\ & & +4\,a_1\,a_2^2\,a_3 + 4\,a_1^2\,a_2\,a_4 + 4\,a_2\,a_3^2\,a_4 + 4\,a_1\,a_3\,a_4^2 \\ & \equiv & (a_1^2 + a_3^2)^2 + (a_2^2 + a_4^2)^2 \\ & & +4\,a_1\,a_3(a_2^2 + a_4^2) + 4\,a_2\,a_4(a_1^2 + a_3^2) \pmod 8. \end{array} \tag{25}$$

Puesto que $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = N_{\mathbb{F}/\mathbb{Q}}(L_2)^2\,N_{\mathbb{K}/\mathbb{Q}}(\varphi) = 4\,N_{\mathbb{K}/\mathbb{Q}}(\varphi)$, debe existir un número par de a_i's pares y un número par de a_i's impares. Si todos son pares, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 0 \pmod 8$ y si todos los a_i's son impares tendremos

$$N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv (1+1)^2 + (1+1)^2 + 4\,(1+1) + 4\,(1+1) \equiv 0 \pmod 8.$$

Esto nos muestra que debe haber dos a_i's pares y dos impares. Puesto que los coeficientes de $L_2 \in \mathcal{O}_{\mathbb{F}}$ son enteros impares, podemos escribir $L_2 = (2\,l_1 + 1) + (2\,l_2 + 1)\sqrt{p}$. Así

$$\alpha = L_2\,\varphi = ((2\,l_1 + 1) + (2\,l_2 + 1)\sqrt{p})(f_1 + f_2\sqrt[4]{p} + f_3\sqrt{p} + f_4\sqrt[4]{p^3}),$$

donde:

$$\begin{array}{rcl} a_1 & = & f_1 + 2\,f_1\,l_1 + f_3\,p + 2\,f_3\,l_2\,p \equiv f_1 + f_3 \pmod 2 \\ a_2 & = & f_2 + 2\,f_2\,l_1 + f_4\,p + 2\,f_4\,l_2\,p \equiv f_2 + f_4 \pmod 2 \\ a_3 & = & f_1 + f_3 + 2\,f_3\,l_1 + 2\,f_1\,l_2 \equiv f_1 + f_3 \pmod 2 \\ a_4 & = & f_2 + f_4 + 2\,f_4\,l_1 + 2\,f_2\,l_2. \equiv f_2 + f_4 \pmod 2. \end{array}$$

Lo anterior nos muestra que tenemos dos posibilidades: a_1, a_3 son impares y a_2, a_4 pares o a_1, a_3 pares y a_2, a_4 impares.

Lema 3.29. *Sea $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ primo racional positivo y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$, donde $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3}$ es libre de cuadrados en todas sus factorizaciones y $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$. Entonces*

$$\beta = \frac{(1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3})\,\sqrt{\alpha}}{2} \in \mathcal{O}_{\mathbb{L}}$$

y $N_{\mathbb{K}/\mathbb{Q}}(\beta)$ es impar.

DEMOSTRACIÓN. Como $\beta^2 \in \mathbb{K}$, entonces $\mathrm{Irr}(\beta, \mathbb{K}) = x^2 - \beta^2$. Para demostrar que $\beta \in \mathcal{O}_{\mathbb{L}}$ basta probar que

$$\beta^2 = \frac{(1+\sqrt{p})^2(1+\sqrt[4]{p})^2\,\alpha}{4} \in \mathcal{O}_{\mathbb{K}}.$$

Como 2 se ramifica totalmente en $\mathcal{O}_{\mathbb{K}}$, $1 - p \equiv 2 \pmod 4$ y

$$N_{\mathbb{K}/\mathbb{Q}}(1+\sqrt{p}) = (1-p)^2, \quad N_{\mathbb{K}/\mathbb{Q}}(1+\sqrt[4]{p}) = (1-p), \quad N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8,$$

entonces $4^4 = 2^8 \mid N_{\mathbb{K}/\mathbb{Q}}(4\,\beta^2)$ y por lo tanto β^2 es un entero algebraico. La segunda afirmación es consecuencia de que $2^9 \nmid N_{\mathbb{K}/\mathbb{Q}}(4\,\beta^2)$. □

Para continuar con el estudio de la ramificación del ideal $\mathfrak{p}_{\mathbb{K}}$, primero vamos a trabajar con el caso a_1 par.

Proposición 3.30. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, $p \equiv 7 \pmod{16}$ un primo racional positivo, $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ donde $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3}$ es libre de cuadrados en todas sus factorizaciones, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$ y β como en el Lema 3.29. Si a_1 es par, entonces $N_{\mathbb{L}/\mathbb{Q}}(1+\beta) = N_{\mathbb{K}/\mathbb{Q}}(1-\beta^2) \equiv 2 \pmod 4$.*

DEMOSTRACIÓN. Consideremos $N_{\mathbb{L}/\mathbb{K}}(1+\beta) = \dfrac{b_1 + b_2\sqrt[4]{p} + b_3\sqrt{p} + b_4\sqrt[4]{p^3}}{4}$. Como $N_{\mathbb{L}/\mathbb{K}}(1+\beta) = 1 - \beta^2$, entonces

$$N_{\mathbb{L}/\mathbb{K}}(1+\beta) = \frac{4 - (1+\sqrt{p})^2(1+\sqrt[4]{p})^2(a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3})}{4}.$$

Puesto que $p \equiv 7 \pmod{16}$ tenemos

$$\begin{aligned} b_1 &\equiv 4 + 2\,a_1 + 4\,a_2 + 2\,a_3 \pmod 8 \\ b_2 &\equiv 2\,a_2 + 4\,a_3 + 2\,a_4 \pmod 8 \\ b_3 &\equiv 6\,a_1 + 2\,a_3 + 4\,a_4 \pmod 8 \\ b_4 &\equiv 4\,a_1 + 6\,a_2 + 2\,a_4 \pmod 8 \end{aligned}$$

y sumando

$$\begin{aligned} b_1 + b_3 &\equiv 4 + 4\,a_2 + 4\,a_3 + 4\,a_4 \pmod 8 \\ b_2 + b_4 &\equiv 4\,a_1 + 4\,a_3 + 4\,a_4 \pmod 8. \end{aligned}$$

Como a_2 y a_4 son impares, entonces $4\,a_2 + 4\,a_4 \equiv 0 \pmod 8$ y como a_3 es par, se sigue que $b_1 + b_3 \equiv 4 \pmod 8$ y $\dfrac{b_1+b_3}{4}$ es impar. Como a_1 y a_3 son pares, entonces $\dfrac{b_1}{4}, \dfrac{b_3}{4} \in \mathbb{Z}$ y por lo anterior tienen distinta paridad. Por otra parte, como a_1 y a_3 son pares y a_4 es impar, entonces $b_2 + b_4 \equiv 4 \pmod 8$, por lo que $\dfrac{b_2}{4}$ y $\dfrac{b_4}{4}$ también son enteros con distinta paridad. De (12) tenemos

$$N_{\mathbb{K}/\mathbb{Q}}\left(N_{\mathbb{L}/\mathbb{K}}(1+\beta)\right) \equiv (b_1^2 + b_3^2)^2 + (b_2^2 + b_4^2)^2 \equiv 1 + 1 \equiv 2 \pmod 4.$$

□

Proposición 3.31. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, $p \equiv 7 \pmod{16}$ un primo racional positivo, $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ donde $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3}$ es libre de cuadrados en todas sus factorizaciones, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$, a_1 es par y β como en el Lema 3.29. Entonces 2 se ramifica totalmente en $\mathbb{L}$.*

DEMOSTRACIÓN. Consideremos el ideal

$$\mathfrak{I}_{\mathbb{L}} = \langle 2, 1+\beta\rangle_{\mathbb{L}} = \langle 2, 1-\beta\rangle_{\mathbb{L}}\,.$$

Como $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) \mid N_{\mathbb{L}/\mathbb{Q}}(1-\beta) \equiv 2 \pmod 4$, entonces existe un ideal $\mathfrak{J}_{\mathbb{L}}$ con $\mathfrak{J}_{\mathbb{L}} \mid 1-\beta^2$ y $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{J}_{\mathbb{L}}) = 2$. Además, $\mathfrak{J}_{\mathbb{L}} \mid 2$, así que $\text{m.c.d.}\left(2^8, N_{\mathbb{L}/\mathbb{Q}}(1-\beta^2)\right) = 2$, lo que implica $\mathfrak{I}_{\mathbb{L}} = \mathfrak{J}_{\mathbb{L}}$ y $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) = 2$. Notemos que

$$\begin{aligned}\mathfrak{I}_{\mathbb{L}}{}^2 &= \langle 2, 1+\beta\rangle_{\mathbb{L}}\langle 2, 1-\beta\rangle_{\mathbb{L}} \\ &= \langle 4, 2(1+\beta), 2(1-\beta), 1-\beta^2\rangle_{\mathbb{L}} \supseteq \langle 4, 1-\beta^2\rangle_{\mathbb{L}}\,.\end{aligned}$$

Consideremos el ideal $\mathfrak{I}_{\mathbb{K}} = \langle 4, 1-\beta^2\rangle_{\mathbb{K}}$. Sea $\mathfrak{p}_{\mathbb{K}}$ el único ideal de $\mathcal{O}_{\mathbb{K}}$ con $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_{\mathbb{K}}) = 2$. Por la Proposición 3.30, $N_{\mathbb{K}/\mathbb{Q}}(1-\beta^2) \equiv 2 \pmod 4$, entonces $\mathfrak{p}_{\mathbb{K}} \mid 1-\beta^2$ y claramente $\mathfrak{p}_{\mathbb{K}} \mid 2$. Como $2 \mid N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}}) \mid \text{m.c.d.}\left(N_{\mathbb{K}/\mathbb{Q}}(2), N_{\mathbb{K}/\mathbb{Q}}(1-\beta^2)\right) = 2$ entonces $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}}) = 2$, es decir, $\mathfrak{I}_{\mathbb{K}} = \mathfrak{p}_{\mathbb{K}}$. Si extendemos $\mathfrak{I}_{\mathbb{K}}$ a $\mathcal{O}_{\mathbb{L}}$, tenemos

$$\mathfrak{I}_{\mathbb{L}}{}^2 \supseteq \langle \mathfrak{I}_{\mathbb{K}}\rangle_{\mathbb{L}} = \left\langle 4, 1-\beta^2\right\rangle_{\mathbb{L}}$$

y como

$$N_{\mathbb{L}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{L}}{}^2\right) = 4, \quad N_{\mathbb{L}/\mathbb{Q}}\left(\left\langle 4, 1-\beta^2\right\rangle_{\mathbb{L}}\right) = N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}})^2 = 4,$$

entonces $\mathfrak{I}_{\mathbb{L}}{}^2 = \langle \mathfrak{I}_{\mathbb{K}}\rangle_{\mathbb{L}}$ y por lo tanto $\mathfrak{I}_{\mathbb{L}}{}^8 = \left\langle \mathfrak{I}_{\mathbb{K}}{}^4\right\rangle_{\mathbb{L}} = \langle 2\rangle_{\mathbb{L}}$. □

Ahora estudiaremos el caso a_1 impar, el cuál es más complicado y requiere que lo estudiemos en varios subcasos.

Proposición 3.32. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo, $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones con a_1 impar, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$,*

$$\beta_1 = \frac{1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}+\sqrt{\alpha}\,(1+\sqrt{p})}{2} = \frac{(1+\sqrt{p})(1+\sqrt[4]{p}+\sqrt{\alpha})}{2} \tag{26}$$

y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. Entonces, $\beta_1 \in \mathcal{O}_{\mathbb{L}}$.

DEMOSTRACIÓN. $\text{Irr}(\beta_1, \mathbb{K}) = x^2 - t_{\mathbb{L}/\mathbb{K}}(\beta_1)\,x + N_{\mathbb{L}/\mathbb{K}}(\beta_1)$. Claramente $t_{\mathbb{L}/\mathbb{K}}(\beta_1) = 1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3}$ es un entero algebraico. Para que $\beta_1 \in \mathcal{O}_{\mathbb{L}}$, es suficiente mostrar que $N_{\mathbb{L}/\mathbb{K}}(\beta_1) \in \mathcal{O}_{\mathbb{K}}$, donde

$$N_{\mathbb{L}/\mathbb{K}}(\beta_1) = \frac{(1+\sqrt{p})^2((1+\sqrt[4]{p})^2-\alpha)}{4}. \tag{27}$$

Como 2 se ramifica totalmente en $\mathbb{K}$, entonces debemos mostrar que $N_{\mathbb{K}/\mathbb{Q}}(4) = 2^8 \mid N_{\mathbb{K}/\mathbb{Q}}\left(4\,N_{\mathbb{L}/\mathbb{K}}(\beta_1)\right)$. Por un lado,

$$N_{\mathbb{K}/\mathbb{Q}}\left((1+\sqrt{p})^2\right) = (1-p)^4 \equiv 2^4 \pmod{2^5} \tag{28}$$

y

$$(1+\sqrt[4]{p})^2 - \alpha = 1 + 2\sqrt[4]{p} + \sqrt{p} - a_1 - a_2\sqrt[4]{p} - a_3\sqrt{p} - a_4\sqrt[4]{p^3}.$$

Como $1-a_1$, $2-a_2$, $1-a_3$ y $-a_4$ son pares, entonces $2 \mid (1+\sqrt[4]{p})^2 - \alpha$ en $\mathcal{O}_{\mathbb{K}}$. Lo anterior implica que $2^4 \mid N_{\mathbb{K}/\mathbb{Q}}\left((1+\sqrt[4]{p})^2-\alpha\right)$ y así $2^8 \mid N_{\mathbb{K}/\mathbb{Q}}\left((1+\sqrt{p})^2((1+\sqrt[4]{p})^2-\alpha)\right)$. Por lo tanto $N_{\mathbb{L}/\mathbb{K}}(\beta_1) \in \mathcal{O}_{\mathbb{K}}$ y $\beta_1 \in \mathcal{O}_{\mathbb{L}}$. □

Proposición 3.33. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo, $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones con a_1 impar y $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$ y β_1 como en (26). Las paridades de $N_{\mathbb{L}/\mathbb{Q}}(\beta_1)$ y $N_{\mathbb{L}/\mathbb{Q}}(1+\beta_1)$ son distintas.*

DEMOSTRACIÓN. Es suficiente demostrar que las paridades de $N_{\mathbb{K}/\mathbb{Q}}\left(N_{\mathbb{L}/\mathbb{K}}(\beta_1)\right)$ y $N_{\mathbb{K}/\mathbb{Q}}\left(N_{\mathbb{L}/\mathbb{K}}(1+\beta_1)\right)$ son distintas. Sea $\mathfrak{p}_{\mathbb{K}}$ el único ideal de $\mathcal{O}_{\mathbb{K}}$ con norma 2, es decir, $|\mathcal{O}_{\mathbb{K}}/\mathfrak{p}_{\mathbb{K}}| = 2$. Lo anterior significa que las normas de dos elementos en $\mathcal{O}_{\mathbb{K}}$ tienen paridades distintas si y sólo si la diferencia de las normas es impar.

$$\begin{aligned} N_{\mathbb{L}/\mathbb{K}}(\beta_1) - N_{\mathbb{L}/\mathbb{K}}(1+\beta_1) &= \frac{(1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})^2 - \alpha(1+\sqrt{p})^2}{4} \\ &\quad - \frac{(3+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})^2 - \alpha(1+\sqrt{p})^2}{4} \\ &= -2 - \sqrt[4]{p} - \sqrt{p} - \sqrt[4]{p^3} \end{aligned}$$

Como $N_{\mathbb{K}/\mathbb{Q}}\left(-2-\sqrt[4]{p}-\sqrt{p}-\sqrt[4]{p^3}\right) = 16 - 17\,p + 7\,p^2 - p^3$ y p es impar, entonces las paridades de $N_{\mathbb{L}/\mathbb{Q}}(\beta)$ y $N_{\mathbb{L}/\mathbb{Q}}(1+\beta)$ son distintas. □

Proposición 3.34. *Sea β_1 como en* (26)*. Si a_1 es impar y $a_2 \equiv a_4 \pmod 4$, entonces $N_{\mathbb{L}/\mathbb{Q}}(\beta_1) \equiv 2 \pmod 4$ ó $N_{\mathbb{L}/\mathbb{Q}}(1+\beta_1) \equiv 2 \pmod 4$.*

DEMOSTRACIÓN. Primero calculemos $N_{\mathbb{L}/\mathbb{K}}(\beta_1)$ y $N_{\mathbb{L}/\mathbb{K}}(1+\beta_1)$. Sean

$$\begin{aligned} \gamma_1 &= 4N_{\mathbb{L}/\mathbb{K}}(\beta_1) = (1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})^2 - \alpha(1+\sqrt{p})^2 \\ \gamma_2 &= 4N_{\mathbb{L}/\mathbb{K}}(1+\beta_1) = (3+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})^2 - \alpha(1+\sqrt{p})^2. \end{aligned}$$

Escribimos $\gamma_1 = b_1 + b_2\sqrt[4]{p} + b_3\sqrt{p} + b_4\sqrt[4]{p^3}$, $\gamma_2 = c_1 + c_2\sqrt[4]{p} + c_3\sqrt{p} + c_4\sqrt[4]{p^3}$ donde los coeficientes están dados por:

$$\begin{aligned} b_1 &= 1 + 3\,p - 2\,a_3\,p - a_1(1+p) & c_1 &= 9 + 3\,p - 2\,a_3\,p - a_1(1+p) \\ b_2 &= 2 + 2\,p - 2\,a_4\,p - a_2(1+p) & c_2 &= 6 + 2\,p - 2\,a_4\,p - a_2(1+p) \\ b_3 &= 3 + p - 2\,a_1 - a_3(1+p) & c_3 &= 7 + p - 2\,a_1 - a_3(1+p) \\ b_4 &= 4 - 2\,a_2 - a_4(1+p) & c_4 &= 8 - 2\,a_2 - a_4(1+p) \end{aligned}$$

Es importante notar que $b_i/4, c_i/4 \in \mathbb{Z}$ para $i = 1,2,3,4$. En la demostración de la Proposición 3.9 vimos que si $\epsilon = e_1 + e_2\sqrt[4]{p} + e_3\sqrt{p} + e_4\sqrt[4]{p^3}$ y $N_{\mathbb{K}/\mathbb{Q}}(\epsilon) \equiv 2 \pmod 4$, es necesario que $e_1 \not\equiv e_3 \pmod 2$ y $e_2 \not\equiv e_4 \pmod 2$. Para ver que $N_{\mathbb{L}/\mathbb{Q}}(\beta_1) \equiv 2 \pmod 4$ ó $N_{\mathbb{L}/\mathbb{Q}}(1+\beta_1) \equiv 2 \pmod 4$ necesitamos que se cumpla alguna de las siguientes condiciones:

$$\frac{b_1+b_3}{4} \equiv \frac{b_2+b_4}{4} \equiv 1 \pmod 2, \quad \frac{c_1+c_3}{4} \equiv \frac{c_2+c_4}{4} \equiv 1 \pmod 2.$$

Sabemos que:

$$b_2 + b_4 \equiv c_2 + c_4 \equiv 4 + 6\,a_2 + 2\,a_4 \pmod 8.$$

Como $a_2 \equiv a_4 \pmod 4$, entonces $b_2 + b_4 \equiv c_2 + c_4 \equiv 4 \pmod 8$. Por lo anterior, $b_2/4$ y $b_4/4$ tienen distinta paridad y $c_2/4, c_4/4$ también tienen distinta paridad. Si $N_{\mathbb{L}/\mathbb{Q}}(\beta_1)$ es

par, entonces $b_i/4$ es par para dos valores de $i \in \{1,2,3,4\}$ y para los otros dos valores es impar. Por lo tanto $N_{\mathbb{L}/\mathbb{Q}}(\beta_1) \equiv 2 \pmod 4$. Si $N_{\mathbb{L}/\mathbb{Q}}(1+\beta_1)$ es par, la argumentación es la misma. □

Proposición 3.35. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo, $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones con a_1 impar, $a_2 \equiv a_4 \pmod 4$, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$, $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ y β_1 como en (26). Entonces 2 se ramifica totalmente en $\mathbb{L}$.*

DEMOSTRACIÓN. Denotemos por β al elemento β_1 ó $1+\beta_1$ tal que $N_{\mathbb{L}/\mathbb{Q}}(\beta)$ es par. Sea $\mathfrak{I}_{\mathbb{L}} = \langle 2, \beta\rangle_{\mathbb{L}}$. Como $N_{\mathbb{L}/\mathbb{Q}}(\beta) \equiv 2 \pmod 4$, entonces $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) = 2$. Si $\mathfrak{p}_{\mathbb{K}}$ es el único ideal de $\mathcal{O}_{\mathbb{K}}$ con norma 2, entonces $\mathfrak{I}_{\mathbb{L}} \supseteq \mathfrak{I}_{\mathbb{L}} \cap \mathbb{K} = \mathfrak{p}_{\mathbb{K}}$. Sea β' el conjugado de β en $\mathbb{L}/\mathbb{K}$ como se definió en el Lema 3.25. Así

$$\beta_1 + \beta_1' = 1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3} = (1+\sqrt[4]{p})(1+\sqrt{p}).$$

Además, $\beta_1+\beta_1' \in \mathcal{O}_{\mathbb{K}}$, con $N_{\mathbb{K}/\mathbb{Q}}(\beta_1+\beta_1') = (1-p)^3 \in 2\mathbb{Z}$. Entonces $\beta_1+\beta_1' \in \langle \mathfrak{p}_{\mathbb{K}}\rangle_{\mathbb{L}} \subseteq \mathfrak{I}_{\mathbb{L}}$. Por lo anterior $\beta_1 \equiv -\beta_1' \pmod{\mathfrak{I}_{\mathbb{L}}}$, es decir, $\mathfrak{I}_{\mathbb{L}} = \langle 2,\beta\rangle_{\mathbb{L}} = \langle 2,-\beta'\rangle_{\mathbb{L}} = \langle 2,\beta'\rangle_{\mathbb{L}}$. Por el Lema 3.25, 2 se ramifica totalmente en $\mathbb{L}$. □

Proposición 3.36. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo, $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones, a_1, a_3 impares, $a_2 \equiv 2 \pmod 4$, $a_4 \equiv 0 \pmod 4$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. Consideremos los siguientes datos:*

Condición	β	$N_{\mathbb{L}/\mathbb{K}}(\beta) - N_{\mathbb{L}/\mathbb{K}}(1+\beta)$
$a_1 \not\equiv a_3 \pmod 4$	$\dfrac{\sqrt[4]{p} + \sqrt[4]{p^3} + \sqrt{\alpha}\,(1+\sqrt[4]{p})}{2}$	$-1 - \sqrt[4]{p} - \sqrt[4]{p^3}$
$a_1 \equiv a_3 \equiv 1 \pmod 4$	$\dfrac{1 + \sqrt[4]{p} + \sqrt{\alpha}}{2}$	$-2 - \sqrt[4]{p}$
$a_1 \equiv a_3 \equiv 3 \pmod 4$	$\dfrac{1 + \sqrt[4]{p} + \sqrt{p\,\alpha}}{2}$	$-2 - \sqrt[4]{p}$

donde además, si $a_1 \equiv a_3 \pmod 4$ agregamos la condición $a_1 \equiv a_3 + 4 \pmod 8$. En los tres casos:

1. $\beta \in \mathcal{O}_{\mathbb{L}}$.
2. *Las paridades de $N_{\mathbb{L}/\mathbb{Q}}(\beta)$ y $N_{\mathbb{L}/\mathbb{Q}}(1+\beta)$ son distintas.*
3. $N_{\mathbb{L}/\mathbb{Q}}(\beta) \equiv 2 \pmod 4$ *ó* $N_{\mathbb{L}/\mathbb{Q}}(1+\beta) \equiv 2 \pmod 4$.
4. 2 *se ramifica totalmente en* $\mathbb{L}$.

DEMOSTRACIÓN. Consideremos el caso $a_1 \not\equiv a_3 \pmod 4$. Observemos que:

$$t_{\mathbb{L}/\mathbb{K}}(\beta) = \sqrt[4]{p} + \sqrt[4]{p^3} \quad \text{y} \quad N_{\mathbb{L}/\mathbb{K}}(\beta) = \frac{(\sqrt[4]{p} + \sqrt[4]{p^3})^2 - \alpha(1+\sqrt[4]{p})^2}{4}.$$

De lo anterior,

$$\begin{aligned} 4N_{\mathbb{L}/\mathbb{K}}(\beta) &= (\sqrt[4]{p} + \sqrt[4]{p^3})^2 - \alpha\,(1+\sqrt[4]{p})^2 \\ &= \sqrt{p} + 2\,p + p\,\sqrt{p} - \alpha(1 + 2\,\sqrt[4]{p} + \sqrt{p}) \\ &= (-a_1 + 2\,p - a_3\,p - 2\,p\,a_4) + (-2\,a_1 - a_2 - a_4\,p)\sqrt[4]{p} \\ &\quad +(1 + p - a_1 - 2\,a_2 - a_3)\sqrt{p} + (-a_2 - 2\,a_3 - a_4)\sqrt[4]{p^3}. \end{aligned}$$

Dadas las condiciones de la proposición,

$$-a_1 + 2\,p - a_3\,p - 2\,p\,a_4 \equiv -2\,a_1 - a_2 - a_4\,p \equiv 0 \pmod 4$$

$$1 + p - a_1 - 2\,a_2 - a_3 \equiv -a_2 - 2\,a_3 - a_4 \equiv 0 \pmod 4,$$

lo que implica $N_{\mathbb{L}/\mathbb{K}}(\beta) \in \mathcal{O}_{\mathbb{K}}$. Claramente $t_{\mathbb{L}/\mathbb{K}}(\beta) \in \mathcal{O}_{\mathbb{K}}$, por lo que $\beta \in \mathcal{O}_{\mathbb{L}}$. Los otros dos casos se demuestran de la misma forma.

Las pruebas de 2, 3 y 4 son idénticas a las que usamos para β_1 en las Proposiciones 3.33, 3.34 y 3.35, tomando en cuenta los valores de $N_{\mathbb{L}/\mathbb{K}}(\beta) - N_{\mathbb{L}/\mathbb{K}}(1+\beta)$ de la tabla. □

Proposición 3.37. *Sean* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo,* $\alpha = a_1 + a_2\,\sqrt[4]{p} + a_3\,\sqrt{p} + a_4\,\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ *libre de cuadrados en todas sus factorizaciones,* a_1, a_3 *impares,* $a_2 \equiv 0 \pmod 4$, $a_4 \equiv 2 \pmod 4$ *y* $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. *Consideremos los siguientes datos:*

a_1	a_3	β	$N_{\mathbb{L}/\mathbb{K}}(\beta) - N_{\mathbb{L}/\mathbb{K}}(1+\beta)$
$a_1 \equiv a_3 \pmod 4$		$\dfrac{1 + \sqrt{p} + \sqrt{\alpha}(1+\sqrt[4]{p})}{2}$	$-2 - \sqrt{p}$
$\equiv 1 \pmod 4$	$\equiv 3 \pmod 4$	$\dfrac{1 + \sqrt[4]{p} + \sqrt{\alpha}(\sqrt[4]{p})}{2}$	$-2 - \sqrt[4]{p}$
$\equiv 3 \pmod 4$	$\equiv 1 \pmod 4$	$\dfrac{1 + \sqrt[4]{p} + \sqrt{\alpha}(\sqrt[4]{p^3})}{2}$	$-2 - \sqrt[4]{p}$

donde además, si $a_1 \equiv a_3 \pmod 4$ *agregamos la condición* $a_1 + a_3 \equiv 4 \pmod 8$. *En los tres casos:*

1. $\beta \in \mathcal{O}_{\mathbb{L}}$.
2. *Las paridades de* $N_{\mathbb{L}/\mathbb{Q}}(\beta)$ *y* $N_{\mathbb{L}/\mathbb{Q}}(1+\beta)$ *son distintas.*
3. $N_{\mathbb{L}/\mathbb{Q}}(\beta) \equiv 2 \pmod 4$ *ó* $N_{\mathbb{L}/\mathbb{Q}}(1+\beta) \equiv 2 \pmod 4$.
4. 2 *se ramifica totalmente en* $\mathbb{L}$.

□

Proposición 3.38. *Sean* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo,* $\alpha = a_1 + a_2\,\sqrt[4]{p} + a_3\,\sqrt{p} + a_4\,\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ *libre de cuadrados en todas sus factorizaciones,* $a_1 \equiv a_3 \pmod 8$ *impares,* $a_2 \equiv 2 \pmod 4$, $a_4 \equiv 0 \pmod 4$, $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ *y* $\mathfrak{p}_{\mathbb{K}}$ *el único ideal de* $\mathcal{O}_{\mathbb{K}}$ *con* $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_{\mathbb{K}}) = 2$. *Entonces,* $\mathfrak{p}_{\mathbb{K}}$ *no se ramifica en* $\mathbb{L}/\mathbb{K}$.

DEMOSTRACIÓN. La idea de la demostración consiste en encontrar una base de $\mathbb{L}$ como $\mathbb{Q}$-espacio vectorial que confirme que $\delta_{\mathbb{L}/\mathbb{K}}$ es un ideal con norma impar.

En la Proposición 3.36 vimos que si $a_1 \equiv 1 \pmod 4$, $\gamma_1 = \dfrac{1+\sqrt[4]{p}+\sqrt{\alpha}}{2} \in \mathcal{O}_{\mathbb{L}}$ y si $a_1 \equiv 3 \pmod 4$, entonces $\gamma_2 = \dfrac{1+\sqrt[4]{p}+\sqrt{p\,\alpha}}{2} \in \mathcal{O}_{\mathbb{L}}$.

Como $a_1 \equiv a_3 \pmod 4$, entonces $a_1+a_3 \equiv 2 \pmod 4$, así que $a_1+a_2+a_3+a_4 \equiv 0 \pmod 4$.

Supongamos $a_1 \equiv a_3 \equiv 1 \pmod 4$ y $a_1+a_2+a_3+a_4 \equiv 0 \pmod 8$. Mostraremos que $\gamma_3 = \dfrac{2+\sqrt{\alpha}(1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})}{4} \in \mathcal{O}_{\mathbb{L}}$. Es claro que $t_{\mathbb{L}/\mathbb{K}}(\gamma_3) = 1 \in \mathcal{O}_{\mathbb{K}}$ y

$$N_{\mathbb{L}/\mathbb{K}}(\gamma_3) = \frac{4-\alpha(1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})^2}{16} = \frac{b_1+b_2\sqrt[4]{p}+b_3\sqrt{p}+b_4\sqrt[4]{p^3}}{16},$$

donde

$$\begin{aligned}
b_1 &= 4-a_1-3\,p\,a_1-4\,p\,a_2-3\,p\,a_3-p^2\,a_3-2\,p\,a_4-2\,p^2\,a_4\\
b_2 &= -2\,a_1-2\,p\,a_1-a_2-3\,p\,a_2-4\,p\,a_3-3\,p\,a_4-p^2\,a_4\\
b_3 &= -3\,a_1-p\,a_1-2\,a_2-2\,p\,a_2-a_3-3\,p\,a_3-4\,p\,a_4\\
b_4 &= -4\,a_1-3\,a_2-p\,a_2-2\,a_3-2\,p\,a_3-a_4-3\,p\,a_4
\end{aligned}$$

$$\begin{aligned}
b_1 &\equiv 4+10\,a_1+4\,a_2+10\,a_3 \equiv 4+10(a_1+a_3)+4\,a_2 \pmod{16}\\
b_2 &\equiv 10\,a_2+4\,a_3+10\,a_4 \equiv 10(a_2+a_4)+4\,a_3 \pmod{16}\\
b_3 &\equiv 6\,a_1+10\,a_3+4\,a_4 \pmod{16}\\
b_4 &\equiv 12\,a_1+6\,a_2+10\,a_4 \equiv 12\,a_1+10(a_2+a_4)-4\,a_2 \pmod{16}
\end{aligned}$$

El único valor posible de a_1+a_3 módulo 8 es 2, así que $10(a_1+a_3) \equiv 4 \pmod{16}$, y como $a_2 \equiv 2 \pmod 4$, entonces $b_1 \equiv 0 \pmod{16}$. Como $a_1 \equiv a_3 \equiv 1,5 \pmod 8$, entonces $a_1+a_3 \equiv 2 \pmod 8$ y $a_2+a_4 \equiv 6 \pmod 8$, esto implica que $10(a_2+a_4) \equiv 12 \pmod{16}$. Además, $4\,a_3 \equiv 4 \pmod{16}$ para cualquier $a_3 \equiv 1 \pmod 4$. Por lo tanto, $b_2 \equiv 0 \pmod{16}$. Como a_1 y a_3 son congruentes módulo 8, entonces $3\,a_1+5\,a_3 \equiv 3\,a_1+5\,a_1 \equiv 0 \pmod 8$ y dado que $4 \mid a_4$, entonces $4\,a_4 \equiv 0 \pmod{16}$. Por esto, $b_3 \equiv 0 \pmod{16}$. Para cualquier $a_1 \equiv 1 \pmod 4$ se tiene $12\,a_1 \equiv 12 \pmod{16}$, $4\,a_2 \equiv 8 \pmod{16}$ y como $a_2+a_4 \equiv 6 \pmod 8$, entonces $10(a_2+a_4) \equiv 12 \pmod{16}$, por lo anterior $b_4 \equiv 0 \pmod{16}$. Esto implica que $N_{\mathbb{L}/\mathbb{K}}(\gamma_3) \in \mathcal{O}_{\mathbb{K}}$.

Ahora consideremos los siguientes casos: si $a_1 \equiv a_3 \equiv 1 \pmod 4$ y $a_1+a_2+a_3+a_4 \equiv 4 \pmod 8$, entonces

$$\gamma_4 = \frac{2(\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})+\sqrt{\alpha}(1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})}{4} \in \mathcal{O}_{\mathbb{K}};$$

si $a_1 \equiv a_3 \equiv 3 \pmod 4$ y $a_1+a_2+a_3+a_4 \equiv 0 \pmod 8$, entonces

$$\gamma_5 = \frac{2+\sqrt{p\,\alpha}(1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})}{4} \in \mathcal{O}_{\mathbb{K}};$$

finalmente, si $a_1 \equiv a_3 \equiv 3 \pmod 4$ y $a_1+a_2+a_3+a_4 \equiv 4 \pmod 8$, entonces

$$\gamma_6 = \frac{2(\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})+\sqrt{p\,\alpha}(1+\sqrt[4]{p}+\sqrt{p}+\sqrt[4]{p^3})}{4} \in \mathcal{O}_{\mathbb{K}}.$$

La demostración de que $\gamma_4, \gamma_5, \gamma_6 \in \mathcal{O}_{\mathbb{K}}$ es idéntica a la que usamos para γ_3.

Como ya vimos en (21), el discriminante de la base (20) es $\Delta(\mathcal{B}) = -2^{24}p^6 N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ y sabemos que $\delta_{\mathbb{K}} = 2^8\, p^3$. Como $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$, entonces $2^{26} \mid\mid \Delta(\mathcal{B})$.

Si $a_1 \equiv a_3 \equiv 1 \pmod 4$ y $a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod 8$, entonces

$$\mathcal{B}_1 = \{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_1, \gamma_1\sqrt[4]{p}, \gamma_1\sqrt{p}, \gamma_3\}$$

es una base de $\mathbb{L}$ como $\mathbb{Q}$-espacio vectorial con $|\Delta(\mathcal{B}_1)| = 2^{16}p^6 N_{\mathbb{K}/\mathbb{Q}}(\alpha)$, ya que el denominador de γ_1 es 2 y el de γ_3 es 4. Usando la Proposición 1.26, $\mathfrak{p}_{\mathbb{K}}$ no se ramifica en $\mathbb{L}$. La demostración para los demás casos es análoga usando las siguientes bases:

$$\mathcal{B}_2 = \{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_1, \gamma_1\sqrt[4]{p}, \gamma_1\sqrt{p}, \gamma_4\}$$

cuando $a_1 \equiv a_3 \equiv 1 \pmod 4$ y $a_1 + a_2 + a_3 + a_4 \equiv 4 \pmod 8$;

$$\mathcal{B}_3 = \{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_2, \gamma_2\sqrt[4]{p}, \gamma_2\sqrt{p}, \gamma_5\}$$

si $a_1 \equiv a_3 \equiv 3 \pmod 4$ y $a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod 8$ y

$$\mathcal{B}_4 = \{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_2, \gamma_2\sqrt[4]{p}, \gamma_2\sqrt{p}, \gamma_6\}$$

si $a_1 \equiv a_3 \equiv 3 \pmod 4$ y $a_1 + a_2 + a_3 + a_4 \equiv 4 \pmod 8$. □

Proposición 3.39. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo, $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones, $a_1 + a_3 \equiv 0 \pmod 8$ impares (lo que implica $a_1 \not\equiv a_3 \pmod 4$), $a_2 \equiv 0 \pmod 4$, $a_4 \equiv 2 \pmod 4$, $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ y $\mathfrak{p}_{\mathbb{K}}$ el único ideal de $\mathcal{O}_{\mathbb{K}}$ con $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_{\mathbb{K}}) = 2$. Entonces, $\mathfrak{p}_{\mathbb{K}}$ no se ramifica en $\mathbb{L}/\mathbb{K}$.*

DEMOSTRACIÓN. Sean

$$\begin{aligned}
\gamma_1 &= \frac{1 + \sqrt[4]{p} + \sqrt[4]{p}\,\sqrt{\alpha}}{2},\\
\gamma_2 &= \frac{1 + \sqrt[4]{p} + \sqrt[4]{p^3}\,\sqrt{\alpha}}{2},\\
\gamma_3 &= \frac{2\sqrt[4]{p} + \sqrt{\alpha}(7 + 7\sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3})}{4},\\
\gamma_4 &= \frac{2(1 + \sqrt{p} + \sqrt[4]{p^3}) + \sqrt{\alpha}(7 + 7\sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3})}{4},\\
\gamma_5 &= \frac{2\sqrt[4]{p} + \sqrt{\alpha}(1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3})}{4},\\
\gamma_6 &= \frac{2(1 + \sqrt{p} + \sqrt[4]{p^3}) + \sqrt{\alpha}(1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3})}{4},
\end{aligned}$$

y $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ y $\mathcal{B}_4$ como en la Proposición 3.38, pero con las nuevas definiciones de $\gamma_1, \ldots, \gamma_6$. La demostración de que $\delta_{\mathbb{L}/\mathbb{K}}$ es impar es análoga a la que hicimos en la Proposición 3.38 usando $\mathcal{B}_1$ si $a_1 \equiv 1 \pmod 4$, $a_3 \equiv 3 \pmod 4$ y $a_2 + a_4 \equiv 2 \pmod 4$; $\mathcal{B}_2$ cuando $a_1 \equiv 1 \pmod 4$, $a_3 \equiv 3 \pmod 4$ y $a_2 + a_4 \equiv 6 \pmod 4$; $\mathcal{B}_3$ si $a_1 \equiv 3 \pmod 4$, $a_3 \equiv 1 \pmod 4$ y $a_2 + a_4 \equiv 6 \pmod 4$ y usaremos la base $\mathcal{B}_4$ si $a_1 \equiv 3 \pmod 4$, $a_3 \equiv 1 \pmod 4$ y $a_2 + a_4 \equiv 2 \pmod 4$. □

El siguiente teorema agrupa las últimas proposiciones.

Teorema 3.40. *Sean* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo,* $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ *libre de cuadrados en todas sus factorizaciones, con* $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$ *y* $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$*. Entonces,* 2 *se ramifica totalmente en* $\mathbb{L}$ *si y sólo si se cumple alguna de las siguientes condiciones:*

1. a_1, a_3 *son pares y* a_2, a_4 *son impares.*
2. a_1, a_3 *son impares y* $a_2 \equiv a_4 \pmod 4$ *son pares.*
3. $a_1 \not\equiv a_3 \pmod 4$ *impares,* $a_2 \equiv 2 \pmod 4$ *y* $a_4 \equiv 0 \pmod 4$.
4. $a_1 \equiv a_3 + 4 \pmod 8$ *impares,* $a_2 \equiv 2 \pmod 4$ *y* $a_4 \equiv 0 \pmod 4$.
5. $a_1 \equiv a_3 \pmod 4$ *impares,* $a_2 \equiv 0 \pmod 4$ *y* $a_4 \equiv 2 \pmod 4$.
6. $a_1 + a_3 \equiv 4 \pmod 8$ *impares,* $a_2 \equiv 0 \pmod 4$ *y* $a_4 \equiv 2 \pmod 4$.

Equivalentemente, 2 *no se ramifica totalmente en* $\mathbb{L}$ *si y sólo si se cumple alguna de las siguientes condiciones:*

1. $a_1 \equiv a_3 \pmod 8$ *impares,* $a_2 \equiv 2 \pmod 4$ *y* $a_4 \equiv 0 \pmod 4$.
2. $a_1 \not\equiv a_3 \pmod 4$, $a_1 + a_3 \equiv 0 \pmod 8$, $a_2 \equiv 0 \pmod 4$ *y* $a_4 \equiv 2 \pmod 4$. □

3.4.3. $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ impar

Vamos a estudiar la ramificación de 2 en $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ cuando $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ es impar y α libre de cuadrados en todas sus factorizaciones. Sea $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3}$. Para que $N_{\mathbb{L}/\mathbb{Q}}(\alpha)$ sea impar, es necesario que haya un número impar de a_i's pares y, como consecuencia, una cantidad impar de coeficientes impares. Cuando esto sucede, existen tres coeficientes con la misma paridad y uno con paridad distinta a la de los demás. Primero estudiaremos el caso en que a_1 es el coeficiente con paridad distinta a los demás y después el caso en que a_2 es el que tiene paridad distinta. Los otros dos casos se reducen a alguno de estos dos multiplicando α por $\sqrt{p}$, ya que

$$\mathbb{K}(\sqrt{\alpha}) = \mathbb{K}(\sqrt{\alpha}\sqrt[4]{p}) = \mathbb{K}\left(\sqrt{\alpha\sqrt{p}}\right).$$

Proposición 3.41. *Sea* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo,* $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ *libre de cuadrados en todas sus factorizaciones con* a_1 *par y* a_2, a_3, a_4 *impares y* $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$*. Entonces,* 2 *se ramifica totalmente en* $\mathbb{L}$*.*

DEMOSTRACIÓN. Sea

$$\beta = \frac{(1+\sqrt[4]{p})(1+\sqrt{p})(1+\sqrt{\alpha})}{2}.$$

Es fácil ver que $2^2 \mid\mid N_{\mathbb{L}/\mathbb{Q}}\left(1+\sqrt[4]{p}\right)$ y $2^4 \mid\mid N_{\mathbb{L}/\mathbb{Q}}\left(1+\sqrt{p}\right)$. Además, $N_{\mathbb{L}/\mathbb{K}}(1+\sqrt{\alpha}) = 1-\alpha$ y por (13), $N_{\mathbb{K}/\mathbb{Q}}(1-\alpha) \equiv 8 \pmod{16}$. Por lo tanto,

$$N_{\mathbb{L}/\mathbb{Q}}\left(\frac{(1+\sqrt[4]{p})(1+\sqrt{p})(1+\sqrt{\alpha})}{2}\right) \equiv 2 \pmod 4.$$

El ideal $\mathfrak{I}_{\mathbb{L}} = \langle 2, \beta\rangle_{\mathbb{L}}$ cumple $N_{\mathbb{L}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{L}}) = 2$, y como $N_{\mathbb{K}/\mathbb{Q}}\left((1+\sqrt[4]{p})(1+\sqrt{p})\right)$ es par, entonces $(1+\sqrt[4]{p})(1+\sqrt{p}) \in \mathfrak{p}_{\mathbb{K}}$, donde $\mathfrak{p}_{\mathbb{K}}$ es el único ideal de $\mathcal{O}_{\mathbb{K}}$ con norma 2. Como

$\mathfrak{I}_{\mathbb{L}} \cap \mathbb{K} = \mathfrak{p}_{\mathbb{K}}$, entonces $(1 + \sqrt[4]{p})(1 + \sqrt{p}) \in \mathfrak{I}_{\mathbb{L}}$, por lo que el conjugado $\beta' \in \mathfrak{I}_{\mathbb{L}}$. Por el Lema 3.25, 2 se ramifica totalmente en $\mathbb{L}$. □

Proposición 3.42. *Sea $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo, $\alpha = a_1 + a_2 \sqrt[4]{p} + a_3 \sqrt{p} + a_4 \sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones con a_1 impar, a_2, a_3, a_4 pares y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. Entonces, 2 se ramifica totalmente en $\mathbb{L}$ si y sólo si se cumple una de las siguientes condiciones:*

1. $a_2 \not\equiv a_4 \pmod{4}$.
2. $a_3 \equiv 2 \pmod{4}$ *y* $a_2 \equiv a_4 \pmod{4}$.

Equivalentemente, 2 no se ramifica totalmente en $\mathbb{L}$ si y sólo si $a_3 \equiv 0 \pmod{4}$ y $a_2 \equiv a_4 \pmod{4}$.

DEMOSTRACIÓN. La demostración de que bajo las primeras condiciones 2 se ramifica totalmente es similar a la que hemos usado a lo largo del capítulo considerando los valores de β siguientes:

Condiciones	β
$a_2 \not\equiv a_4 \pmod{4}$	$\dfrac{(1+\sqrt{p})(1+\sqrt{\alpha})}{2}$
$a_1 \equiv 3 \pmod{4}$ y $a_2 \equiv a_3 \equiv a_4 \equiv 2 \pmod{4}$	$\dfrac{(1+\sqrt[4]{p})(1+\sqrt{\alpha})}{2}$
$a_1 \equiv 1 \pmod{4}$ y $a_2 \equiv a_3 \equiv a_4 \equiv 2 \pmod{4}$	$\dfrac{(1+\sqrt[4]{p})(1+\sqrt{p\,\alpha})}{2}$
$a_3 \equiv 2 \pmod{4}$ y $a_2 \equiv a_4 \equiv 0 \pmod{4}$	$\dfrac{(1+\sqrt{p})(1+\sqrt{\alpha})}{2}$

Para comprobar los casos en los que no hay ramificación debemos utilizar los siguientes elementos con las bases que se describirán posteriormente:

$$\gamma_1 = \frac{1+\sqrt{\alpha}}{2}, \quad \gamma_2 = \frac{1+\sqrt{p\,\alpha}}{2},$$
$$\gamma_3 = \frac{1+\sqrt{\alpha}(1+\sqrt[4]{p}+\sqrt[4]{p^3})}{2}, \quad \gamma_4 = \frac{1+\sqrt{p\,\alpha}(1+\sqrt[4]{p}+\sqrt[4]{p^3})}{2}.$$

Las bases que usaremos son las siguientes: si $a_1 \equiv 1 \pmod{4}$, $a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{4}$,

$$\mathcal{B}_1 = \left\{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_1, \gamma_1\sqrt[4]{p}, \gamma_1\sqrt{p}, \gamma_1\sqrt[4]{p^3}\right\};$$

si $a_1 \equiv 3 \pmod{4}$, $a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{4}$,

$$\mathcal{B}_2 = \left\{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_2, \gamma_2\sqrt[4]{p}, \gamma_2\sqrt{p}, \gamma_2\sqrt[4]{p^3}\right\};$$

si $a_1 \equiv 3 \pmod{4}$, $a_3 \equiv 0 \pmod{4}$ y $a_2 \equiv a_4 \equiv 2 \pmod{4}$,

$$\mathcal{B}_3 = \left\{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_3, \gamma_3\sqrt[4]{p}, \gamma_3\sqrt{p}, \gamma_3\sqrt[4]{p^3}\right\};$$

si $a_1 \equiv 1 \pmod 4$, $a_3 \equiv 0 \pmod 4$ y $a_2 \equiv a_4 \equiv 2 \pmod 4$,

$$\mathcal{B}_4 = \left\{1, \sqrt[4]{p}, \sqrt{p}, \sqrt[4]{p^3}, \gamma_4, \gamma_4\sqrt[4]{p}, \gamma_4\sqrt{p}, \gamma_4\sqrt[4]{p^3}\right\}.$$

□

Ahora estudiaremos el caso en que a_2 es el coeficiente que tiene paridad distinta a la de los demás:

Proposición 3.43. *Sea $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo, $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_\mathbb{K}$ libre de cuadrados en todas sus factorizaciones con $a_1 \equiv a_3 \equiv a_4 \pmod 2$, $a_1 \not\equiv a_2 \pmod 2$ y $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$. Entonces, 2 se ramifica totalmente.*

DEMOSTRACIÓN. Sea $\mathcal{B}$ como en (20). De acuerdo a (22) tenemos la contención

$$\langle 2^8\, N_{\mathbb{K}/\mathbb{Q}}(\alpha)\rangle \subseteq \langle N_{\mathbb{K}/\mathbb{Q}}\left(\delta_{\mathbb{L}/\mathbb{K}}\right)\rangle.$$

Aplicando la Proposición 3.18, podemos inferir de la contención anterior que es posible dividir entre 2 a lo más a cuatro elementos de $\mathcal{B}$. Vamos a probar que ninguno es divisible entre 2.

En la Proposición 3.19, vimos que cuando $\alpha \in \mathcal{U}_\mathbb{K}$ y $\mathcal{B}$ no es una base entera, entonces

$$\gamma = \frac{1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3}}{2}(1 + \sqrt{\alpha}) \in \mathcal{O}_\mathbb{L}.$$

En el caso $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ impar, lo que podemos garantizar, siguiendo la misma demostración, es que si se divide entre 2 algún elemento de $\mathcal{B}$, entonces $\gamma \in \mathcal{O}_\mathbb{L}$. Nuevamente tenemos

$$\operatorname{ord}_2\left(N_{\mathbb{L}/\mathbb{Q}}\left(1 + \sqrt[4]{p} + \sqrt{p} + \sqrt[4]{p^3}\right)\right) = 6, \quad \operatorname{ord}_2\left(N_{\mathbb{L}/\mathbb{Q}}(2)\right) = 8.$$

Además, $N_{\mathbb{L}/\mathbb{K}}(1 + \sqrt{\alpha}) = 1 - \alpha = 1 - a_1 - a_2\sqrt[4]{p} - a_3\sqrt{p} - a_4\sqrt[4]{p^3}$, donde $1 - a_1 \equiv -a_2 \pmod 2$ tienen distinta paridad que $-a_3 \equiv -a_4 \pmod 2$. Por esto y (12), $N_{\mathbb{L}/\mathbb{Q}}(1 + \sqrt{\alpha}) \equiv 2 \pmod 4$. Así, $N_{\mathbb{L}/\mathbb{Q}}(\gamma) \notin \mathbb{Z}$ y esto implica que $\gamma \notin \mathcal{O}_\mathbb{L}$. Por lo tanto, no podemos dividir entre 2 a ninguno de los elementos de $\mathcal{B}$, lo que significa que $\langle 2^8\rangle \mid \left\langle N_{\mathbb{K}/\mathbb{Q}}\left(\delta_{\mathbb{L}/\mathbb{K}}\right)\right\rangle$ y 2 se ramifica totalmente en $\mathbb{L}$. □

3.5. El 2-grupo de clases de $\mathbb{K}$

Sea $\mathbb{K}$ un campo de números y $\mathbb{H}_\mathbb{K}$ su campo de clases de Hilbert. La ramificación en extensiones cuadráticas está estrechamente relacionada con el 2-rango de $Cl_\mathbb{K}$. Como $Cl_\mathbb{K} \cong C_{n_1} \times \cdots \times C_{n_k}$ donde $n_i = p_i^{e_i}$ para algún p_i primo racional positivo, entonces existe $C_2^r \cong H \subseteq Cl_\mathbb{K}$, donde $r \in \mathbb{N}$ es el 2-rango de $Cl_\mathbb{K}$. Además, r es el máximo entero que cumple esta condición. El grupo de Galois del campo de clases de Hilbert sobre el campo base es isomorfo a $Cl_\mathbb{K}$, así que existe $H_1 \subseteq \text{Gal}(\mathbb{H}_\mathbb{K}/\mathbb{K})$ tal que $H_1 \cong Cl_\mathbb{K}/H$. El grupo de Galois del campo fijo $\mathbb{H}_\mathbb{K}^{H_1}$ sobre $\mathbb{K}$ es isomorfo a C_2^r. De esta forma, si encontramos la máxima extensión no ramificada sobre $\mathbb{K}$ con grupo de Galois C_2^r, entonces el 2-rango de $Cl_\mathbb{K}$ es r. En esta sección usaremos esta idea para demostrar que si $p \equiv 7 \pmod{16}$ es un primo racional, $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ y $\mathbb{F} = \mathbb{Q}(\sqrt{p})$, entonces Cl_2, el 2-grupo de clases de $\mathbb{K}$, cumple $Cl_2 \cong \mathbb{Z}/2\mathbb{Z}$. Para esto, necesitamos probar que cualquier extensión de la forma $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ es ramificada para cualquier α tal que $\mathbb{L} \neq \mathbb{K}(U_\mathbb{F})$.

Con lo realizado anteriormente, observamos que 2 se ramifica totalmente en $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ para cualquier α salvo en los siguientes tres casos descritos en el Teorema 3.40 y la Proposición 3.42:

1. $a_1 \equiv a_3 \pmod 8$ impares, $a_2 \equiv 2 \pmod 4$ y $a_4 \equiv 0 \pmod 4$ con $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$.
2. $a_1 \not\equiv a_3 \pmod 4$, $a_1 + a_3 \equiv 0 \pmod 8$, $a_2 \equiv 0 \pmod 4$ y $a_4 \equiv 2 \pmod 4$ con $N_{\mathbb{K}/\mathbb{Q}}(\alpha) \equiv 4 \pmod 8$.
3. a_1 impar, $a_2 \equiv a_4 \pmod 4$ pares y $a_3 \equiv 0 \pmod 4$. con $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ impar.

Primero vamos a estudiar lo que sucede cuando no existe ningún ideal $\mathfrak{I}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$ tal que ${\mathfrak{I}_{\mathbb{K}}}^2 = \langle\alpha\rangle_{\mathbb{K}}$.

Proposición 3.44. *Sea $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ con p un primo racional positivo y $\alpha \in \mathcal{O}_{\mathbb{K}}$ libre de cuadrados en todas sus factorizaciones. Supongamos que existe un ideal $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{K}}$ tal que $\operatorname{ord}_{\mathfrak{p}}(\langle\alpha\rangle_{\mathbb{K}})$ es impar. Entonces $\mathfrak{p}$ se ramifica totalmente en $\mathbb{L}/\mathbb{K}$.*

DEMOSTRACIÓN. Sea $\langle\mathfrak{p}, \sqrt{\alpha}\rangle_{\mathbb{L}}$. Como $\operatorname{ord}_{\mathfrak{p}}(\langle\alpha\rangle_{\mathbb{K}})$, es impar, entonces existe $t \in \mathbb{N}$ impar tal que $\langle\mathfrak{p}\rangle_{\mathbb{K}}^t \mid\mid \langle\alpha\rangle_{\mathbb{K}}$. El ideal $\langle\alpha\rangle_{\mathbb{L}}$ es un cuadrado porque $\sqrt{\alpha} \in \mathbb{L}$, lo que implica que cada ideal primo que divide a $\langle\alpha\rangle_{\mathbb{L}}$ debe estar elevada a una potencia par. Como t es impar, para que $\mathfrak{q}_{\mathbb{L}}^{2t} \mid\mid \langle\alpha\rangle_{\mathbb{L}}$, necesariamente $\langle\mathfrak{p}\rangle_{\mathbb{L}} = \mathfrak{q}_{\mathbb{L}}^2$. Entonces $\mathfrak{p}$ se ramifica totalmente en $\mathbb{L}/\mathbb{K}$. □

La proposición anterior nos muestra que si $\langle\alpha\rangle_{\mathbb{K}}$ no es un cuadrado, entonces la extensión $\mathbb{L}/\mathbb{K}$ es ramificada. De esta forma nos falta considerar los casos en que $\langle\alpha\rangle_{\mathbb{K}} = {\mathfrak{I}_{\mathbb{K}}}^2$ para algún ideal $\mathfrak{I}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$. Notemos que, por el Teorema del 2-rango de Gauss, si $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ con p un primo racional, entonces $h_{\mathbb{F}}$ es impar.

Lema 3.45. *Sean $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$ y $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ con $p \equiv 7 \pmod{16}$ un primo racional positivo. Si $\alpha \in \mathbb{K}$ es tal que $\langle\alpha\rangle_{\mathbb{K}} = {\mathfrak{I}_{\mathbb{K}}}^2$ para algún ideal $\mathfrak{I}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$, entonces existe $\beta \in \mathcal{O}_{\mathbb{K}}$ tal que $\langle\beta\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ y $N_{\mathbb{K}/\mathbb{F}}(\beta) = B^2$ para algún $B \in \mathcal{O}_{\mathbb{F}}$.*

DEMOSTRACIÓN. Como la norma de ideales es multiplicativa y $\langle\alpha\rangle_{\mathbb{K}} = {\mathfrak{I}_{\mathbb{K}}}^2$, entonces $N_{\mathbb{K}/\mathbb{F}}(\langle\alpha\rangle_{\mathbb{K}}) = {\mathfrak{I}_{\mathbb{F}}}^2$, para algún $\mathfrak{I}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{F}}$. Además, para cierto $B \in \mathcal{O}_{\mathbb{F}}$, $\mathfrak{I}_{\mathbb{F}} = \langle B\rangle_{\mathbb{F}}$ ya que $h_{\mathbb{F}}$ es impar. Así $N_{\mathbb{K}/\mathbb{F}}(\langle\alpha\rangle_{\mathbb{K}}) = \langle N_{\mathbb{K}/\mathbb{F}}(\alpha)\rangle_{\mathbb{F}} = \langle B^2\rangle_{\mathbb{F}}$. De la igualdad anterior, $N_{\mathbb{K}/\mathbb{F}}(\alpha) = B^2\,U$ con $U \in \mathcal{U}_{\mathbb{F}}$. Podemos suponer $U = \pm 1$ ó $U = \pm U_{\mathbb{F}}$. Si $U = \pm U_{\mathbb{F}}$, entonces $N_{\mathbb{K}/\mathbb{F}}(\alpha/\mu_2) = \pm B^2$, donde μ_2 es el generador de $\mathcal{U}_{\mathbb{K}}$ con $N_{\mathbb{K}/\mathbb{F}}(\mu_2) = U_{\mathbb{F}}$. Sea $\beta = \alpha$ ó $\beta = \alpha/\mu_2$ tal que $N_{\mathbb{K}/\mathbb{F}}(\beta) = \pm B^2$.

En $\mathcal{O}_{\mathbb{F}}$, $(a_1 + a_2\sqrt{p})^2 = a_1^2 + p\,a_2^2 + 2\,a_1\,a_2\,\sqrt{p}$, así, los cuadrados módulo $\langle\sqrt{p}\rangle_{\mathbb{F}}$ son los mismos cuadrados de $\mathbb{Z}$ módulo p. Si $a \in \mathbb{Z}$, entonces $\left(\dfrac{a}{p}\right) = 1$ implica $\left(\dfrac{-a}{p}\right) = -1$, así que, si $A \in \mathcal{O}_{\mathbb{F}}$ es un cuadrado módulo $\langle\sqrt{p}\rangle_{\mathbb{F}}$ entonces $-A$ no es un cuadrado módulo $\langle\sqrt{p}\rangle_{\mathbb{F}}$. Por otra parte, si $\beta = b_1 + b_2\sqrt[4]{p} + b_3\sqrt{p} + b_4\sqrt[4]{p^3}$, tenemos:

$$\begin{aligned} N_{\mathbb{K}/\mathbb{F}}(\beta) &= (b_1 + b_3\sqrt{p})^2 - \sqrt{p}(b_2 + b_4\sqrt{p})^2 \\ &= (b_1^2 + b_3^2\,p - 2\,p\,b_2\,a_4) + \sqrt{p}(2\,b_1\,b_3 - b_2^2 - p\,b_4^2). \end{aligned}$$

Lo anterior nos muestra que $N_{\mathbb{K}/\mathbb{F}}(\beta) \equiv b_1^2 \pmod{\langle\sqrt{p}\rangle_{\mathbb{F}}}$ es un cuadrado módulo $\langle\sqrt{p}\rangle_{\mathbb{F}}$, por lo que $N_{\mathbb{K}/\mathbb{F}}(\beta) = B^2$. □

La parte importante de la siguiente proposición es la afirmación 7, los primeros seis incisos sirven como guía para justificar que $\mathfrak{I}_{\mathbb{K}}$ es un ideal principal.

Proposición 3.46. *Sean* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo* $A_1 = a_1 + a_3\sqrt{p}$, $A_2 = a_2 + a_4\sqrt{p}$ *y* $\alpha = A_1 + A_2\sqrt[4]{p} \in \mathcal{O}_{\mathbb{K}} - \mathcal{O}_{\mathbb{F}}$ *tal que* $\langle\alpha\rangle_{\mathbb{K}} = {\mathfrak{I}_{\mathbb{K}}}^2$, $N_{\mathbb{K}/\mathbb{F}}(\alpha) = B^2$ *y* α *cumple las condiciones de los casos* 1, 2 *ó* 3 *descritos al principio de esta sección. Entonces se cumplen las siguientes afirmaciones:*

1. *Si* $B = b_1 + b_2\sqrt{p}$, *entonces* b_1, b_2 *tienen la misma paridad en los casos* 1 *y* 2, *mientras que en el caso* 3, b_1 *es impar y* $b_2 \equiv 0 \pmod{4}$.
2. $\langle L_2\rangle_{\mathbb{F}}^2 \mid\mid \langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}}$.
3. *En los casos* 1 *y* 2, $\langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}} = \langle L_2\rangle_{\mathbb{F}}(\langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}})$. *En el caso* 3, $\langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}} = \langle 2\rangle_{\mathbb{F}}(\langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}})$.
4. *Sea* $\mathfrak{p}_{\mathbb{F}}$ *un ideal de* $\mathcal{O}_{\mathbb{F}}$ *tal que* $\mathfrak{p}_{\mathbb{F}} \mid \langle A_1\rangle_{\mathbb{F}}$ *y* $\mathfrak{p}_{\mathbb{F}} \mid \langle B\rangle_{\mathbb{F}}$. *Si* $\mathfrak{p}_{\mathbb{F}}$ *es inerte en* $\mathbb{K}/\mathbb{F}$ *y* $\mathfrak{p}_{\mathbb{F}}^k \mid\mid \langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}}$, *entonces* k *es par.*
5. *Sea* $\mathfrak{p}_{\mathbb{F}}$ *un ideal de* $\mathcal{O}_{\mathbb{F}}$ *tal que* $\mathfrak{p}_{\mathbb{F}} \mid \langle A_1\rangle_{\mathbb{F}}$ *y* $\mathfrak{p}_{\mathbb{F}} \mid \langle B\rangle_{\mathbb{F}}$. *Si* $\mathfrak{p}_{\mathbb{F}}$ *se descompone en* $\mathbb{K}/\mathbb{F}$ *y* $\mathfrak{p}_{\mathbb{F}}^k \mid\mid \langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}}$, *entonces* k *es par.*
6. $\langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}} = \langle 2\sqrt{p}^t\rangle_{\mathbb{F}} {\mathfrak{I}_{\mathbb{F}}}^2$ *para algún* $t \in \mathbb{N}_0$ *y* $\mathfrak{I}_{\mathbb{F}}$ *un ideal de* $\mathcal{O}_{\mathbb{F}}$ *tal que* $\mathfrak{I}_{\mathbb{F}} + \langle 2\sqrt{p}\rangle_{\mathbb{F}} = \mathcal{O}_{\mathbb{F}}$.
7. $\mathfrak{I}_{\mathbb{K}}$ *es principal.*

DEMOSTRACIÓN. Primero observemos que

$$B^2 = (a_1 + a_3\sqrt{p})^2 - \sqrt{p}(a_2 + a_4\sqrt{p})^2 \quad \text{y} \quad B^2 = b_1^2 + p\,b_2^2 + 2\,b_1\,b_2\sqrt{p},$$

así:

$$(a_1^2 + a_3^2\,p - 2\,p\,a_2\,a_4) + \sqrt{p}(2\,a_1\,a_3 - a_2^2 - p\,a_4^2) = b_1^2 + p\,b_2^2 + 2\,b_1\,b_2\sqrt{p}. \tag{29}$$

En los primeros dos casos, como a_1, a_3 son impares y a_2, a_4 son pares, tenemos

$$(a_1^2 + a_3^2\,p - 2\,p\,a_2\,a_4) = b_1^2 + p\,b_2^2 \equiv 0 \pmod{4},$$

así, b_1, b_2 deben tener la misma paridad. Con esto demostramos la afirmación 1 en los primeros dos casos, pero podemos decir más acerca de b_1 y b_2. Primero notemos que $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = N_{\mathbb{F}/\mathbb{Q}}(B^2) \equiv 4 \pmod{8}$, entonces $N_{\mathbb{F}/\mathbb{Q}}(B) \equiv 2 \pmod{4}$, de donde b_1, b_2 son impares. En el caso 1, $a_1\,a_3 \equiv 1 \pmod{4}$, así:

$$2\,a_1\,a_3 - a_2^2 - p\,a_4^2 \equiv 2 - 4 - 0 \equiv 6 \pmod{8},$$

lo que implica $b_1 \not\equiv b_2 \pmod{4}$. En el caso 2, $a_1\,a_3 \equiv 3 \pmod{4}$ y

$$2\,a_1\,a_3 - a_2^2 - p\,a_4^2 \equiv 6 - 0 - 4 \equiv 2 \pmod{8},$$

por tanto, $b_1 \equiv b_2 \pmod{4}$.

Ahora estudiemos el tercer caso. Aquí tenemos a_1 impar y $a_3 \equiv 0 \pmod{4}$. Por otra parte,

$$b_1^2 + p\,b_2^2 = (a_1^2 + a_3^2\,p - 2\,p\,a_2\,a_4) \equiv 1 + 0 - 0 \pmod{8},$$

y debido a que $p \equiv 7 \pmod{8}$, entonces b_1 es impar y b_2 es par, más aún, $b_2 \equiv 0 \pmod{4}$.

Sea $f(x) = x^2 - 2(a_1 + a_3\sqrt{p})x + B^2 \in \mathcal{O}_{\mathbb{F}}[x]$. Observemos que $f(\alpha) = 0$ y como $\alpha \in \mathcal{O}_{\mathbb{K}} - \mathcal{O}_{\mathbb{F}}$, por la Proposición 3.10 existe $C \in \mathcal{O}_{\mathbb{F}}$ tal que

$$4A_1^2 - 4B^2 = 4\,(A_1 + B)\,(A_1 - B) = C^2\sqrt{p}, \tag{30}$$

donde $A_1 = a_1 + a_3\sqrt{p}$ y $B = b_1 + b_2\sqrt{p}$.

En el caso 1, $a_1 \equiv a_3 \pmod 4$ y $b_1 \not\equiv b_2 \pmod 4$, así que $a_1 + b_1 \not\equiv a_3 + b_2 \pmod 4$ y $a_1 - b_1 \not\equiv a_3 - b_2 \pmod 4$. Consecuentemente, si $A_1 + B = c_1 + c_2\sqrt{p}$, entonces $c_1 \not\equiv c_2 \pmod 4$ y ambos son pares. Es claro que $2 \mid A_1 + B$. Por otra parte $\dfrac{c_1 + c_2\sqrt{p}}{2}$ tiene un coeficiente par y uno impar, entonces $N_{\mathbb{F}/\mathbb{Q}}\left(\dfrac{c_1 + c_2\sqrt{p}}{2}\right)$ es impar y $2\,L_2 \nmid A_1 + B$. De la misma forma $2 \mid A_1 - B$ pero $2\,L_2 \nmid A_1 - B$. En el caso 2, $a_1 \not\equiv a_3 \pmod 4$ y $b_1 \equiv b_2 \pmod 4$, por lo que, de nuevo $a_1 + b_1 \not\equiv a_3 + b_2 \pmod 4$. También en este caso se cumple la afirmación 2. Para el caso 3, tenemos dos posibilidades, si $a_1 \equiv b_1 \pmod 4$, entonces $A_1 + B \equiv 2 + 0\sqrt{p} \pmod 4$ y $A_1 - B \equiv 0 + 0\sqrt{p} \pmod 4$. Por otra parte, si $a_1 \not\equiv b_1 \pmod 4$, entonces $A_1 + B \equiv 0 + 0\sqrt{p} \pmod 4$ y $A_1 - B \equiv 2 + 0\sqrt{p} \pmod 4$. Así que $L_2^2 \mid\mid A_1 \pm B$ y $L_2^4 \mid A_1 \mp B$ donde los signos son elegidos dependiendo de que a_1 y b_1 sean iguales o distintos módulo 4. Por lo tanto $\langle L_2\rangle_{\mathbb{F}}^2 \mid\mid \langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}}$, concluyendo la demostración de la afirmación 2.

Para la afirmación 3, observemos primero que $2\,A_1, 2\,B \in \langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}}$ y $A_1 + B, A_1 - B \in \langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}}$, así

$$2(\langle A_1\rangle_{\mathbb{F}} + \langle B\rangle) \subseteq \langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}} \subseteq \langle A_1\rangle_{\mathbb{F}} + \langle B\rangle\,.$$

Esto nos muestra que $\langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}} = L_2^r(\langle A_1\rangle_{\mathbb{F}} + \langle B\rangle)$ con $0 \le r \le 2$. En los casos 1 y 2, como $N_{\mathbb{F}/\mathbb{Q}}(B) \equiv 2 \pmod 4$, entonces $r > 0$. Además, a_1 y a_3 tienen la misma paridad, por lo que $N_{\mathbb{F}/\mathbb{Q}}(A_1)$ es par, así $\langle L_2\rangle_{\mathbb{F}} \mid\mid \langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}}$ y $r = 1$. En el caso 3, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = N_{\mathbb{F}/\mathbb{Q}}(B^2)$ es impar y por tanto $r = 2$.

Ahora vamos a demostrar la afirmación 4. Como $\mathfrak{p}_{\mathbb{F}}$ es inerte, entonces $\mathfrak{p}_{\mathbb{K}} = \langle \mathfrak{p}_{\mathbb{F}}\rangle_{\mathbb{K}}$ es un ideal primo en $\mathcal{O}_{\mathbb{K}}$. Supongamos que $\mathfrak{p}_{\mathbb{F}}^k \mid\mid \langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}}$ y $\mathfrak{p}_{\mathbb{K}}^t \mid\mid \langle\alpha\rangle_{\mathbb{K}}$. Como $B^2 = A_1^2 - \sqrt{p}\,A_2^2$, $\mathfrak{p}_{\mathbb{F}}^{2k} \mid B^2$ y $\mathfrak{p}_{\mathbb{F}}^{2k} \mid A_1^2$, entonces $\mathfrak{p}_{\mathbb{F}}^k \mid A_2$. Por lo anterior, $\mathfrak{p}_{\mathbb{K}}^k \mid \left\langle A_1 + \sqrt[4]{p}\,A_2\right\rangle_{\mathbb{K}} = \langle\alpha\rangle_{\mathbb{K}}$ y $k \le t$. Por otra parte, $\mathfrak{p}_{\mathbb{K}}^{2t} \mid\mid N_{\mathbb{K}/\mathbb{Q}}(\alpha) = A_1^2 - \sqrt{p}\,A_2^2 = B^2$ y $\mathfrak{p}_{\mathbb{K}}^t \mid\mid \langle B\rangle_{\mathbb{K}}$. Como el polinomio irreducible de α en $\mathbb{F}[x]$ es $f(x) = x^2 - 2\,A_1\,x + B^2$, entonces $\mathfrak{p}_{\mathbb{K}}^{2t} \mid \alpha^2 - 2\,A_1\,\alpha + B^2 = 0$. Lo anterior, $\mathfrak{p}_{\mathbb{K}}^{2t} \mid B^2$ y $\mathfrak{p}_{\mathbb{K}}^{2t} \mid \alpha^2$, implican $\mathfrak{p}_{\mathbb{K}}^{2t} \mid 2\,A_1\,\alpha$. Puesto que $\mathfrak{p}_{\mathbb{K}}^t \mid\mid \alpha$ y $\langle 2\rangle_{\mathbb{K}} + \mathfrak{p}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}$, entonces $\mathfrak{p}_{\mathbb{K}}^t \mid \langle A_1\rangle_{\mathbb{K}}$. Como $\mathfrak{p}_{\mathbb{K}} = \langle \mathfrak{p}_{\mathbb{F}}\rangle_{\mathbb{K}}$, entonces $t \le k$ y así $t = k$. De la igualdad $\langle\alpha\rangle_{\mathbb{K}} = {\mathfrak{J}_{\mathbb{K}}}^2$, tenemos que t debe ser par y por lo tanto k es par.

Para demostrar la afirmación 5, si $\mathfrak{p}_{\mathbb{F}}$ se descompone, entonces $\langle \mathfrak{p}_{\mathbb{F}}\rangle_{\mathbb{K}} = \mathfrak{q}_1\mathfrak{q}_2$, con $\mathfrak{q}_1, \mathfrak{q}_2$ ideales primos de $\mathcal{O}_{\mathbb{K}}$. Supongamos que $\mathfrak{q}_1^{2t} \mid\mid \langle\alpha\rangle_{\mathbb{K}}$ y $\mathfrak{q}_2^{2r} \mid\mid \langle\alpha\rangle_{\mathbb{K}}$. Entonces $\langle\alpha\rangle_{\mathbb{K}} = \mathfrak{q}_1^{2t}\mathfrak{q}_2^{2r}\mathfrak{J}_{\mathbb{K}}$ para algún $\mathfrak{J}_{\mathbb{K}}$ tal que $\langle \mathfrak{p}_{\mathbb{F}}\rangle_{\mathbb{K}} + \mathfrak{J}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}$. Como $N_{\mathbb{K}/\mathbb{F}}(\mathfrak{q}_1) = N_{\mathbb{K}/\mathbb{F}}(\mathfrak{q}_2) = \mathfrak{p}_{\mathbb{F}}$, entonces

$$N_{\mathbb{K}/\mathbb{F}}(\langle\alpha\rangle_{\mathbb{K}}) = \mathfrak{p}_{\mathbb{F}}^{2(t+r)} N_{\mathbb{K}/\mathbb{F}}(\mathfrak{J}_{\mathbb{K}}) = \left\langle B^2\right\rangle_{\mathbb{F}},$$

por lo que $\mathfrak{p}_{\mathbb{F}}^{2(t+r)} \mid\mid B^2$. Sin pérdida de generalidad, supongamos $r > t$. Entonces $r = t + s$ para algún $s \in \mathbb{N}$ y

$$\mathfrak{q}_1^{4t} \mid\mid \left\langle\alpha^2\right\rangle_{\mathbb{K}}, \quad \mathfrak{q}_1^{4t+2s} \mid\mid B^2, \quad \mathfrak{q}_2^{4t+4s} \mid\mid \alpha^2, \quad \mathfrak{q}_2^{4t+2s} \mid\mid B^2.$$

Usando esto en la igualdad $\alpha^2 - 2\,A_1\,\alpha + B^2 = 0$, tenemos que $\mathfrak{q}_1^{4t} \mid 2\,A_1\,\alpha$ y $\mathfrak{q}_2^{4t+2s} \mid 2\,A_1\,\alpha$. Como $\mathfrak{q}_1^{2t} \mid\mid \langle\alpha\rangle_{\mathbb{K}}$ y $\mathfrak{q}_2^{2t+2s} \mid\mid \langle\alpha\rangle_{\mathbb{K}}$, entonces $(\mathfrak{q}_1\mathfrak{q}_2)^{2t} = \langle \mathfrak{p}_{\mathbb{F}}\rangle_{\mathbb{K}}^{2t} \mid \langle A_1\rangle_{\mathbb{K}}$. Mostraremos que $\langle \mathfrak{p}_{\mathbb{F}}\rangle_{\mathbb{K}}^{2t} \mid\mid \langle A_1\rangle_{\mathbb{K}}$. Supongamos que $\mathfrak{q}_1^{2t+1} \mid \langle A_1\rangle_{\mathbb{K}}$. Como $\mathfrak{q}_1^{2t+1} \mid B$, entonces $\mathfrak{q}_1^{4t+2} \mid B^2 = A_1^2 - \sqrt{p}\,A_2^2$, lo que implica $\mathfrak{q}_1^{2t+1} \mid A_2$. De esto se sigue que $\mathfrak{q}_1^{2t+1} \mid \langle\alpha\rangle_{\mathbb{K}}$, lo cual no es posible. Por lo tanto $\mathfrak{q}_1^{2t} \mid\mid \langle A_1\rangle_{\mathbb{K}}$. Por otra parte, como $A_1 \in \mathcal{O}_{\mathbb{F}}$, entonces por cada $\mathfrak{q}_1$ que divide a A_1 debe existir un $\mathfrak{q}_2$ que divide a A_1, por lo que $\mathfrak{q}_2^{2t} \mid\mid \langle A_1\rangle_{\mathbb{K}}$,

de esta forma $\mathfrak{p}_{\mathbb{F}}^{2t} \mid\mid \langle A_1\rangle_{\mathbb{F}}$. Por otro lado, $\mathfrak{p}_{\mathbb{F}}^{2t+s} \mid\mid \langle B\rangle_{\mathbb{F}}$, así que $\mathfrak{p}_{\mathbb{F}}^{2t} \mid \langle B\rangle_{\mathbb{F}}$. Por lo tanto, $\mathfrak{p}_{\mathbb{F}}^{2t} \mid\mid \langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}}$, donde $k = 2t$ como se quería para la afirmación 5.

De acuerdo a las afirmaciones 4 y 5, los únicos ideales primos que pueden aparecer un número impar de veces en la factorización de $\langle A_1\rangle_{\mathbb{F}} + \langle B\rangle_{\mathbb{F}}$ son los ideales ramificados. En este caso, estos ideales son $\left\langle \sqrt{p}\right\rangle_{\mathbb{F}}$ y $\langle L_2\rangle_{\mathbb{F}}$. Usando la igualdad de la afirmación 3, podemos decir lo mismo sobre el ideal $\langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}}$. Por la afirmación 2, sabemos que $\langle L_2\rangle_{\mathbb{F}}^2 \mid\mid \langle A_1 + B\rangle_{\mathbb{F}} + \langle A_1 - B\rangle_{\mathbb{F}}$. Con esto queda demostrada la afirmación 6.

Finalmente, por 6,

$$\left\langle \frac{A_1 + B}{2\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}} + \left\langle \frac{A_1 - B}{2\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}} = \mathcal{O}_{\mathbb{F}}. \tag{31}$$

Si escribimos la ecuación (30) como una igualdad de ideales, entonces

$$\langle 4\,(A_1 + B)\,(A_1 - B)\rangle_{\mathbb{F}} = \left\langle 4\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2 \right\rangle_{\mathbb{F}}^2 \left\langle \frac{A_1 + B}{2\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}} \left\langle \frac{A_1 - B}{2\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}} = \langle C\rangle_{\mathbb{F}}^2 \langle\sqrt{p}\rangle_{\mathbb{F}},$$

que podemos reescribir como:

$$\left\langle \frac{A_1 + B}{2\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}} \left\langle \frac{A_1 - B}{2\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}} = \left\langle \frac{C}{4\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}}^2 \langle\sqrt{p}\rangle_{\mathbb{F}},$$

donde todos los ideales que aparecen en la igualdad anterior son enteros. Por (31), los ideales del lado izquierdo son primos relativos, así que uno de ellos debe de ser un cuadrado y el otro es un cuadrado por $\left\langle \sqrt{p}\right\rangle_{\mathbb{F}}$. Supongamos que:

$$\left\langle \frac{A_1 \pm B}{2\sqrt{p}^k \mathfrak{J}_{\mathbb{F}}{}^2} \right\rangle_{\mathbb{F}} = \mathfrak{J}_1^2, \qquad \langle 2\,A_1 \pm 2\,B\rangle_{\mathbb{F}} = \left\langle 2^2\sqrt{p}^k \right\rangle_{\mathbb{F}} \mathfrak{J}_{\mathbb{F}}{}^2 \mathfrak{J}_1^2.$$

De esta forma, si k es par, entonces $\langle 2\,A_1 \pm 2\,B\rangle_{\mathbb{F}} = \mathfrak{J}_2^2$, donde $\mathfrak{J}_2^2$ es el ideal del lado derecho de la igualdad y si k es impar, entonces, existe $\mathfrak{J}_2 \subseteq \mathcal{O}_{\mathbb{F}}$ tal que $\langle 2\,A_1 \mp 2\,B\rangle_{\mathbb{F}} = \mathfrak{J}_2^2$. En ambos casos, $\mathfrak{J}_2^2$ es un ideal principal y, como el número de clases de $\mathbb{Q}(\sqrt{p})$ es impar, entonces $\mathfrak{J}_2$ debe de ser principal, digamos $\mathfrak{J}_2 = \langle D\rangle_{\mathbb{F}}$. Si $A = 2\,A_1$, entonces $A \pm 2B = D^2\,U$ para alguna $U \in \mathcal{U}_{\mathbb{K}}$, donde podemos suponer que $U = \pm 1$ ó $U = \pm U_{\mathbb{F}}$. Si $U = 1$, por la Proposición 3.11, $\sqrt{\alpha} \in \mathcal{O}_{\mathbb{K}}$. Si $U = -1$, tenemos que $N_{\mathbb{K}/\mathbb{F}}(-\alpha) = B^2$ y $t_{\mathbb{K}/\mathbb{F}}(-\alpha) = -2\,A_1 = -A$, con $-A \mp 2\,B = D^2$, por lo que $\sqrt{-\alpha} \in \mathcal{O}_{\mathbb{K}}$. Si $U = \pm U_{\mathbb{F}}$, entonces $N_{\mathbb{K}/\mathbb{F}}(\alpha\,U_{\mathbb{F}}) = (B\,U_{\mathbb{F}})^2$ y $t_{\mathbb{K}/\mathbb{F}}(\alpha\,U_{\mathbb{F}}) = 2\,A_1\,U_{\mathbb{F}}$ y así $A_1\,U_{\mathbb{F}} + B\,U_{\mathbb{F}} = \pm(D\,U_{\mathbb{F}})^2$. Ahora procedemos como en los casos anteriores. Por lo tanto, existe $\mu \in \mathcal{U}_{\mathbb{K}}$ tal que $\sqrt{\alpha\,\mu} \in \mathcal{O}_{\mathbb{K}}$ y es un generador de $\mathfrak{I}_{\mathbb{K}}$. □

El resultado anterior nos pide $\alpha \notin \mathcal{O}_{\mathbb{F}}$. Si esta condición no se cumple, podemos multiplicar α por μ_1^2 donde $N_{\mathbb{K}/\mathbb{F}}(\mu_1) = 1$, de esta forma la norma se mantiene, $\mathbb{K}(\sqrt{\alpha}) = \mathbb{K}(\sqrt{\alpha\mu_1^2})$ y $\alpha\mu_1^2 \notin \mathcal{O}_{\mathbb{F}}$. Observemos que la condición $p \equiv 7 \pmod{16}$ es indispensable pues la descripción de $\mathcal{U}_{\mathbb{K}}$ depende de esta cualidad de p.

Corolario 3.47. *Sean* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo,* $\alpha = a_1 + a_2\sqrt[4]{p} + a_3\sqrt{p} + a_4\sqrt[4]{p^3} \in \mathcal{O}_{\mathbb{K}} - \mathcal{O}_{\mathbb{F}}$ *tal que* $\langle\alpha\rangle_{\mathbb{K}} = \mathfrak{I}_{\mathbb{K}}{}^2$, α *cumple las condiciones de los casos* 1, 2 *ó* 3 *descritos al principio de la sección y* $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$

con $\mathbb{L} \neq \mathbb{K}$. *Entonces,* $\mathbb{L}/\mathbb{K}$ *es una extensión ramificada ó* $\mathbb{L} = \mathbb{K}(\sqrt{\mu})$ *para alguna* $\mu \in \mathcal{U}_{\mathbb{K}}$. □

Finalmente, usando todo lo que hemos hecho en este capítulo tenemos:

Teorema 3.48. *Sean* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{p})$, $\mathbb{F} = \mathbb{Q}(\sqrt{p})$ *con* $p \equiv 7 \pmod{16}$ *un primo racional positivo y* $Cl_2 \subseteq Cl_{\mathbb{K}}$ *el* 2*-grupo de clases de ideales de* $\mathbb{K}$. *Entonces* $Cl_2 \cong \mathbb{Z}/2\mathbb{Z}$.

DEMOSTRACIÓN. Sea $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ para $\alpha \in \mathbb{K}$ libre de cuadrados en todas sus factorizaciones. Si α no es una unidad, hemos demostrado que 2 se ramifica totalmente en $\mathbb{L}$ para cualquier α salvo en los casos 1, 2 y 3, en donde siempre se ramifica algún otro ideal. En el caso α unidad, todas las extensiones $\mathbb{L}/\mathbb{K}$ son ramificadas salvo $\mathbb{K}(\sqrt{U_{\mathbb{F}}})$. Esta última es la única extensión cuadrática de $\mathbb{K}$ no ramificada, por lo que el 2-rango de $Cl_{\mathbb{K}}$ es 1.

Ahora vamos a demostrar que el orden del grupo es 2. Sea $\mathfrak{p}_2$ el único ideal de $\mathcal{O}_{\mathbb{K}}$ con $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_2) = 2$. Sabemos que $\mathfrak{p}_2$ no es principal pero $\mathfrak{p}_2^2 = \langle L_2 \rangle_{\mathbb{K}}$, así que $\overline{\mathfrak{p}_2}$ es la única clase de orden 2 de Cl_2. Supongamos que existe $\mathfrak{I}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$ tal que $\overline{\mathfrak{I}_{\mathbb{K}}}^2 = \overline{\mathfrak{p}_2}$. Puesto que $\overline{\mathfrak{p}_2}$ es su propio inverso, tenemos $\overline{\mathfrak{I}_{\mathbb{K}}}^2 \overline{\mathfrak{p}_2} = \overline{\mathcal{O}_{\mathbb{F}}}$, por lo que $\mathfrak{I}_{\mathbb{K}}^2 \mathfrak{p}_2$ es un ideal principal. Podemos suponer que $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}})$ es impar, pues, si fuera par, $\mathfrak{p}_2 \mid \mathfrak{I}_{\mathbb{K}}$, es decir, $\mathfrak{I}_{\mathbb{K}} = \mathfrak{p}_2 \mathfrak{J}_{\mathbb{K}}$. Entonces, $\mathfrak{I}_{\mathbb{K}}^2 \mathfrak{p}_2 = \mathfrak{p}_2^2 \mathfrak{J}_{\mathbb{K}}^2 \mathfrak{p}_2 = \langle L_2 \rangle_{\mathbb{K}} \mathfrak{J}_{\mathbb{K}}^2 \mathfrak{p}_2$, por lo que $\mathfrak{J}_{\mathbb{K}}^2 \mathfrak{p}_2$ está relacionado con $\mathfrak{I}_{\mathbb{K}}^2 \mathfrak{p}_2$ y $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{J}_{\mathbb{K}}) = \dfrac{N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}})}{2}$. Si $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}})$ es impar, entonces $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{\mathbb{K}})^2 \equiv 1, 9 \pmod{16}$, por lo que $N_{\mathbb{K}/\mathbb{Q}}\left(\mathfrak{I}_{\mathbb{K}}{}^2 \mathfrak{p}_2\right) \equiv 2 \pmod{16}$. Por esto, debe existir un elemento en $\mathcal{O}_{\mathbb{K}}$ con norma ± 2, lo que ya vimos que no es posible en la demostración de la Proposición 3.9. Entonces no existe $\mathfrak{I}_{\mathbb{K}}$ tal que $\overline{\mathfrak{I}_{\mathbb{K}}}^2 = \overline{\mathfrak{p}_2}$ y por lo tanto $Cl_2 \cong \mathbb{Z}/2\mathbb{Z}$. □

Ejemplo 3.49. *Sea* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{7})$ *y* $\mathbb{F} = \mathbb{Q}(\sqrt{7})$. *Podemos aplicar el Teorema 3.48, que nos afirma que* $Cl_2 \subseteq Cl_{\mathbb{K}}$ *tiene orden* 2. *De hecho, en este caso* $Cl_{\mathbb{K}} \cong \mathbb{Z}/2\mathbb{Z}$.

En la siguiente tabla damos los primeros primos racionales positivos $p \equiv 7 \pmod{16}$ y el valor correspondiente de $h_{\mathbb{K}}$.

p	$h_{\mathbb{K}}$	p	$h_{\mathbb{K}}$	p	$h_{\mathbb{K}}$	p	$h_{\mathbb{K}}$
7	2	503	2	1063	2	1831	6
23	2	599	2	1223	42	1847	6
71	2	631	2	1303	6	1879	6
103	2	647	2	1319	2	2039	2
151	2	727	330	1367	6	2087	2
167	2	743	2	1399	2	2311	2
199	2	823	2	1447	2	2423	6
263	2	839	18	1511	2	2503	2
311	2	919	2	1543	154	2551	2
359	6	967	2	1559	2	2647	2
439	50	983	2	1607	6	2663	2
487	2	1031	2	1783	2	2711	6

Conclusiones y expectativas

A lo largo de este trabajo hemos presentado algunos resultados relacionados con el 2-grupo de clases de algunas extensiones de grado 2 ó 4. En el segundo capítulo encontramos un método para construir el Cl_2 para cualquier campo cuadrático así como algunas propiedades que se pueden utilizar suponiendo que conocemos Cl_2. Una pregunta natural es si podemos realizar algo similar para algún primo distinto de 2. Los ejemplos que hemos realizado parecen indicar que un estudio similar para el resto de los primos no es posible, al menos no lo es si usamos el símbolo de Legendre. Sin embargo, resulta interesante buscar alguna herramienta alternativa que pueda servir de alguna forma similar para estudiar el resto de los p-grupos.

La intención que teníamos cuando comenzamos a estudiar los temas del tercer capítulo era encontrar resultados similares a los que estudiamos en los campos cuadráticos pero en otras extensiones. Un resultado que fue importante en el estudio de los campos cuadráticos fue el Teorema de Gauss del 2-rango del grupo de clases de ideales (Teorema 2.4). En [**20**], los autores encuentran una fórmula para encontrar el 2-rango del grupo de clases de ideales de una extensión bicíclica bicuadrática imaginaria, es decir, una de la forma $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. En [**24**], se afirma que existe una infinidad de campos puros $\mathbb{Q}(\sqrt[n]{d})$ en los que el 2-grupo de clases tiene ciertas cualidades. Sin embargo, no conocemos en la literatura un resultado que dé explícitamente el 2-rango del grupo de clases de ideales de $\mathbb{Q}(\sqrt[4]{d})$. En el tercer capítulo estudiamos un resultado parcial de esto, por lo que uno de nuestros objetivos a mediano plazo es terminar esta clasificación y utilizar este resultado para poder llevar, lo más que sea posible, los resultados del segundo capítulo a extensiones de grado 4.

En el Capítulo 3 nos concentramos en el caso $p \equiv 7 \pmod{16}$ debido a que nuestro principal objetivo era el Teorema 3.48. Sin embargo, resultará interesante resolver los mismos problemas para el resto de los casos. Por ejemplo, un problema particularmente importante es dar condiciones necesarias y suficientes para que en $\mathcal{O}_{\mathbb{K}}$ exista una unidad μ_2 tal que $N_{\mathbb{K}/\mathbb{Q}}(\mu_2) = \pm U_{\mathbb{F}}$, donde $U_{\mathbb{F}}$ es la unidad fundamental de $\mathbb{Q}(\sqrt{d})$. En algunas ocasiones, para demostrar que 2 no se ramifica, fue necesario encontrar una base $\mathcal{B}$ tal que $\Delta(\mathcal{B}) = 2^{16}p^6$. Lo que en realidad encontramos fue una 2-base entera (ver [**3**]). Hallar las 2-bases enteras o, en general, las bases enteras del resto de las extensiones $\mathbb{L} = \mathbb{K}(\sqrt{\alpha})$ es otro de los problemas que queda por resolver y que, como vimos en el trabajo, está relacionado con el estudio de la ramificación de los ideales primos de $\mathbb{K}$.

La razón por la que decidimos continuar con los campos cuárticos fue por su similitud con las extensiones cuadráticas. Una posible línea de investigación es estudiar el p-grupo de clases de ideales en extensiones de grado p. Hay trabajos realizados al respecto, por ejemplo, en [**11**], [**12**], [**13**], [**14**], [**15**] y [**16**], F. Gerth estudia el 3-grupo de clases de ideales en extensiones cúbicas. Wittman estudia el p-grupo de algunas extensiones de grado

p en [**32**]. Estudiar el p-grupo de clases de ideales en una extensión con grado primo relativo a p es más complicado, pero también ha sido estudiado, por ejemplo en [**23**] y [**33**].

Índice alfabético

Bibliografía

[1] Aguilar-Zavoznik A., Pineda-Ruelas M., 2-class group of quadratic fields, *JP J. Algebra Number Theory Appl.*, **22**, no. 2, 155-174, (2011).

[2] Aguilar-Zavoznik A., Pineda-Ruelas M., A relation between ideals, Diophantine equations and factorization in quadratic fields $\mathbb{F}$ with $h_{\mathbb{F}} = 2$, *International Journal of Algebra*, **6**, no. 15, 729-745, (2012).

[3] Alaca,S., p-integral bases of algebraic number fields, *Util. Math.*, **56**, pp. 97-106, (1999).

[4] Alaca,S., Williams, K. S., *Introductory Algebraic Number Theory*, Cambridge University Press, 2004.

[5] Basilla J. M., Wada H., On efficient computation of the 2-parts of ideal class groups of quadratic fields. *Proc. Japan Acad. Ser. A Math. Sci.*, **80**, no. 10, 191-193, (2004).

[6] Bosma W., Stevenhagen P., On the Computation of Quadratic 2-class groups. *J. de Théorie des Nombres de Bordeaux*, **8**, no. 2, 283-313, (1996).

[7] Childress N., *Class Field Theory*, Springer-Verlag, UTX, (2009).

[8] Cohen H., Roblot X. F., Computing the Hilbert class field of real quadratic fields, *Math. Comp.*, **69**, no. 231, 1229-1244, (1999).

[9] Daberkow M., Fieker C., Klüners J., Pohst M., Roegner K., Wildanger K., KANT V4, *J. Symbolic Comp.*, **24**, 267-283, (1997).

[10] Funakura T, On integral bases of pure quartic fields, *Math. J. Okayama Univ.*, vol. **26**, issue 1, 27-41, (1984).

[11] Gerth, F., On 3-class groups of pure cubic fields, *J. Reine Angew. Math.*, **278/279**, 52-62, (1976).

[12] Gerth, F., On 3-class groups of cyclic cubic extensions of certain number fields, *J. Number Theory*, **8**, no. 1, 84-98, (1976).

[13] Gerth, F., Ranks of 3-class groups of non-Galois cubic fields, *Acta Arith.*, **30**, no. 4, 307-322, (1976).

[14] Gerth, F., Densities for 33-class ranks of pure cubic fields, *Acta Arith.*, **46**, no. 3, 227-242, (1986).

[15] Gerth, F., Densities for 33-class ranks in certain cubic extensions, *J. Reine Angew. Math.*, **381**, 161-180, (1987).

[16] Gerth, F., On 3-class groups of certain pure cubic fields, *Bull. Austral. Math. Soc.*, **72**, no. 3, 471-476, (2005).

[17] Hasse H., An algorithm for determining the structure of the 2-Sylow-subgroups of the divisor class group of a quadratic number field. *Symposia Mathematica*, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973). Academic Press, 341-352, (1975).

[18] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, GTM **84**, 2a edición, (1990).

[19] Januz G. J., *Algebraic Number Fields*, 2nd edition, American Mathematical Society, GSM **7**, (1996).

[20] McCall T. M., Parry, C. J., Ranalli, R. R., The 2-rank of the class group of imaginary bicyclic biquadratic fields, *Canad. J. Math.*, **49**, 283-300, (1997).

[21] Mollin R., *Algebraic Number Theory*, CRC Press, (1999).

[22] Murty M. R., Esmonde J., *Problems in algebraic number theory*, Springer-Verlag, Second edition. GTM, **190**, (2005).

[23] Nakahara, T., The structure of 3-class groups in the real quadratic fields $\mathbb{Q}(\sqrt{D}$ for D less than $1\,200\,000$ and for a few values of D between $2\,000\,000$ and $4\,033\,723$, *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, **23**, no. 1-2, 9-90, (1995).

[24] Nakano, S., On the 2-rank of the ideal class groups of pure number fields, *Arch. Math. (Basel)*, **42**, no. 1, 53-57, (1984).

[25] Narkiewicz W., *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, 3rd edition, SMM, (2004).
[26] Ribenboim P., *Clasical theory of algebraic numbers*, Springer-Velag, UTX, (2001).
[27] Roberson Ashford S., Dyadic ramification and quartic number fields, *J. Number Theory*, **45**, no. 1, 68-91, (1993).
[28] Shanks D., Gauss's ternary form reduction and the 2-Sylow subgroup. *Math. Comp.*, **25**, 837-853, (1971).
[29] Stark H., On complex quadratic fields with class-number two (Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday), *Math. Comp.*, **29**, 289-302, (1975).
[30] Stein W. A., et al, *Sage Mathematics Software (Version 4.6.1)*, The Sage Development Team, http://www.sagemath.org (2010).
[31] Stewart I., Tall D., *Algebraic Number Theory and Fermat's Last Theorem*, A K Peters, 3rd edition, (2001).
[32] Wittmann, C., p-class groups of certain extensions of degree p, *Math. Comp.*, **74**, no. 250, 937-947, (2005).
[33] Yoshida, E., On the 3-class field tower of some biquadratic fields, *Acta Arith.*, **107**, no. 4, 327-336, (2003).