UNIVERSIDAD AUTÓNOMA METROPOLITANA
Iztapalapa

FRACCIONES CONTINUAS Y DIVISORES DEL NÚMERO DE CLASES EN CAMPOS CUADRÁTICOS REALES

Presenta
JANETH ANABELLE MAGAÑA ZAPATA

Asesor
Dr. MARIO PINEDA RUELAS

TESIS
PARA OBTENER EL GRADO DE MAESTRA EN CIENCIAS MATEMÁTICAS

DEPARTAMENTO DE MATEMÁTICAS

Agradecimientos

A mis papás Juan y Nena, por su cariño, comprensión y su apoyo incondicional. A mis hermanos: Juan, Rigel y Gisseth por ser la motivación para seguir adelante.

Agradezco de manera especial al Dr. Mario Pineda Ruelas por aceptarme para realizar esta tesis bajo su dirección, por su paciencia, por sus consejos y su apoyo durante mis estudios de maestría y por haberme dedicado tiempo para elaborar este trabajo.

A mis sinodales: Dra. Martha Rzedowski Calderón, Dr. Arturo Cueto Hernández y Dr. Carlos Signoret Poillon, por sus comentarios y observaciones, las cuales enriquecieron este manuscrito.

A mi amigo Alejandro por sus sugerencias y opiniones que me ayudaron bastante para elaborar este trabajo, a mi amigo Henry por su ayuda con el longtable.

Sin tí mi vida en el D.F hubiera sido muy triste: Gracias Juan Carlos.

A Luis por escucharme, por sus consejos y sobre todo por su amor.

A todos mis amigos, gracias por darme ánimos, por estar conmigo en los momentos de alegría y tristeza. Agradezco de manera especial a mis amigos que conocí en la Ciudad de México, por brindarme su amistad y compañía, por hacerme sentir feliz aún no estando en mi tierra.

A todos mis profesores y en especial a los de la UAM-I, por ser parte de mi formación académica.

A las secretarias del departamento de Matemáticas de la UAM-I y a la maestra Iseo quienes siempre me trataron con amabilidad.

A mis tios Mario y Lilí (E. P. D.) y a mis primas, por estar siempre cerca de mis papás y por esa alegría que nos dan cada vez que están en casa.

Al Consejo Nacional de Ciencia y Tecnología.

Índice general

Introducción

En el artículo 304 de las célebres Disquisiciones Aritméticas [**4**], Gauss afirmaba:

Es curioso y sería digno de un geómetra, investigar la ley que justifique el hecho de que los determinantes con una clase por cada género se hacen menos frecuentes. Hasta el momento no podemos asegurar teóricamente ni conjeturar por observación si hay un número finito de ellos (esto es poco probable) o si se hacen infinitamente raros o que su frecuencia tiende a un límite fijo.

En el lenguaje de la teoría de números, la afirmación de Gauss queda traducida como:

Existe una infinidad de campos cuadráticos reales cuyo anillo de enteros es de ideales principales.

Esta afirmación se conoce actualmente con el nombre de *Conjetura de Gauss* y sólo se tienen algunos resultados parciales. Por ejemplo, Biró [**1**] [**2**] determinó todos los campos cuadráticos reales de la forma $\mathbb{Q}(\sqrt{n^2+1})$ y $\mathbb{Q}(\sqrt{n^2+4})$ con número de clases 1. También, Byeon, Kim y Lee [**3**] determinaron todos los campos cuadráticos reales de la forma $\mathbb{Q}(\sqrt{n^2-4})$ con número de clases 1, sólo por mencionar algunos de ellos.

En contraparte a la conjetura de Gauss, el objetivo de este trabajo consiste en estudiar la ecuación diofantina

$$d = \sigma^2 a^m + b^2$$

por medio de la teoría de los números algebraicos y la teoría elemental de las fracciones continuas. Mostraremos algunos criterios de divisibilidad del número de clases del campo cuadrático real $\mathbb{Q}(\sqrt{\sigma^2 a^m + b^2})$, bajo ciertas suposiciones sobre el entero d.

En el Capítulo 1 damos una introducción a la teoría de los números algebraicos. Uno de los resultados más importantes en este capítulo es la finitud del número de clases h_F de un campo de números F. Estudiando el número de clases h_F veremos cuándo el anillo de enteros A_F es un dominio de factorización única. Por último daremos la caracterización de los campos cuadráticos reales y de sus anillos de enteros.

El Capítulo 2 contiene los conceptos básicos acerca de las fracciones continuas simples. Estudiaremos los irracionales cuadráticos y su representación en fracciones continuas, algunas propiedades aritméticas de los convergentes, que es básicamente lo que nos servirá en el Capítulo 3.

El Capítulo 3 es el objetivo de este trabajo. Aquí estudiaremos los ideales de un anillo cuadrático A_F, veremos que en la clase de un ideal de A_F siempre hay al menos un ideal primitivo y uno reducido. Involucraremos las fracciones continuas con el generador irracional de un ideal primitivo I, con base en esto probaremos el teorema principal de este capítulo y de este trabajo, el cual describe todos los ideales reducidos equivalentes a un ideal dado I. Un corolario de dicho teorema relaciona la longitud del período de la fracción continua del generador irracional de I con un ciclo de ideales reducidos equivalentes a I.

Como aplicación de lo anterior probaremos un teorema que nos da un criterio de divisibilidad para el número de clases de un campo cuadrático real. Finalmente, utilizaremos este resultado para hallar una familia infinita de anillos cuadráticos asociados a un campo cuadrático real con número de clases par.

En la literatura no encontramos una lista de campos cuadráticos reales con número de clases par con las condiciones del Ejemplo 3.3.30 del Capítulo 3. La aproximación más cercana es la que aparece en [**11**], página 274.

Capítulo 1

Preliminares

Este capítulo contiene la teoría esencial para conocer los campos de números y sus anillos de enteros. El objetivo principal es estudiar el número de clases de un campo de números F e involucrar este concepto para saber cuándo el anillo de enteros de F es un dominio de factorización única (DFU). Por último aplicaremos esta teoría a los anillos cuadráticos.

En este capítulo siempre hablaremos de una extensión finita de campos L/K. L se puede ver como un espacio vectorial sobre K. A la dimensión de L como espacio vectorial sobre K se le llama el grado de L sobre K y lo denotaremos por $[L : K]$. La idea de la teoría de Galois es asociarle a cada extensión finita, normal y separable de campos L/K el grupo $\mathrm{Aut}(L/K)$ para obtener información de la estructura de la extensión. $\mathrm{Aut}(L/K)$ es el grupo, bajo composición, de isomorfismos $\sigma : L \to L$ tales que $\sigma(k) = k$ para toda $k \in K$, a estos isomorfismos los llamaremos K-automorfismos de L. Si L/K es una extensión finita, normal y separable, le llamaremos una **extensión de Galois** y el grupo $\mathrm{Aut}(L/K)$ se llama **el grupo de Galois de** L **sobre** K, denotado por $\mathrm{Gal}(L/K)$. Cuando L/K es una extensión de Galois, se tiene que K es el campo fijo de $\mathrm{Gal}(L/K)$, es decir, $K = L^{\mathrm{Gal}(L/K)}$ y en este caso $|\mathrm{Gal}(L/K)| = [L : K]$.

1.1. Norma, Traza y Discriminante

Esta sección será un breve resumen de lo que necesitamos saber en este trabajo sobre la norma, la traza y el discriminante. Lo referente a esta sección se puede consultar en [**6**].

Consideremos una extensión finita de campos L/K, de dimensión $[L : K] = n$. Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base de L/K y $\alpha \in L$. Entonces $\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, con $a_{ij} \in K$.

Definición 1.1.1. *La **norma** de α se define como $N_{L/K}(\alpha) = \det(a_{ij})$ y la **traza** de α se define como $tr_{L/K}(\alpha) = \sum_{i=1}^{n} a_{ii}$.*

Cuando esté clara la extensión en la cual estamos trabajando, denotaremos la norma y la traza como $N(\alpha) = \det(a_{ij})$ y $tr(\alpha) = \sum_{i=1}^{n} a_{ij}$.

Proposición 1.1.2. *La norma y la traza no dependen de la elección de la base.*

□

A continuación daremos algunas propiedades de la norma y la traza.

Proposición 1.1.3. *Sean $\alpha, \beta \in L$ y $a \in K$. Entonces:*

1. $N(\alpha\beta) = N(\alpha)N(\beta)$,
2. $N(a\beta) = a^n N(\beta)$,
3. $N(1) = 1$,
4. *si* $\alpha \neq 0$, $N(\alpha^{-1}) = N(\alpha)^{-1}$,
5. $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$,
6. $tr(a\alpha) = at(\alpha)$.

□

Proposición 1.1.4. *Si L/K es una extensión de Galois, entonces*

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

donde $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$ *y* $\alpha^{(i)} = \sigma_i(\alpha)$.

□

Definición 1.1.5. *Sean $\alpha_1, \ldots, \alpha_n \in L$. Definimos el* ***discriminante*** *de $\alpha_1, \ldots, \alpha_n$ como $\Delta(\alpha_1, \ldots, \alpha_n) = \det(tr(\alpha_i\alpha_j))$.*

Proposición 1.1.6. *Si $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base de L/K. Si L/K es una extensión separable y $\{\alpha_1, \ldots, \alpha_n\}$ es una base de L/K, entonces $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.*

DEMOSTRACIÓN. Ver [**6**] página 173, Proposición 12.1.1. □

Proposición 1.1.7. *Sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ dos bases de L/K. Si $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, con $a_{ij} \in K$, entonces $\Delta(\alpha_1, \ldots, \alpha_n) = (\det(a_{ij}))^2 \Delta(\beta_1, \ldots, \beta_n)$.*

DEMOSTRACIÓN. Escribimos $\alpha_i\alpha_k = \sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{kl}\beta_j\beta_l$. Tomando la traza en ambos lados se tiene que

$$tr(\alpha_i\alpha_k) = \sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{kl}tr(\beta_j\beta_l).$$

Sean $A = (tr(\alpha_i\alpha_k))$, $B = (tr(\beta_j\beta_l))$ y $C = (a_{ij})$. Entonces $A = CBC^T$. □

1.2. Campos de Números y Anillos de Enteros

El tema principal de esta sección son los anillos de enteros y sus propiedades.

Definición 1.2.1. *Un **número álgebraico** es un número complejo que es raíz de algún polinomio distinto de cero en $\mathbb{Q}[x]$. Un **entero álgebraico** es un número complejo que es raíz de algún polinomio mónico en $\mathbb{Z}[x]$.*

Proposición 1.2.2. *El conjunto de los números algebraicos forman un campo.*

DEMOSTRACIÓN. Ver [**6**] página 67, Proposición 6.1.3. □

Proposición 1.2.3. *El conjunto de los enteros algebraicos forman un anillo.*

DEMOSTRACIÓN. Ver [**6**] página 68, Proposición 6.1.5. □

Denotaremos al anillo de enteros algebraicos como Ω.

Definición 1.2.4. *Un subcampo F de los números complejos, se llama **campo de números** si $[F : \mathbb{Q}]$ es finito. Sea $A_F = F \cap \Omega$. Llamaremos a A_F el anillo de enteros algebraicos de F.*

Observación 1. *Ya que $[F : \mathbb{Q}]$ es finito tenemos que $F/\mathbb{Q}$ es una extensión algebraica, por lo tanto F consta únicamente de números algebraicos.*

A lo largo de esta sección trabajaremos con la extensión $F/\mathbb{Q}$ y vamos a suponer que $[F : \mathbb{Q}] = n$.

Lema 1.2.5. *Supongamos que $\beta \in F$. Entonces existe $b \in \mathbb{Z}, b \neq 0$, tal que $b\beta \in A_F$.*

DEMOSTRACIÓN. Como $\beta \in F$, tenemos que β satisface una ecuación

$$a_0 + a_1\beta + \cdots + a_n\beta^n = 0 \quad a_i \in \mathbb{Z}, a_n \neq 0.$$

Multiplicando ambos lados de la ecuación anterior por a_n^{n-1}, se tiene que

$$a_0 a_n^{n-1} + a_n^{n-1}a_1\beta + a_n^{n-1}a_2\beta^2 + \cdots + a_n^{n-1}a_n\beta^n = 0,$$

entonces

$$a_0 a_n^{n-1} + a_n^{n-2}a_1(a_n\beta) + a_n^{n-3}a_2(a_n\beta)^2 + \cdots + (a_n\beta)^n = 0.$$

De donde

$$f(x) = a_0 a_n^{n-1} + a_n^{n-2}a_1 x + a_n^{n-3}a_2 x^2 + \cdots + x^n$$

es un polinomio mónico con coeficientes en $\mathbb{Z}$ y $a_n\beta$ es raíz de $f(x)$. Por lo tanto $a_n\beta \in A_F$. □

Proposición 1.2.6. *Cada ideal $I \neq 0$ de A_F contiene una base para F sobre $\mathbb{Q}$.*

DEMOSTRACIÓN. Si $\{\beta_1, \ldots, \beta_n\}$ es una base de F sobre $\mathbb{Q}$, entonces por el Lema 1.2.5 existen $b_i \in \mathbb{Z}, b_i \neq 0$ tal que $b_1\beta_1, \ldots, b_n\beta_n \in A_F$. Sea $\alpha \in I, \alpha \neq 0$. Como I es ideal de A_F, se tiene que $b_1\beta_1\alpha, \ldots, b_n\beta_n\alpha \in I$. Es claro que $\{b_i\beta_i\alpha\}_{i=1}^n$ es una base de F sobre $\mathbb{Q}$ contenida en I.

□

Veamos ahora qué sucede con la norma y traza de un elemento en A_F.

Lema 1.2.7. *Un número racional $r \in \mathbb{Q}$ es un entero algebraico si y sólo si $r \in \mathbb{Z}$.*

DEMOSTRACIÓN. Si $r \in \mathbb{Z}$, entonces r satisface el polinomio mónico con coeficientes enteros $x - r$. Por lo tanto r es un entero algebraico.

Supongamos ahora que $r \in \mathbb{Q}$ y es un entero algebraico. Entonces r satisface un polinomio mónico en $\mathbb{Z}[x]$, digamos

$$p(x) = b_0 + b_1x + \cdots + x^n,$$

con $b_i \in \mathbb{Z}$. Sea $r = \dfrac{c}{d}$ con $c, d \in \mathbb{Z}$ y $mcd(c, d) = 1$. Luego,

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

Multiplicando la ecuación anterior por d^n, se tiene que

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

De donde $d|c^n$. Puesto que $mcd(d, c) = 1$, se tiene $mcd(d, c^n) = 1$, por lo que $d|1$. De ahí, $d = \pm 1$ y se concluye que $r \in \mathbb{Z}$. □

Proposición 1.2.8. *Sea $\alpha \in A_F$. Entonces $N(\alpha), tr(\alpha) \in \mathbb{Z}$.*

DEMOSTRACIÓN. Como $\alpha \in A_F$ satisface un polinomio mónico en $\mathbb{Z}[x]$, tenemos

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

con $a_i \in \mathbb{Z}$. Sea $\sigma \in \mathrm{Aut}(F/\mathbb{Q})$. Entonces

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

De ahí se obtiene que $\sigma(\alpha)$ satisface un polinomio mónico con coeficientes en $\mathbb{Z}$, es decir, $\sigma(\alpha) \in A_F$. Ahora como

$$N(\alpha) = \prod_{\sigma \in \mathrm{Aut}(F/\mathbb{Q})} \sigma(\alpha) \text{ y } tr(\alpha) = \sum_{\sigma \in \mathrm{Aut}(F/\mathbb{Q})} \sigma(\alpha), \tag{1}$$

y ya que A_F es un anillo, se tiene $N(\alpha), tr(\alpha) \in A_F$. Ahora veamos que la norma y traza son funciones de F en $\mathbb{Q}$. Sea $\rho \in \mathrm{Aut}(F/\mathbb{Q})$. Entonces por (1) se tiene que

$$\rho(N(\alpha)) = \prod_{\sigma \in \mathrm{Aut}(F/\mathbb{Q})} \rho\sigma(\alpha) = \prod_{\tau \in \mathrm{Aut}(F/\mathbb{Q})} \tau(\alpha) = N(\alpha).$$

Es decir, cualquier automorfismo $\rho \in \mathrm{Aut}(F/\mathbb{Q})$ fija a la norma. Entonces ésta debe estar en $\mathbb{Q}$. Con un argumento análogo al anterior, se concluye que la función traza va de F a $\mathbb{Q}$. Luego por el Lema 1.2.7 se tiene que $N(\alpha), tr(\alpha) \in \mathbb{Z}$. □

Corolario 1.2.9. *Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de F sobre $\mathbb{Q}$ tal que $\alpha_i \in A_F$ para $1 \leq i \leq n$. Entonces $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.*

DEMOSTRACIÓN. Se tiene que $\Delta(\alpha_1, \ldots, \alpha_n) = \det(tr(\alpha_i\alpha_j))$. Luego por la Proposición 1.2.8 se tiene que $tr(\alpha_i\alpha_j) \in \mathbb{Z}$. Entonces $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. □

Proposición 1.2.10. *Sean I un ideal en A_F y $\{\alpha_1, \ldots, \alpha_n\} \subseteq I$ una base de $F/\mathbb{Q}$ tal que $|\Delta(\alpha_1, \ldots, \alpha_n)|$ es mínimo. Entonces $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$.*

DEMOSTRACIÓN. Como $\alpha_i \in A_F$ se tiene $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, por lo que existe tal base con $|\Delta(\alpha_1, \ldots, \alpha_n)|$ mínimo. Si $\alpha \in I$, entonces $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n$ con $\gamma_i \in \mathbb{Q}$ para $1 \leq i \leq n$. Probaremos que $\gamma_i \in \mathbb{Z}$. Supongamos que $\gamma_i \notin \mathbb{Z}$ para algún i. Sin pérdida de generalidad podemos suponer que $\gamma_1 \notin \mathbb{Z}$. Por lo tanto $\gamma_1 \in \mathbb{Q}\backslash\mathbb{Z}$ y así $\gamma_1 = m + \theta$ donde $m \in \mathbb{Z}$ y $0 < \theta < 1$.

Sean $\beta_1 = \alpha - m\alpha_1,\ \beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n$. Como $m \in A_F$ e I es un ideal de A_F, tenemos $m\alpha_1 \in I$ y por tanto $\alpha - m\alpha_1 \in I$, así que $\{\beta_1, \ldots, \beta_n\} \subseteq I$. Probemos que $\{\beta_i\}_{i=1}^n$ es una base para $F/\mathbb{Q}$. Supongamos que $q_1\beta_1 + \cdots + q_n\beta_n = 0$ con $q_i \in \mathbb{Q}$ para $1 \leq i \leq n$. Se tiene que

$$\begin{aligned} 0 &= q_1(\alpha - m\alpha_1) + q_2\alpha_2 + \cdots + q_n\alpha_n \\ 0 &= q_1(\gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n) - q_1m\alpha_1 + q_2\alpha_2 + \cdots + q_n\alpha_n \\ 0 &= (q_1\gamma_1 - q_1m)\alpha_1 + (q_1\gamma_2 + q_2)\alpha_2 + \cdots + (q_1\gamma_n + q_n)\alpha_n. \end{aligned}$$

Pero como $\{\alpha_i\}_{i=1}^n$ es base para $F/\mathbb{Q}$, entonces $q_1\gamma_1 - q_1m = 0$ y $q_1\gamma_j + q_j = 0$ para $2 \leq j \leq n$. De ahí se obtiene que $q_j = 0$ para $1 \leq j \leq n$ y como $[F : \mathbb{Q}] = n$, se concluye que $\{\beta_i\}_{i=1}^n$ es base para $F/\mathbb{Q}$. Por otro lado, sean

$$\beta_1 = \alpha - m\alpha_1 = \theta\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n$$

$$\beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n.$$

La matriz cambio de base entre esas dos bases es

$$\begin{pmatrix} \theta & \gamma_2 & \cdots & \gamma_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

El determinante de esa matriz es θ, luego por la Proposición 1.1.7, se tiene que $|\Delta(\beta_1, \ldots, \beta_n)| = \theta^2|\Delta(\alpha_1, \ldots, \alpha_n)|$ y como $0 < \theta^2 < 1$, se llega a que

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

Lo cual es una contradicción al hecho de que $|\Delta(\alpha_1, \ldots, \alpha_n)|$ es mínimo. Por lo tanto se concluye que $\gamma_i \in \mathbb{Z}$ para $1 \leq i \leq n$ y así $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. □

Para la siguiente definición consideremos a A_F como ideal de sí mismo.

Definición 1.2.11. *Si $\{\alpha_1, \ldots, \alpha_n\} \subseteq A_F$ es una de base de $F/\mathbb{Q}$, tal que $A_F = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$, entonces diremos que $\{\alpha_1, \ldots, \alpha_n\}$ es una **base entera** para $F/\mathbb{Q}$.*

Corolario 1.2.12. *Sean $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ y $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ dos bases enteras arbitrarias para $F/\mathbb{Q}$. Entonces el discriminante de $\mathcal{A}$ es igual al discriminante de $\mathcal{B}$.*

DEMOSTRACIÓN. Puesto que $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$ con $a_{ij} \in \mathbb{Z}$, se tiene por la Proposición 1.1.7

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

Ya que $\beta_j = \sum_{k=1}^{n} c_{jk}\alpha_k$, con $c_{jk} \in \mathbb{Z}$, es fácil ver que $\det((a_{ij})(c_{jk})) = 1$. De ahí que $\det(a_{ij}) = \pm 1$. Por lo tanto $\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\beta_1, \ldots, \beta_n)$. □

Definición 1.2.13. ***El discriminante de** A_F es el discriminante de una base entera de $F/\mathbb{Q}$ y se denota por δ_F. También δ_F se llama el **discriminante de** $F/\mathbb{Q}$.*

A partir de este momento siempre consideraremos ideales de A_F distintos de cero.

Lema 1.2.14. *Sea I un ideal de A_F. Entonces $I \cap \mathbb{Z} \neq 0$.*

DEMOSTRACIÓN. Sea $\alpha \in I$, $\alpha \neq 0$. Entonces α satisface un polinomio mónico en $\mathbb{Z}[x]$, digamos $p(x) = a_0 + a_1 x + \cdots + x^n$ y tal que sea el de grado mínimo. Entonces $a_0 \neq 0$. Luego $a_0 = -a_1\alpha - \cdots - \alpha^n \in I \cap \mathbb{Z}$. □

Proposición 1.2.15. *Para cada ideal I de A_F, A_F/I es finito.*

DEMOSTRACIÓN. Por el Lema 1.2.14 existe $a \in I \cap \mathbb{Z}$, $a \neq 0$. Sea (a) el ideal principal generado por a en A_F. Consideremos la función f dada por

$$f : A_F/(a) \longrightarrow A_F/I$$

$$f(d + (a)) = d + I.$$

La función f está bien definida porque si $d_1 + (a) = d_2 + (a)$, entonces $d_1 - d_2 \in (a) \subseteq I$ y por tanto $d_1 + I = d_2 + I$, es decir, $f(d_1 + (a)) = f(d_2 + (a))$.

Además es claro que f es una función sobre, por lo que $|A_F/I| \leq |A_F/(a)|$, así que para mostrar que A_F/I es finito basta probar que $A_F/(a)$ lo es.

Sea $\{w_1, w_2, \ldots, w_n\}$ una base entera para $F/\mathbb{Q}$, es decir, $A_F = \mathbb{Z}w_1 + \mathbb{Z}w_2 + \cdots + \mathbb{Z}w_n$ con $w_i \in A_F$. Sea

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

y veamos que S es un conjunto de representantes de $A_F/(a)$. Si $w \in A_F$, entonces $w = \sum_{i=1}^{n} m_i w_i$ con $m_i \in \mathbb{Z}$ para $1 \leq i \leq n$. Luego por el algoritmo de la división se tiene que $m_i = q_i a + \gamma_i$ con $0 \leq \gamma_i < |a|$. Por otro lado se tiene que

$$\begin{aligned} w - \sum_{i=1}^{n} \gamma_i w_i &= (m_1 - \gamma_1)w_1 + \cdots + (m_n - \gamma_n)w_n \\ &= a(q_1 w_1 + \cdots + q_n w_n), \end{aligned}$$

de lo cual $w \equiv \sum_{i=1}^{n} \gamma_i w_i \pmod{(a)}$ y por tanto para cada clase de $A_F/(a)$ hay una de $S/(a)$.

Veamos ahora que todos los elementos de $S/(a)$ son distintos. Supongamos entonces que existen $\sum_{i=1}^{n} \gamma_i w_i$ y $\sum_{i=1}^{n} \beta_i w_i$ dos elementos distintos de S tal que $\sum_{i=1}^{n} \gamma_i w_i + (a) = \sum_{i=1}^{n} \beta_i w_i + (a)$. De ahí que

$$(\gamma_1 - \beta_1)w_1 + \cdots + (\gamma_n - \beta_n)w_n = at$$

para algún $t \in A_F$. Así que

$$(\gamma_1 - \beta_1)w_1 + \cdots + (\gamma_n - \beta_n)w_n = a(z_1 w_1 + \cdots + z_n w_n)$$

con $z_i \in \mathbb{Z}$. Por lo que

$$(\gamma_1 - \beta_1 - az_1)w_1 + \cdots + (\gamma_n - \beta_n - az_n)w_n = 0.$$

Pero como $\{w_i\}_{i=1}^{n}$ es una base sobre $\mathbb{Q}$, obtenemos que $\gamma_i - \beta_i - az_i = 0$ para $1 \leq i \leq n$. Luego por el hecho de que $0 \leq \gamma_i, \beta_i < a$, se tiene que $-a < az_i < a$ y entonces $-1 < z_i < 1$, por lo que $z_i = 0$ para toda i. Entonces $\gamma_i = \beta_i$, por lo cual concluimos que todos los elementos de $S/(a)$ son distintos. Luego como hay una biyección de $S + (a)$ a $A_F/(a)$ y $|S| = a^n$, entonces $|A_F/(a)| = a^n$. □

Corolario 1.2.16. *A_F es un anillo noetheriano.*

DEMOSTRACIÓN. Es consecuencia directa de la Proposición 1.2.15. □

De la teoría básica del Álgebra Conmutativa se sabe que son equivalentes:

i) A_F es noetheriano
ii) Cualquier familia no vacía de ideales tiene un elemento maximal.

Corolario 1.2.17. *Cada ideal primo de A_F es maximal.*

DEMOSTRACIÓN. Si P es un ideal primo de A_F, entonces A_F/P es un dominio entero y además es finito, por lo tanto A_F/P es un campo. De ahí se sigue que P es maximal. □

Corolario 1.2.18. *La factorización en irreducibles es posible en A_F.*

DEMOSTRACIÓN. Supongamos que existe $x \neq 0$, $x \in A_F$ que no es unidad y que no tiene una expresión como un producto finito de irreducibles. Sean $X = \{x \in A_F : x \neq 0, x \text{ no es unidad y no es producto finito de irreducibles}\}$ y $A = \{(x) \subseteq A_F : x \in X\}$. Entonces A tiene elementos maximales, digamos (x) es maximal. Puesto que x no puede ser irreducible, se tiene $x = yz$, donde y, z no son unidades. De Ahí que $(x) \subsetneq (y)$ y $(x) \subsetneq (z)$. Por la maximalidad de (x) se tiene que $y = p_1 \cdots p_n$ y $z = q_1 \cdots q_m$, donde p_i y q_i son irreducibles. De ahí que x tiene una expresión como un producto finito de irreducibles, lo cual contradice nuestra suposición. □

Lema 1.2.19. *Sea $I \subseteq A_F$ un ideal. Si $\beta \in F$ es tal que $\beta I \subseteq I$, entonces $\beta \in A_F$.*

DEMOSTRACIÓN. Sean I un ideal de A_F, $\beta \in F$ y $\{a_i\}_{i=1}^n \subseteq I$ una base de $F/\mathbb{Q}$ tal que $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Se tiene que $\beta a_i \in \beta I \subseteq I$, por lo que existen $b_{ij} \in \mathbb{Z}$ tal que $\beta a_i = \sum_{j=1}^n b_{ij} a_j$. Entonces $\sum_{j=1}^n b_{ij} a_j - \beta a_i = 0$ y de ahí tenemos el siguiente sistema homogéneo de ecuaciones

$$\begin{array}{rcl} (b_{11} - \beta)a_1 + b_{12}a_2 + \cdots + b_{1n}a_n & = & 0 \\ b_{12}a_2 + (b_{22} - \beta)a_2 + \cdots + b_{2n}a_n & = & 0 \\ \vdots & \vdots & \vdots \\ b_{n1}a_1 + b_{n2}a_2 + \cdots + (b_{nn} - \beta)a_n & = & 0. \end{array}$$

Sea $B = (b_{ij})$ y consideremos el sistema lineal homogéneo $(B - I\beta)X = 0$, el cual tiene una solución no trivial $(a_1, \ldots, a_n)$ y por lo tanto el $\det(B - I\beta) = 0$.

Sea $p(x)$ el polinomio característico de B, es decir, $p(x) = \det(B - Ix)$. Como $b_{ij} \in \mathbb{Z}$, tenemos que $p(x) \in \mathbb{Z}[x]$, además es mónico y β es raíz de $p(x)$. Luego, $\beta \in A_F$. □

Lema 1.2.20. *Si I y J son ideales de A_F tal que $I = IJ$, entonces $J = A_F$.*

DEMOSTRACIÓN. Si $I = IJ$, $\{a_i\}_{i=1}^n$ es una base de $F/\mathbb{Q}$ tal que $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, entonces $a_i \in I = IJ$. Luego, existen $\alpha_{ij} \in I$ y $\beta_{ij} \in J$, tal que $a_i = \sum_{j=1}^n \alpha_{ij}\beta_{ij}$ para $i = 1, \ldots, n$. Pero como $\alpha_{ij} \in I$, existen $l_{ijk} \in \mathbb{Z}$ tal que $\alpha_{ij} = \sum_{k=1}^n l_{ijk} a_k$. Entonces se tiene que:

$$a_i = \sum_{j=1}^n \left(\sum_{k=1}^n l_{ijk} a_k \right) \beta_{ij} = \sum_{k=1}^n a_k \sum_{j=1}^n l_{ijk}\beta_{ij}.$$

Sea $\gamma_{ik} = \sum_{j=1}^n l_{ijk}\beta_{ij} \in J$. Entonces $a_i = \sum_{k=1}^n \gamma_{ik} a_k$, de lo cual se tiene

$$\begin{array}{rcl} (\gamma_{11} - 1)a_1 + \gamma_{12}a_2 + \cdots + \gamma_{1n}a_n & = & 0 \\ \gamma_{21}a_1 + (\gamma_{22} - 1)a_2 + \cdots + \gamma_{2n}a_n & = & 0 \\ \vdots & \vdots & \vdots \\ \gamma_{n1}a_{n1} + \gamma_{n2}a_2 + \cdots + (\gamma_{nn} - 1)a_n & = & 0. \end{array}$$

Sea $\Gamma = (\gamma_{ik})$. Así que $\det(\Gamma - I) = 0$. Sea $p(x) = \det(\Gamma - Ix)$. Como $\gamma_{ik} \in J$ se tiene que $p(x) \in J[x]$. Además $p(x)$ es mónico y 1 es raíz de $p(x)$. Supongamos que $p(x) = \sum_{i=1}^{n-1} c_i x^i + x^n$ con $c_i \in J$. Entonces $0 = p(1) = \sum_{i=1}^{n-1} c_i + 1$ y de ahí $1 \in J$. Por lo tanto $J = A_F$. □

Proposición 1.2.21. *Sean I, J ideales de A_F y $w \in A_F$ tal que $(w)I = JI$. Entonces $(w) = J$.*

DEMOSTRACIÓN. Sea $\beta \in J$. Probemos primero que $\left(\frac{\beta}{w}\right) I \subseteq I$. Sea $\alpha \in I$. Entonces $\alpha\beta \in IJ = (w)I$. Como los elementos de $(w)I$ son de la forma $w\gamma$ con $\gamma \in I$, tenemos que $\alpha\beta = w\gamma$ para algún $\gamma \in I$. De ahí se sigue que $\frac{\beta}{w}\alpha = \gamma \in I$ para toda $\alpha \in I$. Entonces $\left(\frac{\beta}{w}\right) I \subseteq I$. Por el Lema 1.2.19 se tiene que $\frac{\beta}{w} \in A_F$, entonces $\beta \in (w)$. De ahí $J \subseteq (w)$, por lo que $w^{-1}J \subseteq A_F$. Observemos que $w^{-1}J$ es un ideal de A_F. Por hipótesis $(w)I = JI$, así que $I = w^{-1}JI$. Por el Lema 1.2.20 se tiene que $w^{-1}J = A_F$ y por lo tanto $(w) = J$. □

1.3. El Número de Clases

En esta sección introduciremos una relación de equivalencia en la familia

$$\{I \neq (0) : \text{ I es un ideal de } A_F\}.$$

Veremos que el número h_F de clases de equivalencia es finito. Éste es uno de los invariantes más importantes asociado a F.

Definición 1.3.1. *Sean I, J ideales no nulos de A_F. Escribiremos $I \sim J$, si existen $\alpha, \beta \in A_F$ distintos de cero tal que $(\alpha)I = (\beta)J$.*

Proposición 1.3.2. *$\sim$ es de equivalencia.*

DEMOSTRACIÓN. Sean I, J, M ideales de A_F. Basta probar que $\sim$ es transitiva. Supongamos que $I \sim J$ y $J \sim M$, entonces existen $\alpha, \beta_1, \beta_2, \gamma$ en A_F distintos de cero tal que

$$(\alpha)I = (\beta_1)J \quad \text{y} \quad (\beta_2)J = (\gamma)M.$$

De donde

$$(\alpha)(\beta_2)I = (\beta_1)(\beta_2)J = (\beta_1)(\gamma)M,$$

entonces

$$(\alpha\beta_2)I = (\beta_1\gamma)M.$$

□

Definición 1.3.3. *A las clases de equivalencia le llamaremos **clases de ideales**. Al número de clases de ideales en A_F le llamaremos el **número de clases de** F y lo denotaremos por h_F.*

La siguiente proposición nos dice en términos del número de clases cuándo A_F es un dominio de ideales principales (DIP) y luego veremos que este resultado también nos dirá cuándo A_F es un dominio de factorización única (DFU), lo cual será de importancia en el último capítulo.

Proposición 1.3.4. *$h_F = 1$ si y sólo si A_F es un dominio de ideales principales.*

DEMOSTRACIÓN. Supongamos que $h_F = 1$ y sea I un ideal de A_F. Se tiene entonces que $I \sim A_F$, por lo que existen α, β en A_F distintos de cero tal que $(\alpha)I = (\beta)A_F = (\beta)$. Entonces $\beta = \alpha \sum_{i=1}^{n} \alpha_i' a_i$ con $\alpha_i' \in A_F$ y $a_i \in I$, de ahí que α divide a β en A_F. Luego $\frac{\beta}{\alpha} = \sum_{i=1}^{n} \alpha_i' a_i \in I$, así que para $x \in A_F$, se tiene que $\frac{x\beta}{\alpha} \in I$ y por lo tanto $\left(\frac{\beta}{\alpha}\right) \subseteq I$. Sea $a \in I$. Entonces $\alpha a = \beta r$ para algún $r \in A_F$ y así $a = \frac{\beta}{\alpha} r$, por lo que $I \subseteq \left(\frac{\beta}{\alpha}\right)$. Entonces $I = \left(\frac{\beta}{\alpha}\right)$ y por tanto A_F es un dominio de ideales principales. Es inmediato que si A_F es un dominio de ideales principales, entonces $h_F = 1$. □

Para mostrar que $h_F < \infty$ necesitamos los siguientes resultados:

Lema 1.3.5. *Para todo $\gamma \in F$, existe un entero positivo M que depende únicamente del campo F, tal que $|N(t\gamma - w)| < 1$ para algún entero $1 \leq t \leq M$ y algún $w \in A_F$.*

DEMOSTRACIÓN. Ver [**6**], página 178, Lema 5.

Corolario 1.3.6. ***(Hurwitz)** Existe un entero positivo M que depende únicamente de F con la siguiente propiedad: Dados $\alpha, \beta \in A_F$, con $\beta \neq 0$, existen un entero $1 \leq t \leq M$ y $w \in A_F$ tal que $|N(t\alpha - w\beta)| < |N(\beta)|$.*

DEMOSTRACIÓN. Sea $\gamma = \frac{\alpha}{\beta} \in F$. Entonces por el Lema 1.3.5 existe un entero positivo M que depende sólo del campo F tal que $|N(t\gamma - w)| < 1$ para algún entero $1 \leq t \leq M$ y algún $w \in A_F$. De ahí $\left|N\left(\frac{t\alpha}{\beta} - w\right)\right| < 1$. Ya que $\beta \neq 0$,

se tiene que $N(\beta) \neq 0$ y así

$$|N(t\alpha - w\beta)|\frac{1}{|N(\beta)|} = |N(t\alpha - w\beta)||N(\beta^{-1})| = |N((t\alpha - w\beta)\beta^{-1})|$$
$$= \left|N\left(\frac{t\alpha - w\beta}{\beta}\right)\right| < 1.$$

Por lo tanto $|N(t\alpha - w\beta)| < |N(\beta)|$. □

Teorema 1.3.7. *El número de clases es finito.*

DEMOSTRACIÓN. Sea I un ideal de A_F. Para toda $\alpha \in I$, se tiene que $N(\alpha) \in \mathbb{Z}$. Escogemos $\beta \neq 0$, $\beta \in I$, tal que $|N(\beta)|$ es mínimo. Por el Corolario 1.3.6 para $\alpha \in I$ y β como antes, existen $1 \leq t \leq M$ y $w \in A_F$ tal que $|N(t\alpha - w\beta)| < |N(\beta)|$. Como $t\alpha - w\beta \in I$ y puesto que $|N(\beta)|$ es mínimo, se tiene que $|N(t\alpha - w\beta)| = 0$ y así $t\alpha - w\beta = 0$, es decir, $t\alpha = w\beta$.

Por otro lado como $t \leq M$ tenemos que $t|M!$, entonces $\frac{M!}{t}w\beta \in (\beta)$ y por el párrafo anterior $\frac{M!}{t}t\alpha \in (\beta)$, por lo que $M!\alpha \in (\beta)$. De ahí

$$M!I \subseteq (\beta). \tag{2}$$

Si $J = \frac{1}{\beta}M!I$, por (2) se tiene que $J \subseteq A_F$ y es fácil ver que J es un ideal de A_F. Luego

$$(\beta)J = \beta A_F J = M!I = (M!)I, \tag{3}$$

de ahí $I \sim J$. Como $\beta \in I$, se tiene $M!\beta \in M!I = (\beta)J$. Por lo que

$$M!\beta = \beta\sum_{i=1}^{n}\gamma_i j_i,$$

para algunos $\gamma_i \in A_F$ y $j_i \in J$. Luego $M! = \sum_{i=1}^{n}\gamma_i j_i \in J$ y por tanto $M!A_F \subseteq J$ y así

$$\frac{J}{M!A_F} < \frac{A_F}{M!A_F} \quad \text{(como grupos)}. \tag{4}$$

Puesto que $\left|\frac{A_F}{M!A_F}\right|$ es finito, hay un número finito de subgrupos en $\frac{A_F}{M!A_F}$, es decir, hay un número finito de subgrupos de A_F que contienen a $M!A_F$.

Sea $\{J_i,\ 1 \leq i \leq n\ :\ J_i$ es un ideal de A_F y $M!A_F \subseteq J_i\}$. Tal conjunto es finito y por (3) se tiene que $I \sim J_i$, para algún $1 \leq i \leq n$. De ahí que hay un número finito de clases de ideales, por lo tanto h_F es finito. □

Al conjunto de clases de ideales en A_F se le puede dar estructura de grupo abeliano multiplicativo. La siguiente proposición es una aplicación del Teorema 1.3.7 y nos ayudará a definir los inversos de dicho grupo.

Proposición 1.3.8. *Si I es un ideal de A_F, entonces existe un entero $1 \leq k \leq h_F$ tal que I^k es principal.*

DEMOSTRACIÓN. Considere el conjunto de ideales $\{I, I^2, \ldots, I^{h_F+1}\}$. Entonces al menos dos de esos ideales están en la misma clase. Por tanto existen $i \neq j$ tal que $1 \leq i, j \leq h_F + 1$ y tal que $I^i \sim I^j$. Supongamos sin pérdida de generalidad que $i < j$ y sea $k = j - i$. Entonces I^k es principal. □

Si I es un ideal de A_F, denotamos por $\overline{I}$ a la clase del ideal I. Sea J cualquier otro ideal de A_F. Definimos el producto de $\overline{I}$ y $\overline{J}$ como $\overline{IJ}$. Esta operación está bien definida y es asociativa. Observemos que $A_F I = I$, para cualquier ideal I. Así que $\overline{A_F}$ es el neutro. También nótese que $(1)(\alpha) = (\alpha)A_F$. Por tanto, cualquier ideal principal no nulo está relacionado con A_F. Sea I un ideal de A_F. Por el Teorema 1.3.8, existe un entero $1 \leq k \leq h_F$, tal que $I^k = (\alpha)$ para algún $\alpha \in A_F$. De ahí que

$$\overline{I} \cdot \overline{I^{k-1}} = \overline{II^{k-1}} = \overline{I^k} = \overline{(\alpha)}.$$

Por lo tanto el conjunto de clases de ideales en A_F tiene estructura de grupo abeliano multiplicativo.

Definición 1.3.9. *Sea F un campo de números. El* ***grupo de clases de ideales de*** *A_F es*

$$\{\overline{I} : I \text{ es ideal de } A_F\}.$$

Proposición 1.3.10. *Si I, J y K son ideales de A_F, tal que $IJ = IK$, entonces $J = K$.*

DEMOSTRACIÓN. Por la Proposición 1.3.8, existe $k > 0$ tal que $I^k = (\alpha)$, para algún $\alpha \in A_F$. Como $IJ = IK$, entonces

$$I^{k-1}(IJ) = I^{k-1}(IK).$$

De ahí que $(\alpha)J = (\alpha)K$. Sea $b \in J$. Entonces $\alpha b \in (\alpha)J = (\alpha)K$. Así que $\alpha b = \alpha c$, para algun $c \in K$, de donde $b = c$. Por lo tanto $b \in K$ y entonces $J \subseteq K$. Análogamente $K \subseteq J$ y así $J = K$. □

Proposición 1.3.11. *Sean I, J ideales de A_F, tal que $I \subseteq J$. Entonces existe un ideal K de A_F con la propiedad de que $I = JK$.*

DEMOSTRACIÓN. Por la Proposición 1.3.8, existe $k > 0$ tal que $J^k = (\beta)$. Luego como $I \subseteq J$, se tiene que

$$J^{k-1}I \subseteq J^{k-1}J = (\beta).$$

De ahí que $\dfrac{1}{\beta}J^{k-1}I \subseteq A_F$. Sea $K = \dfrac{1}{\beta}J^{k-1}I$. Luego K es un ideal de A_F y

$$JK = J\left(\frac{1}{\beta}J^{k-1}I\right) = \frac{1}{\beta}(\beta)I = A_F I = I.$$ □

1.4. Factorización de Ideales en los Anillos de Enteros

En esta sección demostraremos que los ideales no cero de A_F se pueden escribir en forma única como producto finito de ideales primos. También veremos de manera breve el concepto de norma de un ideal y por último, involucrando al número de clases, veremos cuándo A_F es un DFU.

Lema 1.4.1. *Sea $I \subsetneq A_F$ un ideal. Entonces I está contenido en un ideal maximal.*

DEMOSTRACIÓN. Es consecuencia del Lema de Zorn. □

Proposición 1.4.2. *Todo ideal distinto de cero de A_F puede escribirse como producto de un número finito de ideales primos.*

DEMOSTRACIÓN. Sea I un ideal propio de A_F. Si I es un ideal primo entonces no hay nada que probar. Si I no es un ideal primo, entonces por el Lema 1.4.1 I está contenido en un ideal maximal P_1 y por la Proposición 1.3.11 se tiene que

$$I = P_1 J_1$$

para algún ideal J_1 de A_F. Como $J_1 \neq A_F$, entonces existe un ideal maximal P_2 que lo contiene y así $J_1 = P_2 J_2$, para algún ideal J_2 de A_F. Luego se tiene que

$$I = P_1 P_2 J_2.$$

Si $J_2 = A_F$ el proceso anterior termina, de lo contrario existe un ideal maximal P_3 que lo contiene y el proceso continua. Observemos que

$$I \subsetneq J_1 \subsetneq J_2 \subsetneq \cdots$$

y como A_F es noetheriano, el proceso anterior termina en un número finito de pasos, es decir, existe k tal que $J_k = A_F$. Por lo tanto

$$I = P_1 P_2 \cdots P_{k-1}.$$

□

En la Proposición 1.4.2 los ideales primos no necesariamente son diferentes.

Nótese que si P es un ideal primo, entonces la cadena

$$P \supsetneq P^2 \supsetneq P^3 \supsetneq \cdots$$

es de contenciones propias, pues de lo contrario, existe i tal que $P^i = P^{i+1}$ y por el Lema 1.2.20 se tendría que $P = A_F$, lo que es una contradicción.

Definición 1.4.3. *Sean P un ideal primo, I un ideal. Definimos $ord_P I$ como el único entero no negativo t tal que $P^t \supseteq I$ y $P^{t+1} \not\supseteq I$.*

Proposición 1.4.4. *Sean P un ideal primo, I, J ideales de A_F. Entonces*

i) $ord_P P = 1$.
ii) *Si $P' \neq P$, donde P' es primo, entonces $ord_P P' = 0$.*
iii) $ord_P IJ = ord_P I + ord_P J$.

DEMOSTRACIÓN. i) Es evidente.

ii) Si $ord_P P' > 0$, entonces $P' \subsetneq P$. Por el Corolario 1.2.17 P' es maximal, por lo que $P' = P$, que es una contradicción.

iii) Sean $ord_P I = t, ord_P J = s$. Entonces $I \subseteq P^t, J \subseteq P^s$ y $J \nsubseteq P^{s+1}, I \nsubseteq P^{t+1}$. De ahí que $I = P^t I_1, J = P^s J_1$ con $I_1 \nsubseteq P, J_1 \nsubseteq P$. Luego

$$IJ = P^{t+s} I_1 J_1 \subseteq P^{t+s}.$$

Si $IJ \subseteq P^{t+s+1}$, entonces $IJ = P^{t+s+1}K$. Así que

$$P^{t+s} I_1 J_1 = P^{t+s+1} K$$

y por la Proposición 1.3.10 $I_1 J_1 = PK \subseteq P$. Puesto que P es primo, $I_1 \subseteq P$ ó $J_1 \subseteq P$, lo cual es una contradicción. Por lo tanto

$$ord_P IJ = t + s = ord_P I + ord_P J.$$

□

Teorema 1.4.5. *Sea $I \subseteq A_F$ un ideal. Entonces*

$$I = \prod P^{a(P)}, \tag{5}$$

donde el producto es sobre el conjunto de todos los ideales primos de A_F y los $a(P)$ son enteros no negativos de los cuales sólo un número finito no es cero. Los enteros $a(P)$ están determinados de manera única por $a(P) = ord_P I$.

DEMOSTRACIÓN. Por la Proposición 1.4.2, se tiene que I se puede escribir como un producto de ideales primos. Sea P_0 un ideal primo. Aplicando ord_{P_0} a ambos lados de (5) y utilizando la Proposición 1.4.4, tenemos que

$$ord_{P_0} I = ord_{P_0} \prod P^{a(P)} = \sum_P a(P) ord_{P_0} P = a(P_0) ord_{P_0} P_0 = a(P_0).$$

Por lo que la factorización en ideales primos es única. □

Definición 1.4.6. *Sea I un ideal de A_F. Definimos la* ***norma del ideal*** *I como $N(I) = |A_F/I|$.*

Según la Proposición 1.2.15 $N(I) < \infty$. Los siguientes resultados son algunas propiedades de la norma de un ideal que nos servirán más adelante.

Teorema 1.4.7. *Sean I y J ideales de A_F. Entonces*

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

DEMOSTRACIÓN. Por el Teorema 1.4.5 y por inducción en el número de factores basta probar que

$$N(IP) = N(I)N(P),$$

donde P es un ideal primo. Probaremos que

$$|A_F/IP| = |A_F/I||I/IP| \tag{6}$$

y

$$|I/IP| = |A_F/P|. \tag{7}$$

Consideremos el homomorfismo de anillos $\varphi : AF/IP \to A_F/I$ definido por $\varphi(x + IP) = x + I$. Es claro que φ es sobre y ker$\varphi = I/IP$. Por lo tanto

$$A_F/I \cong \frac{A_F/IP}{I/IP},$$

de ahí que

$$|A_F/IP| = |A_F/I||I/IP|.$$

Para probar (7), primero nótese que $I \neq IP$, por lo que $IP \subsetneq I$. Supongamos que

$$IP \subseteq J \subseteq I,$$

donde J es un ideal de A_F. De ahí que $P \subseteq I^{-1}J \subseteq A_F$. Puesto que $I^{-1}J \subseteq A$, se puede ver que $I^{-1}J$ es un ideal de A_F y como P es maximal, se tiene que $I^{-1}J = A_F$ o $I^{-1}J = P$. De ahí

$$J = I \quad \text{o} \quad J = IP.$$

Sea $a \in I \backslash IP$. Entonces $IP + (a) = I$, puesto que $IP \subsetneq IP + (a) \subseteq I$. Sea $\psi : A_F \to I/IP$, definido por $\psi(x) = ax + IP$. Puesto que $IP + (a) = I$, se tiene que ψ es un epimorfismo de A_F-módulos. El kernel de ψ satisface que $P \subseteq$ kerψ. También ker$\psi \neq A_F$, pues de lo contrario se tendría $I = IP$. Puesto que P es maximal, se tiene $P =$ kerψ. Por tanto

$$A_F/P \cong I/IP,$$

como A_F-módulos. De ahí $|A_F/P| = |I/IP|$. □

Teorema 1.4.8. *Sea I un ideal de A_F. Entonces*

i) *Si $N(I)$ es primo, entonces I también es primo.*
ii) *$N(I)$ es un elemento de I, o equivalentemente $I|(N(I))$.*

DEMOSTRACIÓN. i) Escribimos I como un producto de ideales primos y aplicamos la norma.

ii) Puesto que $N(I) = |A_F/I|$ es el orden del grupo A_F/I, tenemos que para todo $x + I \in A_F/I$, se tiene que $N(I)(x + I) = I$, de donde $N(I)x \in I$, luego $N(I) = N(I)1 \in I$. □

Siempre es cierto que un DIP es un DFU, pero no necesariamente un DFU es un DIP, por ejemplo el anillo $\mathbb{R}[x, y]$ es un DFU y no es un DIP. El caso A_F es particularmente interesante.

Teorema 1.4.9. *La factorización de elementos de A_F en irreducibles es única si y sólo si A_F es un DIP.*

DEMOSTRACIÓN. Siempre se tiene que un DIP es un DFU, entonces falta probar que A_F es un DIP si A_F es un DFU. Para esto basta probar que cada ideal primo es principal, puesto que cada ideal en A_F se puede escribir como un producto de ideales primos.

Sea P un ideal primo en A_F. Por ii) del Teorema 1.4.8 tenemos que $P|(N(P))$. Supongamos que $N(P) = |A_F/P| = n$, para algún $n \in \mathbb{N}$.

Por el Corolario 1.2.18, n se puede factorizar como un producto de elementos irreducibles en A_F, digamos

$$n = \pi_1 \cdots \pi_s \quad \text{con } \pi_i \in A_F.$$

Como $P|(n)$ y P es un ideal primo, tenemos

$$P|(\pi_i), \tag{8}$$

para algún i. Por hipótesis A_F es un DFU, por lo que π_i es primo y por tanto (π_i) es primo. Por el hecho de que en A_F la factorización es única respecto a ideales y por (8), se tiene que $P = (\pi_i)$. De ahí que A_F es un DIP puesto que el producto de ideales principales es principal. □

Observemos que por la Proposición 1.3.4 y el Teorema 1.4.9, tenemos que:

$$h_F = 1 \text{ si y sólo si } A_F \text{ es un DFU.}$$

Esta conclusión nos servirá en el último capítulo.

1.5. Campos Cuadráticos

Un campo F tal que $[F : \mathbb{Q}] = 2$ le llamaremos **campo cuadrático**. En esta sección veremos cómo es un campo cuadrático y cómo es su anillo de enteros. Si F es un campo cuadrático, entonces $F = \mathbb{Q}(\alpha)$, donde α satisface una ecuación cuadrática, digamos, $ax^2 + bx + c$ donde $a, b, c \in \mathbb{Z}$, $a \neq 0$. Así que

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Si $A = b^2 - 4ac$, entonces $F = \mathbb{Q}(\sqrt{A})$. Si $A = A_1^2 d$, donde $A_1, d \in \mathbb{Z}$ y d es libre de cuadrados, entonces $F = \mathbb{Q}(\sqrt{d})$. Un campo cuadrático se llama real si $d > 0$ e imaginario si $d < 0$. En los siguientes capítulos sólo trabajaremos con campos cuadráticos reales. Cualquier extensión cuadrática sobre $\mathbb{Q}$ es de Galois.

Sea $\mathrm{Gal}(F/\mathbb{Q})$ el grupo de Galois de la extensión cuadrática $F/\mathbb{Q}$ y $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Si $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, con $a, b \in \mathbb{Q}$, tenemos que

$$\sigma(\alpha) = a + b\sigma(\sqrt{d}).$$

Así que para conocer $\mathrm{Gal}(F/\mathbb{Q})$, basta ver como es $\sigma(\sqrt{d})$. Por lo que

$$d = \sigma(d) = \sigma(\sqrt{d}^2) = \sigma(\sqrt{d})^2,$$

de ahí que

$$\sigma(\sqrt{d}) = \pm\sqrt{d}.$$

Por lo tanto $\mathrm{Gal}(F/\mathbb{Q}) = \{\mathrm{Id}, \sigma\}$, donde σ es el $\mathbb{Q}$-automorfismo que manda $\sqrt{d}$ en $-\sqrt{d}$. Entonces $\sigma(\alpha) = a - b\sqrt{d}$ y denotaremos $\sigma(\alpha) = \alpha'$. Por la Proposición 1.1.4, se tiene que

$$tr(\alpha) = \mathrm{Id}(\alpha) + \sigma(\alpha) = \alpha + \alpha' = a + b\sqrt{d} + a - b\sqrt{d} = 2a$$

y

$$N(\alpha) = \mathrm{Id}(\alpha)\sigma(\alpha) = \alpha\alpha' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d.$$

Proposición 1.5.1. *Sea $\alpha \in F$. Se tiene que $\alpha \in A_F$ si y sólo si $tr(\alpha) \in \mathbb{Z}$ y $N(\alpha) \in \mathbb{Z}$.*

DEMOSTRACIÓN. Por la Proposición 1.2.8 tenemos que si $\alpha \in A_F$, entonces $tr(\alpha), N(\alpha) \in \mathbb{Z}$. Supongamos ahora que $tr(\alpha) \in \mathbb{Z}$ y $N(\alpha) \in \mathbb{Z}$. Luego

$$(x - \alpha)(x - \alpha') = x^2 - tr(\alpha)x + N(\alpha),$$

de ahí que α satisface un polinomio mónico con coeficientes en $\mathbb{Z}$, es decir, $\alpha \in A_F$. □

La siguiente proposición muestra cómo es el anillo de enteros de un campo cuadrático.

Proposición 1.5.2. *Si $d \equiv 2, 3 \pmod 4$, entonces $A_F = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ y si $d \equiv 1 \pmod 4$, entonces $A_F = \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{d}}{2}\right)$.*

DEMOSTRACIÓN. Sea $\alpha = a + b\sqrt{d} \in A_F$, para ciertos $a, b \in \mathbb{Q}$. Entonces $t(\alpha) = 2a \in \mathbb{Z}$ y $N(\alpha) = a^2 - b^2 d \in \mathbb{Z}$. Así que $4a^2 - 4b^2 d \in \mathbb{Z}$, por lo que $4b^2 d \in \mathbb{Z}$ y ya que d es libre de cuadrados $2b \in \mathbb{Z}$. Sean $2a = m$ y $2b = n$. Luego $4a^2 - 4b^2 d = 4z_1$, donde $z_1 = a^2 - b^2 d \in \mathbb{Z}$, entonces $m^2 - n^2 d = 4z_1$. Se sigue que

$$m^2 - n^2 d \equiv 0 \pmod 4.$$

Observemos que hasta ahora no ha importado d.

Supongamos que $d \equiv 2, 3 \pmod 4$ y sea $\alpha = a + b\sqrt{d} \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Puesto que α es raíz de $f(x) = x^2 - tr(\alpha) + N(\alpha)$, se tiene que $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq A_F$. Para la otra contención sea $\alpha = a + b\sqrt{d} \in A_F$, para ciertos $a, b \in \mathbb{Q}$.
Si $d \equiv 2 \pmod 4$, se obtiene que

$$m^2 - n^2 d \equiv m^2 - 2n^2 \equiv m^2 + 2n^2 \pmod 4,$$

Si $d \equiv 3 \pmod 4$, se tiene que

$$m^2 - n^2 d \equiv m^2 - 3n^2 \equiv m^2 + n^2 \pmod 4.$$

Entonces $m^2 + 2n^2 \equiv 0 \pmod 4$ y $m^2 + n^2 \equiv 0 \pmod 4$, cuando m y n son pares. Puesto que $2a = m$ y $2b = n$, se tiene que m y n son pares si y sólo si $a, b \in \mathbb{Z}$. De ahí que $\alpha = a + b\sqrt{d}$, donde $a, b \in \mathbb{Z}$, es decir, $A_F = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

Si $d \equiv 1 \pmod 4$. Entonces

$$m^2 - n^2 d \equiv m^2 - n^2 \pmod 4.$$

Luego $m^2 - n^2 \equiv 0 \pmod 4$ cuando m y n tienen la misma paridad. Así que

$$A_F = \left\{ \frac{m + n\sqrt{d}}{2} : \ m \equiv n \pmod 2 \right\}.$$

Entonces $\alpha = \dfrac{m + n\sqrt{d}}{2}$, donde $m \equiv n \pmod 2$. Nótese que

$$\alpha = \frac{m - n}{2} + n\left(\frac{1 + \sqrt{d}}{2}\right)$$

y puesto que $m \equiv n \pmod 2$, tenemos $\dfrac{m - n}{2} \in \mathbb{Z}$. Por lo que

$$A_F \subseteq \mathbb{Z} + \mathbb{Z}\left(\frac{1 + \sqrt{d}}{2}\right).$$

Para la otra contención basta probar que $\dfrac{1 + \sqrt{d}}{2} \in A_F$. Como $d \equiv 1 \pmod 4$, tenemos $d = 1 + 4q$, para algún $q \in \mathbb{Z}$. Así que

$$\left(\frac{1 + \sqrt{d}}{2}\right) = \left(\frac{1 + \sqrt{1 + 4q}}{2}\right).$$

De donde se puede ver que $\dfrac{1 + \sqrt{d}}{2}$ es raíz de $x^2 - x - q$. Por lo tanto $\dfrac{1 + \sqrt{d}}{2} \in A_F$. □

La siguiente proposición muestra cómo es el discriminante de un campo cuadrático.

Proposición 1.5.3. *Sea δ_F el discriminante de $F = \mathbb{Q}(\sqrt{d})$. Si $d \equiv 2, 3 \pmod 4$, entonces $\delta_F = 4d$ y si $d \equiv 1 \pmod 4$, entonces $\delta_F = d$.*

DEMOSTRACIÓN. Si $d \equiv 2, 3 \pmod 4$, entonces $A_F = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, de esto $\{1, \sqrt{d}\}$ es una base entera para $F/\mathbb{Q}$. Si $w_1 = 1$ y $w_2 = \sqrt{d}$, entonces

$$\begin{aligned} \delta_F &= \det(tr(w_i w_j)) = \begin{vmatrix} tr(w_1 w_1) & tr(w_1 w_2) \\ tr(w_2 w1) & tr(w_2 w_2) \end{vmatrix} \\ &= \begin{vmatrix} tr(1) & tr(\sqrt{d}) \\ tr(\sqrt{d}) & tr(d) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d. \end{aligned}$$

Si $d \equiv 1 \pmod 4$, entonces $A_F = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$ y $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ es una base entera para $F/\mathbb{Q}$. Como en el caso anterior sean $w_1 = 1$ y $w_2 = \frac{1+\sqrt{d}}{2}$, entonces

$$\begin{aligned} \delta_F &= \det(tr(w_i w_j)) = \begin{vmatrix} tr(1) & tr\left(\frac{1+\sqrt{d}}{2}\right) \\ tr\left(\frac{1+\sqrt{d}}{2}\right) & tr\left(\frac{d+1+2\sqrt{d}}{4}\right) \end{vmatrix} \\ &= \begin{vmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{vmatrix} = d. \end{aligned}$$

□

Definición 1.5.4. *Si A_F es el anillo de enteros de un campo cuadrático, llamaremos a A_F* ***anillo cuadrático****.*

Capítulo 2

Fracciones Continuas

A lo largo de este capítulo desarrollaremos la teoría necesaria de las fracciones continuas para, en el Capítulo 3, aplicarla al generador irracional de un ideal distinto de cero del anillo de enteros de una extensión cuadrática de $\mathbb{Q}$. La presentación que haremos se encuentra esencialmente en [**5**] y [**12**].

2.1. Fracciones Continuas

Consideremos el número racional $\frac{325}{57}$. Mediante el algoritmo de Euclides calculemos el $mcd(57, 325)$:

$$
\begin{aligned}
(1) \qquad 325 &= 57 \cdot 5 + 40, \\
(2) \qquad 57 &= 40 \cdot 1 + 17, \\
(3) \qquad 40 &= 17 \cdot 2 + 6, \\
(4) \qquad 17 &= 6 \cdot 2 + 5, \\
(5) \qquad 6 &= 5 \cdot 1 + 1, \\
(6) \qquad 5 &= 1 \cdot 5 + 0.
\end{aligned}
$$

De (1), se obtiene

$$(7) \qquad \frac{325}{57} = 5 + \frac{40}{57}.$$

De (2) tenemos que $\frac{57}{40} = 1 + \frac{17}{40}$, por lo que $\frac{40}{57} = \frac{1}{1 + \frac{17}{40}}$. Entonces sustituyendo en (7) obtenemos

$$(8) \qquad \frac{325}{57} = 5 + \frac{1}{1 + \frac{17}{40}}.$$

Ahora de (3) tenemos $\frac{40}{17} = 2 + \frac{6}{17}$, de ahí que $\frac{17}{40} = \frac{1}{2 + \frac{6}{17}}$. Sustituyendo en (8) llegamos a

$$\frac{325}{57} = 5 + \frac{1}{1 + \frac{1}{2 + \frac{6}{17}}}.$$

Siguiendo un procedimiento análogo al anterior se llega a que

$$\frac{325}{57} = 5 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{5}}}}}. \tag{9}$$

Podemos observar de (9) que hemos obtenido una expresión para el racional $\frac{325}{57}$ y usaremos la siguiente notación:

$$\frac{325}{57} = [5, 1, 2, 2, 1, 5],$$

donde la sucesión de números $5, 1, 2, 2, 1, 5$, son los cocientes del algoritmo de la división.

Definición 2.1.1. *Una **fracción continua infinita** es una expresión de la forma*

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}}}$$

*donde los $q_i \in \mathbb{R}^+$ para $i \geq 1$ y $q_0 \in \mathbb{R}$. En el caso que $q_0 \in \mathbb{Z}$ y $q_i \in \mathbb{N}$ para $i \geq 1$ la llamaremos **fracción continua simple**. Denotaremos por $[q_0, q_1, q_2, q_3, \ldots]$ a la fracción continua.*

Primero estudiaremos el caso en el que una fracción continua simple es finita.

Lema 2.1.2. *Sea $\frac{a}{b} \in \mathbb{Q}$ con $b > 0$. Entonces $\frac{a}{b} = [q_0, q_1, \ldots, q_{k-1}, q_k]$, donde $q_k \in \mathbb{N}$ para $k \geq 1$.*

DEMOSTRACIÓN. Los q_k se obtienen a partir del algoritmo de Euclides al calcular el $mcd(a, b)$. Tal como se hizo en el ejemplo. □

El siguiente teorema asegura que cualquier número racional se puede expresar como una fracción continua simple finita.

Teorema 2.1.3. *$\alpha \in \mathbb{Q}$ si y sólo si $\alpha = [q_0, q_1, \ldots, q_n]$*

DEMOSTRACIÓN. Por el Lema 2.1.2 se tiene que la fracción continua de α es finita. Es claro que si $\alpha = [q_0, q_1, \ldots, q_n]$, entonces $\alpha \in \mathbb{Q}$. □

La representación en fracción continua simple de un número racional no es única. Nótese que la útima entrada de $[q_0, q_1, \ldots, q_k]$ o es 1 o es $\neq 1$. Si $q_k = 1$,

entonces

$$[q_0, q_1, \ldots, q_{k-1}, 1] = [q_0, q_1, \ldots, q_{k-2}, q_{k-1} + 1]$$

y si $q_k > 1$

$$[q_0, q_1, \ldots, q_k] = [q_0, q_1, \ldots, q_k - 1, 1].$$

Por ejemplo se tiene que $\dfrac{325}{57} = [5, 1, 2, 2, 1, 5] = [5, 1, 2, 2, 1, 4, 1]$.

A continuación veremos algunos conceptos básicos de las fracciones continuas para después probar que cualquier número real se puede representar como una fracción continua simple.

Definición 2.1.4. *Sea* $[q_0, q_1, q_2, \ldots, q_n, \ldots]$ *una fracción continua. Llamaremos* ***n-ésimo convergente*** *a la fracción continua finita* $[q_0, q_1, \ldots, q_n]$.

Observemos que cada convergente debe ser un cociente de números reales. Escribiremos

$$[q_0, q_1, \ldots, q_n] = \frac{A_n}{B_n}.$$

Por ejemplo:

- Si $n = 0$, tenemos que $[q_0] = \dfrac{q_0}{1}$ y en este caso $A_0 = q_0$ y $B_0 = 1$.
- Si $n = 1$, tenemos que $[q_0, q_1] = q_0 + \dfrac{1}{q_1} = \dfrac{q_1 q_0 + 1}{q_1}$, por lo que $A_1 = q_1 q_0 + 1$ y $B_1 = q_1$.
- Si $n = 2$, tenemos que $[q_0, q_1, q_2] = \dfrac{q_2 q_1 q_0 + q_2 + q_0}{q_2 q_1 + 1}$ y en este caso $A_2 = q_2 q_1 q_0 + q_2 + q_0$ y $B_2 = q_2 q_1 + 1$.

El siguiente resultado nos da una fórmula recursiva para A_n y B_n.

Teorema 2.1.5. *Sea* $[q_0, q_1, \ldots, q_n]$ *el n-ésimo convergente de la fracción continua* $[q_0, q_1, \ldots, q_n, \ldots]$. *Para* $n \in \mathbb{Z}, n \geq -2$ *definimos*

$$A_{-2} = 0, \quad A_{-1} = 1, \quad A_n = q_n A_{n-1} + A_{n-2}$$

y

$$B_{-2} = 1, \quad B_{-1} = 0, \quad B_n = q_n B_{n-1} + B_{n-2}.$$

Entonces

$$[q_0, q_1, \ldots, q_n] = \frac{A_n}{B_n} = \frac{q_n A_{n-1} + A_{n-2}}{q_n B_{n-1} + B_{n-2}}.$$

DEMOSTRACIÓN. La prueba será por inducción sobre n. Si $n = 0$, entonces

$$[q_0] = \frac{A_0}{B_0} = q_0 = \frac{q_0 A_{-1} + A_{-2}}{q_0 B_{-1} + B_{-2}}.$$

Supongamos que la afirmación es cierta para n. Es claro que

$$[q_0, q_1, \ldots, q_n, q_{n+1}] = \left[q_0, q_1, \ldots, q_{n-1}, q_n + \frac{1}{q_{n+1}}\right].$$

Entonces por la hipótesis de inducción se tiene que

$$\begin{aligned}\left[q_0, q_1, \ldots, q_{n-1}, q_n + \frac{1}{q_{n+1}}\right] &= \frac{\left(q_n + \frac{1}{q_{n+1}}\right) A_{n-1} + A_{n-2}}{\left(q_n + \frac{1}{q_{n+1}}\right) B_{n-1} + B_{n-2}} \\ &= \frac{(q_n q_{n+1} + 1) A_{n-1} + q_{n+1} A_{n-2}}{(q_n q_{n+1} + 1) B_{n-1} + q_{n+1} B_{n-2}} \\ &= \frac{A_{n-1} + q_{n+1}(q_n A_{n-1} + A_{n-2})}{B_{n-1} + q_{n+1}(q_n B_{n-1} + B_{n-2})} \\ &= \frac{A_{n-1} + q_{n+1} A_n}{B_{n-1} + q_{n+1} B_n} = \frac{A_{n+1}}{B_{n+1}}.\end{aligned}$$

□

Corolario 2.1.6. *Sea $\alpha = [q_0, q_1, \ldots, q_n, q_{n+1}, \ldots]$ y $x = [q_{n+1}, q_{n+2}, \ldots]$. Entonces*

$$\alpha = \frac{x A_n + A_{n-1}}{x B_n + B_{n-1}}.$$

DEMOSTRACIÓN. Del Teorema 2.1.5, obtenemos el resultado puesto que:

$$\alpha = [q_0, q_1, \ldots, q_n, x] = \frac{A_{n+1}}{B_{n+1}} = \frac{x A_n + A_{n-1}}{x B_n + B_{n-1}}.$$

□

Corolario 2.1.7. *En una fracción continua simple se cumple que $B_n > B_{n-1}$ para $n \geq 2$ y $B_n \geq n$, con la desigualdad estricta cuando $n > 3$.*

DEMOSTRACIÓN. Supongamos que $n \geq 2$. Por el Teorema 2.1.5 y puesto que $q_n \geq 1$, se tiene

$$B_n = q_n B_{n-1} + B_{n-2} \geq B_{n-1} + B_{n-2},$$

pero $B_{n-2} \geq 1$, por lo que $B_n \geq B_{n-1} + 1 > B_{n-1}$.

Por el Teorema 2.1.5 es claro que $B_n \geq n$, para $n = 0, 1, 2, 3$. Ahora por la primera parte del corolario y por el Teorema 2.1.5, se tiene lo siguiente:

$$B_4 = q_4 B_3 + B_2 > q_4 B_3 + B_1 = q_1 q_2 q_3 q_4 + q_1 q_4 + q_3 q_4 + q_1 \geq 4,$$

por lo tanto $B_4 > 4$. Supongamos que $B_n > n$ y $B_{n-1} \geq n-1$ para algún $n \geq 4$. Entonces

$$B_{n+1} \geq B_n + B_{n-1} \geq n + n - 1 = 2n - 1,$$

pero $2n - n = n \geq 4 > 2$, así que $2n - 1 > n + 1$ y por tanto $B_{n+1} > n + 1$. □

Corolario 2.1.8. *En una fracción continua simple si $q_0 > 0$, entonces $A_n > A_{n-1}$ para $n \geq 1$.*

DEMOSTRACIÓN. Se tiene que $A_0 = q_0$ y $A_1 = q_0 q_1 + 1$. De ahí es claro que $A_1 > A_0$. Supongamos que $A_n > A_{n-1}$. Por el Teorema 2.1.5 y ya que $q_{n+1} \geq 1$, se obtiene

$$A_{n+1} = q_{n+1} A_n + A_{n-1} \geq A_n + A_{n-1}.$$

Entonces de ahí y de la hipótesis de inducción se tiene que $A_{n+1} > A_n$. □

Los Corolarios 2.1.7 y 2.1.8 son válidos para fracciones continuas en general con la hipótesis adicional $q_i \geq 1$ para $i \in \mathbb{N}$.

Corolario 2.1.9. *Sea $[q_0, q_1, \ldots, q_n]$ el n-ésimo convergente de la fracción continua $[q_0, q_1, \ldots, q_n, \ldots]$ tal que $q_j > 0$ para $j \geq 0$. Entonces*

$$\frac{A_n}{A_{n-1}} = [q_n, q_{n-1}, \ldots, q_1, q_0] \quad y \quad \frac{B_n}{B_{n-1}} = [q_n, q_{n-1}, \ldots, q_2, q_1]$$

para $n \geq 1$.

DEMOSTRACIÓN. La prueba será por inducción sobre n. Si $n = 1$, entonces por el Teorema 2.1.5

$$\frac{A_1}{A_0} = \frac{q_1 A_0 + A_{-1}}{A_0} = q_1 + \frac{1}{A_0} = q_1 + \frac{1}{q_0} = [q_1, q_0].$$

Supongamos que $\dfrac{A_{n-1}}{A_{n-2}} = [q_{n-1}, q_{n-2}, \ldots, q_0]$. Por el Teorema 2.1.5, se tiene que

$$\frac{A_n}{A_{n-1}} = \frac{q_n A_{n-1} + A_{n-2}}{A_{n-1}} = q_n + \frac{A_{n-2}}{A_{n-1}} = q_n + \frac{1}{\dfrac{A_{n-1}}{A_{n-2}}}.$$

De esto y por la hipótesis de inducción obtenemos

$$\frac{A_n}{A_{n-1}} = q_n + \frac{1}{[q_{n-1}, q_{n-2}, \ldots, q_0]} = [q_n, q_{n-1}, \ldots, q_0].$$

La prueba para B_n es similar. □

Por las definiciones de A_n y B_n en el teorema 2.1.5 tenemos lo siguiente:

- Si $n = -1$, entonces $A_{-1}B_{-2} - A_{-2}B_{-1} = 1$.
- Si $n = 0$, entonces $A_0 B_{-1} - A_{-1} B_0 = -1$ y $A_0 B_{-2} - A_{-2} B_0 = q_0$.

En general se tiene

Teorema 2.1.10. *Para $n \geq 1$, A_n y B_n satisfacen las siguientes propiedades:*

1. $A_nB_{n-1} - A_{n-1}B_n = (-1)^{n-1}$.
2. $\dfrac{A_n}{B_n} - \dfrac{A_{n-1}}{B_{n-1}} = \dfrac{(-1)^{n-1}}{B_nB_{n-1}}$.
3. $A_nB_{n-2} - A_{n-2}B_n = q_n(-1)^n$.
4. $\dfrac{A_n}{B_n} - \dfrac{A_{n-2}}{B_{n-2}} = \dfrac{(-1)^n q_n}{B_nB_{n-2}}$, *para* $n \geq 2$.

DEMOSTRACIÓN. La prueba de la parte 1 la haremos por inducción sobre n. Se tiene

$$A_0 = q_0, \quad B_0 = 1, \quad A_1 = q_1q_0 + 1, \quad B_1 = q_1,$$

así que

$$A_1B_0 - A_0B_1 = q_1q_0 + 1 - q_0q_1 = 1.$$

De donde la parte 1 del teorema es válida para $n = 1$. Ahora supongamos que se cumple

$$A_nB_{n-1} - A_{n-1}B_n = (-1)^{n-1}.$$

Luego por las definiciones de A_n y B_n en el Teorema 2.1.5, se obtiene que

$$\begin{aligned} A_{n+1}B_n - A_nB_{n+1} &= (q_{n+1}A_n + A_{n-1})B_n - A_n(q_{n+1}B_n + B_{n-1}) \\ &= -(A_nB_{n-1} - A_{n-1}B_n) = -1(-1)^{n-1} = (-1)^n. \end{aligned}$$

Por otro lado como $B_nB_{n-1} \neq 0$, entonces

$$\frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}} = \frac{A_nB_{n-1} - A_{n-1}B_n}{B_nB_{n-1}} = \frac{(-1)^{n-1}}{B_nB_{n-1}}.$$

De ahí se tiene claramente la parte 2 del teorema.

Para la parte 3 del teorema, de nuevo usamos las definiciones de A_n y B_n y aplicamos la parte 1, entonces

$$\begin{aligned} A_nB_{n-2} - A_{n-2}B_n &= (q_nA_{n-1} + A_{n-2})B_{n-2} - A_{n-2}(q_nB_{n-1} + B_{n-2}) \\ &= q_n(A_{n-1}B_{n-2} - A_{n-2}B_{n-1}) = q_n(-1)^{n-2} = q_n(-1)^n. \end{aligned}$$

Para la parte 4 del teorema se tiene

$$\frac{A_n}{B_n} - \frac{A_{n-2}}{B_{n-2}} = \frac{A_nB_{n-2} - A_{n-2}B_n}{B_nB_{n-2}},$$

entonces por la parte 3, se tiene el resultado. □

A partir de ahora denotaremos al n-ésimo convergente de $[q_0, q_1, \ldots, q_n, \ldots]$ como $C_n = \dfrac{A_n}{B_n}$.

Observación 1. *Las partes* 2 *y* 4 *del Teorema 2.1.10, se pueden reescribir como*

$$C_n - C_{n-1} = \frac{(-1)^{n-1}}{B_n B_{n-1}} \quad y \quad C_n - C_{n-2} = \frac{(-1)^n q_n}{B_n B_{n-2}},$$

respectivamente, donde la primera igualdad es para $n \geq 1$ *y la segunda igualdad es para* $n \geq 2$*.*

De ahora en adelante solamente trabajaremos con fracciones continuas simples.

Observación 2. *Nótese que de la parte* 4 *del teorema 2.1.10 se tiene que si* n *es par, entonces* $C_n - C_{n-2} > 0$ *y de ahí que la sucesión de los convergentes pares es monótona creciente. También se puede ver que si* n *es impar, entonces* $C_n - C_{n-2} < 0$*, por lo que la sucesión de los convergentes impares es monótona decreciente.*

Corolario 2.1.11. *Cualquier convergente impar es mayor que cualquier convergente par, es decir,* $C_{2m-1} > C_{2n}$ *para cualquier* m*,* $n \in \mathbb{N}$*.*

DEMOSTRACIÓN. Por la Observación 2, tenemos que $C_{2m-1} > C_{2m+2n-1}$ y $C_{2m+2n} > C_{2n}$, para cualquier m y $n \in \mathbb{N}$. Luego de la parte 2 del Teorema 2.1.10, se tiene que

$$C_{2m+2n} - C_{2m+2n-1} = \frac{(-1)^{2m+2n-1}}{B_{2m+2n} B_{2m+2n-1}} < 0.$$

De todo lo anterior se obtiene lo siguiente:

$$C_{2m-1} > C_{2m+2n-1} > C_{2m+2n} > C_{2n}.$$

□

Si C_n es el *n*-ésimo convergente de $[q_0, q_1, \ldots, q_n, \ldots]$, entonces el Corolario 2.1.11 nos dice lo siguiente:

$$C_1 > C_3 > C_5 > \cdots > C_{2n+1} > C_{2n} > C_{2n-2} > \cdots > C_4 > C_2 > C_0.$$

Corolario 2.1.12. *Las sucesiones* $\{C_{2n}\}$ *y* $\{C_{2n+1}\}$ *son convergentes.*

DEMOSTRACIÓN. Como la sucesión $\{C_{2n}\}$ es monóntona creciente y por el Corolario 2.1.11 está acotada superiormente por cualquier C_{2m+1}, entonces $\{C_{2n}\}$ es convergente. Análogamente la sucesión $\{C_{2n+1}\}$ es monótona decreciente y está acotada inferiormente por cualquier C_{2m}, entonces es convergente. □

Proposición 2.1.13. *Sea* $\alpha = [q_0, q_1, \ldots, q_n, \ldots]$*. La sucesión* $\{C_n\}$ *satisface* $|\alpha - C_n| < \frac{1}{B_n^2}$.

DEMOSTRACIÓN. Sea $x = [q_{n+1}, q_{n+2}, \ldots]$. Por el Corolario 2.1.6, se sigue que $\alpha = \dfrac{xA_n + A_{n-1}}{xB_n + B_{n-1}}$. Por lo tanto

$$|\alpha - C_n| = \left|\frac{xA_n + A_{n-1}}{xB_n + B_{n-1}} - \frac{A_n}{B_n}\right| = \left|\frac{B_nA_{n-1} - A_nB_{n-1}}{B_n(xB_n + B_{n-1})}\right|$$

$$= \frac{1}{B_n(xB_n + B_{n-1})} < \frac{1}{B_n^2}.$$

□

La Proposición 2.1.13, nos dice lo siguiente:

Corolario 2.1.14. $\lim\limits_{n\to\infty}\{C_n\} = \alpha$.

DEMOSTRACIÓN. Por el Corolario 2.1.7 se tiene $B_n > n$, así que $\dfrac{1}{B_n^2} < \dfrac{1}{n^2}$. Por la Proposición 2.1.13 y por el hecho de que $\lim\limits_{n\to\infty}\dfrac{1}{n^2} = 0$, tenemos que

$$\lim_{n\to\infty}\{C_n\} = \alpha.$$

□

Como $\{C_{2n}\}$ y $\{C_{2n+1}\}$ son subsucesiones de $\{C_n\}$, entonces convergen al mismo límite de la sucesión $\{C_n\}$, esto es,

$$\lim_{n\to\infty}\{C_{2n}\} = \lim_{n\to\infty}\{C_{2n+1}\} = \lim_{n\to\infty}\{C_n\} = \alpha = [q_0, q_1, \ldots, q_n, \ldots].$$

Teorema 2.1.15. *Cualquier fracción continua simple infinita* $[q_0, q_1, \ldots, q_n, \ldots]$ *es un número irracional.*

DEMOSTRACIÓN. Es consecuencia del Corolario 2.1.14 y del Teorema 2.1.3. □

El siguiente resultado es el recíproco del Teorema 2.1.15 y nos describe un algoritmo que produce la fracción continua simple infinita que representa a un número irracional.

Definición 2.1.16. *Si* $\alpha \in \mathbb{R}$*, entonces* $\lfloor\alpha\rfloor$ *denota el mayor entero* $\leq \alpha$.

Teorema 2.1.17. ***(Algoritmo de las fracciones continuas)*** *Si* $\alpha \notin \mathbb{Q}$*, entonces* α *está representada por una fracción continua simple infinita.*

DEMOSTRACIÓN. Sea $q_0 = \lfloor \alpha \rfloor$. Como $\alpha \neq \lfloor \alpha \rfloor$, existe un único $\alpha_1 \in \mathbb{R}^+$ tal que

$$\alpha = q_0 + \frac{1}{\alpha_1}.$$

Nótese que $0 < \dfrac{1}{\alpha_1} < 1$. Sea $q_1 = \lfloor \alpha_1 \rfloor$; es claro que $q_1 \neq \alpha_1$ ya que de lo contrario $\alpha \in \mathbb{Q}$. Entonces $\alpha_1 = q_1 + \dfrac{1}{\alpha_2}$, para algún $\alpha_2 > 1$. Hasta aquí se tiene

$$\alpha = q_0 + \frac{1}{\alpha_1} = q_0 + \frac{1}{q_1 + \dfrac{1}{\alpha_2}}.$$

Este proceso es infinito, pues si para alguna i, $q_i = \alpha_i$, entonces α sería un número racional. Probemos ahora que este proceso infinito produce la fracción continua simple $[q_0, q_1, \ldots, q_n, \ldots]$ que converge a α. Es claro que $\alpha = [q_0, q_1, \ldots, q_n, \alpha_{n+1}]$. Luego como $q_{n+1} = \lfloor \alpha_{n+1} \rfloor < \alpha_{n+1}$, entonces también se tiene que

$$\alpha > [q_0, q_1, \ldots, q_n, q_{n+1}]$$

para n impar y

$$\alpha < [q_0, q_1, \ldots, q_n, q_{n+1}]$$

para n par. Así que

$$C_0 < C_2 < \cdots < C_{2n} < \cdots < \alpha < \cdots < C_{2n-1} < \cdots < C_3 < C_1,$$

donde los C_i son los convergentes de $[q_0, q_1, \ldots, q_n, \ldots]$. De ahí se deduce que $\alpha = [q_0, q_1, \ldots, q_n, \ldots]$. □

Corolario 2.1.18. *Si α es un irracional, entonces su representación como fracción continua simple es única.*

DEMOSTRACIÓN. Supongamos que $\alpha = [q_0, q_1, \ldots, q_n, \ldots] = [a_0, a_1, \ldots, a_n, \ldots]$. Así que

$$q_0 < [q_0, q_1, \ldots, q_n, \ldots] < q_0 + 1 \quad \text{y} \quad a_0 < [a_0, a_1, \ldots, a_n, \ldots] < a_0 + 1,$$

de donde

$$q_0 = \lfloor [q_0, q_1, \ldots, q_n, \ldots] \rfloor \quad \text{y} \quad a_0 = \lfloor [a_0, a_1, \ldots, a_n, \ldots] \rfloor.$$

Por lo que $\lfloor \alpha \rfloor = q_0 = a_0$, lo cual implica $[q_1, \ldots, q_n, \ldots] = [a_1, \ldots, a_n, \ldots]$. Repitiendo el argumento anterior, obtenemos $q_1 = a_1$. Luego, por inducción se obtiene que $q_i = a_i$ para $i \geq 0$. □

A continuación daremos un ejemplo de cómo hallar la representación en fracción continua simple de $\alpha \notin \mathbb{Q}$, aplicando el algoritmo de las fracciones continuas.

Ejemplo 2.1.19. *Consideremos la siguiente aproximación de* $e-1$*:*

$$e-1 \sim 1.71828182846.$$

Puesto que $e-1 \neq \lfloor e-1 \rfloor$*, tenemos*

$$e-1 \sim 1+0.71828182846 \sim 1+\frac{1}{1.39221119118}.$$

Así que $q_0 = \lfloor e-1 \rfloor = 1$*. Luego*

$$1.39221119118 = 1+0.39221119118 \sim 1+\frac{1}{2.54964677830}.$$

Entonces $q_1 = \lfloor 1.39221119118 \rfloor = 1$ *y luego*

$$2.54964677830 = 2+0.54964677830 \sim 2+\frac{1}{1.81935024360},$$

de ahí observamos que $q_2 = 2$ *y* $q_3 = 1$*. De lo anterior tenemos que*

$$e-1 \sim 1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+0.81935024360}}}.$$

Continuando de la misma manera y siguiendo la demostración del Teorema 2.1.17, podemos ver que las primeras entradas de la fracción continua simple que representa a $e-1$ *es*

$$e-1 = [1,1,2,1,1,4,1,1,6,1,1,8,1,1,10,1,1,12,1,1,14,1,1,16,\ 1,1,18,\ldots].$$

Observemos que de la demostración del Teorema 2.1.17 tenemos que si $\alpha = \alpha_0 = [q_0, q_1, \ldots, q_k, \ldots]$, entonces

$$\alpha_k = \frac{1}{\alpha_{k-1} - q_{k-1}} \quad \text{y} \quad q_{k-1} = \lfloor \alpha_{k-1} \rfloor \quad \text{para } k \in \mathbb{N}.$$

Corolario 2.1.20. *Sean* $\alpha = [q_0, q_1, \ldots, q_k, \ldots]$ *una fracción continua simple infinita y*

$$\alpha_{k+1} = \frac{1}{\alpha_k - q_k}$$

para $k \geq 0$*, donde* $\alpha = \alpha_0$*. Entonces* $\alpha_{k+1} = [q_{k+1}, q_{k+2}, \ldots]$ *para* $k \geq 0$*.*

DEMOSTRACIÓN. La prueba será por inducción sobre k. Se tiene que

$$\alpha_1 = \frac{1}{\alpha_0 - q_0} = \cfrac{1}{\cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots}}}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots}}.$$

De ahí que $\alpha_1 = [q_1, q_2, \ldots]$. Supongamos que $\alpha_k = [q_k, q_{k+1}, q_{k+2}, \ldots]$. Así que

$$\alpha_{k+1} = \frac{1}{\alpha_k - q_k} = \cfrac{1}{\cfrac{1}{q_{k+1} + \cfrac{1}{q_{k+2} + \cfrac{1}{\ddots}}}}.$$

Por lo tanto $\alpha_{k+1} = [q_{k+1}, q_{k+2}, \ldots]$. □

2.2. Irracionales Cuadráticos y Fracciones Continuas Periódicas

Ahora estudiaremos ciertos números irracionales cuya representación en fracción continua simple es periódica.

Definición 2.2.1. *Una fracción continua simple infinita $\alpha = [q_0, q_1, \ldots, q_n, \ldots]$ diremos que es **periódica** si existen $k \geq 0$ y $l \in \mathbb{N}$ tal que $q_n = q_{n+l}$ para todo $n > k$. Al menor entero l que satisface la condición anterior lo llamaremos la **longitud del período de** α y lo denotaremos por $l = l(\alpha)$.*

La definición anterior, nos dice que una fracción continua simple es periódica con longitud del período l, si

$$[q_0, q_1, \ldots, q_k, q_{k+1}, \ldots, q_{k+l}, q_{k+1}, \ldots, q_{k+l}, \ldots]$$

y la notación que usaremos es la siguiente:

$$[q_0, q_1, \ldots, q_k, \overline{q_{k+1}, \ldots, q_{k+l}}].$$

Ejemplo 2.2.2. *Consideremos $\sqrt{5}+3$ con la aproximación $\sqrt{5}+3 \sim 5\,.\,23606797750$. Por el teorema 2.1.17, se tiene que $q_0 = \lfloor \sqrt{5} + 3 \rfloor = 5$, luego*

$$\sqrt{5} + 3 \sim 5 + 0.23606797750 \sim 5 + \frac{1}{4.23606797750}$$

y

$$4.23606797750 = 4 + 0.23606797750 \sim 4 + \frac{1}{4.23606797750}.$$

De ahí se puede ver que $q_1 = q_2 = 4$.

Notemos que 0.23606797750 se seguirá repitiendo, por lo que la representación en fracción continua simple de $\sqrt{5} + 3$ es periódica con longitud del período $l(\sqrt{5} + 3) = 1$, esto es

$$\sqrt{5} + 3 = [5, 4, 4, 4, \ldots] = [5, \overline{4}].$$

Corolario 2.2.3. *Si $\alpha = [\overline{q_0, q_1, \ldots, q_n}]$, entonces α es solución de algún polinomio cuadrático en $\mathbb{Z}[x]$.*

DEMOSTRACIÓN. Notemos que α se puede escribir como $\alpha = [q_0, q_1, \ldots, q_n, \alpha]$ y por el Corolario 2.1.6 se tiene que

$$\alpha = \frac{\alpha A_n + A_{n-1}}{\alpha B_n + B_{n-1}}.$$

De donde se obtiene que $\alpha^2 B_n + \alpha(B_{n-1} - A_n) - A_{n-1} = 0$. □

Definición 2.2.4. *Un **irracional cuadrático** α es un número irracional que es raíz de algún polinomio cuadrático con coeficientes en $\mathbb{Q}$.*

Es claro que un número irracional α cuya representación en fracción continua simple es como en el Corolario 2.2.3, es un irracional cuadrático.

Veamos qué pasa si el período de la fracción continua simple no empieza desde el principio.

Corolario 2.2.5. *Sea $\alpha = [q_0, q_1, \ldots, q_n, \overline{a_1, a_2, \ldots, a_k}]$. Entonces α es un irracional cuadrático.*

DEMOSTRACIÓN. Sea $\beta = [\overline{a_1, a_2, \ldots, a_k}]$. Es claro que $\alpha = [q_0, q_1, \ldots, q_n, \beta]$ y por el Corolario 2.1.6 se tiene que

$$\alpha = \frac{\beta A_n + A_{n-1}}{\beta B_n + B_{n-1}}. \tag{10}$$

Vamos a probar que α es raíz de algún polinomio cuadrático si y sólo si β lo es.

Supongamos que $a\alpha^2 + b\alpha + c = 0$ para $a, b, c \in \mathbb{Z}$. Entonces por (10) se tiene que $a\alpha^2 + b\alpha + c = 0$ si y sólo si

$$a(\beta A_n + A_{n-1})^2 + b(\beta A_n + A_{n-1})(\beta B_n + B_{n-1}) + c(\beta B_n + B_{n-1})^2 = 0.$$

De esto se tiene que

$$\beta^2(aA_n^2 + bA_nB_n + cB_n^2) + \beta(2aA_nA_{n-1} + b(A_nB_{n-1} + A_{n-1}B_n) + 2cB_nB_{n-1}) + (aA_{n-1}^2 + bA_{n-1}B_{n-1} + cB_{n-1}^2) = 0.$$

Por lo tanto β es raíz de un polinomio cuadrático.

Por otro lado, según el Corolario 2.2.3 se tiene que β es raíz de algún polinomio cuadrático. Supongamos que $a\beta^2 + b\beta + c = 0$, para ciertos $a, b, c \in \mathbb{Z}$. De (10) se obtiene que

$$\beta = \frac{-\alpha B_{n-1} + A_{n-1}}{\alpha B_n - A_n},$$

así que

$$\alpha^2(aB_{n-1}^2 - bB_{n-1}B_n + cB_n^2) + \alpha(-2aB_{n-1}A_{n-1} + b(B_{n-1}A_n + A_{n-1}B_n) - 2cB_nA_n) + (aA_{n-1}^2 - bA_{n-1}A_n + cA_n^2) = 0.$$

De ahí que α es raíz de un polinomio cuadrático. □

Ejemplo 2.2.6. *En el Ejemplo 2.2.2, vimos que*

$$\alpha = \sqrt{5} + 3 = [5, \overline{4}].$$

Por el Corolario 2.2.5 tenemos que α es un irracional cuadrático que es raíz del polinomio

$$x^2 - 6x + 4.$$

El recíproco del Corolario 2.2.5 también se cumple, es decir, si α es un irracional cuadrático, entonces la fracción continua simple que representa a α es periódica.

Teorema 2.2.7. *Sea α un irracional cuadrático. Entonces la fracción continua simple que representa a α es periódica.*

DEMOSTRACIÓN. Ver [**5**] página 144, Teorema 177. □

En seguida veremos una manera de cómo expresar un irracional cuadrático α que involucra los coeficientes del polinomio del cual α es raíz.

Supongamos que α es un irracional cuadrático, es decir, $a\alpha^2 + b\alpha + c = 0$, para ciertos $a, b, c \in \mathbb{Z}$ $(a \neq 0)$. Entonces

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Así que podemos escribir

$$\alpha = \frac{A \pm \sqrt{B}}{C} = \frac{AC \pm \sqrt{BC^2}}{C^2} = \frac{P \pm \sqrt{d}}{Q},$$

donde $P = AC$, $d = BC^2$ y $Q = C^2$. Entonces un irracional cuadrático α se puede escribir de la forma

$$\alpha = \frac{P + \sqrt{d}}{Q}, \tag{11}$$

para ciertos $P, Q \in \mathbb{Z}$ $(Q \neq 0)$ y tal que $d > 1$ no es un cuadrado perfecto. La otra raíz $\dfrac{P - \sqrt{d}}{Q}$ de $ax^2 + bx + c$ es el **conjugado de** α y lo denotaremos como α'.

Lema 2.2.8. *Sean $d > 1$ un entero que no es un cuadrado perfecto y*

$$\alpha = \alpha_0 = \frac{P_0 + \sqrt{d}}{Q_0}$$

un irracional cuadrático. Definimos lo siguiente para $k \geq 0$

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}, \quad q_k = \lfloor \alpha_k \rfloor$$

$$P_{k+1} = q_k Q_k - P_k \quad y \quad Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}.$$

Entonces $P_k, Q_k \in \mathbb{Z}, Q_k | P_k^2 - d$, $Q_k \neq 0$ *y* $\alpha_k = [q_k, q_{k+1}, \ldots]$ *para* $k \geq 0$.

DEMOSTRACIÓN. La prueba de la primera parte del teorema será por inducción sobre k. Si $k = 0$, es claro que P_0, Q_0 son enteros distintos de cero. También tenemos del párrafo anterior que

$$P_0^2 - d = A^2C^2 - BC^2 = C^2(A^2 - B) = Q_0(A^2 - d),$$

por lo que $Q_0 | P_0^2 - d$. Supongamos que $P_k, Q_k \in \mathbb{Z}, Q_k \neq 0$ y $Q_k | P_k^2 - d$. Luego

$$P_{k+1} = q_k Q_k - P_k \in \mathbb{Z}.$$

También se tiene que

$$Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k} = \frac{d - (q_k Q_k - P_k)^2}{Q_k} = \frac{d - P_k^2}{Q_k} + (2q_k P_k - q_k^2 Q_k)$$

y por la hipótesis de inducción es claro que $Q_{k+1} \in \mathbb{Z}$ y $Q_{k+1} \neq 0$. Como $Q_{k+1} = \dfrac{d - P_{k+1}^2}{Q_k}$, entonces $Q_{k+1} | P_{k+1}^2 - d$.

Por el Corolario 2.1.20 para verificar que $\alpha_k = [q_k, q_{k+1}, \ldots]$ es suficiente mostrar que

$$\alpha_{k+1} = \frac{1}{\alpha_k - q_k},$$

pero

$$\alpha_k - q_k = \frac{P_k + \sqrt{d}}{Q_k} - q_k = \frac{\sqrt{d} - (q_k Q_k - P_k)}{Q_k} = \frac{\sqrt{d} - P_{k+1}}{Q_k} =$$

$$\frac{(\sqrt{d} - P_{k+1})(\sqrt{d} + P_{k+1})}{Q_k(\sqrt{d} + P_{k+1})} = \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} = \frac{Q_{k+1}}{\sqrt{d} + P_{k+1}} = \frac{1}{\alpha_{k+1}}.$$

□

Nótese que el Lema 2.2.8 también es un algoritmo para encontrar la representación en fracción continua simple de un irracional cuadrático α.

Ejemplo 2.2.9. *Sea* $\alpha = \alpha_0 = \dfrac{7 + \sqrt{53}}{4}$ *un irracional cuadrático. Siguiendo el Lema 2.2.8, tenemos que* $P_0 = 7$, $Q_0 = 4$ *y* $q_0 = \lfloor \alpha_0 \rfloor = 3$. *Entonces*

$$P_1 = q_0 Q_0 - P_0 = 5 \quad y \quad Q_1 = \frac{d - P_1^2}{Q_0} = 7,$$

por lo que $\alpha_1 = \dfrac{5 + \sqrt{53}}{7}$ *y* $q_1 = \lfloor \alpha_1 \rfloor = 1$. *Continuando de esta manera tenemos*

j	0	1	2	3	4	5
P_j	7	5	2	5	7	7
Q_j	4	7	7	4	1	4
q_k	3	1	1	3	14	3

.

Entonces por el Lema 2.2.8 tenemos que $\alpha_0 = [\overline{3, 1, 1, 3, 14}]$*, con longitud del período* $l(\alpha_0) = 5$.

2.2.1. Fracciones Continuas Puramente Periódicas

A continuación estudiaremos el caso en el que el período de una fracción continua simple empieza desde el principio.

Definición 2.2.10. *Una fracción continua simple infinita* α *es llamada* ***puramente periódica*** *si* $\alpha = [\overline{q_0, q_1, \ldots, q_{l-1}}]$ *con longitud del período* $l = l(\alpha)$.

Definición 2.2.11. *Un irracional cuadrático* α *se llama* ***reducido*** *si*

$$\alpha > 1 \quad y \quad -1 < \alpha' < 0.$$

Los siguientes lemas serán de ayuda para probar un teorema que relaciona los irracionales cuadráticos reducidos y las fracciones continuas simples puramente periódicas.

Lema 2.2.12. *Sea* $\alpha = \alpha_0$ *un irracional cuadrático reducido y* α_k *como en el Lema 2.2.8. Entonces* $-1 < \alpha'_k < 0$*, para* $k \geq 0$.

DEMOSTRACIÓN. La prueba será por inducción sobre k. Por hipótesis $-1 < \alpha'_0 < 0$. Ahora supongamos cierto que $-1 < \alpha'_k < 0$. Antes de seguir con la prueba, primero veamos que

$$\alpha'_{k+1} = \frac{1}{\alpha'_k - q_k}.$$

Utilizando las definiciones del Lema 2.2.8, se tiene

$$\alpha_{k+1}\alpha'_{k+1} = \frac{P_{k+1}^2 - d}{Q_{k+1}^2} = -\frac{Q_{k+1}Q_K}{Q_{k+1}^2} = -\frac{Q_k}{Q_{k+1}}.$$

De ahí

$$\begin{aligned}\alpha'_{k+1} &= -\frac{Q_k}{Q_{k+1}\alpha_{k+1}} = -\frac{Q_k}{P_{k+1} + \sqrt{d}} = \frac{Q_k}{P_k - q_k Q_k - \sqrt{d}} \\ &= \frac{1}{\dfrac{P_k - \sqrt{d} - q_k Q_k}{Q_k}} = \frac{1}{\alpha'_k - q_k}.\end{aligned}$$

Por hipótesis de inducción se obtiene

$$-(1+q_k) < \alpha'_k - q_k < -q_k$$

y de ahí $\dfrac{-1}{q_k} < \alpha'_{k+1} < \dfrac{-1}{1+q_k}$. Como $\alpha > 1$, tenemos $q_k \geq 1$ para $k \geq 0$. Por lo tanto $-1 < \alpha'_{k+1} < 0$. □

Teorema 2.2.13. *La representación en fracción continua simple de un irracional cuadrático α es puramente periódica si y sólo si α es reducido.*

DEMOSTRACIÓN. Primero supongamos que α es un irracional cuadrático reducido. Por la demostración del Lema 2.2.12 se tiene que $\dfrac{-1}{\alpha'_{k+1}} = q_k - \alpha'_k$ y por su enunciado $0 < -\alpha'_k < 1$. De ahí que

$$\left\lfloor \frac{1}{\alpha'_{k+1}} \right\rfloor = \lfloor q_k - \alpha'_k \rfloor = q_k. \tag{12}$$

Por el Teorema 2.2.7 se tiene que $\alpha_m = \alpha_n$ para ciertos $m, n \in \mathbb{N}$ con $m < n$. Entonces $\dfrac{-1}{\alpha'_m} = \dfrac{-1}{\alpha'_n}$ y por (12) se obtiene $q_{m-1} = q_{n-1}$. Por lo tanto

$$q_{m-1} + \frac{1}{\alpha_m} = q_{n-1} + \frac{1}{\alpha_n},$$

así que

$$\alpha_{m-1} = \alpha_{n-1}.$$

Continuamos de la misma manera hasta obtener $\alpha_{m-i} = \alpha_{n-i}$ para $i = 0, 1, \ldots, m$. Es decir,

$$\alpha = \alpha_0 = [\overline{q_0, q_1, \ldots, q_{m-n-1}}].$$

Ahora supongamos que la representación en fracción continua simple de α es puramente periódica, digamos $\alpha = [\overline{q_0, q_1, \ldots, q_k}]$. Entonces q_0 coincide con algún q_j, por lo que $\alpha > q_0 \geq 1$. De ahí que $\alpha > 1$. Luego por el Corolario 2.1.6

$$\alpha = \frac{\alpha A_k + A_{k-1}}{\alpha B_k + B_{k-1}}.$$

De lo cual se obtiene

$$B_k\alpha^2 + (B_{k-1} - A_k)\alpha - A_{k-1} = 0,$$

por lo tanto α es raíz de $f(x) = B_k x^2 + (B_{k-1} - A_k)x - A_{k-1}$. También se tiene que $f(\alpha') = 0$. Por otro lado

$$f(0) = -A_{k-1} < 0 \quad \text{y} \quad f(-1) = B_k - B_{k-1} + A_k - A_{k-1}.$$

Los Corolarios 2.1.7 y 2.1.8 implican que $f(-1) > 0$. Entonces por el Teorema del Valor Intermedio $-1 < \alpha' < 0$. □

Ejemplo 2.2.14. *El irracional cuadrático* $\alpha = \dfrac{7+\sqrt{53}}{4} = 3.57003$ *es reducido puesto que* $\alpha > 1$ *y*

$$-1 < \alpha' = \frac{7-\sqrt{53}}{4} = -0.0700275 < 0.$$

Por el Teorema 2.2.13 sabemos que su representación en fracción continua simple es puramente periódica. En efecto pues en el ejemplo 2.2.9 vimos que

$$\frac{7+\sqrt{53}}{4} = [\overline{3, 1, 1, 3, 14}].$$

El siguiente resultado es un un caso especial del Teorema 2.2.13

Corolario 2.2.15. *Sea* $d > 1$ *un entero que no es un cuadrado perfecto. Entonces*

$$\sqrt{d} = [q_0, \overline{q_1, \ldots, q_{l-1}, 2q_0}],$$

donde $q_j = q_{l-j}$ *para* $j = 1, 2, \ldots, l-1$ *y* $q_0 = \lfloor \sqrt{d} \rfloor$.

DEMOSTRACIÓN. Sea $\alpha = \lfloor \sqrt{d} \rfloor + \sqrt{d}$. Se tiene que α es reducido puesto que $\alpha > 1$ y $-1 < \alpha' = \lfloor \sqrt{d} \rfloor - \sqrt{d} < 0$. Entonces por el Teorema 2.2.13 la representación en fracción continua simple de α es puramente periódica, por lo que

$$\alpha = [\overline{a_0, a_1, a_2, \ldots, a_{l-1}}],$$

donde $a_0 = \lfloor \alpha \rfloor = 2\lfloor \sqrt{d} \rfloor$. Luego es claro que

$$\sqrt{d} = \alpha - \lfloor \sqrt{d} \rfloor = \left[\lfloor \sqrt{d} \rfloor, \overline{a_1, a_2, \ldots, a_{l-1}, 2\lfloor \sqrt{d} \rfloor} \right], \tag{13}$$

donde $q_0 = \lfloor \sqrt{d} \rfloor, q_1 = a_1, \ldots, q_{l-1} = a_{l-1}, q_l = 2\lfloor \sqrt{d} \rfloor = 2q_0$.

Por el Corolario 2.1.6 tenemos

$$\alpha = [a_0, a_1, \ldots, a_{l-1}, \alpha] = \frac{\alpha A_{l-1} + A_{l-2}}{\alpha B_{l-1} + B_{l-2}},$$

lo cual implica que α es raíz de

$$f(x) = B_{l-1}x^2 + (B_{l-2} - A_{l-1})x - A_{l-2}.$$

El Corolario 2.1.9 aplicado a α nos dice que

$$\frac{A_{l-1}}{A_{l-2}} = [a_{l-1}, a_{l-2}, \ldots, a_0] \quad \text{y} \quad \frac{B_{l-1}}{B_{l-2}} = [a_{l-1}, a_{l-2}, \ldots, a_1]. \tag{14}$$

Sea $\gamma = [\overline{a_{l-1}, a_{l-2}, \ldots, a_0}]$. Entonces el $(l-1)$-ésimo convergente de γ es $[a_{l-1}, a_{l-2}, \ldots, a_0]$ y el $(l-2)$-ésimo convergentes de γ es $[a_{l-1}, a_{l-2}, \ldots, a_1]$. Por el Corolario 2.1.6 y (14) se tiene

$$\gamma = \frac{\gamma A_{l-1} + B_{l-1}}{\gamma A_{l-2} + B_{l-2}}.$$

Así

$$A_{l-2}\gamma^2 + (B_{l-2} - A_{l-1})\gamma - B_{l-1} = 0$$

y reescribiendo se tiene

$$B_{l-1}\left(\frac{-1}{\gamma}\right)^2 + (B_{l-2} - A_{l-1})\left(\frac{-1}{\gamma}\right) - A_{l-2} = 0.$$

La ecuación anterior implica que $\dfrac{-1}{\gamma}$ es raíz de $f(x)$. Pero las únicas raíces de $f(x)$ son α y α', por lo que $\alpha' = \dfrac{-1}{\gamma}$. Así que

$$-\alpha' = \frac{1}{\gamma} = \frac{1}{\overline{[a_{l-1}, a_{l-2}, \ldots, a_0]}} = [0, \overline{a_{l-1}, a_{l-2}, \ldots, a_1, a_0}].$$

De (13), se obtiene

$$-\alpha' = \sqrt{d} - \lfloor\sqrt{d}\rfloor = [0, \overline{a_1, a_2, \ldots, a_{l-1}, 2\lfloor\sqrt{d}\rfloor}].$$

Por lo tanto se concluye que $q_j = a_j = a_{l-j} = q_{l-j}$ para $j = 1, \ldots, l-1$. □

Ejemplo 2.2.16. *Consideremos el irracional cuadrático $\sqrt{106}$, el cual no es reducido puesto que $-\sqrt{106} < -1$. La representación en fracción continua simple de $\sqrt{106}$ es*

$$\sqrt{106} = [10, \overline{3, 2, 1, 1, 1, 1, 2, 3, 20}],$$

donde $l(\sqrt{106}) = 9$. Notemos que $q_0 = 10$, $q_9 = 2q_0 = 20$ y $q_j = q_{9-j}$ para $j = 1, 2, \ldots, 8$, tal como lo dice el Corolario 2.2.15.

De la demostración del Corolario 2.2.15, tenemos que $\alpha = \sqrt{106} + \lfloor\sqrt{106}\rfloor$ es un irracional cuadrático reducido, en efecto puesto que

$$\alpha > 1 \quad y \quad -1 < \alpha' = \lfloor\sqrt{106}\rfloor - \sqrt{106} < 0.$$

Entonces la representación en fracción continua simple de α es puramente periódica y es como sigue

$$\alpha = \sqrt{106} + \lfloor\sqrt{106}\rfloor = [\overline{20, 3, 2, 1, 1, 1, 1, 2, 3}].$$

Capítulo 3

Divisores del Número de Clases en Campos Cuadráticos Reales

El objetivo de este capítulo es involucrar las fracciones continuas simples con el generador irracional de un ideal de un anillo cuadrático con la finalidad de encontrar algunas condiciones para el número de clases de un campo cuadrático real. Primero daremos algunas propiedades de los ideales y definiremos dos tipos de ellos: Primitivos y Reducidos. El teorema principal de este capítulo describe todos los ideales reducidos que son equivalentes a un ideal primitivo y aplicaremos este resultado para encontrar criterios de divisibilidad para el número de clases de un campo cuadrático real. Por último daremos ejemplos de campos cuadráticos reales con número de clases par, obteniendo así anillos de enteros que no son de factorización única.

3.1. El Orden O_Δ

En esta sección daremos otra notación para el anillo de enteros de un campo cuadrático.

Sea d_0 un entero libre de cuadrados y sea

$$\sigma_0 = \begin{cases} 2 & \text{si } d_0 \equiv 1 \pmod 4 \\ 1 & \text{si } d_0 \equiv 2,3 \pmod 4 \end{cases}.$$

Si $w_0 = \dfrac{\sigma_0 - 1 + \sqrt{d_0}}{\sigma_0}$ y $w_0' = \dfrac{\sigma_0 - 1 - \sqrt{d_0}}{\sigma_0}$, entonces el número $\Delta_0 = (w_0 - w_0')^2 = \dfrac{4d_0}{\sigma_0^2}$ también se puede escribir como

$$\Delta_0 = \begin{cases} d_0 & \text{si } d_0 \equiv 1 \pmod 4 \\ 4d_0 & \text{si } d_0 \equiv 2,3 \pmod 4 \end{cases}.$$

Definición 3.1.1. *Al valor Δ_0 le llamaremos* ***discriminante fundamental con radicando fundamental*** *d_0 y a w_0 le llamaremos* ***irracional fundamental principal asociado a*** *Δ_0.*

Sea $\Delta = f_\Delta^2 \Delta_0$ para algún $f_\Delta \in \mathbb{N}$. Si $g = mcd(f_\Delta, \sigma_0)$, $\sigma = \dfrac{\sigma_0}{g}$ y $d = \left(\dfrac{f_\Delta}{g}\right)^2 d_0$, entonces

$$d = \frac{f_\Delta^2 d_0}{g^2} = \frac{f_\Delta^2 d_0}{(\sigma_0/\sigma)^2} = \frac{\sigma^2 f_\Delta^2 \sigma_0^2 \Delta_0}{4\sigma_0^2} = \frac{\sigma^2 \Delta}{4}.$$

De donde $\Delta = \dfrac{4d}{\sigma^2}$, que también se puede escribir como:

$$\Delta = \begin{cases} d & \text{si} \quad \sigma = 2 \\ 4d & \text{si} \quad \sigma = 1 \end{cases}.$$

Ahora hagamos un análisis para ver cómo es d.

- Si $\sigma_0 = 2$ y f_Δ es par, entonces $d_0 \equiv 1 \pmod 4$, $g = mcd(f_\Delta, 2) = 2$. Por lo tanto $\sigma = 1$ y $d = \left(\dfrac{f_\Delta}{2}\right)^2 d_0$.
- Si $\sigma_0 = 2$ y f_Δ es impar, entonces $d_0 \equiv 1 \pmod 4$, $g = mcd(f_\Delta, 2) = 1$. Por lo tanto $\sigma = 2$ y $d = f_\Delta^2 d_0$.
- Si $\sigma_0 = 1$ y $f_\Delta \in \mathbb{N}$, entonces $d_0 \equiv 2, 3 \pmod 4$, $g = mcd(f_\Delta, 1) = 1$. Por lo tanto $\sigma = 1$ y $d = f_\Delta^2 d_0$.

De lo anterior se concluye lo siguiente:

$$d = \begin{cases} f_\Delta^2 d_0 & \text{si} \quad d_0 \equiv 1 \pmod 4 \quad \text{y} \quad f_\Delta \text{ impar} \\ f_\Delta^2 d_0 & \text{si} \quad d_0 \equiv 2, 3 \pmod 4 \\ \left(\dfrac{f_\Delta}{2}\right)^2 d_0 & \text{si} \quad d_0 \equiv 1 \pmod 4 \quad \text{y} \quad f_\Delta \text{ par} \end{cases} \tag{1}$$

y

$$\Delta = \begin{cases} d & \text{si} \quad d_0 \equiv 1 \pmod 4 \quad \text{y} \quad f_\Delta \text{ impar} \\ 4d & \text{si} \quad \sigma_0 = g \end{cases}.$$

Definición 3.1.2. *Al valor Δ le llamaremos **discriminante con conductor f_Δ y radicando** d.*

Definición 3.1.3. *Al valor $w_\Delta = \dfrac{\sigma - 1 + \sqrt{d}}{\sigma}$, le llamaremos **irracional principal asociado al discriminante** Δ.*

Es fácil ver que

$$w_\Delta = \begin{cases} \dfrac{1 + \sqrt{d}}{2} & \text{si} \quad \sigma = 2 \\ \sqrt{d} & \text{si} \quad \sigma = 1 \end{cases}$$

o equivalentemente

$$w_\Delta = \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{si} \quad \Delta = d \\ \sqrt{d} & \text{si} \quad \Delta = 4d \end{cases} .$$

Nótese que $\Delta = (w_\Delta - w'_\Delta)^2$, donde $w'_\Delta = \dfrac{\sigma - 1 - \sqrt{d}}{\sigma}$.

Utilizando (1), se puede comprobar fácilmente que $w_\Delta = f_\Delta w_0 + h$, donde $h \in \mathbb{Z}$ y es como sigue:

$$h = \begin{cases} \dfrac{1-f_\Delta}{2} & \text{si} \quad d_0 \equiv 1 \pmod 4 \quad \text{y} \quad f_\Delta \; impar \\ 0 & \text{si} \quad d_0 \equiv 2,3 \pmod 4 \\ -\dfrac{f_\Delta}{2} & \text{si} \quad d_0 \equiv 1 \pmod 4 \quad \text{y} \quad f_\Delta \text{ par} \end{cases} .$$

Recordemos del Capítulo 1, Sección 1.5 que $F = \mathbb{Q}(\sqrt{d})$ con d un entero libre de cuadrados, es un campo cuadrático. Entonces con la notación que acabamos de introducir $F = \mathbb{Q}(\sqrt{d_0}) = \mathbb{Q}(\sqrt{\Delta})$.

Si $\alpha \in F$, entonces $\alpha = a + b\sqrt{d_0}$ con $a, b \in \mathbb{Q}$ y el conjugado de α es $\alpha' = a - b\sqrt{d_0}$.

Definición 3.1.4. *Sean $\alpha, \beta \in F = \mathbb{Q}(\sqrt{d_0})$. Definimos el $\mathbb{Z}$-módulo $[\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$. Si α, β son $\mathbb{Q}$-linealmente independientes, entonces diremos que el $\mathbb{Z}$-módulo $[\alpha, \beta]$ es un **orden** en F.*

Observemos que $O_\Delta = [1, w_\Delta]$ es un orden en $F = \mathbb{Q}(\sqrt{d_0})$. Del hecho de que $w_\Delta = f_\Delta w_0 + h$, para cierta $h \in \mathbb{Z}$, se tiene que

$$O_\Delta = [1, w_\Delta] = [1, f_\Delta w_0].$$

Observación 1. *Nótese que si $f_\Delta = 1$, entonces O_Δ es el anillo de enteros de F, es decir,*

$$O_\Delta = A_F.$$

Donde A_F es como en la Proposición 1.5.2.

De acuerdo a la Proposición 1.2.6, cualquier $\mathbb{Z}$-módulo contenido en A_F tiene rango ≤ 2.

A continuación daremos algunos ejemplos, para que sea más claro todo lo anterior.

Ejemplo 3.1.5. *Sea* $\Delta = 13$. *Como* $13 \equiv 1 \pmod 4$, *entonces* $f_\Delta = 1$ *y* $\Delta = \Delta_0 = d_0$. *Por lo tanto*

$$O_{13} = [1, w_0] = \left[1, \frac{1+\sqrt{13}}{2}\right]$$

es el anillo de enteros de $F = \mathbb{Q}(\sqrt{13})$, *es decir,* $O_{13} = A_F$.

Ejemplo 3.1.6. *Sea* $\Delta = -12$. *Como* $\Delta = 4(-3)$, *entonces* $f_\Delta = 2$ *y* $\Delta_0 = -3$. *Ya que* $-3 \equiv 1 \pmod 4$, *entonces* $\Delta_0 = d_0$ *y por tanto* $w_0 = \dfrac{1+\sqrt{-3}}{2}$

Por la Proposición 1.5.2, se tiene que

$$\left[1, \frac{1+\sqrt{-3}}{2}\right]$$

es el anillo de enteros de $\mathbb{Q}(\sqrt{-3})$. *Así que*

$$O_{-12} = [1, w_\Delta] = [1, f_\Delta w_0] = [1, 1+\sqrt{-3}] = [1, \sqrt{-3}]$$

es un orden en $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{-12})$.

3.2. Ideales en O_Δ

A lo largo de esta sección vamos a describir los ideales de O_Δ y daremos algunas propiedades de sus generadores.

Teorema 3.2.1. ***(Criterio para ideales)*** *Sea* Δ *un discriminante. Sea* $(0) \neq I$ *un* $\mathbb{Z}$*-submódulo de* O_Δ. *Entonces* I *tiene una representación de la forma*

$$I = [a, b + cw_\Delta],$$

para ciertos $a, c \in \mathbb{N}$ *y* $b \in \mathbb{Z}$. *Además* I *es un ideal de* O_Δ *si y sólo si esta representación satisface que* $c|a, c|b$ *y* $ac|N(b + cw_\Delta)$.

DEMOSTRACIÓN. Como $I \subseteq O_\Delta = [1, w_\Delta] = \mathbb{Z} + \mathbb{Z}w_\Delta$, entonces $I = [\alpha_1, \alpha_2]$, donde $\alpha_1, \alpha_2 \in O_\Delta$.

Si $\gamma \in I$, entonces $\gamma = x\alpha_1 + y\alpha_2$ para ciertos $x, y \in \mathbb{Z}$. También se tiene que $\alpha_j = a_j + b_j w_\Delta$, donde $a_j, b_j \in \mathbb{Z}$ y $j = 1, 2$. Por lo que

$$\begin{aligned} \gamma &= x(a_1 + b_1 w_\Delta) + y(a_2 + b_2 w_\Delta) \\ &= (a_1 x + a_2 y) + (b_1 x + b_2 y) w_\Delta. \end{aligned} \tag{2}$$

Se observa que $I \cap \mathbb{Z} \neq (0)$. Sea $a \in I$ el menor entero racional positivo. De (2) se tiene que

$$a = x_1 a_1 + y_1 a_2 \quad \text{y tal que} \quad x_1 b_1 + y_1 b_2 = 0$$

donde $x_1, y_1 \in \mathbb{Z}$ y al menos uno de ellos es distinto de cero. Elegimos x_1, y_1 mínimos en valor absoluto con la propiedad anterior.

De todos los elementos en I, elijamos $\beta = b + cw_\Delta$ tal que $b \in \mathbb{Z}$, $c \in \mathbb{N}$ con c mínimo. De lo anterior $[a, \beta] \subseteq I$.

Nótese que de (2), c se puede escribir como una combinación lineal de b_1 y b_2. Pero como c es mínimo, entonces dicha combinación lineal es la mínima. Por lo tanto $c = mcd(b_1, b_2)$.

Por otro lado se tiene que $b_j = ct_j + r_j$ tal que $0 \leq r_j < c$ para ciertos $r_j, t_j \in \mathbb{Z}$ con $j = 1, 2$. Luego

$$\begin{aligned} \alpha_j - t_j\beta &= a_j + b_j w_\Delta - bt_j - ct_j w_\Delta \\ &= a_j - bt_j + (b_j - ct_j)w_\Delta \\ &= a_j - bt_j + r_j w_\Delta. \end{aligned} \tag{3}$$

De lo cual es claro que $\alpha_j - t_j\beta \in I$. Por lo que $r_j = 0$, ya que si $0 < r_j < c$, la igualdad (3) sería una contradicción a la minimalidad de c.

Así que $\alpha_j - t_j\beta = a_j - bt_j \in \mathbb{Z}$. También $b_j = ct_j$ con $j = 1, 2$ y de ahí obsérvese que (2) toma la forma

$$\gamma = m + cnw_\Delta, \tag{4}$$

donde $m, n \in \mathbb{Z}$.

Por el algoritmo de la división tenemos que $\alpha_j - t_j\beta = aq + s$ para ciertos $q, s \in \mathbb{Z}$ y tal que $0 \leq s < a$. Por tanto $s = \alpha_j - t_j\beta - aq \in \mathbb{Z} \cap I$. Por la minimalidad de a se tiene que $s = 0$ y así

$$\alpha_j - t_j\beta = aq.$$

De ahí es claro que $\alpha_j \in [a, \beta]$ para $j = 1, 2$. Por lo tanto $I = [a, \beta]$.

Ahora supongamos que I es un ideal. Entonces $aw_\Delta \in I$ pues $a \in I = [a, \beta]$. Por (4) se tiene que $c|a$.

Por la Definición 3.1.3 se tiene que $w_\Delta = \dfrac{\sigma - 1 + \sqrt{d}}{\sigma}$. Se puede ver fácilmente que $w_\Delta = \sigma - 1 - w'_\Delta$. Como $b + cw_\Delta \in I$, se tiene $w_\Delta(b + cw_\Delta) \in I$. Luego

$$\begin{aligned} w_\Delta(b + cw_\Delta) &= (\sigma - 1 - w'_\Delta)(b + cw_\Delta) \\ &= b(\sigma - 1) - b(\sigma - 1 - w_\Delta) + (\sigma c - c)w_\Delta - cw_\Delta w'_\Delta \\ &= -cw_\Delta w'_\Delta + (b + c(\sigma - 1))w_\Delta. \end{aligned}$$

Pero $-cw_\Delta w'_\Delta \in \mathbb{Z}$, entonces por (4) se tiene que $c|(b + c(\sigma - 1))$. De ahí que $c|b$.

Por otro lado $\left(\dfrac{b}{c} + w'_\Delta\right)(b + cw_\Delta) \in I$, pues $c|b$ y así $\left(\dfrac{b}{c} + w'_\Delta\right) \in O_\Delta$. También $\left(\dfrac{b}{c} + w'_\Delta\right)(b + cw_\Delta) = \dfrac{N(b + cw_\Delta)}{c} \in I$. Pero

$$\begin{aligned} N(b + cw_\Delta) &= (b + cw_\Delta)(b + cw'_\Delta) = b^2 + c(bw'_\Delta + bw_\Delta + cw_\Delta w'_\Delta) \\ &= b^2 + c(b(\sigma - 1) + cw_\Delta w'_\Delta). \end{aligned}$$

Como $c|b$ y $(b(\sigma-1)+cw_\Delta w'_\Delta)\in\mathbb{Z}$, tenemos $c|N(b+cw_\Delta)$. Así que

$$\frac{N(b+cw_\Delta)}{c}\in I\cap\mathbb{Z}.$$

Sea $\dfrac{N(b+cw_\Delta)}{c}=aq+r$, para ciertos $q,r\in\mathbb{Z}$ y $0\leq r<a$. Luego, $r=\dfrac{N(b+cw_\Delta)}{c}-aq\in I\cap\mathbb{Z}$. Entonces por la minimalidad de a, se tiene que $r=0$ y por lo tanto $ac|N(b+cw_\Delta)$.

Supongamos ahora que $I=[a,b+cw_\Delta]$ satisface las condiciones del teorema.

Para probar que I es un ideal en O_Δ, sólo falta probar que si $\gamma\in I$ entonces para toda $\alpha\in O_\Delta$ se tiene que $\alpha\gamma\in I$. Así que basta probar que $aw_\Delta\in I$ y que $(b+cw_\Delta)w_\Delta\in I$.

Como $c|b$ y $c|a$, se tiene que $\left(\dfrac{-b}{c}\right)a+\left(\dfrac{a}{c}\right)(b+cw_\Delta)\in I$. Luego

$$aw_\Delta=\left(\frac{-b}{c}\right)a+\left(\frac{a}{c}\right)(b+cw_\Delta)\in I.$$

Ya que $ac|N(b+cw_\Delta)$ y $\left(\sigma-1+\dfrac{b}{c}\right)\in\mathbb{Z}$, tenemos

$$\frac{-N(b+cw_\Delta)}{c}+\left(\sigma-1+\frac{b}{c}\right)(b+cw_\Delta)\in I.$$

Pero

$$\frac{-N(b+cw_\Delta)}{c}+\left(\sigma-1+\frac{b}{c}\right)(b+cw_\Delta)=\frac{-(b+cw_\Delta)(b+cw'_\Delta)+(\sigma c-c+b)(b+cw_\Delta)}{c}$$

$$=\frac{cw_\Delta(b+cw_\Delta)}{c}=bw_\Delta+cw_\Delta^2.$$

Por lo tanto $(b+cw_\Delta)w_\Delta\in I$. □

Definición 3.2.2. *A un ideal en O_Δ que satisface las condiciones del Teorema 3.2.1 le llamaremos O_Δ-**ideal**.*

Ejemplo 3.2.3. *Si $\Delta=5$, entonces $O_5=A_F=\left[1,\dfrac{1+\sqrt{5}}{2}\right]$. Por el Teorema 3.2.1*

$$I=\left[1,3\left(\frac{1+\sqrt{5}}{2}\right)\right]$$

es un $\mathbb{Z}$-submódulo de O_5, donde $a=1,b=0$ y $c=3$. Como $c\nmid a$, entonces I no es un O_5-ideal.

Observación 2. *Si $I = [a, b + cw_\Delta]$ es un O_Δ-ideal, entonces b se puede elegir de tal forma que $0 \leq b < a$. En efecto si $b = aq + r$ con $0 \leq r < a$, entonces $aq \in I$ y puesto que $b + cw_\Delta \in I$, se tiene que*

$$r + cw_\Delta = b + cw_\Delta - aq \in I.$$

De ahí es claro que $[a, r + cw_\Delta] \subseteq [a, b + cw_\Delta]$. Para la otra contención nótese que $b + cw_\Delta = aq + (r + cw_\Delta)$. Por tanto $I = [a, b + cw_\Delta] = [a, r + cw_\Delta]$, con $0 \leq r < a$. Falta mostrar que $c|r$ y $ac|N(r + cw_\Delta)$. Como $c|b$, entonces $b = cs$ para cierta $s \in \mathbb{Z}$. De ahí que $r = cs - aq$ y puesto que $c|a$ entonces es claro que $c|r$. Ahora $N(r + cw_\Delta) = r^2 + c(r(\sigma - 1) + cw_\Delta w'_\Delta)$, como $c|r$, tenemos $c|N(r + cw_\Delta)$. Análogamente a la prueba de $ac|N(b + cw_\Delta)$ en el Teorema 3.2.1, se tiene que $ac|N(r + cw_\Delta)$.

El Teorema 3.2.1 nos ayuda a distinguir $\mathbb{Z}$-submódulos en O_Δ de O_Δ-ideales. Además, describe un algoritmo para construir O_Δ-ideales:

Dado $b \in \mathbb{Z}$ y un discriminate Δ, podemos encontrar O_Δ-ideales.

- Primero hallamos los divisores positivos de b, es decir, buscamos $c \in \mathbb{N}$ tal que $c|b$. Para cada divisor podemos construir en algunos casos O_Δ-ideales.
- Luego hallamos $a \in \mathbb{N}$ con la condición $ac|N(b + cw_\Delta)$ y $c|a$.
- Adicionalmente si fuera necesario, podemos elegir b de tal forma que $0 \leq b < a$.

Ejemplo 3.2.4. *Si $\Delta = 15$, entonces $O_{15} = A_F = [1, \sqrt{15}]$. Sea $b = 3$. Entonces para el divisor $c = 3$, construyamos un O_{15}-ideal. Así que*

$$b + cw_\Delta = 3 + 3\sqrt{15}$$

y

$$N(3 + 3\sqrt{15}) = (3 + 3\sqrt{15})(3 - 3\sqrt{15}) = -126.$$

Para $a = 6$, se cumple que

$$ac|N(3 + 3\sqrt{15}) \text{ y que } c|a.$$

Entonces por el Teorema 3.2.1

$$I = [6, 3 + 3\sqrt{15}]$$

es un O_{15}-ideal. Para el divisor $c = 1$, $b + cw_\Delta = 3 + \sqrt{15}$ y

$$N(3 + \sqrt{15}) = (3 + \sqrt{15})(3 - \sqrt{15}) = -6.$$

Notemos que para $a = 1, 2, 3, 6$, los $I = [a, 3 + \sqrt{15}]$ van a ser O_{15}-ideales, puesto que $c = 1$.

Por ejemplo, si $a = 2$, se cumple que $ac|N((3+\sqrt{15}))$, $c|a$ y $c|b$. Como $b > a$, por la Observación 2 se tiene que

$$I = [2, 1 + \sqrt{15}]$$

es un O_{15}-ideal.

Lema 3.2.5. *Sea $I = [A + Bw_\Delta, C + Dw_\Delta]$ un $\mathbb{Z}$-submódulo de O_Δ, donde $A, B, C, D \in \mathbb{Z}$. Entonces $I = [(A + Bw_\Delta) \pm n(C + Dw_\Delta), C + Dw_\Delta] = [A + Bw_\Delta, (C + Dw_\Delta) \pm n(A + Bw_\Delta)]$, para toda $n \in \mathbb{Z}$.*

DEMOSTRACIÓN. Es claro que

$$[(A + Bw_\Delta) \pm n(C + Dw_\Delta), C + Dw_\Delta] \subseteq [A + Bw_\Delta, C + Dw_\Delta].$$

La otra contención se sigue de

$$A + Bw_\Delta = (A + Bw_\Delta) \pm n(C + Dw_\Delta) \mp n(C + Dw_\Delta).$$

□

Con el Lema 3.2.5, podemos alterar los generadores de un $\mathbb{Z}$-submódulo para obtener la forma que asegura el Teorema 3.2.1.

Corolario 3.2.6. *Sea $I = [A + Bw_\Delta, C + Dw_\Delta]$ un $\mathbb{Z}$-submódulo de O_Δ donde $A, B, C, D \in \mathbb{Z}$. Entonces $I = [A_0, B_0 + C_0 w_\Delta]$ donde $A_0, B_0, C_0 \in \mathbb{Z}$ y $C_0 = mcd(B, D)$.*

DEMOSTRACIÓN. Supongamos que $D > B$. Mediante el algoritmo de Euclides hallemos el $mcd(B, D)$:

$$\begin{aligned}
D &= q_0 B + r_1 && 0 \le r_1 < |B| \\
B &= q_1 r_1 + r_2 && 0 \le r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 && 0 \le r_3 < r_2 \\
\vdots &= \vdots && \vdots \\
r_{k-1} &= q_k r_k + r_{k+1} && 0 \le r_{k+1} < r_k \\
r_k &= q_{k+1} r_{k+1} + 0. &&
\end{aligned} \tag{5}$$

Entonces $mcd(B, D) = r_{k+1}$. Luego aplicando el Lema 3.2.5 y (5) se tiene que

$$\begin{aligned}
I &= [A + Bw_\Delta, C + Dw_\Delta] = [A + Bw_\Delta, (C + Dw_\Delta) - q_0(A + Bw_\Delta)] \\
&= [A + Bw_\Delta, A_1 + r_1 w_\Delta] \qquad \text{donde} \quad A_1 = C - q_0 A.
\end{aligned}$$

Luego

$$\begin{aligned}
I &= [A + Bw_\Delta, A_1 + r_1 w_\Delta] = [(A + Bw_\Delta) - q_1(A_1 + r_1 w_\Delta), A_1 + r_1 w_\Delta] \\
&= [A_2 + r_2 w_\Delta, A_1 + r_1 w_\Delta] \qquad \text{donde} \quad A_2 = A - q_1 A_1.
\end{aligned}$$

Continuando de esta manera se tiene lo siguiente

$$\begin{aligned} I &= [A_k + r_{k-1}w_\Delta, A_{k+1} + r_k w_\Delta] \\ &= [(A_k + r_{k-1}w_\Delta) - q_k(A_{k+1} + r_k w_\Delta), A_{k+1} + r_k w_\Delta] \\ &= [A_{k+2} + r_{k+1}w_\Delta, A_{k+1} + r_k w_\Delta] \qquad \text{donde} \quad A_{k+2} = A_k - q_k A_{k+1} \end{aligned}$$

y por último

$$\begin{aligned} I &= [A_{k+2} + r_{k+1}w_\Delta, A_{k+1} + r_k w_\Delta] \\ &= [A_{k+2} + r_{k+1}w_\Delta, (A_{k+1} + r_k w_\Delta) - q_{k+1}(A_{k+2} + r_{k+1}w_\Delta)] \\ &= [A_{k+2} + r_{k+1}w_\Delta, A_{k+3}] = [A_{k+2} + mcd(B, D)w_\Delta, A_{k+3}] \end{aligned}$$

donde $A_{k+3} = A_{k+1} - q_{k+1}A_{k+2}$.

Por lo tanto $I = [A_0, B_0 + C_0 w_\Delta]$ donde $A_0 = A_{k+3}, B_0 = A_{k+2}$ y $C_0 = mcd(B, D)$. □

3.2.1. Ideales Primitivos y Norma

En la demostración del Teorema 3.2.1 vimos que si $I = [a, b + cw_\Delta]$ es un O_Δ-ideal, entonces a es el menor entero racional positivo en I.

Definición 3.2.7. *Sean Δ un discriminante, $I = [a, b + cw_\Delta]$ un O_Δ-ideal. Definimos la* ***norma de*** *I como $N(I) = ac$. Si $c = 1$, diremos que I es un O_Δ-**ideal primitivo**.*

Por la Definición 3.2.7 la norma de un O_Δ-ideal primitivo I es el menor entero racional positivo en I, es decir, $N(I) = a$.

El siguiente teorema prueba que la definición de norma de un O_Δ-ideal coincide con la Definición 1.4.6 de norma de un ideal del Capítulo 1.

Teorema 3.2.8. *Sea $I = [a, b + cw_\Delta]$ un O_Δ-ideal. Entonces $|O_\Delta/I| = ac$.*

DEMOSTRACIÓN. Sea $z_1 + z_2 w_\Delta \in O_\Delta$. Así que $(z_1 + z_2 w_\Delta) + I \in O_\Delta/I$. Supongamos que $z_2 = cq_1 + r_1$ con $0 \leq r_1 < c$. Luego como $(b + cw_\Delta)q_1 \in I$, se tiene lo siguiente:

$$\begin{aligned} (z_1 + z_2 w_\Delta) + I &= (z_1 + (cq_1 + r_1)w_\Delta) + I \\ &= (z_1 + (cq_1 + r_1)w_\Delta) - (b + cw_\Delta)q_1 + I \\ &= (z_1 - bq_1) + r_1 w_\Delta + I. \end{aligned}$$

Dividiendo entre a tenemos que $z_1 - bq_1 = aq_2 + r_2$ con $0 \leq r_2 < a$. De ahí y por el hecho que $aq_2 \in I$ se tiene que

$$(z_1 + z_2 w_\Delta) + I = aq_2 + r_2 + r_1 w_\Delta + I = (r_2 + r_1 w_\Delta) + I.$$

Entonces $(z_1 + z_2 w_\Delta) + I = (r_2 + r_1 w_\Delta) + I$, donde $0 \leq r_1 < c$ y $0 \leq r_2 < a$. Por lo tanto hay a lo más ac elementos en O_Δ/I. Ahora probemos que todos esos elementos son distintos.

Sean $(r_2 + r_1 w_\Delta) + I$, $(r_2' + r_1' w_\Delta) + I$ elementos de O_Δ/I tal que $0 \leq r_2, r_2' < a$, $0 \leq r_1, r_1' < c$.

Supongamos que $(r_2 + r_1 w_\Delta) + I = (r_2' + r_1' w_\Delta) + I$. De ahí se tiene que $(r_2 - r_2') + (r_1 - r_1')w_\Delta \in I$. Entonces

$$(r_2 - r_2') + (r_1 - r_1')w_\Delta = as + (b + cw_\Delta)t, \tag{6}$$

para ciertos $s, t \in \mathbb{Z}$. De lo anterior $r_1 - r_1' = ct$. Puesto que $-c < r_1 - r_1' < c$, se tiene que $t = 0$ y así $r_1 = r_1'$. De ahí y por (6), $r_2 - r_2' = as$. Ya que $-a < r_2 - r_2' < a$, se tiene que $s = 0$ y así $r_2 = r_2'$. □

Corolario 3.2.9. *Si $I = [1, b + w_\Delta]$ es un O_Δ-ideal, entonces $I = O_\Delta$.*

□

Observación 3. *Si $I = [A + Bw_\Delta, A' + B'w_\Delta]$ es un $\mathbb{Z}$-submódulo de O_Δ, entonces por el Lema 3.2.5 se tiene que*

$$\begin{aligned} I &= [(A + Bw_\Delta) \pm n(A' + B'w_\Delta), A' + B'w_\Delta] \\ &= [(A \pm nA') + (B \pm nB')w_\Delta, A' + B'w_\Delta] \end{aligned}$$

para toda $n \in \mathbb{Z}$. Por otro lado

$$\begin{aligned} |AB' - A'B| &= \left|\det \begin{pmatrix} A & B \\ A' & B' \end{pmatrix}\right| = \left|\det \begin{pmatrix} A \pm nA' & B \pm nB' \\ A' & B' \end{pmatrix}\right| \\ &= |(A \pm nA')B' - A'(B \pm nB')|. \end{aligned}$$

Es decir

$$|AB' - A'B| = |(A \pm nA')B' - A'(B \pm nB')|. \tag{7}$$

De ahí se ve que $|AB' - A'B|$ es constante en todos los pasos del Corolario 3.2.6. También por el Corolario 3.2.6 se llega a un momento en el que

$$I = [A_0, B_0 + C_0 w_\Delta].$$

En particular si I es un O_Δ-ideal, por la definición 3.2.7 se tiene que $N(I) = A_0C_0$. Por (7) se tiene lo siguiente:

$$A_0C_0 = \left|\det \begin{pmatrix} A_0 & 0 \\ B_0 & C_0 \end{pmatrix}\right| = |AB' - A'B|.$$

Por lo tanto si $I = [A + Bw_\Delta, A' + B'w_\Delta]$ es un ideal en O_Δ, entonces $N(I) = |AB' - A'B|$.

Para calcular la norma de un ideal en O_Δ no es necesario que esté escrito en la forma de O_Δ-ideal.

Teorema 3.2.10. *Sea $\alpha \in O_\Delta$ y sea I un O_Δ-ideal. Si $J = (\alpha)I$, entonces $N(J) = |N(\alpha)|N(I)$.*

DEMOSTRACIÓN. Primero hagamos la prueba para el caso $w_\Delta = \sqrt{d}$. Si $\alpha \in O_\Delta$, entonces $\alpha = z_1 + z_2 w_\Delta$ para ciertos $z_1, z_2 \in \mathbb{Z}$. Sea $I = [a, b+cw_\Delta]$ un O_Δ-ideal. Entonces

$$\begin{aligned}(\alpha)I &= (z_1 + z_2 w_\Delta)[a, b + cw_\Delta] = [az_1 + az_2 w_\Delta, (z_1 + z_2 w_\Delta)(b + cw_\Delta)] \\ &= [az_1 + az_2 w_\Delta, (bz_1 + cz_2 d) + (bz_2 + cz_1)w_\Delta]. \qquad (8)\end{aligned}$$

Por otra parte se tiene que $|N(\alpha)| = |N(z_1 + z_2 w_\Delta)| = |z_1^2 - z_2^2 d|$ y $N(I) = ac$. Así que $|N(\alpha)|N(I) = |z_1^2 - z_2^2 d|ac$.

Nótese que de (8) tenemos que $(\alpha)I = [A + Bw_\Delta, A' + B'w_\Delta]$, donde

$$A = az_1, \qquad B = az_2, \qquad A' = bz_1 + cz_2 d \quad \text{y} \quad B' = bz_2 + cz_1.$$

Entonces hallemos $N(J)$ utilizando la Observación 3, es decir, calculemos $|AB' - A'B|$:

$$\begin{aligned}|AB' - A'B| &= |az_1(bz_2 + cz_1) - (bz_1 + cz_2 d)az_2| = |acz_1^2 - acz_2^2 d| \\ &= ac|z_1^2 - z_2^2 d|.\end{aligned}$$

Por lo tanto $N(J) = |N(\alpha)|N(I)$.

Ahora hagamos la prueba para el caso $w_\Delta = \dfrac{1+\sqrt{d}}{2}$. Entonces

$$\begin{aligned}(\alpha)I &= [az_1 + az_2 w_\Delta, (z_1 + z_2 w_\Delta)(b + cw_\Delta)] \\ &= \left[az_1 + az_2 w_\Delta, bz_1 + (cz_1 + bz_2)w_\Delta + cz_2\left(\frac{1 + 2\sqrt{d} + d}{4}\right)\right] \\ &= \left[az_1 + az_2 w_\Delta, bz_1 + (cz_1 + bz_2)w_\Delta + cz_2\left(\frac{1+\sqrt{d}}{2} + \frac{d-1}{4}\right)\right].\end{aligned}$$

Como en este caso $d \equiv 1 \pmod 4$, entonces $(d-1)/4 \in \mathbb{Z}$ y así

$$(\alpha)I = \left[az_1 + az_2 w_\Delta, bz_1 + \frac{cz_2(d-1)}{4} + (cz_1 + bz_2 + cz_2)w_\Delta\right]. \qquad (9)$$

Por otro lado tenemos que $|N(\alpha)| = \left|\dfrac{z_2^2(1-d) + 4z_1(z_1+z_2)}{4}\right|$ y $N(I) = ac$. De ahí que

$$|N(\alpha)|N(I) = \left|\frac{z_2^2(1-d) + 4z_1(z_1+z_2)}{4}\right| ac.$$

De (9) se puede ver que $(\alpha)I = [A + Bw_\Delta, A' + B'w_\Delta]$, donde

$$A = az_1, \quad B = az_2, \quad A' = bz_1 + \frac{cz_2(d-1)}{4} \quad \text{y} \quad B' = cz_1 + bz_2 + cz_2.$$

Calculemos entonces

$$\begin{aligned}|AB' - A'B| &= \left| az_1(cz_1 + bz_2 + cz_2) - \left(bz_1 + \frac{cz_2(d-1)}{4}\right) az_2 \right| \\ &= \left| \frac{ac(4z_1^2 + 4z_1z_2 - dz_2^2 + z_2^2)}{4} \right| \\ &= ac \left| \frac{z_2^2(1-d) + 4z_1(z_1+z_2)}{4} \right|.\end{aligned}$$

De ahí es claro que $|AB' - A'B| = |N(\alpha)|N(I)$ y por la Observación 3 se tiene que

$$N(J) = |AB' - A'B| = |N(\alpha)|N(I). \quad \square$$

Corolario 3.2.11. *Si $I = (\alpha)$, entonces $N(I) = |N(\alpha)|$.*

DEMOSTRACIÓN. Se tiene que $I = (\alpha)O_\Delta$. Como $O_\Delta = [1, w_\Delta]$, entonces $N(O_\Delta) = 1$. Así que utilizando el Teorema 3.2.10, se tiene el resultado. $\square$

Observación 4. *Si $I = [A + Bw_\Delta, A' + B'w_\Delta]$ es un ideal en O_Δ, entonces*

$$I = [A + Bw_\Delta, A' + B'w_\Delta] = \left[\frac{N(I)}{mcd(B, B')}, (Al_1 + A'l_2) + mcd(B, B')w_\Delta \right],$$

donde $mcd(B, B') = Bl_1 + B'l_2$.

El siguiente teorema explica el interés en O_Δ-ideales primitivos.

Teorema 3.2.12. *Si J es un O_Δ-ideal, entonces existe un O_Δ-ideal primitivo I tal que $J \sim I$.*

DEMOSTRACIÓN. Sea $J = [a, b + cw_\Delta]$. Entonces

$$J = (c)\left[\frac{a}{c}, \frac{b}{c} + w_\Delta\right]. \tag{10}$$

Sea $I = \left[\frac{a}{c}, \frac{b}{c} + w_\Delta\right]$. Como J es un O_Δ-ideal, entonces $\frac{a}{c} \in \mathbb{N}$, $\frac{b}{c} \in \mathbb{Z}$. Para que I sea un O_Δ-ideal sólo basta ver que $\frac{a}{c} \mid N\left(\frac{b}{c} + w_\Delta\right)$. Así

$$N\left(\frac{b}{c} + w_\Delta\right) = \left(\frac{1}{c^2}\right) N(b + cw_\Delta). \tag{11}$$

Como J es un O_Δ-ideal, se tiene que $N(b + cw_\Delta) = acq$ para cierto $q \in \mathbb{Z}$, así sustituyendo en (11), se obtiene que

$$N\left(\frac{b}{c} + w_\Delta\right) = \frac{acq}{c^2} = \frac{aq}{c},$$

es decir, $\frac{a}{c} \mid N\left(\frac{b}{c} + w_\Delta\right)$. Es claro que I es primitivo. Por (10) se tiene que $(1)J = (c)I$, lo que nos dice que $J \sim I$. □

Por el Lema 3.2.5 un O_Δ-ideal primitivo tiene varias representaciones, así que tiene sentido dar una representación canónica. Para esto primero veamos la siguiente observación.

Observación 5. *Sea $I = [a, b + w_\Delta]$ un O_Δ-ideal primitivo. Si $w_\Delta = \frac{1+\sqrt{d}}{2}$, entonces $\Delta = d$ y así*

$$I = \left[a, b + \frac{1+\sqrt{d}}{2}\right] = \left[a, \frac{2b+1+\sqrt{\Delta}}{2}\right].$$

De lo cual se tiene que

$$I = \left[a, \frac{b_1+\sqrt{\Delta}}{2}\right],$$

donde $b_1 = 2b + 1 \in \mathbb{Z}$.

Si $w_\Delta = \sqrt{d}$, entonces $\Delta = 4d$ y así

$$I = [a, b + \sqrt{d}] = \left[a, b + \sqrt{\frac{\Delta}{4}}\right] = \left[a, \frac{2b+\sqrt{\Delta}}{2}\right].$$

Es decir,

$$I = \left[a, \frac{b_1+\sqrt{\Delta}}{2}\right]$$

donde $b_1 = 2b \in \mathbb{Z}$. Se puede ver que en ambos casos un O_Δ-ideal primitivo se puede escribir como

$$I = \left[a, \frac{b_1+\sqrt{\Delta}}{2}\right], \tag{12}$$

con $b_1 \in \mathbb{Z}$.

Corolario 3.2.13. *Sea Δ un discriminante y sea $I = \left[a, \frac{b_1+\sqrt{\Delta}}{2}\right]$ un O_Δ-ideal primitivo como en (12). Entonces $I = \left[a, na \pm \frac{b_1+\sqrt{\Delta}}{2}\right]$ para toda $n \in \mathbb{Z}$.*

DEMOSTRACIÓN. La contención $\left[a, na \pm \frac{b_1+\sqrt{\Delta}}{2}\right] \subseteq \left[a, \frac{b_1+\sqrt{\Delta}}{2}\right]$ es clara. La otra contención se tiene puesto que $\frac{b_1+\sqrt{\Delta}}{2} = na - na + \frac{b_1+\sqrt{\Delta}}{2}$. □

Notemos que

$$I = \left[a, na \pm \frac{b_1 + \sqrt{\Delta}}{2}\right] = \left[a, \frac{b + \sqrt{\Delta}}{2}\right],$$

donde $b = 2na \pm b_1$.

Definición 3.2.14. *Sea* $I = \left[a, \dfrac{b + \sqrt{\Delta}}{2}\right]$ *un* O_Δ*-ideal primitivo como en el Corolario 3.2.13. Si*

$$-N(I) = -a \leq tr\left(\frac{b + \sqrt{\Delta}}{2}\right) < a = N(I),$$

entonces diremos que la representación de I *es canónica.*

Si I está representado en forma canónica, ésta es única.

Teorema 3.2.15. *(Unicidad). Sea* $I = [N(I), \alpha]$ *un* O_Δ*-ideal primitivo, donde* $\alpha = \dfrac{b_1 + \sqrt{\Delta}}{2}$ *y tal que* $-N(I) \leq tr(\alpha) = b_1 < N(I)$*. Si existe* $\beta = \dfrac{b_2 + \sqrt{\Delta}}{2} \in O_\Delta$*, tal que* $I = [N(I), \beta]$ *y* $-N(I) \leq tr(\beta) = b_2 < N(I)$*, entonces* $\alpha = \beta$*.*

DEMOSTRACIÓN. Supongamos que $I = [N(I), \alpha] = [N(I), \beta]$. Entonces se tiene que $\alpha = nN(I) + m\beta$ para ciertos $n, m \in \mathbb{Z}$, así que

$$\begin{aligned}\frac{b_1 + \sqrt{\Delta}}{2} &= nN(I) + \frac{m(b_2 + \sqrt{\Delta})}{2} \\ &= \left(nN(I) + \frac{mb_2}{2}\right) + \frac{m\sqrt{\Delta}}{2}.\end{aligned}$$

Como $\sqrt{\Delta}$ es irracional, $\{1, \sqrt{\Delta}\}$ es $\mathbb{Q}$-linealmente independiente. Por lo que $\dfrac{1}{2} = \dfrac{m}{2}$ y de ahí que $m = 1$. Por lo tanto $\alpha = nN(I) + \beta$. Ahora mostremos que $n = 0$.

Si $n > 0$, se tiene que

$$tr(\alpha) = 2nN(I) + tr(\beta) \geq 2N(I) + tr(\beta) \geq 2N(I) - N(I) = N(I).$$

Es decir, $tr(\alpha) \geq N(I)$, lo cual es una contradicción.

Si $n < 0$, se tiene que

$$\begin{aligned}tr(\beta) &= tr(\alpha) - 2nN(I) = tr(\alpha) + 2|n|N(I) \geq tr(\alpha) + 2N(I) \\ &\geq 2N(I) - N(I) = N(I).\end{aligned}$$

Es decir, $tr(\beta) \geq N(I)$, lo cual también es una contradicción. Por lo tanto $n = 0$ y entonces $\alpha = \beta$. □

Observación 6. *Sea* $I = \left[a, \dfrac{b_1+\sqrt{\Delta}}{2}\right]$ *un* O_Δ*-ideal primitivo como en la Observación 5, con* $b_1 = 2b+1$ *o* $2b$ *y* $0 \leq b < a$ *como en la Observación 2. Supongamos que* I *no está en forma canónica, es decir,*

$$N(I) \leq tr\left(\frac{b_1+\sqrt{\Delta}}{2}\right) = b_1 \quad o \quad b_1 = tr\left(\frac{b_1+\sqrt{\Delta}}{2}\right) < -N(I).$$

Si $b_1 = 2b+1$*. Supongamos que* $b_1 < -N(I) = -a$*. De ahí* $2b+1 < -a \leq -1$*, de donde* $b < 0$*, lo cual no puede ser puesto que* $0 \leq b < a$*. Por tanto* $b_1 \geq N(I) = a$*. De ahí* $2b+1 \geq 2a-a$*, de donde*

$$2b+1-2a \geq -a.$$

También se tiene que $2b+1 < 2a+1 \leq 2a+a$*, es decir,* $2b+1-2a < a$*.*

Si $b_1 = 2b$*. Supongamos que* $2b < -a$*. De ahí* $2b < -a \leq -1$*, de donde* $b < 0$*, lo cual no puede ser puesto que* $0 \leq b < a$*. Por tanto* $2b \geq a$*, por lo que* $2b-2a \geq a-2a$*, es decir,*

$$2b-2a \geq -a.$$

También se tiene que $2b < 2a < 2a+a$*, de donde,* $2b-2a < a$*.*

En ambos casos I *siempre se puede escribir en forma canónica.*

Ejemplo 3.2.16. *Sea* $\Delta = 17$*, entonces* $O_{17} = A_F = \left[1, \dfrac{1+\sqrt{17}}{2}\right]$*. Sea*

$$I = \left[4, 3+\frac{1+\sqrt{17}}{2}\right] = \left[4, \frac{7+\sqrt{17}}{2}\right]$$

un O_{17}*-ideal primitivo. Por el Corolario 3.2.13, se tiene que*

$$I = \left[4, \frac{7+\sqrt{17}}{2}\right] = \left[4, \frac{15+\sqrt{17}}{2}\right] = \left[4, \frac{23+\sqrt{17}}{2}\right] = \cdots$$
$$= \left[4, \frac{-1+\sqrt{17}}{2}\right] = \left[4, \frac{-9+\sqrt{17}}{2}\right] = \left[4, \frac{-17+\sqrt{17}}{2}\right] = \cdots$$

Por la Observación 6, $I = \left[4, -4+\dfrac{7+\sqrt{17}}{2}\right] = \left[4, \dfrac{-1+\sqrt{17}}{2}\right]$*, es la representación canónica de* I*. En efecto, pues*

$$-4 < tr\left(\frac{-1+\sqrt{17}}{2}\right) = -1 < 4 = N(I).$$

Notemos que para cualquier otra elección de b*,*

$$\left|tr\left(\frac{b+\sqrt{17}}{2}\right)\right| > N(I) = 4.$$

3.3. Fracciones Continuas Aplicadas a Campos Cuadráticos Reales

Ahora vamos a relacionar las fracciones continuas simples con el generador irracional de un O_Δ-ideal Primitivo. Esto nos ayudará a probar que todo O_Δ-ideal primitivo es equivalente a un ideal que llamaremos reducido. Luego daremos un criterio de divisibilidad para el número de clases de un campo cuadrático real y con esto daremos ejemplos de anillos cuadráticos que no son de factorización única.

Primero se hará un cambio de notación del O_Δ-ideal primitivo y veremos que uno de sus generadores es un irracional cuadrático de los cuales ya sabemos exactamente como es su fracción continua simple.

De aquí en adelante $\Delta = \Delta_0$, es decir, O_Δ es el anillo de enteros.

Sea $I = [a, b + w_\Delta]$ un O_Δ-ideal primitivo y

$$\sigma = \begin{cases} 2 & \text{si} \quad d \equiv 1 \pmod 4 \\ 1 & \text{si} \quad d \equiv 2 \text{ ó } 3 \pmod 4 \end{cases}.$$

Escribimos $\sigma a = Q$ y $b = \begin{cases} \dfrac{P-1}{2} & \text{si} \quad \sigma = 2 \\ P & \text{si} \quad \sigma = 1, \end{cases}$

donde $P \in \mathbb{Z}$ y $Q \in \mathbb{N}$.

Observemos que si $\sigma = 2$, se tiene

$$I = \left[\frac{Q}{2}, \frac{P-1}{2} + \frac{1+\sqrt{d}}{2}\right] = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right],$$

y si $\sigma = 1$, se tiene

$$I = \left[Q, P + \sqrt{d}\right] = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right].$$

Nótese que ambos casos

$$I = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right]. \tag{13}$$

Ejemplo 3.3.1. *Sea* $A_F = O_\Delta = \left[1, \dfrac{1+\sqrt{33}}{2}\right]$ *y sea* $I = \left[4, 3 + \dfrac{1+\sqrt{33}}{2}\right]$ *un* O_Δ*-ideal primitivo. Ya que* $33 \equiv 1 \pmod 4$*, se tiene que* $\sigma = 2$*, por lo que*

- $Q = \sigma a = 2 \cdot 4 = 8$
- $P = 2b + 1 = 7$.

Por lo tanto $I = \left[\dfrac{8}{2}, \dfrac{7+\sqrt{33}}{2}\right]$.

Con las definiciones de σ, P y Q que se establecieron al principio de esta sección, tenemos una pregunta inmediata: ¿Si $I = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right]$, entonces I es un O_Δ-ideal primitivo? La respuesta es afirmativa bajo cierta condición como veremos enseguida.

Teorema 3.3.2. *$I = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right]$ es un O_Δ-ideal primitivo si y sólo si $P^2 \equiv d \pmod{\sigma Q}$.*

DEMOSTRACIÓN. Supongamos que $P^2 \equiv d \pmod{\sigma Q}$. Si $\sigma = 2$ veamos que $I = \left[\frac{Q}{2}, \frac{P-1}{2} + \frac{1+\sqrt{d}}{2}\right]$ es un O_Δ-ideal. Por el Teorema 3.2.1, debemos mostrar que $\frac{Q}{2} \mid N\left(\frac{P+\sqrt{d}}{2}\right)$. Puesto que $P^2 \equiv d \pmod{2Q}$ se tiene

$$N\left(\frac{P+\sqrt{d}}{2}\right) = \frac{P^2-d}{4} = \frac{2Qr}{4} = \frac{Q}{2}\cdot r \tag{14}$$

para algún $r \in \mathbb{Z}$, luego $\frac{Q}{2} \mid N\left(\frac{P+\sqrt{d}}{2}\right)$.

Ahora si $\sigma = 1$, veamos que $I = \left[Q, P+\sqrt{d}\right]$ es un O_Δ-ideal. Por el Teorema 3.2.1, basta ver que $Q|N\left(P+\sqrt{d}\right)$. Puesto que $P^2 \equiv d \pmod{Q}$, tenemos que

$$N\left(P+\sqrt{d}\right) = P^2 - d = Qr,$$

para algún $r \in \mathbb{Z}$, luego $Q|N\left(P+\sqrt{d}\right)$. Claramente en ambos casos I es primitivo.

Supongamos ahora que $I = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right]$ es un O_Δ-ideal primitivo.

Si $\sigma = 2$, se tiene que $I = \left[\frac{Q}{2}, \frac{P+\sqrt{d}}{2}\right]$. Por el Teorema 3.2.1 tenemos que $\frac{Q}{2} \mid N\left(\frac{P+\sqrt{d}}{2}\right)$, es decir, $\frac{P^2-d}{4} = \frac{Q}{2}t$ para cierta $t \in \mathbb{Z}$. De donde

$$P^2 - d = 2Qt, \text{ por lo que } P^2 \equiv d \pmod{2Q}.$$

Si $\sigma = 1$, por el Teorema 3.2.1, $Q|N\left(P+\sqrt{d}\right)$ y por tanto $P^2 \equiv d \pmod{Q}$. □

Lema 3.3.3. *$\dfrac{P+\sqrt{d}}{\sigma Q}$ es un irracional cuadrático si y sólo si $\dfrac{P+\sqrt{d}}{Q}$ es un irracional cuadrático.*

DEMOSTRACIÓN. Basta hacer la prueba para $\sigma = 2$. Sea $\alpha = \dfrac{P+\sqrt{d}}{Q}$ y supongamos que α es un irracional cuadrático. Así que α es raíz del polinomio $x^2 - tr(\alpha)x + N(\alpha)$, por lo que $\alpha^2 - tr(\alpha)\alpha + N(\alpha) = 0$. Luego por la Proposición 1.1.3 del Capítulo 1

$$\left(\frac{\alpha}{2}\right)^2 - \left(tr\left(\frac{\alpha}{2}\right)\right)\frac{\alpha}{2} + N\left(\frac{\alpha}{2}\right) = \frac{\alpha^2}{4} - \frac{1}{2}tr(\alpha)\frac{\alpha}{2} + \left(\frac{1}{2}\right)^2 N(\alpha)$$
$$= \frac{\alpha^2}{4} - \frac{tr(\alpha)\alpha}{4} + \frac{N(\alpha)}{4} = 0.$$

Por lo que $\dfrac{\alpha}{2} = \dfrac{P+\sqrt{d}}{2Q}$ satisface el polinomio $y^2 - tr\left(\dfrac{\alpha}{2}\right)y + N\left(\dfrac{\alpha}{2}\right)$, luego $\dfrac{P+\sqrt{d}}{2Q}$ es un irracional cuadrático.

La prueba de que si $\dfrac{P+\sqrt{d}}{2Q}$ es un irracional cuadrático implica que $\dfrac{P+\sqrt{d}}{Q}$ es un irracional cuadrático es análoga a la anterior. □

Por (11) del Capítulo 2, el Teorema 3.3.2 y el Lema 3.3.3 nos dicen que $I = \left[\dfrac{Q}{\sigma}, \dfrac{P+\sqrt{d}}{\sigma}\right]$ es un O_Δ-ideal primitivo si y sólo si $\dfrac{P+\sqrt{d}}{\sigma Q}$ es un irracional cuadrático si y sólo si $\dfrac{P+\sqrt{d}}{Q}$ es un irracional cuadrático.

De lo anterior, existe una función entre el conjunto de irracionales cuadráticos y el conjunto de los O_Δ-ideales primitivos. Dicha función está dada por:

$$\alpha \longrightarrow [\alpha], \tag{15}$$

donde $\alpha = \dfrac{P+\sqrt{d}}{Q}$ y $[\alpha] = I = \left[\dfrac{Q}{\sigma}, \dfrac{P+\sqrt{d}}{\sigma}\right]$.

Ejemplo 3.3.4. *Por el Ejemplo 3.3.1 podemos ver que $I = \left[\dfrac{8}{2}, \dfrac{7+\sqrt{33}}{2}\right]$ es un O_Δ-ideal primitivo de $O_\Delta = \left[1, \dfrac{1+\sqrt{33}}{2}\right]$. Entonces $\alpha = \dfrac{7+\sqrt{33}}{8}$ es un irracional cuadrático que es raíz de $x^2 - \dfrac{7}{4}x + \dfrac{1}{4}$.*

Veamos con un ejemplo que la función $\alpha \longrightarrow [\alpha]$ no es inyectiva.

Ejemplo 3.3.5. *Sea* $\alpha = \dfrac{9+\sqrt{53}}{14}$ *un irracional cuadrático. Ya que* $53 \equiv 1 \pmod 4$*, tenemos* $\sigma = 2, P = 9$ *y* $Q = 14$*. Entonces*

$$\alpha \longrightarrow I = \left[\frac{14}{2}, \frac{9+\sqrt{53}}{2}\right].$$

Si ahora $\gamma = \dfrac{23+\sqrt{53}}{14}$*, entonces* $\sigma = 2, P = 23$ *y* $Q = 14$*. Entonces*

$$\gamma \longrightarrow J = \left[\frac{14}{2}, \frac{23+\sqrt{53}}{2}\right].$$

Por el Corolario 3.2.13, tenemos que

$$I = \left[7, \frac{9+\sqrt{53}}{2}\right] = \left[7, 7 + \frac{9+\sqrt{53}}{2}\right] = J.$$

Por lo tanto $\alpha \longrightarrow [\alpha]$ *no es inyectiva.*

Veamos de manera más general lo que nos dice el Ejemplo 3.3.5.

Sean $d > 1$ un entero libre de cuadrados tal que $d \equiv 2, 3 \pmod 4$ y $\alpha = \dfrac{b+\sqrt{d}}{a}$ un irracional cudrático, donde $b \in \mathbb{Z}, a \in \mathbb{N}$. Entonces $\sigma = 1, P = b$ y $Q = a$. Por tanto

$$\alpha \longrightarrow I = \left[a, b+\sqrt{d}\right].$$

Ahora sea $\gamma = \dfrac{na \pm b + \sqrt{d}}{a}$, para algún $n \in \mathbb{Z}/\{0\}$. Entonces $\sigma = 1, P = na \pm b$ y $Q = a$, por lo tanto

$$\gamma \longrightarrow J = \left[a, na \pm b + \sqrt{d}\right].$$

Por el Corolario 3.2.13, tenemos que

$$I = \left[a, b+\sqrt{d}\right] = \left[a, na \pm b + \sqrt{d}\right] = J.$$

De ahí se ve que α y γ son irracionales cuadráticos distintos que van al mismo ideal.

Ahora sea $\alpha = \dfrac{2b+1+\sqrt{d}}{2a}$, donde $d \equiv 1 \pmod 4$. Entonces $\sigma = 2, P = 2b+1$ y $Q = 2a$. Por lo que

$$\alpha \longrightarrow I = \left[a, \frac{2b+1+\sqrt{d}}{2}\right].$$

Si ahora $\gamma = \dfrac{2(na \pm b) + 1 + \sqrt{d}}{2a}$, para algún $n \in \mathbb{Z}/\{0\}$, entonces $\sigma = 2, P = 2(na \pm b) + 1$ y $Q = 2a$, por lo tanto

$$\gamma \longrightarrow J = \left[a, \frac{2(na \pm b) + 1 + \sqrt{d}}{2}\right].$$

Por el Corolario 3.2.13, obtenemos que

$$I = \left[a, \frac{2b + 1 + \sqrt{d}}{2}\right] = \left[a, na \pm \frac{2b + 1 + \sqrt{d}}{2}\right] = J.$$

Por lo que α y γ son irracionales cuadráticos distintos que van al mismo ideal. Por lo tanto podemos concluir que la función definida en (15) no es inyectiva.

3.3.1. Ideales Reducidos

Por la Definición 3.2.7 y por (12) un O_Δ-ideal primitivo I se puede escribir como $I = [N(I), \alpha]$, donde $\alpha = \dfrac{b + \sqrt{\Delta}}{2}$ para algún $b \in \mathbb{Z}$.

Definición 3.3.6. *Sea $\Delta > 0$ un discriminante. Sea $I = [N(I), \alpha]$ un O_Δ-ideal primitivo. Diremos que I* ***es reducido*** *si no existe $\gamma \in I$ distinto de cero, tal que*

$$|\gamma| < N(I) \qquad y \qquad |\gamma'| < N(I).$$

donde γ' es el conjugado de γ.

Hemos visto que cualquier O_Δ-ideal es equivalente a un O_Δ-ideal primitivo. Veremos luego que todo O_Δ-ideal primitivo es equivalente a un ideal reducido. Así que ahora probemos algunos teoremas que nos dan criterios para saber cuándo un O_Δ-ideal es reducido.

Teorema 3.3.7. *Sea $\Delta > 0$ un discriminante y sea I un O_Δ-ideal primitivo. Entonces I es reducido si y sólo si existe $\beta \in I$ tal que*

$$I = [N(I), \beta], \quad \beta > N(I) \quad y \quad -N(I) < \beta' < 0.$$

DEMOSTRACIÓN. Sea $I = [a, \alpha]$ un O_Δ-ideal primitivo, donde $a = N(I)$ y $\alpha = \dfrac{b + \sqrt{\Delta}}{2}$ para algún $b \in \mathbb{Z}$.

Supongamos que I es reducido. Sea $\beta_0 = \left\lfloor \dfrac{-\alpha'}{a} \right\rfloor a + \alpha \in I$. Entonces

$$\beta_0' = \left\lfloor \frac{-\alpha'}{a} \right\rfloor a + \alpha' = -\left(-\left\lfloor \frac{-\alpha'}{a} \right\rfloor a - \alpha'\right),$$

por lo que $|\beta_0'| = -\left\lfloor \frac{-\alpha'}{a} \right\rfloor a - \alpha'$. Puesto que $\lfloor x \rfloor > x - 1$, para $x \in \mathbb{R}$, se tiene que

$$\left\lfloor \frac{-\alpha'}{a} \right\rfloor > \frac{-\alpha'}{a} - 1.$$

Así que

$$|\beta_0'| < \left(\frac{\alpha'}{a} + 1 \right) a - \alpha' = \alpha' + a - \alpha' = a,$$

es decir, $|\beta_0'| < a$.

Si $\beta_0 < 0$, entonces como I es reducido se tiene que $|\beta_0| = -\beta_0 > a$. De ahí que

$$-\left\lfloor \frac{-\alpha'}{a} \right\rfloor a - \alpha > a > -\left\lfloor \frac{-\alpha'}{a} \right\rfloor a - \alpha'.$$

Por lo que $\alpha < \alpha'$ y entonces $\sqrt{\Delta} < -\sqrt{\Delta}$, lo cual es una contradicción. Observe que $\beta_0 = 0$ no es posible. Por lo tanto $\beta_0 > 0$. Luego existe al menos un elemento $\beta = na + \alpha \in I$ para cierta $n \in \mathbb{Z}$, tal que $|\beta'| < a$ y $\beta_0 \geq \beta > 0$. Podemos suponer sin pérdida de generalidad que β es el mínimo con tales propiedades.

Es claro que $I = [a, \beta]$. Como I es reducido y $|\beta'| < a$, tenemos $\beta = |\beta| > a = N(I)$. Ya que $0 < \beta - a < \beta$ y $\beta - a = (n-1)a + \alpha$, se tiene que $|\beta' - a| > a$ por la minimalidad de β. También se tiene que $-a < \beta' < a$, por lo que $\beta' - a < 0$. Así que $a - \beta' = |\beta' - a| > a$ y de ahí $\beta' < 0$. Luego como $|\beta'| < a$, tenemos $-\beta' < a$, es decir, $\beta' > -N(I)$.

Inversamente, supongamos que $I = [a, \alpha]$ tal que $\alpha > a$ y $-a < \alpha' < 0$. Sea $\gamma \in I$ tal que $|\gamma| < a$ y $|\gamma'| < a$. Probemos que $\gamma = 0$.

Escribimos $\gamma = ma + n\alpha$ para ciertos $m, n \in \mathbb{Z}$. Así que $|ma + n\alpha| < a$ y $|ma + n\alpha'| < a$. Mostraremos que $m = n = 0$.

Supongamos $m > 0$ y $n > 0$. Como $a > 0$ y $\alpha > 0$, se sigue que $ma > 0$ y $n\alpha > 0$. Luego $a < ma + n\alpha$, por lo que $|ma + n\alpha| > |a| = a$. Lo cual es una contradicción al hecho que $|ma + n\alpha| < a$.

Si $m < 0$ y $n < 0$, entonces $-m > 0$ y $-n > 0$. Y el argumento es el mismo al del caso anterior.

Si $m > 0$ y $n < 0$, como $\alpha' < 0$, entonces $ma > 0$ y $n\alpha' > 0$. De ahí que $a < ma + n\alpha'$ y así $|ma + n\alpha'| > a$, lo cual es una contradicción.

Si $m < 0$ y $n > 0$, entonces $-m > 0$ y $-n < 0$. Y el argumento es el mismo al del caso anterior.

Si $m = 0$ y $n \neq 0$, entonces $|ma + n\alpha| = |n\alpha| < a$ y

$$\alpha \leq |n|\alpha = |n\alpha| < a,$$

lo cual es una contradicción.

Si $m \neq 0$ y $n = 0$, se tiene que $|ma + n\alpha| = |ma| < a$. De ahí que $|m|a = |ma| < a$, lo cual es una contradicción.

En conclusión, $m = n = 0$ y entonces I es reducido. □

Ejemplo 3.3.8. *Sea* $O_\Delta = \left[1, \frac{1+\sqrt{145}}{2}\right]$. *El* O_Δ*-ideal*

$$I = \left[4, 3 + \frac{1+\sqrt{145}}{2}\right] = \left[4, \frac{7+\sqrt{145}}{2}\right] = [N(I), \beta],$$

es reducido ya que $\beta > N(I)$ *y* $-4 < \beta' < 0$.

El siguiente corolario es consecuencia inmediata del Teorema 3.3.7.

Corolario 3.3.9. *Si* $\alpha = \frac{P+\sqrt{d}}{Q}$ *es un irracional cuadrático reducido, donde* $P \in \mathbb{Z}$, $Q \in \mathbb{N}$ *y* $d > 1$ *es un entero libre de cuadrados, entonces* $I = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right]$ *es reducido.*

DEMOSTRACIÓN. Como $\alpha > 1$, entonces $P + \sqrt{d} > Q$. Por lo tanto

$$\frac{P+\sqrt{d}}{\sigma} > \frac{Q}{\sigma}.$$

Puesto que $-1 < \alpha' < 0$, entonces

$$\frac{-Q}{\sigma} < \frac{P-\sqrt{d}}{\sigma} < 0.$$

Por el Teorema 3.3.7, se tiene que I es reducido. □

El siguiente ejemplo nos muestra que la función que se definió en (15), no asegura que si $[\alpha]$ es reducido, entonces α es un irracional cuadrático reducido.

Ejemplo 3.3.10. *Sea* $\Delta = 53$. *Entonces* $A_F = O_\Delta = \left[1, \frac{1+\sqrt{53}}{2}\right]$. *Tomemos* O_Δ *como un* O_Δ*-ideal. Entonces por el Corolario 3.2.13, se tiene que*

$$O_\Delta = \left[1, 3 + \frac{1+\sqrt{53}}{2}\right] = \left[1, \frac{7+\sqrt{53}}{2}\right],$$

donde $\frac{7+\sqrt{53}}{2} > N(I) = 1$ *y* $-N(I) = -1 < \frac{7-\sqrt{53}}{2} < 0$. *Entonces por el Teorema 3.3.7,* O_Δ *es un ideal reducido.*

Sin embargo $\alpha = \frac{1+\sqrt{53}}{2}$ *no es un irracional cuadrático reducido ya que* $\alpha' = \frac{1-\sqrt{53}}{2} < -1$.

Observación 7. *Nótese que si $I = [N(I), \beta]$ es un ideal reducido con β que satisface el Teorema 3.3.7, entonces $\alpha = \dfrac{\beta}{N(I)}$ satisface que $\alpha > 1$ y $-1 < \alpha' < 0$. Es decir, α es un irracional cuadrático reducido por la Definición 2.2.11 del Capítulo 2.*

Los siguientes resultados son consecuencia del Teorema 3.3.7 y nos hacen más fácil ver cuando un O_Δ-ideal es reducido en términos de la norma del ideal.

Corolario 3.3.11. *Sean $\Delta > 0$ un discriminante, I un O_Δ-ideal. Si I es reducido, entonces $N(I) < \sqrt{\Delta}$.*

DEMOSTRACIÓN. Como I es reducido, tenemos que I es un O_Δ-ideal primitivo. Sea $I = \left[N(I), \dfrac{b+\sqrt{\Delta}}{2}\right]$ para algún $b \in \mathbb{Z}$. Por el Teorema 3.3.7 existe $\beta \in I$, tal que

$$I = [N(I), \beta], \quad \beta > N(I) \quad \text{y} \quad -N(I) < \beta' < 0.$$

Luego se tiene que

$$N(I) < N(I) - \beta' < \beta - \beta'. \tag{16}$$

Pero $\beta = nN(I) + m\left(\dfrac{b+\sqrt{\Delta}}{2}\right)$, para ciertos $n, m \in \mathbb{Z}$. También se tiene que

$$\frac{b+\sqrt{\Delta}}{2} = xN(I) + y\beta, \text{ para ciertos } x, y \in \mathbb{Z}.$$

Entonces

$$\frac{b+\sqrt{\Delta}}{2} = xN(I) + ynN(I) + \frac{ymb}{2} + \frac{ym\sqrt{\Delta}}{2}.$$

Como $\{\sqrt{\Delta}, 1\}$ es una base de la extensión $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, se tiene que $\dfrac{1}{2} = \dfrac{ym}{2}$ y de ahí $y = m = \pm 1$.

Si $y = -1$, entonces $m = -1$. Por lo que $\beta = nN(I) - \dfrac{b+\sqrt{\Delta}}{2}$ y así

$$\beta' = nN(I) - \frac{b}{2} + \frac{\sqrt{\Delta}}{2}.$$

De ahí que $\beta - \beta' = -\sqrt{\Delta}$. Entonces por (16), se tiene que

$$N(I) < -\sqrt{\Delta},$$

lo cual es una contradicción pues $N(I) > 0$. Por lo tanto $y = m = 1$ y así $\beta = nN(I) + \dfrac{b+\sqrt{\Delta}}{2}$. Por lo que

$$N(I) < \beta - \beta' = \sqrt{\Delta}.$$

□

Corolario 3.3.12. *Sean $\Delta > 0$ un discriminante, I un O_Δ-ideal primitivo. Si $N(I) < \dfrac{\sqrt{\Delta}}{2}$, entonces I es reducido.*

DEMOSTRACIÓN. Sea $I = [N(I), \alpha]$ un O_Δ-ideal primitivo, donde $\alpha = \dfrac{b+\sqrt{\Delta}}{2}$, para algún $b \in \mathbb{Z}$. Sea $\beta = \alpha + \left\lfloor \dfrac{-\alpha'}{N(I)} \right\rfloor N(I) \in I$. Entonces por el Corolario 3.2.13, se tiene que $I = [N(I), \beta]$. Por otro lado

$$\beta' = \alpha' + \left\lfloor \frac{-\alpha'}{N(I)} \right\rfloor N(I).$$

Puesto que $x - 1 < \lfloor x \rfloor \leq x$ para $x \in \mathbb{R}$, se sigue que

$$\begin{aligned} 0 = \alpha' + \left(\frac{-\alpha'}{N(I)}\right) N(I) &\geq \alpha' + \left\lfloor \frac{-\alpha'}{N(I)} \right\rfloor N(I) = \beta' \\ &> \alpha' + \left(\frac{-\alpha'}{N(I)} - 1\right) N(I) = -N(I). \end{aligned}$$

De lo anterior

$$-N(I) < \beta' < 0.$$

También se tiene $\beta - \beta' = \alpha - \alpha' = \sqrt{\Delta}$ y puesto que $N(I) < \dfrac{\sqrt{\Delta}}{2}$, se sigue

$$\beta = \sqrt{\Delta} + \beta' > 2N(I) - N(I),$$

es decir, $\beta > N(I)$. Entonces por el Teorema 3.3.7, I es reducido. □

Ejemplo 3.3.13. *En el Ejemplo 3.3.8, se tiene que*

$$N(I) = 4 < \frac{\sqrt{145}}{2} = \frac{\sqrt{\Delta}}{2}.$$

Entonces por el Corolario 3.3.12, I es reducido.

3.3.2. Ciclos de Ideales Reducidos y Divisores del Número de Clases

A continuación probaremos algunos resultados que nos servirán para justificar el teorema principal de este capítulo.

Lema 3.3.14. *Sea α un irracional cuadrático. Entonces para $k \geq 1$,*

$$(-1)^k(A_{k-1} - \alpha B_{k-1}) = \prod_{j=1}^{k} (\alpha_{j-1} - q_{j-1}).$$

Donde A_k, B_k y α_k, q_k son como se definieron en el Teorema 2.1.5 y Lema 2.2.8 del Capítulo 2, respectivamente.

DEMOSTRACIÓN. Sea $\alpha = [q_0, q_1, \ldots, q_k, \ldots]$. Entonces $\alpha = [q_0, \ldots, \alpha_{j-1}]$, donde $\alpha_{j-1} = [q_{j-1}, q_j, \ldots]$. Así que por el Corolario 2.1.6 del Capítulo 2, se tiene

$$\alpha = \frac{\alpha_{j-1}A_{j-2} + A_{j-3}}{\alpha_{j-1}B_{j-2} + B_{j-3}},\ (j \geq 1).$$

De ahí se obtiene que

$$\alpha_{j-1} = \frac{A_{j-3} - \alpha B_{j-3}}{\alpha B_{j-2} - A_{j-2}}. \tag{17}$$

Para $k = 1$, se tiene $\prod_{j=1}^{1}(\alpha_{j-1} - q_{j-1}) = \alpha_0 - q_0 = \alpha - q_0$. Luego por el Teorema 2.1.5, se sigue que $B_0 = q_0B_{-1} + B_{-2} = 1$ y $A_0 = q_0A_{-1} + A_{-2} = q_0$. Por lo que

$$\prod_{j=1}^{k}(\alpha_{j-1} - q_{j-1}) = \alpha - q_0 = B_0\alpha - A_0 = (-1)(A_0 - \alpha B_0).$$

Ahora supongamos que $(-1)^k(A_{k-1} - \alpha B_{k-1}) = \prod_{j=1}^{k}(\alpha_{j-1} - q_{j-1})$ se cumple hasta $k = n - 1$. Entonces

$$\prod_{j=1}^{n}(\alpha_{j-1} - q_{j-1}) = (-1)^{n-1}(A_{n-2} - \alpha B_{n-2})(\alpha_{n-1} - q_{n-1}).$$

Pero por (17) y el Teorema 2.1.5:

$$\begin{aligned}
\alpha_{n-1} - q_{n-1} &= \frac{A_{n-3} - \alpha B_{n-3}}{\alpha B_{n-2} - A_{n-2}} - q_{n-1} \\
&= \frac{A_{n-3} + q_{n-1}A_{n-2} - \alpha(B_{n-3} + q_{n-1}B_{n-2})}{\alpha B_{n-2} - A_{n-2}} \\
&= \frac{A_{n-1} - \alpha B_{n-1}}{\alpha B_{n-2} - A_{n-2}}.
\end{aligned}$$

Así que

$$\begin{aligned}
\prod_{j=1}^{n}(\alpha_{j-1} - q_{j-1}) &= (-1)^{n-1}(A_{n-2} - \alpha B_{n-2})\left(\frac{A_{n-1} - \alpha B_{n-1}}{\alpha B_{n-2} - A_{n-2}}\right) \\
&= \frac{(-1)^{n-1}(A_{n-2} - \alpha B_{n-2})(A_{n-1} - \alpha B_{n-1})}{(-1)(A_{n-2} - \alpha B_{n-2})} \\
&= (-1)^n(A_{n-1} - \alpha B_{n-1}).
\end{aligned}$$

□

Lema 3.3.15. *Sea* $\theta_k = \prod_{j=1}^{k-1}(\alpha_{j-1} - q_{j-1})$ *para* $k \geq 2$. *Entonces*

$$\theta_{k+1}^{-1} = B_{k-1}\alpha_k + B_{k-2}$$

para $k \geq 1$.

DEMOSTRACIÓN. Por el Lema 3.3.14, se tiene que

$$\theta_k = (-1)^{k-1}(A_{k-2} - \alpha B_{k-2}).$$

De ahí y por el Teorema 2.1.10

$$\begin{aligned}\theta_{k+1} &= (-1)^k(A_{k-1} - \alpha B_{k-1}) = (-1)^k\left(A_{k-1} - \left(\frac{\alpha_k A_{k-1} + A_{k-2}}{\alpha_k B_{k-1} + B_{k-2}}\right)B_{k-1}\right) \\ &= (-1)^k\left(\frac{A_{k-1}B_{k-2} - A_{k-2}B_{k-1}}{\alpha_k B_{k-1} + B_{k-2}}\right) = (-1)^k\left(\frac{(-1)^{k-2}}{\alpha_k B_{k-1} + B_{k-2}}\right) \\ &= \frac{(-1)^{2k-2}}{\alpha_k B_{k-1} + B_{k-2}}.\end{aligned}$$

Por lo tanto

$$\theta_{k+1}^{-1} = \alpha_k B_{k-1} + B_{k-2}$$

para $k \geq 1$. □

Lema 3.3.16. $\theta_{k+1}^{-1} = \prod_{j=1}^{k} \alpha_j$ *para* $k \geq 1$.

DEMOSTRACIÓN. La prueba es por inducción sobre k. Si $k = 1$, por el Teorema 2.1.5, se tiene que

$$\theta_2^{-1} = \alpha_1 B_0 + B_{-1} = \alpha_1.$$

Supongamos que $\theta_{m+1}^{-1} = \prod_{j=1}^{m} \alpha_j$ hasta $m = k - 1$. Entonces

$$\prod_{j=1}^{k} \alpha_j = \prod_{j=1}^{k-1} \alpha_j\alpha_k = \theta_k^{-1}\alpha_k = (\alpha_{k-1}B_{k-2} + B_{k-3})\alpha_k. \tag{18}$$

De (17)

$$\alpha_{k-1} = \frac{A_{k-3} - \alpha B_{k-3}}{\alpha B_{k-2} - A_{k-2}}.$$

Sustituyendo en (18)

$$\begin{aligned}\theta_k^{-1}\alpha_k &= \left(\frac{B_{k-2}A_{k-3}-\alpha B_{k-2}B_{k-3}}{\alpha B_{k-2}-A_{k-2}}+B_{k-3}\right)\alpha_k \\ &= \frac{-\alpha_k(A_{k-2}B_{k-3}-B_{k-2}A_{k-3})}{\alpha B_{k-2}-A_{k-2}} = \frac{-\alpha_k(-1)^{k-3}}{\alpha B_{k-2}-A_{k-2}} \\ &= \frac{\alpha_k(-1)^{k-2}}{\alpha B_{k-2}-A_{k-2}} = \frac{\alpha_k(-1)^{k-2}}{\left(\frac{\alpha_k A_{k-1}+A_{k-2}}{\alpha_k B_{k-1}+B_{k-2}}\right)B_{k-2}-A_{k-2}} \\ &= \frac{\alpha_k(-1)^{k-2}(\alpha_k B_{k-1}+B_{k-2})}{\alpha_k(A_{k-1}B_{k-2}-A_{k-2}B_{k-1})} = \frac{\alpha_k(-1)^{k-2}(\alpha_k B_{k-1}+B_{k-2})}{\alpha_k(-1)^{k-2}} \\ &= \alpha_k B_{k-1}+B_{k-2} = \theta_{k+1}^{-1}.\end{aligned}$$

□

Lema 3.3.17. *Sea $f:\mathbb{N}\to\mathbb{R}$ dada por $f(k)=\theta_{k+1}^{-1}$. Entonces f es una función monótona creciente.*

DEMOSTRACIÓN. Notemos que por el Lema 3.3.16, para $k=2$ se tiene

$$\theta_3^{-1}=\alpha_1\alpha_2 \quad \text{y} \quad \theta_2^{-1}=\alpha_1, \quad \text{con} \quad \alpha_1,\alpha_2>1.$$

Así que

$$\theta_3^{-1}>\theta_2^{-1}.$$

Puesto que $\alpha_k>1$, por inducción tenemos

$$\theta_{k+1}^{-1}=\prod_{j=1}^{k}\alpha_j=\prod_{j=1}^{k-1}\alpha_j\alpha_k>\prod_{j=1}^{k-1}\alpha_j=\theta_k^{-1}.$$

□

Lema 3.3.18. *Sean $[\alpha,\beta]$ y $[\gamma,\delta]$ $\mathbb{Z}$-submódulos, donde $\alpha,\beta,\gamma,\delta\in O_\Delta$. Entonces $[\alpha,\beta]=[\gamma,\delta]$ si y sólo si $\alpha=x\gamma+y\delta$ y $\beta=w\gamma+z\delta$, donde $x,y,z,w\in\mathbb{Z}$ satisfacen $xz-wy=\pm1$, es decir, $[\alpha,\beta]=[\gamma,\delta]$ si y sólo si $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=X\begin{pmatrix}\gamma\\ \delta\end{pmatrix}$ es soluble en $GL_2(\mathbb{Z})$.*

DEMOSTRACIÓN. Supongamos que $\alpha=x\gamma+y\delta$ y $\beta=w\gamma+z\delta$, para ciertas $x,y,z,w\in\mathbb{Z}$ y tal que $xz-wy=\pm1$. Entonces es claro que $[\alpha,\beta]\subseteq[\gamma,\delta]$.

Por otro lado se tiene

$$\alpha z-\beta y=xz\gamma+yz\delta-wy\gamma-zy\delta=\gamma(xz-wy)=\gamma(\pm1)$$

y

$$\beta x-\alpha w=wx\gamma+zx\delta-xw\gamma-yw\delta=\delta(zx-yw)=\delta(\pm1).$$

De lo anterior se tiene que $[\gamma,\delta]\subseteq[\alpha,\beta]$.

Ahora supongamos que $[\alpha, \beta] = [\gamma, \delta]$. Entonces $\alpha = x\gamma + y\delta$ y $\beta = w\gamma + z\delta$, para ciertas $x, y, w, z \in \mathbb{Z}$. De ahí se tiene

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix}.$$

Análogamente, existen $x_0, y_0, w_0, z_0 \in \mathbb{Z}$, tal que

$$\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} x_0 & y_0 \\ w_0 & z_0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Por lo tanto

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \begin{pmatrix} x_0 & y_0 \\ w_0 & z_0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Si $X = \begin{pmatrix} x & y \\ w & z \end{pmatrix}$ y $Y = \begin{pmatrix} x_0 & y_0 \\ w_0 & z_0 \end{pmatrix}$, entonces $1 = \det XY = \det X \det Y$. Por lo que $\det X = \det Y = \pm 1$ y así $X \in GL_2(\mathbb{Z})$.

Definición 3.3.19. *La **sucesión de Fibonacci** se define como:*

$$F_1 = F_2 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad (n \geq 3).$$

*Llamaremos a F_n **el n-ésimo número de Fibonacci**.*

Uno de los números más conocidos en varias disciplinas de la matemática, es la **razón dorada**:

$$\mathfrak{g} = \frac{1 + \sqrt{5}}{2}.$$

Es fácil ver que $\mathfrak{g} > 1$ y debido a que $\mathfrak{g}^2 = \mathfrak{g} + 1$, se tiene que $\mathfrak{g}$ es un irracional cuadrático.

Proposición 3.3.20. *$F_n \geq \mathfrak{g}^{n-2}$ para toda $n \in \mathbb{N}$.*

DEMOSTRACIÓN. La prueba es por inducción sobre n. Si $n = 1$

$$F_1 = 1 > \frac{1}{\mathfrak{g}} = \mathfrak{g}^{-1}.$$

Supongamos que la afirmación de la proposición se cumple hasta n, es decir, $F_n \geq \mathfrak{g}^{n-2}$. Entonces

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \geq \mathfrak{g}^{n-2} + \mathfrak{g}^{n-3} = \mathfrak{g}^{n-3}(\mathfrak{g} + 1) \\ &= \mathfrak{g}^{n-3}(\mathfrak{g}^2) = \mathfrak{g}^{n-1}. \end{aligned}$$

Por lo tanto $F_n \geq \mathfrak{g}^{n-2}$ para toda $n \in \mathbb{N}$. □

Proposición 3.3.21. *$B_k \geq F_{k+1}$ para toda $k \in \mathbb{N}$, donde F_{k+1} es el $(k+1)$-ésimo número de Fibonacci y*

$$B_k = q_k B_{k-1} + B_{k-2}, \quad B_{-2} = 1 \quad y \quad B_{-1} = 0.$$

DEMOSTRACIÓN. La prueba es por inducción sobre k.

Si $k = 1$, entonces

$$B_1 = q_1 B_0 + B_{-1} = q_1 \geq 1 = F_2.$$

Supongamos que $B_m \geq F_{m+1}$ para toda $m \in \mathbb{N}$ con $m < k$.

Luego

$$B_k = q_k B_{k-1} + B_{k-2} \geq q_k F_k + F_{k-1} \geq F_k + F_{k-1} = F_{k+1}.$$

□

Lema 3.3.22. *Sea $\Delta > 0$ un discriminante y sea $I = I_1 = \left[\frac{Q_0}{\sigma}, \frac{P_0 + \sqrt{d}}{\sigma}\right]$ un O_Δ-ideal primitivo. Sea*

$$\alpha = \alpha_0 = \frac{P_0 + \sqrt{d}}{Q_0}$$

y P_k, Q_k, α_k y q_k para $k \geq 0$, definidos como en el Lema 2.2.8 del Capítulo 2. Entonces

$$I_k = \left[\frac{Q_{k-1}}{\sigma}, \frac{P_{k-1} + \sqrt{d}}{\sigma}\right],$$

es un O_Δ-ideal primitivo para toda $k \in \mathbb{N}$.

DEMOSTRACIÓN. El Lema 2.2.8, asegura que

$$P_{k-1}^2 - d = -Q_{k-2} Q_{k-1}.$$

Aplicando el Teorema 3.3.2, I_k es un O_Δ-ideal primitivo. □

Ahora sí ya tenemos todo para probar el teorema principal de este capítulo, el cual produce todos los ideales reducidos equivalentes a un O_Δ-ideal primitivo dado.

Teorema 3.3.23. *Sea $\Delta > 0$ un discriminante y sea $I = I_1 = \left[\frac{Q_0}{\sigma}, \frac{P_0 + \sqrt{d}}{\sigma}\right]$ un O_Δ-ideal primitivo. Sea*

$$\alpha = \alpha_0 = \frac{P_0 + \sqrt{d}}{Q_0}$$

y P_k, Q_k, α_k y q_k para $k \geq 0$, definidos como en el Lema 2.2.8 del Capítulo 2. Si

$$I_k = \left[\frac{Q_{k-1}}{\sigma}, \frac{P_{k-1} + \sqrt{d}}{\sigma}\right],$$

entonces $I_1 \sim I_k$ para toda $k \in \mathbb{N}$. Además, existe un valor mínimo $n_0 \in \mathbb{N}$ tal que I_{n_0+j} es reducido para toda $j \geq 0$. Estos I_{n_0+j} son todos los ideales reducidos equivalentes a I_1.

DEMOSTRACIÓN. Sea $\theta_k = \prod_{j=1}^{k-1}(\alpha_{j-1} - q_{j-1})$ para $k \geq 2$. Entonces por el Lema 3.3.14, se tiene que

$$\theta_k = (-1)^{k-1}(A_{k-2} - \alpha B_{k-2}) = (-1)^{k-1}(A_{k-2} - \alpha_0 B_{k-2}). \tag{19}$$

Vamos a mostrar que

$$(Q_0\theta_k)I_k = (Q_{k-1})I_1$$

para $k \geq 2$. Sea $X = (-1)^k \begin{pmatrix} -A_{k-2} & B_{k-2} \\ A_{k-1} & -B_{k-1} \end{pmatrix}$. Entonces

$$\begin{aligned} X \begin{pmatrix} 1 \\ \alpha_o \end{pmatrix} &= \begin{pmatrix} (-1)^{k-1}A_{k-2} & (-1)^k B_{k-2} \\ (-1)^k A_{k-1} & (-1)^{k-1}B_{k-1} \end{pmatrix} \begin{pmatrix} 1 \\ \alpha_o \end{pmatrix} \\ &= \begin{pmatrix} (-1)^{k-1}A_{k-2} + \alpha_0(-1)^k B_{k-2} \\ (-1)^k A_{k-1} + \alpha_0(-1)^{k-1}B_{k-1} \end{pmatrix} \\ &= \begin{pmatrix} (-1)^{k-1}(A_{k-2} - \alpha_0 B_{k-2}) \\ (-1)^k(A_{k-1} - \alpha_0 B_{k-1}) \end{pmatrix}. \end{aligned}$$

Por (19), se tiene que

$$\begin{pmatrix} \theta_k \\ \theta_{k+1} \end{pmatrix} = X \begin{pmatrix} 1 \\ \alpha_0 \end{pmatrix}.$$

También tenemos que

$$\begin{aligned} \det X &= (-1)^k(A_{k-2}B_{k-1} - A_{k-1}B_{k-2}) = (-1)^k(-(A_{k-1}B_{k-2} - A_{k-2}B_{k-1})) \\ &= (-1)^k(-(-1)^{k-2}) = (-1)^k(-1)^{k-1} = (-1)^{-1} = -1. \end{aligned}$$

Por lo que $X \in GL_2(\mathbb{Z})$. Entonces por el Lema 3.3.18, se tiene que

$$[\theta_k, \theta_{k+1}] = [1, \alpha_0]. \tag{20}$$

Por otro lado

$$\begin{aligned} \theta_k(\alpha_{k-1} - q_{k-1}) &= \prod_{j=1}^{k-1}(\alpha_{j-1} - q_{j-1})(\alpha_{k-1} - q_{k-1}) \\ &= \prod_{j=1}^{k}(\alpha_{j-1} - q_{j-1}) = \theta_{k+1}. \end{aligned}$$

Entonces

$$\begin{aligned} [\theta_k, \theta_{k+1}] &= [\theta_k, \theta_k(\alpha_{k-1} - q_{k-1})] = (\theta_k)[1, \alpha_{k-1} - q_{k-1}] \\ &= (\theta_k)\left[1, \frac{P_{k-1} + \sqrt{d}}{Q_{k-1}} - q_{k-1}\right] \\ &= (\theta_k)\left[1, \frac{P_{k-1} + \sqrt{d} - q_{k-1}Q_{k-1}}{Q_{k-1}}\right]. \end{aligned}$$

De ahí que

$$(Q_{k-1})[\theta_k, \theta_{k+1}] = (\theta_k)[Q_{k-1}, P_{k-1} + \sqrt{d} - q_{k-1}Q_{k-1}],$$

y por (20)

$$(Q_{k-1})[1, \alpha_0] = (\theta_k)[Q_{k-1}, P_{k-1} + \sqrt{d} - q_{k-1}Q_{k-1}] = (\theta_k)[Q_{k-1}, P_{k-1} + \sqrt{d}],$$

es decir,

$$(Q_{k-1})\left[1, \frac{P_0 + \sqrt{d}}{Q_0}\right] = (\theta_k)[Q_{k-1}, P_{k-1} + \sqrt{d}].$$

De ahí que

$$(Q_{k-1})[Q_0, P_0 + \sqrt{d}] = (Q_0\theta_k)[Q_{k-1}, P_{k-1} + \sqrt{d}].$$

Entonces

$$(Q_{k-1})\left[\frac{Q_0}{\sigma}, \frac{P_0 + \sqrt{d}}{\sigma}\right] = (Q_0\theta_k)\left[\frac{Q_{k-1}}{\sigma}, \frac{P_{k-1} + \sqrt{d}}{\sigma}\right].$$

Por lo tanto $(Q_{k-1})I_1 = (\theta_k Q_0)I_k$. Ya que $\theta_k \in O_\Delta$, entonces $\theta_k Q_0 \in O_\Delta$. Así $I_1 \sim I_k$ para toda $k \geq 2$.

Ahora demostraremos que existe algún $n_0 \in \mathbb{N}$, tal que I_{n_0+j} es reducido para toda $j \geq 0$. Esta prueba la haremos con base en varias afirmaciones.

Afirmación 1. Si $k \in \mathbb{N} \cup \{0\}$, entonces $\alpha'_k < 0$ si y sólo si $P_k < \sqrt{d}$ y $Q_k > 0$.

Si $Q_k > 0$ y $P_k < \sqrt{d}$, entonces es claro que $\alpha'_k = \dfrac{P_k - \sqrt{d}}{Q_k} < 0$.

Inversamente, supongamos que $\alpha'_k = \dfrac{P_k - \sqrt{d}}{Q_k} < 0$. Puesto que $\lfloor \alpha_k \rfloor = q_k \geq 1$, se tiene $\alpha_k > 1$. Entonces $\alpha_k - \alpha'_k > 0$, luego

$$\frac{2\sqrt{d}}{Q_k} = \alpha_k - \alpha'_k > 0.$$

Puesto que $\Delta > 0$, tenemos $2\sqrt{d} > 0$, por tanto $Q_k > 0$. De ahí $P_k - \sqrt{d} < 0$.

Afirmación 2. Si $\alpha'_k < 0$, entonces $\alpha'_{k+j} < 0$ para toda $j \in \mathbb{N} \cup \{0\}$.

La prueba es por inducción sobre j. Si $j = 0$, la afirmación es evidente. Supongamos que la afirmación es válida para j y que

$$\alpha'_{k+j+1} = \frac{P_{k+j+1} - \sqrt{d}}{Q_{k+j+1}} > 0.$$

Caso 1. Si $P_{k+j+1} - \sqrt{d} > 0$ y $Q_{k+j+1} > 0$, entonces $P_{k+j+1} + \sqrt{d} > 2\sqrt{d} > 0$, por lo que

$$0 < (P_{k+j+1} + \sqrt{d})(P_{k+j+1} - \sqrt{d}).$$

Por otro lado se tiene que por el Lema 2.2.8

$$(P_{k+j+1} + \sqrt{d})(P_{k+j+1} - \sqrt{d}) = P_{k+j+1}^2 - d = -Q_{k+j}Q_{k+j+1}.$$

Por la hipótesis de inducción tenemos $\alpha'_{k+j} < 0$, así que de la Afirmación 1 obtenemos que $Q_{k+j} > 0$. Entonces de lo anterior se obtiene

$$0 < -Q_{k+j+1}Q_{k+j} < 0,$$

lo cual es una contradicción.

Caso 2. Supongamos $P_{k+j+1} - \sqrt{d} < 0$ y $Q_{k+j+1} < 0$. Por un lado se tiene que

$$(P_{k+j+1} - \sqrt{d})(P_{k+j+1} + \sqrt{d}) = P_{k+j+1}^2 - d = -Q_{k+j}Q_{k+j+1}. \tag{21}$$

Por la hipótesis de inducción se tiene $Q_{k+j} > 0$, entonces $-Q_{k+j}Q_{k+j+1} > 0$. Veremos que $(P_{k+j+1} - \sqrt{d})(P_{k+j+1} + \sqrt{d}) < 0$. Para esto probemos que $(P_{k+j+1} + \sqrt{d}) > 0$. Por el Lema 2.2.8, se tiene que probar que

$$q_{k+j}Q_{k+j} - P_{k+j} + \sqrt{d} > 0.$$

Puesto que $\lfloor \alpha_k \rfloor = q_{k+j} \geq 1$ y $Q_{k+j} > 0$, se tiene que $q_{k+j}Q_{k+j} > 0$. También, como $\alpha'_{k+j} < 0$, por la Afirmación 1, $\sqrt{d} - P_{k+j} > 0$ y por tanto

$$P_{k+j+1} + \sqrt{d} = q_{k+j}Q_{k+j} - P_{k+j} + \sqrt{d} > 0.$$

De ahí y por (21)

$$0 < (P_{k+j+1} - \sqrt{d})(P_{k+j+1} + \sqrt{d}) < 0,$$

lo cual es una contradicción. Por lo tanto $\alpha'_{k+j+1} < 0$.

Afirmación 3. Si $\alpha'_k < 0$, entonces I_{k+1} es un ideal reducido, para todo $k \in \mathbb{N} \cup \{0\}$.

Por la Afirmación 1, $Q_k > 0$. Como $\lfloor \alpha_k \rfloor = q_k \geq 1$, tenemos $\alpha_k > 1$. Así que $P_k + \sqrt{d} > Q_k > 0$. Sea $\gamma = \dfrac{P_k + \sqrt{d}}{\sigma} > 0$. Entonces

$$\gamma = \frac{P_k + \sqrt{d}}{\sigma} > \frac{Q_k}{\sigma} = N(I_{k+1}).$$

De la Afirmación 1, también se tiene que $P_k < \sqrt{d}$, por lo que $\gamma' = \dfrac{P_k - \sqrt{d}}{\sigma} < 0$.

Sea $\beta = \left\lfloor \dfrac{-\gamma'}{N(I_{k+1})} \right\rfloor N(I_{k+1}) + \gamma$. Como $\left\lfloor \dfrac{-\gamma'}{N(I_{k+1})} \right\rfloor \geq 0$, se sigue que $\beta \geq \gamma > N(I_{k+1})$. El Corolario 3.2.13 nos asegura

$$I_{k+1} = [N(I_{k+1}), \gamma] = [N(I_{k+1}), \beta].$$

Puesto que $-\gamma' \notin \mathbb{Q}$, se tiene que $\left\lfloor \dfrac{-\gamma'}{N(I_{k+1})} \right\rfloor < \dfrac{-\gamma'}{N(I_{k+1})}$, por tanto

$$\begin{aligned} \beta' &= \left\lfloor \frac{-\gamma'}{N(I_{k+1})} \right\rfloor N(I_{k+1}) + \gamma' < \left(\frac{-\gamma'}{N(I_{k+1})} \right) N(I_{k+1}) + \gamma' \\ &= -\gamma' + \gamma' = 0. \end{aligned}$$

y

$$\beta' = \left\lfloor \frac{-\gamma'}{N(I_{k+1})} \right\rfloor N(I_{k+1}) + \gamma' > \left(\frac{-\gamma'}{N(I_{k+1})} - 1 \right) N(I_{k+1}) + \gamma'$$
$$= -\gamma' - N(I_{k+1}) + \gamma' = -N(I_{k+1}).$$

De lo anterior $-N(I_{k+1}) < \beta' < 0$. Así que por el Teorema 3.3.7, I_{k+1} es un ideal reducido.

Resumiendo las tres afirmaciones anteriores se tiene que si $\alpha'_k < 0$, entonces $\alpha'_{k+j} < 0$ para toda $j \geq 0$ y por tanto I_{k+j+1} es un ideal reducido para toda $j \geq 0$. Así que nos falta mostrar que existe una $k \in \mathbb{N}$, tal que $\alpha'_k < 0$. Para esto probemos las siguientes afirmaciones.

Afirmación 4. Si I_{k+1} es reducido, entonces $\alpha'_{k+1} < 0$.
Por el Corolario 3.2.13 y el Lema 2.2.8 se tiene que

$$I_{k+1} = \left[\frac{Q_k}{\sigma}, \frac{P_k + \sqrt{d}}{\sigma} \right] = \left[\frac{Q_k}{\sigma}, \frac{P_k - q_k Q_k + \sqrt{d}}{\sigma} \right]$$
$$= \left[\frac{Q_k}{\sigma}, \frac{\sqrt{d} - P_{k+1}}{\sigma} \right].$$

Sea $\delta = \dfrac{\sqrt{d} - P_{k+1}}{\sigma}$. Entonces es claro que $\delta \in I_{k+1}$ y

$$\delta = \frac{(d - P_{k+1}^2)}{\sigma(\sqrt{d} + P_{k+1})} = \frac{Q_{k+1}Q_k}{\sigma(\sqrt{d} + P_{k+1})} = \frac{Q_k}{\sigma \alpha_{k+1}}.$$

Como I_{k+1} es primitivo, se tiene que $Q_k > 0$. Además $\sigma > 0$ y $\alpha_{k+1} > 1$, por lo que $\delta > 0$. También

$$\delta = \frac{Q_k}{\sigma(\alpha_{k+1})} < \frac{Q_k}{\sigma} = N(I_{k+1}).$$

Así que $0 < \delta < N(I_{k+1})$. Como I_{k+1} es reducido, por definición $|\delta'| > N(I_{k+1})$. Luego

$$|\delta'| = \left| \frac{-P_{k+1} - \sqrt{d}}{\sigma} \right| = \frac{|-(P_{k+1} + \sqrt{d})|}{\sigma} = \frac{P_{k+1} + \sqrt{d}}{\sigma} = -\delta'.$$

De ahí que

$$-\delta' > \frac{Q_k}{\sigma} > 0.$$

Así

$$\delta' = \frac{Q_k}{\alpha'_{k+1}\sigma} < 0$$

y por lo tanto $\alpha'_{k+1} < 0$, pues $Q_k, \sigma > 0$.

Afirmación 5. Si $| \alpha_0 - \alpha'_0 | > \dfrac{1}{B_{k-1}B_{k-2}}$, entonces $\alpha'_k < 0$ para $k \geq 2$.

Sean $\alpha_0 = [q_0, q_1, \ldots]$ y $\alpha_k = [q_k, q_{k+1}, \ldots]$. Entonces por el Corolario 2.1.6 y el Teorema 2.1.10, se tiene

$$\begin{aligned}
\alpha_0 &= \frac{\alpha_k A_{k-1} + A_{k-2}}{\alpha_k B_{k-1} + B_{k-2}} = \frac{\alpha_k A_{k-1} B_{k-1} + A_{k-2} B_{k-1}}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} \\
&= \frac{\alpha_k A_{k-1} B_{k-1} + A_{k-1} B_{k-2} + A_{k-2} B_{k-1} - A_{k-1} B_{k-2}}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} \\
&= \frac{A_{k-1}(\alpha_k B_{k-1} + B_{k-2})}{B_{k-1}(\alpha_k B_{k-1} + B_{k-2})} + \frac{A_{k-2} B_{k-1} - A_{k-1} B_{k-2}}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} \\
&= \frac{A_{k-1}}{B_{k-1}} - \frac{(A_{k-1} B_{k-2} - A_{k-2} B_{k-1})}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} = \frac{A_{k-1}}{B_{k-1}} - \frac{(-1)^{k-2}}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} \\
&= \frac{A_{k-1}}{B_{k-1}} + \frac{(-1)^{k-1}}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}}.
\end{aligned}$$

Análogamente se tiene que $\alpha_0' = \dfrac{A_{k-1}}{B_{k-1}} + \dfrac{(-1)^{k-1}}{\alpha_k' B_{k-1}^2 + B_{k-2} B_{k-1}}$. Entonces

$$(-1)^k(\alpha_0 - \alpha_0') = \frac{1}{\alpha_k' B_{k-1}^2 + B_{k-2} B_{k-1}} - \frac{1}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}}$$

y por tanto

$$\begin{aligned}
\mid \alpha_0 - \alpha_0' \mid &= \mid (-1)^k(\alpha_0 - \alpha_0') \mid \\
&= \left| \frac{1}{\alpha_k' B_{k-1}^2 + B_{k-2} B_{k-1}} - \frac{1}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} \right|.
\end{aligned}$$

Supongamos que $\alpha_k' > 0$. Entonces $\alpha_k' B_{k-1}^2 + B_{k-2} B_{k-1} > 0$. De ahí que

$$\mid \alpha_0 - \alpha_0' \mid < \text{máx} \left\{ \frac{1}{\alpha_k' B_{k-1}^2 + B_{k-2} B_{k-1}}, \frac{1}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} \right\}.$$

Como $\alpha_k' B_{k-1}^2 + B_{k-2} B_{k-1} > B_{k-2} B_{k-1}$ pues $\alpha_k' B_{k-1}^2 > 0$, tenemos

$$\frac{1}{\alpha_k' B_{k-1}^2 + B_{k-2} B_{k-1}} < \frac{1}{B_{k-2} B_{k-1}}.$$

También $\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1} > B_{k-2} B_{k-1}$, por lo que

$$\frac{1}{\alpha_k B_{k-1}^2 + B_{k-2} B_{k-1}} < \frac{1}{B_{k-2} B_{k-1}}.$$

Por tanto

$$\mid \alpha_0 - \alpha_0' \mid < \frac{1}{B_{k-1} B_{k-2}},$$

lo cual contradice la hipótesis. Así que $\alpha_k' < 0$.

En la siguiente afirmación $\log n$ significa $\log_e n$.

Afirmación 6. Supongamos que

$$M_0 = \text{máx}\left\{2, \frac{5}{2} + \frac{\log\left(\frac{|Q_0|}{2\sqrt{d}}\right)}{2\log \mathfrak{g}}\right\}$$

donde $\mathfrak{g} = \dfrac{1+\sqrt{5}}{2}$. Entonces $\alpha_k' < 0$ para toda $k \geq M_0$.

Por las Proposiciones 3.3.21 y 3.3.20, se tiene que $B_k \geq F_{k+1} \geq \mathfrak{g}^{k-1}$ para toda $k \geq 1$. De ahí que

$$B_{k-1}B_{k-2} \geq \mathfrak{g}^{k-2}\mathfrak{g}^{k-3} = \mathfrak{g}^{2k-5}.$$

Supongamos que $k \geq M_0$. Si $M_0 = \dfrac{5}{2} + \dfrac{\log\left(\frac{|Q_0|}{2\sqrt{d}}\right)}{2\log \mathfrak{g}}$, entonces

$$2k - 5 \geq \frac{\log\left(\frac{|Q_0|}{2\sqrt{d}}\right)}{\log \mathfrak{g}}.$$

Si $M_0 = 2$, entonces

$$k \geq 2 > \frac{5}{2} + \frac{\log\left(\frac{|Q_0|}{2\sqrt{d}}\right)}{2\log \mathfrak{g}}.$$

De ambas desigualdades obtenemos

$$2k - 5 \geq \frac{\log\left(\frac{|Q_0|}{2\sqrt{d}}\right)}{\log \mathfrak{g}}$$

y así

$$B_{k-1}B_{k-2} \geq \mathfrak{g}^{2k-5} \geq \mathfrak{g}^{\frac{\log\left(\frac{|Q_0|}{2\sqrt{d}}\right)}{\log \mathfrak{g}}} = \mathfrak{g}^{\log_{\mathfrak{g}}\left(\frac{|Q_0|}{2\sqrt{d}}\right)},$$

por lo que

$$B_{k-1}B_{k-2} \geq \frac{|\ Q_0\ |}{2\sqrt{d}}.$$

Pero

$$\frac{1}{|\ \alpha_0 - \alpha_0'\ |} = \frac{1}{\left|\frac{P_0+\sqrt{d}}{Q_0} - \frac{P_0-\sqrt{d}}{Q_0}\right|} = \frac{|Q_0|}{2\sqrt{d}} \in \mathbb{R}\backslash\mathbb{Q},$$

así que

$$B_{k-1}B_{k-2} > \frac{|Q_0|}{2\sqrt{d}} = \frac{1}{|\alpha_0 - \alpha_0'|}.$$

Entonces por la Afirmación 5, se tiene que $\alpha_k' < 0$.

Sea $A = \{n \in \mathbb{N} | \alpha_n' < 0\}$. Es claro que $A \neq \emptyset$ ya que $n = \lfloor M_0 \rfloor \in A$. Por el principio del buen orden, sea $n_0 \in A$ el mínimo. Hasta aquí hemos establecido la existencia de una sucesión de ideales reducidos I_k equivalentes a I_1 en O_Δ, para

toda $k \geq n_0$. Ahora veamos que dichos ideales son los únicos ideales reducidos equivalentes a I_1. Esto lo haremos con dos últimas afirmaciones.

Afirmación 7. Sean I, J ideales primitivos equivalentes en O_Δ. Entonces existe $\delta \in I$, tal que $(\delta)J = (N(J))I$, con $0 < \delta < N(I)$.

Como $I \sim J$, existen α, β distintos de cero en O_Δ, tal que $(\alpha)I = (\beta)J$. De ahí para ciertos enteros b_1, b_2, se tiene

$$(\alpha)\left[N(I), \frac{b_1 + \sqrt{\Delta}}{2}\right] = (\beta)\left[N(J), \frac{b_2 + \sqrt{\Delta}}{2}\right].$$

Entonces, para algún $\lambda \in I$, $\lambda > 0$

$$|\beta|N(J) = |\alpha|\lambda. \tag{22}$$

Sea μ que pertenece al grupo de unidades de O_Δ, tal que $0 < \mu < 1$. Entonces existe $j \in \mathbb{Z}$ tal que $\mu^j \lambda < N(I)$.

Sean $\delta = \mu^j \lambda$ y $L = (\delta)J = (\mu^j)(\lambda)J = (\lambda)J$. De ahí y por (22), se tiene que

$$(N(J)\beta)J = (\alpha\lambda)J = (\alpha)(\lambda)J = (\alpha)L.$$

Luego

$$(\alpha)(N(J))I = (N(J))(\alpha)I = (N(J))(\beta)J = (N(J)\beta)J = (\alpha)L.$$

De ahí que

$$(\alpha)(N(J))I = (\alpha)L$$

y por tanto

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

Entonces

$$(\delta)J = L = (N(J))I.$$

Sea J un ideal reducido en O_Δ, tal que $J \sim I_1$. Como $I_{n_0} \sim I_1$, tenemos $J \sim I_{n_0}$. Sin pérdida de generalidad podemos suponer que $I_{n_0} = I_1$, es decir, que I_1 es un ideal reducido en O_Δ.

Afirmación 8. Sean $I = I_1$ y J ideales reducidos quivalentes en O_Δ. Entonces existe $k \in \mathbb{N}$ tal que $\delta = \theta_k N(I) = \dfrac{\theta_k Q_0}{\sigma}$, donde $\theta_1 = 1$.

Por las Proposiciones 3.3.21 y 3.3.20, se tiene que

$$B_k \geq \mathfrak{g}^{k-1} \quad \text{para} \quad k \geq 1. \tag{23}$$

Sea $f(k) = \theta_{k+1}^{-1}$ como en el Lema 3.3.17. Ahora por el Lema 3.3.15 y (23), se tiene que

$$f(k) = \theta_{k+1}^{-1} = \alpha_k B_{k-1} + B_{k-2} > B_{k-2} \geq \mathfrak{g}^{k-3},$$

Pues $B_{k-1}\alpha_k > 0$. Por otro lado $\mathfrak{g} > 1$, por lo que $\mathfrak{g}^{k-3}$ es monótona creciente para $k \geq 3$ y así $\lim_{k\to\infty} \mathfrak{g}^{k-3} \to \infty$. Entonces de ahí y del Lema 3.3.17 tenemos que f es una función monótona creciente y no acotada.

De la Afirmación 7, se sigue que existe $\delta \in I$, tal que $0 < \delta < N(I)$ y $(\delta)J = (N(J))I$. De ahí que $1 < \dfrac{N(I)}{\delta}$. Luego por ser f monótona creciente y $\theta_1 = 1$, existe $k \in \mathbb{N}$ tal que

$$\theta_k^{-1} \leq \frac{N(I)}{\delta} < \theta_{k+1}^{-1}. \tag{24}$$

Entonces

$$\theta_{k+1} < \frac{\delta}{N(I)} \leq \theta_k. \tag{25}$$

Vamos a mostrar que para esta k, se cumple que $\delta = \theta_k N(I)$. Supongamos que $\delta \neq N(I)\theta_k$. Por (20), se tiene que

$$\begin{aligned}\delta \in I = \left[\frac{Q_0}{\sigma}, \frac{P_0+\sqrt{d}}{\sigma}\right] &= \frac{Q_0}{\sigma}\left[1, \frac{P_0+\sqrt{d}}{Q_0}\right] = \frac{Q_0}{\sigma}[1, \alpha_0] \\ &= \frac{Q_0}{\sigma}[\theta_{k+1}, \theta_k] = \left[\frac{Q_0\theta_{k+1}}{\sigma}, \frac{Q_0\theta_k}{\sigma}\right].\end{aligned}$$

De donde $\delta = yN(I)\theta_{k+1} + xN(I)\theta_k$ para ciertos $x, y \in \mathbb{Z}$ no ambos cero pues $\delta > 0$. Entonces

$$\frac{\delta}{N(I)} = y\theta_{k+1} + x\theta_k. \tag{26}$$

para ciertos $x, y \in \mathbb{Z}$ no ambos cero. Ahora supongamos que

$$|\delta'| \geq |\theta'_{k+1}|N(I). \tag{27}$$

Sea $\lambda = N(I)\theta_{k+1} \in I$. Como $(N(J))I = (\delta)J$, entonces $N(J)\lambda = \delta\rho$ para algún $0 \neq \rho \in J$. De ahí que $|\rho| = N(J)\left|\dfrac{\lambda}{\delta}\right|$. Pero

$$\left|\frac{\lambda}{\delta}\right| = \left|\frac{N(I)\theta_{k+1}}{\delta}\right| = \left|\frac{N(I)}{\delta}\right||\theta_{k+1}| < |\theta_{k+1}^{-1}||\theta_{k+1}| = 1$$

Así que $|\rho| < N(J)$.

Luego por (27) tenemos que

$$|\rho'| = N(J)\left|\frac{\lambda'}{\delta'}\right| = N(J)\left|\frac{N(I)\theta'_{k+1}}{\delta'}\right| \leq N(J)\frac{N(I)|\theta'_{k+1}|}{|\theta'_{k+1}|N(I)} = N(J).$$

Pero $|\rho'| \neq N(J)$, pues de lo contrario $\rho' \in \mathbb{Z}$ y de ahí se tendría que $N(J) = |\rho'| = |\rho| < N(J)$. Por lo tanto $|\rho'| < N(J)$, lo cual contradice que J es reducido. Entonces necesariamente

$$|\delta'| < |\theta'_{k+1}|N(I).$$

De (25) se tiene que $\dfrac{\delta}{N(I)} < \theta_k$ pues $\dfrac{\delta}{N(I)} \neq \theta_k$ ya que estamos suponiendo $\delta \neq N(I)\theta_k$. De ahí y de (26), obtenemos que

$$|x\theta_k + y\theta_{k+1}| = \left|\frac{\delta}{N(I)}\right| < |\theta_k| = \theta_k, \tag{28}$$

θ_k es positivo, pues $\theta_k^{-1} > 0$ como se observa en el Lema 3.3.15.

De (26), también se tiene que $\dfrac{\delta'}{N(I)} = x\theta'_k + y\theta'_{k+1}$ y así

$$|x\theta'_k + y\theta'_{k+1}| = \frac{|\delta'|}{N(I)} < \frac{|\theta'_{k+1}|N(I)}{N(I)} = |\theta'_{k+1}|. \tag{29}$$

Para $k \geq 2$ se tiene $\theta_k = \prod_{j=1}^{k-1}(\alpha_{j-1} - q_{j-1})$. Entonces

$$\theta_k(\alpha_{k-1} - q_{k-1}) = \prod_{j=1}^{k}(\alpha_{j-1} - q_{j-1}) = \theta_{k+1}.$$

De esto

$$\theta'_{k+1} = \theta'_k(\alpha'_{k-1} - q_{k-1}). \tag{30}$$

Como $I = I_1$ es reducido, por la Afirmación 4, tenemos que $\alpha'_1 < 0$. Luego por la Afirmación 2, se obtiene $\alpha'_{1+j} < 0$ para toda $j \geq 0$. Así que $\alpha'_{k-1} < 0$ y por tanto $\alpha'_{k-1} - q_{k-1} < 0$. De ahí y de (30) observamos que θ'_{k+1} y θ'_k tienen signos diferentes, lo cual a continuación mostraremos que contradice (28) y (29).

Primero notemos que por (28), $y \neq 0$. Ya que si $y = 0$, tendríamos que

$$|x|\theta_k = |x\theta_k| < \theta_k.$$

De lo cual $|x| < 1$ y por lo tanto $x = 0$, es decir, $\delta = 0$, lo cual contradice que $\delta > 0$. Análogamente de (29), se tiene que $x \neq 0$.

Ahora probemos lo siguiente:

(31) Si $\quad |x\theta_k + y\theta_{k+1}| < \theta_k,$ entonces x y y tienen signos diferentes.

Por la observación anterior x y y son distintos de cero. Supongamos que $x > 0$ y $y > 0$. Puesto que θ_k y θ_{k+1} son positivos, entonces por (28)

$$|x\theta_k + y\theta_{k+1}| = x\theta_k + y\theta_{k+1} < \theta_k. \tag{32}$$

También $x\theta_k \geq \theta_k$, entonces $x\theta_k + y\theta_{k+1} > \theta_k$. De ahí y de (32), se obtiene

$$\theta_k < x\theta_k + y\theta_{k+1} < \theta_k,$$

es decir $\theta_k < \theta_k$, lo cual es una contradicción.

Ahora supongamos $x < 0$ y $y < 0$. Se tiene que

$$|x\theta_k + y\theta_{k+1}| = |(-1)(-x\theta_k - y\theta_{k+1})| = |-x\theta_k - y\theta_{k+1}| < \theta_k.$$

Como $-x > 0$ y $-y > 0$, por el caso anterior se obtiene una contradicción.

Por lo tanto si $|x\theta_k + y\theta_{k+1}| < \theta_k$, entonces x y y tienen signos distintos.

Ahora por (31) y por el hecho de que θ'_k y θ'_{k+1} tienen signos diferentes, se puede ver que $x\theta'_k$ y $y\theta'_{k+1}$ tienen signos iguales. Pero si $x\theta'_k > 0$ y $y\theta'_{k+1} > 0$, entonces se tiene

$$|x\theta'_k + y\theta'_{k+1}| = x\theta'_k + y\theta'_{k+1} > y\theta'_{k+1} = |y\theta'_{k+1}| = |y||\theta'_{k+1}| \geq |\theta'_{k+1}|,$$

contradiciendo a (29).

Ahora si $x\theta'_k < 0$ y $y\theta'_{k+1} < 0$, entonces

$$|x\theta'_k + y\theta'_{k+1}| = |(-1)(-x\theta'_k - y\theta'_{k+1})| = | - x\theta'_k - y\theta'_{k+1}| = -x\theta'_k - y\theta'_{k+1}$$
$$> -y\theta'_{k+1} = |y\theta'_{k+1}| = |y||\theta'_{k+1}| \geq |\theta'_{k+1}|,$$

lo cual contradice a (29).

Por lo que se concluye que

$$\delta = N(I)\theta_k.$$

Finalmente, vamos a usar las afirmaciones anteriores para concluir nuestro teorema.

Previo a la justificación de la Afirmación 1 mostramos que $(Q_0\theta_k)I_k = (Q_{k-1})I_1$ para $k \geq 2$. Entonces

$$\frac{1}{\sigma}(Q_0\theta_k)I_k = \frac{1}{\sigma}(Q_{k-1})I_1,$$

es decir,

$$(N(I)\theta_k)I_k = (N(I_k))I_1. \tag{33}$$

Entonces

$$N((N(I)\theta_k)I_k) = N((N(I_k))I_1). \tag{34}$$

Por el Teorema 3.2.10 tenemos que

$$N((N(I)\theta_k)I_k) = |N(N(I)\theta_k)|N(I_k) = |N(I)^2N(\theta_k)|N(I_k)$$
$$= N(I)^2|N(\theta_k)|N(I_k). \tag{35}$$

y

$$N((N(I_k))I_1) = N(I_k)^2N(I_1). \tag{36}$$

Sustituyendo (35) y (36) en (34), tenemos que

$$N(I)^2|N(\theta_k)|N(I_k) = N(I_k)^2N(I_1). \tag{37}$$

Como $\delta = N(I)\theta_k$, tenemos $N(\delta) = N(N(I)\theta_k) = N(I)^2N(\theta_k)$. Luego por (37), se obtiene que

$$|N(\delta)|N(I_k) = N(I)^2|N(\theta_k)|N(I_k) = N(I_k)^2N(I_1).$$

De ahí

$$|N(\delta)| = N(I_k)N(I). \tag{38}$$

Por la parte final de la Afirmación 7, tenemos $(\delta)J = (N(J))I$, así que $N((\delta)J) = N((N(J))I)$ y de lo cual

$$|N(\delta)|N(J) = N(J)^2N(I).$$

Por lo que

$$|N(\delta)| = N(J)N(I).$$

Entonces de ahí y de (38), obtenemos que

$$N(J) = \frac{|N(\delta)|}{N(I)} = \frac{N(I_k)N(I)}{N(I)} = N(I_k).$$

Luego de la igualdad anterior y de (33) se tiene

$$(\delta)I_k = (N(I)\theta_k)I_k = (N(I_k))I = (N(J))I = (\delta)J,$$

entonces

$$(\delta)I_k = (\delta)J.$$

Por lo tanto $I_k = J$.

La Afirmación 8 nos dice que un ideal reducido equivalente a I_1, debe ser un I_k para alguna $k \geq 1$. □

La siguiente proposición es consecuencia del Teorema 3.3.23 y relaciona la longitud del período de la fracción continua simple de uno de los generadores de un O_Δ-ideal primitivo con el número de ideales reducidos que son equivalentes a dicho ideal.

Proposición 3.3.24. *Sean $\Delta > 0$ un discriminante, $I = I_1 = \left[\frac{Q_0}{\sigma}, \frac{P_0 + \sqrt{d}}{\sigma}\right]$ un ideal primitivo en O_Δ y $\alpha_0 = \frac{P_0 + \sqrt{d}}{Q_0}$ el irracional cuadrático que le corresponde vía (15). Entonces el número de ideales reducidos equivalentes a I es menor o igual a la longitud del período de la fracción continua de α_0 ($l(\alpha_0)$).*

DEMOSTRACIÓN. Como α_0 es un irracional cuadrático entonces por el Teorema 2.2.7 su representación en fracción continua es periódica. Es decir, existen un entero $m \geq 0$ y $l \in \mathbb{N}$ tal que $q_n = q_{n+l}$ para toda $n \geq m$. Esto es,

$$\alpha = \alpha_0 = [q_0, \ldots, q_{m-1}, \overline{q_m, q_{m+1}, \ldots, q_{l+m-1}}],$$

donde $l = l(\alpha_0)$ es la longitud del período de α_0.

Como en el Lema 2.2.8 se tiene que

$$\alpha_k = [q_k, q_{k+1}, \ldots]$$

para $k \geq 0$.

Sea

$$I_k = \left[\frac{Q_{k-1}}{\sigma}, \frac{P_{k-1} + \sqrt{d}}{\sigma}\right],$$

como en el Teorema 3.3.23.

Ahora por la correspondencia de irracionales cuadráticos a O_Δ-ideales primitivos dada en (15), tenemos que

$$\alpha_{k-1} \longrightarrow [\alpha_{k-1}] = I_k.$$

Entonces

$$\begin{array}{rcll}
\alpha = \alpha_0 & = & [q_0, \ldots, q_{m-1}, \overline{q_m, q_{m+1}, \ldots, q_{l+m-1}}] & \longrightarrow I = I_1 \\
\alpha_1 & = & [q_1, \ldots, q_{m-1}, \overline{q_m, q_{m+1}, \ldots, q_{l+m-1}}] & \longrightarrow I_2 \\
\vdots & \vdots & \vdots & \vdots \\
\alpha_m & = & [\overline{q_m, q_{m+1}, \ldots, q_{l+m-1}}] & \longrightarrow I_{m+1} \\
\alpha_{m+1} & = & [q_{m+1}, \ldots, q_{l+m-1}, \overline{q_m, q_{m+1}, \ldots, q_{l+m-1}}] & \longrightarrow I_{m+2} \\
\vdots & \vdots & \vdots & \vdots
\end{array}$$

De lo anterior notemos que $l(\alpha_0) = l(\alpha_k)$ para toda $k \geq 1$ y que

$$\alpha_{m+1} = [\overline{q_{m+1}, \ldots, q_{l+m-1}, q_m}].$$

Luego por el hecho de que la fracción continua de α_0 es periódica, se tiene que

$$\alpha_{l+m} = [\overline{q_{l+m}, q_{l+m+1}, \ldots, q_{2l+m-1}}] = [\overline{q_m, q_{m+1}, \ldots, q_{l+m-1}}] = \alpha_m.$$

De ahí que

$$I_{l+m+1} = I_{m+1}.$$

Entonces para toda $k \geq m$, la representación en fracción continua de α_k es puramente periódica con $\alpha_k = \alpha_{k+l}$, donde $l = l(\alpha_0) = l(\alpha_k)$. Por lo que

$$I_{k+1} = I_{k+l+1} \quad \text{para toda} \quad k \geq m.$$

Así que a partir de I_{m+1} comienza un ciclo periódico de ideales de longitud $l = l(\alpha_0)$. Entonces por el Teorema 3.3.23 aplicado a I_{m+1}, se tiene que

$$I_{m+1} \sim I_{m+2} \sim \ldots \sim I_{l+m+1} = I_{m+1}.$$

Puesto que α_k es puramente periódica para toda $k \geq m$, entonces por el Teorema 2.2.13 tenemos que α_k es un irracional cuadrático reducido para toda $k \geq m$. Luego por el Corolario 3.3.9 obtenemos que I_{k+1} es reducido para toda $k \geq m$. Así que por el Teorema 3.3.23 el ciclo de ideales

$$I_{m+1}, I_{m+2}, \ldots, I_{l+m}$$

está formado por ideales reducidos y esos son todos los ideales reducidos equivalentes a I_{m+1}.

Si los ideales $I_{m+1}, \ldots, I_{l+m}$ son todos distintos, entonces tenemos que:

Número de ideales reducidos equivalentes a $I_{m+1} = l(\alpha_m)$.

Si al menos dos ideales de $I_{m+1}, \ldots, I_{l+m}$ son iguales, entonces:

Número de ideales reducidos equivalentes a $I_{m+1} < l(\alpha_m)$.

Por lo tanto:

Número de ideales reducidos equivalentes a $I_{m+1} \leq l(\alpha_m)$.

Pero también por el Teorema 3.3.23 para toda $k \geq 1$ se tiene que $I \sim I_k$. De ahí que el número de ideales reducidos equivalentes I es igual al número de ideales reducidos equivalentes a I_{m+1}. Por tanto

Número de ideales reducidos equivalentes a $I \leq l = l(\alpha_0) = l(\alpha_m)$.

□

Ejemplo 3.3.25. *Si* $\Delta = 233$*, entonces* $A_F = O_\Delta = \left[1, \frac{1+\sqrt{233}}{2}\right]$*. Sea*

$$I = I_1 = \left[14, 8 + \frac{1+\sqrt{233}}{2}\right] = \left[14, \frac{17+\sqrt{233}}{2}\right]$$

un O_Δ*-ideal primitivo. Entonces*

$$\alpha_0 = \frac{17+\sqrt{233}}{28}.$$

Por el Teorema 3.3.23 tenemos que

$$I_1 = \left[14, \frac{17+\sqrt{233}}{2}\right] \sim I_2 = \left[2, \frac{11+\sqrt{233}}{2}\right] \sim I_3 = \left[8, \frac{13+\sqrt{233}}{2}\right]$$
$$\sim I_4 = \left[7, \frac{3+\sqrt{233}}{2}\right] \sim I_5 = \left[4, \frac{11+\sqrt{233}}{2}\right] \sim I_6 = \left[4, \frac{13+\sqrt{233}}{2}\right]$$
$$\sim I_7 = \left[7, \frac{11+\sqrt{233}}{2}\right] \sim I_8 = \left[8, \frac{3+\sqrt{233}}{2}\right] \sim I_9 = \left[2, \frac{13+\sqrt{233}}{2}\right]$$
$$\sim I_{10} = \left[1, \frac{15+\sqrt{233}}{2}\right] \sim I_{11} = \left[2, \frac{15+\sqrt{233}}{2}\right] = I_2.$$

Veamos que I_1 *no es un ideal reducido. Por el Corolario 3.2.13, tenemos que*

$$I_1 = \left[14, \frac{2n14+17+\sqrt{233}}{2}\right],$$

para toda $n \in \mathbb{Z}$*. Si* $n > 0$*, siempre se cumple que*

$$\frac{2n14+17-\sqrt{233}}{2} > 0.$$

Si $n < 0$*, siempre se cumple que*

$$\frac{2n14+17+\sqrt{233}}{2} < N(I_1) = 14.$$

Entonces por la contrapositiva del Teorema 3.3.7, I_1 *no es un ideal reducido.*

Es fácil ver que I_r *con* $r = 2, 3, \ldots, 10$ *son ideales reducidos. Por otro lado la fracción continua simple de* α_0 *es:*

$$\alpha_0 = [1, 6, \overline{1, 1, 3, 3, 1, 1, 7, 15, 7}],$$

de donde observamos que $l(\alpha_0) = 9$*.*

Así que en efecto, como dice la Proposición 3.3.24, el número de ideales reducidos equivalentes a I_1 *coincide con la longitud del período de* α_0*.*

El siguiente resultado es una aplicación de todo lo antes visto que nos da un criterio de divisibilidad para el número de clases de un campo cuadrático.

Teorema 3.3.26. *Sea $\Delta = \Delta_0 > 0$ un discriminante fundamental con radicando $d = d_0 = \sigma^2 a^m + b^2$, tal que $a > 1$ y $m > 1$. Entonces existe un divisor n de m tal que $n|h_\Delta$ y $n > \dfrac{\log_a(d/\sigma^2)}{l+1}$, donde $l = l(w_\Delta)$ es el período de la fracción continua de w_Δ y h_Δ es el número de clases de $\mathbb{Q}(\sqrt{d_0})$.*

DEMOSTRACIÓN. Primero supongamos que $mcd(a,b) = s > 1$. Entonces $s|a$ y $s|b$. De ahí que $s^2|a^m$ y $s^2|b^2$. También $s^2|\sigma^2 a^m$. Así que $s^2|\sigma^2 a^m + b^2 = d$, lo cual contradice que d es libre de cuadrados. Por lo tanto $mcd(a,b) = 1$.

Sea $I = \left[a, \dfrac{b+\sqrt{d}}{\sigma}\right]$ un ideal en O_Δ. Probemos que $I^m = \left[a^m, \dfrac{b+\sqrt{d}}{\sigma}\right]$. Si $m = 2$, sea $\alpha \in I^2$, entonces

$$\begin{aligned}
\alpha &= \sum_{i=1}^{n} a_i b_i \quad \text{con} \quad a_i \in I \quad \text{y} \quad b_i \in I \\
&= \sum_{i=1}^{n} \left(\alpha_i a + \frac{\beta_i(b+\sqrt{d})}{\sigma}\right)\left(\gamma_i a + \frac{\delta_i(b+\sqrt{d})}{\sigma}\right) \quad \text{con } \alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{Z} \\
&= \sum_{i=1}^{n} \left(\alpha_i\gamma_i a^2 + \left(\frac{b+\sqrt{d}}{\sigma}\right)(\alpha_i\delta_i a + \beta_i\gamma_i a) + \beta_i\delta_i\left(\frac{b+\sqrt{d}}{\sigma}\right)^2\right) \\
&= \sum_{i=1}^{n} \left(\alpha_i\gamma_i a^2 + \left(\frac{b+\sqrt{d}}{\sigma}\right)(\alpha_i\delta_i a + \beta_i\gamma_i a)\right) \\
&+ \sum_{i=1}^{n} \beta_i\delta_i\left(\frac{b^2 + 2b\sqrt{d} + \sigma^2 a^2 + b^2}{\sigma^2}\right) \\
&= \sum_{i=1}^{n} \left(\alpha_i\gamma_i a^2 + \left(\frac{b+\sqrt{d}}{\sigma}\right)(\alpha_i\delta_i a + \beta_i\gamma_i a)\right) \\
&+ \sum_{i=1}^{n} \beta_i\delta_i\left(\frac{2b}{\sigma}\left(\frac{b+\sqrt{d}}{\sigma}\right) + a^2\right) \\
&= \sum_{i=1}^{n} \left(a^2(\alpha_i\gamma_i + \beta_i\delta_i) + \left(\frac{b+\sqrt{d}}{\sigma}\right)\left(\alpha_i\delta_i a + \beta_i\gamma_i a + \frac{\beta_i\delta_i 2b}{\sigma}\right)\right).
\end{aligned}$$

De ahí se obtiene que $I^2 \subseteq a^2\mathbb{Z} + \left(\dfrac{b+\sqrt{d}}{\sigma}\right)\mathbb{Z}$.

Por otro lado es claro que $a^2 \in I^2$. Vamos a probar que $\dfrac{b+\sqrt{d}}{\sigma} \in I^2$. Se tiene que

$$\frac{2b}{\sigma}\left(\frac{b+\sqrt{d}}{\sigma}\right) + a^2 = \left(\frac{b+\sqrt{d}}{\sigma}\right)\left(\frac{b+\sqrt{d}}{\sigma}\right) \in I^2,$$

de lo cual $\frac{2b}{\sigma}\left(\frac{b+\sqrt{d}}{\sigma}\right) \in I^2$. También $a\left(\frac{b+\sqrt{d}}{\sigma}\right) \in I^2$. Por lo tanto cualquier combinación entera de $\frac{2b}{\sigma}\left(\frac{b+\sqrt{d}}{\sigma}\right)$ y $a\left(\frac{b+\sqrt{d}}{\sigma}\right)$ pertenece a I^2. Como $mcd(a,b)=1$, tenemos que $ax+by=1$ para ciertos $x, y \in \mathbb{Z}$. Si $\sigma = 2$, entonces

$$\frac{b+\sqrt{d}}{2} = a\left(\frac{b+\sqrt{d}}{2}\right)x + b\left(\frac{b+\sqrt{2}}{2}\right)y \in I^2.$$

Si $\sigma = 1$ y a es impar, entonces $mcd(a,2b)=1$ puesto que $mcd(a,b)=1$. De ahí y análogamente al argumento anterior, se obtiene que $b+\sqrt{d} \in I^2$. Ahora si $\sigma = 1$ y a es par, entonces b es impar ya que $mcd(a,b)=1$. Así que $b^2 \equiv 1 \pmod 4$ y $a^2 \equiv 0 \pmod 4$, de donde $d = a^2+b^2 \equiv 1 \pmod 4$. Lo cual es imposible puesto que $\sigma = 1$ implica que $d \equiv 2,3 \pmod 4$. Por lo tanto este último caso no puede suceder. Luego $\frac{b+\sqrt{d}}{\sigma} \in I^2$ y entonces $I^2 = \left[a^2, \frac{b+\sqrt{d}}{\sigma}\right]$.

Por inducción tenemos que $I^m = \left[a^m, \frac{b+\sqrt{d}}{\sigma}\right]$. Si $I' = \left[a, \frac{b-\sqrt{d}}{\sigma}\right]$ análogamente a lo anterior se prueba que $I'^m = \left[a^m, \frac{b-\sqrt{d}}{\sigma}\right]$. Ahora probemos que $I^m \sim 1$.

$$\begin{aligned} I^m &= \left[a^m, \frac{b+\sqrt{d}}{\sigma}\right] = \left[\frac{d-b^2}{\sigma^2}, \frac{b+\sqrt{d}}{\sigma}\right] = \left(\frac{b+\sqrt{d}}{\sigma}\right)\left[\frac{\sqrt{d}-b}{\sigma}, 1\right] \\ &= \left(\frac{b+\sqrt{d}}{\sigma}\right)\left[1, \frac{\sqrt{d}-b}{\sigma}\right]. \end{aligned}$$

Si $\sigma = 1$, por el Corolario 3.2.13, se tiene que

$$I^m = \left(b+\sqrt{d}\right)[1, \sqrt{d}-b] = \left(b+\sqrt{d}\right)[1, b+\sqrt{d}-b] = \left(b+\sqrt{d}\right)[1, w_\Delta].$$

Si $\sigma = 2$. Se tiene que b es impar pues de lo contrario $d = 4a^m + b^2$ tendría un cuadrado. Así que $\frac{b+1}{2} \in \mathbb{Z}$. Entonces por el Corolario 3.2.13 tenemos que

$$\begin{aligned} I^m &= \left(\frac{b+\sqrt{d}}{2}\right)\left[1, \frac{\sqrt{d}-b}{2}\right] = \left(\frac{b+\sqrt{d}}{2}\right)\left[1, \frac{b+1}{2} + \frac{\sqrt{d}-b}{2}\right] \\ &= \left(\frac{b+\sqrt{d}}{2}\right)[1, w_\Delta]. \end{aligned}$$

En ambos casos $I^m \sim 1$ y análogamente $I'^m \sim 1$. Si n es el orden de la clase de I en el grupo de clases de ideales de O_Δ, entonces $n | h_\Delta$. Como $I^m \sim 1$, entonces $n|m$.

Ahora probemos que $n > \dfrac{\log_a(d/\sigma^2)}{l+1}$. Sea $r = \left\lfloor \dfrac{\log_a(d/\sigma^2)}{2n} \right\rfloor$. Primero vamos a ver que $\{I^{jn}, I'^{jn}\}_{j=0}^{r}$ son $2r+1$ ideales principales distintos. Puesto que $I^n = (\gamma)$, para cierta $\gamma \in O_\Delta$, tenemos $I'^n = (\gamma')$. De hecho se puede ver fácilmente que n también es el orden de I'.

Probemos entonces que los I^{jn} son distintos para $j = 0, 1, \ldots, r$. Como $I^n = (\gamma)$, se tiene $I^{r_1 n} = (\gamma^{r_1})$ e $I^{r_2 n} = (\gamma^{r_2})$ para $r_1, r_2 \in \mathbb{N}_0$, tal que $0 \leq r_1, r_2 \leq r$. Supongamos sin pérdida de generalidad que $r_1 < r_2$ y que

$$(\gamma^{r_1}) = (\gamma^{r_2}).$$

Entonces $\gamma^{r_1} = \gamma^{r_2}\beta$ para cierta $\beta \in O_\Delta$. De ahí tenemos que $1 = \gamma^{r_2 - r_1}\beta$ $(r_2 - r_1 > 0)$. Así que γ es unidad y por tanto $I^n = O_\Delta$. Como $I^n \subseteq I$, tenemos $I = O_\Delta$. De ahí se tiene que $1 = as + \left(\dfrac{b+\sqrt{d}}{\sigma}\right)t$, para ciertos $s, t \in \mathbb{Z}$. Obtenemos de ahí que $t = 0$ y así $1 = as$. Pero $1 = as$ es una contradicción pues $a > 1$. Entonces $r_2 \leq r_1$. Análogamente al argumento anterior obtenemos una contradicción cuando $r_2 < r_1$. Por lo tanto $r_2 = r_1$.

La prueba de que los I'^{jn} son distintos para $j = 0, \ldots, r$ es análoga a la anterior. Veamos ahora que los I^{jn} son distintos a los I'^{jn}. Sean $I^{r_1 n} = (\gamma^{r_1})$, $I'^{r_2 n} = (\gamma'^{r_2})$, para $r_1, r_2 \in \mathbb{N}_0$, tal que $0 \leq r_1, r_2 \leq r$. Supongamos que $(\gamma^{r_1}) = (\gamma'^{r_2})$. Entonces $\gamma^{r_1} = \gamma'^{r_2}\alpha$ para cierta $\alpha \in O_\Delta$ y α unidad. Luego

$$N(\gamma^{r_1}) = N(\gamma'^{r_2}\alpha) = N(\gamma'^{r_2})N(\alpha) = \pm(N(\gamma'))^{r_2}.$$

De ahí que

$$(N(\gamma))^{r_1} = \pm(N(\gamma'))^{r_2} = \pm(N(\gamma))^{r_2}.$$

Por lo que $r_1 = r_2$ y así $(\gamma^{r_1}) = (\gamma'^{r_1})$, es decir, $(\gamma)^{r_1} = (\gamma')^{r_1}$. Entonces $(\gamma) = (\gamma')$, es decir, $I^n = I'^n$, por lo que $I = I'$. Así que

$$\left[a, \frac{b+\sqrt{d}}{\sigma}\right] = \left[a, \frac{b-\sqrt{d}}{\sigma}\right],$$

de lo cual $\dfrac{b+\sqrt{d}}{\sigma} = as + t\left(\dfrac{b-\sqrt{d}}{\sigma}\right)$ para ciertos $s, t \in \mathbb{Z}$. De ahí que $b = as\sigma + tb$ y $t = -1$. Así que $b = as\sigma - b$ y entonces $as\sigma = 2b$. De donde $a|2b$ y como $mcd(a, b) = 1$, entonces $a|2$. Como $a > 1$, se tiene que $a = 2$, por lo que

$$I = \left[2, \frac{b+\sqrt{d}}{\sigma}\right].$$

Pero I de esa forma es imposible, puesto que si $\sigma = 2$, tenemos que $4s = 2b$, por lo que b es par, lo cual no puede ser pues $mcd(a, b) = 1$. Si $\sigma = 1$, tenemos que $d = 2^m + b^2$. Si b es impar tenemos que $b^2 \equiv 1 \pmod 4$ y como $2^m \equiv 0 \pmod 4$, entonces $d \equiv 1 \pmod 4$, lo cual no es posible pues $\sigma = 1$ implica que $d \equiv 2, 3 \pmod 4$. Ahora si b es par se tiene que $b^2 \equiv 0 \pmod 4$, por lo que $d \equiv 0 \pmod 4$, lo cual tampoco puede ser. Por lo tanto $I^{r_1 n} \neq I'^{r_2 n}$.

Ahora $N(I^{rn}) = N(I^{jn})N(I^{rn-jn}) \geq N(I^{jn})$ para $0 \leq j \leq r$. Como $a \in I$, entonces $a^{rn} \in I^{rn}$ por lo que $N(I^{rn}) \leq a^{rn}$. De lo anterior

$$N(I^{jn}) \leq N(I^{rn}) \leq a^{rn}. \tag{39}$$

Luego

$$\begin{aligned} a^{rn} &= a^{\left\lfloor \frac{\log_a\left(d/\sigma^2\right)}{2n} \right\rfloor n} \leq a^{\left(\frac{\log_a\left(d/\sigma^2\right)}{2n}\right)n} = a^{\frac{\log_a\left(d/\sigma^2\right)}{2}} \\ &= \left(a^{\log_a(d/\sigma^2)}\right)^{\frac{1}{2}} = \left(\frac{d}{\sigma^2}\right)^{\frac{1}{2}} = \frac{\sqrt{d}}{\sigma}. \end{aligned}$$

De ahí que $a^{rn} \leq \dfrac{\sqrt{d}}{\sigma}$. Nótese que la desigualdad es estricta ya que a^{rn} es un entero. De lo anterior y de (39)

$$N(I^{jn}) \leq a^{rn} < \frac{\sqrt{d}}{\sigma} = \frac{\sqrt{\Delta}}{2}.$$

Por el Corolario 3.3.12, tenemos que I^{jn} es reducido para $0 \leq j \leq r$. Análogamente se puede mostrar que $N(I'^{jn}) < \dfrac{\sqrt{\Delta}}{2}$ para $0 \leq j \leq r$, por lo que I'^{jn} también es reducido para $0 \leq j \leq r$. Así que por la Proposición 3.3.24 se tiene que $l = l(w_\Delta) \geq 2r + 1$. Por otro lado se tiene que

$$2r + 1 = 2\left\lfloor \frac{\log_a(d/\sigma^2)}{2n} \right\rfloor + 1 > 2\left(\frac{\log_a(d/\sigma^2)}{2n} - 1\right) + 1 = \frac{\log_a(d/\sigma^2)}{n} - 1.$$

Entonces

$$l \geq 2r + 1 > \frac{\log_a(d/\sigma^2)}{n} - 1.$$

De donde

$$n > \frac{\log_a(d/\sigma^2)}{l+1}.$$

□

Ejemplo 3.3.27. *Sea* $d = 65 \equiv 1 \pmod 4$. *Entonces* $A_F = O_\Delta = \left[1, \dfrac{1+\sqrt{65}}{2}\right]$. *Observemos que* $\sigma = 2$ *y que* $65 = 2^2 \cdot 2^2 + 7^2$. *Siguiendo el Teorema 3.3.26, tenemos que* $a = 2, b = 7$ *y* $m = 2$. *Entonces los divisores de* m *son* 1 *o* 2. *Por otro lado* $w_\Delta = \dfrac{1+\sqrt{65}}{2} = [4, \overline{1, 1, 7}]$, *por lo que* $l = l(w_\Delta) = 3$ *y así* $\dfrac{\log_a(d/\sigma^2)}{l+1} = 1.0056$. *Por el Teorema 3.3.26 se sigue que* $n = 2$ *y que* $2|h_\Delta$, *es decir,* h_Δ *es par. Entonces* $h_\Delta > 1$ *y por tanto* $A_F = O_\Delta = \left[1, \dfrac{1+\sqrt{65}}{2}\right]$ *no es de factorización única.*

Corolario 3.3.28. *Si $d = \sigma^2 a^p + b^2$ es un radicando fundamental donde p es primo y $l < p$, entonces $p|h_\Delta$.*

DEMOSTRACIÓN. Puesto que $l < p$, se tiene $l \leq p - 1$. Pero

$$p - 1 = \log_a(a^p) - 1 = \log_a\left(\frac{d - b^2}{\sigma^2}\right) - 1 \leq \log_a\left(\frac{d}{\sigma^2}\right) - 1.$$

Notemos que la desigualdad $p - 1 \leq \log_a(\frac{d}{\sigma^2}) - 1$ es estricta pues si $\log_a\left(\frac{d}{\sigma^2}\right) = p$, entonces $\frac{d}{\sigma^2} = a^p$. De ahí que $d = a^p\sigma^2$, lo cual no puede ser pues d es libre de cuadrados. Por lo tanto

$$l \leq p - 1 < \log_a\left(\frac{d}{\sigma^2}\right) - 1,$$

de donde

$$l + 1 < \log_a\left(\frac{d}{\sigma^2}\right).$$

Por lo que

$$1 < \frac{\log_a\left(\frac{d}{\sigma^2}\right)}{l + 1}. \tag{40}$$

Por el Teorema 3.3.26 existe un divisor n de p, tal que $n|h_\Delta$ y $n > \frac{\log_a\left(\frac{d}{\sigma^2}\right)}{l + 1}$. Puesto que p es primo tenemos que $n = 1$ o $n = p$. Si $n = 1$, por (40) se tiene

$$1 > \frac{\log_a\left(\frac{d}{\sigma^2}\right)}{l + 1} > 1,$$

lo cual es una contradicción. Por lo tanto $n = p$ y $n|h_\Delta$. □

Finalmente daremos un ejemplo del Corolario 3.3.28, en el cual daremos una familia de anillos de enteros que no son de factorización única. Previamente probaremos el siguiente lema.

Lema 3.3.29. *Sea $n \in \mathbb{N}$ libre de cuadrados. Entonces $l(\sqrt{n}) = 1$ si y sólo si $n = a^2 + 1$ para algún $a \in \mathbb{N}$.*

DEMOSTRACIÓN. Si $l(\sqrt{n}) = 1$, por el Corolario 2.2.15, podemos observar

$$\sqrt{n} = [a, \overline{2a}],$$

para algún $a \in \mathbb{N}$. Entonces

$$\begin{aligned}\sqrt{n} - a &= \frac{1}{2a + \dfrac{1}{2a + (\sqrt{n} - a)}} = \frac{1}{\dfrac{4a^2 + 2a\sqrt{n} - 2a^2 + 1}{a + \sqrt{n}}} \\ &= \frac{a + \sqrt{n}}{2a^2 + 2a\sqrt{n} + 1}.\end{aligned}$$

De ahí que

$$\begin{aligned} a+\sqrt{n} &= (2a^2+2a\sqrt{n}+1)(\sqrt{n}-a) \\ &= 2a^2\sqrt{n}+2an+\sqrt{n}-2a^3-2a^2\sqrt{n}-a. \end{aligned}$$

De lo cual obtenemos $2an-2a^3-2a=0$ y por tanto $n=a^2+1$.

Supongamos que $n=a^2+1$ y hallemos la fracción continua de $\sqrt{n}$. Sea $q_0=\lfloor\sqrt{a^2+1}\rfloor$. Puesto que $a^2+1>a^2$, se tiene que $\sqrt{a^2+1}>a$ y por tanto $\lfloor\sqrt{a^2+1}\rfloor\geq\lfloor a\rfloor=a$. También se tiene que $a^2+1<(a^2+1)^2$, por lo que $\sqrt{a^2+1}<a+1$ y por tanto $\lfloor\sqrt{a^2+1}\rfloor<a+1$. Entonces $a\leq\lfloor\sqrt{a^2+1}\rfloor<a+1$ y ya que $a\in\mathbb{N}$ se tiene que $\lfloor\sqrt{a^2+1}\rfloor=a$. Por lo tanto $q_0=a$ y por el Teorema 2.1.17, tenemos

$$\sqrt{a^2+1}=[a,q_1,\ldots].$$

Luego

$$\sqrt{a^2+1}=a+\frac{1}{r_1}, \tag{41}$$

para algún $r_1\in\mathbb{R}$, tal que $r_1>1$. Por el Teorema 2.1.17 sea $q_1=\lfloor r_1\rfloor$. Por (41) $r_1(\sqrt{a^2+1}-a)=1$, entonces

$$r_1=\frac{1}{\sqrt{a^2+1}-a}\cdot\frac{\sqrt{a^2+1}+a}{\sqrt{a^2+1}+a}=\sqrt{a^2+1}+a.$$

Así

$$q_1=\lfloor r_1\rfloor=\lfloor\sqrt{a^2+1}+a\rfloor=a+\lfloor\sqrt{a^2+1}\rfloor=2a.$$

Luego $r_1=2a+\dfrac{1}{r_2}$, para algún $r_2\in\mathbb{R}$, tal que $r_2>1$. Sea $q_2=\lfloor r_2\rfloor$ y ya que $r_2(r_1-2a)=1$, se tiene

$$r_2=\frac{1}{r_1-2a}=\frac{1}{\sqrt{a^2+1}+a-2a}=\frac{1}{\sqrt{a^2+1}-a}.$$

De ahí es claro que $r_2=r_1$ y así $q_2=\lfloor r_1\rfloor=2a$. Entonces siguiendo un procedimiento análogo a lo anterior y por el Teorema 2.1.17, tenemos

$$\sqrt{a^2+1}=[a,\overline{2a}].$$

Es decir, la representación en fracción continua de $\sqrt{a^2+1}$ es periódica de longitud $l=1$. □

Ejemplo 3.3.30. *Sea $d=a^2+1$ libre de cuadrados y $a>1$. Siguiendo el Corolario 3.3.28, vemos que $\sigma=1$, $p=2$ y $b=1$. Puesto que $\sigma=1$, se tiene que $d\equiv 2$ o $3\pmod 4$. Si a fuera par, se tendría que $d\equiv 1\pmod 4$ y ese no es el caso de d. Así que a tiene que ser impar y por tanto $d\equiv 2\pmod 4$. Por el Lema 3.3.29, tenemos que $l(\sqrt{d})$ es 1. Entonces por el Corolario 3.3.28, se tiene que $2|h_\Delta$. Luego, $h_\Delta>1$ y por tanto*

$$A_F=O_\Delta=[1,\sqrt{a^2+1}]$$

no es de factorización única.

Sean $d = a^2 + 1$ con a impar $(a > 1)$ y d libre de cuadrados, h_Δ el número de clases de $\mathbb{Q}(\sqrt{d})$. Entonces usando el programa Mathematica© V. 5.2 se obtiene la siguiente tabla, la cual confirma el Ejemplo 3.3.30.

Algunos campos cuadráticos con número de clases par

♯	a	$d = a^2 + 1$	h_Δ
1	3	10	2
2	5	26	2
3	9	82	4
4	11	122	2
5	13	170	4
6	15	226	8
7	17	290	4
8	19	362	2
9	21	442	8
10	23	530	4
11	25	626	4
12	27	730	12
13	29	842	6
14	31	962	4
15	33	1090	12
16	35	1226	10
17	37	1370	4
18	39	1522	12
19	45	2026	14
20	47	2210	8
21	49	2402	8
22	51	2602	10
23	53	2810	8
24	55	3026	16
25	59	3482	6
26	61	3722	10
27	63	3970	20
28	65	4226	8
29	67	4490	8
30	69	4762	22
31	71	5042	12
32	73	5330	8

♯	a	$d = a^2 + 1$	h_Δ
33	75	5626	28
34	77	5930	12
35	79	6242	8
36	81	6562	16
37	83	6890	16
38	85	7226	18
39	87	7570	20
40	89	7922	8
41	91	8282	12
42	95	9026	16
43	97	9410	20
44	101	10202	14
45	103	10610	12
46	105	11026	44
47	109	11882	12
48	111	12322	20
49	113	12770	12
50	115	13226	16
51	119	14162	16
52	121	14642	12
53	123	15130	32
54	125	15626	24
55	127	16130	20
56	129	16642	28
57	131	17162	14
58	133	17690	24
59	135	18226	36
60	137	18770	20
61	139	19322	18
62	141	19882	34
63	145	21026	24
64	147	21610	48

♯	a	$d = a^2 + 1$	h_Δ
65	149	22202	12
66	151	22802	12
67	153	23410	52
68	155	24026	20
69	159	25282	32
70	161	25922	20
71	163	26570	20
72	165	27226	58
73	167	27890	20
74	169	28562	20
75	171	29242	38
76	173	29930	16
77	175	30626	32
78	177	31330	40
79	179	32042	16
80	181	32762	18
81	183	33490	48
82	185	34226	36
83	187	34970	24
84	189	35722	44
85	191	36482	16
86	195	38026	74
87	197	38810	24
88	199	39602	20
89	201	40402	28
90	203	41210	32
91	205	42026	30
92	209	43682	24
93	211	44522	36
94	213	45370	32
95	215	46226	28
96	217	47090	32
97	219	47962	38
98	221	48842	18
99	223	49730	28
100	225	50626	96

♯	a	$d = a^2 + 1$	h_Δ
101	227	51530	20
102	229	52442	20
103	231	53362	68
104	233	54290	24
105	235	55226	24
106	237	56170	88
107	241	58082	16
108	245	60026	42
109	247	61010	36
110	249	62002	36
111	253	64010	32
112	255	65026	72
113	259	67082	24
114	261	68122	34
115	263	69170	28
116	265	70226	40
117	267	71290	64
118	269	72362	28
119	271	73442	24
120	273	74530	88
121	275	75626	34
122	277	76730	36
123	279	77842	52
124	281	78962	44
125	283	80090	32
126	285	81226	64
127	287	82370	28
128	289	83522	32
129	291	84682	44
130	295	87026	52
131	297	88210	44
132	299	89402	38
133	301	90602	32
134	303	91810	60
135	305	93026	32
136	309	95482	70

♯	a	$d = a^2 + 1$	h_Δ
137	311	96722	24
138	313	97970	40
139	315	99226	94
140	317	100490	32
141	319	101762	32
142	321	103042	96
143	323	104330	36
144	325	105626	46
145	329	108242	36
146	331	109562	24
147	333	110890	64
148	335	112226	72
149	337	113570	32
150	339	114922	56
151	341	116282	32
152	345	119026	68
153	347	120410	40
154	349	121802	30
155	351	123202	60
156	353	124610	24
157	355	126026	40
158	359	128882	28
159	361	130322	32
160	363	131770	100
161	365	133226	64
162	367	134690	36
163	369	136162	76
164	371	137642	30
165	373	139130	36
166	375	140626	108
167	377	142130	48
168	379	143642	42
169	381	145162	64
170	383	146690	36
171	385	148226	68
172	387	149770	88

♯	a	$d = a^2 + 1$	h_Δ
173	389	151322	24
174	391	152882	44
175	395	156026	48
176	397	157610	32
177	399	159202	80
178	401	160802	40
179	403	162410	40
180	405	164026	130
181	409	167282	36
182	411	168922	56
183	413	170570	80
184	415	172226	48
185	417	173890	68
186	419	175562	48
187	421	177242	40
188	423	178930	80
189	425	180626	52
190	427	182330	68
191	429	184042	76
192	431	185762	28
193	433	187490	60
194	435	189226	154
195	439	192722	28
196	441	194482	84
197	445	198026	54
198	447	199810	128
199	449	201602	56
200	451	203402	38
201	453	205210	88
202	455	207026	72
203	459	210682	78
204	461	212522	38
205	463	214370	48
206	465	216226	112
207	467	218090	40
208	469	219962	40

♯	a	$d = a^2 + 1$	h_Δ
209	471	221842	100
210	473	223730	56
211	475	225626	84
212	477	227530	144
213	479	229442	32
214	481	231362	36
215	483	233290	96
216	485	235226	56
217	487	237170	32
218	489	239122	104
219	491	241082	48
220	495	245026	108
221	497	247010	72
222	499	249002	40
223	501	251002	84
224	503	253010	76
225	505	255026	76
226	509	259082	32
227	511	261122	80
228	513	263170	100
229	517	267290	80
230	519	269362	108
231	521	271442	28
232	523	273530	56
233	525	275626	116
234	527	277730	52
235	529	279842	40
236	531	281962	100
237	533	284090	80
238	535	286226	44
239	537	288370	124
240	539	290522	52
241	541	292682	48
242	545	297026	88
243	547	299210	64
244	549	301402	96

♯	a	$d = a^2 + 1$	h_Δ
245	551	303602	44
246	553	305810	56
247	555	308026	144
248	559	312482	64
249	561	314722	140
250	563	316970	56
251	565	319226	72
252	567	321490	152
253	569	323762	36
254	571	326042	38
255	573	328330	108
256	575	330626	88
257	579	335242	74
258	581	337562	58
259	583	339890	48
260	585	342226	176
261	587	344570	60
262	589	346922	88
263	591	349282	96
264	595	354026	90
265	597	356410	88
266	599	358802	48
267	601	361202	48
268	603	363610	160
269	605	366026	68
270	609	370882	80
271	611	373322	64
272	613	375770	48
273	615	378226	160
274	617	380690	84
275	619	383162	44
276	621	385642	104
277	623	388130	72
278	625	390626	80
279	627	393130	140
280	629	395642	84

♯	a	$d = a^2 + 1$	h_Δ
281	631	398162	52
282	633	400690	112
283	635	403226	56
284	637	405770	68
285	639	408322	88
286	641	410882	56
287	645	416026	188
288	647	418610	64
289	649	421202	52
290	651	423802	172
291	653	426410	64
292	655	429026	72
293	659	434282	64
294	661	436922	42
295	663	439570	136
296	665	442226	104
297	667	444890	72
298	669	447562	90
299	671	450242	60
300	673	452930	92
301	675	455626	140
302	677	458330	60
303	679	461042	76
304	681	463762	100
305	683	466490	48
306	685	469226	126
307	687	471970	152
308	689	474722	56
309	691	477482	52
310	695	483026	68
311	697	485810	64
312	699	488602	158
313	701	491402	56
314	703	494210	64
315	705	497026	124
316	709	502682	52

♯	a	$d = a^2 + 1$	h_Δ
317	711	505522	108
318	713	508370	120
319	715	511226	126
320	717	514090	136
321	719	516962	52
322	721	519842	68
323	723	522730	104
324	725	525626	72
325	727	528530	72
326	729	531442	120
327	731	534362	72
328	733	537290	48
329	735	540226	240
330	737	543170	80
331	739	546122	54
332	741	549082	192
333	745	555026	108
334	747	558010	96
335	749	561002	64
336	751	564002	64
337	753	567010	148
338	755	570026	96
339	759	576082	116
340	761	579122	48
341	763	582170	84
342	765	585226	200
343	767	588290	56
344	769	591362	64
345	771	594442	144
346	773	597530	52
347	777	603730	220
348	779	606842	54
349	781	609962	66
350	783	613090	256
351	785	616226	104
352	787	619370	64

♯	a	$d=a^2+1$	h_Δ
353	789	622522	124
354	791	625682	76
355	795	632026	136
356	797	635210	96
357	799	638402	80
358	801	641602	108
359	803	644810	88
360	805	648026	120
361	809	654482	76
362	811	657722	72
363	813	660970	160
364	815	664226	96
365	817	667490	68
366	819	670762	202
367	821	674042	58
368	823	677330	92
369	825	680626	204
370	827	683930	104
371	831	690562	128
372	833	693890	76
373	835	697226	96
374	837	700570	128
375	839	703922	60
376	841	707282	100
377	845	714026	108
378	847	717410	84
379	849	720802	128
380	851	724202	56
381	853	727610	96
382	855	731026	252
383	859	737882	60
384	861	741322	166
385	863	744770	80
386	865	748226	84
387	867	751690	248
388	869	755162	74

♯	a	$d=a^2+1$	h_Δ
389	871	758642	64
390	873	762130	124
391	875	765626	134
392	877	769130	60
393	879	772642	132
394	881	776162	72
395	883	779690	120
396	885	783226	222
397	887	786770	72
398	889	790322	88
399	891	793882	152
400	895	801026	96
401	897	804610	288
402	899	808202	60
403	901	811802	66
404	903	815410	160
405	909	826282	118
406	911	829922	88
407	913	833570	116
408	917	840890	112
409	919	844562	80
410	921	848242	108
411	923	851930	108
412	925	855626	106
413	927	859330	132
414	929	863042	80
415	931	866762	80
416	933	870490	224
417	935	874226	108
418	937	877970	92
419	939	881722	160
420	941	885482	80
421	945	893026	296
422	947	896810	64
423	949	900602	58
424	951	904402	196

♯	a	$d = a^2 + 1$	h_Δ
425	953	908210	100
426	955	912026	102
427	959	919682	144
428	961	923522	48
429	963	927370	148
430	965	931226	152
431	967	935090	104
432	969	938962	132
433	971	942842	72
434	973	946730	136
435	975	950626	192
436	977	954530	96
437	979	958442	126
438	981	962362	174
439	983	966290	72
440	985	970226	108
441	987	974170	176
442	989	978122	58
443	991	982082	64
444	995	990026	144
445	997	994010	72
446	999	998002	184
447	1001	1002002	124
448	1003	1006010	88
449	1005	1010026	224
450	1009	1018082	84
451	1011	1022122	138
452	1013	1026170	80
453	1015	1030226	108
454	1017	1034290	216
455	1019	1038362	64
456	1021	1042442	124
457	1023	1046530	248
458	1025	1050626	112
459	1027	1054730	80
460	1029	1058842	174

♯	a	$d = a^2 + 1$	h_Δ
461	1031	1062962	68
462	1033	1067090	72
463	1035	1071226	312
464	1037	1075370	104
465	1039	1079522	64
466	1041	1083682	128
467	1045	1092026	136
468	1047	1096210	196
469	1049	1100402	96
470	1051	1104602	98
471	1053	1108810	176
472	1055	1113026	112
473	1059	1121482	160
474	1061	1125722	80
475	1063	1129970	116
476	1065	1134226	308
477	1067	1138490	96
478	1069	1142762	82
479	1071	1147042	184
480	1073	1151330	100
481	1075	1155626	112
482	1077	1159930	184
483	1079	1164242	92
484	1081	1168562	76
485	1083	1172890	224
486	1085	1177226	132
487	1087	1181570	128
488	1089	1185922	192
489	1091	1190282	90
490	1095	1199026	316
491	1097	1203410	72
492	1099	1207802	78
493	1101	1212202	144
494	1103	1216610	68
495	1105	1221026	188
496	1109	1229882	88

♯	a	$d=a^2+1$	h_Δ
497	1111	1234322	84
498	1115	1243226	120
499	1117	1247690	120
500	1119	1252162	156
501	1121	1256642	100
502	1123	1261130	96
503	1125	1265626	186
504	1127	1270130	152
505	1129	1274642	68
506	1131	1279162	168
507	1133	1283690	120
508	1135	1288226	192
509	1137	1292770	156
510	1139	1297322	88
511	1141	1301882	88
512	1145	1311026	120
513	1147	1315610	136
514	1149	1320202	288
515	1151	1324802	72
516	1153	1329410	88
517	1155	1334026	394
518	1159	1343282	72
519	1161	1347922	276
520	1163	1352570	116
521	1165	1357226	84
522	1167	1361890	148
523	1169	1366562	112
524	1171	1371242	74
525	1173	1375930	196
526	1175	1380626	188
527	1177	1385330	128
528	1179	1390042	190
529	1181	1394762	66
530	1183	1399490	168
531	1185	1404226	200
532	1187	1408970	116

♯	a	$d=a^2+1$	h_Δ
533	1189	1413722	100
534	1191	1418482	232
535	1195	1428026	144
536	1197	1432810	304
537	1199	1437602	88
538	1201	1442402	104
539	1203	1447210	200
540	1205	1452026	186
541	1209	1461682	164
542	1211	1466522	104
543	1213	1471370	84
544	1215	1476226	204
545	1217	1481090	112
546	1219	1485962	146
547	1221	1490842	152
548	1223	1495730	96
549	1225	1500626	172
550	1227	1505530	192
551	1229	1510442	84
552	1231	1515362	108
553	1233	1520290	300
554	1235	1525226	120
555	1237	1530170	128
556	1239	1535122	240
557	1241	1540082	84
558	1245	1550026	412
559	1247	1555010	116
560	1249	1560002	92
561	1251	1565002	170
562	1255	1575026	108
563	1259	1585082	132
564	1261	1590122	120
565	1263	1595170	248
566	1265	1600226	184
567	1267	1605290	120
568	1269	1610362	176

♯	a	$d = a^2 + 1$	h_Δ
569	1271	1615442	96
570	1273	1620530	124
571	1275	1625626	320
572	1277	1630730	96
573	1279	1635842	72
574	1281	1640962	224
575	1283	1646090	104
576	1285	1651226	130
577	1287	1656370	408
578	1289	1661522	116
579	1291	1666682	84
580	1295	1677026	160
581	1297	1682210	112
582	1299	1687402	130
583	1301	1692602	104
584	1305	1703026	264
585	1309	1713482	160
586	1311	1718722	176
587	1313	1723970	120
588	1315	1729226	174
589	1317	1734490	232
590	1319	1739762	84
591	1321	1745042	112
592	1323	1750330	296
593	1325	1755626	152
594	1327	1760930	96
595	1329	1766242	264
596	1331	1771562	120
597	1333	1776890	120
598	1335	1782226	284
599	1337	1787570	116
600	1339	1792922	88
601	1341	1798282	128
602	1345	1809026	144
603	1347	1814410	288
604	1349	1819802	86

♯	a	$d = a^2 + 1$	h_Δ
605	1351	1825202	116
606	1353	1830610	240
607	1355	1836026	192
608	1359	1846882	296
609	1361	1852322	104
610	1363	1857770	104
611	1365	1863226	408
612	1367	1868690	100
613	1369	1874162	88
614	1371	1879642	204
615	1373	1885130	192
616	1375	1890626	152
617	1377	1896130	220
618	1379	1901642	120
619	1381	1907162	116
620	1383	1912690	184
621	1385	1918226	160
622	1387	1923770	180
623	1389	1929322	162
624	1391	1934882	104
625	1395	1946026	368
626	1397	1951610	104
627	1399	1957202	116
628	1401	1962802	300
629	1403	1968410	128
630	1405	1974026	106
631	1409	1985282	72
632	1411	1990922	90
633	1413	1996570	300
634	1415	2002226	144
635	1417	2007890	148
636	1419	2013562	198
637	1421	2019242	186
638	1423	2024930	108
639	1425	2030626	300
640	1427	2036330	176

Bibliografía

[1] Biró, A., *Chowlas conjecture*. Acta Arith. **107**, 179-194, (2003).

[2] Biró, A., *Yokoi's conjecture*. Acta Arith. **106**, 85-104, (2003).

[3] Byeon, D., Kim M., Lee J., *Mollin's conjecture*. Acta Arith. **126**, 99-114, (2007).

[4] Gauss, C., F., *Disquisitiones Arithmeticae*. Academia Colombiana de Ciencias Exactas, Físicas y Naturales. Colección Enrique Pérez Arbelaez, No. **10**.

[5] Hardy, G. H., Wright, E. M., *An introduction to the theory of numbers. Fifth edition*, Oxford, at the Clarendon Press, (1979).

[6] Ireland K., Rosen, M., *A classical introduction to modern number theory*. GTM **84** Springer Verlag (1982).

[7] Louboutin, S., Mollin, R. A., Williams, H. C., *Class Numbers of Real Quadratic Fields, Continued Fractions, Reduced Ideals, Prime-Producing Quadratic Polynomials and Quadratic Residue Covers*. Can. J. Math. **44**, 824-842, (1992).

[8] Mollin, R.A., *Fundamental Number Theory with Applications*. CRC Press, serie Discrete Mathematics and its Applications, Boca Raton (1998).

[9] Mollin, R. A., *Palindromy and Ambiguous Ideals Revisited*. Journal of Number Theory. **74**, 98-110, (1999).

[10] Mollin, R. A., *Simple Continued Fraction Solutions for Diophantine Equations*. Expo. Math. **19**, 55-73, (2001).

[11] Mollin, R. A., *Quadratics*. CRC Press, Boca Raton (1996).

[12] Pineda Ruelas, M.,Villa Salvador, G.D., *Teoría Clásica de Números*. En preparación.

[13] Stewart, I., Tall, D., *Algebraic Number Theory*. Chapman and Hall, London, A Halsted Press Book, John Wiley and Sons, New York. (1979)

[14] Williams, H. C., Wunderlich, M. C., *On the Parallel Generation of the Residues for the Continued Fraction Factoring Algorithm*. Mathematics of Computation. **48**, No.177, 405-423 (1987).

Índice alfabético