ORDENES EN CUERPOS CUADRÁTICOS Y EL GRUPO DE CLASES

ANIBAL ARAVENA

1. Introducción

En esta sección veremos los principales resultados sobre ordenes en campos cuadráticos. Usaremos como guía la sección A, capitulo 5 del libro de Cox [Cox89], junto con algunos resultados de la sección 7, capitulo 2 del libro [BS66].

Definición 1.1. (Ordenes) Sea $K/\mathbb{Q}$ una extensión cuadrática. Un orden $\mathcal{O}$ es un subconjunto de K tal que satisface las siguientes condiciones:

1. $\mathcal{O}$ es un anillo con unidad 1.
2. $\mathcal{O}$ es un $\mathbb{Z}$-módulo libre de rango $[K:\mathbb{Q}]=2$ i.e. $\mathcal{O}=\mathbb{Z}\alpha+\mathbb{Z}\beta$ con α,β una base para la extensión $K/\mathbb{Q}$.

Proposición 1.2. *El conjunto $\mathcal{O}_K$ de los enteros algebraicos de K i.e. los elementos $\alpha\in K$ que satisfacen alguna ecuación $f(\alpha)=0$ con f un polinomio mónico en $\mathbb{Z}[x]$, es un orden.*

Demostración: Usaremos el siguiente Teorema

Teorema 1.3. *Escribimos $K=\mathbb{Q}(\sqrt{d})$ donde d un entero libre de cuadrados. Luego $\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\omega_K$, donde*

$$\omega_K := \begin{cases} \frac{1+\sqrt{d}}{2} & si\ d\equiv 1 \mod 4 \\ \sqrt{d} & si\ d\not\equiv 1 \mod 4 \end{cases}.$$

Demostración: [del Teorema 1.3] Los elementos α de $\mathbb{Q}(\sqrt{d})$ tienen la forma

$$\alpha=a+b\sqrt{d},$$

con a y b racionales. Denotamos $\overline{\alpha}$ la conjugación algebraica de α. Luego

$$(x-\alpha)(x-\overline{\alpha})=x^2-2ax+a^2-db^2.$$

Así, α es entero algebraico si y sólo si $2a$ y a^2-db^2 son enteros. Escribimos $2a=m$ con m entero. Luego

$$a^2-db^2=(m^2/4)-db^2\in\mathbb{Z} \text{ entonces } d4b^2\in\mathbb{Z},$$

y ya que d es libre de cuadrados, se tiene que el denominador de b en su forma reducida debe ser divisor de 2.
Escribimos $b=n/2$. Así $a^2-db^2=(m^2/4)-d(n^2/4)$ es entero si y sólo si la congruencia

$$m^2-dn^2\equiv 0 \mod 4, \tag{1.1}$$

tiene solución. Analicemos los residuos de d módulo 4. Si $d\equiv 1 \mod 4$, entonces la congruencia 1.1 toma la forma $m^2\equiv n^2 \mod 4$ y tiene solución si y sólo si m y n tienen la misma paridad. Así

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

donde n y l son enteros fijos. Luego si los enteros m y n varían sobre los enteros teniendo la misma paridad, entonces los enteros n y l recorren todos los enteros. Esto demuestra que $\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$ si $d\equiv 1 \mod 4$.
Supongamos que $d\equiv 2 \mod 4$ o $d\equiv 3 \mod 4$. Si la congruencia 1.1 tiene solución para n impar, luego $d\equiv m^2 \mod 4$, lo cual es imposible. Si n es par i.e. $n=2k$ con k entero, luego la congruencia 1.1 toma la forma $m^2\equiv 0 \mod 4$, luego m es par y escribimos $m=2l$ con l entero. Así

$$\alpha=\frac{m}{2}+\frac{n}{2}\sqrt{d}=l+k\sqrt{d}.$$

Análogamente, si los pares m y n varían sobre el conjunto de los enteros pares, entonces los enteros l y k toman todos los valores enteros posibles. Esto demuestra que $\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}(\sqrt{d})$ si

$d \not\equiv 1 \mod 4$ (notar que el caso $d \equiv 0 \mod 4$ no es considerado ya que d es libre de cuadrados). □

Continuación de la Demostración de la Proposición 1.2. Ya que $\omega_K \notin \mathbb{Q}$, luego $\mathcal{O}_K$ satisface la condición (2). Para demostrar que es anillo con unidad 1, la única dificultad que surge es verificar la propiedad multiplicativa.
Sean $\alpha, \beta \in \mathcal{O}_K$, aplicando el Teorema 1.3 escribimos

$$\alpha = m_1 + n_1\omega_K$$
$$\beta = m_2 + n_2\omega_K,$$

donde $m_i, n_i \in \mathbb{Z}$. Notemos primero que

$$\omega_K^2 = \begin{cases} \omega_K + \frac{1-d}{4} & \text{si } d \equiv 1 \mod 4 \\ d & \text{si } d \not\equiv 1 \mod 4 \end{cases},$$

el cual claramente esta en $\mathcal{O}_K$. Luego

$$\begin{aligned} \alpha \cdot \beta &= (m_1 + n_1\omega_K)(m_2 + n_2\omega_K) \\ &= m_1m_2 + n_1n_2\omega_K^2 + (m_1n_2 + m_2n_1)\omega_K, \end{aligned}$$

el cual está en $\mathcal{O}_K$. □

Proposición 1.4. *Todo orden $\mathcal{O}$ es subconjunto de $\mathcal{O}_K$.*

Demostración: Sea $\mathcal{O}$ un orden y $\alpha \in \mathcal{O}$. Escribimos $\mathcal{O} = \mathbb{Z}\theta_1 + \mathbb{Z}\theta_2$ con θ_i base de $K/\mathbb{Q}$. Definimos

$$\alpha\theta_i = a_{i1}\theta_1 + a_{i2}\theta_2, \qquad a_{ij} \in \mathbb{Z}.$$

Consideremos la matriz $A = [a_{ij}] - \alpha I$. Luego la relación anterior en términos matriciales corresponde a

$$A \begin{pmatrix} \theta_1 \\ \theta_2 \end{pmatrix} = 0.$$

Multiplicando ambos lados por la adjunta B de A, tenemos que

$$BA \begin{pmatrix} \theta_1 \\ \theta_2 \end{pmatrix} = \det A \begin{pmatrix} \theta_1 \\ \theta_2 \end{pmatrix} = 0.$$

Por lo tanto $\det A = 0$ y la ecuación

$$0 = \det A = |[a_{ij}] - \alpha I| = (a_{11} - \alpha)(a_{22} - \alpha) - a_{12}a_{12},$$

determina una relación de integridad para α. Luego $\alpha \in \mathcal{O}_K$. □

Proposición 1.5. *Sea $\mathcal{O}$ un orden, luego existe entero positivo f tal que*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}(f \cdot w_K).$$

Demostración: Ya que $\mathcal{O} \subset \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}w_k$, todo elemento $\alpha \in \mathcal{O}$ se escribe de manera única como

$$\alpha = n_\alpha + m_\alpha\omega_k, \qquad n_\alpha, m_\alpha \in \mathbb{Z}.$$

Sea

$$f = \min\{|m_\alpha| : \alpha \in \mathcal{O}, m_\alpha \neq 0\}.$$

Si $m_\alpha = 0$ para todo $\alpha \in \mathcal{O}$, entonces $\mathcal{O} \subset \mathbb{Z}$ lo cual es imposible por condición (2) de ser orden, luego este f existe y es positivo. Sea $\alpha \in \mathcal{O}$ tal que $\alpha = n_\alpha + f\omega_K$ con $n_\alpha \in \mathbb{Z}$. Ya que $\mathbb{Z} \subset \mathcal{O}$ podemos suponer que $n_\alpha = 0$. Sea $\beta = n + m\omega_k \in \mathcal{O}$ y $m = pf + r$ con $p, r \in \mathbb{Z}$ y $0 \leq r < f$. Luego

$$\beta - p\alpha = n + m\omega_K - pf\omega_K = n + r\omega_K \in \mathcal{O}.$$

Ya que $0 \leq r < f$, por minimalidad de f se tiene que $r = 0$ i.e. f divide m. Esto demuestra la inclusión $\mathcal{O} \subset \mathbb{Z} + \mathbb{Z}(f \cdot \omega_K)$. La otra inclusión viene del hecho que $1, f\omega_K \in \mathcal{O}$ y $\mathcal{O}$ es anillo. □

Definición 1.6. El entero positivo f se denomina el conductor del orden $\mathcal{O}$.

Observación 1.7. Dado $\mathcal{O}_K$ orden maximal, todo orden $\mathcal{O} \subset K$ esta completamente determinado por su conductor f.

Definición 1.8. (Discriminante de un Orden) Sea $\mathcal{O} = \mathbb{Z} + \mathbb{Z}f\omega_K$ el orden de conductor f. El valor

$$D_{\mathcal{O}} = \begin{vmatrix} 1 & f\omega_K \\ 1 & f\overline{\omega_K} \end{vmatrix}^2 = \begin{cases} f^2 d & \text{si } d \equiv 1 \mod 4 \\ 4f^2 d & \text{si } d \not\equiv 1 \mod 4, \end{cases}$$

se denomina el discriminante del orden $\mathcal{O}$.

Proposición 1.9. *Si $\mathcal{O} = \mathbb{Z}\alpha + \mathbb{Z}\beta$, donde $\{\alpha, \beta\}$ es una base cualquiera para el orden $\mathcal{O}$ de conductor f. Entonces*

$$D_{\mathcal{O}} = \begin{vmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{vmatrix}^2.$$

Demostración: Ya que $\mathcal{O} = \mathbb{Z} + \mathbb{Z}f\omega_k = \mathbb{Z}\alpha + \mathbb{Z}\beta$, entonces existe $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$ tal que

$$\begin{pmatrix} \alpha & \beta \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} 1 & f\omega_K \end{pmatrix}.$$

Luego

$$\begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} 1 & f\omega_K \\ 1 & f\overline{\omega}_K \end{pmatrix}.$$

Tomando determinante y elevando al cuadrado se demuestra la proposición. □

Observaciones 1.10.

1. El discriminante es un entero no cero.
2. Notemos que $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$, luego un orden $\mathcal{O}$ está completamente determinado por su discriminante. En efecto sea $\mathcal{O}, \mathcal{O}'$ ordenes de discriminante D en los campos cuadráticos $\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d'})$ con d, d' libre de cuadrados respectivamente. Como $\mathbb{Q}(\sqrt{d'}) = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$, un ejercicio sencillo muestra que $d = d'$. Dado que sus discriminantes son iguales, se tiene que sus conductores son iguales. Luego por la Observación 1.7, se tiene que $\mathcal{O} = \mathcal{O}'$.

2. Ideales propios y el grupo de clases

Sea $\mathcal{O}$ un orden. Para establecer los principales resultados de esta sección, usaremos las siguientes dos Proposiciones

Proposición 2.1. *$\mathcal{O}$ es noetheriano.*

Proposición 2.2. *Todo $\mathcal{O}$-modulo $I \subset K$ distinto de 0 finitamente generado, se puede escribir como:*

$$I = \mathbb{Z}\alpha + \mathbb{Z}\beta$$

Donde α y β forman una base para la extensión $K/\mathbb{Q}$.

Para demostrarlas, usaremos el siguiente Lema.

Lema 2.3. *Sea $\mathfrak{a}$ un ideal no cero de $\mathcal{O}$. Luego el cociente $\mathcal{O}/\mathfrak{a}$ es finito.*

Demostración: [del Lema]. Primero demostraremos que existe c entero distinto de cero tal que $c \in \mathfrak{a}$. Sea $\alpha \in \mathfrak{a}$ distinto de cero. Ya que $\alpha \in \mathcal{O} \subset \mathcal{O}_K$, este satisface una relación del tipo

$$\alpha^2 + b\alpha + c = 0,$$

donde $b, c \in \mathbb{Z}$ y $c \neq 0$. Luego $c \in \mathfrak{a}$ y se cumple lo pedido. Ya que $c\mathcal{O} \subset \mathfrak{a}$, la función proyección $\pi_{\mathfrak{a}} : \mathcal{O} \to \mathcal{O}/\mathfrak{a}$, la cual es sobreyectiva, induce una función sobreyectiva $\overline{\pi}_{\mathfrak{a}} : \mathcal{O}/(c\mathcal{O}) \to \mathcal{O}/\mathfrak{a}$. Por lo tanto, para demostrar que $\mathcal{O}/\mathfrak{a}$ es finito, basta demostrar que $\mathcal{O}/(c\mathcal{O})$ es finito.
Ya que $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(f\omega_K)$, un conjunto de clases representativas para el cociente $\mathcal{O}/(c\mathcal{O})$ esta dado por

$$\{l + k(f\omega_K), 0 \leq l, k \leq c - 1\}$$

luego $|\mathcal{O}/(c\mathcal{O})| = c^2$, en particular es finito y esto demuestra el Lema. □

Demostración: [de la Proposición 2.1]. Sea $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ una cadena ascendente de ideales. Consideramos la cadena

$$\mathcal{O}/\mathfrak{a}_1 \xrightarrow{\varphi_1} \mathcal{O}/\mathfrak{a}_2 \xrightarrow{\varphi_2} \cdots,$$

de morfismos sobreyectivos $\varphi_i : \mathcal{O}/\mathfrak{a}_i \to \mathcal{O}/\mathfrak{a}_{i+1}$. Usando que $|\mathcal{O}/\mathfrak{a}_i|$ es finito y $|\mathcal{O}/\mathfrak{a}_i| \geq |\mathcal{O}/\mathfrak{a}_{i+1}|$, la cadena $|\mathcal{O}/\mathfrak{a}_1| \geq |\mathcal{O}/\mathfrak{a}_2| \geq \cdots$ se estabiliza. Dado que φ_i es inyectiva si y solo sí $\mathfrak{a}_i = \mathfrak{a}_{i+1}$, la desigualdad es estricta si y sólo si $\mathfrak{a}_i \neq \mathfrak{a}_{i+1}$, luego la cadena $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ se estabiliza. Por lo tanto $\mathcal{O}$ es noetheriano. □

Demostración: [de la Proposición 2.2]. Ya que el campo de fracciones de $\mathcal{O}$ es K e I es finitamente generado, existe $a \in \mathcal{O}$ tal que $aI \subset \mathcal{O}$, luego para efectos de la demostración podemos suponer que $I \subset \mathcal{O}$. Sea $\alpha \in I$ distinto de cero. Ya que $I \subset \mathcal{O} = \mathbb{Z} + \mathbb{Z}(f\omega_K)$, α se escribe de manera única como

$$\alpha = n_\alpha + m_\alpha(f\omega_K).$$

Ya que $\alpha \neq 0$, algunos de los enteros n_α, m_α es distinto de cero. Sin perdida de generalidad suponemos que $n_\alpha \neq 0$. Definimos

$$n = \text{mín}\{|n_\alpha| : \alpha \in I, n_\alpha \neq 0\},$$

y sea $\theta_1 \in I$ tal que $\theta_1 = n + m_{\theta_1} f\omega_K$. Por un argumento similar al hecho en la Proposición 1.5, se tiene que para todo $\beta = n_\beta + m_\beta(f\omega_K) \in I$, n_β es divisible por n. Luego para $p_\beta = n_\beta/n \in \mathbb{Z}$, $\beta - p_\beta\theta_1 = r_\beta(f\omega_K) \in \mathbb{Z}(f\omega_K)$ con $r_\beta = m_\beta - p_\beta m_{\theta_1}$. Si $\beta - p_\beta\theta_1 = 0$ para todo $\beta \in I$, entonces $I = \mathbb{Z}\theta_1$, pero el cociente

$$\mathcal{O}/I = (\mathbb{Z} + \mathbb{Z}(f\omega_K))/(\mathbb{Z}\theta_1),$$

es infinito lo cual es imposible por Lema 2.3. Definimos

$$r = \text{mín}\{|r_\beta| : \beta \in I, r_\beta \neq 0\},$$

el cual existe. Análogamente como en Proposición 1.5, se tiene que $\beta \in I$ si y solo si r_β es divisible por r. Si $\theta_2 \in I$ es tal que $\theta_2 = rf\omega_K = \beta - p_\beta\theta_1$ para algún β, entonces todo $\gamma \in I$ satisface $\gamma - p_\gamma\theta_1 \in \mathbb{Z}\theta_2$, esto demuestra que $I = \mathbb{Z}\theta_1 + \mathbb{Z}\theta_2$.
Si θ_1, θ_2 son l.d. entonces existe un racional r tal que

$$r\theta_1 = \theta_2.$$

Luego

$$I = \mathbb{Z}\theta_1 + \mathbb{Z}\theta_2 = \mathbb{Z}(\theta_1 + r\theta_1),$$

lo cual es imposible. Esto demuestra la proposición. □

Definición 2.4. (Ideal fraccionario) Un ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}$ es un $\mathcal{O}$-módulo contenido en K finitamente generado. Si $\mathfrak{a} \subset \mathcal{O}$ diremos que el ideal es entero o simplemente ideal.

Observaciones 2.5.

1. La Proposición 2.1 justifica la ultima frase.
2. La Proposición 2.2 nos dice que

$$\mathfrak{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta,$$

donde α, β forman una base para la extensión $K/\mathbb{Q}$.

Definición 2.6 (Ideal invertible)**.** Sea $\mathfrak{a}$ un ideal fraccionario de $\mathcal{O}$. Diremos que $\mathfrak{a}$ es invertible si existe un ideal fraccionario $\mathfrak{b}$ de $\mathcal{O}$, tal que:

$$\mathfrak{ab} = \mathcal{O}.$$

Definición 2.7. (Ideal propio) Sea $\mathfrak{a}$ un ideal fraccionario de $\mathcal{O}$, diremos que $\mathfrak{a}$ es propio si

$$\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}.$$

Observación 2.8. Ya que $\mathcal{O}$ es un anillo, se tiene que $\mathcal{O} \subset \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$ para todo $\mathfrak{a}$ ideal fraccionario de $\mathcal{O}$. Usando que $1 \in \mathcal{O}$, se tiene que

$$\{\beta \in K : \beta\mathcal{O} \subset \mathcal{O}\} = \mathcal{O}.$$

Además, para todo ideal fraccionario $\mathfrak{a}$ y $\alpha \neq 0$ se cumple que

$$\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \{\beta \in K : \beta(\alpha\mathfrak{a}) \subset (\alpha\mathfrak{a})\}.$$

Luego $\mathfrak{a}$ es propio si y solamente si $\alpha\mathfrak{a}$ es propio. En particular ideales fraccionarios principales i.e. ideales fraccionarios de la forma $\mathfrak{a} = \alpha\mathcal{O}$ con $\alpha \in K$, son propios.

Ejemplo 2.9. (Ideal fraccionario no propio) Consideremos el campo cuadrático imaginario $\mathbb{Q}(\sqrt{-3})$. Por Teorema 1.2 se tiene que $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$ y $\mathcal{O} = \mathbb{Z}+\mathbb{Z}(1+\sqrt{-3})$ es el orden de conductor 2. Sea $\mathfrak{a}$ el ideal fraccionario de $\mathcal{O}$ generado por 2 y $1+\sqrt{-3}$ como $\mathcal{O}$-módulo. Consideremos $\beta_0 = \left(\frac{1+\sqrt{-3}}{2}\right) \in \mathcal{O}_K$. Entonces

$$\begin{aligned}\beta_0 \cdot 2 &= \left(\tfrac{1+\sqrt{-3}}{2}\right) 2 = 1+\sqrt{-3} \in \mathfrak{a}\\ \beta_0 \cdot (1+\sqrt{-3}) &= \left(\tfrac{1+\sqrt{-3}}{2}\right)\left(1+\tfrac{1+\sqrt{-3}}{2}\right)\\ &= -5+(1+\sqrt{-3}) \in \mathfrak{a}.\end{aligned}$$

Luego $\beta_0 \in \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$, pero β_0 no es un elemento de $\mathcal{O}$. Por lo tanto $\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} \neq \mathcal{O}$ y $\mathfrak{a}$ no es ideal propio.

Proposición 2.10. *Sea $\mathcal{O}$ un orden de un campo cuadrático K. Luego un ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}$ es propio si y sólo si $\mathfrak{a}$ es invertible.*

Demostración: ($\Leftarrow$) Supongamos que $\mathfrak{a}$ es invertible. Luego existe ideal fraccionario $\mathfrak{b}$ de $\mathcal{O}$, tal que $\mathfrak{ab} = \mathcal{O}$. Sea $\beta \in K$ con $\beta\mathfrak{a} \subset \mathfrak{a}$. Luego

$$\beta\mathcal{O} = \beta(\mathfrak{ab}) = (\beta\mathfrak{a})\mathfrak{b} \subset \mathfrak{ab} = \mathcal{O}.$$

Luego $\beta \in \mathcal{O}$. Para la implicancia ($\Rightarrow$), usamos el siguiente lema.

Lema 2.11. *Sea $K = \mathbb{Q}(\tau)$ un campo cuadrático y $f_\tau(x) = ax^2+bx+c \in \mathbb{Z}[x]$ con $f_\tau(\tau) = 0$, $(a,b,c) = 1$ y $a > 0$. Luego $\mathfrak{a} = \mathbb{Z}+\mathbb{Z}\tau$ es ideal fraccionario propio del orden $\mathcal{O} = \mathbb{Z}+\mathbb{Z}a\tau$ de K de discriminante b^2-4ac.*

Demostración: [Del Lema] Demostremos primero que $\mathcal{O}$ es efectivamente un orden.
Como $af(\tau) = 0$ si y sólo si $(a\tau)^2 = -b(a\tau) - ac$, se tiene

$$\begin{aligned}(n_1+m_2a\tau)(n_2+m_2a\tau) &= n_1n_2 + m_1m_2(a\tau)^2 + (n_1m_2+n_2m_1)a\tau\\ &= n_1n_2 - acm_1m_2 + (n_1m_2+n_2m_1-bm_1m_2)a\tau \in \mathcal{O}.\end{aligned}$$

Veamos ahora que $\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathbb{Z}+\mathbb{Z}a\tau$. Sea $\beta = x+y\tau \in K$ con x, y números racionales, la condición $\beta\mathfrak{a} \subset \mathfrak{a}$ es equivalente a

$$\begin{aligned}&\beta \cdot 1 = x+y\tau \in \mathfrak{a}\\ &\beta \cdot \tau = x\tau + y\tau^2 = x\tau + \frac{y}{a}(-b\tau - c) = -\frac{cy}{a} + \left(x - \frac{by}{a}\right)\tau \in \mathfrak{a}.\end{aligned}$$

Esto ocurre si y solamente si los números racionales

$$x, y, \frac{cy}{a}, \frac{by}{a},$$

son enteros. Ya que $(a,b,c) = 1$ esto pasa solamente si x, y son enteros e y es divisible por a. Esto demuestra que $\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathbb{Z}+\mathbb{Z}a\tau = \mathcal{O}$.
Luego solamente falta verificar que $\mathfrak{a}$ es ideal fraccionario de $\mathcal{O}$. Para ello notemos que $\mathfrak{a}\mathcal{O} \subset \mathfrak{a}$, luego $\mathfrak{a}$ es $\mathcal{O}$-módulo, además $a\mathfrak{a} = \mathbb{Z}a+\mathbb{Z}a\tau \subset \mathcal{O}$, luego $a\mathfrak{a}$ es ideal de $\mathcal{O}$. Como $\mathcal{O}$ es noetheriano, $a\mathfrak{a}$ es finitamente generado, por lo tanto, así lo es $\mathfrak{a}$.
Por un calculo directo del discriminante D de $\mathcal{O}$ usando la base $1, a\tau$, se tiene que $D = b^2-4ac$.
□

Continuación de la dem Proposición 2.10($\Rightarrow$). Supongamos que $\mathfrak{a}$ es ideal fraccionario propio de $\mathcal{O}$. Por la Proposición 2.2, podemos escribir $\mathfrak{a}$ como

$$\mathfrak{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta = \alpha(\mathbb{Z}+\mathbb{Z}\tau), \qquad \tau = \beta/\alpha \text{ y } \alpha, \beta \text{ base para } K/\mathbb{Q}.$$

Sea $f_\tau(x) = ax^2+bx+c$ como en el lema anterior y $\overline{\tau}$ la otra raíz de f_τ.
Supongamos primero que $\alpha = 1$ i.e. $\mathfrak{a} = \mathbb{Z}+\mathbb{Z}\tau$. Por lema anterior se tiene que $\mathcal{O} = \mathbb{Z}+\mathbb{Z}a\tau$, mas aún, el ideal fraccionario $\mathfrak{a}' = \mathbb{Z}+\mathbb{Z}\overline{\tau}$ es ideal fraccionario propio de $\mathbb{Z}+\mathbb{Z}a\overline{\tau} = \mathbb{Z}+\mathbb{Z}a\tau = \mathcal{O}$

y satisface la relación:

$$\begin{aligned}
\mathfrak{a}\mathfrak{a}' &= (\mathbb{Z}+\mathbb{Z}\tau)(\mathbb{Z}+\mathbb{Z}\overline{\tau}) \\
&= \mathbb{Z}+\mathbb{Z}\tau+\mathbb{Z}\overline{\tau}+\mathbb{Z}\tau\overline{\tau} \\
&= \mathbb{Z}+\mathbb{Z}\tau+\mathbb{Z}(-\tau-b/a)+\mathbb{Z}(-c/a) \\
&= \mathbb{Z}+\mathbb{Z}\tau+\mathbb{Z}(-b/a)+\mathbb{Z}(-c/a) \\
&= \frac{1}{a}(\mathbb{Z}a+\mathbb{Z}b+\mathbb{Z}c+\mathbb{Z}a\tau) \\
&= \frac{1}{a}(\mathbb{Z}+\mathbb{Z}a\tau) && (a,b,c)=1 \\
&= \frac{1}{a}\mathcal{O}.
\end{aligned}$$

Luego $\mathfrak{a}$ es invertible con inversa $a\mathfrak{a}'$. Para el caso general $\mathfrak{a} = \alpha(\mathbb{Z}+\mathbb{Z}\tau)$, consideramos $\mathfrak{a}' = \overline{\alpha}(\mathbb{Z}+\mathbb{Z}\overline{\tau})$, luego tenemos que

$$\mathfrak{a}\mathfrak{a}' = \alpha(\mathbb{Z}+\mathbb{Z}\tau)\,\overline{\alpha}(\mathbb{Z}+\mathbb{Z}\overline{\tau}) = \overline{\alpha}\alpha(\mathbb{Z}+\mathbb{Z}\tau)(\mathbb{Z}+\mathbb{Z}\overline{\tau}) = \frac{\alpha\overline{\alpha}}{a}\mathcal{O}.$$

Luego $\mathfrak{a}$ es invertible con inversa $\mathfrak{a}'a/(\alpha\overline{\alpha})$. □

Observación 2.12. Sea $\mathfrak{a} = \mathbb{Z}\alpha+\mathbb{Z}\beta$ el $\mathbb{Z}$-módulo generado por α,β tal que $\tau = \alpha/\beta \notin \mathbb{Q}$ y sea $K = \mathbb{Q}(\tau)$ un campo cuadrático. Luego por el Lema 2.11 y la Proposición 1.4, se tiene que

$$\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} \subset \mathcal{O}_K.$$

En particular todo ideal fraccionario de $\mathcal{O}_K$ es propio.

Teorema 2.13 (Grupo de ideales fraccionarios)**.** *Dado un orden $\mathcal{O}$, sea $I(\mathcal{O})$ el conjunto de todos los ideales fraccionarios propios de $\mathcal{O}$. Luego $I(\mathcal{O})$ forma un grupo abeliano con la operación de multiplicación y $P(\mathcal{O})$, el conjunto de todos los ideales fraccionarios principales forma un subgrupo de $I(\mathcal{O})$.*

Demostración: Veamos que la operación está bien definida i.e. si $\mathfrak{a},\mathfrak{b} \in I(\mathcal{O})$, entonces $\mathfrak{a}\mathfrak{b} \in I(\mathcal{O})$. Por Proposisión 2.10, existen $\mathfrak{a}^{-1},\mathfrak{b}^{-1} \in I(\mathcal{O})$ tal que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$. Luego

$$\mathfrak{a}\mathfrak{b}\mathfrak{b}^{-1}\mathfrak{a}^{-1} = \mathcal{O}.$$

Por lo tanto $\mathfrak{a}\mathfrak{b}$ es invertible y por la Proposisión 2.10 es propio.
$P(\mathcal{O}) \subset I(\mathcal{O})$ y por la Observación 2.8 claramente es subgrupo. □

Definición 2.14 (Grupo de Clases)**.** El grupo de clases $C(\mathcal{O})$ de un orden $\mathcal{O}$ se define por:

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

3. Cálculo del grupo de Clases

En esta sección veremos como calcular el grupo de clases para ciertos órdenes en campos cuadráticos imaginarios. Al igual que en el estudio del grupo de formas cuadráticas, utilizaremos una teoría de reducción. Esta sección es un tratado basado en la sección 7.7 del capitulo 2 del libro [BS66].
Dado $\mathfrak{a} = \mathbb{Z}\theta_1+\mathbb{Z}\theta_2$ ideal fraccionario de un orden $\mathcal{O}$ de discriminante $D<0$, el conjunto $\{\theta_1,\theta_2\}$ será l.i. sobre $\mathbb{Q}$, mas aún, ya que $K = \mathbb{Q}(\sqrt{D})$ es cuadrático imaginario, luego $K\cap\mathbb{R} = \mathbb{Q}$ y $\{\alpha,\beta\}$ serán también l.i. sobre $\mathbb{R}$. Así, podemos considerar $\mathfrak{a}$ como un reticulado en el plano complejo. Para $\alpha,\beta \in \mathfrak{a}$, denotamos $|\alpha|^2 = \alpha\overline{\alpha}$ el largo al cuadrado de α y $\varphi_{\alpha,\beta}$ el único ángulo en $[0,2\pi)$ entre α y β calculado en sentido antihorario. Definimos

$$\begin{aligned}
A &= \min_{\alpha\in\mathfrak{a}-\{0\}}\{|\alpha|\}, \\
B_\alpha &= \min_{\beta\in\mathfrak{a}-\{\mathbb{Q}\alpha\}}\{|\beta|\}, \qquad \text{para } \alpha\in\mathfrak{a},
\end{aligned}$$

y sea $W = \{\alpha\in\mathfrak{a} : |\alpha| = A\}$ y $V_\alpha = \{\beta\in\mathfrak{a}-\{\mathbb{Q}\alpha\} : |\beta| = B_\alpha\}$.

Proposición 3.1. *Sea $\alpha\in W$ y $\beta\in V_\alpha$, luego $\{\alpha,\beta\}$ generan $\mathfrak{a}$ como $\mathbb{Z}$-módulo.*

Demostración: Primero notemos que que cada par $(\alpha, \beta) \in W \times V_\alpha$ es una base para la extensión $K/\mathbb{Q}$ que cumple $|\beta| \geq |\alpha|$. Supongamos por contradicción que existe $\zeta \in \mathfrak{a}$ tal que $\zeta \notin \mathbb{Z}\alpha + \mathbb{Z}\beta$, luego $\zeta = u\alpha + v\beta$ donde $u, v \in \mathbb{Q}$ no son ambos enteros. Sumando, si es necesario un elemento de $\mathbb{Z}\alpha + \mathbb{Z}\beta$, podemos suponer que $|u| \leq 1/2$ y $|v| \leq 1/2$ y $\zeta \neq 0$. Si $v \neq 0$, luego ζ no es colineal con α. Así

$$|\zeta| = |u\alpha + v\beta| < |u\alpha| + |v\beta| \leq \frac{1}{2}|\alpha| + \frac{1}{2}|\beta| \leq |\beta|.$$

Luego $|\zeta| < |\beta|$ lo cual contradice la elección de β. Si $v = 0$, entonces $|\zeta| = |u\alpha| \leq |\alpha|/2 < |\alpha|$, lo cual contradice la elección de α. Así $\mathfrak{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta$ demostrando la Proposición. □

Sea $(\alpha, \beta) \in W \times V_\alpha$ un par ordenado como antes. Veamos algunas propiedades adicionales que satisface este par para introducir el concepto de base reducida.

Lema 3.2. *Sea $\alpha \in W$ y $\beta \in V_\alpha$. Luego $-\frac{|\alpha|}{2|\beta|} \leq \cos(\varphi_{\alpha,\beta}) \leq \frac{|\alpha|}{2|\beta|}$.*

Demostración: Supongamos primero que $\varphi_{\alpha,\beta} \in (0, \pi)$. Si $\frac{|\alpha|}{2|\beta|} < \cos(\varphi_{\alpha,\beta}) < 1$, aplicando el teorema del coseno se tiene que

$$|\beta - \alpha|^2 = |\alpha|^2 + |\beta|^2 - 2|\beta||\alpha|\cos(\varphi_{\alpha,\beta}) < |\alpha|^2 + |\beta|^2 - 2|\alpha||\alpha|/2 = |\beta|^2.$$

Luego $|\beta - \alpha| < |\beta|$ lo cual es una contradicción por la elección de β. Si $-1 < \cos(\varphi_{\alpha,\beta}) < -\frac{|\alpha|}{2|\beta|}$, luego $\frac{|\alpha|}{2|\beta|} < \cos(\pi - \varphi_{\alpha,\beta}) < 1$ con $\pi - \varphi_{\alpha,\beta} \in (0, \pi)$ y se concluye de manera análoga aplicando el teorema del coseno para $\beta + \alpha$ y $\pi - \varphi_{\alpha,\beta}$. Ahora si $\varphi_{\alpha,\beta} \in (\pi, 2\pi)$, entonces $\varphi_{\alpha,-\beta} = \varphi_{\alpha,\beta} - \pi \in (0, \pi)$ y $|\beta| = |-\beta|$, luego $\cos(\varphi_{\alpha,-\beta}) = -\cos(\varphi_{\alpha,\beta})$ y podemos aplicar el argumento anterior para el par $(\alpha, -\beta)$ concluyendo el Lema. □

Definición 3.3. (Base reducida). Sea $(\alpha, \beta) \in W \times V_\alpha$, diremos que el par ordenado (α, β) es una base reducida para $\mathfrak{a}$ si satisface las siguientes condiciones:

1. $\varphi_{\alpha,\beta} \in (0, \pi)$.
2. $-\frac{|\alpha|}{2|\beta|} \leq \cos(\varphi_{\alpha,\beta}) < \frac{|\alpha|}{2|\beta|}$.
3. Si $|\beta| = |\alpha|$, entonces $-\frac{|\alpha|}{2|\beta|} \leq \cos(\varphi_{\alpha,\beta}) \leq 0$.

Proposición 3.4. *Todo ideal fraccionario tiene base reducida.*

Demostración: Construimos una base reducida de la siguiente manera. Si $\varphi_{\alpha,\beta} \in (\pi, 2\pi)$, elegimos el par $(\alpha, -\beta)$ el cual esta en $W \times V_\alpha$ y satisface la primera condición de ser base reducida. Si la condición (2) no ocurre, por Lema 3.2, necesariamente se tiene que $\cos(\varphi_{\alpha,\beta}) = \frac{|\alpha|}{2|\beta|}$. Sea $\beta' = \beta - \alpha$, aplicando el Teorema del coseno obtenemos que:

$$|\beta'|^2 = |\beta - \alpha|^2 = |\beta|^2 + |\alpha|^2 - 2|\alpha||\beta|\cos(\varphi_{\alpha,\beta}) = |\beta|^2 + |\alpha|^2 - 2|\alpha||\beta|\frac{|\alpha|}{2|\beta|} = |\beta|^2,$$

luego $|\beta'| = |\beta|$. Además, claramente β' es no colineal con α y cumple $\varphi_{\alpha,\beta'} \in (0, \pi)$ (aquí supusimos que $\varphi_{\alpha,\beta'} \in (0, \pi)$ por la primera parte). Como $\beta' \neq \beta$, entonces $\varphi_{\alpha,\beta'} \neq \varphi_{\alpha,\beta}$ y por el Lema 3.2 se tiene que $\cos(\varphi_{\alpha,\beta'}) < \frac{|\alpha|}{2|\beta|}$. Por lo tanto el par $(\alpha, \beta') \in W \times V_\alpha$ satisface la condición (1) y (2).
Si el par (α, β) no satisface la condición (3), (suponiendo que satisface las condiciones (1) y (2)), entonces $|\alpha| = |\beta|$ y por el Lema 3.2 se tiene que $0 < \cos(\varphi_{\alpha,\beta}) < \frac{|\alpha|}{2|\beta|}$. Luego el par $(\beta, -\alpha) \in W \times V_\beta$ cumple que $\varphi_{\beta,-\alpha} = \pi - \varphi_{\alpha,\beta}$ y claramente satisfaces la condición (1), (2) y (3) de ser base reducida. Esto demuestra la proposición. □

Otro Lema útil para el tratamiento de bases reducidas es el siguiente.

Lema 3.5. *Sea $\alpha \in W$ y $\beta_1, \beta_2 \in V_\alpha$. Supongamos que $\varphi_{\alpha,\beta_1}, \varphi_{\alpha,\beta_2} \in (0, \pi)$ y $\varphi_{\alpha,\beta_2} \geq \varphi_{\alpha,\beta_1}$. Entonces $|\beta_1 - \beta_2| \in \{0, |\alpha|\}$. Mas aún, $|\beta_1 - \beta_2| = |\alpha|$ si y sólo si $\cos(\varphi_{\alpha,\beta_1}) = \frac{|\alpha|}{2|\beta_1|}$ y $\cos(\varphi_{\alpha,\beta_2}) = -\frac{|\alpha|}{2|\beta_1|}$*

Demostración: Aplicando el teorema del coseno para $\beta_1 - \beta_2$ y $\varphi^* = \varphi_{\alpha,\beta_2} - \varphi_{\alpha,\beta_1} \in (0, \pi)$, obtenemos

$$|\beta_1 - \beta_2|^2 = |\beta_1|^2 + |\beta_2|^2 - 2|\beta_1||\beta_2|\cos(\varphi^*) = 2|\beta_1|^2(1 - \cos(\varphi^*)).$$

Como la función $\cos(x)$ es estrictamente decreciente en el intervalo $[0, \pi)$, el valor máximo para $|\beta_1 - \beta_2|$ se alcanza únicamente cuando φ^* es máximo. Sean $\varphi_{\alpha,\beta_1,\min}, \varphi_{\alpha,\beta_2,\max} \in (0, \pi)$ tal que

$\cos(\varphi_{\alpha,\beta_2,\max}) = -\frac{|\alpha|}{2|\beta_1|}$ y $\cos(\varphi_{\alpha,\beta_1,\min}) = \frac{|\alpha|}{2|\beta_2|}$ y definimos $\varphi^*_{\max} = \varphi_{\alpha,\beta_2,\max} - \varphi_{\alpha,\beta_1,\min} \in (0,\pi)$. Luego por Lema 3.2 se tiene que $\varphi_{\alpha,\beta_1,\min} \leq \varphi_{\alpha,\beta_1}$ y $\varphi_{\alpha,\beta_2,\max} \geq \varphi_{\alpha,\beta_2}$. Entonces $\varphi^* \leq \varphi^*_{\max}$ y así

$$|\beta_1 - \beta_2|^2 = 2|\beta_1|^2(1-\cos(\varphi^*)) \leq 2|\beta_1|^2(1-\cos(\varphi^*_{\max})) = 4|\beta_1|^2 \sin\left(\frac{\varphi^*_{\max}}{2}\right)^2. \tag{3.2}$$

Por otra parte se tiene que $\varphi_{\alpha,\beta_2,\max} = \pi - \varphi_{\alpha,\beta_1,\min}$, por lo tanto

$$\begin{aligned}\frac{|\alpha|}{|\beta|} &= \cos(\varphi_{\alpha,\beta_1,\max}) - \cos(\varphi_{\alpha,\beta_2,\min}) \\ &= -2\sin\left(\frac{\varphi_{\alpha,\beta_1,\max} + \varphi_{\alpha,\beta_2,\min}}{2}\right)\sin\left(-\frac{\varphi^*_{\max}}{2}\right) \\ &= 2\sin\left(\frac{\pi}{2}\right)\sin\left(\frac{\varphi^*_{\max}}{2}\right) \\ &= 2\sin\left(\frac{\varphi^*_{\max}}{2}\right).\end{aligned}$$

Luego la desigualdad 3.2 se trasforma en

$$|\beta_1 - \beta_2|^2 \leq 4|\beta|^2 \sin\left(\frac{\varphi^*_{\max}}{2}\right)^2 = |\alpha|^2.$$

Así $|\beta_1 - \beta_2| \leq |\alpha|$ y por minimalidad de α se concluye el Lema. □

Proposición 3.6. *Si (α,β) y (α',β') son dos bases reducidas para $\mathfrak{a}$, entonces existe $\eta \in K$, el cual es una raíz de la unidad de grado 1,2,3,4 o 6, tal que $(\eta\alpha,\eta\beta) = (\alpha',\beta')$.*

Demostración: Notemos primero que si $\eta \in K$ es tal que $\eta\alpha = \alpha'$, entonces $\eta\beta = \beta'$, en efecto, como $|\eta| = 1$, el par $(\eta\alpha,\eta\beta)$ es una base reducida, luego aplicando el Lema 3.5 con $\eta\beta'$ y β y usando la condición (2) de ser base reducida obtenemos que $\beta' = \eta\beta$.
Supongamos primero que $|\beta| > |\alpha|$. Sea $\gamma \in W$, por la Proposición 3.1 escribimos $\gamma = m\alpha + n\beta$ con $m,n \in \mathbb{Z}$. Como β es un elemento mas chico no colineal con α y $|\beta| > |\gamma|$, obtenemos $n = 0$, luego $|\gamma| = |m\alpha| = |\alpha|$ y así $W = \{\pm\alpha\}$. Luego existe $\eta \in \{\pm 1\}$, tal que $\eta\alpha = \alpha'$ y por el comentario inicial se tiene que $(-\alpha,-\beta) = (\alpha',\beta')$, tomando $\eta = -1$ demostramos lo pedido.
Si $|\beta| = |\alpha|$ y $\alpha' \notin \{\pm\alpha\}$, entonces $\alpha' \in V_\alpha$. Sea $\zeta \in \{\pm 1\}$ tal que $\varphi_{\alpha,\zeta\alpha'} \in (0,\pi)$. Aplicando el Lema 3.5 con $\zeta\alpha'$ y β obtenemos dos casos:
Caso 1: $|\beta - \zeta\alpha'| = |\alpha|$. Ya que (α,β) es base reducida, por condición (3) y por Lema 3.5, se tiene que necesariamente que $\cos(\varphi_{\alpha,\zeta\alpha'}) = \frac{|\alpha|}{2|\beta|} = \frac{1}{2}$, luego $\varphi_{\alpha,\zeta\alpha'} = \pi/3$ y así $e^{i\pi/3}\zeta\alpha = \alpha'$, luego por el comentario inicial se concluye con $\eta = e^{i\pi/3}\zeta$.
Caso 2: $\beta = \zeta\alpha'$. Entonces los pares $(\zeta\alpha',\zeta\beta'),(\beta,-\alpha) \in W \times V_\beta$ satisfacen $\varphi_{\zeta\alpha',\zeta\beta'},\varphi_{\beta,\alpha} \in (0,\pi)$. Aplicando el Lema 3.5, obtenemos que $|\zeta\beta' + \alpha| \in \{0,|\alpha|\}$. Si $|\zeta\beta' + \alpha| = |\alpha|$, entonces por un argumento similar al caso 1 con el par $(\zeta\alpha',\zeta\beta')$ y $-\alpha$ obtenemos que $e^{i\pi/3}\zeta\alpha' = -\alpha$, luego $\eta = -\zeta e^{i\pi/3}$ cumple lo pedido. Si $\zeta\alpha' = -\alpha$, entonces tenemos que los pares $(\alpha,\beta),(\zeta\alpha',\zeta\beta) = (\beta,-\alpha)$ son bases reducidas, luego por condición (3) necesariamente tenemos que $\varphi_{\alpha,\beta} = \pi/2$. Así $i\alpha = \beta = \zeta\alpha'$, luego $\eta = i\zeta$ cumple lo pedido. Esto demuestra el Lema. □

Corolario 3.7. *Dos ideales fraccionarios $\mathfrak{a}$ y $\mathfrak{b}$ con bases reducidas (α,β) y (α',β') respectivamente pertenecen a una misma clase en $C(\mathcal{O})$ si y solamente existe $\zeta \in K$, tal que $(\zeta\alpha,\zeta\beta) = (\alpha',\beta')$.*

Demostración: ($\Rightarrow$). Si $\mathfrak{a}$ y $\mathfrak{b}$ pertenecen a la misma clase en $C(\mathcal{O})$, entonces existe $\gamma \in K$ tal que $\mathfrak{a} = \gamma\mathfrak{b}$, luego claramente $(\gamma\alpha,\gamma\beta)$ es una base reducida para $\mathfrak{b}$ y por Proposición 3.6, existe η tal que $(\eta\gamma\alpha,\eta\gamma\beta) = (\alpha',\beta')$, luego $\zeta = \eta\gamma$ cumple lo pedido.
($\Leftarrow$). Si $(\zeta\alpha,\zeta\beta) = (\alpha',\beta')$ para algún $\zeta \in K$, entonces $\zeta\mathfrak{a} = \mathfrak{b}$, luego $\mathfrak{a},\mathfrak{b}$ pertenecen a la misma clase en $C(\mathcal{O})$. □

Si $\mathfrak{a}$ es ideal fraccionario con base reducida (α,β), entonces el ideal fraccionario $\mathfrak{a}' = \mathbb{Z} + \mathbb{Z}\tau$ con $\tau = \beta/\alpha$ es equivalente a $\mathfrak{a}$ y tiene base reducida $(1,\tau)$. Ya que $|\beta| \geq |\alpha|$, entonces $|\tau| \geq 1$, mas aún, las condiciones (1), (2) y (3) se convierten en:

$$\begin{aligned}&\mathrm{Im}(\tau) > 0. \\ &-1/2 \leq \mathrm{Re}(\tau) < 1/2. \\ &\text{Si } |\tau| = 1, \text{ entonces } -1/2 \leq \mathrm{Re}(\tau) \leq 0.\end{aligned} \tag{3.3}$$

Definición 3.8. Un elemento $\tau \in K$ con $|\tau| \geq 1$ se dice reducido si satisface las propiedades (3.3). Un ideal fraccionario propio $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\tau$ se dice reducido si τ lo es.

Proposición 3.9. *Cada clase en $C(\mathcal{O})$, contiene un único ideal reducido.*

Demostración: Acabamos de ver que todo ideal fraccionario propio es equivalente a un ideal fraccionario de la forma $\mathbb{Z}+\mathbb{Z}\tau$ con τ elemento reducido. Si dos ideales reducidos $\mathbb{Z}+\mathbb{Z}\tau, \mathbb{Z}+\mathbb{Z}\tau'$ son equivalentes, por Proposición 3.6, existe η tal que $(\eta 1, \eta\tau) = (1, \tau')$, luego $\eta = 1$ y $\tau = \tau'$, esto demuestra la unicidad. □

Sea $f_\tau(x) = ax^2 + bx + c \in \mathbb{Z}$ como en Lema 2.11. Ya que $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\tau$ es ideal fraccionario propio del Orden $\mathcal{O}$, por Lema 2.11 $b^2 - 4ac = D$ es el discriminante de $\mathcal{O}$. Más aún, ya que $\tau = \frac{-b}{2a} + \frac{\sqrt{D}}{2a}$ y $|\tau|^2 = \tau\overline{\tau} = c/a$, las propiedades (3.3) y $|\tau| \geq 1$, en términos de a, b y c corresponden a:

$$a > 0, \quad a \leq c$$
$$-a \leq -b < a$$
$$\text{Si } a = c, \text{ entonces } b \geq 0.$$

Por lo tanto el polinomio $f_\tau(x, y) = ax^2 + bxy + cy^2$ es una forma reducida de discrimante igual al discriminante del orden.

Ejemplo 3.10. Usando la Proposición 3.9 y la observación anterior, se puede construir los grupos $C(\mathcal{O})$ a partir de su discriminante de manera análoga a como se hizo en charla 1-2.

1. En $K = \mathbb{Q}(\sqrt{-3})$. El conjunto $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(1 + \sqrt{-3})$ es el orden de conductor 2 y discriminante -12. Usando Proposición 2.1 de la charla anterior, se tiene que $a \leq \sqrt{\frac{12}{3}} = 2$, luego $a \in \{1, 2\}$.
   Si $a = 1$, ya que b es par y $|b| \leq a$, entonces $b = 0$ y $c = 3$. Asi $\tau = \frac{\sqrt{-12}}{2} = \sqrt{-3}$
   Si $a = 2$, entonces $b \in \{0, \pm 2\}$. El caso $b = -2$ es descartado ya que $|b| = a$ implica $b = a > 0$. Si $b = 0$, entonces $-8c = -12$, lo cual es imposible en $\mathbb{Z}$. Si $b = 2$, entonces $4^2 - 8c = -12$, asi $c = 2$ lo cual es imposible ya que $(a, b, c,) = 1$. Por lo tanto tenemos que
   $$C(\mathbb{Z} + \mathbb{Z}(1 + \sqrt{-3})) = \{[\mathbb{Z} + \mathbb{Z}\sqrt{-3}]\}.$$
2. En $K = \mathbb{Q}(\sqrt{-1})$, $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\sqrt{-1}$ es el orden de discriminate -4. Por Ejemplo 1, sección 2.2, charla 1-2, se tiene una única tripleta: $a = c = 1, b = 0$ y $\tau = \frac{\sqrt{-4}}{2} = i$. Así
   $$C(\mathbb{Z} + \mathbb{Z}\sqrt{-1}) = \{[\mathbb{Z} + \mathbb{Z}i]\}.$$
3. En $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\sqrt{-5}$ es el orden de discriminante -20. Mirando el Ejemplo 2, sección 2.2, charla 1-2, una tripleta esta dada por $a = 1, c = 5, b = 0$ y $\tau = \frac{\sqrt{-20}}{2} = \sqrt{-5}$. Mientras que la otra corresponde a: $a = 2, b = 0, c = 3$ y $\tau = \frac{\sqrt{-20}}{4} = \sqrt{-5}/4$. Luego
   $$C\left(\mathbb{Z} + \mathbb{Z}\sqrt{-5}\right) = \{[\mathbb{Z} + \mathbb{Z}(\sqrt{-5})], [\mathbb{Z} + \mathbb{Z}\left(\tfrac{\sqrt{-5}}{2}\right)]\}.$$

Referencias

[BS66] Zenon I. Borevich and Igor R. Shafarevich. *Number Theory.* Pure & Applied Mathematics. Academic Press, New York, NY, 1966. 1, 3

[Cox89] D.A. Cox. *Primes of the Form X2 + Ny2: Fermat, Class Field Theory, and Complex Multiplication.* Monographs and textbooks in pure and applied mathematics. Wiley, 1989. 1

Anibal Aravena. Pontificia Universidad Católica de Chile, Facultad de Matemáticas, Vicuña Mackenna 4860, Santiago, Chile.

Email address: akaravena@uc.cl