ÓRDENES EN CUERPOS CUADRÁTICOS Y EL GRUPO DE CLASES

ANIBAL ARAVENA

Definition. (Ordenes) Sea $K/\mathbb{Q}$ una extensión cuadrática. Un orden $\mathcal{O}$ es un subjconjunto 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 $K/\mathbb{Q}$

Proposition 0.1. 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.

Proof. Viene del siguiente teorema. ■

Theorem 0.1. Escribimos $K = \mathbb{Q}(\sqrt{d})$ donde d un entero libre de cuadrados. Luego $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega_K$, donde

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

Proof of Theorem. Los elementos α de $\mathbb{Q}(\sqrt{d})$ tienen la forma

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

Donde a y b son 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 de ssi $2a$ y $a^2 - db^2$ son enteros. Escribimos $2a = m$ con m entero. Ya que si

$$a^2 - db^2 = (m^2/4) - db^2 \in \mathbb{Z} \text{ entonces } d4b^2 = d4(p/q)^2 \in \mathbb{Z}$$

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

$$m^2 - dn^2 \equiv 0 \mod 4$$

Tiene solución. Analicemos los residuos de d en módulo 4. Si $d \equiv 1 \mod 4$, entonces la congruencia toma la forma $m^2 \equiv n^2 \mod 4$ y tiene solución ssi 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. Supongamos que $d \equiv 2 \mod 4$ y $d \equiv 3 \mod 4$. Si la congruencia tiene solución para n impar, luego $d \equiv m^2 \mod 4$, lo cual es imposible. Si n es par, luego la congruencia toma la forma $m^2 \equiv 0 \mod 4$ ssi m es par. Así

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

■

Proposition 0.2. Todo orden $\mathcal{O}$ es subconjunto de $\mathcal{O}_K$

Proof. Sea $\mathcal{O}$ un orden y $\alpha \in \mathcal{O}$. Escribimos $\mathcal{O} = \mathbb{Z}\theta_1 + \mathbb{Z}\theta_2$ con θ_i l.i. Definimos

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

Definimos la matriz $A = [a_{ij}] - \alpha I$. Luego la relación anterior es equivalente 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 integrad para α. Luego $\alpha \in \mathcal{O}_k$. ■

Proposition 0.3. Sea $\mathcal{O}$ orden, luego existe entero positivo $f_{\mathcal{O}}$ tal que

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

Proof. Ya que $\mathcal{O} \subset \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}w_k$. Luego 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

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

Usando que $\mathbb{Z} \subset \mathcal{O}$ fácilmente vemos que $n + m\omega_k \in \mathcal{O}$ ssi $f_{\mathcal{O}}$ divide m, esto demuestra la proposión. ■

Notación: El entero positivo $f_{\mathcal{O}}$ se denomina el conductor del orden $\mathcal{O}$.

Definition. (Discriminante de un Orden) Sea $\mathcal{O} = \mathbb{Z} + \mathbb{Z}f_{\mathcal{O}}\omega_K$ un orden. El valor

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

Se denomina el discriminante del orden $\mathcal{O}$

Observaciones

- El discriminante es un entero.

1. Ideales propios y el grupo de clases

1.1. Resultados pendientes.

Sea $\mathcal{O}$ un orden.

Proposition 1.1. Todo $\mathcal{O}$ es noetheriano.

Proposition 1.2. Todo $\mathcal{O}$-modulo $I \subset K$ finitamente generado, se puede escribir como:

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

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

Definition. (Ideal fraccional) Un ideal fraccional $\mathfrak{a}$ de $\mathcal{O}$ es un subconjunto de K tal que es finitamente generado como $\mathcal{O}$-módulo. Si $\mathfrak{a} \subset \mathcal{O}$ diremos que el ideal es entero o simplemente ideal.

Observaciones:

- Proposisión 1.1 nos justifica la ultima frase.
- Proposición 1.2 nos dice que

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

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

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

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

Definition (Ideal propio)**.** Sea $\mathfrak{a}$ un ideal fraccional de $\mathcal{O}$, diremos que $\mathfrak{a}$ es propio si

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

Observaciones:

- $\mathcal{O} \subset \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$ para todo $\mathfrak{a}$ ideal fraccional de $\mathcal{O}$.
- Todo ideal fraccional principal i.e. $\mathfrak{a} = \alpha\mathcal{O}$ con $\alpha \in K$, es propio.
- Si $\mathfrak{a}$ es propio, luego para $\alpha \in K$, $\alpha\mathfrak{a}$ es también propio.
- $\{b \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$ es un orden. En particular, todo ideal fraccional de $\mathcal{O}_k$ es propio.

Proposition 1.3. Sea $\mathcal{O}$ un orden de un campo cuadrático K. Luego un ideal fraccional $\mathfrak{a}$ de $\mathcal{O}$ es propio ssi $\mathfrak{a}$ es invertible

Proof. ($\Leftarrow$) Supongamos que $\mathfrak{a}$ es invertible. Luego existe ideal fraccional $\mathfrak{b}$ 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.

Lemma 1.1. Sea $K = \mathbb{Q}(\tau)$ un campo cuadrático y $f_\tau(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ con $f(\tau) = 0$ y $(a, b, c) = 1$. Luego $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\tau$ es ideal fraccional propio del orden $\mathcal{O} = \mathbb{Z} + \mathbb{Z}a\tau$ de K.

Proof of Lemma. Demostremos primero que $\mathcal{O}$ es efectivamente un orden.
Ya que $af(\tau) = 0$ ssi $(a\tau)^2 = -b(a\tau) - ac$. Luego

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

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 numeros racionales, la condición $\beta\mathfrak{a} \subset \mathfrak{a}$ es equivalente a

$$\beta \cdot 1 = x + y\tau \in \mathfrak{a}$$

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

Si y solamente si los numeros 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 fraccional 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 $\mathcal{O}$, ya que $\mathcal{O}$ es noetheriano, $a\mathfrak{a}$ es finitamente generado, por lo tanto, así lo es $\mathfrak{a}$. ■

(continuación de la dem prop)($\Rightarrow$). Supongamos que $\mathfrak{a}$ es ideal fraccional propio de $\mathcal{O}$. Por Proposición 1.2, 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.
Supongamos primero que $\alpha = 1$ i.e. $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\tau$. Por lema anterior $\mathcal{O} = \mathbb{Z} + \mathbb{Z}a\tau$, mas aún, el

ideal fraccional $\mathfrak{a}' = \mathbb{Z} + \mathbb{Z}\overline{\tau}$ es ideal fraccional 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 $\mathfrak{a}$ tiene 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 $\mathfrak{a}' a/(\alpha\overline{\alpha})$. ■

Theorem 1.2 (Grupo de ideales fraccionales)**.** Dado orden $\mathcal{O}$, sea $I(\mathcal{O})$ el conjunto de todos los ideales fraccionales 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 fraccionales principales forma un subgrupo de $I(\mathcal{O})$.

Proof. Veamos que la operación esta bien definida i.e. si $\mathfrak{a}, \mathfrak{b} \in I(\mathcal{O})$, entonces $\mathfrak{a}\mathfrak{b} \in I(\mathcal{O})$. Por Proposisión 1.3, 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

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

Luego $\mathfrak{a}\mathfrak{b}$ es invertible y por proposisión 1.3 es propio.
$P(\mathcal{O}) \subset I(\mathcal{O})$ por observación hecha anteriormente y claramente es grupo. ■

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

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

Anibal Aravena. Pontificia Universidad Católica de Chile, Facultad de Matemáticas, Vicuña Mackenna 4860, Santiago, Chile.
Email address: akaravena@uc.cl