IDEALES COPRIMOS AL CONDUCTOR

Sea $\mathcal{O} = [1, fw_K] = \mathbb{Z} + f\mathcal{O}_K$ un orden de conductor f en un cuerpo cuadrático imaginario K. El objetivo principal de esta charla es describir el grupo de clases de ideales $C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$ en términos del orden maximal $\mathcal{O}_K$. Más precisamente, hallaremos un isomorfismo de $C(\mathcal{O})$ con un grupo de clases de ciertos ideales de $\mathcal{O}_K$ que definiremos más adelante (ver Proposición 0.3). Para esto, necesitaremos encontrar una relación entre $\mathcal{O}$-ideales propios y $\mathcal{O}_K$-ideales. Esto lo haremos estudiando *$\mathcal{O}$-ideales coprimos al conductor f*. Al final, veremos una fórmula para el número de clases $h(\mathcal{O})$ en términos de su conductor f y el número de clases $h(\mathcal{O}_K)$ (ver Teorema 0.1)(su demostración quedará pendiente para la Versión Final). Comenzamos con la siguiente definición

Definición 0.1. Diremos que un $\mathcal{O}$-ideal $\mathfrak{a} \neq 0$ es *coprimo a f* si $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

Los $\mathcal{O}$-ideales coprimos al conductor satisfacen las siguientes propiedades básicas

Lema 0.1. *Sea $\mathcal{O}$ un orden de conductor f.*

(1) *Un $\mathcal{O}$-ideal $\mathfrak{a}$ es coprimo a f si y sólo si* $\mathrm{mcd}(N(\mathfrak{a}), f) = 1$.
(2) *Todo $\mathcal{O}$-ideal coprimo a f es propio.*

Proof. (1): Sea $m_f : \mathcal{O}/\mathfrak{a} \to \mathcal{O}/\mathfrak{a}$ la aplicación multiplicación por f. Notar que m_f es un homomorfismo de grupos abelianos finitos de orden $N(\mathfrak{a})$. Se verifica que

$$\mathfrak{a} + f\mathcal{O} = \mathcal{O} \Leftrightarrow m_f \text{ es sobreyectiva } \Leftrightarrow m_f \text{ es isomorfismo de grupos.}$$

Por el teorema de estructura para grupos abelianos finitos, se tiene que m_f es un isomorfismo de grupos si y sólo si $\mathrm{mcd}(N(\mathfrak{a}), f) = 1$. Esto muestra (1).

(2): Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f. Mostraremos que $\mathfrak{a}$ es un $\mathcal{O}$-ideal propio, e.d.,

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

Como $\mathfrak{a}$ es un $\mathcal{O}$-ideal, la inclusión $\supset$ es directa. Para probar la otra inclusión, sea $\beta \in K$ tal que $\beta\mathfrak{a} \subset \mathfrak{a}$. Se verifica que $\beta \in \mathcal{O}_K$, así obtenemos

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subset \mathfrak{a} + f\mathcal{O}_K.$$

Además, $f\mathcal{O}_K \subset \mathbb{Z} + f\mathcal{O}_K = \mathcal{O}$, lo que junto con la inclusión anterior prueba $\beta\mathcal{O} \subset \mathcal{O}$. Por tanto $\beta = \beta \cdot 1 \in \beta\mathcal{O} \subset \mathcal{O}$. Esto muestra que $\mathfrak{a}$ es propio. □

Se sigue que los $\mathcal{O}$-ideales coprimos a f están en $I(\mathcal{O})$ y son cerrados bajo multiplicación (pues $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ también será coprimo a f). Por tanto, ellos generan un subgrupo de $I(\mathcal{O})$ que denotamos $I(\mathcal{O}, f) \subset I(\mathcal{O})$. Dentro de $I(\mathcal{O}, f)$ tenemos el subgrupo $P(\mathcal{O}, f)$ generado por los ideales pricipales $\alpha\mathcal{O}$ donde $\alpha \in \mathcal{O}$ satisface $\mathrm{mcd}(N(\mathfrak{a}), f) = 1$. Así, podemos describir $C(\mathcal{O})$ en términos de $I(\mathcal{O}, f)$ y $P(\mathcal{O}, f)$ como sigue:

Proposición 0.1. *Se tiene un isomorfismo de grupos de clases de ideales*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I(\mathcal{O})/P(\mathcal{O}) =: C(\mathcal{O})$$

Proof. Por Corolario 0.1 de Charla 4, cada clase de ideales en $C(\mathcal{O})$ contiene un $\mathcal{O}$-ideal coprimo a f. Así, la aplicación natural $I(\mathcal{O}, f) \to C(\mathcal{O})$ es sobreyectiva, y es claro que su núcleo es $I(\mathcal{O}, f) \cap P(\mathcal{O})$. Entonces basta probar

$$P(\mathcal{O}, f) = I(\mathcal{O}, f) \cap P(\mathcal{O}).$$

La inclusión $P(\mathcal{O}, f) \subset I(\mathcal{O}, f) \cap P(\mathcal{O})$ es obvia. Para probar la otra inclusión, notar que un elemento arbitrario de $I(\mathcal{O}, f) \cap P(\mathcal{O})$ es de la forma $\alpha\mathcal{O} = \mathfrak{ab}^{-1}$, donde $\alpha \in K$ y $\mathfrak{a}, \mathfrak{b}$ son $\mathcal{O}$-ideales coprimos a f. Escribiendo $m = N(\mathfrak{b})$, se verifica que $m\alpha \in \mathcal{O}$. Esto prueba que $m\alpha\mathcal{O} \in P(\mathcal{O}, f)$, pues $N(m\alpha\mathcal{O}) = N(\mathfrak{a})N(\mathfrak{b})$ es coprimo a f. También $m\mathcal{O} \in P(\mathcal{O}, f)$, porque tiene norma $N(\mathfrak{b})^2$ (coprimo a f). Por tanto $\alpha\mathcal{O} = m\alpha\mathcal{O} \cdot (m\mathcal{O})^{-1} \in P(\mathcal{O}, f)$. □

Para cada orden $\mathcal{O}$ de conductor f, los $\mathcal{O}$-ideales coprimos f se relacionan bien con ciertos ideales del orden maximal $\mathcal{O}_K$ que ahora definimos

Definición 0.2. Dado un entero positivo m, un $\mathcal{O}_K$-ideal $\mathfrak{a}$ es *coprimo a* m si $\mathfrak{a}+m\mathcal{O}_K = \mathcal{O}_K$.

Igual como en el Lema 0.1, se prueba que esto es equivalente a $\mathrm{mcd}(N(\mathfrak{a}), m) = 1$. Por tanto, los $\mathcal{O}_K$-ideales coprimos a m generan un subgrupo de $I_K :=$ grupo de $\mathcal{O}_K$-ideales fraccionarios, que denotamos $I_K(m) \subset I_K$. Ahora veremos la relación que dijimos antes

Proposición 0.2. *Sea $\mathcal{O}$ un orden de conductor f en un cuerpo cuadrático imaginario K.*

(1) *Si $\mathfrak{a}$ es un $\mathcal{O}_K$-ideal coprimo a f, entonces $\mathfrak{a}\cap\mathcal{O}$ es un $\mathcal{O}$-ideal coprimo a f de la misma norma.*
(2) *Si $\mathfrak{a}$ es un $\mathcal{O}$-ideal coprimo a f, entonces $\mathfrak{a}\mathcal{O}_K$ es un $\mathcal{O}_K$-ideal coprimo a f de la misma norma.*
(3) *La aplicación $\mathfrak{a} \mapsto \mathfrak{a}\cap\mathcal{O}$ induce un isomorfimo de grupos $I_K(f) \xrightarrow{\sim} I(\mathcal{O}, f)$, y la inversa de esta aplicación es dada por $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.*

Proof. (1): Sea $\mathfrak{a}$ un $\mathcal{O}_K$-ideal coprimo a f. La aplicación natural

$$\mathcal{O}/\mathfrak{a}\cap\mathcal{O} \to \mathcal{O}_K/\mathfrak{a}$$

es inyectiva, así que $N(\mathfrak{a}\cap\mathcal{O})$ divide a $N(\mathfrak{a})$. Luego, como $N(\mathfrak{a})$ es coprimo a f, entonces $N(\mathfrak{a}\cap\mathcal{O})$ también lo es, lo que prueba que $\mathfrak{a}\cap\mathcal{O}$ es coprimo a f. Para demostrar la igualdad de normas, basta ver que la aplicación anterior es sobreyectiva. Como $N(\mathfrak{a})$ es coprimo a f, multiplicación por f induce un isomorfismo (de grupos) de $\mathcal{O}_K/\mathfrak{a}$. Pero además $f\mathcal{O}_K \subset \mathcal{O}$, entonces se obtiene la sobreyectividad. Esto muestra (1).

Antes de mostrar (2) y (3), probaremos las dos igualdades de ideales siguientes:

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K\cap\mathcal{O} &= \mathfrak{a} \quad \text{si } \mathfrak{a} \text{ es un } \mathcal{O}\text{-ideal coprimo a } f \\ (\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K &= \mathfrak{a} \quad \text{si } \mathfrak{a} \text{ es un } \mathcal{O}_K\text{-ideal coprimo a } f. \end{aligned} \tag{0.1}$$

Para probar la primera, sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f, luego

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K\cap\mathcal{O} &= (\mathfrak{a}\mathcal{O}_K\cap\mathcal{O})\mathcal{O} \\ &= (\mathfrak{a}\mathcal{O}_K\cap\mathcal{O})(\mathfrak{a}+f\mathcal{O}) \\ &\subset \mathfrak{a} + f(\mathfrak{a}\mathcal{O}_K\cap\mathcal{O}) \subset \mathfrak{a}+\mathfrak{a}\cdot f\mathcal{O}_K. \end{aligned}$$

Como $f\mathcal{O}_K \subset \mathcal{O}$, esto prueba $\mathfrak{a}\mathcal{O}_K\cap\mathcal{O} \subset \mathfrak{a}$. La otra inclusión es directa, por tanto se verifica la primera igualdad. Para probar la segunda igualdad, sea $\mathfrak{a}$ un $\mathcal{O}_K$-ideal coprimo a f. Luego

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a}\cap\mathcal{O} + f\mathcal{O}) \subset (\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K + f\mathfrak{a}.$$

Además, $f\mathfrak{a} \subset f\mathcal{O}_K \subset \mathcal{O}$, de modo que $f\mathfrak{a} \subset \mathfrak{a}\cap\mathcal{O} \subset (\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K$, lo que junto con la inclusión anterior, prueba que $\mathfrak{a} \subset (\mathfrak{a}\cap\mathcal{O})\mathcal{O}_K$. La otra inclusión es directa, por tanto se cumple la segunda igualdad.

(2): Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal coprimo a f. La igualdad

$$\mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K = (\mathfrak{a}+f\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K$$

muestra que $\mathfrak{a}\mathcal{O}_K$ también es coprimo a f. Ahora, usando (1) y la primera igualdad de (0.1), se obtiene directamente

$$N(\mathfrak{a}\mathcal{O}_K) = N(\mathfrak{a}\mathcal{O}_K\cap\mathcal{O}) = N(\mathfrak{a}),$$

lo que completa la demostración de (2).

(3): Usando las igualdades de (0.1), se obtiene directamente una biyección entre los monoides de $\mathcal{O}$- y $\mathcal{O}_K$-ideales coprimos a f, vía $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$. Además, la igualdad

$$(\mathfrak{a}\mathfrak{b})\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K\cdot\mathfrak{b}\mathcal{O}_K$$

muestra que esta aplicación es multiplicativa. Por tanto, esta biyección de monoides se extiende a un isomorfismo de grupos $I(\mathcal{O}, f) \simeq I_K(f)$, cuya inversa es $\mathfrak{a} \mapsto \mathfrak{a}\cap\mathcal{O}$. Esto muestra (3). □

Observación 0.1. Usando la factorización única de ideales en $\mathcal{O}_K$ y la Proposición 0.2, se puede probar que cada $\mathcal{O}$-ideal coprimo a f se puede factorizar de manera única como producto de $\mathcal{O}$-ideales primos que también son coprimos a f (ver Ejercicio 7.26).

Ahora podemos describir $C(\mathcal{O})$ en términos del orden maximal:

Proposición 0.3. *Sea $\mathcal{O}$ un orden de conductor f en un cuerpo cuadrático imaginario K. Entonces hay isomorfismos naturales*

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f),$$

donde $P_{K,\mathbb{Z}}(f)$ es el subgrupo de $I_K(f)$ generado por los ideales principales de la forma $\alpha\mathcal{O}_K$, donde $\alpha \in \mathcal{O}_K$ satisface $\alpha \equiv a \mod f\mathcal{O}_K$ para algún entero a coprimo a f.

Observación 0.2. Para no confundirse, recordamos que el subíndice K lo ocupamos para el orden maximal $\mathcal{O}_K$ (como en $I_K, I_K(f)$, etc.), mientras que no ponemos subíndices para el orden $\mathcal{O}$ (como en $I(\mathcal{O}), I(\mathcal{O}, f)$, etc.).

Proof. El primer isomorfismo $C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f)$ fue probado en la Proposición 0.1. Para probar el segundo isomorfismo, consideremos el isomorfismo $I(\mathcal{O}, f) \xrightarrow{\sim} I_K(f)$, $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ obtenido en la Proposición 0.2. Bajo este isomorfismo, el subgrupo $P(\mathcal{O}, f)$ de $I(\mathcal{O}, f)$ es mapeado a un subgrupo $\tilde{P}$ de $I_K(f)$, de modo que

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/\tilde{P}.$$

Por tanto, basta probar que $\tilde{P} = P_{K,\mathbb{Z}}(f)$. Para esto, usaremos el hecho que para cada $\alpha \in \mathcal{O}_K$ se cumple (demostración sencilla en Versión Final)

$$\begin{aligned} \alpha \equiv a \mod f\mathcal{O}_K,\ a \in \mathbb{Z},\ \mathrm{mcd}(a, f) = 1 \\ \iff \alpha \in \mathcal{O},\ \mathrm{mcd}(N(\alpha), f) = 1. \end{aligned} \tag{0.2}$$

Por definición, $P(\mathcal{O}, f)$ es generado por los ideales $\alpha\mathcal{O}$, donde $\alpha \in \mathcal{O}$ y $\mathrm{mcd}(N(\alpha), f) = 1$. Entonces $\tilde{P}$ es generado por los ideales $\alpha\mathcal{O}_K$ correspondientes, y por la equivalencia (0.2), esto implica que $\tilde{P} = P_{K,\mathbb{Z}}(\mathcal{O}, f)$. □

EL NÚMERO DE CLASES

Ahora aplicaremos la Proposición 0.3 para obtener una fórmula para el número de clases $h(\mathcal{O})$ en términos de su conductor y el número de clases $h(\mathcal{O}_K)$ del orden maximal. Antes de enunciar la fórmula, necesitamos recordar algunas notaciones:

d_K = discriminante de $\mathcal{O}_K$. Dado un primo impar p, tenemos el *símbolo de Legendre*

$$\left(\frac{d_K}{p}\right) = \begin{cases} 0 & \text{si } p|d_K \\ 1 & \text{si } p \nmid d_K \text{ y } d_K \text{ es residuo cuadrático módulo } p \\ -1 & \text{si } p \nmid d_K \text{ y } d_K \text{ no es residuo cuadrático módulo } p \end{cases}$$

Recordamos que se llama *residuo cuadrático* módulo m a cualquier entero r coprimo con m para el que tenga solución la congruencia

$$x^2 \equiv r \mod m$$

e.d., cuando r tiene una raíz cuadrada módulo m. Para $p = 2$ tenemos el *símbolo de Kronecker*

$$\left(\frac{d_K}{2}\right) = \begin{cases} 0 & \text{si } 2|d_K \\ 1 & \text{si } d_K \equiv 1 \mod 8 \\ -1 & \text{si } d_K \equiv \mod 8 \end{cases}$$

Recordar que $d_K \equiv 1 \mod 4$ si d_K es impar. Ahora enunciamos la fórmula para $h(\mathcal{O})$:

Teorema 0.1. *Sea $\mathcal{O}$ un orden de conductor f en un cuerpo cuadrático imaginario K. Entonces*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

Más aún, $h(\mathcal{O})$ es siempre un múltiplo entero de $h(\mathcal{O}_K)$.

Proof. (Idea de demostración). Por Corolario 0.1 de Charla 4, cada clase en $C(\mathcal{O}_K)$ contiene un $\mathcal{O}_K$-ideal cuya norma es coprimo a f. Esto implica que la aplicación natural

$$C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f) \to I_K/P_K =: C(\mathcal{O}_K)$$

es sobreyectiva, lo que prueba que $h(\mathcal{O}_K)$ divide a $h(\mathcal{O})$. Más aún, construyendo un par de sucesiones exactas se obtiene (esto queda pendiente para la Versión Final)

$$h(\mathcal{O}) = h(\mathcal{O}_K)\frac{|(\mathcal{O}_K/f\mathcal{O}_K)^*|}{|(\mathbb{Z}/f\mathbb{Z})^*|[\mathcal{O}_K^* : \mathcal{O}^*]}. \tag{0.3}$$

Además, se sabe que

$$|(\mathbb{Z}/f\mathbb{Z})^*| = \varphi(f) = f\prod_{p|f}\left(1-\frac{1}{p}\right).$$

En los Ejercicios 7.28 y 7.29 (pendiente) se prueba que si $\mathfrak{a} \neq 0$ es un $\mathcal{O}_K$-ideal, entonces

$$|(\mathcal{O}_K/\mathfrak{a})^*| = N(\mathfrak{a})\prod_{\mathfrak{p}|\mathfrak{a}}\left(1-\frac{1}{N(\mathfrak{p})}\right),$$

en particular, se concluye que

$$|(\mathcal{O}_K/f\mathcal{O}_K)^*| = f^2\prod_{f|p}\left(1-\frac{1}{p}\right)\left(1-\left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

Reemplazando esto en la ecuación (0.3) se obtiene la fórmula. □