EL GRUPO DE CLASES

¿Cómo se estudian los ideales enteros?

1. Discriminante de un ideal

Definición 1. *Si $K \subset \mathbb{C}$ es un cuerpo numérico (c.n.); i.e., $[K:\mathbb{Q}] = n$, $\alpha \in K$ es un **entero algebraico** (e.a.) si su polmin tiene coeficientes enteros.*

Sabemos que el conjunto de los e.a. de K forman un subanillo, $O_K \subset K$.

Definición 2. *$I \subset O_K$ es un ideal, si es un subgrupo aditivo y es lícito para la multiplicación. Lo denotamos por $I < O_K$.*

Lema 1. *Si $\alpha \in K$, existe un $0 \neq a \in \mathbb{Z}$ tal que $a\alpha$ es e.a. Además, $\mathbb{Z} \subsetneq O_K$.*

Demostración: Si $\alpha \in \mathbb{Z}$, satisface $x - a \in \mathbb{Z}[x]$. En otro caso, por ser $[K:\mathbb{Q}] = n$, α satisface una ecuación con coeficientes en $\mathbb{Q}$. Si multiplicamos su polmin por el mcm de sus denominadores, existen enteros $a_i \in \mathbb{Z}$, con $a_m \neq 0$

$$a_m\alpha^m + \cdots + a_1\alpha + a_0 = 0 \Longleftrightarrow (a_m)^m\alpha^m + \cdots + a_1(a_m)^{m-1}\alpha + a_0(a_m)^{m-1} = 0$$

Luego, $(a_m\alpha)^m + \cdots + a_1(a_m)^{m-2}(a_m\alpha) + a_0(a_m)^{m-1} = 0$ y el elemento $a_m\alpha$ de K es un e.a. que no es entero cuando α no es racional. □

Lema 2. *Cada ideal I de O_K contiene una base de K sobre $\mathbb{Q}$.*

Demostración: Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de K sobre $\mathbb{Q}$. Por el lema anterior, existe un entero, $a \neq 0$, tal que $a\alpha_1, \ldots, a\alpha_n \in O_K$ y son $\mathbb{Q}$-l.i. Si tomamos un $\alpha \neq 0$ en I, por ser ideal, $a\alpha\alpha_1, \ldots, a\alpha\alpha_n \in I$ son $\mathbb{Q}$-l.i. y forman base. □

Si $\alpha \in O_K$, la homotecia $\varphi_\alpha : \beta \mapsto \alpha\beta$ tiene un polinomio característico con coeficientes enteros porque es una potencia del polmin de α que es entero. Por tanto, $N_{K/Q}(\alpha)$ y $tr_{K/Q}(\alpha)$ son números enteros. En consecuencia,

Lema 3. *Si $\alpha_1, \ldots, \alpha_m \in O_K$, su discriminante es un entero. Si además es distinto de cero, son $\mathbb{Q}$-l.i. Por tanto, si $m = n$ forman una base de $K/\mathbb{Q}$.*

Demostración: Como la matriz $\left(tr_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)$ está formada por enteros, también, $D(\alpha_1, \ldots, \alpha_m) = \det\left(tr_{E/K}(\alpha_i\alpha_j)\right)$, es un entero.
Finalmente, $x_1\alpha_1 + \cdots + x_m\alpha_m = 0$ implica el s.l.

$$\sum_{j=1}^{m} tr_{K/\mathbb{Q}}(\alpha_i\alpha_j)x_j = tr_{K/\mathbb{Q}}\Big(\alpha_i \sum_{j=1}^{m} x_j\alpha_j\Big) = tr_{K/\mathbb{Q}}(0) = 0, \quad i = 1, \ldots, m$$

que admite sólo la solución trivial cuando $D\big(\alpha_1, \ldots, \alpha_m\big) \neq 0$. □

Teorema 1. *Si I es ideal de O_K y $\{\alpha_1, \ldots, \alpha_n\} \subset I$, forman una base de $K/\mathbb{Q}$ con $d = \left|D\big(\alpha_1, \ldots, \alpha_n\big)\right|$ mínimo. Entonces, $I = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$.*

Demostración: Como I contiene una base de $K/\mathbb{Q}$ y el valor absoluto del discriminante es un entero positivo existe una base en I con d mínimo.

Si $\alpha \in I$, existen $\gamma_i \in \mathbb{Q}$ tales que $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n$. Si algún γ_i no fuera entero, renumerando $\gamma_1 \notin \mathbb{Z}$ y $\gamma_1 = m + \theta$ con $m \in \mathbb{Z}$ y $0 < \theta < 1$.

Si tomamos $\beta_1 = \alpha - m\alpha_1 = \theta\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n \in I$, $\beta_i = \alpha_i$ para $i > 1$. La matriz de cambio P tiene determinante distinto de cero y los $\beta_1, \ldots, \beta_n \in I$.

$$P = \begin{pmatrix} \theta & \gamma_2 & \ldots & \gamma_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \Longrightarrow 0 < |P| = \theta < 1$$

Finalmente, como $D(\beta_1, \ldots, \beta_n) = D(\alpha_1, \ldots, \alpha_n)|P|^2 < D(\alpha_1, \ldots, \alpha_n)$ tenemos una contradicción porque $d = \left|D(\alpha_1, \ldots, \alpha_n)\right|$ era mínimo. □

Definición 3. $\{\alpha_1, \ldots, \alpha_n\} \subset I$ *es una* ***base entera de I*** *si* $I = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$.

Lema 4. *Si* $\{\beta_1, \ldots, \beta_n\}$ *y* $\{\alpha_1, \ldots, \alpha_n\}$ *son bases de* $K/\mathbb{Q}$*, sus discriminantes se diferencian en un racional al cuadrado.*

Demostración: Por ser base, existen $c_{ij} \in \mathbb{Q}$ tales que $\beta_j = \sum_{k=1}^{n} c_{kj}\alpha_k$, entonces $\sigma_i(\beta_j) = \sum_{k=1}^{n} c_{kj}\sigma_i(\alpha_k)$ para $Id = \sigma_1, \ldots, \sigma_n$ las $\mathbb{Q}$-inmersiones de K en su clausura normal. Y matricialmente, se tiene

$$\big(\sigma_i(\beta_j)\big) = \left(\sum_{k=1}^{n} \sigma_i(\alpha_k)c_{kj}\right) = \big(\sigma_i(\alpha_j)\big)\big(c_{ij}\big) \Longrightarrow$$

$$D(\beta_1, \ldots, \beta_n) = \big(\det\big(\sigma_i(\beta_j)\big)\big)^2 = \det\Big(\big(\sigma_i(\beta_j)\big)^t\big(\sigma_i(\beta_j)\big)\Big) = \big|c_{ij}\big|^2 D(\alpha_1, \ldots, \alpha_n)$$

Corolario 1. *Todas las bases enteras de* $I < O_K$*, tienen el mismo discriminante y su valor absoluto es mínimo entre todas las bases dentro del ideal.*

Demostración: Si $\{\beta_1,\ldots,\beta_n\},\{\alpha_1,\ldots,\alpha_n\}\subset I$, satisfacen

$$I=\beta_1\mathbb{Z}+\cdots+\beta_n=\alpha_1\mathbb{Z}+\cdots+\alpha_n\mathbb{Z}$$

una matriz de cambio, (c_{ij}), entre ambos conjuntos tiene inversa y es una matriz entera. Por tanto, tiene determinante ±1 (es unimodular) y por tanto

$$D(\beta_1,\ldots,\beta_n)=|c_{ij}|^2D(\alpha_1,\ldots,\alpha_n)=D(\alpha_1,\ldots,\alpha_n)$$

sus discriminantes son iguales y por el teorema anterior su valor absoluto es mínimo entre todas las bases contenidas en el ideal. □

Definición 4. *Se llama* ***discriminante del ideal****, al discriminante de cualquier base entera de I. Lo denotamos por d_I.*

Como el propio c.n. K es un ideal,

Corolario 2. *Todas las bases enteras de O_K, tienen el mismo discriminante, d_K, y su valor absoluto es mínimo entre todas las bases dentro de O_K.*

Definición 5. *$\{\alpha_1,\ldots,\alpha_n\}$ es* ***base entera de K*** *si $O_K=\alpha_1\mathbb{Z}+\cdots+\alpha_n\mathbb{Z}$. El discriminante de cualquier base entera de K es el* ***discriminante del cuerpo****.*

Si $\{\alpha_1,\ldots,\alpha_n\}$ es una base entera de K y $\{\beta_1,\ldots,\beta_n\}$ es una base entera del ideal I, existen números enteros $c_{ij}\in Z$ tales que $\beta_i=\sum_{j=1}^n c_{ij}\alpha_j$ [1] y se tiene

$$d_K<d_I=|c_{ij}|^2d_K$$

[1] Pero no al revés, ya que entonces los coeficientes son racionales.

Ejemplo 1. *Para el cuerpo cuadrático* $K=\mathbb{Q}(\sqrt{5})$*, sabemos que* $O_K=\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$*. O sea, una* $\mathbb{Z}$*-base de* O_K *es* $\left\{1,\alpha=\frac{1+\sqrt{5}}{2}\right\}$*. El discriminante del cuerpo es el de esa base entera que también es primitiva y la habíamos calculado antes*

$$d_{\mathbb{Q}(\sqrt{5})}=D_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}\left(1,\frac{1+\sqrt{5}}{2}\right)=5$$

y es menor en valor absoluto que cualquier otro discriminante de ideales.

Si $K=\mathbb{Q}(\sqrt{n})$ es un c.c. arbitrario, con n entero libre de cuadrados, sabemos

$$O_{\mathbb{Q}(\sqrt{n})}=\begin{cases}\mathbb{Z}[\sqrt{n}] & \text{Si } n\equiv 2,3 \pmod 4\\ \mathbb{Z}[\frac{1+\sqrt{n}}{2}] & \text{Si } n\equiv 1 \pmod 4\end{cases}$$

Ejemplo 2. *Si* $n\equiv 2,3 \pmod 4$*, una* $\mathbb{Z}$*-base de* $O_{\mathbb{Q}(\sqrt{n})}$ *es* $\{1,\sqrt{n}\}$*, tenemos*

$$d_{\sqrt{n}}=D_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}\left(1,\sqrt{n}\right)=\begin{vmatrix}1 & \sqrt{n}\\ 1 & -\sqrt{n}\end{vmatrix}^2=\left(-2\sqrt{n}\right)^2=4n$$

que puede ser negativo cuando n lo sea. Por ej., $d_{\mathbb{Q}(i)}=-4$.

Ejemplo 3. *Si* $n\equiv 1 \pmod 4$*, una* $\mathbb{Z}$*-base de* $O_{\mathbb{Q}(\sqrt{n})}$ *es* $\left\{1,\alpha=\frac{1+\sqrt{n}}{2}\right\}$*,*

$$d_{\sqrt{n}}=D_{\mathbb{Q}(\sqrt{n})/\mathbb{Q}}\left(1,\alpha\right)=\begin{vmatrix}1 & \frac{1+\sqrt{n}}{2}\\ 1 & \frac{1-\sqrt{n}}{2}\end{vmatrix}^2=\left(-\sqrt{n}\right)^2=n$$

que puede ser negativo cuando n lo sea. Por ej., $d_{\mathbb{Q}(\sqrt{-3})}=-3$.

2. Norma de un ideal

Definición 6. *Llamamos* ***norma de I*** *al tamaño del cociente* $N(I) = [O_K : I]$.

Recordamos que un grupo abeliano es libre de rango n cuando es isomorfo a $\mathbb{Z}^n$. Por lo anterior, todo ideal de O_K lo es. También, I que es un subgrupo aditivo suyo. Como ambos son de rango n, el cociente O_K/I es un grupo finito. Por el teorema de estructura de grupos abelianos f.g., su tamaño coincide con el valor absoluto del determinante de la matriz de transición. Así,

$$N(I) = [O_K : I] = |\det(c_{ij})| \Longrightarrow d_I = [O_K : I]^2 d_K = N(I)^2 d_K$$

La justificación para la anterior definición es el siguiente

Lema 5. *Si* $I = \langle\alpha\rangle = \alpha O_K$ *es un ideal principal de* O_K, $N(I) = \left|N_{K/\mathbb{Q}}(\alpha)\right|$.

Demostración: Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de K, como $O_K = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$, entonces $I = a\alpha_1\mathbb{Z} + \cdots + a\alpha_n\mathbb{Z}$. O sea, $\{a\alpha_1, \ldots, a\alpha_n\}$ es una $\mathbb{Z}$-base de I. Como existen $c_{ij} \in \mathbb{Z}$ tales que $a\alpha_i = \sum_{j=1}^{n} c_{ij}\alpha_j$, se tiene

$$N(I) = [O_K : \alpha O_K] = |\det(c_{ij})| = |N_{K/\mathbb{Q}}(\alpha)| \qquad \square$$

Ejemplo 4. *Como* $5 \equiv 1 \pmod 4$, *sabemos que* $O_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. *O sea, una* $\mathbb{Z}$*-base de* O_K *es* $\left\{1, \alpha = \frac{1+\sqrt{5}}{2}\right\}$. *Entonces, el ideal principal* $I = \left(\sqrt{5}\right)$ *de* O_K *tiene por norma* $N(I) = N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}\left(\sqrt{5}\right) = \left|\sqrt{5}\left(-\sqrt{5}\right)\right| = 5$.

Otra forma es considerar la $\mathbb{Z}$-base $\{\sqrt{5}, \sqrt{5}\alpha\}$ de I y calcular

$$\left.\begin{array}{l}\sqrt{5} = 2\alpha - 1 \\ \sqrt{5}\alpha = 2\alpha^2 - \alpha = 2(\alpha+1) - \alpha = \alpha + 2\end{array}\right\} \Longrightarrow N(I) = \left|\det\begin{pmatrix}-1 & 2\\ 2 & 1\end{pmatrix}\right| = |-5| = 5$$

También, podemos hallar los factores invariantes de esta matriz entera por t.e. de filas y columnas con coeficientes enteros y comprobamos que los

$$\begin{pmatrix}-1 & 2\\ 2 & 1\end{pmatrix} \sim \begin{pmatrix}-1 & 2\\ 0 & 5\end{pmatrix} \sim \begin{pmatrix}-1 & 0\\ 0 & 5\end{pmatrix} \Longrightarrow N(I) = 5$$

factores invariantes son $1, 5$*, el grupo cociente es* C_5 *y* $\mathbb{Q}(\sqrt{5})/\langle\sqrt{5}\rangle \cong \mathbb{Z}_5$.

Finalmente, como también, $d_{\mathbb{Q}(\sqrt{5})} = 5$*, se tiene* $d_I = N(I)^2 d_K = 5^2 * 5 = 125$.

Ejemplo 5. *Como* $-5 \equiv 3 \pmod 4$*, para el c.c.* $K = \mathbb{Q}(\sqrt{-5})$*, sabemos que* $O_K = \mathbb{Z}[\sqrt{-5}]$*. O sea, una* $\mathbb{Z}$*-base de* O_K *es* $\{1, \sqrt{-5}\}$*. Para hallar la norma del ideal* $I = \left(3, 1+\sqrt{-5}\right) < O_K$ *tenemos que hallar primero una* $\mathbb{Z}$*-base.*

Por definición, para todo $\alpha \in \left(3, 1+\sqrt{-5}\right)$*, existen* $a, b, c, d \in \mathbb{Z}$ *tales que* $\alpha = 3\left(a + b\sqrt{-5}\right) + \left(1+\sqrt{-5}\right)\left(c + d\sqrt{-5}\right) = 3a + b3\sqrt{-5} + c\left(1+\sqrt{-5}\right) + d\left(-5+\sqrt{-5}\right)$.

O sea, todo $\alpha \in I$ *es un c.l. entera de* $3,\ 3\sqrt{-5},\ 1+\sqrt{-5},\ -5+\sqrt{-5}$*. Pero*

$$3\sqrt{-5} = 3\left(1+\sqrt{-5}\right) - 3, \quad -5+\sqrt{-5} = -2*3 + \left(1+\sqrt{-5}\right)$$

Luego, $I = \langle 3, 1+\sqrt{5}\rangle = 3\mathbb{Z} + (1+\sqrt{-5})\,\mathbb{Z}$ *y tenemos una* $\mathbb{Z}$*-base. Por tanto,*

$$N(I) = N\left(\left\langle 3, 1+\sqrt{5}\right\rangle\right) = \left|\det\begin{pmatrix} 3 & 0 \\ 1 & 1 \end{pmatrix}\right| = 3 \Longrightarrow O_K/I \cong \mathbb{Z}_3$$

Como el anillo cociente, $\mathbb{Z}_3$*, es un cuerpo. El ideal* I *es maximal y primo. Además, si el ideal fuera principal, existirían enteros* $a, b \in \mathbb{Z}$ *tal que*

$$I = (a + b\sqrt{-5}) \Longrightarrow N_{K/\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2 = 3 \Longrightarrow b = 0,\ a^2 = 3$$

Como 3 no es cuadrado perfecto, I *no es principal y* $\mathbb{Q}(\sqrt{-5})$ *no es un DIP. También, se puede comprobar que* $\mathbb{Q}(\sqrt{-5})$ *no es un DFU porque*

$$6 = 2 * 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$$

y la ecuación $a^2+5b^2 = 2$ *no tiene soluciones enteras. Como* $U_{\mathbb{Q}(\sqrt{-5})} = \{\pm 1\}$, 2, 3, $1+\sqrt{-5}$ *y* $1-\sqrt{-5}$ *son irreducibles no asociados.*
Ahora, calculamos el discriminante del cuerpo, $d_{\mathbb{Q}(\sqrt{-5})}$

$$d_{\mathbb{Q}(\sqrt{-5})} = D_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}\left(1, \sqrt{-5}\right) = \begin{vmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{vmatrix}^2 = \left(-2\sqrt{-5}\right)^2 = -20$$

También, del ideal I*. Como* $\{3, 1+\sqrt{-5}\}$ *es una base entera de* I

$$d_I = D_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}\left(3, 1+\sqrt{-5}\right) = \begin{vmatrix} 3 & 1+\sqrt{-5} \\ 3 & 1-\sqrt{-5} \end{vmatrix}^2 = \left(-6\sqrt{-5}\right)^2 = -180$$

Finalmente, también se tiene $d_I = N(I)^2 d_K = 3^2 * (-20) = -180$.

Ejemplo 6. *Análogamente, para el ideal* $I = \left(3, 1-\sqrt{5}\right) < O_{\mathbb{Q}(\sqrt{-5})}$ *una base entera es* $\left\{3, 1-\sqrt{-5}\right\}$ *y por tanto también*

$$N(I) = N\left(\left\langle 3, 1-\sqrt{5}\right\rangle\right) = \left|\det\begin{pmatrix} 3 & 0 \\ 1 & -1 \end{pmatrix}\right| = 3 \Longrightarrow O_K/I \cong \mathbb{Z}_3$$

El cociente, $\mathbb{Z}_3$*, es un cuerpo. El ideal I es maximal, primo y no es principal, Ahora, calculamos el discriminante del ideal, usando su base entera.*

$$d_I = D_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}\left(3, 1-\sqrt{-5}\right) = \begin{vmatrix} 3 & 1-\sqrt{-5} \\ 3 & 1+\sqrt{-5} \end{vmatrix}^2 = \left(6\sqrt{-5}\right)^2 = -180$$

Y también se tiene $d_I = N(I)^2 d_K = 3^2 * (-20) = -180$.

Ejemplo 7. *Ahora, para el ideal* $I = \left(2, 1+\sqrt{-5}\right) < O_{\mathbb{Q}(\sqrt{-5})}$*, se puede comprobar que una* $\mathbb{Z}$*-base es* $\left\{2, 1+\sqrt{-5}\right\}$*, pero también lo es* $\left\{2, 1-\sqrt{-5}\right\}$*. O sea,* $I = \left\langle 2, 1+\sqrt{-5}\right\rangle = \left\langle 2, 1-\sqrt{-5}\right\rangle$ *y su norma es*

$$N(I) = N\left(\left\langle 2, 1+\sqrt{-5}\right\rangle\right) = \left|\det\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}\right| = 2 \Longrightarrow O_K/I \cong \mathbb{Z}_2$$

El cociente, $\mathbb{Z}_2$*, es un cuerpo. El ideal I es maximal, primo y no es principal, Ahora, calculamos el discriminante del ideal, usando su base entera.*

$$d_I = D_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}\left(2, 1+\sqrt{-5}\right) = \begin{vmatrix} 2 & 1+\sqrt{-5} \\ 2 & 1-\sqrt{-5} \end{vmatrix}^2 = \left(-4\sqrt{-5}\right)^2 = -80$$

Y también se tiene $d_I = N(I)^2 d_K = 2^2 * (-20) = -80$.

3. El anillo de Dedekind de un cuerpo de numéros

Como consecuencia, de la finitud del anillo cociente O_K/I, considerando la proyección, $\pi : O_K \longrightarrow O_K/I$, por el tercer teorema de isomorfía, una cadena ascendente de ideales de O_k corresponde a una cadena ascendente en O_k/I. Por tanto, toda cadena ascendente $I = I_1 \subset I_2 \subset I_3 \subset \ldots$ estaciona. O sea,

Teorema 2. *O_K es un anillo noetheriano.*

Además, si $P < O_K$ es un ideal primo, el anillo cociente O_K/P es un DI finito. Por tanto, para todo $\overline{\alpha} \in O_K/P$, existen $n, m \in \mathbb{N}$ tales que $\overline{\alpha}^n = \overline{\alpha}^m \Rightarrow \overline{\alpha}^{n-m} = 1$ y por tanto $\overline{\alpha}^{-1} = \overline{\alpha}^{n-m-1}$. O sea, O_K/P es un cuerpo y por tanto

Teorema 3. *Todo ideal primo, P de O_K, es maximal.*

Si $\beta \in K$ es entero sobre O_K, existen $\alpha_1, \ldots, \alpha_m \in O_K$ y $c_{ij} \in \mathbb{Z}$ tales que

$$\beta^m = \alpha_1\beta^{m-1} + \cdots + \alpha_{m-1}\beta + \alpha_m = \sum_{j=1}^{m} \alpha_j \beta^{m-j}$$
$$\alpha_i^{n_i} = c_{i1}\alpha_i^{n_i-1} + \cdots + c_{in_i} = \sum_{j=1}^{n_i} c_{ij}\alpha_i^{n_i-j}$$

Ahora, si consideramos todos los productos $\{\alpha_i^{r_i}\beta^s\}$ con $i = 1, \ldots, m$, $r_i = 1, \ldots, n_i - 1$, $s = 1, \ldots, m-1$, es fácil de comprobar que cualquier producto de β por algunos de ellos, $\alpha_i^{r_i}\beta^{s+1}$, se puede poner como c.l. de los mismos productos con coeficientes enteros. Por tanto, β satisface un polinomio mónico con coeficientes enteros. O sea, β es un e.a. en K y hemos demostrado

Teorema 4. *Si K es un c.n., O_K es íntegramente cerrado en K.*

Por tanto, O_K es noetheriano, i.c. y todo ideal primo es maximal. O sea,

Corolario 3. *Si K es un c.n., O_K es un dominio de Dedekind.*

Es un resultado clásico de álgebra conmutativa que todo ideal de un anillo de Dedekind descompone de forma única como producto de ideales primos.

Para O_K, lo demostraremos explícitamente. Primero, para $A, B < R$ ideales

Definición 7.

La suma	$A+B=\{a+b : a\in A, b\in B\}$
El producto	$AB=\{\sum_{i=1}^{n} a_i b_i : a\in A, b\in B, n\in\mathbb{N}\}$
La intersección	$A\cap B=\{c : c\in A, c\in B\}$

Por la definición de ideal, claramente se tiene que

Lema 6. *Si $A, B < R$, la suma , producto e intersección son de nuevo ideales.*

Como el anillo de enteros de un c.n. es noetheriano todo ideal es f.g. Así,

$$\left.\begin{array}{l} A=(a_1,\ldots,a_r) \\ B=(b_1,\ldots,b_s) \end{array}\right\} \Longrightarrow \left.\begin{array}{l} A+B=(a_1,\ldots,a_r,b_1,\ldots,b_s) \\ AB=(a_1b_1,\ldots,a_ib_j,\ldots,a_rb_s) \end{array}\right\}$$

El producto de ideales es asociativo, conmutativo y el propio anillo actúa como elemento neutro ya que por ser lícito para la multiplicación, $AR = A$. O sea, los ideales forman un monoide abeliano con la multiplicación.

Para $[K:\mathbb{Q}] = n$ un c.n. y un ideal $A < O_K$, como existe una base entera $\{\alpha_1,\ldots,\alpha_n\}$ tal que $A = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$, si $\beta \in K$ satisface $\beta A \subset A$, entonces existen $c_{ij} \in \mathbb{Z}$ tales que $\beta\alpha_i = \sum_{j=1}^{n} c_{ij}\alpha_j$ y se tiene para todo $i = 1,\ldots n$

$$c_{i1}\alpha_1 + \cdots + (c_{ii} - \beta)\alpha_i + \cdots + c_{in}\alpha_n = 0 \Longrightarrow \det\left(\beta\delta_{ij} - c_{ij}\right) = 0$$

O sea, un s.l. homogeneo que admite por soluciones los α_j. Por el teorema de Rouché-Frobenius, el determinante de su matriz es cero. O sea, β satisface, $f(x) = |xId - C| = 0$, un polinomio mónico entero y por tanto es un e.a. de K y por ser O_K i.c. también $\beta \in O_K$. Y hemos demostrado

Lema 7. *Si $0 \neq A < O_K$, para todo $\beta \in K$, $\beta A \subset A$, implica $\beta \in O_K$.*

Lema 8. *Si $0 \neq A$ y B son ideales de O_K. Entonces, $A = AB$ implica $B = O_K$.*

Demostración: Si $\{\alpha_1,\ldots,\alpha_n\}$ es una base entera del ideal $A < O_K$, existen $\beta_{ij} \in B$ tales que $\alpha_i = \sum_{j=1}^{n} \beta_{ij}\alpha_j$. Por tanto, el determinante de la matriz $\left(\delta_{ij} - \beta_{ij}\right)$ es cero. Despejando, se tiene que $1 \in B$ y por tanto $B = O_K$. □

Como consecuencia, si $A < O_K$, no es ni el ideal cero ni el total, y $A^n = A^{n+1}$ entonces como $A \neq O_K$, por el lema anterior $A^n = 0$. Pero entonces, para todo $a \in A$, se tiene $a^n = 0 \Longrightarrow a = 0$. Absurdo, por tanto, hemos demostrado

Corolario 4. *Para todo ideal entero propio, $A < O_K$, la sucesión descendente $A \supset A^2 \supset \cdots \supset A^i \supset \ldots$ no estaciona y por tanto es infinita*[2].

[2] O sea, O_K no es artiniano aunque si es noetheriano.

En particular, si $P < O_K$ es un ideal entero primo propio, sus potencias P^i son todas diferentes. Pero, recordamos la definición de ideal primo,

Definición 8. *P es un ideal primo en un DI, R, si para cualesquiera $a, b \in R$, $ab \in P$ implica que $a \in P$ o bien $b \in P$.*

En un DI, el ideal cero $0 = \{0\}$ es primo. Además, si $P < R$ primo no nulo y $PA = 0$, como existe un $0 \neq p \in P$, $pa = 0 \Longrightarrow a = 0$ para todo $a \in A$. O sea,

Lema 9. *En un DI, si $P < R$ con P primo no nulo y $PA = 0$, entonces $A = 0$.*

Análogamente, si $A, B, P < R$ en un DI con P primo, entonces si $AB \subset P$ y existe un $0 \neq a \in A$, con $a \notin P$, $ab \in P$ implica $b \in P$ para todo $b \in B$. O sea,

Lema 10. *En un DI, si P primo y $AB \subset P$, entonces $A \subset P$ o bien $B \subset P$.*

Ahora, si $A_1 \cdots A_r \subset P$ y $A_1 \not\subset P$, entonces $A_2 \cdots A_r \subset P$ y por inducción

Lema 11. *En un DI, si P primo y $A_1 \cdots A_r \subset P$, entonces $\exists i$ tal que $A_i \subset P$.*

Volviendo al anillo de enteros, O_K de un c.n. Si $P_1 \cdots P_r = Q_1 \ldots Q_s$ para $P_i, Q_j < O_k$ primos, como todo ideal primo es maximal en O_K se tiene

$$Q_1 \ldots Q_s \subset P_1 \Longrightarrow \exists j \text{ tal que } Q_j \subset P_1 \Longrightarrow Q_j = P_1$$

Demostraremos mas adelante que se puede cancelar el ideal repetido y por inducción, tendremos que los productos finitos de ideales primos en O_K son todos distintos. Y por tanto, forman un monoide abeliano libre.

4. El grupo de clases de un cuerpo numérico

A partir de ahora, todos los ideales que consideremos serán no nulos aunque pueden ser el total. Las siguientes definiciones son fundamentales.

Definición 9. *A y B se dicen* ***equivalentes*** *si $(\alpha)A = (\beta)B$ con $0 \neq \alpha, \beta \in O_K$.*

Al definirse con una igualdad, esta relación es reflexiva, transitiva y simétrica.

Definición 10. *Las clases de equivalencia de ideales enteros se llaman* ***clases de ideales****. El número de clases, h_K, se le llama el* ***número de clases de K****.*

Si O_K es un DIP, todo ideal entero es principal, $A = (\alpha)$, $B = (\beta)$ y entonces

$$(\beta)A = (\alpha)B \Longrightarrow h_K = 1$$

Recíprocamente, si $h_K = 1$, para todo ideal, $A \sim O_K$, existen $0 \neq \alpha, \beta \in O_K$

$$(\alpha)A = (\beta)O_K = (\beta) \Longrightarrow \beta/\alpha \in A,\ A = (\beta/\alpha)$$

y todo ideal es principal. Esto es, O_K es un DIP. Y hemos demostrado

Teorema 5. *Para todo c.n. K, O_K es un DIP si y sólo si $h_K = 1$.*

Así, el número de clases de K, mide lo lejos que está O_K de ser un DIP.
El siguiente lema es una generalización débil del algoritmo de Euclides.

Lema 12. ***A. Hurwitz, 1919***. *Para todo c.c. K, existe $0 < M \in \mathbb{Z}$ tal que para todo $\alpha, \beta \in O_K$ con $\beta \neq 0$ existe un natural $t < M$ y un e.a. $w \in O_K$ tal que*

$$\left|N_{K/\mathbb{Q}}(t\alpha - w\beta)\right| < \left|N_{K/\mathbb{Q}}(\beta)\right|$$

Demostración: Dados $\alpha, \beta \in O_K$ con $\beta \neq 0$, definimos $\gamma = \alpha/\beta \in K$. Entonces, es suficiente probar que existe $0 < M \in \mathbb{Z}$ tal que para todo $\gamma \in K$, $\left|N_{K/\mathbb{Q}}(t\gamma - w)\right| < 1$ para un natural $t < M$ y un e.a. $w \in O_K$.

Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de O_K, existen $a_i \in \mathbb{Q}$ tales que $\gamma = \sum_{i=1}^n a_i \alpha_i$. Como existe $a = \max_i |a_i| \in \mathbb{Q}^+$. Entonces,

$$\left|N_{K/\mathbb{Q}}(\gamma)\right| = \left|\prod_{j=1}^n \sigma_j\left(\sum_{i=1}^n a_i \alpha_i\right)\right| = \left|\prod_{j=1}^n \sum_{i=1}^n a_i \sigma_j(\alpha_i)\right| < a^n \prod_{j=1}^n \sum_{i=1}^n \left|\sigma_j(\alpha_i)\right| = a^n C$$

Ahora, elegimos un natural $m > \sqrt[n]{C}$ y tomamos $M = m^n$. Entonces, para $\gamma = \sum_{i=1}^n a_i \alpha_i$, descomponemos $a_i = b_i + \epsilon_i$, con $b_i \in \mathbb{Z}$ y $0 \leq \epsilon_i < 1$. Definimos,

$$\left.\begin{array}{l} q(\gamma) = \sum_{i=1}^n b_i \alpha_i \in O_K \\ r(\gamma) = \sum_{i=1}^n \epsilon_i \alpha_i \in K \end{array}\right\} \Longrightarrow \gamma = q(\gamma) + r(\gamma)$$

También, definimos $\varphi : K \longrightarrow \mathbb{Q}^n$ tal que para todo $\gamma = \sum_{i=1}^n a_i \alpha_i$

$$\varphi(\gamma) = (a_1, \ldots, a_n) \in \mathbb{Q}^n$$

Como sus coordenadas son menores que 1, $\varphi(r(\gamma))$ está en cubo unidad. Ahora, dividimos el cubo unidad en m^n subcubos de lados $1/m$ y consideramos todos los puntos $\varphi\big(r(k\gamma)\big)$ para $1 \le k \le m^n+1$. Por el pincipio del nido de paloma, dos de ellos $h\gamma$ y $l\gamma$ deben estar en el mismo subcubo, con $l < h$.

$$\left.\begin{array}{l} h\gamma = q(h\gamma) + r(h\gamma) \\ l\gamma = q(l\gamma) + r(l\gamma) \end{array}\right\} \Longrightarrow t\gamma = (h-l)\gamma = w + \delta$$

donde $w = q(h\gamma) - q(l\gamma) \in O_K$ y $\delta = r(h\gamma) - r(l\gamma)$ tiene sus coordenadas con valor absoluto menor o igual que $1/m$. Por tanto, $\delta = t\gamma - w$ y se tiene

$$\big|N_{K/\mathbb{Q}}\big(t\gamma - w\big)\big| = \big|N_{K/\mathbb{Q}}\big(\delta\big)\big| < (1/m)^n C < m^n/m^n = 1 \qquad \square$$

Ejemplo 8. *Como* $5 \equiv 1 \pmod 4$, *una* $\mathbb{Z}$*-base de* $O_{\mathbb{Q}(\sqrt{5})}$ *es* $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$.

$$\left.\begin{array}{l} C = \prod_{j=1}^{n} \sum_{i=1}^{n} \big|\sigma_j(\alpha_i)\big| = \left(1 + \frac{1+\sqrt{5}}{2}\right)\left(1 + \frac{-1+\sqrt{5}}{2}\right) \approx 4.23607 \\ \Longrightarrow \sqrt{C} \approx 2.05817 < 3 \Longrightarrow M_{\mathbb{Q}(\sqrt{5})} = 3^2 = 9 \end{array}\right\}$$

Ejemplo 9. *Como* $-5 \equiv 3 \pmod 4$. *Para* $\mathbb{Q}(\sqrt{-5})$, *una base entera es* $\{1, \sqrt{5}\}$,

$$C = \prod_{j=1}^{n} \sum_{i=1}^{n} \big|\sigma_j(\alpha_i)\big| = \left(1 + \sqrt{5}\right)^2 \approx 10.47 \Longrightarrow \sqrt{C} \approx 3.23 < 4 \Longrightarrow M_{\mathbb{Q}(\sqrt{-5})} = 4^2 = 16$$

Ahora podemos demostrar

Teorema 6. *El número de clases,* h_K*, de un c.n. es finito.*

Demostración: Si $A < O_K$, para $0 \neq \alpha \in A$, $\left|N_{K/\mathbb{Q}}(\alpha)\right|$ es un entero positivo y podemos elegir $0 \neq \beta \in A$, tal que $\left|N_{K/\mathbb{Q}}(\beta)\right|$ sea mínimo. Por el lema de Hurwitz, existe un t, $1 \leq t \leq M_K$, tal que $\left|N_{K/\mathbb{Q}}\left(t\alpha - w\beta\right)\right| < \left|N_{K/\mathbb{Q}}\left(\beta\right)\right|$.

Como $w \in O_K$ y A es lícito para la multiplicación, $t\alpha - w\beta \in A$. Por la minimalidad de la norma de β, se tiene

$$t\alpha - w\beta = 0 \Longrightarrow t\alpha \in \left(\beta\right) \Longrightarrow M_K!A \subset \left(\beta\right)$$

Ahora, si definimos $B = (1/\beta)M_K!A \subset A$ sale un ideal entero tal que

$$M_K!A = \left(\beta\right)B \Longrightarrow A \sim B$$

Pero $\beta \in A$ implica que $M_K!\beta \in \left(\beta\right)B \Longrightarrow M_K! \in B$. Finalmente, como $O_K/(M_K!)$ es un anillo finito, tiene un número finito de ideales. Por el tercer teorema de isomorfía, existe un número finito de B, tales que $M_K! \in B$ y h_K es finito. □

La cota que se obtiene de la demostración anterior es poco práctica. Por ej.

Ejemplo 10. *Hemos visto antes que* $\mathbb{Q}(\sqrt{-5})$ *no era un DIP. Luego,* $1 < h_{\mathbb{Q}(\sqrt{-5})}$. *Ahora, como hemos visto en un ejemplo anterior que* $M_{\mathbb{Q}(\sqrt{-5})} = 16$ *y* $16! = 20922789888000$. *Por tanto, el número de clases,* $h_{\mathbb{Q}(\sqrt{-5})}$ *está acotado por el número de ideales del anillo cociente* $O_{\mathbb{Q}(\sqrt{-5})}/(20922789888000)$.

Sin embargo, el interés teórico es grande. Así

Teorema 7. *Para cada ideal* $A < O_K$, *existe un* $k \in \mathbb{N}$, *tal que* A^k *es principal. Por tanto,* $A^k \sim (1) = O_K$ *y la clase de* A *tiene por inversa la clase de* A^{k-1}.

Demostración: Consideramos el conjunto de ideales enteros $\{A^i : 1 \le i \le h_K + 1\}$. al menos, dos de ellos pertenecen a la misma clase, $A^i \sim A^j$ con $i < j$. O sea, existen $\alpha, \beta \in O_K$ tales que $(\alpha)A^i = (\beta)A^j$. Ahora, tomamos $k = j - i$ y $B = A^k$. Veremos que B es principal.

$$(\alpha)A^i = (\beta)BA^i \Longrightarrow (\alpha/\beta)A^i \subset A^i \Longrightarrow \alpha/\beta \in O_K$$

Finalmente, si llamamos $w = \alpha/\beta$, tenemos $(w)A^i = BA^i \Longrightarrow B = (w) \sim O_K$.

Corolario 5. *Para todo c.n., K, el conjunto de las clases de ideales enteros es un grupo abeliano finito.*

Una consecuencia, es que para todo ideal entero, $A < O_K$, $A^{h_K} \sim O_K$.
O sea, $0 \neq \alpha, \beta \in O_K$, $(\alpha)A^{h_K} = (\beta)O_K = (\beta) \Longrightarrow \beta/\alpha \in A^{h_K}$, $A^{h_K} = (\beta/\alpha)$ y para todo ideal una potencia suya es principal.

Ahora, podemos demostrar que el monoide multiplicativo de los ideales enteros de un c.n. es cancelativo. Como existe un $k \in \mathbb{N}$ tal que $A^k = (\alpha)$, multiplicando por A^{k-1} y por ser O_k DI se tiene

$$AB = AC \Longrightarrow (\alpha)B = (\alpha)C \Longrightarrow B = C$$

Corolario 6. *Si $A, B, C < O_k$ son ideales, $AB = AC$ implica que $B = C$.* □

Ahora, demostramos que si un ideal contiene a otro entonces lo divide.

Corolario 7. *Si $A \subset B$ son ideales, existe un $C < O_K$ tal que $A = BC$.*

Demostración: Como antes, existe un $k \in \mathbb{N}$ tal que $B^k = (\beta)$. Por tanto,

$$B^{k-1}A \subset B^k = (\beta) \Longrightarrow C = (1/\beta)B^{k-1}A \subset O_K$$
$$\Longrightarrow BC = (1/\beta)B^k A = (1/\beta)(\beta)A = A \qquad \square$$

Ahora, podemos demostrar que todo ideal entero de un c.n. descompone de forma única como producto de ideales primos. En efecto, si $A < O_K$, como O_K es noetheriano, existe un ideal maximal, P_1, que lo contiene[3]. Por tanto, $A = P_1 A_1$. Análogamente, $A_1 = P_2 A_2$. Tenemos una sucesión ascendente

$$A \subset A_1 \subset A_2 \subset \cdots$$

debe estacionar porque O_K es noetheriano. El último $A_r = P_r$ es maximal y

$$A = P_1 \cdots P_r$$

Teorema 8. *Todo ideal entero $A < O_K$ descompone de forma única como producto de ideales primos salvo el orden de los factores.*

Demostración: Queda la unicidad. Si $P_1 \cdots P_r = Q_1 \ldots Q_s$ para $P_i, Q_j < O_k$ primos, con $s \leq r$. Como todo ideal primo es maximal en O_K se tiene

$$Q_1 \ldots Q_s \subset P_1 \Longrightarrow \exists j \text{ tal que } Q_j \subset P_1 \Longrightarrow Q_j = P_1$$

por 6, podemos cancelar el ideal repetido y por inducción, llegamos a que $P_1 \cdots P_{r-s} = O_K$, lo cual es absurdo salvo que $r = s$, como queremos. $\square$

[3] En realidad, como O_K / A es finito, A está contenido en un número finito de maximales.

Además, la relación de equivalencia $A \sim B \Longleftrightarrow (\alpha)A = (\beta)B$ con $\alpha, \beta \in O_K$ no nulos, es una congruencia para la multiplicación de ideales. En efecto, si $A \sim A_1$, $B \sim B_1$, entonces $(\alpha)A = (\alpha_1)A_1$, $(\beta)B = (\beta_1)B_1$ y se tiene

$$(\alpha\beta)AB = (\alpha_1\beta)A_1B = (\alpha_1\beta_1)A_1B_1 \Longrightarrow AB \sim A_1B_1$$

Por todo lo anterior, hemos demostrado que

Corolario 8. *El conjunto de los ideales enteros de un c.n. K es un monoide abeliano libre generado por los ideales primos. Su cociente por la congruencia $\sim$ es un grupo abeliano finito de tamaño h_K.*

Ejemplo 11. *Hemos visto en ejemplos anteriores que los ideales $P_1 = (3, 1+\sqrt{-5})$ y $P_2 = (3, 1-\sqrt{-5})$ en $O_{\mathbb{Q}(\sqrt{-5})}$ tienen norma 3. Además, sus generadores son sus $\mathbb{Z}$-bases. O sea, $P_1 = 3\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z}$ y $P_1 = 3\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z}$.*

$P_1 \neq P_2$ porque si $1-\sqrt{-5} \in P_1$ existirían, $a, b \in \mathbb{Z}$, tales que $1-\sqrt{-5} = a3 + (1+\sqrt{-5})b$. Pero como 1 y $\sqrt{-5}$ son $\mathbb{Q}$.l.i. se tendría $1 = 3a + b$, $-1 = b \Longrightarrow a = 3/2$, lo que es absurdo. Por tanto, P_1 y P_2 son primos distintos.

Como $3 \in P1$ y $3 \in P_2$ ambos dividen al ideal principal (3); o sea, $3 \in P_1P_2$. Luego $N(P_1P_2) \leq N(3) = 3^2 = 9$. Por el TCR, $N(P_1P_2) = N(P_1)N(P_2) = 9$. Por tanto, la descomposición única en ideales primos[4] es

$$(3) = \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right)$$

[4]Como consecuencia, aunque 3 es irreducible en $O_{\mathbb{Q}(\sqrt{-5})}$ no es primo en el mismo anillo.

Ejemplo 12. *Hemos visto también, en un ejemplo anterior, que* $P = \left(2, 1+\sqrt{-5}\right)$ *en* $O_{\mathbb{Q}(\sqrt{-5})}$ *tiene norma 2, es primo y sus generadores son una base entera. O sea,* $P = 2\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z}$. *Lo mismo le pasa al ideal* $\left(2, 1-\sqrt{-5}\right)$. *Pero en este caso, son el mismo ideal P ya que*

$$1-\sqrt{-5} = a2 + (1+\sqrt{-5})b \Longrightarrow 1 = 2a+b,\ -1 = b \Longrightarrow a = 2/2 = 1$$

$$P^2 = \left(4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\right) = \left(4, 2+2\sqrt{-5}, 2\sqrt{-5}\right) = \left(2, 2\sqrt{-5}\right) = (2).$$

Por tanto, la descomposición única en ideales primos[5] *es*

$$(2) = \left(2, 1+\sqrt{-5}\right)^2$$

Ejemplo 13. *Sustituyendo las dos factorizaciones anteriores, tenemos*

$$(6) = (2)(3) = \left(2, 1+\sqrt{-5}\right)^2 \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right) = P^2 P_1 P_2$$

que es su descomposición únicas en ideales primos. Sin embargo, como

$$6 = 2 * 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) \in O_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}$$

se tienen dos descomposiciones en irreducibles no asociados del mismo elemento. Lo que demuestra que el anillo $O_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}$ *no es un DFU.*

Una consecuencia de la factorización única de los ideales en primos es que

Teorema 9. *Un dominio de Dedekind es un DIP si y sólo si es un DFU.*

[5] Como consecuencia, aunque 2 es irreducible en $O_{\mathbb{Q}(\sqrt{-5})}$ no es primo en el mismo anillo.

Demostración: Si R es un DD y además un DFU, entonces como todo ideal no nulo $I < R$, contiene un $0 \neq \alpha \in I$. Por ser R DFU, α descompone de forma única en irreducibles $\alpha = p_1 \cdots p_r$ pero entonces también se tiene una igualdad entre los ideales principales $(\alpha) = (p_1) \cdots (p_r)$.

Pero, en un DFU si $p \in R$ es irreducible, el ideal principal (p) es primo ya que por la factorización única en elementos irreducibles

$$ab \in (p) \Longleftrightarrow ab = cp \Longrightarrow p|a \text{ o bien } p|b \Longrightarrow (p) \text{ es ideal primo}$$

Como $(\alpha) \subset I$, I divide a (α) y existe un ideal $B < R$ tal que reordenando

$$(p_1) \cdots (p_r) = (\alpha) = IB \Longrightarrow I = (p_1) \cdots (p_s) \text{ con } s < r$$

Como el producto de ideales principales es principal, I es principal y R DIP. La implicación DIP $\Rightarrow$ DFU, es general y en este caso también inmediata. □

Antes, vimos que $(2) = \left(2, 1 + \sqrt{-5}\right)^2$. Este ejemplo se puede generalizar.

Ejemplo 14. *Si $m \equiv 3 \pmod 4$ libre de cuadrados, sabemos que una base entera del cuerpo $\mathbb{Q}(\sqrt{m})$[6] es $1, \sqrt{m}$. Entonces, $P = \left(2, 1 + \sqrt{m}\right)$ en $O_{\mathbb{Q}(\sqrt{m})}$ tiene norma 2, es primo y sus generadores son una base entera.*
En efecto, para todo $\alpha \in P$, existen $a, b, c, d \in \mathbb{Z}$ tales que

$$\alpha = 2\left(a + b\sqrt{m}\right) + \left(1 + \sqrt{m}\right)\left(c + d\sqrt{m}\right) = 2a + 2b\sqrt{m} + c\left(1 + \sqrt{m}\right) + d\left(m + \sqrt{m}\right)$$

[6] Porque $m \not\equiv 1 \pmod 4$.

O sea, todo $\alpha \in P$ *es un c.l. entera de* $2,\ 2\sqrt{m},\ 1+\sqrt{m},\ m+\sqrt{m}$. *Pero como*

$$2\sqrt{m} = 2\left(1+\sqrt{m}\right) - 2 \Longrightarrow \text{ sobra } 2\sqrt{m}$$

Ahora, como $m \equiv 3 \pmod 4 \Longleftrightarrow m = 3+4\lambda$, *se tiene*

$$m+\sqrt{m} = 3+\sqrt{m}+4\lambda = 4-(1-\sqrt{m})+4\lambda$$

y como $1-\sqrt{m} = 2-(1+\sqrt{m})$, *una* $\mathbb{Z}$*-base es* $2,\ 1+\sqrt{m}$ *o bien* $2,\ 1-\sqrt{m}$. *O sea,* $P = \langle 2, 1+\sqrt{m}\rangle = \langle 2, 1-\sqrt{m}\rangle$ *son el mismo ideal. Además,*

$$N(P) = N\left(\langle 2, 1+\sqrt{m}\rangle\right) = \left|\det\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}\right| = 2 \Longrightarrow O_K/I \cong \mathbb{Z}_2$$

Y el cociente ,$\mathbb{Z}_2$, *es un cuerpo. Por tanto,* P *es maximal y primo. Finalmente, como* $m+1 = 4+4\lambda$ *es múltiplo de 4, se tiene*

$$P^2 = \left(4, 2+2\sqrt{m}, m+1+2\sqrt{m}\right) = \left(4, 2+2\sqrt{m}, 2\sqrt{m}\right) = \left(2, 2\sqrt{m}\right) = (2)$$

O sea, si $m \equiv 3 \pmod 4$, el discriminante $d_{\mathbb{Q}(\sqrt{m})} = 4m$ y $(2) = \left(2, 1+\sqrt{m}\right)^2$.

Ejemplo 15. *Si* $p|m$, *con* p *primo impar y* m *libre de cuadrados, entonces* $(p) = \left(p, 1+\sqrt{m}\right)^2 < O_{\mathbb{Q}(\sqrt{m})}$. *En efecto, como* $m = pm'$, *entonces* $mcd(p^2, m) = p$ *y existen enteros* $\lambda, \mu \in \mathbb{Z}$ *tales que*

$$p = \lambda p^2 + \mu m \Longrightarrow p \in \left(p, 1+\sqrt{m}\right)^2 = \left(p^2, p\sqrt{m}, m\right) \Longrightarrow (p) = \left(p, 1+\sqrt{m}\right)^2$$

Como consecuencia de los dos ejemplos, para todo $p \in \mathbb{Z}$ primo entero

Corolario 9. *Si* $p|d_{\mathbb{Q}(\sqrt{m})}$, *entonces* $(p) = \left(p, 1+\sqrt{m}\right)^2$.

5. Ramificación y grado

Dado un ideal primo $P < O_k$, como la sucesión descendente $P^0 = O_K \supset P \supset \cdots \supset P^i \supset \cdots$ es infinita y $A \subset P^0 = O_K$, para todo ideal entero, A, existe r entero no negativo tal que $A \subset P^r$ pero $A \not\subset P^{r+1}$ ya que en caso contrario $A = P^r B_r$ para todo $i \in \mathbb{N}$ y la descomposición en primos no sería única.

Definición 11. *Llamamos orden de A en P, a ese entero* $\boldsymbol{ord_P(A)}$ *no negativo.*

Claramente, para ideales A, B y primos P, Q de O_K, se tiene

$$ord_P(P) = 1,\ ord_P(Q) = 0 \text{ y } ord_P(AB) = ord_P(A) + ord_P(B)$$

Como consecuencia de la descomposición única, se tiene que para todo ideal

$$A = \prod_{P \text{ primo}} P^{ord_P(A)}$$

Recordemos que todo ideal entero $A < O_K$ no nulo, contiene al menos un entero no nulo y por tanto existe el mínimo y $A \cap \mathbb{Z} = (n)$. Además,

Lema 13. *n coincide con la característica del anillo cociente finito* O_K / A.

Demostración: Como la clase de $\overline{n} = \overline{0} \in O_K / A$, basta ver $\overline{m} \neq \overline{0}$ para todo $m < n$, lo que es inmediato porque sino $m \in A$. □

Si P primo, ese mínimo es un primo entero $p \in P \cap \mathbb{Z}$, $\mathbb{Z}_p$ está contenido en el cuerpo finito $F = O_K / P$ que es un $\mathbb{Z}_p$-esp. vect. de dimensión finita $f \in \mathbb{N}$.

Definición 12. *Dado $P < O_K$ primo, $e = ord_P((p))$ es el* ***índice de ramificación de*** *P y $f = \dim_{\mathbb{Z}_p}(O_K/P)$ es el* ***grado de inercia de*** *P.*

Si $A < O_K$ es un ideal, sabemos que descompone de forma única como producto de primos. Aplicando el teorema chino de los restos en O_K, tenemos

$$A = P_1^{e_1} \cdots P_r^{e_r} \Longrightarrow O_K/A \cong \left(O_K/P_1\right)^{e_1} \cdots \left(O_K/P_r\right)^{e_r}$$

Por tanto, $N_{K/\mathbb{Q}}(A) = |O_K/A| = \left|O_K/P_1^{e_1}\right| \times \cdots \times \left|O_K/P_r^{e_r}\right|$.
Calculamos ahora el orden de un cociente $|O_K/P^e|$ para $e \in \mathbb{N}$ y P primo.

Si $e = 1$, como $\mathbb{Z} \cap P = (p)$ con $p \in \mathbb{Z}$ primo y $\mathbb{Z}_p \subset O_K/P$, el cociente es un cuerpo finito de tamaño $|O_K/P| = p^f$, con f el grado de inercia de P.

Para $e > 1$, como la aplicación $\pi : O_K/P^e \longrightarrow O_K/P^{e-1}$, $\pi(\alpha + P^e) = \alpha + P^{e-1}$ está bien definida porque $P^e \subset P^{e-1}$, π es un homomorfismo de anillos que además es sobreyectivo y su núcleo es $N(\pi) = P^{e-1}/P^e$. Por tanto,

$$\left|O_K/P^e\right| = \left|P^{e-1}/P^e\right| \times \left|O_K/P^{e-1}\right|$$

Ahora, calculamos el orden del cociente P^{e-1}/P^e. Como la inclusión, $P^e \subset P^{e-1}$, es propia existe un $\alpha \in P^{e-1}$ tal que $\alpha \notin P^e$. Pero el ideal intermedio

$$P^e \subset (\alpha) + P^e \subseteq P^{e-1}$$

es un divisor de P^e y un múltiplo de P^{e-1}. Por la descomposición única en primos debe ser una potencia de P y $(\alpha) + P^e = P^{e-1}$. Ahora, fácilmente se ve que $O_k/P \cong P^{e-1}/P^e$ y por tanto, $\left|P^{e-1}/P^e\right| = N_{K/\mathbb{Q}}(P) = p^f$.

Teorema 10. *Para todo $P < O_K$ primo, $N_{K/\mathbb{Q}}(P^e) = N_{K/\mathbb{Q}}(P)^e = p^{ef}$.*

Demostración: Por inducción, suponemos $N_{K/\mathbb{Q}}(P^{e-1}) = N_{K/\mathbb{Q}}(P)^{e-1}$, pero

$$N_{K/\mathbb{Q}}(P^e) = \left|O_K/P^e\right| = \left|P^{e-1}/P^e\right| \times \left|O_K/P^{e-1}\right| = N_{K/\mathbb{Q}}(P) N_{K/\mathbb{Q}}(P)^{e-1} = p^f\, p^{(e-1)f}$$

Como consecuencia, para todo ideal $A < O_K$, si $A = P_1^{e_1} \cdots P_r^{e_r}$, se tiene

$$N_{K/\mathbb{Q}}(A) = N_{K/\mathbb{Q}}(P_1)^{e_1} \cdots N_{K/\mathbb{Q}}(P_r)^{e_r} = p_1^{e_1 f_1} \cdots p_r^{e_r f_r}$$

Si $p \in \mathbb{Z}$ es un primo entero, el ideal $A = (p) < O_K$ descompone de forma única como cualquier otro ideal de O_K, $(p) = P_1^{e_1} \cdots P_r^{e_r}$, pero como todos los cuerpos cocientes O_K/P_itiene la misma característica p. Entonces

$$N_{K/\mathbb{Q}}(p) = p^{[K:\mathbb{Q}]} = p^{e_1 f_1} \cdots p^{e_r f_r} = p^{\sum_{i=1}^r e_r f_r} \Longrightarrow [K:\mathbb{Q}] = \sum_{i=1}^r e_r f_r$$

Definición 13. *Si algún $e_i > 1$ decimos que p* ***ramifica en K****. Si todos los $e_i = 1$, decimos que* ***escinde****. Si $(p) < O_K$ es primo decimos que es* ***inerte****.*

Ahora, podemos demostrar que

Teorema 11. *La norma de ideales en O_k es multiplicativa.*

Demostración: Si admitimos exponentes cero, podemos suponer $A = P_1^{e_1} \cdots P_r^{e_r}$ y $B = P_1^{e'_1} \cdots P_r^{e'_r}$. Entonces, $AB = P_1^{e_1+e'_1} \cdots P_r^{e_r+e'_r}$ y por tanto

$$N_{K/\mathbb{Q}}(AB) = N_{K/\mathbb{Q}}(P_1)^{e_1+e'_1} \cdots N_{K/\mathbb{Q}}(P_r)^{e_r+e'_r} = N_{K/\mathbb{Q}}(A) N_{K/\mathbb{Q}}(B)$$

Ya sabíamos que si $A < O_K$ y $N_{K/\mathbb{Q}}(A) = p$ primo entero. Entonces, el anillo cociente $O_K/A \cong \mathbb{Z}_p$ y A es ideal maximal y primo. O sea,

Corolario 10. *Si $A < O_K$ y $N_{K/\mathbb{Q}}(A) = p$. Entonces es A es primo.*

Pero tampoco hace falta calcular su norma. Basta ver que contiene propiamente a otro cuya norma sea el cuadrado de un primo entero. Ya que, si $A \subset B$ y $N_{K/\mathbb{Q}}(A) = p^2$ para $p \in \mathbb{Z}$ primo. Existe un ideal $C < O_K$ tal que

$$A = BC \Longrightarrow N(A) = N(B)N(C) \Longrightarrow N(B) = N(C) = p$$

Corolario 11. *Si $A \subsetneq B \subsetneq O_K$ ideales enteros y $N(A) = p^2$. Entonces, $N(B) = p$ y B es primo.*

Ejemplo 16. *Si $m \equiv 1 \pmod 8$ libre de cuadrados, entonces una base entera del cuerpo $\mathbb{Q}(\sqrt{m})$ es $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$. O sea, $O_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.*

Veremos que $P = \left(2, \frac{1+\sqrt{m}}{2}\right) < O_{\mathbb{Q}(\sqrt{m})}$ tiene norma 2, sin calcularla. Claramente, $A = (2) \subset P$ y $N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(A) = N_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(2) = 2^2$.

Falta ver que $P = \left(2, \frac{1+\sqrt{m}}{2}\right) \neq O_{\mathbb{Q}(\sqrt{m})}$. Lo razonamos al final.

Ahora, si $Q = \left(2, \frac{1-\sqrt{m}}{2}\right)$. Como $1 - m = 8\lambda$ y $1 + \sqrt{m} + 1 - \sqrt{m} = 2$, tenemos

$$PQ = \left(4,\ 1+\sqrt{m},\ 1-\sqrt{m},\ \frac{1-m}{4}\right) = \left(2,\ 1+\sqrt{m}\right) = (2)$$

Y si $P = O_{\mathbb{Q}(\sqrt{m})}$, entonces $Q = (2)$ y $\frac{1-\sqrt{m}}{2} \in (2)$ lo que es absurdo.

Sin calcular bases enteras ni normas, hemos visto que si $m \equiv 1 \pmod 8$ libre de cuadrados, entonces $\left(2, \frac{1+\sqrt{m}}{2}\right)$ y $\left(2, \frac{1-\sqrt{m}}{2}\right)$ tienen norma 2 y

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

es una descomposición única en ideales primos diferentes.

Ejemplo 17. *Si $p \in \mathbb{Z}$ primo impar, $p \nmid m$ y $m \equiv n^2 \pmod p$ libre de cuadrados. Entonces, $P = \left(p, n+\sqrt{m}\right)$ y $Q = \left(p, n-\sqrt{m}\right)$ en $O_{\mathbb{Q}(\sqrt{m})}$ tienen norma p. En efecto,*

$$PQ = \left(p^2,\ pn + p\sqrt{m},\ pn - p\sqrt{m},\ n^2 - m\right) = \left(p^2,\ pn + p\sqrt{m},\ 2pn,\ \lambda p\right) \subseteq (p)$$

Pero $p \nmid m \Longrightarrow p \nmid n$. Entonces, $mcd(p^2, 2pn) = p \Longrightarrow p = ap^2 + b2pn$.
Por tanto, $(p) \subseteq PQ$ y se tiene la igualdad

$$(p) = \left(p, n+\sqrt{m}\right)\left(p, n-\sqrt{m}\right)$$

$P \neq Q$. En caso contrario $2n = n + \sqrt{m} + n - \sqrt{m} \in P = Q$ y como $(2n, p) = 1 \in P$, $(p) = PQ = Q = O_{\mathbb{Q}(\sqrt{m})}$. Pero entonces existiría $\alpha \in O_{\mathbb{Q}(\sqrt{m})}$ tal que $1 = p\alpha \Longleftrightarrow \alpha = 1/p$ sería un racional y e.a. sería entero lo que es absurdo.

Finalmente, si $P = O_{\mathbb{Q}(\sqrt{m})}$ entonces $(p) = Q$ y $n - \sqrt{m} \in (p)$ lo que también es absurdo. Por tanto, P y Q tienen norma p y son primos diferentes.

Si m libre de cuadrados, $K = \mathbb{Q}(\sqrt{m})$ es un c.c. Además, hemos visto que si $A = P_1^{e_1} \cdots P_r^{e_r} < O_K$ es su descomposición única en primos, entonces

$$2 = [K : \mathbb{Q}] = \sum_{i=1}^{r} e_r f_r$$

Por tanto, las posibilidades de descomposición son $A = P^2$, $A = PQ$ o bien $A = P$ si A ideal primo. Por tanto, si $A = (p)$ con $p \in \mathbb{Z}$ primo entero, tenemos

$$(p) = \begin{cases} P^2 & \text{Si } f(P/p) = 1 & A = (p) \text{ ramifica} \\ PQ & \text{Si } f(P/p) = f(Q/p) = 1 & A = (p) \text{ escinde} \\ P & \text{Si } f(P/p) = 2 & A = (p) \text{ es inerte} \end{cases}$$

Vamos a ver ahora, cuando se da la tercera posibilidad. O sea, cuando el grado de inercia es $f(P/p) = 2$ para algún $P < O_{\mathbb{Q}(\sqrt{m})}$ ideal primo sobre (p).

Por definición, el grado de inercia es la dimensión del cuerpo finito $P/(p)$ sobre $\mathbb{Z}_p$. Para que sea 2, basta con que contenga algún $\alpha \notin \mathbb{Z}_p$. Por tanto,

Lema 14. *Si $p \in \mathbb{Z}$ primo impar, m libre de cuadrados, $p \nmid m$ y $m \not\equiv n^2 \pmod{p}$. Entonces, (p) es inerte. O sea, es un ideal primo en $O_{\mathbb{Q}(\sqrt{m})}$.*

Demostración: Consideramos, $h(x) = x^2 - m \in \mathbb{Z}[x]$, que tiene sus raíces en el anillo $O_{\mathbb{Q}(\sqrt{m})}$ por que son e.a. Como el anillo es noetheriano, existe un ideal primo $P < O_{\mathbb{Q}(\sqrt{m})}$ tal que $p \in P$. En el anillo cociente, $V = O_{\mathbb{Q}(\sqrt{m})}/P$ también hay raíces de $x^2 - m$. Pero por la hipótesis, $m \not\equiv n^2 \pmod{p}$, en $\mathbb{Z}_p$ no tiene ninguna raíz. Luego $f(P/p) = dim_{\mathbb{Z}_p}(V) = 2$. □

Lema 15. *Si m impar libre de cuadrados y $m \equiv 5 \pmod 8$. Entonces, (2) es inerte. O sea, es un ideal primo en $O_{\mathbb{Q}(\sqrt{m})}$.*

Demostración: Consideramos, $h(x) = x^2 - x + \frac{1-m}{4} \in \mathbb{Z}[x]$, sus raíces son $\frac{1\pm\sqrt{m}}{2}$ que están en el anillo $O_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Como el anillo es noetheriano, existe un ideal primo $P < O_{\mathbb{Q}(\sqrt{m})}$ tal que $2 \in P$.

En el anillo cociente, $V = O_{\mathbb{Q}(\sqrt{m})}/P$ también hay raíces. Pero por la hipótesis, $\frac{1-m}{4} = \frac{4+8\lambda m}{4} = 1 + 2\lambda m \equiv 1 \pmod 2$, y el polinomio $\overline{h(x)} = x^2 - x + 1 \in \mathbb{Z}_2[x]$ no tiene ninguna raíz en $\mathbb{Z}_2$. Luego $f(P/p) = dim_{\mathbb{Z}_p}(V) = 2$. □

Como resumen de lo anterior. Si p primo y m libre de cuadrados. Entonces,

Teorema 12. *Si $p|m$, $(p) = \left(p, 1+\sqrt{m}\right)^2$. Y si p impar, $p \nmid m$, entonces*

$$(p) = \begin{cases} \left(p, n+\sqrt{m}\right)\left(p, n-\sqrt{m}\right) & Si\ m \equiv n^2 \pmod p \\ (p)\ primo & Si\ m \not\equiv n^2 \pmod p \end{cases}$$

Teorema 13. *Si m impar. Entonces*

$$(2) = \begin{cases} \left(2, 1+\sqrt{m}\right)^2 & Si\ m \equiv 3 \pmod 4 \\ \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & Si\ m \equiv 1 \pmod 8 \\ (2)\ primo & Si\ m \equiv 5 \pmod 8 \end{cases}$$

Teorema 14. *Los ideales primos listados son todos los que hay en $O_{\mathbb{Q}(\sqrt{m})}$.*
Demostración: Como todo $P < O_{\mathbb{Q}(\sqrt{m})}$ primo contiene un entero primo $p \in P$, se tiene $P|(p)$. Por la descomposición única, P es uno de los listados.

Ejemplo 18. *Si* $A = \left(3, 1+\sqrt{-5}\right) < O_{\mathbb{Q}(\sqrt{-5})}$, *vemos que* $m = -5 \equiv -2 \equiv 1 \pmod 3$ *es un cuadrado. Y* $n = 1 \pmod 3$ *es su raíz cuadrada. Por tanto,* $(3) = \left(3, 1+\sqrt{-5}\right)\left(3, 1+\sqrt{-5}\right)$ *es una factorización en primos y* $N(A) = 3$.

Ejemplo 19. *Si* $A = \left(3, 1+\sqrt{17}\right) < O_{\mathbb{Q}(\sqrt{17})}$ *vemos que* $m = 17 \equiv 2 \pmod 3$ *no es un cuadrado. Por tanto,* (3) *es un ideal primo. Pero* $(3) \subset A$ *y no lo divide. Luego* $A = O_{\mathbb{Q}(\sqrt{17})}$. *En efecto,* $-16 = (1+\sqrt{17})(1-\sqrt{17}) \in A$ *y por tanto* $1 = 16 - 3 * 5 \in A$. *O sea, A es ideal primo impropio.*

Como consecuencia, si $O_{\mathbb{Q}(\sqrt{m})}$ es DIP, todos los ideales listados son principales y p ramifica, escinde o permanece primo (inerte) según los casos.

Traduciendo todo lo anterior para c.c. con $h_K = 1$, tenemos

Corolario 12. *Si* $\mathbb{Q}(\sqrt{m})$ *es un DIP, entonces.*

- *Un primo entero* p *es o bien un primo* π *o bien el producto,* $\pi_1\pi_2$, *de dos primos de* $O_{\mathbb{Q}(\sqrt{m})}$ *no necesariamente distintos. Todos estos primos,* $\pi, \pi_1\pi_2$, *con sus asociados son todos los primos de* $O_{\mathbb{Q}(\sqrt{m})}$.
- *Si* $p|m$ *con* p *primo,* p *es asociado del cuadrado de un primo* π.
- *Un primo* $p \in \mathbb{Z}$, *con* $(p, m) = 1$ *es un producto* $\pi_1\pi_2$ *si y sólo si* $\left(\frac{m}{p}\right) = 1$. *En este caso,* π_i *es asociado de* $\overline{\pi_j}$. *Pero* π_1 *y* π_2 *no lo son.*
- *Si* $(2, m) = 1$, 2 *es el asociado del cuadrado de un primo si* $m \equiv 3 \pmod 4$. 2 *es primo si* $m \equiv 5 \pmod 8$. *y* 2 *es el producto de dos primos distintos si* $m \equiv 1 \pmod 8$.

Observamos que $(\alpha) = (\beta)$ en O_K si y sólo si $\beta = u\alpha$ para $u \in U(O_K)$ una unidad en el anillo. Y si $\alpha, \beta \in \mathbb{Z}$, $u \in \mathbb{Q} \cap O_K = \mathbb{Z}$ y $\beta = \pm\alpha$.

Corolario 13. *Si $O_{\mathbb{Q}(\sqrt{m})}$ tiene, $h_K = 1$, sus ideales primos vienen de resolver $4p = \left|x^2 - my^2\right|$ en números enteros, para $p \in \mathbb{Z}$ primo.*

Demostración: Si $h_K = 1$, $O_{\mathbb{Q}(\sqrt{m})}$ es un DIP. Por tanto, todos los ideales primos listados son principales. Viendo los casos listados, si $(p) < O_{\mathbb{Q}(\sqrt{m})}$ escinde o ramifica[7] lo hace en el producto de dos ideales conjugados.

$$(p) = \left(a + b\sqrt{m}\right)\left(a - b\sqrt{m}\right) = \left(a^2 - mb^2\right) \Longleftrightarrow p = \left|a^2 - mb^2\right| \quad \text{Si } m \not\equiv 1 \pmod 4$$
$$(p) = \left(\tfrac{a+b\sqrt{m}}{2}\right)\left(\tfrac{a-b\sqrt{m}}{2}\right) = \left(\tfrac{a^2-mb^2}{4}\right) \Longleftrightarrow 4p = \left|a^2 - mb^2\right| \quad \text{Si } m \equiv 1 \pmod 4$$

Pero si $p = \left|x^2 - my^2\right|$ tiene solución en números enteros también tiene solución $4p = \left|x^2 - my^2\right|$. Luego (p) escinde o ramifica si y sólo si la segunda tiene solución. Y es inerte cuando no tiene solución en números enteros. □

Si $P < O_{\mathbb{Q}(\sqrt{m})}$ ideal primo no nulo, existe $0 \neq \alpha \in P$ y $N(\alpha) = \alpha\overline{\alpha} \in \mathbb{Z} \cap P$[8]. Existe el menor entero positivo, p, contenido en P y es primo. Luego, P divide a (p), y como la norma es multiplicativa, $N(P)$ divide a $N(p) = p^2$. Por tanto, $N(P) = p$ o $N(P) = p^2$. Luego si buscamos ideales primos de norma menor que M, basta descomponer (p) con p primo tal que $p < M$.

[7] Si ramifica es el cuadrado de un ideal autoconjugado.

[8] Porque es el término constante del polinomio mínimo de α.

Ejemplo 20. *Vamos a calcular todos los ideales primos de norma menor que 10, en el c.c.* $\mathbb{Q}(\sqrt{65537})$. *Sabemos que* $m = 65537 = 2^{16}+1$ *es el* $F_4 = 2^{2^4}+1$ *primo de Fermat. Por tanto,* $m \equiv 1 \pmod 4$ *y su anillo de enteros es*

$$O_{\mathbb{Q}(\sqrt{65537})} = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\langle 1, \frac{1+\sqrt{m}}{2}\right\rangle = \left\{a + b\frac{1+\sqrt{m}}{2} : \ a, b \in \mathbb{Z}\right\}$$

Vamos a descomponer (p) *para* $p = 2, 3, 5$ *y* 7 *que son menores que 10.*

Como $m = 65537 \equiv 1 \pmod 8$. *Entonces* $(2) = \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right)$

Como el discriminante del cuerpo es $d_{\sqrt{65537}} = 65537$. *El único primo que lo divide es 65537.* $(65537) = \left(65537, 1+\sqrt{65537}\right)^2$ *ramifica pero no tiene norma menor que 10. Ahora, como*

$$\left(\frac{m}{3}\right) = \left(\frac{m}{5}\right) = \left(\frac{m}{7}\right) = -1$$

Para los tres primos $m = 65537$ *no es un residuo cuadrático. Por tanto, los ideales principales* (3), (5) *y* (7) *son inertes. O sea, permanecen primos y por tanto también los enteros 3, 5 y 7 son primos en* $O_{\mathbb{Q}(\sqrt{65537})}$.

Si queremos hallar los ideales de norma menor o igual que 10. Por la factorización única en ideales primos. Llamando $A = \left(2, \frac{1+\sqrt{m}}{2}\right)$, $B = \left(2, \frac{1-\sqrt{m}}{2}\right)$ *que tienen norma 2. Los ideales con norma* ≤ 10 *son*

$$A,\ B,\ (2),\ (3),\ (3)A,\ (3)B,\ (5),\ (5)A,\ (5)B,\ (7)$$

6. Dominios euclídeos.

Si R es un dominio de integridad (DI), definimos

Definición 14. ***función euclídea*** *(f.e.)* $\phi : R^* \longrightarrow \mathbb{Z}^+$ *si para todo* $a, b \in R$

(1) $ab \neq 0 \Longrightarrow \phi(a) \leq \phi(ab)$
(2) $b \neq 0 \Longrightarrow \exists q, r \in R : \ a = bq + r$ *con* $\phi(r) < \phi(b)$ *o bien* $r = 0$

Si existe una f.e. decimos que el DI R es un ***dominio euclídeo*** *(DE). Y decimos que satisface el* ***algoritmo de Euclides*** *para* ϕ.

Así, $O_{\mathbb{Q}(\sqrt{m})}$ es un DE si satisface el algoritmo de Euclides para alguna f.e. La función valor absoluto de la norma satisface (1) y en general no (2).

$$O_K \longrightarrow \mathbb{Z}^+, \ \alpha \mapsto |N(\alpha)|$$

Pero puede servir como f.e. en algunos casos[9].

Corolario 14. *Si para todo* $\alpha, \beta \in O_K$, *con* $\beta \neq 0$, *existen e.a.* γ, δ *tales que* $\alpha = \gamma\beta + \delta$ *con* $|N(\delta)| < |N(\beta)|$ *o bien* $\delta = 0$. *Entonces,* $O_{\mathbb{Q}(\sqrt{m})}$ *es un DE. En este caso, diremos que el c.n.* $K = \mathbb{Q}(\sqrt{m})$ *es* ***euclídeo***.

Como es conocido se verifica $DE \Longrightarrow DIP \Longrightarrow DFU \Longrightarrow DI$. Por tanto, si $O_{\mathbb{Q}(\sqrt{m})}$ es un DE todo ideal entero es principal y todo e.a. α descompone de forma única como producto de irreducibles.

[9] Hay anillos cuadráticos de e.a. que son DE para otras f.e.

Teorema 15. *$\mathbb{Q}(\sqrt{m})$ es euclídeo para $m = -1, -2, -3, -7, -11,\ 2,\ 3$ y 5.*

Demostración: Sean $\alpha, \beta \in O_K$, con $\beta \neq 0$, entonces $\frac{\alpha}{\beta} = u + v\sqrt{m}$ con u y v números racionales. Si tomamos los enteros mas cercanos a ambos.

$$0 \leq |u - a| \leq \frac{1}{2}, \quad 0 \leq |v - b| \leq \frac{1}{2}$$

y definimos $\gamma = a + b\sqrt{m}$ y $\delta = \alpha - \gamma\beta$. Ambos son e.a. de $\mathbb{Q}(\sqrt{m})$ y tenemos

$$N(\delta) = N(\alpha - \gamma\beta) = N(\beta)\, N\left(\frac{\alpha}{\beta} - \gamma\right) = N(\beta)\, N\left((u-a) + (v-b)\sqrt{m}\right)$$

$$\left|N(\delta)\right| = \left|N(\beta)\right| \left|(u-a)^2 - m(v-b)^2\right| \Longrightarrow \begin{cases} \left|N(\delta)\right| \leq \left|N(\beta)\right| \frac{m}{4} & \text{Si } \ 0 < m \\ \left|N(\delta)\right| \leq \left|N(\beta)\right| \frac{1-m}{4} & \text{Si } \ m < 0 \end{cases}$$

Ya que tenemos las siguientes acotaciones

$$\begin{array}{rcll} -\frac{m}{4} & \leq & (u-a)^2 - m(v-b)^2 & \leq \frac{1}{4} \qquad \text{Si } \ 0 < m \\ 0 & \leq & (u-a)^2 - m(v-b)^2 & \leq \frac{1}{4} + \frac{1}{4}(-m) \qquad \text{Si } \ m < 0 \end{array}$$

Luego, para $m = -1, -2,\ 2$ y 3 ya tenemos $|N(\delta)| \leq \left|N(\beta)\right| \frac{3}{4} < \left|N(\beta)\right|$. Para el resto de casos, elegimos γ de una forma diferente. Elegimos el entero s mas cercano a $2v$. O sea, $|2v - s| \leq \frac{1}{2}$. Después el entero r mas cercano a $2u$ pero tal que $r \equiv s \pmod 2$. Y tenemos $|2u - r| \leq 1$.

Ahora, los casos que quedan $-3, -7, -11$ y 5 son todos congruentes con 1 módulo 4. Por tanto, su anillo de enteros es $\mathbb{Z}\left[\frac{1+m}{2}\right]$. Y en los 4 casos, $\gamma = \frac{r+s\sqrt{m}}{2}$ es un e.a. del cuerpo $\mathbb{Q}(\sqrt{m})$. Por tanto, también $\delta = \alpha - \gamma\beta$.

Para $m=-3,-7,-11$, tenemos las desigualdades

$$N(\delta)=N(\beta)N\left(\frac{\alpha}{\beta}-\gamma\right)=N(\beta)\left(\left(u-\tfrac{r}{2}\right)^2-m\left(v-\tfrac{s}{2}\right)^2\right)\Longrightarrow$$
$$|N(\delta)|\leq\left|N(\beta)\right|\left(\tfrac{1}{4}+(-m)\tfrac{1}{16}\right)=\left|N(\beta)\right|\tfrac{4-m}{16}<\left|N(\beta)\right|\tfrac{15}{16}<\left|N(\beta)\right|$$

Y para $m=5$, tenemos las siguientes

$$-\tfrac{5}{16}\leq\left(u-\tfrac{r}{2}\right)^2-5\left(v-\tfrac{s}{2}\right)^2\leq\tfrac{1}{4}\Longrightarrow$$
$$|N(\delta)|\leq\left|N(\beta)\right|\tfrac{5}{16}<\left|N(\beta)\right|$$

O sea, para los casos $-3,-7,-11$ y 5 nos sirve $\gamma=\frac{r+s\sqrt{m}}{2}$ como cociente. □

Damos sin demostración la lista de los c.c. $\mathbb{Q}(\sqrt{m})$ que son euclídeos:

Teorema 16. *$\mathbb{Q}(\sqrt{m})$ es euclídeo si y sólo si* $m=-11,-7,-3,-2,-1,\ 2,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73.$

Los anillos de e.a. anteriores son DE respecto del valor absoluto de la norma. Para $0<m<100$, además de los anteriores son DE respecto de alguna f.e. distinta del valor absoluto de la norma, los siguientes.

$m=14,22,23,31,35,38,43,46,47,53,59,61,62,67,69,71,77,83,86,89,93,94,97$

Para m negativos, se sabe que no hay mas DE que los citados $m=-11,-7,-3,-2,-1$. Pero hay $O_{\mathbb{Q}(\sqrt{m})}$ que son DIP[10]. Así, para $m<0$

Teorema 17. *$O_{\mathbb{Q}(\sqrt{m})}$ es DIP si y sólo si* $m=-1,-2,-3,-7,-11,-19,-43,-67,-163.$

[10] O sea, hay ejemplos de DIP que no son DE.

Ejemplo 21. *Vamos a descomponer* $p = 65537$ *en* $O_{\mathbb{Q}(\sqrt{-11})}$. *Como* $-11 \equiv 1 \pmod 4$, *sabemos que* $O_{\mathbb{Q}(\sqrt{-11})} = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$. *Además, como* $65537 = 2^{16} + 1 \equiv 1 \pmod 4$ *el símbolo de Jacobi* $\left(\frac{m}{p}\right)$ *es*

$$\left(\frac{-11}{65537}\right) = \left(\frac{-1}{65537}\right)\left(\frac{11}{65537}\right) = (-1)^{(p-1)/2}\left(\frac{65537}{11}\right) = \left(\frac{10}{11}\right) = \left(\frac{-1}{11}\right) = (-1)^{10/2} = -1$$

Por tanto, $x^2 \equiv -11 \pmod{65537}$ *no tiene solución,* (65537) *es inerte y permanece primo. Y su generador* $p = 65537$ *también es primo en* $O_{\mathbb{Q}(\sqrt{-11})}$.

Ejemplo 22. *Vamos a descomponer* $p = 27213649$ *en* $O_{\mathbb{Q}(\sqrt{-11})}$. *Sabemos que* 27213649 *es primo porque 13 es un elemento primitivo en* $\mathbb{Z}_{27213649}$. *Además, si calculamos el símbolo de Jacobi sale* $\left(\frac{-11}{p}\right) = 1$. *Por tanto,* $x^2 \equiv -11 \pmod{27213649}$ *tiene soluciones, que se pueden calcular con el algoritmo de Tonelli-Shanks. En este caso, las soluciones son* 9019282 *y* 18194367. *Tomamos la impar* $n = 18194367$ *y como* $p = 27213649$ *es un primo impar y no divide a* $m = -11$, *tenemos la descomposición*

$$(p) = \left(p, n + \sqrt{m}\right)\left(p, n - \sqrt{m}\right)$$

Ahora, según el algoritmo de Cornachia- Smith modificado, si aplicamos el AE a $2p$ *y n, después de 7 divisiones, obtenemos el primer resto* $r = 350$ *que es menor que* $2\sqrt{p} \approx 10433.3$. *Este nos da la factorización* $4p = 350^2 + 11 * 3144^2 \Rightarrow p = 175^2 + 11 * 1572^2 = \left(175 + 1572\sqrt{-11}\right)\left(175 - 1572\sqrt{-11}\right)$.
O sea, hemos encontrado los generadores de los ideales $\left(p, n \pm \sqrt{m}\right)$.

7. Ejercicios.

Ejercicio 1. *Razona* $(2) = \left(2, 1+\sqrt{-5}\right)^2$. *¿Qué norma tienen estos ideales?*

Ejercicio 2. *Razona que la factorización siguiente es en ideales primos*

$$(6) = \left(2, 1+\sqrt{-5}\right)^2 \left(3, 1+\sqrt{-5}\right)\left(3, 1+\sqrt{-5}\right)$$

Razona que 2 y 3 son irreducibles pero no primos en $O_{\mathbb{Q}(\sqrt{-5})}$

Ejercicio 3. *Razona que las factorizaciones siguientes*

$$13 = \left(1+2\sqrt{-3}\right)\left(1-2\sqrt{-3}\right) = \frac{7+\sqrt{-3}}{2} \cdot \frac{7-\sqrt{-3}}{2}$$

son compatibles con que $O_{\mathbb{Q}(\sqrt{-3})}$ *es DFU.*

Ejercicio 4. *Prueba que* $\sqrt{3}-1$ *y* $\sqrt{3}-1$ *son asociados en* $\mathbb{Q}(\sqrt{3})$.

Ejercicio 5. *Prueba que los primos de* $O_{\mathbb{Q}(\sqrt{3})}$ *son* $\sqrt{3}-1$ *y* $\sqrt{3}$, *todos los primos enteros* $p \equiv \pm 5 \pmod{12}$ *y todos los factores* $a+b\sqrt{3}$ *de primos enteros* $p \equiv \pm 1 \pmod{12}$. *Y todos sus asociados.*

Ejercicio 6. *Prueba que los primos de* $O_{\mathbb{Q}(\sqrt{2})}$ *son* $\sqrt{2}$, *todos los primos enteros* $p \equiv \pm 3 \pmod{8}$ *y todos los factores* $a+b\sqrt{3}$ *de primos enteros* $p \equiv \pm 1 \pmod{8}$. *Y todos sus asociados.*

Ejercicio 7. *¿ Cómo son todos los ideales primos de* $O_{\mathbb{Q}(\sqrt{-2})}$*?*

Ejercicio 8. *Sabiendo que* $h_{\mathbb{Q}(\sqrt{-11})} = 1$. *Halla todos sus ideales enteros primos de norma menor que 10.*

Ejercicio 9. *Razona que* $\left(65537, 8820 \pm \sqrt{-19}\right) < O_{\mathbb{Q}(\sqrt{-19})}$ *son id. primos.*

Ejercicio 10. *Encuentra generadores que demuestren que los ideales* $\left(65537, 8820 \pm \sqrt{-19}\right)$ *son principales en* $O_{\mathbb{Q}(\sqrt{-19})}$.

8. Referencias.

[1] Borevich Z.I., Shafarevich I.R.: *Number Theory*, Academic Press, New York, 1966.

[2] Bressoud D., Wagon S.: *A Course in Computational Number Theory*, John Wiley & Sons, Hoboken, NJ, USA, 2000.

[3] Fine B., Rosenberger G.: *Number Theory. An introduction via the distribution of primes*, Birkhäuser, Boston, 2007.

[4] Irelan K., Rosen M.: *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1982.

[5] Lidl R., Niederreiter H.: *Finite Fields*, Cambridge University Press, U.K., 1997.

[6] Niven I., Zuckerman H.S., Montgomery H.L.: *An Introduction to the Theory of Numbers*, John Wiley and sons, USA, 1991.

9. TEST DE REPASO.

Para comenzar el cuestionario pulsa el botón de inicio.
Cuando termines pulsa el botón de finalizar.
Para marcar una respuesta coloca el ratón en la letra correspondiente y pulsa el botón de la izquierda (del ratón).

Inicio del Test

1. Dado un ideal entero de un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es la correcta?.

(a) Su discriminante puede ser irracional.
(b) Su discriminante a veces es un número entero.
(c) Todos los ideales enteros tienen el mismo discriminante.
(d) Su discriminante a veces es muy grande.

2. Dado un ideal entero de un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) Su discriminante puede ser cero.
(b) Su discriminante puede ser negativo.
(c) Su discriminante es mínimo siempre.
(d) Su discriminante a veces no existe.

3. Dado un ideal I de un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) A veces tiene una base entera.
(b) Tiene un discriminante positivo.
(c) Es siempre un subgrupo aditivo de rango máximo de O_K.
(d) Es siempre un subgrupo aditivo finito.

4. Dado un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) Todas sus base enteras tienen discriminante positivo.
(b) Todas sus base enteras tienen discriminante mínimo.
(c) Todas sus base enteras tienen discriminante negativo.
(d) Sus bases enteras sirven para definir el discriminante del c.n. K.

5. Dado un ideal I de un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) Su norma a veces coincide con su discriminante.
(b) Su norma puede ser negativa.
(c) Su norma siempre es un cuadrado.
(d) Su discriminante puede ser el discriminante del c.n. K.

6. Dado un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) O_K a veces es noetheriano.
(b) O_K nunca es artiniano.
(c) O_K es un anillo de Dedekind
(d) Puede tener ideales primos no maximales.

7. Dado un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) Sus ideales primos forman un monoide abeliano libre respecto de la multiplicación.
(b) El producto de ideales primos a veces no es cancelativo.
(c) Sus ideales primos forman un monoide abeliano respecto de la multiplicación finitamente generado.
(d) Sus ideales primos son principales.

8. Dado un anillo de números O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) Siempre es un DIP.
(b) Siempre es un DFU.
(c) Nunca es DIP ni DFU.

(d) Si es DFU es DIP.

9. Dado el conjunto de las clases de ideales enteros de un a.n. O_K.
¿Cuál de las siguientes afirmaciones es verdadera?.

(a) A veces en un grupo infinito.
(b) A veces en un grupo no conmutativo.
(c) Puede ser sólo un monoide.
(d) Su tamaño h_K lo llamamos el número de clases del c.n. K.

10. ¿Cuál de las siguientes afirmaciones es verdadera?.

(a) Existe un número finito de c.c. $\mathbb{Q}(\sqrt{m})$ que son DIP.
(b) Existe un número finito de c.c. $\mathbb{Q}(\sqrt{m})$ con $m > 0$ que son DIP.
(c) Existe un número infinito de c.c. $\mathbb{Q}(\sqrt{m})$ con $m > 0$ que son DIP.
(d) Existe un número finito de c.c. $\mathbb{Q}(\sqrt{m})$ con $m < 0$ que son DIP.

Final del Test | Puntos: