UNIVERSIDAD AUTÓNOMA METROPOLITANA
Iztapalapa

Departamento de Matemáticas

Órdenes en Campos de Números y el Teorema de Furtwängler

Presenta:
MAT. JULIO PÉREZ HERNÁNDEZ

para la obtención del grado
MAESTRO EN CIENCIAS (MATEMÁTICAS)

Asesor: Dr. Alejandro Aguilar Zavoznik

México
3 de Marzo de 2017

Índice general

Introducción

Pierre de Fermat fue uno de los principales matemáticos de la primera mitad del siglo XVII, gracias a él se renovó el interés por la teoría de números. Tras su muerte, uno de sus hijos publicó las notas de su padre, entre las cuales se encontraba una pequeña declaración de haber probado lo que desde entonces se conoce como *el último teorema de Fermat*, el cual es:

Si $n \geq 3$, no existen enteros diferentes de cero x, y, z que satisfagan la siguiente ecuación

$$x^n + y^n = z^n$$

Este teorema fue demostrado en 1995 por el matemático *Andrew Wiles*.

Euler (1706-1783), en su manuscrito *Algebra* de 1770, dio una prueba para el caso $n = 3$ del último teorema de Fermat; sin embargo, su demostración contenía un sutil error. Euler trabajó con números algebraicos de la forma $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$, creyendo que estos números poseían las mismas propiedades que los enteros ordinarios, incluyendo la factorización única. A pesar de que $\mathcal{O}$ no tiene esta última propiedad, da la casualidad de que los elementos con los que trabajó tienen únicamente una descomposición en elementos irreducibles. Esta omisión pasó desapercibida en aquel momento, no obstante el caso $n = 3$ se le atribuye a Euler, dado que él publicó una prueba alternativa (ver [**17**], pág. 184).

En este trabajo estudiaremos las propiedades de ciertos subanillos de los campos de números llamados órdenes, concentrándonos en las propiedades aritméticas de éstos, entre las que destaca el estudio de un ideal llamado conductor y su caracterización mediante el teorema de Furtwängler. En particular $\mathcal{O}$ es un orden de $\mathbb{Q}(\sqrt{-3})$.

Comenzaremos con la introducción a la teoría de los números algebraicos la cual será presentada en el capítulo 1, en el que incluiremos el teorema chino del residuo, el cual será importante debido a que lo usaremos en la demostración del teorema de Furtwängler. Por último veremos qué forma tienen los anillos de enteros en campos cuadráticos y en extensiones cúbicas puras.

En el capítulo 2 damos la definición de orden y conductor, veremos las propiedades que cumplen los ideales que son primos relativos al conductor. Al final de la sección 2.2 mostraremos que los elementos de $\mathcal{O}$ con norma impar tienen factorización única. Por último veremos la relación entre el número de clases del anillo de enteros y el número de clases de un orden, presentando algunos resultados propios, de cómo calcular explícitamente el número de clases de un orden dado en un campo cuadrático imaginario.

Finalmente, en el capítulo 3 vamos a demostrar el teorema de Furtwängler, el cual nos servirá para saber qué ideales del anillo de enteros son conductores de algún orden. Por último damos la caracterización de los ideales conductor en campos cuadráticos y extensiones cúbicas.

Capítulo 1

Antecedentes

Este capítulo contiene la teoría necesaria que se requiere para entender la aritmética del anillo de enteros de un campo de números. Veremos cuándo el anillo de enteros es un anillo de factorización única y para ello necesitamos estudiar el número de clases de un campo de números.

Primero recordemos que si R es un anillo conmutativo con unidad. Un R-**módulo** es un par (M,μ), donde M es un grupo (aditivo) abeliano y μ es una aplicación de $R \times M$ en M tal que, representando por ax a $\mu(a, x)$ ($a \in R$, $x \in M$), se satisfacen los siguientes axiomas:

$$a(x + y) = ax + ay$$

$$(a + b)x = ax + bx$$

$$(ab)x = a(bx)$$

$$1x = x,$$

para $a, b \in R$ y $x, y \in M$.

Un **submódulo** M' de M es un subgrupo aditivo de M que es cerrado respecto a la multiplicación por elemento de R.

El lector interesado en la teoría de módulos puede consultar **[3]**.

A lo largo de la tesis, trabajaremos con extensiones finitas sobre $\mathbb{Q}$, a menos que se diga lo contrario.

1.1. La norma, la traza y el discriminante

Sean L/K una extensión con $[L : K] = n$, $\mathbb{Q} \subseteq K \subseteq L$ y $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base de L como K-espacio vectorial. Para $\alpha \in L$ definimos la transformación lineal $T_\alpha : L \to L$ como:

$$T_\alpha(\alpha_i) = \alpha\alpha_i = \sum_{j=1}^{n} a_{ji}\alpha_j,$$

donde a_{ji} son los coeficientes de $\alpha\alpha_i$ usando la base $\mathcal{B}$. Denotaremos por (a_{ij}) a la matriz cuyas entradas son los coeficientes que acabamos de obtener. Usando lo anterior definiremos dos funciones que serán muy importantes a lo largo de este trabajo.

Definición 1.1. *La* **norma** *de* $\alpha \in L$ *es* $N(\alpha) = \det(a_{ij})$ *y la* **traza** *de* α *es* $tr(\alpha) = \sum_{i=1}^{n} a_{ii}$.

La siguiente proposición nos muestra que la norma y la traza de un elemento en L no dependen de la base de L que elijamos.

Proposición 1.2. *Sean* $\{\alpha_1, \ldots, \alpha_n\}$, $\{\beta_1, \ldots, \beta_n\}$ *bases de* L/K *y* $\alpha \in L$, *con* $A = (a_{ij})$ *construida con* $\{\alpha_1, \ldots, \alpha_n\}$ *y* $B = (b_{ij})$ *construida con* $\{\beta_1, \ldots, \beta_n\}$. *Entonces* $\det(A) = \det(B)$ *y* $tr(A) = tr(B)$.

DEMOSTRACIÓN. Sea N la matriz tal que $A = N^{-1}BN$, tenemos:

$$\det(A) = \det(N^{-1}BN) = \det(N)^{-1}\det(B)\det(N) = \det(B)$$

debido a que el determinante es multiplicativo y

$$tr(A) = tr(N^{-1}BN) = tr(NN^{-1}B) = tr(IB) = tr(B),$$

pues la traza satisface la propiedad $tr(CD) = tr(DC)$, para $C, D \in M_n(\mathbb{R})$. □

El resultado que a continuación se presenta, da una forma más sencilla de cómo calcular la norma y la traza de un elemento.

Proposición 1.3. *Si* L/K *es separable, con* $[L : K] = n$ *y* $\{\sigma_1, \ldots, \sigma_n\}$ *los* K*-isomorfismos distintos de* L *a una cerradura algebraica de* K, *entonces para* $\alpha \in L$ *tenemos que* $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ *y* $tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.

DEMOSTRACIÓN. Ver [**12**], proposición 2.6, pág. 9. □

Teorema 1.4. *Sean* L/K *una extensión finita de grado* n, $\alpha, \beta \in L$ *y* $a \in K$. *Entonces:*

(i) $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$.
(ii) $tr(a\alpha) = a \cdot tr(\alpha)$.
(iii) $N(a\alpha) = a^n \cdot N(\alpha)$.
(iv) $N(\alpha\beta) = N(\alpha)N(\beta)$.
(v) *Si* $\alpha \neq 0$, *entonces* $N(\alpha^{-1}) = N(\alpha)^{-1}$.
(vi) $N(a) = a^n$.
(vii) $tr(a) = n \cdot a$.

DEMOSTRACIÓN. Se sigue inmediatamente de la definición de norma y traza. □

Notemos que de (i) y (ii) del teorema 1.4 podemos deducir que la traza es lineal.

Definición 1.5. *Sea* L/K *una extensión finita y* $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset L$ *un conjunto cualquiera, el* **discriminante** *de* $\mathcal{B}$ *se define como:*

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(tr(\alpha_i\alpha_j))$$

Proposición 1.6. *Sea* L/K *una extensión finita de grado* n. *Entonces*

(i) *Si* $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$, *entonces* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *es una base de* L *como* K*-espacio vectorial.*
(ii) *Si* L/K *es separable y* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *es base, entonces* $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$.

DEMOSTRACIÓN. (i) Está demostración se hará por contraposición.
Supongamos que $\alpha_1, \alpha_2, \ldots, \alpha_n$ son linealmente dependientes y tomemos la combinación lineal $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = 0$ con algunos $a_i \neq 0$. Si multiplicamos esta ecuación por α_j tenemos

$$a_1\alpha_1\alpha_j + a_2\alpha_2\alpha_j + \ldots + a_n\alpha_n\alpha_j = 0$$

Sacamos la traza a la ecuación anterior, y por la linealidad de la traza obtenemos

$$\sum_{i=1}^{n} a_i tr(\alpha_i\alpha_j) = tr(0) = 0 \quad \text{para cada } j = 1, \ldots, n$$

Es decir, $(a_1, \ldots, a_n)$ es una solución no trivial de

$$\begin{aligned} tr(\alpha_1\alpha_1)x_1 + \cdots + tr(\alpha_n\alpha_1)x_n &= 0 \\ tr(\alpha_1\alpha_2)x_1 + \cdots + tr(\alpha_n\alpha_2)x_n &= 0 \\ &\vdots \\ tr(\alpha_1\alpha_n)x_1 + \cdots + tr(\alpha_n\alpha_n)x_n &= 0 \end{aligned}$$

Si consideramos la matriz $A = (tr(\alpha_i\alpha_j))$, tenemos $\det(A) = 0 = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

(ii) Supongamos que L/K es separable, $\{\alpha_1, \ldots, \alpha_n\}$ es base de L/K y además que $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. Entonces el sistema

$$\sum_{i=1}^{n} x_i tr(\alpha_i\alpha_j) = 0$$

tiene al menos una solución no trivial $(a_1, \ldots, a_n)$, donde $a_i \neq 0$ para algún i.
Consideramos $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$, donde $\alpha \neq 0$ pues $\{\alpha_1, \ldots, \alpha_n\}$ es base y al menos un $a_i \neq 0$. Dado que la traza es lineal, tenemos

$$tr(\alpha\alpha_j) = \sum_{i=1}^{n} a_i tr(\alpha_i\alpha_j) = 0.$$

Sea $\beta = \sum_{i=1}^{n} b_i\alpha_i$ un elemento cualquiera de L, entonces $\alpha\beta = \sum_{i=1}^{n} b_i\alpha\alpha_i$. Sacando la traza

$$tr(\alpha\beta) = \sum_{i=1}^{n} b_i tr(\alpha\alpha_i) = \sum_{i=1}^{n} b_i \cdot 0 = 0.$$

En particular si $\beta = \frac{1}{\alpha}$ tenemos $0 = tr(\alpha\beta) = tr(\alpha\frac{1}{\alpha}) = tr(1) = [L : K] = n$, lo cual no puede ser porque la extensión es separable.

□

Las siguientes dos proposiciones nos dan algunas propiedades del discriminante de una base.

Proposición 1.7. *Sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ bases de una extensión finita L/K. Entonces*

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

donde (a_{ij}) es la matriz cambio de base.

DEMOSTRACIÓN. Notemos que $\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i$ y $\alpha_k = \sum_{l=1}^{n} a_{lk}\beta_l$ por tanto:

$$\alpha_j\alpha_k = \sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{lk}\beta_j\beta_l.$$

Al tomar la traza en ambos lados:

$$tr(\alpha_j\alpha_k) = \sum_{j=1}^{n}\sum_{l=1}^{n} a_{ij}a_{lk}tr(\beta_i\beta_l).$$

Sean $A = (tr(\alpha_j\alpha_k))$, $B = (tr(\beta_i\beta_l))$ y $C = (a_{ij})$ y obsevemos que $A = CBC^T$. Finalmente, usando propiedades del determinante,

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

. □

Proposición 1.8. *Sea L/K separable de grado n. Si $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$, entonces*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\alpha_i^{(j)})^2$$

donde $\alpha_i^{(j)} = \sigma_j(\alpha_i)$ y $\{\sigma_1, \ldots, \sigma_n\}$ son los K-isomorfismos distintos de L a una cerradura algebraica de K.

DEMOSTRACIÓN. Ver [**7**], pág. 173, proposición 12.1.3. □

1.2. Anillo de enteros asociado a un campo de números

En esta sección veremos qué es el anillo de enteros de un campo de números y cuáles son las propiedades que cumple dicho anillo.

Definición 1.9. *$z \in \mathbb{C}$ es un* **entero algebraico** *si z es raíz de algún polinomio mónico con coeficientes enteros. Definimos*

$$\Omega = \{z \in \mathbb{C} : z \text{ es un entero algebraico}\}.$$

Antes de continuar necesitamos los siguientes resultados.

Definición 1.10. *Sea A un anillo conmutativo con 1. Diremos que A es un* **anillo noetheriano** *si toda cadena ascendente de ideales propios*

$$I_1 \subseteq I_2 \cdots \subseteq I_r \subseteq \cdots$$

se detiene, es decir existe m tal que $I_m = I_{m+1} = \cdots$.

Definición 1.11. *Un $\mathbb{Z}$-módulo finitamente generado, es un subconjunto no vacío $W \subseteq \mathbb{C}$ tal que:*

i) *Si $a \in \mathbb{Z}$ y $\gamma \in W$, entonces $a\gamma \in W$.*
ii) *Si $\gamma_1, \gamma_2 \in W$, entonces $\gamma_1 + \gamma_2 \in W$.*
iii) *Existen $\gamma_1, \gamma_2, \ldots, \gamma_n \in W$ tales que $W = \gamma_1\mathbb{Z} + \gamma_2\mathbb{Z} + \cdots + \gamma_n\mathbb{Z}$.*

Proposición 1.12. *Sean W un $\mathbb{Z}$-módulo, con $W \neq \{0\}$ y $\omega \in \mathbb{C}$ tal que $\omega\gamma \in W$ para todo $\gamma \in W$. Entonces $\omega \in \Omega$.*

DEMOSTRACIÓN. Sean $\gamma_1, \ldots, \gamma_n$ una base de W. Por hipótesis, $\omega\gamma_i \in W$ para $1 \leq i \leq n$. Lo que implica

$$\omega\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j \tag{1}$$

con $a_{ij} \in \mathbb{Z}$. Sea δ_{ij} la función delta de Kronecker. Entonces

$$\omega\gamma_i = \delta_{ii}\omega\gamma_i = \sum_{j=1}^{n} \delta_{ij}\omega\gamma_j. \tag{2}$$

De las ecuaciones (1) y (2)

$$0 = \sum_{j=1}^{n} \delta_{ij}\omega\gamma_j - \sum_{j=1}^{n} a_{ij}\gamma_j = \sum_{j=1}^{n} (\delta_{ij}\omega - a_{ij})\gamma_j.$$

Si $A = (\delta_{ij}\omega - a_{ij})$, observamos que $\det(A) = 0$ y $\det(\delta_{ij}x - a_{ij})$ es un polinomio mónico de grado n con coeficientes enteros del cual ω es raíz. Por lo tanto $\omega \in \Omega$. □

Proposición 1.13. *Ω es un anillo.*

DEMOSTRACIÓN. Ver [**1**], pág. 26, teorema 2.3 □

Veamos algunos ejemplos.

Ejemplo 1.14. *Los números $z = \dfrac{-1 \pm i\sqrt{3}}{2}$ son enteros algebraicos ya que $f(z) = 0$, con $f(x) = 1 + x + x^2 \in \mathbb{Z}[x]$.*

Ejemplo 1.15. *Los números $\dfrac{-1+i}{\sqrt{2}}, \dfrac{1-i}{\sqrt{2}}, \dfrac{1+i}{\sqrt{2}}, \dfrac{-1-i}{\sqrt{2}}$ son enteros algebraicos pues son raíces de $f(x) = 1 + x^4$.*

Definición 1.16. *Sea F un subcampo de $\mathbb{C}$. Diremos que F es un campo de números si $[F : \mathbb{Q}] < \infty$. El* **anillo de enteros** *de un campo de números F es el conjunto*

$$\mathcal{O}_F = \{\alpha \in F : \alpha \textit{ es un entero algebraico}\}.$$

El conjunto $\mathcal{O}_F$ tiene estructura de anillo pues claramente $\mathcal{O}_F = F \cap \Omega$.

Lema 1.17. *Sea $\beta \in F$. Existe $b \in \mathbb{Z} \setminus \{0\}$ tal que $b\beta \in \mathcal{O}_F$.*

DEMOSTRACIÓN. Como $\beta \in F$, entonces β es raíz de algún polinomio $f(x) = b_0 + b_1x + \cdots + b_nx^n \in \mathbb{Z}[x]$, es decir

$$f(\beta) = 0 = b_0 + b_1\beta + \cdots + b_n\beta^n.$$

Multiplicamos por b_n^{n-1}

$$\begin{aligned} 0 &= b_0b_n^{n-1} + b_1b_n^{n-1}\beta + \cdots + b_nb_n^{n-1}\beta^n \\ &= b_0b_n^{n-1} + b_1b_n^{n-2}(b_n\beta) + b_2b_n^{n-3}(b_n\beta)^2 + \cdots + (b_n\beta)^n \end{aligned}$$

Sea $h(x) = b_0 b_n^{n-1} + b_1 b_n^{n-2} x + b_2 b_n^{n-3} x^2 + \cdots + x^n$ y notemos que $h(b_n\beta) = 0$, por tanto $b_n\beta \in \mathcal{O}_F$. Así, $b = b_n$. □

Corolario 1.18. *Sean $\beta_1, \beta_2, \ldots, \beta_r \in F$. Existe $b \in \mathbb{Z} \setminus \{0\}$ tal que $b\beta_1, b\beta_2, \ldots, b\beta_r \in \mathcal{O}_F$.*

DEMOSTRACIÓN. Sea $b_i \in \mathbb{Z} \setminus \{0\}$ tal que $b_i\beta_i \in \mathcal{O}_F$. Si $b = mcm(b_1, \ldots, b_r)$, entonces $b_i \mid b$ de donde $b = b_i t_i$, para algún $t_i \in \mathbb{Z}$. Como $b_i\beta_i \in \mathcal{O}_F$, tenemos $b_i t_i \beta_i \in \mathcal{O}_F$ y $b\beta_i = b_i t_i \beta_i \in \mathcal{O}_F$. □

Proposición 1.19. *Sea $I \neq 0$ un ideal de $\mathcal{O}_F$. Entonces I contiene una base de F como $\mathbb{Q}$-espacio vectorial.*

DEMOSTRACIÓN. Sean $\{\beta_1, \ldots, \beta_n\}$ base de $F/\mathbb{Q}$ y $b \in \mathbb{Z}\setminus\{0\}$ tal que $b\beta_1, b\beta_2, \ldots, b\beta_n \in \mathcal{O}_F$.

Sea $l \in I \setminus \{0\}$, $lb\beta_1, lb\beta_2, \ldots, lb\beta_n \in I$. Supongamos

$$(\alpha_1 lb)\beta_1 + (\alpha_2 lb)\beta_2 + \cdots + (\alpha_n lb)\beta_n = 0,$$

para algunos $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$. Como $\{\beta_1, \ldots, \beta_n\}$ es una base de $F/\mathbb{Q}$, tenemos $\alpha_i lb = 0$, para cada $i = 1, \ldots, n$. Así, $\alpha_i = 0$ para todo $i = 1, \ldots, n$, es decir, $\{lb\beta_1, lb\beta_2, \ldots, lb\beta_n\}$ es linealmente independiente y claramente genera a F. Por lo tanto $\{lb\beta_1, lb\beta_2, \ldots, lb\beta_n\}$ es base de $F/\mathbb{Q}$. □

Lema 1.20. *Un número racional $\alpha \in \mathbb{Q}$ es un entero algebraico si y sólo si $\alpha \in \mathbb{Z}$.*

DEMOSTRACIÓN. Si $\alpha \in \mathbb{Q}$ es un entero algebraico, α satisface un polinomio mónico con coeficientes enteros, digamos $f(x) = b_0 + b_1 x + \cdots + x^n$, con $b_i \in \mathbb{Z}$. Sea $\alpha = \dfrac{c}{d}$, con $c, d \in \mathbb{Z}$ y $mcd(c, d) = 1$. Por tanto

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

Multiplicamos por d^n la ecuación anterior,

$$\begin{aligned} c^n &= -(b_0 d^n + b_1 c d^{n-1} + \cdots + b_{n-1} c^{n-1} d) \\ &= -d(b_0 d^{n-1} + b_1 c d^{n-2} + \cdots + b_{n-1} c^{n-1}) \end{aligned}$$

y tenemos $d \mid c^n$. Dado que $mcd(c, d) = 1$, se tiene $mcd(c^n, d) = 1$. Así, $d \mid 1$. Por lo tanto, $d = \pm 1$, es decir $\alpha \in \mathbb{Z}$.

Ahora si $\alpha \in \mathbb{Z}$, él satisface al polinomio $f(x) = x - \alpha \in \mathbb{Z}[x]$, se concluye que α es un entero algebraico. □

A partir de ahora, diremos que un elemento en $\mathbb{Z}$ es un entero racional para no confundirlos con los enteros algebraicos.

Proposición 1.21. *Sea $\alpha \in \mathcal{O}_F$. Entonces $N(\alpha)$, $tr(\alpha) \in \mathbb{Z}$.*

DEMOSTRACIÓN. Como $\alpha \in \mathcal{O}_F$, α satisface un polinomio mónico con coeficientes enteros $f(x) = a_0 + a_1 x + \cdots + x^n$, de donde $0 = a_0 + a_1\alpha + \cdots + \alpha^n$. Sea $\sigma \in \mathrm{Aut}(F/\mathbb{Q})$. Entonces

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

es decir, $\sigma(\alpha) \in \mathcal{O}_F$ y dado que $N(\alpha) = \prod_{\sigma \in \mathrm{Aut}(F/\mathbb{Q})} \sigma(\alpha)$ y $tr(\alpha) = \sum_{\sigma \in \mathrm{Aut}(F/\mathbb{Q})} \sigma(\alpha)$ tenemos $N(\alpha), tr(\alpha) \in \mathcal{O}_F$.

Por otro lado $N(\alpha), tr(\alpha) \in \mathbb{Q}$. Por lo tanto, por el lema anterior, $N(\alpha), tr(\alpha) \in \mathbb{Z}$. □

Corolario 1.22. *Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathcal{O}_F$ una base de F sobre $\mathbb{Q}$. Entonces,*

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$$

.

DEMOSTRACIÓN. Sabemos que $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(tr(\alpha_i\alpha_j))$ y por la propociión 1.21, $tr(\alpha_i\alpha_j) \in \mathbb{Z}$. Por lo tanto, $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$. □

Teorema 1.23. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_F$ y $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq I$ una base de $F/\mathbb{Q}$ de tal forma que $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ es mínimo. Entonces, $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\,\alpha_n$.*[1]

DEMOSTRACIÓN. Como $\alpha_i \in I$ e I es un ideal, $\mathbb{Z}\alpha_i \subseteq I$. Entonces, $I \supseteq \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$.

Inversamente, sea $\alpha \in I$ y como $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base, $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, con $a_i \in \mathbb{Q}$ para cada $i = 1, \ldots, n$. Probaremos que $a_i \in \mathbb{Z}$.

Supongamos que $a_i \notin \mathbb{Z}$ para algún $i = 1, \ldots, n$. Sin perdida de generalidad, supongamos que $a_1 \notin \mathbb{Z}$, es decir $a_1 = m + \theta$, donde $m \in \mathbb{Z}$ y $\theta \in (0, 1)$.

Sean $\beta_1 = \alpha - m\alpha_1, \beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n$. Como $m \in \mathcal{O}_F$ e I es un ideal de $\mathcal{O}_F$, tenemos $m\alpha_1 \in I$ y, por tanto, $\alpha - m\alpha_1 \in I$, es decir, $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\} \subseteq I$. Veremos que $\mathcal{B}$ es una base para $F/\mathbb{Q}$.

Supongamos que $0 = q_1\beta_1 + q_2\beta_2 + \cdots + q_n\beta_n$, con $q_i \in \mathbb{Q}$, para $i = 1, \ldots, n$. Así,

$$\begin{aligned} 0 &= q_1(\alpha - m\alpha_1) + q_2\alpha_2 + \cdots + q_n\alpha_n \\ &= q_1(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) - q_1 m\alpha_1 + q_2\alpha_2 + \cdots + q_n\alpha_n \\ &= (q_1a_1 - q_1m)\alpha_1 + (q_1a_2 + q_2)\alpha_2 + \cdots + (q_1a_n + q_n)\alpha_n \end{aligned}$$

y dado que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de $F/\mathbb{Q}$, tenemos $q_1a_1 - q_1m = 0$ y $q_1a_j + q_j = 0$ para $j = 2, \ldots, n$. Por tanto, $q_j = 0$ para cada $j = 1, \ldots, n$ y, como $[F : \mathbb{Q}] = n$, tenemos $\mathcal{B}$ es una base para $F/\mathbb{Q}$.

Por otro lado, la matriz cambio de base de $\{\beta_1, \beta_2, \ldots, \beta_n\}$ a $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es

$$A = \begin{pmatrix} \theta & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

[1] Notemos que $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\,\alpha_n$ es una suma directa, ya que $\{\alpha_1, \ldots, \alpha_n\}$ es una base.

Dado que $\det(A) = \theta$, por la proposición 1.7, $|\Delta(\beta_1, \beta_2, \ldots, \beta_n)| = \theta^2 |\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ y $\theta \in (0, 1)$. De lo anterior,

$$|\Delta(\beta_1, \beta_2, \ldots, \beta_n)| < |\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|,$$

lo cual es una contradicción al hecho de que $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ es mínimo. Entonces, tenemos $a_i \in \mathbb{Z}$ para $i = 1, \ldots, n$. Así, $I \subseteq \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. Por lo tanto, $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. □

Definición 1.24. *Si $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq I$ es una base de $F/\mathbb{Q}$ tal que $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ es mínimo, entonces llamaremos a $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una* **base entera** *de I.*

Observemos que $\mathcal{O}_F$ es un ideal de sí mismo, por lo tanto $\mathcal{O}_F$ contiene una base entera, la cual se llama **base entera de** $F/\mathbb{Q}$.

Proposición 1.25. *Sea $\{\alpha_1, \ldots, \alpha_n\} \subseteq I$ una $\mathbb{Q}$-base de F tal que $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de I.*

DEMOSTRACIÓN. Sea $\{\beta_1, \ldots, \beta_n\} \subseteq I$ una $\mathbb{Q}$-base cualquiera de F. Veremos que $|\Delta(\alpha_1, \ldots, \alpha_n)| \leq |\Delta(\beta_1, \ldots, \beta_n)|$.

Notemos que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, con $a_{ij} \in \mathbb{Z}$, entonces

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

y como $a_{ij} \in \mathbb{Z}$, tenemos $\det(a_{ij}) \geq 1$. Así, $\Delta(\beta_1, \ldots, \beta_n) \geq \Delta(\alpha_1, \ldots, \alpha_n)$ y por tanto $|\Delta(\alpha_1, \ldots, \alpha_n)| \leq |\Delta(\beta_1, \ldots, \beta_n)|$. □

Con el teorema 1.23 y la proposición anterior tenemos que $\{\alpha_1, \ldots, \alpha_n\} \subseteq I$ es base entera de I si y sólo si $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

Corolario 1.26. *Sean $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$,$\{\beta_1, \beta_2, \ldots, \beta_n\}$ dos bases enteras de $F/\mathbb{Q}$. Entonces $\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

DEMOSTRACIÓN. Sean $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, con $a_{ij} \in \mathbb{Z}$, $\beta_j = \sum_{k=1}^{n} b_{jk}\alpha_k$, con $b_{jk} \in \mathbb{Z}$ y (a_{ij}) y (b_{jk}) las matrices con entradas los coeficientes obtenidos anteriormente. Por la proposición 1.7,

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) = (\det(a_{ij}))^2 \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Es fácil ver que $\det((a_{ij})(b_{jk})) = 1$, de donde $\det(a_{ij}) = \pm 1$. Por lo tanto

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

□

Definición 1.27. *El* **discriminante** *de $\mathcal{O}_F$ es el discrimininante de una base entera de $F/\mathbb{Q}$ y se denota por δ_F.*

Lema 1.28. *Sea $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Q}$-base de F formada por enteros algebraicos y $d = \Delta(\alpha_1, \ldots, \alpha_n)$. Entonces cada entero algebraico $\alpha \in \mathcal{O}_F$ se puede expresar de la forma*

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d},$$

donde los $m_i \in \mathbb{Z}$ y $d|m_i^2$.

DEMOSTRACIÓN. Si $\alpha \in \mathcal{O}_F$, existen $a_1, \ldots, a_n \in \mathbb{Q}$ tales que $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$. Si $\sigma_1, \ldots, \sigma_n$ son los monomorfismos de F en $\mathbb{C}$, se tiene el sistema de ecuaciones lineales

$$\begin{aligned} \sigma_1(\alpha) &= a_1\sigma_1(\alpha_1) + \cdots + a_n\sigma_1(\alpha_n) \\ &\vdots \\ \sigma_n(\alpha) &= a_1\sigma_n(\alpha_1) + \cdots + a_n\sigma_n(\alpha_n) \end{aligned}$$

que puede ser resuelto usando la regla de Cramer, esto da lugar a

$$a_j = \frac{\gamma_j}{\Delta} \quad \text{para} \quad j = 1, \ldots, n$$

donde Δ es el determinante de la matriz $(\sigma_j(\alpha_i))$ y γ_j es el determinante de esa matriz cambiando la j-ésima columna por el vector columna $(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))^T$, por lo que γ_j y Δ son enteros algebraicos y $\Delta^2 = d$. Como $\Delta^2 = d \in \mathbb{Z}$, $da_j = \Delta\gamma_j \in \mathbb{Z}$, por lo que $m_j = da_j \in \mathbb{Z}$. Notemos que $\dfrac{m_j^2}{d} = \dfrac{(\Delta\gamma_j)^2}{d} = \gamma_j^2 \in \mathcal{O}_F \cap \mathbb{Q} = \mathbb{Z}$. Por tanto, $d|m_j^2$. □

Con este lema hemos mostrado que si $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Q}$-base de F formada por enteros algebraicos, entonces

$$\mathcal{O}_F \subseteq \mathbb{Z}\frac{\alpha_1}{d} \oplus \mathbb{Z}\frac{\alpha_2}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}$$

Lema 1.29. *Sean $F = \mathbb{Q}(\alpha)$ con $[F : \mathbb{Q}] = n$, $f(x)$ y $g(x)$ dos polinomios de grado menor que n tales que $f(\alpha) = g(\alpha)$. Entonces $f(x) = g(x)$.*

DEMOSTRACIÓN. Supongamos que $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ y $g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$, no necesariamente del mismo grado. Por hipótesis tenemos

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

se sigue

$$(a_0 - b_0) + (a_1 - b_1)\alpha + \cdots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0.$$

Como $F = \mathbb{Q}(\alpha)$, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de F como $\mathbb{Q}$-espacio vectorial, en particular es linealmente independiente, es decir, $(a_0 - b_0) = (a_1 - b_1) = \cdots = (a_{n-1} - b_{n-1}) = 0$. Por lo tanto $f(x) = g(x)$. □

Teorema 1.30 (Teorema de la base entera especial)**.** *Sea $F = \mathbb{Q}(\alpha)$ una extensión de grado n sobre $\mathbb{Q}$. Si α es entero algebraico, entonces existe una base entera de F de la forma*

$$\left\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right\},$$

donde $d_i \in \mathbb{Z}$ con $d_1|d_2|\cdots|d_{n-1}$ y f_i es un polinomio mónico de grado i con coeficientes enteros.

DEMOSTRACIÓN. Por las hipótesis del enunciado, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una $\mathbb{Q}$-base de F. Por el lema 1.28, si $d = \Delta(1, \alpha, \ldots, \alpha^{n-1})$ se tiene que

$$\mathcal{O}_F \subseteq \mathbb{Z}\frac{1}{d} \oplus \mathbb{Z}\frac{\alpha}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha^{n-1}}{d}.$$

Para cada $1 \leq i \leq n$, sea $K_i = \mathbb{Z}\frac{1}{d} \oplus \mathbb{Z}\frac{\alpha}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha^{i-1}}{d} \cong \mathbb{Z}^i$ y $R_i = \mathcal{O}_F \cap K_i$. Entonces

$$R_1 = K_1 \cap \mathcal{O}_F = \mathbb{Z}\frac{1}{d} \cap \mathcal{O}_F \subseteq \mathbb{Q} \cap \mathcal{O}_F = \mathbb{Z} \subseteq R_1,$$

es decir $R_1 = \mathbb{Z}$. Ademas, como

$$\mathcal{O}_F \subseteq \mathbb{Z}\frac{1}{d} \oplus \mathbb{Z}\frac{\alpha}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha^{n-1}}{d},$$

$R_n = \mathcal{O}_F \cap K_n = \mathcal{O}_F$.

Obtendremos la existencia de la base por inducción sobre i. Para $i = 1$ basta tomar la base $\{1\}$.

Supongamos ahora que $i < n$ y que R_i tiene una base de la forma indicada, donde los d_i están en $\mathbb{Z}$ con $d_1|d_2| \cdots |d_{i-1}$ y los f_i son polinomios mónicos de grado i. Sea

$$\pi : K_{i+1} = K_i \oplus \mathbb{Z}\frac{\alpha^i}{d} \longrightarrow \mathbb{Z}\frac{\alpha^i}{d}$$

la proyección canónica. Notemos que

$$\pi(R_{i+1}) \subseteq \mathbb{Z}\frac{\alpha^i}{d}$$

y $\pi(R_{i+1}) \neq 0$, pues contiene a α^i. Por lo tanto, es un grupo abeliano libre de rango 1 y existe $\beta \in R_{i+1}$ tal que $\pi(R_{i+1}) = \mathbb{Z}\pi(\beta)$. Con estas condiciones, vamos a demostrar que

$$\mathcal{B}_{i+1} = \left\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{i-1}(\alpha)}{d_{i-1}}, \beta\right\}$$

es una $\mathbb{Z}$-base de R_{i+1}.

Sea $\gamma \in R_{i+1}$. Sabemos que $\pi(\gamma) = m\pi(\beta)$ con $m \in \mathbb{Z}$, de donde

$$\gamma - m\beta \in \mathrm{Ker}(\pi) \cap \mathcal{O}_F = K_i \cap \mathcal{O}_F = R_i$$

y, por hipótesis de inducción,

$$\gamma - m\beta = m_0 1 + m_1\frac{f_1(\alpha)}{d_1} + \cdots + m_{i-1}\frac{f_{i-1}(\alpha)}{d_{i-1}},$$

es decir

$$\gamma = m_0 1 + m_1\frac{f_1(\alpha)}{d_1} + \cdots + m_{i-1}\frac{f_{i-1}(\alpha)}{d_{i-1}} + m\beta.$$

Por lo anterior, $\mathcal{B}_{i+1}$ genera a R_{i+1}. Además, $\mathcal{B}_{i+1}$ es linealmente independiente, pues si

$$m_0 1 + m_1\frac{f_1(\alpha)}{d_1} + \cdots + m_{i-1}\frac{f_{i-1}(\alpha)}{d_{i-1}} + m\beta = 0$$

con $m_0, m_1, \ldots, m_{i-1}, m \in \mathbb{Z}$, entonces $0 = \pi(m\beta) = m\pi(\beta)$, de donde $m = 0$ y, por hipótesis de inducción, $m_1 = m_2 = \cdots = m_{i-1} = 0$.

A continuación veremos que β se puede tomar de la forma deseada. Como $\alpha \in \mathcal{O}_F$ y $\dfrac{f_{i-1}(\alpha)}{d_{i-1}} \in R_i$ tenemos

$$\alpha\frac{f_{i-1}(\alpha)}{d_{i-1}} \in \mathcal{O}_F \cap \left(\mathbb{Z}\frac{\alpha}{d} \oplus \mathbb{Z}\frac{\alpha^2}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha^i}{d}\right) \subseteq \mathcal{O}_F \cap K_{i+1} = R_{i+1}.$$

Más concretamente, si

$$f_{i-1}(\alpha) = a_0 + a_1\alpha + \cdots + a_{i-2}\alpha^{i-2} + \alpha^{i-1},$$

se tiene

$$\pi\left(\alpha\frac{f_{i-1}(\alpha)}{d_{i-1}}\right) = \frac{1}{d_{i-1}}\alpha^i$$

y, por lo tanto, existe $m \in \mathbb{Z}$ tal que

$$\frac{1}{d_{i-1}}\alpha^i = m\pi(\beta),$$

de donde

$$\pi(\beta) = \frac{\alpha^i}{d_i} \quad \text{con} \quad d_i = md_{i-1}.$$

Si

$$\beta = \frac{1}{d}\left(b_0 + b_1\alpha + \cdots + b_{i-1}\alpha^{i-1} + b_i\alpha^i\right),$$

entonces $\dfrac{b_i}{d} = \dfrac{1}{d_i}$, $b_i d_i = d$ y

$$\beta = \frac{1}{d_i}\left(\frac{b_0}{b_i} + \frac{b_1}{b_i}\alpha + \cdots + \frac{b_{i-1}}{b_i}\alpha^{i-1} + \alpha^i\right) = \frac{f_i(\alpha)}{d_i}$$

con

$$f_i(x) = \frac{b_0}{b_i} + \frac{b_1}{b_i}x + \cdots + \frac{b_{i-1}}{b_i}x^{i-1} + x^i \in \mathbb{Q}[x]$$

mónico de grado i. Por tanto

$$d\frac{f_i(\alpha)}{d_i} = d\beta = b_0 + b_1\alpha + \cdots + b_{i-1}\alpha^{i-1} + b_i\alpha^i$$

y

$$\frac{f_i(\alpha)}{d_{i-1}} = \frac{mf_i(\alpha)}{md_{i-1}} = \frac{mf_i(\alpha)}{d_i} = m\beta \in \mathcal{O}_F.$$

Definamos

$$\gamma = \frac{f_i(\alpha)}{d_{i-1}} - \frac{\alpha f_{i-1}(\alpha)}{d_{i-1}} \in \mathcal{O}_F.$$

$$\pi(\gamma) = \pi\left(\frac{f_i(\alpha)}{d_{i-1}}\right) - \pi\left(\frac{\alpha f_{i-1}(\alpha)}{d_{i-1}}\right) = \pi(m\beta) - m\pi(\beta) = 0,$$

por lo que $\gamma \in \mathcal{O}_F \cap K_i = R_i$. Por consiguiente, existen $a_0, a_1, \ldots, a_{i-1} \in \mathbb{Z}$ tales que

$$\gamma = a_0 1 + a_1\frac{f_1(\alpha)}{d_1} + \cdots + a_{i-1}\frac{f_{i-1}(\alpha)}{d_{i-1}} = \frac{g(\alpha)}{d_{i-1}}$$

con $g(x) \in \mathbb{Z}[x]$ y $gr(g(x)) < i$, de donde $\dfrac{f_i(\alpha) - \alpha f_{i-1}(\alpha)}{d_{i-1}} = \dfrac{g(\alpha)}{d_{i-1}}$ y también $f_i(\alpha) - \alpha f_{i-1}(\alpha) = g(\alpha)$. Por el lema anterior,

$$f_i(x) - x f_{i-1}(x) = g(x),$$

así

$$f_i(x) = g(x) + x f_{i-1}(x) \in \mathbb{Z}[x]$$

Por lo tanto se tiene la base deseada para R_{i+1}. □

Del teorema anterior tenemos algunas observaciones:

- $\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \Delta(1, f_1(\alpha), \ldots, f_{n-1}(\alpha)) = (d_1 \cdots d_{n-1})^2 \delta_F$.
- Si $i + j < n$ con $i, j \in \{1, \ldots, n-2\}$, entonces $d_i d_j | d_{i+j}$.
- Teniendo en cuenta los dos puntos anteriores si $i < n$, entonces $d_1^i | d_i$ y también $d_1^{n(n-1)} | \Delta(1, \alpha, \ldots, \alpha^{n-1})$.
- Los polinomios f_i del teorema anterior pueden ser sustituidos por cualquier otro polinomio mónico $g_i(x) \in \mathbb{Z}[x]$, tales que, $gr(g_i) = i$ y $g_i(\alpha)/d_i \in \mathcal{O}_F$ para cada $i = 1, \ldots, n-1$. Es decir $\left\{1, \dfrac{g_1(\alpha)}{d_1}, \ldots, \dfrac{g_{n-1}(\alpha)}{d_{n-1}}\right\}$ es una base entera de $\mathcal{O}_F$.

Lema 1.31. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_F$. Entonces $I \cap \mathbb{Z} \neq \{0\}$.*

DEMOSTRACIÓN. Si $\alpha \in I \neq \{0\}$, α satisface un polinomio $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ irreducible, luego $a_0 \neq 0$ y así

$$0 = f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n,$$

$$a_0 = -(a_1\alpha + \cdots + a_n\alpha^n) \in I.$$

Por lo tanto, $a_0 \in I \cap \mathbb{Z}$. □

Lema 1.32. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_F$, con $[F : \mathbb{Q}] = n$. Entonces $|\mathcal{O}_F/I|$ es finito.*

DEMOSTRACIÓN. Por el lema 1.31 existe $a \in I \cap \mathbb{Z}$, con $a > 0$. Sea $\langle a \rangle$ el ideal principal generado por a en $\mathcal{O}_F$, es decir $a\mathcal{O}_F = \langle a \rangle$. Definimos

$$\varphi : \mathcal{O}_F/\langle a \rangle \longrightarrow \mathcal{O}_F/I$$
$$x + \langle a \rangle \mapsto x + I.$$

La función φ está bien definida pues si $x_1 + \langle a \rangle = x_2 + \langle a \rangle$, entonces $x_1 - x_2 \in \langle a \rangle \subseteq I$ y por tanto $x_1 + I = x_2 + I$, es decir $\varphi(x_1 + \langle a \rangle) = \varphi(x_2 + \langle a \rangle)$. Además es claro que φ es una función sobre, por lo que $|\mathcal{O}_F/I| \leq |\mathcal{O}_F/\langle a \rangle|$, así que para probar que $\mathcal{O}_F/I$ es finito basta probar que $\mathcal{O}_F/\langle a \rangle$ lo es.

Sean $\{\omega_1, \ldots, \omega_n\}$ una base entera de $F/\mathbb{Q}$, es decir $\mathcal{O}_F = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$, con $\omega_i \in \mathcal{O}_F$ y

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

Observemos que S es un conjunto de representantes de $\mathcal{O}_F/\langle a\rangle$ y que $|S| = a^n$. Tomemos $\omega \in \mathcal{O}_F$, $\omega = m_1\omega_1 + \cdots + m_n\omega_n$, con $m_i \in \mathbb{Z}$ para $i = 1, \ldots, n$. Por el algoritmo de la división en $\mathbb{Z}$, $m_i = q_i a + \gamma_i$, con $0 \leq \gamma_i < a$.

$$\begin{aligned}\omega + \langle a\rangle &= (m_1\omega_1 + \cdots + m_n\omega_n) + \langle a\rangle \\ &= (m_1\omega_1 + \langle a\rangle) + \cdots + (m_n\omega_n + \langle a\rangle) \\ &= ((q_1a + \gamma_1)\omega_1 + \langle a\rangle) + \cdots + ((q_na + \gamma_n)\omega_n + \langle a\rangle).\end{aligned}$$

Como $(q_ia + \gamma_i)\omega_i + \langle a\rangle = q_ia\omega_i + \gamma_i\omega_i + \langle a\rangle = \gamma_i\omega_i + \langle a\rangle$, tenemos

$$\omega + \langle a\rangle = (\gamma_1\omega_1 + \langle a\rangle) + \cdots + (\gamma_n\omega_n + \langle a\rangle) = \sum_{i=1}^{n} \gamma_i\omega_i + \langle a\rangle$$

y $\displaystyle\sum_{i=1}^{n} \gamma_i\omega_i \in S$.

Por otro lado, si $\displaystyle\sum_{i=1}^{n} \gamma_i\omega_i = \sum_{i=1}^{n} \gamma_i'\omega_i$, con $0 \leq \gamma_i < a$ y $0 \leq \gamma_i' < a$, se cumple $\gamma_i = \gamma_i'$ ya que $\{\omega_1, \ldots, \omega_n\}$ es una base. Por tanto, $|S| = a^n$ y $|\mathcal{O}_F/\langle a\rangle| = |S|$. Así, $|\mathcal{O}_F/I| \leq a^n$. □

Observemos que si $P \neq \{0\}$ es un ideal primo de $\mathcal{O}_F$, entonces $P \cap \mathbb{Z} = p\mathbb{Z}$, con p un primo racional.

Definición 1.33. *Sea I un ideal no cero de $\mathcal{O}_F$. La* **norma** *de I es $|\mathcal{O}_F/I|$ y la denotaremos por $N(I)$.*

Teorema 1.34. *Sea I un ideal no cero de $\mathcal{O}_F$. Entonces $N(I) = \sqrt{\dfrac{\Delta(\beta_1, \ldots, \beta_n)}{\delta_F}}$, donde $\{\beta_1, \ldots, \beta_n\}$ es una base entera de I.*

DEMOSTRACIÓN. Ver [**17**] pág. 114, teorema 5.9. □

Proposición 1.35. *Sean I, J ideales no cero de $\mathcal{O}_F$. Entonces*

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

DEMOSTRACIÓN. Ver [**17**] pág. 116, teorema 5.12. □

Corolario 1.36. *$\mathcal{O}_F$ es un anillo noetheriano.*

DEMOSTRACIÓN. Sea $I_1 \neq \{0\}$ un ideal de $\mathcal{O}_F$, por el lema 1.32, $\mathcal{O}_F/I_1$ es finito. Consideremos $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ una cadena ascendente de ideales en $\mathcal{O}_F$. Como I_j/I_1 es un ideal de $\mathcal{O}_F/I_1$ y a lo más hay un número finito de subconjuntos de éste, la cadena $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n = I_{n+1} = \cdots$ se detiene en algún $n \in \mathbb{Z}$. Por lo tanto, $\mathcal{O}_F$ es noetheriano. □

Corolario 1.37. *Si $P \neq \{0\}$ es un ideal primo de $\mathcal{O}_F$, entonces P es máximo.*

DEMOSTRACIÓN. Como P es primo, entonces $\mathcal{O}_F/P$ es un dominio entero finito, de donde $\mathcal{O}_F/P$ es un campo y por tanto P es un ideal máximo. □

Corolario 1.38. *La factorización en irreducibles es posible en $\mathcal{O}_F$.*

DEMOSTRACIÓN. Sea $x \in \mathcal{O}_F$, con $x \neq 0$ y no unidad. Supongamos que x no tiene una expresión como producto finito de irreducibles.

Sean $X = \{x \in \mathcal{O}_F : x \text{ no es unidad}, x \neq 0 \text{ y no es producto finito de irreducibles}\}$ y $A = \{\langle x\rangle \subseteq \mathcal{O}_F : x \in X\}$. Entonces, por el corolario 1.36, A tiene elementos maximales, digamos $\langle x\rangle$ es maximal. Puesto que x no es irreducible, se tiene $x = yz$, donde y, z no son unidades. Por tanto, $\langle x\rangle \subsetneq \langle y\rangle$ y $\langle x\rangle \subsetneq \langle z\rangle$. Por la maximalidad de $\langle x\rangle$, se tiene que $y = p_1 \cdots p_n$ y $z = q_1 \cdots q_m$, donde p_i, q_i son irreducibles. Así, x tiene una expresión como producto finito de irreducibles, lo cual es una contradicción a nuestra suposición. □

Lema 1.39. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_F$. Si $\beta \in F$, con $\beta \neq 0$ es tal que $\beta I \subseteq I$, entonces $\beta \in \mathcal{O}_F$.*

DEMOSTRACIÓN. Como I es un $\mathbb{Z}$-módulo, por la proposición 1.12, $\beta \in \mathcal{O}_F$. □

Lema 1.40. *Sean I, J ideales no cero de $\mathcal{O}_F$ tales que $IJ = I$. Entonces $J = \mathcal{O}_F$.*

DEMOSTRACIÓN. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de I, es decir, $I = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$. Dado que $\alpha_i \in I = IJ$, existen $b_{ij} \in J$ tales que $\alpha_i = \sum_{i=1}^{n} b_{ij}\alpha_j$. Entonces

$$\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ n_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

de donde

$$\begin{pmatrix} b_{11} - 1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} - 1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ n_{n1} & b_{n2} & \cdots & b_{nn} - 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

es decir, tenemos el siguiente sistema homogéneo

$$\begin{aligned} 0 &= (b_{11} - 1)x_1 + b_{12}x_2 + \cdots + b_{1n}x_n \\ 0 &= b_{21}x_1 + (b_{22} - 1)x_2 + \cdots + b_{2n}x_n \\ &\vdots \\ 0 &= b_{n1}x_1 + b_{n2}x_2 + \cdots + (b_{nn} - 1)x_n, \end{aligned}$$

el cual tiene una solución no trivial, por lo que

$$\det \begin{pmatrix} b_{11}-1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22}-1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ n_{n1} & b_{n2} & \cdots & b_{nn}-1 \end{pmatrix} = 0.$$

Entonces,

$$(b_{11}-1)|\cdot|_{n-1} - b_{12}|\cdot|_{n-1} + \cdots + (-1)^{n+1}b_{1n}|\cdot|_{n-1} = 0$$

con $r_1 = -b_{12}|\cdot|_{n-1} + \cdots + (-1)^{n+1}b_{1n}|\cdot|_{n-1} \in J$ pues $b_{ij} \in J$. Luego

$$(b_{11}-1)\left[(b_{22}-1)\cdot\det\begin{pmatrix} b_{33}-1 & \cdots & b_{3n} \\ \vdots & \ddots & \vdots \\ n_{n3} & \cdots & b_{nn}-1 \end{pmatrix}\right] + r_1 = 0.$$

Así,

$$\prod_{i=1}^{n}(b_{ii}-1) + r = 0 \quad \text{para algún } r \in J$$

y desarrollando el producto

$$(-1)^n + j = 0 \quad \text{para algún } j \in J,$$

de donde $\pm 1 = j \in J$. Por lo tanto, $J = \mathcal{O}_F$. □

Proposición 1.41. *Sean I, J ideales no cero de $\mathcal{O}_F$ y $\gamma \in \mathcal{O}_F$ tales que se cumple $\langle\gamma\rangle I = JI$. Entonces, $J = \langle\gamma\rangle$.*

DEMOSTRACIÓN. Sean $\alpha \in I$ y $\beta \in J$. Entonces $\alpha\beta \in IJ = \langle\gamma\rangle I$, de donde $\alpha\beta = \gamma\alpha'$, con $\alpha' \in I$. Se tiene $\alpha\dfrac{\beta}{\gamma} = \alpha' \in I$ y $\dfrac{\beta}{\gamma}I \subseteq I$. Por el lema 1.12, $\dfrac{\beta}{\gamma} \in \mathcal{O}_F$, lo que implica $\beta \in \gamma\mathcal{O}_F$. Así, $J \subseteq \gamma\mathcal{O}_F$ y $\gamma^{-1}J$ es un ideal de $\mathcal{O}_F$. Dado que $\gamma I = JI$, $I = (\gamma^{-1}J)I$. Usando el lema anterior, $\gamma^{-1}J = \mathcal{O}_F$ y $J = \gamma\mathcal{O}_F = \langle\gamma\rangle$. □

1.3. El grupo de clases y el número de clases

En la sección anterior vimos qué es el anillo de enteros de un campo de números. En esta sección introduciremos una relación de equivalencia, la cual implicará una partición del anillo de enteros, esta partición da lugar a otro concepto muy importante que es el número de clases.

Definición 1.42. *Un* **ideal fraccionario** *de F es un $\mathcal{O}_F$-submódulo no nulo I de F tal que existe algún elemento no cero $\alpha \in \mathcal{O}_F$ tal que $\alpha I \subseteq \mathcal{O}_F$. En otras palabras los ideales fraccionarios son subconjuntos de F de la forma $\alpha^{-1}J$, donde J es un ideal no nulo de $\mathcal{O}_F$ y α es un elemento no cero de $\mathcal{O}_F$.*

Notemos que todos los ideales de $\mathcal{O}_F$ son ideales fraccionarios, tomando $\alpha = 1$. Recíprocamente, un ideal fraccionario I es un ideal si y sólo si $I \subseteq \mathcal{O}_F$.

Denotaremos por $\mathcal{J}_F$ al conjunto de todos los ideales fraccionarios.

Proposición 1.43. *($\mathcal{J}_F$, $\cdot$) es un grupo abeliano. La identidad es $\langle 1\rangle = \mathcal{O}_F$ y el inverso de I es $I^{-1} = \{\alpha \in F : \alpha I \subseteq \mathcal{O}_F\}$.*

DEMOSTRACIÓN. Ver [**12**], pág. 21, proposición 3.8. □

Denotaremos $\mathcal{P}_F$ al subgrupo de $\mathcal{J}_F$ formado por los ideales fraccionarios principales.

Definición 1.44. *El* **grupo de clases** *de ideales de $\mathcal{O}_F$ es el grupo cociente $Cl_F = \mathcal{J}_F/\mathcal{P}_F$. Se define el* **número de clases** *como $h_F = |Cl_F|$.*

Diremos que dos ideales fraccionarios I, J son **equivalentes** si pertenecen al mismo conjunto $\mathcal{P}_F$ de $\mathcal{J}_F$ y escribimos $I \sim J$.

Denotaremos por $[I]$ a la clase de equivalencia de I. El grupo Cl_F es el conjunto de estas clases de equivalencia.

Notemos que si I es un ideal fraccionario, ya sabemos que $I = \alpha^{-1}J$, donde $\alpha \in \mathcal{O}_F$ y J es un ideal de $\mathcal{O}_F$, entonces $J = \alpha I = \langle\alpha\rangle I$ y como $\langle\alpha\rangle \in \mathcal{P}_F$, tenemos $I \sim J$, es decir, toda clase de equivalencia tiene como representante un ideal.

Ahora sean I, J ideales equivalentes. Entonces $I = LJ$ donde L es un ideal fraccionario principal, digamos que $L = \beta^{-1}K$ para $\beta \in \mathcal{O}_F$ y K un ideal principal. Por lo tanto $\langle\beta\rangle I = KJ$.

Inversamente si $LI = KJ$ para L, K ideales principales, entonces $I \sim J$.

Esto nos permite describir a Cl_F como sigue: si I, J son ideales no cero de $\mathcal{O}_F$, entonces I es equivalente a J ($I \sim J$) si y sólo si existen elementos no cero $\alpha, \beta \in \mathcal{O}_F$ tales que $\langle\alpha\rangle I = \langle\beta\rangle J$.

El lector interesado en los ideales fraccionarios puede consultar [**12**] y [**17**].

Proposición 1.45. *$\sim$ es de equivalencia.*

DEMOSTRACIÓN.

(i) Reflexiva.
$I \sim I$ pues $\langle 1\rangle I = \langle 1\rangle I$.

(ii) Simétrica.
Si $I \sim J$, entonces existen $\alpha, \beta \in \mathcal{O}_F$ distintos de cero tales que $\langle\alpha\rangle I = \langle\beta\rangle J$ y por tanto $J \sim I$.

(iii) Transitiva.
Si $I \sim J$ y $J \sim K$, podemos encontrar $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{O}_F$ distintos de cero tales que $\langle\alpha_1\rangle I = \langle\beta_1\rangle J$ y $\langle\alpha_2\rangle J = \langle\beta_2\rangle K$, por tanto $\langle\alpha_2\rangle\langle\alpha_1\rangle I = \langle\alpha_2\rangle\langle\beta_1\rangle J$ y $\langle\alpha_2\rangle\langle\beta_1\rangle J = \langle\beta_2\rangle\langle\beta_1\rangle K$. Así, $\langle\alpha_2\rangle\langle\alpha_1\rangle I = \langle\beta_2\rangle\langle\beta_1\rangle K$, es decir $I \sim K$. □

Notemos que si $I = \langle\alpha\rangle$ y $J = \langle\beta\rangle$ son ideales principales, entonces $I \sim J$. De esta forma existe una clase que contiene a todos los ideales principales. En particular como $\mathcal{O}_F = \langle 1\rangle$, $\mathcal{O}_F \sim \langle\alpha\rangle$, es decir $[\mathcal{O}_F] = [\langle\alpha\rangle]$. En otras palabras, $\mathcal{O}_F$ es un representante de la clase de los ideales principales.

Lema 1.46. *Existe un entero positivo M que depende únicamente del campo F, tal que para todo $\gamma \in F$ se tiene $|N(t\gamma - \omega)| < 1$ para algún entero $1 \leq t \leq$M y algún $\omega \in \mathcal{O}_F$.*

DEMOSTRACIÓN. Ver [**7**], página 178, lema 5. □

Lema 1.47. *(Hurwitz) Sea F un campo de números de grado n. Existe un entero M tal que dados $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$, existen $1 \leq t \leq M$ y $\omega \in \mathcal{O}_F$ que satisfacen*

$$|N(t\alpha - \omega\beta)| < |N(\beta)|.$$

DEMOSTRACIÓN. Sea $\gamma = \dfrac{\alpha}{\beta} \in F$. Por el lema anterior existe un entero positivo M tal que $|N(t\gamma - \omega)| < 1$ para algún entero $1 \leq t \leq M$ y algún $\omega \in \mathcal{O}_F$. Por tanto,

$$\begin{aligned} |N(t\gamma - \omega)| &= \left|N\left(t\frac{\alpha}{\beta} - \omega\right)\right| = \left|N\left(\frac{t\alpha - \beta\omega}{\beta}\right)\right| \\ &= |N(\beta^{-1})N(t\alpha - \beta\omega)| < 1 \end{aligned}$$

Como $\beta \neq 0$, se tiene $N(\beta) \neq 0$ y $|N(t\alpha - \omega\beta)| < |N(\beta)|$. □

Teorema 1.48. *El número de clases es finito.*

DEMOSTRACIÓN. Tomamos I un ideal no cero de $\mathcal{O}_F$. Si $\alpha \in I$ sabemos que $N(\alpha) \in \mathbb{Z}$. Sea $\beta \in I$, $\beta \neq 0$, tal que $|\beta|$ es mínimo. Para $\alpha \in I$, por el lema de Hurwitz, existen $1 \leq t \leq M$ y $\omega \in \mathcal{O}_F$ con $|N(t\alpha - \omega\beta)| < |N(\beta)|$. Como $\alpha, \beta \in I$, entonces $t\alpha - \omega\beta \in I$. Pero $|N(\beta)|$ es mínimo, de donde $N(t\alpha - \omega\beta) = 0$, por tanto, $t\alpha = \omega\beta$.

Por otro lado como $t \leq M$ se tiene que $t|M!$ y $\dfrac{M!}{t}\omega\beta \in \langle\beta\rangle$ y también $\dfrac{M!}{t}t\alpha \in \langle\beta\rangle$, es decir $M!\alpha \in \langle\beta\rangle$ y $M!I \subsetneq \langle\beta\rangle$.

Si $J = \dfrac{1}{\beta}M!I$ tenemos J es un ideal de $\mathcal{O}_F$. Notemos que

$$\langle\beta\rangle J = \beta\mathcal{O}_F J = M!I = \langle M!\rangle I, \tag{3}$$

de ahí $J \sim I$. Como $\beta \in I$, $M!\beta \in M!I = \langle\beta\rangle J$, entonces $M!\beta = \beta\displaystyle\sum_{i=1}^{n}\gamma_i j_i$, para algunos $\gamma_i \in \mathcal{O}_F$ y $j_i \in J$. Luego $M! = \displaystyle\sum_{i=1}^{n}\gamma_i j_i \in J$ de donde $M!\mathcal{O}_F \subseteq J$. Así

$$J/M!\mathcal{O}_F \leq \mathcal{O}_F/M!\mathcal{O}_F \quad \text{(como grupos)}.$$

Dado que $|\mathcal{O}_F/M!\mathcal{O}_F|$ es finito, hay un número finito de subgrupos en $\mathcal{O}_F/M!\mathcal{O}_F$, es decir hay un número finito de subgrupos de $\mathcal{O}_F$ que contienen a $M!\mathcal{O}_F$.

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

Proposición 1.49. *Si I es un ideal no cero de $\mathcal{O}_F$, entonces existe un entero k, $1 \leq k \leq h_F$ tal que I^k es principal.*

DEMOSTRACIÓN. Si $A = \{I, I^2, \ldots, I^{h_F+1}\}$, por el principio del palomar existe $i < j$ tal que $I^i \sim I^j$, es decir existen $\alpha, \beta \in \mathcal{O}_F\backslash\{0\}$ tales que $\alpha I^i = \beta I^j$.

Demostraremos que si $k = j - i$, entonces I^k es principal. Como $\dfrac{\alpha}{\beta}I^i = I^j = I^{j-i}I^i \subseteq I^i$, se cumple $\dfrac{\alpha}{\beta} \in \mathcal{O}_F$ y así $\left\langle\dfrac{\alpha}{\beta}\right\rangle = I^{j-i} = I^k$. Por lo tanto I^k es principal. □

En Cl_F definimos una operación producto como $[I] \cdot [J] = [IJ]$.

Proposición 1.50. *El producto entre clases de ideales está bien definido.*

DEMOSTRACIÓN. Sean $[I], [J] \in Cl_F$ y supongamos que $[I] = [I']$ y $[J] = [J']$, entonces $\langle\alpha\rangle I = \langle\alpha'\rangle I'$ y $\langle\beta\rangle J = \langle\beta'\rangle J'$ para algunos $\alpha, \alpha', \beta, \beta' \in \mathcal{O}_F \setminus \{0\}$. De lo anterior tenemos $(\langle\alpha\rangle\langle\beta\rangle)IJ = (\langle\alpha\rangle I)(\langle\beta\rangle J) = (\langle\alpha'\rangle\langle\beta'\rangle)I'J'$. Por tanto, $[I] \cdot [J] = [I'] \cdot [J']$. □

Teorema 1.51. $(Cl_F, \cdot)$ *es un grupo abeliano.*

DEMOSTRACIÓN. Se sigue de las propiedades del producto de ideales. □

La siguiente proposición es muy importante, pues nos da información de cuándo $\mathcal{O}_F$ es un anillo de factorización única.

Proposición 1.52. $h_F = 1$ *si y sólo si* $\mathcal{O}_F$ *es un dominio de ideales principales.*

DEMOSTRACIÓN. Supongamos que $h_F = 1$ y sea I un ideal no cero de $\mathcal{O}_F$, por tanto $I \sim \mathcal{O}_F$, es decir existen $\alpha, \beta \in \mathcal{O}_F \setminus \{0\}$ distintos tales que $\langle\alpha\rangle I = \langle\beta\rangle\mathcal{O}_F = \langle\beta\rangle$. Entonces $\beta = \alpha \sum_{i=0}^{n} \alpha_i' a_i$ con $\alpha_i' \in \mathcal{O}_F$ y $a_i \in I$, por tanto α divide a β en $\mathcal{O}_F$. De lo anterior, $\dfrac{\beta}{\alpha} = \sum_{i=0}^{n} \alpha_i' a_i \in I$. Así que, para $\gamma \in I$ tenemos $\gamma\dfrac{\beta}{\alpha} \in I$ y $\left\langle \dfrac{\beta}{\alpha} \right\rangle \subseteq I$. Ahora si $a \in I$, entonces $\alpha a = \beta r$ para algún $r \in \mathcal{O}_F$. De lo anterior, $a = \dfrac{\beta}{\alpha} r$, es decir $I \subseteq \left\langle \dfrac{\beta}{\alpha} \right\rangle$. De esta forma $I = \left\langle \dfrac{\beta}{\alpha} \right\rangle$ es un ideal principal. Por lo tanto, $\mathcal{O}_F$ es un dominio de ideales principales.

Por otro lado, ya vimos que todos los ideales principales están en la misma clase, por lo que si $\mathcal{O}_F$ es un dominio de ideales principales, $h_F = 1$. □

La siguiente proposición se puede interpretar como un tipo de cancelación para el producto entre ideales.

Proposición 1.53. *Sean* I, J, K *ideales no cero de* $\mathcal{O}_F$ *tales que* $IJ = IK$. *Entonces* $J = K$.

DEMOSTRACIÓN. Sea $1 \leq k \leq h_F$ tal que $I^k = \langle\alpha\rangle$, para algún $\alpha \in \mathcal{O}_F$. Multiplicando por I^{k-1}, $I^k J = I^k K = \langle\alpha\rangle J = \langle\alpha\rangle K$.

Sea $j \in J$. Entonces $\alpha j \in \langle\alpha\rangle J = \langle\alpha\rangle K$, por lo que $\alpha j = \alpha l$, para algún $l \in K$. así $j = l \in K$, es decir $J \subseteq K$.

Análogamente $K \subseteq J$. Por lo tanto, $J = K$. □

Corolario 1.54. *Sean I, J ideales no cero de $\mathcal{O}_F$ tales que $I \subseteq J$. Entonces existe K, un ideal no cero de $\mathcal{O}_F$, tal que $I = JK$.*

DEMOSTRACIÓN. Sea k tal que $J^k = \beta\mathcal{O}_F = \langle\beta\rangle$, entonces $J^{k-1}I \subseteq J^k = \beta\mathcal{O}_F$, por tanto $\frac{1}{\beta}J^{k-1}I \subseteq \mathcal{O}_F$. Sea $K = \frac{1}{\beta}J^{k-1}I$. Notemos que K es un ideal de $\mathcal{O}_F$ y que $JK = J\left(\frac{1}{\beta}J^{k-1}I\right) = \frac{1}{\beta}J^kI = \frac{1}{\beta}\beta\mathcal{O}_FI = I.$ □

1.4. Factorización de ideales en $\mathcal{O}_F$

En esta sección se demostrará que cualquier ideal no cero de $\mathcal{O}_F$ se puede escribir de forma única como producto de ideales primos. También veremos el teorema chino del residuo.

Definición 1.55. *Como ya sabemos si $I \subseteq J$, entonces $I = JK$, para algún K ideal de $\mathcal{O}_F$. En este caso diremos que el ideal J* **divide** *al ideal I y lo escribiremos como $J|I$.*

Lema 1.56. *Sea I un ideal no cero de $\mathcal{O}_F$. Entonces I está contenido en un ideal máximo.*

DEMOSTRACIÓN. Es consecuencia del lema de Zorn. □

Proposición 1.57. *Todo ideal no cero de $\mathcal{O}_F$ se puede escribir como producto de un número finito de ideales primos.*

DEMOSTRACIÓN. Sea I un ideal no cero de $\mathcal{O}_F$. Si I es primo, la afirmación se cumple. En caso contrario, por el lema anterior, existe un ideal primo P_1 tal que $I \subseteq P_1$, entonces $I = P_1K_1$, para algún ideal K_1 de $\mathcal{O}_F$.

Si K_1 es un ideal primo, P_1K_1 es la expresión deseada.

Si K_1 no es un ideal primo, repetimos el procedimiento tantas veces como sea posible, de donde tenemos

$$I = P_1P_2K_2 = P_1P_2P_3K_3 = \cdots = P_1P_2\cdots P_rK_r.$$

Así generamos una cadena ascendente $K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_r \subseteq \cdots$. Como $\mathcal{O}_F$ es noetheriano, esta cadena no puede ser infinita por lo que $P_r = K_r$ es primo. □

Teorema 1.58. *La factorización de un ideal $I \neq \{0\}$ de $\mathcal{O}_F$, como producto de ideales primos es única.*

DEMOSTRACIÓN. Supongamos que $I = P_1P_2\cdots P_s = Q_1Q_2\cdots Q_t$, con P_i, Q_j ideales primos. Tenemos 3 casos: $s < t$, $s = t$ y $s > t$.

Supongamos que $s < t$, entonces $P_1P_2\cdots P_s = Q_1Q_2\cdots Q_sQ_{s+1}\cdots Q_t \subseteq P_1$ y como P_1 es primo, tenemos $Q_j \subseteq P_1$ para algún j. Sin pérdida de generalidad, supongamos que $Q_j = Q_1$, es decir $P_1 = Q_1$, pues Q_j es primo. Por la ley de la cancelación, $P_2P_3\cdots P_s = Q_2Q_3\cdots Q_sQ_{s+1}\cdots Q_t \subseteq P_2$. Repitiendo el mismo razonamiento, tenemos $P_1 = Q_1, P_2 = Q_2, \ldots, P_s = Q_s$, lo cual implica que $\mathcal{O}_F = Q_{s+1}\cdots Q_t$. De lo anterior, $\mathcal{O}_F \subseteq Q_{s+1}$, lo cual es una contradicción ya que Q_{s+1} es máximo. Análogamente $t < s$ no es posible, por lo que $s = t$. □

Definición 1.59. *Sean A un anillo conmutativo con 1 e I, J ideales no cero de A. Si $I + J = \langle 1 \rangle = A$, diremos que I, J son* **primos relativos**.

Lema 1.60. *Sean $\mathcal{O}_F$ el anillo de enteros del campo de números F e I un ideal no cero de $\mathcal{O}_F$. Entonces $N(I) \in I$.*

DEMOSTRACIÓN. Ver [**2**] pág. 240, proposición 10.1.6. □

Proposición 1.61. *Sean F un campo de números, $\mathcal{O}_F$ su anillo de enteros e I, J ideales de $\mathcal{O}_F$ tales que $\mathrm{mcd}(N(I), N(J)) = 1$. Entonces $I + J = \mathcal{O}_F$.*

DEMOSTRACIÓN. Como I, J son ideales de $\mathcal{O}_F$, entonces $I + J \subseteq \mathcal{O}_F$. Por otro lado, sea $x \in \mathcal{O}_F$ y $1 = uN(I) + vN(J)$, con $u, v \in \mathbb{Z}$, por el lema anterior, $x = x \cdot 1 = xuN(I) + xvN(J) \in I + J$, es decir $\mathcal{O}_F \subseteq I + J$. Por lo tanto, $I + J = \mathcal{O}_F$. □

Lema 1.62. *Sea A un anillo conmutativo con 1. Supongamos que $I_1, \ldots, I_g$ son ideales no cero de A tales que $I_i + I_j = A$ para $i \neq j$. Entonces $A = I_1 + I_2 I_3 \cdots I_g$.*

DEMOSTRACIÓN. La demostración se puede hacer por inducción sobre g. □

Proposición 1.63. *Sea A un anillo conmutativo con 1. Supongamos que $I_1, \ldots, I_g$ ideales no cero de A tales que $I_i + I_j = A$ para $i \neq j$. Entonces $I_1 I_2 \cdots I_g = I_1 \cap I_2 \cap \cdots \cap I_g$.*

DEMOSTRACIÓN. Se hará por inducción sobre g.

Supongamos que $g = 2$. Claramente $I_1 I_2 \subseteq I_1$ y $I_1 I_2 \subseteq I_2$, entonces $I_1 I_2 \subseteq I_1 \cap I_2$. Por otro lado, como $I_1 + I_2 = A$, tenemos $1 = a_1 + a_2$ para algunos $a_1 \in I_1$ y $a_2 \in I_2$. Sea $x \in I_1 \cap I_2$, observemos que

$$x = x1 = x(a_1 + a_2) = xa_1 + xa_2 \in I_1 I_2.$$

Por lo tanto, $I_1 \cap I_2 = I_1 I_2$.

Ahora supongamos que el resultado es válido hasta $g - 1$. Probaremos que se cumple para g.

Notemos que

$$\begin{aligned} I_1 \cap I_2 \cap \cdots \cap I_{g-1} \cap I_g &= I_1 \cap (I_2 \cap \cdots \cap I_{g-1} \cap I_g) \\ &= I_1 \cap (I_2 \cdots I_g) \quad \text{por hipótesis de inducción} \\ &= I_1 I_2 \cdots I_g. \end{aligned}$$

La última igualad es cierta usando el caso $g = 2$ y notando que $I_1 + I_2 \cdots I_g = A$. □

A continuación veremos el teorema chino del residuo, un resultado muy importante del álgebra, que será usado a lo largo del trabajo.

Teorema 1.64. *(Teorema Chino del Residuo) Sea A un anillo conmutativo con 1. Supongamos que $I_1, \ldots, I_g$ son ideales no cero de A, tales que $I_i + I_j = A$ para $i \neq j$. Si $I = I_1 I_2 \cdots I_g$, entonces*

$$A/I \cong A/I_1 \times A/I_2 \times \cdots \times A/I_g.$$

DEMOSTRACIÓN. Sea $\psi : A/I \longrightarrow A/I_1 \times A/I_2 \times \cdots \times A/I_g$ definido como:

$$a + I \mapsto (a + I_1, a + I_2, \ldots, a + I_g).$$

Sabemos que $I_1 + I_2 I_3 \cdots I_g = A$, entonces existen $v_1 \in I_1$ y $u_1 \in I_2 I_3 \cdots I_g$ tales que $1 = v_1 + u_1$. De lo anterior, tenemos $1 - u_1 = v_1 \in I_1$, es decir:

$$\begin{aligned} u_1 &\equiv 1 \pmod{I_1}, \\ u_1 &\equiv 0 \pmod{I_2 \cdots I_g}. \end{aligned}$$

Si $k = 2, \ldots, g$, entonces $I_2 \cdots I_g \subseteq I_k$, por lo que

$$\begin{aligned} u_1 &\equiv 1 \pmod{I_1}, \\ u_1 &\equiv 0 \pmod{I_2}, \\ &\vdots \\ u_1 &\equiv 0 \pmod{I_g}. \end{aligned}$$

Con lo anterior, hemos hallado una solución del sistema de congruencias:

$$\begin{cases} x \equiv 1 \pmod{I_1} \\ x \equiv 0 \pmod{I_2} \\ \quad \vdots \\ x \equiv 0 \pmod{I_g}. \end{cases}$$

Consideramos el siguiente sistema para algunos $\gamma_1, \ldots, \gamma_g \in A$:

$$(*) \begin{cases} x \equiv \gamma_1 \pmod{I_1} \\ x \equiv \gamma_2 \pmod{I_2} \\ \quad \vdots \\ x \equiv \gamma_g \pmod{I_g}. \end{cases}$$

el cual tiene como solución $x = \gamma_1 u_1 + \cdots + \gamma_g u_g$, para algunos $u_k \in I_k$.

Consideremos las siguientes observaciones:

i) ψ está bien definida.

Supongamos que $a \equiv a' \pmod{I}$. Notemos que

$$\begin{aligned} \psi(a + I) &= (a + I_1, \ldots, a + I_g) \\ &= (a' + I_1, \ldots, a' + I_g) \\ &= \psi(a' + I). \end{aligned}$$

ii) Notemos que ψ es un morfismo de anillos.

$$\begin{aligned}\psi((a+I)+(b+I)) &= \psi((a+b)+I)\\ &= ((a+b)+I_1,\ldots,(a+b)+I_g)\\ &= ((a+I_1)+(b+I_1),\ldots,(a+I_g)+(b+I_g))\\ &= (a+I_1,\ldots,a+I_g)+(b+I_1,\ldots,b+I_g)\\ &= \psi(a+I)+\psi(b+I).\end{aligned}$$

Análogamente, $\psi((a+I)(b+I)) = \psi(a+I)\psi(b+I)$.

iii) Adicionalmente, ψ es un epimorfismo.

Sean $(\gamma_1+I_1,\ldots,\gamma_g+I_g) \in A/I_1 \times A/I_2 \times \cdots \times A/I_g$ y $u_k \in I_k$ construidos como antes. Para $x = \gamma_1 u_1 + \cdots + \gamma_g u_g$, por $(*)$ se tiene que

$$\begin{aligned}\psi(x+I) &= (x+I_1,\ldots,x+I_g)\\ &= (\gamma_1+I_1,\ldots,\gamma_g+I_g).\end{aligned}$$

Por lo tanto, ψ es suprayectivo.

iv) ψ es inyectivo.

$$\begin{aligned}\ker(\psi) &= \{a+I : \psi(a+I) = (I_1,\ldots,I_g)\}\\ &= \{a+I : (a+I_1,\ldots,a+I_g) = (I_1,\ldots,I_g)\}\\ &= \{a+I : a \in I_1 \cap \cdots \cap I_g\}\\ &= \{a+I : a \in I\} = I.\end{aligned}$$

□

Teorema 1.65. *Sean $p \in \mathbb{Z}$ un primo racional y $P_1, P_2, \ldots, P_g$ ideales primos de $\mathcal{O}_F$ con $N(P_i) = p^{f_i}$ y tales que*

$$\langle p\rangle = p\mathcal{O}_F = P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}.$$

Entonces $e_1f_1 + e_2f_2 + \cdots + e_gf_g = n = [F:\mathbb{Q}]$.

DEMOSTRACIÓN. Como $|\mathcal{O}_F/P_i| = p^{f_i}$, tenemos $|\mathcal{O}_F/P_i^{e_i}| = p^{e_if_i}$.

Por el teorema chino del residuo,

$$\mathcal{O}_F/p\mathcal{O}_F = \mathcal{O}_F/P_1^{e_1} \times \mathcal{O}_F/P_2^{e_2} \times \cdots \times \mathcal{O}_F/P_g^{e_g}.$$

Dado que $p \in p\mathcal{O}_F$, se cumple

$$p^n = |\mathcal{O}_F/p\mathcal{O}_F| = \prod_{i=1}^{g} |\mathcal{O}_F/P_i^{e_i}| = \prod_{i=1}^{g} p^{e_if_i} = p^{\sum_{i=1}^{g} e_if_i}.$$

Por lo tanto, $e_1f_1 + e_2f_2 + \cdots + e_gf_g = n$. □

Llamaremos al valor e_i del teorema anterior el **índice de ramificación** de P_i y a f_i el **grado de inercia** de P_i.

1.5. Campos cuadráticos y extensiones cúbicas puras

En esta sección veremos de forma explícita qué forma tienen los anillos de enteros de los campos cuadráticos y de los campos cúbicos puros.

Lema 1.66. *Sean $F = \mathbb{Q}(\sqrt{d})$ y d un entero libre de cuadrados. Entonces $\alpha = a_1 + a_2\sqrt{d} \in \mathcal{O}_F$ si y sólo si $(2a_1)^2 - d(2a_2)^2 \equiv 0 \pmod 4$ y $2a_1, 2a_2 \in \mathbb{Z}$.*

DEMOSTRACIÓN. Supongamos que $\alpha = a_1 + a_2\sqrt{d} \in \mathcal{O}_F$ Entonces $N(\alpha) = a_1^2 - da_2^2 \in \mathbb{Z}$ y $Tr(\alpha) = 2a_1 \in \mathbb{Z}$. Notemos que

$$(2a_1)^2 - d(2a_2)^2 = 4(a_1^2 - da_2^2) \equiv 0 \pmod 4.$$

Falta ver que $2a_2 \in \mathbb{Z}$.

Como $(2a_2)^2 d \in \mathbb{Z}$, digamos que $(2a_2)^2 d = t \in \mathbb{Z}$ y $2a_2 = \dfrac{p}{q}$ con $mcd(p, q) = 1$. Se cumple $t = \dfrac{p^2}{q^2} d$, de donde $q^2 t = p^2 d$ y $q^2 \mid d$, es decir, $d = q^2 l$ para algún $l \in \mathbb{Z}$. Dado que d es libre de cuadrados, se tiene $q^2 = 1$ y así $2a_2 \in \mathbb{Z}$.

Ahora supongamos que $(2a_1)^2 - d(2a_2)^2 \equiv 4(a_1^2 - a_2^2 d) \equiv 0 \pmod 4$ y $2a_1, 2a_2 \in \mathbb{Z}$. De lo anterior, $a_1^2 - a_2^2 d \in \mathbb{Z}$. Sea $f(x) = x^2 - 2a_1 x + (a_1^2 - a_2^2 d) \in \mathbb{Z}[x]$ y observemos que $f(\alpha) = 0$. Por lo tanto, $\alpha = a_1 + a_2\sqrt{d} \in \mathcal{O}_F$. □

Corolario 1.67. *Sea $F = \mathbb{Q}(\sqrt{d})$, con d libre de cuadrados.*

(i) *Si $d \equiv 2, 3 \pmod 4$, entonces $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.*

(ii) *Si $d \equiv 1 \pmod 4$, se tiene que $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\left(\dfrac{1 + \sqrt{d}}{2}\right)$.*

DEMOSTRACIÓN. Sea $\alpha = a_1 + a_2\sqrt{d} \in \mathcal{O}_F$. Si $d \equiv 2 \equiv -2 \pmod 4$, tenemos que $0 \equiv (2a_1)^2 - (2a_2)^2 d \equiv (2a_1)^2 + 2(2a_2)^2 \pmod 4$ y, si $d \equiv 3 \equiv -1 \pmod 4$, entonces $0 \equiv (2a_1)^2 - (2a_2)^2 d \equiv (2a_1)^2 + (2a_2)^2 \pmod 4$. Recordemos que si $x \in \mathbb{Z}$, $x^2 \equiv 0, 1 \pmod 4$, de donde $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. En ambos casos $2a_1$, $2a_2 \in 2\mathbb{Z}$, es decir, $a_1, a_2 \in \mathbb{Z}$. Por tanto, $\mathcal{O}_F \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

Ahora, si $\alpha = a_1 + a_2\sqrt{d} \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$ y $f(x) = x^2 - 2a_1 x + (a_1^2 - a_2^2 d) \in \mathbb{Z}[x]$, entonces $f(\alpha) = 0$, es decir, $\alpha \in \mathcal{O}_F$ y $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathcal{O}_F$. Por lo tanto, $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

Si $d \equiv 1 \pmod 4$, para $\alpha \in \mathcal{O}_F$, tenemos $\alpha = a_1 + a_2\sqrt{d}$ y

$$0 \equiv (2a_1)^2 - (2a_2)^2 d \equiv (2a_1)^2 - (2a_2)^2 \pmod 4,$$

de donde

$$(2a_1)^2 \equiv (2a_2)^2 \pmod 4,$$

es decir, $2a_1$ y $2a_2$ son ambos pares o ambos impares. Por tanto

$$\begin{aligned}
\alpha &= a_1 + a_2\sqrt{d} \\
&= \frac{2a_1 + 2a_2\sqrt{d}}{2} \\
&= \frac{2a_1 + 2a_2\sqrt{d} - 2a_2 + 2a_2}{2} \\
&= \frac{2a_1 - 2a_2}{2} + \frac{2a_2 + 2a_2\sqrt{d}}{2} \quad \text{con} \quad \frac{2a_1 - 2a_2}{2} \in \mathbb{Z} \\
&= \frac{2a_1 - 2a_2}{2} + 2a_2\left(\frac{1+\sqrt{d}}{2}\right) \\
&\in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right).
\end{aligned}$$

De lo anterior, $\mathcal{O}_F \subseteq \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$.

Por otro lado, sea $\alpha = u + v\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$. Como $\mathbb{Z} \subseteq \mathcal{O}_F$, sólo hay que probar que $\left(\frac{1+\sqrt{d}}{2}\right) \in \mathcal{O}_F$. Notemos que, para $f(x) = x^2 - x + \frac{1-d}{4} \in \mathbb{Z}[x]$, $f\left(\frac{1+\sqrt{d}}{2}\right) = 0$, entonces $\left(\frac{1+\sqrt{d}}{2}\right) \in \mathcal{O}_F$, es decir $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) \subseteq \mathcal{O}_F$.

Así, $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$. □

Corolario 1.68. *Sea $F = \mathbb{Q}(\sqrt{d})$, con d libre de cuadrados.*

(i) *Si $d \equiv 2, 3 \pmod 4$, entonces $\delta_F = 4d$.*
(ii) *Si $d \equiv 1 \pmod 4$, entonces $\delta_F = d$.*

DEMOSTRACIÓN. Si $d \equiv 2, 3 \pmod 4$, $\{1, \sqrt{d}\}$ es una base entera, y

$$\begin{aligned}
\delta_F &= \Delta(1, \sqrt{d}) \\
&= \det\begin{pmatrix} tr(1) & tr(\sqrt{d}) \\ tr(\sqrt{d}) & tr(d) \end{pmatrix} \\
&= \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.
\end{aligned}$$

Por lo tanto, $\delta_F = 4d$.

Si $d \equiv 1 \pmod 4$, $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ es una base entera, entonces

$$\begin{aligned}
\delta_F &= \Delta\left(1, \frac{1+\sqrt{d}}{2}\right) \\
&= \det\begin{pmatrix} tr(1) & tr\left(\dfrac{1+\sqrt{d}}{2}\right) \\ tr\left(\dfrac{1+\sqrt{d}}{2}\right) & tr\left(\left(\dfrac{1+\sqrt{d}}{2}\right)^2\right) \end{pmatrix} \\
&= \det\begin{pmatrix} 2 & 1 \\ 1 & \dfrac{1+d}{2} \end{pmatrix}
\end{aligned}$$

Así, $\delta_F = d$. □

La siguiente proposición es muy importante, ya que nos ayuda a ver cuándo un primo racional se ramifica, se descompone o es inerte.

Proposición 1.69. *Sean $\mathcal{O}_F$ el anillo de enteros de $F = \mathbb{Q}(\sqrt{d})$, p un número primo racional impar. Entonces:*

(i) *Si $p \nmid \delta_F$ y $x^2 \equiv d \pmod p$ es soluble en $\mathbb{Z}$, entonces $\langle p\rangle = PP'$, con $P \neq P'$ ideales primos de $\mathcal{O}_F$.*
(ii) *Si $p \nmid \delta_F$ y $x^2 \equiv d \pmod p$ no es soluble en $\mathbb{Z}$, entonces $\langle p\rangle$ es un ideal primo de $\mathcal{O}_F$.*
(iii) *Si $p|\delta_F$, entonces $\langle p\rangle = P^2$ donde P es un ideal primo de $\mathcal{O}_F$.*

DEMOSTRACIÓN. (i) Supongamos que $a^2 \equiv d \pmod p$, $a \in \mathbb{Z}$. Veremos que $\langle p\rangle = \langle p, a+\sqrt{d}\rangle\langle p, a-\sqrt{d}\rangle$.

En efecto

$$\begin{aligned}
\langle p, a+\sqrt{d}\rangle\langle p, a-\sqrt{d}\rangle &= \langle p^2, p(a+\sqrt{d}), p(a-\sqrt{d}), a^2-d\rangle \\
&= \langle p\rangle\left\langle p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p}\right\rangle.
\end{aligned}$$

Notemos que el último ideal es $\mathcal{O}_F$ ya que contiene a p y $2a$, dos números primos relativos.

Claramente $\langle p, a+\sqrt{d}\rangle \neq \langle p, a-\sqrt{d}\rangle$, ya que si fueran iguales, entonces el ideal contendría a p y $2a$, de donde $\langle p\rangle = \mathcal{O}_F$.

(ii) Veremos que el grado de inercia de P es 2.

Supongamos que $f = 1$, entonces $|\mathcal{O}_F/P| = p$, de donde $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_F/P$, por tanto toda clase es representada por un entero racional. Digamos que $a \in \mathbb{Z}$ es tal que $a \equiv \sqrt{d} \pmod p$, entonces $a^2 \equiv d \pmod p$ lo cual es una contradicción al hecho de que $x^2 \equiv d \pmod p$ no es soluble en $\mathbb{Z}$.

(iii) Vamos a demostrar que $\langle p\rangle = \langle p, \sqrt{d}\rangle^2$.

Notemos que,

$$\begin{aligned}\langle p, \sqrt{d}\rangle^2 &= \langle p^2, p\sqrt{d}, d\rangle \\ &= \langle p\rangle \left\langle p, \sqrt{d}, \frac{d}{p}\right\rangle.\end{aligned}$$

Este último ideal es $\mathcal{O}_F$ ya que p y d/p están en él y son primos relativos. □

Proposición 1.70. *Sean $\mathcal{O}_F$ el anillo de enteros de $F = \mathbb{Q}(\sqrt{d})$. Entonces:*

(i) *Si $d \equiv 1 \pmod 8$, entonces $\langle 2\rangle = PP'$, con $P \neq P'$ ideales primos de $\mathcal{O}_F$.*
(ii) *Si $d \equiv 5 \pmod 8$, entonces $\langle 2\rangle$ es un ideal primo de $\mathcal{O}_F$.*
(iii) *Si $d \equiv 2, 3 \pmod 4$, entonces $\langle 2\rangle = P^2$ con P un ideal primo de $\mathcal{O}_F$.*

DEMOSTRACIÓN. (i) Si $d \equiv 1 \pmod 8$, veremos que

$$\langle 2\rangle = \left\langle 2, \frac{1+\sqrt{d}}{2}\right\rangle \left\langle 2, \frac{1-\sqrt{d}}{2}\right\rangle.$$

Operando, obtenemos

$$\left\langle 2, \frac{1+\sqrt{d}}{2}\right\rangle \left\langle 2, \frac{1-\sqrt{d}}{2}\right\rangle = \langle 2\rangle \left\langle 2, \frac{1+\sqrt{d}}{2}, \frac{1-\sqrt{d}}{2}, \frac{1-d}{8}\right\rangle,$$

donde el último ideal es $\mathcal{O}_F$ ya que $1 = \left(\frac{1+\sqrt{d}}{2}\right) + \left(\frac{1-\sqrt{d}}{2}\right)$.

Más aún $\left\langle 2, \frac{1+\sqrt{d}}{2}\right\rangle \neq \left\langle 2, \frac{1-\sqrt{d}}{2}\right\rangle$ ya que de lo contrario el ideal contendría al 1 y se tendría que $\langle 2\rangle = \mathcal{O}_F$.

(ii) Si $d \equiv 5 \pmod 8$, veremos que P tiene grado de inercia 2. Supongamos que no, entonces, como en la parte (ii) de la proposición anterior, existe $a \in \mathbb{Z}$ tal que $a \equiv \frac{1+\sqrt{d}}{2} \pmod P$. Dado que $\frac{1+\sqrt{d}}{2}$ satisface $x^2 - x + \frac{1-d}{4} = 0$, se tiene $a^2 - a + \frac{1-d}{4} \equiv 0 \pmod P$ y así $a^2 - a + \frac{1-d}{4} \equiv 0 \pmod 2$. Sabemos que para todo $a \in \mathbb{Z}$, $a^2 - a$ es par, entonces $\frac{1-d}{4} \equiv 0 \pmod 2$ ó $d \equiv 1 \pmod 8$ lo cual es una contradicción a la hipótesis.

(iii) Si $d \equiv 2 \pmod 4$, tenemos $\langle 2\rangle = \langle 2, \sqrt{d}\rangle^2$ y si $d \equiv 3 \pmod 4$, $\langle 2\rangle = \langle 2, 1 + \sqrt{d}\rangle^2$. □

Consideremos ahora, el caso de una extensión cúbica pura, es decir, aquellas de la forma $F = \mathbb{Q}(\alpha)$ donde $\alpha = \sqrt[3]{m}$, con m un entero libre de cubos. Agrupando por un lado todos los factores primos de m cuyo cuadrado también divide a m y por otro todos los restantes, m se puede expresar de la forma $m = hk^2$, $h, k \in \mathbb{Z}$, libres de cuadrados y $mcd(h, k) = 1$.

Teorema 1.71. *Sea $F = \mathbb{Q}(\alpha)$ una extensión cúbica en las condiciones anteriores, entonces el anillo $\mathcal{O}_F$ de enteros algebraicos de F tiene una base entera de la forma:*

$$\mathcal{B} = \begin{cases} \left\{1, \alpha, \dfrac{\alpha^2}{k}\right\} & \textit{si} \quad m \not\equiv \pm 1 \pmod 9 \\ \left\{1, \alpha, \dfrac{\alpha^2 + k^2\alpha + k^2}{3k}\right\} & \textit{si} \quad m \equiv 1 \pmod 9 \\ \left\{1, \alpha, \dfrac{\alpha^2 - k^2\alpha + k^2}{3k}\right\} & \textit{si} \quad m \equiv -1 \pmod 9. \end{cases}$$

DEMOSTRACIÓN. Por el teorema de la base entera especial, $\mathcal{O}_F$ tiene una base entera de la forma $\left\{1, \dfrac{f_1(\alpha)}{d_1}, \dfrac{f_2(\alpha)}{d_2}\right\}$ con cada $f_i \in \mathbb{Z}[x]$ mónico de grado i y d_1,d_2 números enteros tales que $d_1|d_2$.
Además por las observaciones posteriores a dicho teorema, $d_1^2|d_2$ y

$$d_1^6|\Delta(1, \alpha, \alpha^2) = -27m^2 = (-1)3^3h^2k^4,$$

por lo que $d_1^6|3^3h^2k^4$. Como h y k son libres de cuadrados, se tiene que $d_1 = 1$ salvo si $9|m$, en cuyo caso $d_1 = 1$ o $d_1 = 3$.

Por otro lado, si $d_1 = 3$ y $f_1(x) = a + x \in \mathbb{Z}[x]$, se tendría que $\beta = \dfrac{a + \alpha}{3} \in \mathcal{O}_F$, por lo que $\beta^3 \in \mathcal{O}_F$ y $tr(\beta^3) \in \mathbb{Z}$. Calculando la traza tenemos

$$tr(\beta^3) = \frac{1}{27}(tr(\alpha^3 + 3a\alpha^2 + 3a^2\alpha + a^3)) = \frac{1}{27}(tr(m) + 3atr(\alpha^2) + 3a^2tr(\alpha) + tr(a^3)),$$

donde $tr(\alpha) = 0$ y $tr(\alpha^2) = 0$, por lo que

$$tr(\beta^3) = \frac{1}{27}(3m + 3a^3) = \frac{m + a^3}{9}.$$

Como estamos considerando el caso $9|m$, entonces $9|a^3$ y, por tanto, $3|a$, lo que implica que

$$\frac{\alpha}{3} = \beta - \frac{a}{3} \in \mathcal{O}_F.$$

Considerando $Irr(\frac{\alpha}{3}, \mathbb{Q}) = x^3 - \dfrac{m}{27} \notin \mathbb{Z}[x]$, es claro que $\dfrac{\alpha}{3} \notin \mathcal{O}_F$, lo que contradice la observación anterior, y por lo tanto $d_1 \neq 3$.

Por las observaciones posteriores al teorema de la base entera especial y el hecho de que $d_1 = 1$, se puede considerar $f_1(x) = x$, por lo que el segundo termino de la base entera es, en todos los casos, α.

Veamos ahora que, en cada uno de los casos considerados, el tercer término de la base entera tiene la forma indicada.

Notemos que $Irr(\frac{\alpha^2}{k}, \mathbb{Q}) = x^3 - h^2k \in \mathbb{Z}[x]$ por lo que, en general, $\dfrac{\alpha^2}{k} \in \mathcal{O}_F$ y por consiguiente, $k|d_2$. Si $m \equiv 1 \pmod 9$, tenemos

$$Irr\left(\frac{(\alpha - 1)^2}{3}, \mathbb{Q}\right) = x^3 - x^2 + \frac{1 + 2m}{3}x - \frac{(m - 1)^2}{27} \in \mathbb{Z}[x]$$

y $\dfrac{(\alpha-1)^2}{3} \in \mathcal{O}_F$, de donde

$$\frac{\alpha^2+k^2\alpha+k^2}{3k} = k\frac{(\alpha-1)^2}{3} + \frac{1-k^2}{3}\frac{\alpha^2}{k} + k\alpha \in \mathcal{O}_F$$

y $3k|d_2$.

De manera análoga, si $m \equiv -1 \pmod 9$, consideremos el elemento $\dfrac{(\alpha+1)^2}{3}$, de donde

$$\frac{\alpha^2-k^2\alpha+k^2}{3k} \in \mathcal{O}_F.$$

Por tanto, en este caso también se tiene $3k|d_2$.

Para terminar la demostración bastará probar que $d_2 \leq 3k$ cuando $m \equiv \pm 1 \pmod 9$ y $d_2 \leq k$ en caso contrario.

Como $d_2^2|27m^2 = 3^3m^2$, $d_2|3m$ y así, los únicos números primos distintos de 3 que dividen a d_2 son los que dividen a m o, equivalentemente, los que dividen a h o a k.

Sea p un número primo $p \neq 3$ tal que $p|m$ y supongamos que $p \nmid k$, es decir $p^2 \nmid m$. Consideremos $f_2(x) = x^2+ax+b \in \mathbb{Z}[x]$. Veamos que $p \nmid d_2$. Supongamos lo contrario, entonces, como $\dfrac{f_2(\alpha)}{d_2} \in \mathcal{O}_F$,

$$\frac{f_2(\alpha)}{p} = \frac{\alpha^2+a\alpha+b}{p} = \frac{d_2}{p}\frac{\alpha^2+a\alpha+b}{d_2} \in \mathcal{O}_F,$$

por lo que $\dfrac{3b}{p} = tr\left(\dfrac{\alpha^2+a\alpha+b}{p}\right) \in \mathbb{Z}$ y $p|b$. Así,

$$\frac{\alpha^2+a\alpha}{p} = \frac{\alpha^2+a\alpha+b}{p} - \frac{b}{p} \in \mathcal{O}_F$$

y por consiguiente

$$\left(\frac{\alpha^2+a\alpha}{p}\right)^3 = \frac{1}{p^3}(\alpha^3(\alpha+a)^3) = \frac{1}{p^3}(m(\alpha^3+3a\alpha^2+3a^2\alpha+a^3)) \in \mathcal{O}_F,$$

de donde $tr\left(\left(\dfrac{\alpha^2+a\alpha}{p}\right)^3\right) = \dfrac{m}{p^3}(3(m+a^3)) \in \mathbb{Z}$. Como $p^2 \nmid m$ y $p^3|3m(m+a^3)$, entonces $p^2|m+a^3$ y $p|a$. De lo anterior,

$$\frac{\alpha^2}{p} = \frac{\alpha^2+a\alpha}{p} - \frac{a\alpha}{p} \in \mathcal{O}_F,$$

lo que no es posible, pues

$$Irr\left(\frac{\alpha^2}{p}, \mathbb{Q}\right) = x^3 - \frac{m^2}{p^3} \notin \mathbb{Z}[x],$$

es decir $p \nmid d_2$.

Por tanto los únicos factores primos distintos de 3 que dividen d_2 son los que dividen a k.

Si p es uno de éstos, como k es libre de cuadrados, $p^2 \nmid k$. De forma similar a la anterior, vamos a demostrar que $p^2 \nmid d_2$. Si sucede lo contrario,

$$\frac{f_2(\alpha)}{p^2} = \frac{\alpha^2 + a\alpha + b}{p^2} = \frac{d_2}{p^2}\frac{\alpha^2 + a\alpha + b}{d_2} \in \mathcal{O}_F$$

por lo que $\dfrac{3b}{p^2} = tr\left(\dfrac{\alpha^2 + a\alpha + b}{p^2}\right) \in \mathbb{Z}$ y $p^2|b$. Así,

$$\left(\frac{\alpha^2 + a\alpha}{p^2}\right) \in \mathcal{O}_F \quad \text{y} \quad tr\left(\left(\frac{\alpha^2 + a\alpha}{p^2}\right)\right)^3 = \frac{3m(m + a^3)}{p^6} \in \mathbb{Z}.$$

Como en el caso anterior, $p^3 \nmid m$ y $p^6|3m(m+a^3)$, lo que implica $p^4|m+a^3$. Por lo anterior y $p^2|m$ se tiene que $p|a$ y $p^3|a^3$, de donde $p^3|m$ lo que es una contradicción. Por lo tanto $p^2 \nmid d_2$.

Para terminar, vamos a encontrar la potencia máxima de 3 que divide a d_2. Si $3 \nmid m$, como $d_2|3m$, entonces $9 \nmid d_2$, por lo que, para $m \equiv \pm 1 \pmod 9$, $d_2 = 3k$.

Para el resto de los casos, debido a que $\mathcal{O}_F = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\dfrac{f_2(\alpha)}{d_2}$ y

$$\left(\frac{f_2(\alpha)}{d_2}\right)^2 = \frac{(\alpha^2 + a\alpha + b)^2}{d_2^2} = \frac{(a^2 + 2b)\alpha^2 + (m + 2ab)\alpha + (2am + b^2)}{d_2^2}$$

tenemos $d_2|a^2 + 2b$, $d_2|m + 2ab$ y $d_2|2am + b^2$.

Para el caso $3 \nmid m$ y $m \not\equiv \pm 1 \pmod 9$, veremos que $3 \nmid d_2$. Supongamos lo contrario, entonces $2ab \equiv -m \not\equiv 0 \pmod 3$ por lo que $1 \equiv a^2 \equiv -2b \equiv b \pmod 3$ y $a \equiv -2a \equiv -2ab \equiv m \pmod 3$. Por otro lado, tenemos

$$\frac{\alpha^2 + a\alpha + b}{3} = \frac{d_2}{3}\frac{\alpha^2 + a\alpha + b}{d_2} \in \mathcal{O}_F,$$

por lo que

$$\frac{\alpha^2 + m\alpha + 1}{3} = \frac{\alpha^2 + a\alpha + b}{3} - r\alpha - s \in \mathcal{O}_F,$$

para algunos $r, s \in \mathbb{Z}$. Suponiendo que $m \equiv a \equiv -2 \pmod 3$, se tiene

$$\frac{(\alpha - 1)^2}{3} = \frac{\alpha^2 - 2\alpha + 1}{3} = \frac{\alpha^2 + a\alpha + 1}{3} - t\alpha \in \mathcal{O}_F,$$

para algún $t \in \mathbb{Z}$. Elevando a la cuarta potencia y tomando trazas se llega a que $3^2|m - 1$ y $m \equiv 1 \pmod 9$ lo que es una contradicción.

Si por el contrario, $m \equiv a \equiv 2 \pmod 3$ tenemos

$$\frac{(\alpha + 1)^2}{3} = \frac{\alpha^2 + 2\alpha + 1}{3} = \frac{\alpha^2 + a\alpha + 1}{3} - t\alpha \in \mathcal{O}_F$$

para algún $t \in \mathbb{Z}$ y de igual manera, elevando a la cuarta potencia y tomando trazas, se llega a que $3^2|m + 1$ y $m \equiv -1 \pmod 9$, lo cual también es una contradicción.

Supongamos ahora que $3 \nmid k$ ($9 \nmid m$). Veremos que $3 \nmid d_2$. Si $3|d_2$, entonces $3|a^2 + 2b$, $3|m + 2ab$ y $3|b^2 + 2am$ por lo que $3|a^2 + 2b$, $2ab$, b^2, de donde $3|a$ y $3|b$. Por lo anterior,

$$\frac{\alpha^2}{3} = \frac{\alpha^2 + a\alpha + b}{3} - \frac{a}{3}\alpha - \frac{b}{3} \in \mathcal{O}_F$$

Lo cual no puede ser ya que $9 \nmid m$ y

$$Irr\left(\frac{\alpha^2}{3}, \mathbb{Q}\right) = x^3 - \frac{m^2}{3^3} \notin \mathbb{Z}[x].$$

Por último, si $3|k$ $(9|m)$ y suponemos que $9|d_2$, se tendría $9|a^2+2b$, $9|m+2ab$ y $9|b^2+2am$, de esta última, $9|b^2$ y $3|b$. Como $3|a^2+2b$, entonces $3|a^2$, $9|a^2$ y, como $9|a^2+2b$, $9|b$. Así,

$$\frac{\alpha^2+a\alpha}{9} = \frac{d_2}{9}\frac{\alpha^2+a\alpha+b}{9} - \frac{b}{9} \in \mathcal{O}_F$$

y por tanto $\left(\frac{\alpha^2+a\alpha}{9}\right)^3 \in \mathcal{O}_F$.

$$tr\left(\left(\frac{\alpha^2+a\alpha}{9}\right)^3\right) = 3\frac{m^2+a^3m}{3^6} = \frac{m(m+a^3)}{3^2\cdot 3^3} \in \mathbb{Z}.$$

Como 9 es la potencia de 3 más grande que divide a m, entonces $3^3|m+a^3$. Como a es múltiplo de 3, entonces $3^3|m$ lo cual es imposible.

Con estas últimas consideraciones se ha probado que si $m \not\equiv \pm 1 \pmod 9$ la potencia de 3 en la factorización de d_2 es la misma que en la de k, es decir $d_2 = k$, lo que termina la demostración. □

A continuación veremos algunos ejemplos

Ejemplo 1.72. (i) *Sea* $F = \mathbb{Q}(\sqrt[3]{7})$*, donde* $m = 7$*,*$h = 7$ *y* $k = 1$.
Como $7 \not\equiv \pm 1 \pmod 9$*, por el teorema anterior tenemos*

$$\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{7} + \mathbb{Z}\sqrt[3]{49}.$$

(ii) *Sea* $F = \mathbb{Q}(\sqrt[3]{2})$*, donde* $m = 2$*,*$h = 2$ *y* $k = 1$.
Como $2 \not\equiv \pm 1 \pmod 9$*, entonces por el teorema anterior*

$$\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}.$$

(iii) *Sea* $F = \mathbb{Q}(\sqrt[3]{19})$*, donde* $m = 19$*,*$h = 19$ *y* $k = 1$.
Como $19 \equiv 1 \pmod 9$*, por el teorema anterior se tiene*

$$\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{19} + \mathbb{Z}\frac{\sqrt[3]{361}+\sqrt[3]{19}+1}{3}.$$

Capítulo 2

Órdenes en campos de números

En el capítulo anterior vimos que el anillo de enteros cumple varias propiedades como ser dominio entero, ser anillo noetheriano, los ideales distintos de cero se factorizan de forma única como producto de ideales primos y en algunos casos es de factorización única a nivel de elementos.

En este capítulo estudiaremos subanillos del campo de números llamados órdenes, los cuales en contraste con el anillo de enteros, no son dominios de Dedekind. Por lo tanto, pueden perder propiedades aritméticas como, por ejemplo, la factorización única a nivel de ideales(ver [**14**]).

Dado $\mathcal{O}$ un orden en el campo de números F, vamos a definir un ideal especial en $\mathcal{O}$, llamado el *conductor* de $\mathcal{O}$.

Se demostrará que los ideales no cero en $\mathcal{O}$ que son primos relativos al conductor son invertibles y tienen factorización única como producto de ideales primos en $\mathcal{O}$. Adicionalmente, veremos cuáles son las propiedades que deben cumplir los elementos de $\mathcal{O}$ para que tengan factorización única.

En este capítulo la palabra ideal significará ideal distinto de cero, a menos que se diga lo contrario.

2.1. Órdenes e ideales conductor

En esta sección veremos lo que es un orden y qué es el conductor asociado a dicho orden. A lo largo de este capítulo F es un campo de números, con $[F : \mathbb{Q}] = n$.

Existen diferentes maneras equivalentes de como definir un orden en un campo de números (ver [**14**], [**12**], [**8**]), nosotros elegimos la siguiente.

Definición 2.1. *Un* **$\mathbb{Z}$-módulo** *de un campo de números F es un subgrupo aditivo de F finitamente generado. Los $\mathbb{Z}$-módulos de rango n (número mínimo de generadores) se llaman* **$\mathbb{Z}$-módulos completos**.

Definición 2.2. *Un* **orden** *$\mathcal{O}$ es un $\mathbb{Z}$-módulo completo de F que además es un subanillo con unidad.*

$\mathcal{O}_F$ es un orden de F y como veremos más adelante es el orden máximo.

Ejemplo 2.3. *Sea $F = \mathbb{Q}(\sqrt[3]{19})$. Notemos que,*

$$\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{19} + \mathbb{Z}\frac{\sqrt[3]{361} + \sqrt[3]{19} + 1}{3}$$

y

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt[3]{19} + \mathbb{Z}\sqrt[3]{361}$$

son ordenes de F, además $\mathcal{O} \subsetneq \mathcal{O}_F$.

Lema 2.4. *Todo orden $\mathcal{O}$ de F es un anillo noetheriano.*

DEMOSTRACIÓN. Como $\mathbb{Z}$ es un anillo noetheriano y $\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado, entonces $\mathcal{O}$ es noetheriano. □

La siguiente proposición nos permitirá demostrar un teorema, con el cual podemos verificar que $\mathcal{O}_F$ es el orden más grande.

Proposición 2.5. *Sean $F \neq \mathbb{Q}$ un campo de números, $\mathcal{O}_F = \mathbb{Z} + \alpha_2\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$ con $\{1, \alpha_2, \ldots, \alpha_n\}$ una base entera y $\mathcal{O}$ un subanillo de F con unidad tal que $\mathcal{O} \subseteq \mathcal{O}_F$ y $|\mathcal{O}_F/\mathcal{O}|$ finito. Entonces existen $\beta_2, \ldots, \beta_n \in \mathcal{O}$ tales que $\mathcal{O} = \mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$ donde $\beta_i = a_{i1} + a_{i2}\alpha_2 + \cdots + a_{in}\alpha_n$ con $a_{ij} = 0$ para $i > j$ y $a_{ii} > 0$ el mínimo posible.*

DEMOSTRACIÓN. Primero veremos que existen $\beta_1, \beta_2, \ldots, \beta_n \in \mathcal{O}$ con las condiciones antes mencionadas. Para ello usaremos inducción demostrando que si para algún $i < n$ existen $\beta_1, \ldots, \beta_i$, también existe el elemento β_{i+1}.

Observemos que $\mathbb{Z} \subseteq \mathcal{O}$, pero $\mathbb{Z} \neq \mathcal{O}$ ya que si $\mathbb{Z} = \mathcal{O}$, entonces $|\mathcal{O}_F/\mathcal{O}| = \infty$, lo cual no puede ser, por lo que $\beta_1 = 1 \in \mathcal{O}$. De lo anterior, existe $\beta_2 \in \mathcal{O} \setminus \mathbb{Z}$ con $\beta_2 = a_{21} + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n$. Podemos suponer $a_{21} = 0$, de lo contrario, hacemos $\beta_2' = \beta_2 - a_{21}\beta_1$ para sustituir a β_2. También $a_{22} > 0$, ya que si $a_{22} = 0$, cambiamos el orden de la base $\{1, \alpha_2, \ldots, \alpha_n\}$ en caso de ser necesario. Si $a_{22} < 0$ multiplicamos a β_{22} por -1. Ahora, como los coeficientes de β_2 de los elementos de $\mathcal{O}$ están en $\mathbb{Z}$, podemos elegir a β_2 de tal manera que el coeficiente a_{22} sea mínimo.

Supongamos que el resultado se cumple hasta i. Veremos que se cumple para $i+1$.

Por hipótesis de inducción existen $\beta_1, \beta_2, \ldots, \beta_i \in \mathcal{O}$ tales que $\beta_1\mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_i\mathbb{Z} \subseteq \mathcal{O}$ con

$$\begin{aligned}
\beta_1 &= 1 \\
\beta_2 &= 0 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n \\
&\vdots \\
\beta_i &= 0 + 0 + 0 + \cdots + 0 + a_{ii}\alpha_i + \cdots + a_{nn}\alpha_n.
\end{aligned}$$

además $a_{kk} > 0$ y mínimo para $k = 1, \ldots, i$.

Como $\mathcal{O}_F$ es un $\mathbb{Z}$-módulo libre de rango n y $A_i = \mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_i\mathbb{Z}$ es un $\mathbb{Z}$-módulo libre de rango $i < n$, entonces $|\mathcal{O}_F/A_i| = \infty$, es decir, $A_i \neq \mathcal{O}$. Así, existe $\beta_{i+1} \in \mathcal{O} \setminus A_i$, con $A_i + \beta_{i+1}\mathbb{Z} \subseteq \mathcal{O}$.

Veremos que β_{i+1}, lo podemos tomar de la forma deseada.

Sabemos que $\beta_{i+1} = a_{i+1,1} + a_{i+1,2}\alpha_2 + \cdots + a_{i+1,n}\alpha_n$ y notemos $a_{i+1,1} = 0$ haciendo $\beta_{i+1}' = \beta_{i+1} - a_{i+1,1}\beta_1$. Ahora supongamos que para algún $k \in \{2, \ldots, i\}$, $a_{i+1,r} = 0$ para $r < k$ y $a_{i+1,k} \neq 0$, entonces $mcd(a_{i+1,k}, a_{kk}) = a_{kk}$ ya que de lo contrario, $m = mcd(a_{i+1,k}, a_{kk}) < a_{kk}$, tendríamos $m = ba_{i+1,k} + ca_{kk}$ para algunos $b, c \in \mathbb{Z}$ y luego $\beta_{i+1}' = b\beta_{i+1} + c\beta_i = m\alpha_k + b_{i+1,k+1}\alpha_{k+1} + \cdots + b_{i+1,n}\alpha_n \in \mathcal{O}$, es decir, el primer coeficiente distinto de cero es $a_{i+1,k} = m < a_{kk}$ lo que no es posible por la minimalidad de a_{kk}. Entonces $a_{i+1,k} = a_{kk}t$ para algún $t \in \mathbb{Z}$, de donde $\beta_{i+1}' = \beta_{i+1} - t\beta_k = 0 + \cdots + 0\alpha_k + d_{i+1,k+1}\alpha_{k+1} + \cdots + d_{i+1,n}\alpha_n$.

Así, $\{1, \beta_2, \ldots, \beta_i, \beta_{i+1}\}$ y $\{1, \beta_2, \ldots, \beta_i, \beta_{i+1}'\}$ generan al mismo $\mathbb{Z}$-módulo. Por lo tanto, existe $\beta_{i+1} \neq 0$ donde $a_{ij} = 0$ para $i > j$, con $a_{ii} > 0$ y podemos elegirlo de tal manera que sea mínimo.

Ahora veremos que todo elemento $\gamma \in \mathcal{O}$ se puede expresar como una $\mathbb{Z}$-combinación de $\{\beta_1 = 1, \beta_2, \ldots, \beta_n\}$. Supongamos que existe $\gamma \in \mathcal{O} \setminus A_n$, donde $A_n = \mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$, y sabemos $\gamma = a_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$. Si $a_1 \neq 0$, $mcd(a_1, 1) = 1$ y como $\gamma - a_1\beta_1 \in \mathcal{O} \setminus A_n$ si y sólo si $\gamma \in \mathcal{O} \setminus A_n$, podemos suponer que γ es tal que $a_1 = 0$. Si $a_2 \neq 0$, de forma análoga que en el paso inductivo, se cumple $mcd(a_2, a_{22}) = a_{22}$, es decir, $a_2 = r_2 a_{22}$, para algún $r_2 \in \mathbb{Z}$, y como $\gamma - r_2\beta_2 \in \mathcal{O} \setminus A_n$ si y sólo si $\gamma \in \mathcal{O} \setminus A_n$, concluimos que γ es tal que $a_2 = 0$. Continuando con el mismo procedimiento llegamos a que $0 \in \mathcal{O}/A_n$, lo cual es una contradicción .

Por lo tanto, $\mathcal{O} = \mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$. □

Teorema 2.6. *Sea $\mathcal{O}$ un subanillo de F con unidad. Las siguientes condiciones son equivalentes:*

(i) *$\mathcal{O}$ es un orden.*
(ii) *$\mathcal{O} \subseteq \mathcal{O}_F$ y $|\mathcal{O}_F/\mathcal{O}| < \infty$.*

DEMOSTRACIÓN. Supongamos que $\mathcal{O}$ es un orden, entonces $\mathcal{O} = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$ con $\beta_i \in \mathcal{O}$ para cada $i = 1, \ldots, n$. Notemos que $\beta_i \in F \subset \mathbb{C}$ y $\beta_i\alpha \in \mathcal{O}$ para todo $\alpha \in \mathcal{O}$ pues $\mathcal{O}$ es anillo, por la proposición 1.12, $\beta_i \in \Omega$ para cada $i = 1, \ldots, n$. De donde $\mathcal{O} \subseteq F \cap \Omega = \mathcal{O}_F$.

Veremos que $|\mathcal{O}_F/\mathcal{O}| < \infty$. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de F y $\mathcal{O}_F = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$, como $\mathcal{O} \subseteq \mathcal{O}_F$, escribimos a cada β_i en términos de la base entera

$$\begin{aligned}
\beta_1 &= a_{11}\alpha_1 + a_{21}\alpha_2 + \cdots + a_{n1}\alpha_n \\
\beta_2 &= a_{12}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{n2}\alpha_n \\
&\vdots \\
\beta_n &= a_{1n}\alpha_1 + a_{2n}\alpha_2 + \cdots + a_{nn}\alpha_n.
\end{aligned}$$

Así, $\mathcal{O} = (a_{11} + \cdots + a_{1n})\alpha_1\mathbb{Z} + \cdots + (a_{n1} + \cdots + a_{nn})\alpha_n\mathbb{Z}$, luego

$$\begin{aligned}
\mathcal{O}_F/\mathcal{O} &= \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}/((a_{11} + \cdots + a_{1n})\alpha_1\mathbb{Z} + \cdots + (a_{n1} + \cdots + a_{nn})\alpha_n\mathbb{Z}) \\
&\approx \mathbb{Z}/(a_{11} + \cdots + a_{1n})\mathbb{Z} \times \cdots \times \mathbb{Z}/(a_{n1} + \cdots + a_{nn})\mathbb{Z}.
\end{aligned}$$

Por tanto $|\mathcal{O}_F/\mathcal{O}| = |\mathbb{Z}/(a_{11} + \cdots + a_{1n})\mathbb{Z}| \cdots |\mathbb{Z}/(a_{n1} + \cdots + a_{nn})\mathbb{Z}| < \infty$.

Ahora supongamos que $\mathcal{O} \subseteq \mathcal{O}_F$ y $|\mathcal{O}_F/\mathcal{O}| < \infty$, por la proposición anterior $\mathcal{O}$ es un orden. □

Definición 2.7. *Definimos el* **índice** *de $\mathcal{O}$ como* índ*($\mathcal{O}$)*$= |\mathcal{O}_F/\mathcal{O}|$.

El siguiente lema y proposición son algunas propiedades del anillo de enteros que también se cumplen para el orden.

Lema 2.8. *Sea J un ideal de $\mathcal{O}$. Entonces $|\mathcal{O}/J|$ es finito.*

DEMOSTRACIÓN. La demostración es análoga a la del lema 1.32 □

Proposición 2.9. *Sea P un ideal primo de $\mathcal{O}$. Entonces P es un ideal máximo.*

DEMOSTRACIÓN. Como P es primo, tenemos $\mathcal{O}/P$ es un dominio entero finito, es decir, un campo y por tanto P es máximo. □

Lema 2.10. *Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_F$. Entonces:*

(i) $\mathbb{Z} + I = \{z + a : z \in \mathbb{Z}, a \in I\}$ *es el subanillo con unidad más chico de $\mathcal{O}_F$ que contiene a I.*
(ii) *Si $b_1 =$*mín$(I \cap \mathbb{N})$*, entonces $|(\mathbb{Z} + I)/I| = b_1$.*
(iii) $\mathbb{Z} + I$ *es un orden en F.*
(iv) *Si $N(I) = p$, con p un primo racional, entonces $\mathbb{Z} + I = \mathcal{O}_F$*

DEMOSTRACIÓN. (i) Primero mostraremos que $\mathbb{Z} + I$ es un subanillo de $\mathcal{O}_F$. Sean $x, y \in \mathbb{Z} + I$. Como $x, y \in \mathbb{Z} + I$, entonces $x = z_1 + a_1$ y $y = z_2 + a_2$, con $z_1, z_2 \in \mathbb{Z}$ y $a_1, a_2 \in I$. Por tanto, $x - y = (z_1 + a_1) - (z_2 + a_2) = (z_1 - z_2) + (a_1 - a_2) \in \mathbb{Z} + I$ y $xy = (z_1 + a_1)(z_2 + a_2) = z_1z_2 + (z_1a_2 + z_2a_1 + a_1a_2) \in \mathbb{Z} + I$. Por tanto $\mathbb{Z} + I$ es un subanillo de $\mathcal{O}_F$.

Ahora veremos que $\mathbb{Z} + I$ es el subanillo con unidad más chico que contiene a I. Supongamos que existe un subanillo con unidad A de $\mathcal{O}_F$ tal que $I \subseteq A$. Probaremos que $\mathbb{Z} + I \subseteq A$. Como $1 \in A$, $\mathbb{Z} \subseteq A$, entonces $\mathbb{Z} + I \subseteq A$.

(ii) Sabemos que $(\mathbb{Z} + I)/I \cong \mathbb{Z}/I \cap \mathbb{Z}$ y $\mathbb{Z}/I \cap \mathbb{Z} = \mathbb{Z}/b_1\mathbb{Z}$, entonces $|(\mathbb{Z} + I)/I| = |\mathbb{Z}/b_1\mathbb{Z}| = b_1$.

(iii) Por el teorema 2.6, se tiene que $\mathbb{Z} + I$ es un orden en $\mathcal{O}_F$, pues $|\mathcal{O}_F/(\mathbb{Z} + I)| = \dfrac{N(I)}{b_1} < \infty$.

(iv) Si $N(I) = p$, entonces $b_1 = p$ y así

$$p = N(I) = |\mathcal{O}_F/I| = |\mathcal{O}_F/(\mathbb{Z} + I)| \cdot |(\mathbb{Z} + I)/I| = |\mathcal{O}_F/(\mathbb{Z} + I)| \cdot p$$

Por lo tanto, $|\mathcal{O}_F/(\mathbb{Z} + I)| = 1$, es decir $\mathbb{Z} + I = \mathcal{O}_F$. □

La parte (iv) del lema anterior nos dice que si un ideal de $\mathcal{O}_F$ tiene norma p un primo racional, entonces $\mathcal{O}_F$ toma diferentes expresiones. Tal como lo podemos ver en el siguiente ejemplo.

Ejemplo 2.11. *Sea $\mathcal{O}_F = \mathbb{Z}[i]$ el anillo de enteros de $F = \mathbb{Q}(i)$. Sabemos que en $\mathbb{Z}[i]$ los primos racionales p que son congruentes con 1 módulo 4 ($p \equiv 1 \pmod 4$) se descomponen digamos $p = (a + bi)(a - bi)$, con $a + bi$ y $a - bi$ primos en $\mathbb{Z}[i]$.*

Si tomo $I = \langle a + bi\rangle$ ó $I = \langle a - bi\rangle$, entonces $N(I) = p$ un primo racional. Por lo tanto, podemos ver que $\mathcal{O}_F$ toma diferentes expresiones, algunas de las cuales son : $\mathbb{Z} + \langle 1 + i\rangle = \mathbb{Z} + \langle 1 + 2i\rangle = \mathbb{Z} + \langle 4 + i\rangle = \mathcal{O}_F$

Lema 2.12. *Sean I, J ideales no cero de $\mathcal{O}_F$. Entonces:*

(i) $(\mathbb{Z} + I) + (\mathbb{Z} + J) = \mathbb{Z} + (I + J)$.
(ii) $(\mathbb{Z} + I) \cap (\mathbb{Z} + J) \supseteq \mathbb{Z} + (I \cap J)$.
(iii) *Si* mcd$(N(I), N(J)) = 1$*, entonces* $(\mathbb{Z} + I) \cap (\mathbb{Z} + J) = \mathbb{Z} + (I \cap J) = \mathbb{Z} + IJ$.

DEMOSTRACIÓN. (i) Sea $x \in (\mathbb{Z} + I) + (\mathbb{Z} + J)$. Entonces $x = m + n$, con $m \in \mathbb{Z} + I$ y $n \in \mathbb{Z} + J$, de donde se tiene

$$m = m_1 + i \text{ con } m_1 \in \mathbb{Z}\,,\ i \in I,$$
$$n = n_1 + j \text{ con } n_1 \in \mathbb{Z}\,,\ j \in J.$$

Así, $x = m + n = (m_1 + n_1) + (i + j)$ con $m_1 + n_1 \in \mathbb{Z}$, $i + j \in I + J$, de lo anterior $x \in \mathbb{Z} + (I + J)$, es decir $(\mathbb{Z} + I) + (\mathbb{Z} + J) \subseteq \mathbb{Z} + (I + J)$.

Ahora sea $x \in \mathbb{Z} + (I + J)$. Entonces $x = m + l$, con $m \in \mathbb{Z}$, $l \in I + J$, de donde $l = i + j$ con $i \in I$, $j \in J$. Así,

$x = (m+0)+(i+j) = (m+i)+(0+j)$ con $m+i \in \mathbb{Z}+I$ y $0+j \in \mathbb{Z}+J$, por lo que $x \in (\mathbb{Z}+I)+(\mathbb{Z}+J)$, es decir $(\mathbb{Z}+I)+(\mathbb{Z}+J) \supseteq \mathbb{Z}+(I+J)$. Por lo tanto, se cumple (i).

(ii) Sea $x \in \mathbb{Z}+(I \cap J)$. Entonces $x = n+l$ con $n \in \mathbb{Z}$, $l \in I \cap J$. De lo anterior, $x = n+l \in \mathbb{Z}+I$ y $x = n+l \in \mathbb{Z}+J$. Así, $x \in (\mathbb{Z}+I) \cap (\mathbb{Z}+J)$, es decir $(\mathbb{Z}+I) \cap (\mathbb{Z}+J) \supseteq \mathbb{Z}+(I \cap J)$.

(iii) Dado que mcd$(N(I), N(J)) = 1$, existen $u, v \in \mathbb{Z}$ tales que $uN(I)+vN(J) = 1$. Sea $x \in (\mathbb{Z}+I) \cap (\mathbb{Z}+J)$. Entonces, $x = z_1 + i = z_2 + j$ para algunos $z_1, z_2 \in \mathbb{Z}$, $i \in I$ y $j \in J$. Así,

$$\begin{aligned} i &= (z_2 - z_1) + j \\ &= (z_2 - z_1)(uN(I) + vN(J)) + j \\ &= (z_2 - z_1)uN(I) + (z_2 - z_1)vN(J) + j. \end{aligned}$$

De lo anterior, $i + (z_1 - z_2)uN(I) = j + (z_2 - z_1)vN(J) \in I \cap J$. Por tanto, $x = z_1 + i = z_1 - (z_1 - z_2)uN(I) + i + (z_1 - z_2)uN(I)$ y, dado que $z_1 - (z_1 - z_2)uN(I) \in \mathbb{Z}$, se cumple $x \in \mathbb{Z}+(I \cap J)$. Así, $(\mathbb{Z}+I) \cap (\mathbb{Z}+J) = \mathbb{Z}+(I \cap J)$. Como $mcd(N(I), N(J)) = 1$, entonces I y J son primos relativos y, por la proposición 1.63, $\mathbb{Z}+(I \cap J) = \mathbb{Z}+IJ$. □

A continuación vamos a definir un ideal muy importante para la teoría que estamos desarrollando.

Definición 2.13. (i) *El* **conductor** *de un orden $\mathcal{O}$ en el campo de números F es*

$$\mathfrak{f} = \{x \in F : x\mathcal{O}_F \subseteq \mathcal{O}\}$$

(ii) *Diremos que I es un* **ideal conductor** *si existe algún orden en F con conductor I.*

Como $1 \in \mathcal{O}_F$, se tiene que $\mathfrak{f}$ es un subconjunto de $\mathcal{O}$ y por tanto

$$\mathfrak{f} = \{x \in \mathcal{O}_F : x\mathcal{O}_F \subseteq \mathcal{O}\} = \{x \in \mathcal{O} : x\mathcal{O}_F \subseteq \mathcal{O}\}$$

Ejemplo 2.14. *Sea $F = \mathbb{Q}(i)$, entonces $\mathcal{O}_F = \mathbb{Z}[i]$. Veremos que $\mathcal{O} = \mathbb{Z}[2i] = \mathbb{Z}+2i\mathbb{Z}$ es un orden y que $\mathfrak{f} = \{2m+2ni : m, n \in \mathbb{Z}\}$ es su conductor.*

DEMOSTRACIÓN. Notemos primero $\mathcal{O} \subseteq \mathcal{O}_F$. Dado que $\mathcal{O}_F/\mathcal{O} = \{\mathcal{O}, i+\mathcal{O}\}$, se tiene $|\mathcal{O}_F/\mathcal{O}| = 2$, por el teorema 2.6, $\mathcal{O}$ es un orden.

Vamos a demostrar que para $x \in \mathcal{O}$, se cumple $x\mathcal{O}_F \subseteq \mathcal{O}$ si y sólo si $xi \in \mathcal{O}$. Supongamos que $x\mathcal{O}_F \subseteq \mathcal{O}$, entonces dado que $i \in \mathcal{O}_F$, $xi \in \mathcal{O}$.

Ahora supongamos que $xi \in \mathcal{O}$ y sea $y \in x\mathcal{O}_F$, es decir $y = x(c+di) = xc + d(xi)$, para $c, d \in \mathbb{Z}$ y como $xi \in \mathcal{O}$, tenemos $xi = m + n2i$, con $m, n \in \mathbb{Z}$. Por tanto,

$$y = (a+b2i)c + d(m+n2i)$$

dado que $x \in \mathcal{O}$. Así, $y = (ac+dm) + (bc+dn)2i \in \mathcal{O}$, es decir $x\mathcal{O}_F \subseteq \mathcal{O}$.

Sea $x = a+2ni \in \mathcal{O}$, con $a, n \in \mathbb{Z}$, por la observación anterior tenemos $x \in \mathfrak{f}$ si y sólo si $xi = -2n+ai = l+2mi$, para algunos $l, m \in \mathbb{Z}$, de donde $a = 2m$. Así, $x = 2m+2ni$, es decir, $\mathfrak{f} = \{2k+2bi : k, b \in \mathbb{Z}\}$. □

Lema 2.15. *Sea $\mathcal{O}$ un orden en F con conductor $\mathfrak{f}$. Entonces:*

(i) *$\mathfrak{f}$ es un ideal de $\mathcal{O}$ y de $\mathcal{O}_F$.*
(ii) *Sea I un ideal de $\mathcal{O}_F$. Entonces $I \subseteq \mathcal{O}$ si y sólo si $I \subseteq \mathfrak{f}$.*
(iii) *$\mathbb{Z} + \mathfrak{f}$ es el orden más chico en $\mathcal{O}_F$ con conductor $\mathfrak{f}$.*

DEMOSTRACIÓN. (i) Dado que $1 \in \mathcal{O}_F$, por la definición de conductor, $\mathfrak{f} \subseteq \mathcal{O}$. Es fácil mostrar que $\mathfrak{f}$ es un subgrupo aditivo. Sean $a \in \mathfrak{f}$ y $b \in \mathcal{O}_F$. Entonces $(ab)\mathcal{O}_F = a(b\mathcal{O}_F) \subseteq a\mathcal{O}_F$, dado que $b\mathcal{O}_F \subseteq \mathcal{O}_F$. También tenemos $a\mathcal{O}_F \subseteq \mathcal{O}$, dado que $a \in \mathfrak{f}$. Así, $(ab)\mathcal{O}_F \subseteq \mathcal{O}$, es decir $ab \in \mathfrak{f}$. Por lo tanto, $\mathfrak{f}$ es un ideal de $\mathcal{O}_F$. De manera análoga $\mathfrak{f}$ es un ideal de $\mathcal{O}$.

(ii) Sea I un ideal de $\mathcal{O}_F$ tal que $I \subseteq \mathcal{O}$, entonces $I\mathcal{O}_F = I \subseteq \mathcal{O}$, por tanto $I \subseteq \mathfrak{f}$. Inversamente, si I es un ideal de $\mathcal{O}_F$ con $I \subseteq \mathfrak{f}$, tenemos $I \subseteq \mathfrak{f} \subseteq \mathcal{O}$.

(iii) Por el lema 2.10 (iii), $\mathbb{Z} + \mathfrak{f}$ es un orden en F. Como $\mathfrak{f} \subseteq \mathcal{O}$ y $\mathbb{Z} \subseteq \mathcal{O}$, tenemos $\mathbb{Z} + \mathfrak{f} \subseteq \mathcal{O}$. Por lo tanto, $\mathbb{Z} + \mathfrak{f}$ es el orden más chico que contiene a $\mathfrak{f}$.

Sólo falta mostrar que $\mathfrak{f}$ es el conductor de $\mathbb{Z} + \mathfrak{f}$. Supongamos que $\mathfrak{f}_1$ es el conductor de $\mathbb{Z} + \mathfrak{f}$, entonces $\mathfrak{f}_1$ es un ideal de $\mathcal{O}_F$ con $\mathfrak{f}_1 \subseteq \mathbb{Z} + \mathfrak{f} \subseteq \mathcal{O}$, y por (ii), $\mathfrak{f}_1 \subseteq \mathfrak{f}$. Por otro lado, $\mathfrak{f} \subseteq \mathbb{Z} + \mathfrak{f}$ y por (ii), $\mathfrak{f} \subseteq \mathfrak{f}_1$, es decir $\mathfrak{f}$ es el conductor de $\mathbb{Z} + \mathfrak{f}$. □

En el siguiente ejemplo veremos que no todos los ideales de $\mathcal{O}$ que están contenidos en $\mathfrak{f}$ son ideales en $\mathcal{O}_F$

Ejemplo 2.16. *Sean $F = \mathbb{Q}[i]$, $\mathcal{O}_F = \mathbb{Z}[i]$ y $\mathcal{O} = \mathbb{Z}[2i]$. Entonces el ideal $2\mathcal{O} = \mathbb{Z}2 + \mathbb{Z}4i$ de $\mathcal{O}$ está contenido en $\mathfrak{f} = \mathbb{Z}2 + \mathbb{Z}2i$, pero $2\mathcal{O}$ no es un ideal en $\mathcal{O}_F$, pues $2 \in 2\mathcal{O}$ e $i \in \mathcal{O}_F$, pero $2i \notin 2\mathcal{O}$.*

Lema 2.17. *Sean $F \neq \mathbb{Q}$ un campo de números, I un ideal no cero de $\mathcal{O}_F$ y $\mathcal{O} = \mathbb{Z} + I$ un orden de F con conductor $\mathfrak{f}$, con $I \cap \mathbb{Z} = m\mathbb{Z}$. Entonces, los ideales de $\mathcal{O}$ que contienen a I son aquellos de la forma $d\mathbb{Z} + I$, para algún $d|m$.*

DEMOSTRACIÓN. Veremos que $d\mathbb{Z} + I$, con $d|m$ es ideal de $\mathcal{O}$. Por un lado, es fácil ver que $d\mathbb{Z} + I$ es un subgrupo aditivo de $\mathcal{O}$. Por otro lado, sean $x \in d\mathbb{Z} + I$ y $y \in \mathcal{O} = \mathbb{Z} + I$, entones $x = dn_0 + l_0$, con $n_0 \in \mathbb{Z}$, $l_0 \in I$ y $y = n_1 + l_1$, con $n_1 \in \mathbb{Z}$, $l_1 \in I$, por tanto

$$\begin{aligned} xy &= (dn_0 + l_0)(n_1 + l_1) \\ &= dn_0n_1 + dn_0l_1 + l_0n_1 + l_0l_1 \\ &= d(n_0n_1) + (dn_0l_1 + l_0n_1 + l_0l_1). \end{aligned}$$

Así, $xy \in d\mathbb{Z} + I$, es decir $d\mathbb{Z} + I$ es ideal de $\mathcal{O}$.

Como $(\mathbb{Z} + I)/I \cong \mathbb{Z}/m\mathbb{Z}$, tenemos que los anteriores son todos los ideales de $\mathcal{O}$ que contienen a I.

Por tanto, cualquier ideal de $\mathcal{O}$ que contiene a I tiene la forma $d\mathbb{Z} + I$, con $d|m$. □

Teorema 2.18. *Sean I un ideal de $\mathcal{O}_F$ y $\mathcal{O}$ un orden con conductor $\mathfrak{f}$ tal que $\mathcal{O} = \mathbb{Z} + I$. Entonces $\mathfrak{f} = k\mathbb{Z} + I$, donde $k =$*exp$(\mathcal{O}_F/\mathcal{O})$*, (el exponente* exp$(G)$ *de un grupo G es el menor elemento k tal que para todo $g \in G$, $kg = e$, donde e es el neutro del grupo).*

DEMOSTRACIÓN. Como $k = \exp(\mathcal{O}_F/\mathcal{O})$, tenemos $k\mathcal{O}_F \subseteq \mathcal{O}$, es decir $k \in \mathfrak{f}$, de donde $k\mathbb{Z} + I \subseteq \mathfrak{f}$ y también $I \subseteq \mathfrak{f}$ y por el lema anterior, $\mathfrak{f} = d_1\mathbb{Z} + I$, para algún $d_1|m$. Así, $k\mathbb{Z} + I \subseteq d_1\mathbb{Z} + I$, en consecuencia $k\mathbb{Z} \subseteq d_1\mathbb{Z}$ y $d_1 \leq k$.

Si $d_1 < k$, entonces existe algún $\beta \in \mathcal{O}_F$ tal que $d_1\beta \notin \mathcal{O}$, es decir $d_1 \notin \mathfrak{f}$, lo cual es una contradicción. Por lo tanto, $d_1 = k$. □

Ejemplo 2.19. *Sean* $F = \mathbb{Q}(\sqrt[3]{7})$, $\mathcal{O}_F = \mathbb{Z}[\sqrt[3]{7}] = \mathbb{Z} + \mathbb{Z}(\sqrt[3]{7}) + \mathbb{Z}(\sqrt[3]{7})^2$ *y* $\mathcal{O} = \mathbb{Z} + P^2$, *donde* $P = \langle 3, 1 - \sqrt[3]{7}\rangle$. *Encontraremos al conductor de* $\mathcal{O}$.

DEMOSTRACIÓN. Como $P^2 \cap \mathbb{Z} = 3\mathbb{Z}$, tenemos $\mathcal{O}/P^2 = (\mathbb{Z} + P^2)/P^2 \cong \mathbb{Z}/3\mathbb{Z}$, de donde $|\mathcal{O}/P^2| = 3$, lo que significa que P^2 es un ideal primo en $\mathcal{O}$.

Observemos que $|\mathcal{O}_F/P^2| = N(P)^2 = 9$, por consiguiente $|\mathcal{O}_F/\mathcal{O}| = 3$, un primo racional, entonces $\mathcal{O}_F/\mathcal{O}$ tiene exponente 3. Por el teorema anterior, el conductor de $\mathcal{O}$ es $\mathfrak{f} = 3\mathbb{Z} + P^2 = P^2$. □

Adicionalmente P^2 no es un ideal principal en $\mathcal{O}_F$ dado que $N(P^2) = 9$ y ningún elemento de $\mathcal{O}_F$ tiene norma ± 9, pues

$$N_{F/\mathbb{Q}}(a + b\sqrt[3]{7} + c\sqrt[3]{49}) = a^3 + 7b^3 + 49c^3 - 3 \cdot 7abc. \tag{4}$$

Si $a + b\sqrt[3]{7} + c\sqrt[3]{49}$ tuviera norma ± 9, en (4) reducimos módulo 7 y tenemos $a^3 \equiv \pm 9 \pmod 7$, lo cual es una contradicción, ya que ± 9 no es un cubo módulo 7.

Un caso particular es considerar $I = c\mathcal{O}_F$, con $c \in \mathbb{Z}^+$ y $[F : \mathbb{Q}] \geqslant 2$

Proposición 2.20. *Sea* F *un campo de números, con* $[F : \mathbb{Q}] = n \geq 2$ *y* $\mathcal{O}_F$ *su anillo de enteros. Si* $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_F$ *con* $c \in \mathbb{Z}^+$, *entonces* $\mathfrak{f} = c\mathcal{O}_F$ *es el conductor de* $\mathcal{O}$.

DEMOSTRACIÓN. Por el teorema 2.18, $\mathfrak{f} = k\mathbb{Z} + c\mathcal{O}_F$ es la forma que tiene el conductor de $\mathcal{O}$. Determinemos a k, el exponente del grupo $\mathcal{O}_F/\mathcal{O}$.

Escribimos $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n$, donde $\{e_i\}_{i=1}^n$ es una base entera y $e_1 = 1$, entonces $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}ce_2 + \cdots + \mathbb{Z}ce_n$.

Así,

$$\mathcal{O}_F/\mathcal{O} \cong (\mathbb{Z}/c\mathbb{Z})^{n-1},$$

que como grupo abeliano tiene exponente c.

Concluimos que $k = c$, es decir $\mathfrak{f} = c\mathbb{Z} + c\mathcal{O}_F = c\mathcal{O}_F$. □

Proposición 2.21. *Si* F *es un campo cuadrático, entonces todo orden* $\mathcal{O}$ *en* F *es de la forma* $\mathbb{Z} + c\mathcal{O}_F$ *donde* $c =$índ$(\mathcal{O})$.

DEMOSTRACIÓN. Sea $F = \mathbb{Q}(\alpha)$ con α un entero algebraico, entonces $\mathcal{O}_F = \mathbb{Z} + \alpha\mathbb{Z}$ y sabemos que todo orden es de la forma $\mathcal{O} = \mathbb{Z} + \beta\mathbb{Z} \subseteq \mathcal{O}_F$, para algún β entero algebraico. Así

$$\begin{aligned} \mathcal{O} &= \mathbb{Z} + \beta\mathbb{Z} \\ &= \mathbb{Z} + (a + c\alpha)\mathbb{Z} \\ &= \mathbb{Z} + c\alpha\mathbb{Z}. \\ &= \mathbb{Z} + (c\alpha\mathbb{Z} + c\mathbb{Z}) \\ &= \mathbb{Z} + c\mathcal{O}_F. \end{aligned}$$

Ahora como $\mathcal{O}_F/\mathcal{O} = (\mathbb{Z} + \alpha\mathbb{Z})/(\mathbb{Z} + c\alpha\mathbb{Z}) \cong \mathbb{Z}/c\mathbb{Z}$, tenemos $c = |\mathcal{O}_F/\mathcal{O}|$. □

Para órdenes en campos cuadráticos el nombre *conductor* e *índice* significan lo mismo.

El siguiente es ejemplo de un ideal conductor que no es principal en una extensión de grado 3.

Ejemplo 2.22. *Sea* $F = \mathbb{Q}(\sqrt[3]{19})$. *Al final de la sección 1.5, vimos que* $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{19} + \mathbb{Z}\dfrac{1+\sqrt[3]{19}+\sqrt[3]{361}}{3}$.

Tomamos el orden $\mathcal{O} = \mathbb{Z}[\sqrt[3]{19}] = \mathbb{Z} + \mathbb{Z}\sqrt[3]{19} + \mathbb{Z}\sqrt[3]{361}$. *Veamos quién es el conductor de* $\mathcal{O}$.

Sea $x = a + b\sqrt[3]{19} + c\sqrt[3]{361} \in \mathcal{O}$, y queremos $x\mathcal{O}_F \subseteq \mathcal{O}$. Pero $x\mathcal{O}_F \subseteq \mathcal{O}$ si y sólo si $xe_i \in \mathcal{O}$, donde e_1, e_2, e_3 es una base entera de $\mathcal{O}_F$.

Si $e_1 = 1$, $e_2 = \sqrt[3]{19}$ y $e_3 = \dfrac{1+\sqrt[3]{19}+\sqrt[3]{361}}{3}$, obtenemos $\dfrac{a+b+c}{3} \in \mathbb{Z}$, es decir $a+b+c = 3d$, $d \in \mathbb{Z}$, lo que significa $x = a(1-\sqrt[3]{361}) + b(\sqrt[3]{19} - \sqrt[3]{361}) + d \cdot 3\sqrt[3]{361}$. Por tanto, el conductor de $\mathcal{O}$ es

$$\mathfrak{f} = \mathbb{Z}(1-\sqrt[3]{361}) + \mathbb{Z}(\sqrt[3]{19} - \sqrt[3]{361}) + \mathbb{Z} \cdot 3\sqrt[3]{361}.$$

Veamos que $\mathfrak{f}$ no es principal en $\mathcal{O}_F$.

Expresamos a $(1-\sqrt[3]{361}), (\sqrt[3]{19} - \sqrt[3]{361})$ y $3\sqrt[3]{361}$ en términos de la base entera $\{e_1, e_2, e_3\}$

$$\begin{aligned}
1 - \sqrt[3]{361} &= 2 \cdot 1 + 1 \cdot \sqrt[3]{19} - 3\frac{1+\sqrt[3]{19}+\sqrt[3]{361}}{3} \\
\sqrt[3]{19} - \sqrt[3]{361} &= 1 \cdot 1 + 2 \cdot \sqrt[3]{19} - 3\frac{1+\sqrt[3]{19}+\sqrt[3]{361}}{3} \\
3\sqrt[3]{361} &= 0 \cdot 1 + 3 \cdot \sqrt[3]{19} - 0\frac{1+\sqrt[3]{19}+\sqrt[3]{361}}{3}
\end{aligned}$$

de donde tenemos la matriz

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 3 \\ -3 & -3 & 0 \end{pmatrix}$$

la cual tiene determinante 9. Así, $|\mathcal{O}_F/\mathfrak{f}| = 9$.

Ahora supongamos que $\mathfrak{f} = \alpha\mathcal{O}_F$ para algún $\alpha \in \mathfrak{f}$, entonces $9 = |\mathcal{O}_F/\alpha\mathcal{O}_F| = |N_{F/\mathbb{Q}}(\alpha)|$. Si $\alpha = a + b\sqrt[3]{19} + c\sqrt[3]{361}$ con $a, b, c \in \mathbb{Z}$,

$$N_{F/\mathbb{Q}}(\alpha) = a^3 + 19b^3 + 19^2c^3 - 3 \cdot 19abc. \tag{5}$$

Reducimos módulo 19 en (5) y tenemos $a^3 \equiv 9 \pmod{19}$, lo cual es una contradicción, ya que 9 no es un cubo módulo 19.

A continuación veremos dos órdenes con el mismo conductor

Ejemplo 2.23. *Sea* $F = \mathbb{Q}(\sqrt[3]{2})$ *con anillo de enteros* $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}$. *Veremos que* $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}2\sqrt[3]{4}$ *y* $\mathcal{O}' = \mathbb{Z} + \mathbb{Z}2\sqrt[3]{2} + \mathbb{Z}2\sqrt[3]{4}$ *tienen como conductor a* $2\mathcal{O}_F = \mathbb{Z}2 + \mathbb{Z}2\sqrt[3]{2} + \mathbb{Z}2\sqrt[3]{4}$.

DEMOSTRACIÓN. Como $\mathcal{O}' = \mathbb{Z} + 2\mathcal{O}_F$, por la proposición 2.20, $2\mathcal{O}_F$ es el conductor de $\mathcal{O}'$.

Ahora veremos que $2\mathcal{O}_F$ es conductor de $\mathcal{O}$, es decir $2\mathcal{O}_F = \{x \in \mathcal{O} : x\mathcal{O}_F \subseteq \mathcal{O}\}$. Sean $y = 2a_1 + 2b_1\sqrt[3]{2} + 2c_1\sqrt[3]{4} \in 2\mathcal{O}_F$ y $z = a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4} \in \mathcal{O}_F$ con $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z}$. Tenemos

$$\begin{aligned} yz &= (2a_1 + 2b_1\sqrt[3]{2} + 2c_1\sqrt[3]{4})(a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}) \\ &= (2a_1a_2 + 4c_1b_2 + 4b_1c_2) + (2b_1a_2 + 2a_1b_2 + 2c_1c_2)\sqrt[3]{2} \\ &\quad +(c_1a_2 + b_1b_2 + a_1c_2)2\sqrt[3]{4} \in \mathcal{O}. \end{aligned}$$

De lo anterior $2\mathcal{O}_F \subseteq \{x \in \mathcal{O} : x\mathcal{O}_F \subseteq \mathcal{O}\}$.

Si $y \in \{x \in \mathcal{O} : x\mathcal{O}_F \subseteq \mathcal{O}\}$, tenemos $y = a + b\sqrt[3]{2} + 2c\sqrt[3]{4}$ con $a, b, c \in \mathbb{Z}$, además $y\mathcal{O}_F \subseteq \mathcal{O}$ si y sólo si $y\sqrt[3]{2}, y\sqrt[3]{4} \in \mathcal{O}$, así $a = 2t$ con $t \in \mathbb{Z}$ y $b = 2t'$ con $t' \in \mathbb{Z}$, es decir, $y \in 2\mathcal{O}_F$ y por tanto, $2\mathcal{O}_F \supseteq \{x \in \mathcal{O} : x\mathcal{O}_F \subseteq \mathcal{O}\}$. □

2.2. Ideales primos relativos al conductor

En esta sección se trabajará básicamente en $\mathcal{O}$ un orden en F. Para no confundirnos escribiremos:

i) $\mathcal{O}$-ideal I, para indicar que I es un ideal de $\mathcal{O}$.
ii) $\mathcal{O}_F$-ideal I, para indicar que I es un ideal de $\mathcal{O}_F$.

También veremos qué propiedades cumplen los ideales que son primos relativos al conductor.

Teorema 2.24. *Sea $\mathcal{O}$ un orden en F con conductor $\mathfrak{f}$. Entonces para cada $\mathcal{O}$-ideal I primo relativo al conductor $\mathfrak{f}$ en $\mathcal{O}$, se tiene que $\mathcal{O} = \{x \in F : xI \subseteq I\}$.*

DEMOSTRACIÓN. Sea $y \in \mathcal{O}$. Entonces $y \in F$ y si $a \in I$, tenemos $ya \in I$ pues I es un ideal de $\mathcal{O}$, de donde $y \in \{x \in F : xI \subseteq I\}$ es decir $\mathcal{O} \subseteq \{x \in F : xI \subseteq I\}$.

Ahora sea $y \in F$ tal que $yI \subseteq I$. Como I es un $\mathbb{Z}$-módulo, entonces y es entero sobre $\mathbb{Z}$ es decir $y \in \mathcal{O}_F$. Dado que I y $\mathfrak{f}$ son primos relativos en $\mathcal{O}$ se tiene que $I + \mathfrak{f} = \mathcal{O}$, de donde $m + n = 1$ para algunos $m \in I$ y $n \in \mathfrak{f}$.

Así, $y = y1 = x(m+n) = ym + yn$ con $ym \in I \subseteq \mathcal{O}$ y $yn \in \mathfrak{f} \subseteq \mathcal{O}$, entonces $y \in \mathcal{O}$, es decir, $\mathcal{O} \supseteq \{x \in F : xI \subseteq I\}$.

Por lo tanto $\mathcal{O} = \{x \in F : xI \subseteq I\}$. □

Lema 2.25. *Sea J un $\mathcal{O}$-ideal. Entonces existen ideales primos $P_1, P_2, \ldots, P_r$ de manera que $P_1 \cdots P_r \subseteq J$.*

DEMOSTRACIÓN. Supongamos que no, entonces hay un ideal J tal que no existen ideales primos con las condiciones pedidas y que es maximal entre los ideales para los que esto ocurre.

Notemos que J no puede ser $\mathcal{O}$, ni primo o cumpliría este lema trivialmente. Por tanto, existen ideales I, L tales que $IL \subseteq J$, pero no $I \subseteq J$ ó $L \subseteq J$. Por la maximalidad de J, existen ideales primos $P_1, \ldots, P_s$ y $P_{s+1}, \ldots, P_r$ tales que

$$P_1 \cdots P_s \subseteq J + I \text{ y } P_{s+1} \cdots P_r \subseteq J + L,$$

de donde $P_1 \cdots P_r \subseteq (J + I)(J + L) \subseteq JJ + JI + JL + IL \subseteq J$, lo cual es una contradicción. □

El siguiente lema es muy útil ya que nos dice qué forma tiene el inverso de un ideal fraccionario cuando éste existe.

Lema 2.26. *Sea J un $\mathcal{O}$-ideal fraccionario. Entonces*

(i) *Si J es invertible como un $\mathcal{O}$-ideal fraccionario, entonces su inverso es*

$$J^{-1} = \{x \in F : xJ \subseteq \mathcal{O}\}.$$

(ii) *Si $J \subsetneqq \mathcal{O}$, entonces $\mathcal{O} \subsetneqq J^{-1}$. Esto es, algún $x \notin \mathcal{O}$ satisface $xJ \subseteq \mathcal{O}$.*

DEMOSTRACIÓN. (i) Supongamos que J es invertible como $\mathcal{O}$-ideal fraccionario, y digamos J' es tal que $JJ' = \mathcal{O}$. De lo anterior si $x \in J'$, en particular $xJ \subseteq \mathcal{O}$, es decir $x \in J^{-1}$, de donde $J' \subseteq J^{-1}$. Si multiplicamos por J la contención anterior,

$$\mathcal{O} = JJ' \subseteq JJ^{-1} \subseteq \mathcal{O}, \tag{6}$$

de (6), $\mathcal{O} \subseteq JJ^{-1} \subseteq \mathcal{O}$ es decir $JJ^{-1} = \mathcal{O}$. Ahora multiplicamos por J',

$$J'JJ^{-1} = J'\mathcal{O}, \text{ entonces } \mathcal{O}J^{-1} = J'\mathcal{O},$$

es decir $J^{-1} = J'$.

(ii) Sea M un $\mathcal{O}$-ideal máximo tal que $J \subseteq M$. Entonces $M^{-1} \subseteq J^{-1}$. Basta probar que $\mathcal{O} \subsetneqq M^{-1}$. Sea $x \in M$ no cero, por el lema anterior, sea r el menor natural tal que existen ideales primos para los que $P_1 \cdots P_r \subseteq \langle x \rangle$. Como $\langle x \rangle \subseteq M$ y M es primo, entonces $P_i \subseteq M$ para algún $i = 1, \ldots, r$. Sin perdida de generalidad, supongamos que $P_1 \subseteq M$, como P_1 es máximo, entonces $P_1 = M$ y por la minimalidad de r tenemos $P_2 \cdots P_r \nsubseteq \langle x \rangle$. Tomamos pues un elemento $y \in P_2 \cdots P_r \setminus \langle x \rangle$.

Claramente $yM \subseteq \langle x \rangle$, luego $yx^{-1}M \subseteq x^{-1}\langle x \rangle = \mathcal{O}$, es decir $yx^{-1} \in M^{-1}$. Por otra parte $y \notin \langle x \rangle = x\mathcal{O}$, de donde $yx^{-1} \notin \mathcal{O}$. Así, $\mathcal{O} \subsetneqq M^{-1}$. □

Teorema 2.27. *Sea P un $\mathcal{O}$-ideal primo. Entonces las siguientes afirmaciones son equivalentes.*

(i) *P es invertible como un $\mathcal{O}$-ideal fraccionario.*

(ii) $\mathcal{O} = \{x \in F : xP \subseteq P\}$.

DEMOSTRACIÓN. Supongamos que P es invertible como un $\mathcal{O}$-ideal, además $\mathcal{O} \subseteq \{x \in F : xP \subseteq P\}$ para cualquier ideal de $\mathcal{O}$.

Sea $y \in \{x \in F : xP \subseteq P\}$, entonces $yP \subseteq P$, multiplicamos por P^{-1}, $yPP^{-1} \subseteq PP^{-1}$, de donde $y\mathcal{O} \subseteq \mathcal{O}$ y dado que $1 \in \mathcal{O}$, se tiene $y \in \mathcal{O}$ y por tanto $\{x \in F : xP \subseteq P\} \subseteq \mathcal{O}$. Así, $\mathcal{O} = \{x \in F : xP \subseteq P\}$.

Inversamente supongamos que P no es invertible como un $\mathcal{O}$-ideal. Por el lema 2.26 (ii), existe $y \in F$ tal que $y \notin \mathcal{O}$ y $yP \subseteq \mathcal{O}$, lo que implica

$$P \subseteq (\mathcal{O} + y\mathcal{O})P = P + yP \subseteq \mathcal{O}$$

es decir,

$$P \subseteq (\mathcal{O} + y\mathcal{O})P \subseteq \mathcal{O},$$

entonces $(\mathcal{O} + y\mathcal{O})P = P$ ó $(\mathcal{O} + y\mathcal{O})P = \mathcal{O}$.

Como P no es invertible, tenemos $(\mathcal{O} + y\mathcal{O})P = P$ y, en particular, $yP \subseteq P$, es decir, $y \in \{x \in F : xP \subseteq P\}$. Por tanto, $\mathcal{O} \neq \{x \in F : xP \subseteq P\}$. □

En general, si el ideal que tomamos en $\mathcal{O}$ no es primo, la afirmación (ii) del teorema anterior no implica (i).

Ejemplo 2.28. *Sea $F = \mathbb{Q}(\sqrt[3]{2})$, con anillo de enteros $\mathcal{O}_F = \mathbb{Z}[\sqrt[3]{2}] = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}(\sqrt[3]{4})$ y tomamos el orden $\mathcal{O} = \mathbb{Z} + 2\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}2\sqrt[3]{2} + \mathbb{Z}2(\sqrt[3]{4})$. Veremos que el teorema anterior no se cumple para el $\mathcal{O}$-ideal $J = \mathbb{Z}8 + \mathbb{Z}2\sqrt[3]{2} + \mathbb{Z}2(\sqrt[3]{4})$.*

DEMOSTRACIÓN. Claramente

$$\mathcal{O}/J = (\mathbb{Z} + \mathbb{Z}2\sqrt[3]{2} + \mathbb{Z}2(\sqrt[3]{4}))/(\mathbb{Z}8 + \mathbb{Z}2\sqrt[3]{2} + \mathbb{Z}2(\sqrt[3]{4})) \cong \mathbb{Z}/8\mathbb{Z},$$

entonces J no es un ideal primo de $\mathcal{O}$.

Veremos que $\{x \in F : xJ \subseteq J\} = \mathcal{O}$. Sea $y \in \mathcal{O}$, como J es un ideal de $\mathcal{O}$, tenemos $yJ \subseteq J$, es decir $y \in \{x \in F : xJ \subseteq J\}$.

Si $y \in \{x \in F : xJ \subseteq J\}$, entonces $yJ \subseteq J$. Para $y = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, con $a, b, c \in \mathbb{Q}$ y $2\sqrt[3]{2}, 2\sqrt[3]{4} \in J$, tenemos

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})2\sqrt[3]{2} = 4c + 2a\sqrt[3]{2} + 2b\sqrt[3]{4} \in J = 8\mathbb{Z} + 2\mathbb{Z}\sqrt[3]{2} + 2\mathbb{Z}\sqrt[3]{4},$$

de donde $c \in 2\mathbb{Z}$ y $a, b \in \mathbb{Z}$.

Y también $(a + b\sqrt[3]{2} + c\sqrt[3]{4})2\sqrt[3]{4} = 4b + 4c\sqrt[3]{2} + 2a\sqrt[3]{4} \in J = 8\mathbb{Z} + 2\mathbb{Z}\sqrt[3]{2} + 2\mathbb{Z}\sqrt[3]{4}$, de donde $b \in 2\mathbb{Z}$. De lo anterior $y \in \mathcal{O}$.

Ahora demostraremos que $JJ^{-1} \neq \mathcal{O}$.

Para este caso $J^{-1} = \left\{a + b\sqrt[3]{2} + \frac{c}{2}\sqrt[3]{4} : a, b, c \in \mathbb{Z}\right\}$, ya que si $8d + 2e\sqrt[3]{2} + 2f\sqrt[3]{4} \in J$, entonces $(a + b\sqrt[3]{2} + \frac{c}{2}\sqrt[3]{4})(8d + 2e\sqrt[3]{2} + 2f\sqrt[3]{4}) = (8ad + 4bf + 2ce) + 2(ae + 4bd + cf)\sqrt[3]{2} + 2(af + be + 2cd)\sqrt[3]{4} \in \mathcal{O}$. Y también $J^{-1} = \frac{1}{4}(4\mathbb{Z} + 4\mathbb{Z}\sqrt[3]{2} + 2\mathbb{Z}\sqrt[3]{4})$, es decir J^{-1} es un ideal fraccionario de $\mathcal{O}$.

Notemos que $1 \notin JJ^{-1}$, pues de lo contrario a, b ó c no serían enteros racionales, por tanto $JJ^{-1} \neq \mathcal{O}$. □

Teorema 2.29. *Un ideal de $\mathcal{O}$ que es primo relativo al conductor, es producto de ideales primos invertibles.*

DEMOSTRACIÓN. Sea J un ideal de $\mathcal{O}$ tal que $J + \mathfrak{f} = \mathcal{O}$. Por el teorema 2.24, $\mathcal{O} = \{x \in F : xJ \subseteq J\}$. Hay dos casos; J es un ideal primo o no lo es.

Si J es ideal primo, por el teorema 2.27, J es invertible como $\mathcal{O}$-ideal fraccionario.

Ahora consideremos el caso cuando J no es ideal primo y $J \neq \mathcal{O}$. Sea M_0 un $\mathcal{O}$-ideal máximo tal que $J \subseteq M_0$, entonces $\mathcal{O} = J + \mathfrak{f} \subseteq M_0 + \mathfrak{f}$, es decir $M_0 + \mathfrak{f} = \mathcal{O}$. Dado que M_0 es máximo, luego es primo y, por los teoremas 2.24 y 2.27, M_0 es invertible. Sea $J_0 = M_0^{-1}J$, entonces $J_0 \subseteq \mathcal{O}$ y $J = M_0J_0$. Como $J \neq M_0$, tenemos $J_0 \neq \mathcal{O}$.

Si $J_0 = M_0J_0$, tendríamos $J_0 = M_0^kJ_0 \subseteq M_0^k$, para todo $k \geq 0$. Luego, $J_0 \subseteq M_0^k$ para todo $k \geq 0$, lo cual es una contradicción al hecho de que $|\mathcal{O}/J_0|$ es finito, y $|\mathcal{O}/M_0^k|$ se hace más grande con cada k. Por lo anterior $J = M_0J_0 \subsetneq J_0$, luego $J_0 + \mathfrak{f} = \mathcal{O}$.

Ahora, J_0 es primo o no lo es. Repitiendo el mismo argumento, tenemos una cadena ascendente

$$J \subsetneq J_0 \subsetneq \cdots \subsetneq J_{n-1} \subsetneq J_n \subsetneq \cdots$$

de ideales en $\mathcal{O}$, con $J_k + \mathfrak{f} = \mathcal{O}$ para cada $k \geq 0$. Como $\mathcal{O}$ es noetheriano, la cadena se debe detener, es decir

$$J \subsetneq J_0 \subsetneq \cdots \subsetneq J_{n-1} \subsetneq J_n$$

con J_n un $\mathcal{O}$-ideal máximo, así que es primo y por tanto invertible.

Finalmente, $J = M_0M_1 \cdots M_{n-1}J_n$ es producto de ideales primos invertibles. □

Corolario 2.30. *Cualquier ideal en $\mathcal{O}$ que es primo relativo al conductor es invertible.*

DEMOSTRACIÓN. Sea J un ideal de $\mathcal{O}$ primo relativo al conductor, por el teorema anterior, $J = P_1P_2 \cdots P_n$, donde cada P_i es un $\mathcal{O}$-ideal primo invertible.

Ahora multiplicamos en ambos lados por el inverso de cada P_i, obteniendo

$$JP_n^{-1} \cdots P_1^{-1} = \mathcal{O}.$$

Por lo tanto, J es invertible. □

El siguiente teorema nos muestra que hay una biyección entre los $\mathcal{O}_F$-ideales primos relativos al conductor y los $\mathcal{O}$-ideales primos relativos al conductor.

Teorema 2.31. *Sea $\mathcal{O}$ un orden en F con conductor $\mathfrak{f}$. Entonces*

(i) *Para cualquier $\mathcal{O}_F$-ideal I que es primo relativo a $\mathfrak{f}$, se tiene que $I \cap \mathcal{O}$ es un $\mathcal{O}$-ideal primo relativo a $\mathfrak{f}$ y el homomorfismo natural de anillos $\mathcal{O}/(I\cap\mathcal{O}) \longrightarrow \mathcal{O}_F/I$ es un isomorfismo.*

(ii) *Si J es un $\mathcal{O}$-ideal que es primo relativo a $\mathfrak{f}$, entonces $J\mathcal{O}_F$ es un $\mathcal{O}_F$-ideal que es primo relativo a $\mathfrak{f}$ y el homomorfismo natural de anillos $\mathcal{O}/J \longrightarrow \mathcal{O}_F/J\mathcal{O}_F$ es un isomorfismo.*

(iii) *Los ideales primos relativos a $\mathfrak{f}$ en $\mathcal{O}_F$ y en $\mathcal{O}$ están en biyección por $I \mapsto I \cap \mathcal{O}$ y $J \mapsto J\mathcal{O}_F$ y, además, estas biyecciones son multiplicativas: $(I \cap \mathcal{O})(I' \cap \mathcal{O}) = II' \cap \mathcal{O}$ y $(J\mathcal{O}_F)(J'\mathcal{O}_F) = JJ'\mathcal{O}_F$.*

DEMOSTRACIÓN. (i) Sea $I \neq \{0\}$ un ideal de $\mathcal{O}_F$ tal que $I + \mathfrak{f} = \mathcal{O}_F$.

Notemos que $\mathcal{O} = \mathcal{O}_F \cap \mathcal{O} = (I + \mathfrak{f}) \cap \mathcal{O} \subseteq (I \cap \mathcal{O}) + (\mathfrak{f} \cap \mathcal{O}) = (I \cap \mathcal{O}) + \mathfrak{f} \subseteq \mathcal{O}$, entonces $\mathcal{O} \subseteq (I \cap \mathcal{O}) + \mathfrak{f} \subseteq \mathcal{O}$. Por lo tanto, $(I \cap \mathcal{O}) + \mathfrak{f} = \mathcal{O}$.

Ahora veremos que

$$\Phi : \mathcal{O}/(I \cap \mathcal{O}) \longrightarrow \mathcal{O}_F/I$$
$$\alpha + (I \cap \mathcal{O}) \mapsto \alpha + I$$

es un isomorfismo.

Observemos que:

$$\begin{aligned} \mathrm{Ker}\Phi &= \{\alpha + (I \cap \mathcal{O}) \in \mathcal{O}/(I \cap \mathcal{O}) : \Phi(\alpha + (I \cap \mathcal{O})) = I\} \\ &= \{\alpha + (I \cap \mathcal{O}) \in \mathcal{O}/(I \cap \mathcal{O}) : \alpha + I = I\} \\ &= \{\alpha + (I \cap \mathcal{O}) \in \mathcal{O}/(I \cap \mathcal{O}) : \alpha \in I\} \\ &= I \cap \mathcal{O}, \end{aligned}$$

por tanto Φ es inyectivo.

Para cada elemento $\alpha + I \in \mathcal{O}_F/I$ existe un elemento en $\mathcal{O}/(I\cap\mathcal{O})$, que es $\alpha+(I\cap\mathcal{O})$ tal que $\Phi(\alpha + (I \cap \mathcal{O})) = \alpha + I$. Por lo tanto, Φ es suprayectivo y es un isomorfismo.

(ii) Sea $J \neq \{0\}$ un ideal de $\mathcal{O}$ tal que $J + \mathfrak{f} = \mathcal{O}$. Como $J + \mathfrak{f} = \mathcal{O}$, tenemos $1 \in J + \mathfrak{f}$. Digamos $1 = j + k$ con $j \in J$ y $k \in \mathfrak{f}$, pero $j \in J\mathcal{O}_F$, por lo que $1 \in J\mathcal{O}_F + \mathfrak{f}$, es decir, $J\mathcal{O}_F + \mathfrak{f} = \mathcal{O}_F$.

Ahora veremos que

$$\Psi : \mathcal{O}/J \longrightarrow \mathcal{O}_F/J\mathcal{O}_F$$

$$\alpha + J \mapsto \alpha + J\mathcal{O}_F$$

es un isomorfismo.

Notemos que:

$$\begin{aligned} \mathrm{Ker}\Psi &= \{\alpha + J \in \mathcal{O}/J : \Psi(\alpha + J) = J\mathcal{O}_F\} \\ &= \{\alpha + J \in \mathcal{O}/J : \alpha + J\mathcal{O}_F = J\mathcal{O}_F\} \\ &= \{\alpha + J \in \mathcal{O}/J : \alpha \in J\mathcal{O}_F\} \\ &= J\mathcal{O}_F \cap \mathcal{O} \end{aligned}$$

y también, $J \subseteq J\mathcal{O}_F \cap \mathcal{O} = J\mathcal{O}_F \cap (J + \mathfrak{f}) = J + (J\mathcal{O}_F \cap \mathfrak{f}) = J + (J\mathcal{O}_F)\mathfrak{f} = J + J\mathfrak{f} = J$, $J \subseteq J\mathcal{O}_F \cap \mathcal{O} \subseteq J$, es decir, $J\mathcal{O}_F \cap \mathcal{O} = J$. Por tanto, $\mathrm{Ker}\Psi = J$ y Ψ es inyectivo.

Para cada elemento $\alpha + J\mathcal{O}_F \in \mathcal{O}_F/J\mathcal{O}_F$ existe un elemento en $\mathcal{O}/J$, que es $\alpha + J$ tal que $\Psi(\alpha + J) = \alpha + J\mathcal{O}_F$. Así, Ψ es suprayectivo y es un isomorfismo.

(iii) Si I es un ideal de $\mathcal{O}_F$ tal que $I + \mathfrak{f} = \mathcal{O}_F$, entonces por (i), $(I \cap \mathcal{O}) + \mathfrak{f} = \mathcal{O}$. Notemos que $I = I\mathcal{O} = I((I \cap \mathcal{O}) + \mathfrak{f}) \subseteq I(I \cap \mathcal{O}) + I\mathfrak{f} = I(I \cap \mathcal{O}) + (I \cap \mathcal{O})\mathfrak{f} \subseteq \mathcal{O}_F(I \cap \mathcal{O}) + (I \cap \mathcal{O})\mathcal{O}_F \subseteq I$, luego $I \subseteq (I \cap \mathcal{O})\mathcal{O}_F \subseteq I$ y $(I \cap \mathcal{O})\mathcal{O}_F = I$.

Si J es un ideal de $\mathcal{O}$ tal que $J + \mathfrak{f} = \mathcal{O}$, por (ii), $J\mathcal{O}_F + \mathfrak{f} = \mathcal{O}_F$ y $J\mathcal{O}_F \cap \mathcal{O} = J$. Veremos que $(J\mathcal{O}_F)(J'\mathcal{O}_F) = JJ'\mathcal{O}_F$.

Notemos que $x \in (J\mathcal{O}_F)(J'\mathcal{O}_F)$ si y sólo si $x = \sum_{i=1}^{n} a_i b_i$ con $a_i \in J\mathcal{O}_F$ y $b_i \in J'\mathcal{O}_F$. Lo que es equivalente a $a_i = \sum_{j=1}^{m} l_{ij}k_{ij}$ con $l_{ij} \in J$, $k_{ij} \in \mathcal{O}_F$ y $b_i = \sum_{g=1}^{z} l'_{ig}k'_{ig}$ con $l'_{ig} \in J'$, $k'_{ig} \in \mathcal{O}_F$.

$$\begin{aligned} x &= \sum_{i=1}^{n} a_i b_i \\ &= \sum_{i=1}^{n} \left[\left(\sum_{j=1}^{m} l_{ij}k_{ij} \right) \left(\sum_{g=1}^{z} l'_{ig}k'_{ig} \right) \right] \\ &= \sum_{i=1}^{n} \left[(l_{i1}k_{i1} + \cdots + l_{im}k_{im}) \left(\sum_{g=1}^{z} l'_{ig}k'_{ig} \right) \right] \\ &= \sum_{i=1}^{n} \left[\left(\sum_{g=1}^{z} l'_{ig}k'_{ig} \right) l_{i1}k_{i1} + \cdots + \left(\sum_{g=1}^{z} l'_{ig}k'_{ig} \right) l_{im}k_{im} \right] \\ &= \sum_{i=1}^{n} \left[\left(\sum_{g=1}^{z} l_{i1}l'_{ig} \right) \left(k_{i1}k'_{ig} \right) + \cdots + \left(\sum_{g=1}^{z} l_{im}l'_{ig} \right) \left(k_{im}k'_{ig} \right) \right]. \end{aligned}$$

Hacemos $t_d = \left(\sum_{g=1}^{z} l_{id}l'_{ig} \right) \in JJ'$ y $r_d = \left(k_{id}k'_{ig} \right) \in \mathcal{O}_F$ para $d = 1 \ldots, m$.

$$\begin{aligned} x &= \sum_{i=1}^{n}\left[\left(\sum_{d=1}^{m} t_d r_d\right)\right] \\ &= \sum_{i=1}^{n}\sum_{d=1}^{m}(t_d r_d) \in (JJ')\mathcal{O}_F. \end{aligned}$$

Por lo tanto, $(J\mathcal{O}_F)(J'\mathcal{O}_F) = JJ'\mathcal{O}_F$.

La identidad $(I\cap\mathcal{O})(I'\cap\mathcal{O}) = II'\cap\mathcal{O}$ se cumple por la biyección entre los $\mathcal{O}$-ideales y los $\mathcal{O}_F$-ideales que son primos relativos al conductor. □

Sabemos que en general si P es un ideal primo de $\mathcal{O}_F$, entonces $P\cap\mathcal{O}$ es un ideal primo de $\mathcal{O}$. La afirmación inversa no siempre sucede. Para ello tenemos el siguiente corolario.

Corolario 2.32. *Un ideal J de $\mathcal{O}$ que es primo relativo al conductor de $\mathcal{O}$, es un ideal primo si y sólo si su extension $J\mathcal{O}_F$ es un ideal primo en $\mathcal{O}_F$.*

DEMOSTRACIÓN.

Por el teorema 2.31, $\mathcal{O}/J$ y $\mathcal{O}_F/J\mathcal{O}_F$ son isomorfos, entonces uno es dominio entero si y sólo si el otro es dominio entero.

J es un ideal primo de $\mathcal{O}$ si y sólo si $\mathcal{O}/J$ es un dominio entero, lo que es equivalente a que $\mathcal{O}_F/J\mathcal{O}_F$ es dominio entero si y sólo si $J\mathcal{O}_F$ es un ideal primo. □

Corolario 2.33. *Si $\beta\in\mathcal{O}$ y el ideal principal $\beta\mathcal{O}_F$ es primo relativo al conductor de $\mathcal{O}$, entonces $\beta\mathcal{O}_F\cap\mathcal{O} = \beta\mathcal{O}$.*

DEMOSTRACIÓN. Como $\beta\mathcal{O}_F$ es un ideal primo relativo al conductor de $\mathcal{O}$, por el teorema 2.31, $\mathcal{O}/(\beta\mathcal{O}_F\cap\mathcal{O})$ es isomorfo a $\mathcal{O}_F/\beta\mathcal{O}_F$, entonces $|\mathcal{O}/(\beta\mathcal{O}_F\cap\mathcal{O})| = |\mathcal{O}_F/\beta\mathcal{O}_F|$. Por otro lado,

$$\begin{aligned} |\mathcal{O}_F/\beta\mathcal{O}_F| &= N(\beta\mathcal{O}_F) \\ &= N(\beta) \text{ pues } \beta\in\mathcal{O} \text{ y la norma de un elemento no depende de la base} \\ &= N(\beta\mathcal{O}) \\ &= |\mathcal{O}/\beta\mathcal{O}|, \end{aligned}$$

de donde $|\mathcal{O}/(\beta\mathcal{O}_F\cap\mathcal{O})| = |\mathcal{O}/\beta\mathcal{O}|$.

Dado que $\beta\mathcal{O}\subseteq\beta\mathcal{O}_F\cap\mathcal{O}\subseteq\mathcal{O}$, $|\mathcal{O}/\beta\mathcal{O}| = |\mathcal{O}/(\beta\mathcal{O}\cap\mathcal{O})|\cdot|(\beta\mathcal{O}\cap\mathcal{O})/\beta\mathcal{O}|$ y, por tanto, $|(\beta\mathcal{O}\cap\mathcal{O})/\beta\mathcal{O}| = 1$. De lo anterior, $\beta\mathcal{O}_F\cap\mathcal{O} = \beta\mathcal{O}$. □

Corolario 2.34. *Sea $\mathcal{O}$ un orden en F con conductor $\mathfrak{f}$. Entonces los $\mathcal{O}$-ideales primos relativos a $\mathfrak{f}$ tienen factorización única en ideales primos que son primos relativos al conductor.*

DEMOSTRACIÓN. Sea J un $\mathcal{O}$-ideal no cero tal que $J+\mathfrak{f} = \mathcal{O}$, por el teorema 2.31, $J\mathcal{O}_F$ es un $\mathcal{O}_F$-ideal con $J\mathcal{O}_F+\mathfrak{f} = \mathcal{O}_F$.

Como $J\mathcal{O}_F$ es un ideal del anillo de enteros de F, tiene factorización única como producto de ideales primos, digamos: $J\mathcal{O}_F = P_1P_2\cdots P_n$, donde los P_i son ideales primos

de $\mathcal{O}_F$ con $P_i + \mathfrak{f} = \mathcal{O}_F$ para cada i, pues $J\mathcal{O}_F \subseteq P_i$. Por el teorema 2.31, $J = J\mathcal{O}_F \cap \mathcal{O}$ y $(P_i \cap \mathcal{O}) + \mathfrak{f} = \mathcal{O}$, entonces

$$\begin{aligned} J &= J\mathcal{O}_F \cap \mathcal{O} \\ &= (P_1 P_2 \cdots P_n) \cap \mathcal{O} \\ &= (P_1 \cap \mathcal{O})(P_2 \cap \mathcal{O}) \cdots (P_n \cap \mathcal{O}). \end{aligned}$$

Por el corolario 2.32, los $P_i \cap \mathcal{O}$ son ideales primos en $\mathcal{O}$. Por lo tanto, J tiene factorización única como producto de ideales primos que son primos relativos al conductor.

□

A continuación presentamos algunos contraejemplos para el teorema 2.31 y los corolarios 2.32, 2.33 y 2.34 si quitamos la condición de que los ideales son primos relativos al conductor. En los siguientes ejemplos, sean $F \neq \mathbb{Q}$ un campo de números y $c > 1$ un entero racional.

Ejemplo 2.35. *Sea $\mathcal{O}$ un orden no maximal de F con conductor $\mathfrak{f}$. Notemos que $\mathfrak{f} \cap \mathcal{O} = \mathfrak{f}$ y $\mathfrak{f}\mathcal{O}_F = \mathfrak{f}$. Por lo anterior, el homomorfismo natural de anillos $\mathcal{O}/\mathfrak{f} \longrightarrow \mathcal{O}_F/\mathfrak{f}$ es inyectivo pero no es suprayectivo dado que $\mathcal{O}$ es más pequeño que $\mathcal{O}_F$.*

En particular, si $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_F$, con $c > 1$ un entero racional y $\mathfrak{f} = c\mathcal{O}_F$, entonces el ideal $J = c\mathcal{O}$ en $\mathcal{O}$ satisface $J\mathcal{O}_F \cap \mathcal{O} = c\mathcal{O}_F \cap \mathcal{O} = c\mathcal{O}_F \supsetneq J$.

Ejemplo 2.36. *Sean p un primo inerte en $\mathcal{O}_F$ y $\mathcal{O} = \mathbb{Z} + p\mathcal{O}_F$. El ideal $J = p\mathcal{O}$ no es primo dado que él no es máximo ($p\mathcal{O} \subsetneq p\mathcal{O}_F \subsetneq \mathcal{O}$), pero $J\mathcal{O}_F = p\mathcal{O}_F$ es primo en $\mathcal{O}_F$ pues p es inerte.*

Ejemplo 2.37. *Si $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_F$ con conductor $c\mathcal{O}_F$, entonces $c \in \mathcal{O}$, pero $c\mathcal{O}_F \cap \mathcal{O} = c\mathcal{O}_F \neq c\mathcal{O}$.*

Ejemplo 2.38. *Sean $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_F$. Para cada factor primo p de c, vamos a demostrar que el $\mathcal{O}$-ideal $p\mathcal{O}$ no es producto de ideales primos que son primos relativos al conductor.*

Si $p\mathcal{O} = P_1 P_2 \cdots P_r$, con P_i un ideal primo en $\mathcal{O}$, primo relativo al conductor para cada $i = 1, \ldots, r$, entonces tendríamos

$$p\mathcal{O}_F = p\mathcal{O}\mathcal{O}_F = (P_1 P_2 \cdots P_r)\mathcal{O}_F = (P_1\mathcal{O}_F)(P_2\mathcal{O}_F) \cdots (P_r\mathcal{O}_F).$$

Por un lado, $P_i\mathcal{O}_F + p\mathcal{O}_F = P_i\mathcal{O}_F$ (pues $p\mathcal{O}_F \subseteq P_i\mathcal{O}_F$, para cada i).

Por otro lado, como $P_i\mathcal{O}_F + c\mathcal{O}_F = \mathcal{O}_F$, tenemos $1 = \alpha + c\beta$, con $\alpha \in P_i\mathcal{O}_F$ y $\beta \in \mathcal{O}_F$ de donde $1 = \alpha + pt\beta \in P_i\mathcal{O}_F + p\mathcal{O}_F$ pues $p|c$. De lo anterior, $P_i\mathcal{O}_F + p\mathcal{O}_F = \mathcal{O}_F$, así, $P_i\mathcal{O}_F = \mathcal{O}_F$, lo cual es una contradicción.

Veamos una aplicación del teorema 2.31 y de sus corolarios.

Lema 2.39. *Sean $F = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_F = \mathbb{Z}[\rho]$, con $\rho = \dfrac{-1 + \sqrt{-3}}{2}$ y $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$, con conductor $\mathfrak{f} = 2\mathbb{Z}[\rho]$. Probaremos que los $\mathcal{O}$-ideales primos relativos a $\mathfrak{f}$, son aquellos de la forma $\alpha\mathcal{O}$ con $N(\alpha)$ impar.*

DEMOSTRACIÓN. Claramente $\mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[-1 + \sqrt{-3}] = \mathbb{Z}[2\rho] = \{a + 2b\rho : a, b \in \mathbb{Z}\}$ y sabemos que $\mathcal{O}_F$ es un dominio de ideales principales.

Tenemos dos afirmaciones:

I Sea $\alpha \in \mathcal{O}_F$. Entonces $\alpha\mathcal{O}_F + 2\mathcal{O}_F = \mathcal{O}_F$ si y sólo si $N(\alpha)$ es impar.
Si $N(\alpha)$ es impar, por la proposición 1.61, $\alpha\mathcal{O}_F + 2\mathcal{O}_F = \mathcal{O}_F$.
Si $\alpha\mathcal{O}_F + 2\mathcal{O}_F = \mathcal{O}_F$, entonces $P_i + 2\mathcal{O}_F = \mathcal{O}_F$ para cada $i \in \{1, \ldots, g\}$, donde los P_i son ideales primos tales que $\alpha\mathcal{O}_F = P_1P_2 \cdots P_g$. Por otro lado, por la proposición 1.70, $2\mathcal{O}_F$ es el único ideal primo que está sobre 2, lo que implica que $N(P_i)$ es impar y por tanto $N(\alpha)$ es impar.

II Todo ideal de $\mathcal{O}_F$ con norma impar tiene generador en $\mathcal{O}$.
Sea $\alpha\mathcal{O}_F$ un ideal con $N(\alpha)$ impar y $\alpha = a + b\rho$, con $a, b \in \mathbb{Z}$. La afirmación II se cumple multiplicando a α por ρ o ρ^2 si es necesario para hacer que el coeficiente de ρ sea par.

Sea $\alpha\mathcal{O}_F$ cualquier ideal de $\mathcal{O}_F$ tal que $N(\alpha)$ es impar, por la afirmación II, $\alpha \in \mathcal{O}$ y por el corolario 2.33, $\alpha\mathcal{O}_F \cap \mathcal{O} = \alpha\mathcal{O}$. De la afirmación I y el teorema 2.31 (i), tenemos que $\alpha\mathcal{O}$ es primo relativo a $2\mathcal{O}_F$. □

Proposición 2.40. *Los elementos de $\mathcal{O} = \mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[2\rho]$ con norma impar tienen factorización única como producto de elementos irreducibles, aunque $\mathbb{Z}[\sqrt{-3}]$ no es DFU (pues en $\mathcal{O}$, $4 = (1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$, las cuales son factorizaciones distintas ya que $U(\mathcal{O}) = \{\pm 1\}$).*

DEMOSTRACIÓN.
Sea $\beta \in \mathcal{O}$ con $N(\beta)$ impar tal que tiene dos factorizaciones distintas, digamos $\beta = p_1p_2 \cdots p_l = q_1q_2 \cdots q_g$, con p_i y $q_i \in \mathcal{O}$ irreducibles. Tenemos tres casos: $l < g$, $l = g$ o $l > g$.

Supongamos $l < g$, como la norma de β es impar, por el lema anterior, $\beta\mathcal{O} + 2\mathcal{O}_F = \mathcal{O}$ y notemos que,

$$(p_1\mathcal{O})(p_2\mathcal{O}) \cdots (p_l\mathcal{O}) = (p_1p_2 \cdots p_l)\mathcal{O} = \beta\mathcal{O} = (q_1q_2 \cdots q_g)\mathcal{O} = (q_1\mathcal{O})(q_2\mathcal{O}) \cdots (q_g\mathcal{O})$$

por el corolario 2.34, $\beta\mathcal{O}$ tiene factorización única, es decir, $p_i\mathcal{O} = q_j\mathcal{O}$ para algún j. Sin perdida de generalidad supongamos $p_1\mathcal{O} = q_1\mathcal{O}, \ldots, p_l\mathcal{O} = q_l\mathcal{O}$ y $(q_{l+1}\mathcal{O}) \cdots (q_g\mathcal{O}) = \mathcal{O} \subseteq (q_j\mathcal{O})$ con $l + 1 \leq j \leq g$, es decir $\mathcal{O} = q_j\mathcal{O}$, lo cual es una contradicción, ya que $q_j\mathcal{O}$ es un ideal primo. Análogamente $l > g$ no es posible, por tanto $l = g$. Así, $p_i\mathcal{O} = q_i\mathcal{O}$ para todo $i = 1, \ldots, l$, lo que implica $p_i = q_iu_i$ donde $u_i \in U(\mathcal{O})$. □

2.3. El grupo de clases en un orden

En esta sección veremos el grupo de clases y el número de clases de un orden.
Los siguientes resultados los podemos encontrar en [**8**].

Lema 2.41. *Sean $\mathcal{O}_F$ el anillo de enteros de F, I y J ideales no cero de $\mathcal{O}_F$. Entonces existe un $\alpha \in I$ tal que $\alpha I^{-1} + J = 1$.*

DEMOSTRACIÓN. Hay que probar que α puede tomarse de modo que ninguno de los ideales primos que dividen a J divida a αI^{-1}, o equivalentemente, que $\alpha \notin IP$ para todo $P|J$.

Sean $P_1, P_2, \ldots, P_r$ los ideales primos distintos que dividen a J. Si $r = 1$ basta tomar $\alpha \in I - IP_1$.

Para $r > 1$, sea $I_i = IP_i^{-1}J$. Supongamos que $IP_i \subseteq I_i = IP_i^{-1}J$ para algún $i \in \{1, \ldots, r\}$, entonces $P_i \subseteq P_i^{-1}J$, de donde $J|P_i^2$, y $r = 1$ lo cual es una contradicción. Así, $IP_i \not\subseteq I_i$ para todo $i = 1, \ldots, r$. Por tanto podemos tomar números $\alpha_i \in I_i \setminus IP_i$ para $i = 1, \ldots, r$ y $\alpha = \alpha_1 + \cdots + \alpha_r$. Como cada $\alpha_i \in I_i \subseteq I$, se cumple $\alpha \in I$.

Si se cumpliera $\alpha \in IP_i$ para algún i, como para $j \neq i$ tenemos $\alpha_j \in I_j \subseteq IP_i$, pues $I_j = IP_j^{-1}P_iP_jK$ para algún ideal K; luego despejando a α_i en la definición de α concluiríamos que $\alpha_i \in IP_i$ en contradicción a la elección que hemos hecho de los α_i. □

Si $\mathcal{O}$ es cualquier orden y $\mathfrak{f}$ cualquier ideal de $\mathcal{O}$, definimos $I_{\mathfrak{f}}(\mathcal{O})$ como el conjunto de todos los ideales J de $\mathcal{O}$ tales que $J + \mathfrak{f} = \mathcal{O}$, es decir

$$I_{\mathfrak{f}}(\mathcal{O}) = \{J \text{ ideal de } \mathcal{O} : J + \mathfrak{f} = \mathcal{O}\}.$$

Si $\mathcal{O}$ es cualquier orden no maximal de un campo de números F, con conductor $\mathfrak{f}$ y $\mathcal{O}_F$ es el orden maximal, el teorema 2.31 establece una biyección entre los ideales de $\mathcal{O}$ primos relativos a $\mathfrak{f}$ y los ideales primos relativos a $\mathfrak{f}$ en $\mathcal{O}_F$. Esta correspondencia en general no conserva el carácter principal de un ideal, es decir, si bien es obvio que la imagen en $\mathcal{O}_F$ de un ideal principal de $\mathcal{O}$ es un ideal principal (con el mismo generador), bien puede ocurrir que un ideal principal de $\mathcal{O}_F$ tenga asociado un ideal no principal de $\mathcal{O}$, debido a que ninguno de sus generadores pertenezca a $\mathcal{O}$. Por ello hemos de distinguir entre los ideales de $\mathcal{O}$ principales en $\mathcal{O}$ (luego también en $\mathcal{O}_F$) de los que sólo son principales en $\mathcal{O}_F$.

En particular, el hecho de que todos los ideales de $\mathcal{O}_F$ sean principales no implica necesariamente que todos los ideales de $\mathcal{O}$ lo sean, ni siquiera los primos relativos con el conductor.

Sean F un campo de números, $\mathcal{O}_F$ su orden maximal y $\mathcal{O}$ cualquier orden de F con conductor $\mathfrak{f}$. Definimos

$$I_{\mathfrak{f}}^*(\mathcal{O}_F) = \{IJ^{-1} : I, J \in I_{\mathfrak{f}}(\mathcal{O}_F)\},$$

es decir, $I_{\mathfrak{f}}^*(\mathcal{O}_F)$ es el subgrupo generado por los ideales de $\mathcal{O}_F$ primos relativos a $\mathfrak{f}$ en el grupo de los ideales fraccionario $\mathcal{J}_F$ (definido en el capítulo 1, sección 3).

Similarmente definimos

$$P_{\mathfrak{f}}(\mathcal{O}) = \{\alpha \in \mathcal{O} : \alpha\mathcal{O}_F + \mathfrak{f} = \mathcal{O}_F\}$$

y

$$P_{\mathfrak{f}}^*(\mathcal{O}) = \{\alpha\mathcal{O}_F\beta^{-1}\mathcal{O}_F : \alpha, \beta \in P_{\mathfrak{f}}(\mathcal{O})\}.$$

De este modo $P_{\mathfrak{f}}^*(\mathcal{O})$ es el subgrupo de $I_{\mathfrak{f}}^*(\mathcal{O}_F)$ generado por los ideales principales de $I_{\mathfrak{f}}(\mathcal{O}_F)$ cuya contracción también es un ideal principal primo relativo a $\mathfrak{f}$.

Definición 2.42. *Llamaremos* **grupo de clases** *de $\mathcal{O}$ al grupo cociente*

$$\mathcal{H}(\mathcal{O}) = I_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O}).$$

Notemos que el grupo de clases $\mathcal{H}(\mathcal{O})$, se define de forma similar al grupo Cl_F, la diferencia es que en $\mathcal{H}(\mathcal{O})$ los ideales con los que estamos trabajando son los ideales primos relativos al conductor.

Proposición 2.43. *Todas las clases de $\mathcal{H}(\mathcal{O})$ tienen un representante en $I_{\mathfrak{f}}(\mathcal{O}_F)$.*

DEMOSTRACIÓN. Claramente para todo $I \in I_{\mathfrak{f}}(\mathcal{O}_F)$ tenemos $I + \mathfrak{f} = \mathcal{O}_F$, entonces existen $\alpha \in I$ y $\beta \in \mathfrak{f}$ tales que $\alpha + \beta = 1$, es decir $\alpha\mathcal{O}_F \in I_{\mathfrak{f}}(\mathcal{O}_F)$.

Por la factorización única existe $J \in I_{\mathfrak{f}}(\mathcal{O}_F)$ tal que $IJ = \alpha\mathcal{O}_F$, tomando clases $[I]^{-1} = [J]$.

Ahora sea $KI^{-1} \in I^*_{\mathfrak{f}}(\mathcal{O}_F)$ cualquiera, luego

$$[KI^{-1}] = [K][I^{-1}] = [K][I]^{-1} = [K][J] = [KJ],$$

si ponemos $L = KJ$, tenemos $[KI^{-1}] = [L]$ y como $J + \mathfrak{f} = \mathcal{O}_F$, se tiene $L + \mathfrak{f} = \mathcal{O}_F$, por lo que $L \in I_{\mathfrak{f}}(\mathcal{O}_F)$. □

Si $I, J \in I_{\mathfrak{f}}(\mathcal{O})$, diremos que $I \sim J$ si y sólo si $I\mathcal{O}_F \sim J\mathcal{O}_F$ en $\mathcal{H}(\mathcal{O})$. Como hay una biyección entre $I_{\mathfrak{f}}(\mathcal{O})$ y $I_{\mathfrak{f}}(\mathcal{O}_F)$, entonces el número de clases que hay en la relación entre los elementos de $I_{\mathfrak{f}}(\mathcal{O})$ es igual a $|\mathcal{H}(\mathcal{O})|$.

Definiremos el **número de clases** de $\mathcal{O}$ como $h_{\mathcal{O}} = |\mathcal{H}(\mathcal{O})|$. A la clase trivial en $\mathcal{O}$ la denotaremos por 1, es decir si I es un $\mathcal{O}$-ideal primo relativo al conductor tal que su clase es la trivial, escribiremos $[I] = 1$.

Proposición 2.44. *Un ideal en $I_{\mathfrak{f}}(\mathcal{O})$, es principal si y sólo si su clase es la trivial.*

DEMOSTRACIÓN. Sea $I \in I_{\mathfrak{f}}(\mathcal{O})$ tal que $[I] = 1$ y sea $I' = I\mathcal{O}_F$, entonces $[I'] = [I\mathcal{O}_F] = [\mathcal{O}_F]$ luego $I' \in P^*_{\mathfrak{f}}(\mathcal{O})$, es decir $I' = \gamma\mathcal{O}_F\beta^{-1}\mathcal{O}_F$, con $\gamma, \beta \in P_{\mathfrak{f}}(\mathcal{O})$.

Así, $\beta\mathcal{O}_F I' = \gamma\mathcal{O}_F$, ahora contraemos $\beta\mathcal{O}I = \gamma\mathcal{O}$, luego existe $\alpha \in I$ tal que $\beta\alpha = \gamma$, de donde $\beta\mathcal{O}\alpha\mathcal{O} = \gamma\mathcal{O}$. El hecho de que $\gamma \in P_{\mathfrak{f}}(\mathcal{O})$ implica $\alpha \in P_{\mathfrak{f}}(\mathcal{O})$ y por la factorización única en $I_{\mathfrak{f}}(\mathcal{O})$, $I = \alpha\mathcal{O}$.

Ahora sea $I \in I_{\mathfrak{f}}(\mathcal{O})$ tal que $I = \alpha\mathcal{O}$, extendiendo y tomando clases $[I\mathcal{O}_F] = [\alpha\mathcal{O}_F] = 1$, por tanto $[I] = 1$. □

Lema 2.45. *Sea $\alpha \in \mathcal{O}_F$ tal que $\alpha\mathcal{O}_F + \mathfrak{f} = \mathcal{O}_F$. Entonces $\alpha\mathcal{O}_F \cap \mathcal{O} = \beta\mathcal{O}$, con $\beta \in \mathcal{O}$ si y sólo si $\alpha = u\beta$ donde u es una unidad de $\mathcal{O}_F$.*

DEMOSTRACIÓN. Si $\alpha = u\beta$, entonces $\alpha\mathcal{O}_F \cap \mathcal{O} = (u\beta)\mathcal{O}_F \cap \mathcal{O} = u\mathcal{O}_F\beta\mathcal{O}_F \cap \mathcal{O} = \beta\mathcal{O}_F \cap \mathcal{O}$, y por el corolario 2.33, $\beta\mathcal{O}_F \cap \mathcal{O} = \beta\mathcal{O}$.

Inversamente si $\alpha\mathcal{O}_F \cap \mathcal{O} = \beta\mathcal{O}$, extendiendo $\alpha\mathcal{O}_F = \beta\mathcal{O}\mathcal{O}_F = \beta\mathcal{O}_F$, es decir $\alpha = u\beta$ para alguna unidad u de $\mathcal{O}_F$. □

Aquí vale la pena detenernos, para mencionar que las clases que siguen a continuación, no son las mismas clases que definimos en $\mathcal{H}(\mathcal{O})$.

Lema 2.46. *Sean $(\mathcal{O}_F/\mathfrak{f})^*$ el grupo de unidades del anillo $\mathcal{O}_F/\mathfrak{f}$ y $\mathcal{O}_F^*$ el grupo de unidades de $\mathcal{O}_F$, $\mathcal{O}^*$ el grupo de unidades de $\mathcal{O}$. Denotamos por $[\mathcal{O}_F^*] = \{\alpha + \mathfrak{f} : \alpha \in \mathcal{O}_F^*\}$ y $[P_{\mathfrak{f}}(\mathcal{O})] = \{\gamma + \mathfrak{f} : \gamma \in P_{\mathfrak{f}}(\mathcal{O})\}$. Entonces*

$$\mathcal{O}_F^*/\mathcal{O}^* \cong [\mathcal{O}_F^*]/([\mathcal{O}_F^*] \cap [P_{\mathfrak{f}}(\mathcal{O})]).$$

DEMOSTRACIÓN. Claramente $[\mathcal{O}_F^*] \cap [P_{\mathfrak{f}}(\mathcal{O})] = [\mathcal{O}^*]$ donde $[\mathcal{O}^*] = \{\beta + \mathfrak{f} : \beta \in \mathcal{O}^*\}$.

Sólo falta ver que

$$\mathcal{O}_F^*/\mathcal{O}^* \cong [\mathcal{O}_F^*]/[\mathcal{O}^*].$$

Sea $g : \mathcal{O}_F^*/\mathcal{O}^* \longrightarrow [\mathcal{O}_F^*]/[\mathcal{O}^*]$ dado por $\alpha\mathcal{O}^* \mapsto (\alpha+\mathfrak{f})[\mathcal{O}^*]$. Veremos que g es inyectivo. Supongamos que $(\alpha+\mathfrak{f})[\mathcal{O}^*] = (\beta+\mathfrak{f})[\mathcal{O}^*]$, entonces $(\alpha+\mathfrak{f})(\beta^{-1}+\mathfrak{f}) \in [\mathcal{O}^*]$, de donde $(\alpha\beta^{-1}+\mathfrak{f}) \in [\mathcal{O}^*]$ es decir $\alpha\beta^{-1} \in \mathcal{O}^*$ por tanto $\alpha\mathcal{O}^* = \beta\mathcal{O}^*$. Como g es suprayectivo por su definición, tenemos g es un isomorfismo. □

Lema 2.47. *Sea $(\mathcal{O}/\mathfrak{f})^*$ el grupo de unidades de $\mathcal{O}/\mathfrak{f}$. Entonces $(\mathcal{O}/\mathfrak{f})^* = [P_{\mathfrak{f}}(\mathcal{O})]$.*

DEMOSTRACIÓN. Sea $\alpha+\mathfrak{f} \in (\mathcal{O}/\mathfrak{f})^*$, entonces existe $\beta+\mathfrak{f} \in \mathcal{O}/\mathfrak{f}$ tal que

$$(\alpha+\mathfrak{f})(\beta+\mathfrak{f}) = (\alpha\beta+\mathfrak{f}) = 1+\mathfrak{f},$$

de donde $(\alpha\beta)\mathcal{O}_F + \mathfrak{f} = \mathcal{O}_F$ y como $(\alpha\beta)\mathcal{O}_F \subseteq \alpha\mathcal{O}_F$, se tiene $\alpha\mathcal{O}_F + \mathfrak{f} = \mathcal{O}_F$, es decir $\alpha \in P_{\mathfrak{f}}(\mathcal{O})$ y por tanto $\alpha+\mathfrak{f} \in [P_{\mathfrak{f}}(\mathcal{O})]$.

Ahora sea $\alpha+\mathfrak{f} \in [P_{\mathfrak{f}}(\mathcal{O})]$, es decir $\alpha\mathcal{O}_F+\mathfrak{f} = \mathcal{O}_F$, entonces $\alpha\gamma+y = 1$, con $\gamma \in \mathcal{O}_F$ y $y \in \mathfrak{f}$, de lo anterior $1 \in \alpha\gamma+\mathfrak{f}$, lo que implica $(\alpha\gamma)\mathcal{O}_F+\mathfrak{f} = \mathcal{O}_F$ y así $(\alpha+\mathfrak{f})(\gamma+\mathfrak{f}) = \alpha\gamma+\mathfrak{f} = \mathcal{O}_F = 1+\mathfrak{f}$, es decir $\alpha+\mathfrak{f} \in (\mathcal{O}/\mathfrak{f})^*$. □

El siguiente teorema es muy útil pues nos ayuda a calcular el número de clases de cualquier orden.

Teorema 2.48. *Sean $\mathcal{O}_F$ el anillo de enteros de un campo de números F y $\mathcal{O}$ un orden en F con conductor $\mathfrak{f}$. Entonces el número de clases de $\mathcal{O}$ satisface*

$$h_{\mathcal{O}} = \frac{\Phi(\mathfrak{f})}{e\Phi'(\mathfrak{f})}h_F,$$

donde $\Phi(\mathfrak{f})$ y $\Phi'(\mathfrak{f})$ son, respectivamente, el número de unidades de $\mathcal{O}_F/\mathfrak{f}$ y $\mathcal{O}/\mathfrak{f}$, mientras que h_F es el número de clases de $\mathcal{O}_F$ y e es el índice del grupo de unidades de $\mathcal{O}$ en el grupo de unidades de $\mathcal{O}_F$.

DEMOSTRACIÓN. Sea $\mathcal{H}(\mathcal{O}_F)$ el grupo de clases de $\mathcal{O}_F$. Consideramos el homomorfismo de grupos

$$g : I_{\mathfrak{f}}^*(\mathcal{O}_F) \longrightarrow \mathcal{H}(\mathcal{O}_F)$$
$$I \mapsto [I].$$

Notemos que para cualquier ideal $I \in \mathcal{O}_F$, existe un ideal J de manera que $[I^{-1}] = [J]$, lo que es equivalente a $[I] = [J^{-1}]$.

Por el lema 2.41, existe un ideal $L = \alpha J^{-1}$ tal que $[L] = [I]$ y $L+\mathfrak{f} = \mathcal{O}_F$. Lo anterior implica de g es suprayectivo.

Veremos que $\mathrm{Ker}(g) = P_{\mathfrak{f}}^*(\mathcal{O}_F)$.

$$\begin{aligned}
\mathrm{Ker}(g) &= \{I \in I_{\mathfrak{f}}^*(\mathcal{O}_F) : g(I) = [\mathcal{O}_F]\} \\
&= \{I \in I_{\mathfrak{f}}^*(\mathcal{O}_F) : [I] = [\mathcal{O}_F]\} \\
&= \{I \in I_{\mathfrak{f}}^*(\mathcal{O}_F) : \beta\mathcal{O}_F I = \alpha\mathcal{O}_F, \text{ para algunos } \alpha,\beta \in P_{\mathfrak{f}}(\mathcal{O}_F)\} \\
&= \{I = \alpha\mathcal{O}_F\beta^{-1}\mathcal{O}_F : \alpha,\beta \in P_{\mathfrak{f}}(\mathcal{O}_F)\} \\
&= P_{\mathfrak{f}}^*(\mathcal{O}_F).
\end{aligned}$$

Así, $I_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O}_F) \cong \mathcal{H}(\mathcal{O}_F)$, de donde

$$\begin{aligned} h_{\mathcal{O}} &= |I_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})| \\ &= |I_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O}_F)| \cdot |P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})| \\ &= h_F|P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})|. \end{aligned}$$

Ahora el objetivo es ver quién es $|P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})|$.

Sea $(\mathcal{O}_F/\mathfrak{f})^*$ el grupo de unidades del anillo $\mathcal{O}_F/\mathfrak{f}$ y consideramos el homomorfismo de grupos

$$\begin{aligned} g' : (\mathcal{O}_F/\mathfrak{f})^* &\longrightarrow P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O}) \\ [\alpha] &\mapsto [\alpha\mathcal{O}_F] \end{aligned}$$

Veamos que está bien definido.

Si $[\alpha] = [\beta]$, entonces $\alpha \equiv \beta \pmod{\mathfrak{f}}$ y por ser unidades existe un $\gamma \in \mathcal{O}_F$ tal que $\alpha\gamma \equiv \beta\gamma \equiv 1 \pmod{\mathfrak{f}}$ y como $\mathfrak{f} \subseteq \mathcal{O}$, tenemos $\alpha\gamma, \beta\gamma \in \mathcal{O}$ y de lo anterior,

$$[\alpha\mathcal{O}_F] = [\alpha\mathcal{O}_F(\beta\gamma)\mathcal{O}_F] = [\beta\mathcal{O}_F(\alpha\gamma)\mathcal{O}_F] = [\beta\mathcal{O}_F].$$

Notemos que g' es suprayectivo y por tanto $|P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})| \leq |(\mathcal{O}_F/\mathfrak{f})^*|$, es decir el número de clases de $\mathcal{O}$ es finito.

A continuación probaremos $\text{Ker}(g') = \{[u\beta] : \beta \in P_{\mathfrak{f}}(\mathcal{O})$ y u es una unidad de $\mathcal{O}_F\}$.

$[\alpha] \in Ker(g')$, es equivalente a $[\alpha\mathcal{O}_F] = 1$ lo cual sucede si y sólo si $[\alpha\mathcal{O}_F \cap \mathcal{O}] = 1$, por la proposición 2.44, $\alpha\mathcal{O}_F \cap \mathcal{O} = \beta\mathcal{O}$ con $\beta \in \mathcal{O}$ y por el lema 2.45 $\alpha = u\beta$ para u una unidad de $\mathcal{O}_F$ y $\beta \in P_{\mathfrak{f}}(\mathcal{O})$.

Notemos que $Ker(g') = [\mathcal{O}_F^*]\cdot[P_{\mathfrak{f}}(\mathcal{O})]$, de donde $(\mathcal{O}_F/\mathfrak{f})^*/([\mathcal{O}_F^*]\cdot[P_{\mathfrak{f}}(\mathcal{O})]) \cong P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})$, lo que implica que

$$|P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})| = \frac{|(\mathcal{O}_F/\mathfrak{f})^*|}{|[\mathcal{O}_F^*] \cdot [P_{\mathfrak{f}}(\mathcal{O})]|}.$$

Y sabemos que si $H, N \leq G$, con $N \triangleleft G$ y G un grupo finito, entonces $|HN| = \dfrac{|H| \cdot |N|}{|H \cap N|}$.

Así,

$$|[\mathcal{O}_F^*] \cdot [P_{\mathfrak{f}}(\mathcal{O})]| = \frac{|[\mathcal{O}_F^*]| \cdot |[P_{\mathfrak{f}}(\mathcal{O})]|}{|[\mathcal{O}_F^*] \cap [P_{\mathfrak{f}}(\mathcal{O})]|} = |[\mathcal{O}_F^*]/([\mathcal{O}_F^*] \cap [P_{\mathfrak{f}}(\mathcal{O})])| \cdot |[P_{\mathfrak{f}}(\mathcal{O})]|.$$

Sean $\mathcal{O}^*$ el grupo de unidades de $\mathcal{O}$ y $(\mathcal{O}/\mathfrak{f})^*$ el grupo de unidades de $\mathcal{O}/\mathfrak{f}$, por los lemas 2.46 y 2.47 tenemos

$$|[\mathcal{O}_F^*] \cdot [P_{\mathfrak{f}}(\mathcal{O})]| = |\mathcal{O}_F^*/\mathcal{O}^*| \cdot |(\mathcal{O}/\mathfrak{f})^*|.$$

Por lo tanto,

$$|P_{\mathfrak{f}}^*(\mathcal{O}_F)/P_{\mathfrak{f}}^*(\mathcal{O})| = \frac{|(\mathcal{O}_F/\mathfrak{f})^*|}{|\mathcal{O}_F^*/\mathcal{O}^*| \cdot |(\mathcal{O}/\mathfrak{f})^*|} = \frac{\Phi(\mathfrak{f})}{e\Phi'(\mathfrak{f})}.$$

□

Definición 2.49. *Sea F un campo de números. Llamaremos* **función de Euler generalizada** *de $\mathcal{O}_F$ a la función definida como $\Phi(I) = |(\mathcal{O}_F/I)^*|$, donde I es un $\mathcal{O}_F$-ideal no cero.*

Lema 2.50. *Sea I un ideal no cero de $\mathcal{O}_F$. Entonces*

$$(\mathcal{O}_F/I)^* = \{[\alpha] : \alpha\mathcal{O}_F + I = \mathcal{O}_F\}.$$

DEMOSTRACIÓN. Sea $\alpha + I \in (\mathcal{O}_F/I)^*$, es decir existe $\beta + I \in \mathcal{O}_F/I$ tal que

$$(\alpha + I)(\beta + I) = 1 + I,$$

de donde $\alpha\beta + I = 1 + I$, entonces $1 - \alpha\beta = \gamma$ para algún $\gamma \in I$, lo que implica $1 \in \alpha\mathcal{O}_F + I$ y por lo tanto $\alpha\mathcal{O}_F + I = \mathcal{O}_F$.

Recíprocamente, sea $\alpha + I$ tal que $\alpha\mathcal{O}_F + I = \mathcal{O}_F$. Entonces $1 \in \alpha\mathcal{O}_F + I$ de donde $1 = \alpha\gamma + i$ con $\gamma \in \mathcal{O}_F$ e $i \in I$. Por lo tanto, $(\alpha+I)(\gamma+I) = \alpha\gamma+I = 1-i+I = 1+I$. □

Teorema 2.51. *Sea F un campo de números.*

i) *Si I, J son ideales de $\mathcal{O}_F$ tales que $I + J = \mathcal{O}_F$, entonces $\Phi(IJ) = \Phi(I)\Phi(J)$.*
ii) *Si P es un ideal primo de $\mathcal{O}_F$, entonces $\Phi(P^e) = (N(P) - 1)N(P)^{e-1}$*

DEMOSTRACIÓN. i) Por el teorema chino del residuo $\mathcal{O}_F/IJ = \mathcal{O}_F/I \times \mathcal{O}_F/J$, entonces

$$(\mathcal{O}_F/IJ)^* = (\mathcal{O}_F/I)^* \times (\mathcal{O}_F/J)^*,$$

de donde,

$$|(\mathcal{O}_F/IJ)^*| = |(\mathcal{O}_F/I)^*| \times |(\mathcal{O}_F/J)^*|.$$

Por tanto, $\Phi(IJ) = \Phi(I)\Phi(J)$.

ii) La demostración la haremos por inducción sobre e. $\Phi(P) = N(P) - 1$ pues $\mathcal{O}_F/P$ es un campo.

Supongamos que el resultado se vale hasta e. Veremos que se cumple para $e + 1$.

Sea $\pi \in P\setminus P^2$. Si α recorre un conjunto de representantes de las $N(P^e)$ clases módulo P^e y β recorre un conjunto de representantes de las $N(P)$ clases módulo P, entonces los elementos $\alpha + \pi^e\beta$ son no congruentes dos a dos módulo P^{e+1}, pues si $\alpha_1 + \pi^e\beta_1 \equiv \alpha_2 + \pi^e\beta_2 \pmod{P^{e+1}}$, entonces $(\alpha_1 - \alpha_2) + \pi^e(\beta_1 - \beta_2) \in P^{e+1}$ y como $\pi^e \in P^e$, $\alpha_1 - \alpha_2 \equiv 0 \pmod{P^e}$, es decir $\alpha_1 = \alpha_2$, luego $\pi^e(\beta_1 - \beta_2) \equiv 0 \pmod{P^{e+1}}$, de donde $\beta_1 - \beta_2 \equiv 0 \pmod{P}$ pues $\pi^e \in P^e \setminus P^{e+1}$, por consiguiente $\beta_1 = \beta_2$, es decir $\alpha_1 + \pi^e\beta_1 = \alpha_2 + \pi^e\beta_2$. Dado que hay $N(P)^{e+1}$ de ellos, concluimos que forman un conjunto de representantes de las clases módulo P^{e+1}.

También tenemos mcd$(\alpha + \pi^e\beta, \pi) = 1$ si y sólo si mcd$(\alpha, \pi) = 1$. De lo anterior, las unidades módulo P^{e+1} tienen como representante un α que es unidad módulo P^e y un β cualquiera. Por tanto, por cada unidad $[\alpha]$ módulo P^e hay $N(P)$ unidades $[\alpha + \pi^e\beta]$ módulo P^{e+1}, es decir, se cumple $\Phi(P^{e+1}) = N(P)\Phi(P^e)$ y por hipótesis de inducción,

$$\Phi(P^{e+1}) = N(P)(N(P) - 1)N(P)^{e-1} = (N(P) - 1)N(P)^e.$$

□

Ahora veremos como calcular en número de clases, en el caso particular en que F es un campo cuadrático.

Lema 2.52. *Sea $\mathcal{O}_m = \mathbb{Z} + m\mathcal{O}_F$ un orden en un campo cuadrático F. Entonces*

$$\mathcal{O}_m/m\mathcal{O}_F \cong \mathbb{Z}/m\mathbb{Z}$$

DEMOSTRACIÓN. Si $l \in \mathcal{O}_m$, entonces $l = n + m\alpha$ con $n \in \mathbb{Z}$ y $\alpha \in \mathcal{O}_F$. Luego si $l + m\mathcal{O}_F \in \mathcal{O}_m/m\mathcal{O}_F$, tenemos $l + m\mathcal{O}_F = (n + m\alpha) + m\mathcal{O}_F = n + m\mathcal{O}_F$, es decir, podemos tomar a cualquier elemento de $\mathcal{O}_m/m\mathcal{O}_F$ de manera que el representante sea un número entero racional.

Sea $g : \mathcal{O}_m/m\mathcal{O}_F \longrightarrow \mathbb{Z}/m\mathbb{Z}$ dado por $g(n + m\mathcal{O}_F) = n + m\mathbb{Z}$.

Claramente g está bién definido, pues si $n + m\mathcal{O}_F = n' + m\mathcal{O}_F$, entonces $n - n' \in m\mathcal{O}_F \cap \mathbb{Z} = m\mathbb{Z}$, es decir $g(n + m\mathcal{O}_F) = g(n' + m\mathcal{O}_F)$.

Observemos que g es inyectivo pues si $g(n + m\mathcal{O}_F) = g(n' + m\mathcal{O}_F)$, tenemos $n + m\mathbb{Z} = n' + m\mathbb{Z}$, de donde $n - n' \in m\mathbb{Z} \subseteq m\mathcal{O}_F$, lo que implica $n - n' \in m\mathcal{O}_F$, así $n + m\mathcal{O}_F = n' + m\mathcal{O}_F$. Finalmente, como g es suprayectivo por definición, concluimos $\mathcal{O}_m/m\mathcal{O}_F \cong \mathbb{Z}/m\mathbb{Z}$. □

Teorema 2.53. *Sea $\mathcal{O}_m$ el orden de índice m en un campo cuadrático F. Entonces*

$$h_{\mathcal{O}_m} = \frac{\Phi(m\mathcal{O}_F)}{e\phi(m)} h_F,$$

donde Φ es la función de Euler generalizada, ϕ es la función de Euler usual, e es el índice del grupo de las unidades de $\mathcal{O}_m$ en el grupo de las unidades de $\mathcal{O}_F$ y h_F es el número de clases de $\mathcal{O}_F$.

DEMOSTRACIÓN. Como $\mathcal{O}_m$ es de índice m, tenemos $\mathcal{O}_m = \mathbb{Z} + m\mathcal{O}_F$. Por el teorema 2.48, $h_{\mathcal{O}_m} = \dfrac{\Phi(m\mathcal{O}_F)}{e\Phi'(m\mathcal{O}_F)} h_F$, y dado que $\mathcal{O}_m/m\mathcal{O}_F \cong \mathbb{Z}/m\mathbb{Z}$, se tiene $\Phi'(m\mathcal{O}_F) = \phi(m)$. Por lo tanto,

$$h_{\mathcal{O}_m} = \frac{\Phi(m\mathcal{O}_F)}{e\phi(m)} h_F.$$

□

Apartir de ahora $\langle\alpha\rangle = \alpha\mathcal{O}_F$.

Ejemplo 2.54. *Sea $F = \mathbb{Q}(i)$ un campo de números con anillo de enteros $\mathcal{O}_F = \mathbb{Z}[i]$. Calcularemos el número de clases $h_{\mathcal{O}_2}$ donde $\mathcal{O}_2 = \mathbb{Z}[2i] = \mathbb{Z} + 2\mathbb{Z}[i]$.*

DEMOSTRACIÓN. Por el teorema 2.53, $h_{\mathcal{O}_2} = \dfrac{\Phi(\langle 2\rangle)}{e\phi(2)} h_F$, con $h_F = 1$, $e = |\mathcal{O}_F^*/\mathcal{O}^*| = \dfrac{4}{2} = 2$, $\phi(2) = 2 - 1 = 1$.

Como $\Phi(\langle 2\rangle) = \Phi(\langle 1+i\rangle^2) = (N(\langle 1+i\rangle)-1)N(\langle 1+i\rangle)$ y $N(\langle 1+i\rangle) = N(1+i) = 2$, entonces $\Phi(\langle 2\rangle) = 2$.

Por lo tanto,

$$h_{\mathcal{O}_2} = \frac{2}{2 \cdot 1} 1 = 1.$$

□

A continuación veremos algunos corolarios del teorema anterior, los cuales nos ayudan a simplificar las cuentas para el encontrar el número de clases de un orden dado en un campo cuadrático.

Corolario 2.55. *Sean $\mathcal{O}_F = \mathbb{Z}[i]$ el anillo de enteros de $F = \mathbb{Q}(\sqrt{-1})$ y $\mathcal{O}_m$ el orden de índice m.*

(i) *Si $m = 2^t$, con $t \in \mathbb{N}$, entonces $h_{\mathcal{O}_m} = 2^{t-1}$.*

(ii) *Si $m = p^t$, con $t \in \mathbb{N}$ y $p \equiv 3 \pmod 4$, entonces $h_{\mathcal{O}_m} = \left(\frac{p+1}{2}\right) p^{t-1}$.*

(iii) *Si $m = p^t$, con $t \in \mathbb{N}$ y $p \equiv 1 \pmod 4$, entonces $h_{\mathcal{O}_m} = \left(\frac{p-1}{2}\right) p^{t-1}$.*

DEMOSTRACIÓN. Para todos lo casos tenemos, por el teorema anterior, $h_{\mathcal{O}_m} = \dfrac{\Phi(\langle m\rangle)}{e\phi(m)} h_F$ y sabemos que $h_F = 1$, $e = [\mathcal{O}_F^* : \mathcal{O}_m^*] = \dfrac{4}{2} = 2$ y si p es un primo racional, $\phi(p^t) = (p-1)p^{t-1}$. Sólo falta calcular $\Phi(\langle m\rangle)$ en cada caso.

(i) En este caso

$$\begin{aligned} \Phi(\langle m\rangle) &= \Phi(\langle 2\rangle^t) \\ &= \Phi(\langle 1+i\rangle^{2t}) \\ &= (N(\langle 1+i\rangle) - 1)N(\langle 1+i\rangle)^{2t-1} \\ &= (2-1)2^{2t-1} = 2^{2t-1}. \end{aligned}$$

Así, $h_{\mathcal{O}_m} = \dfrac{2^{2t-1}}{2(2^{t-1})} 1 = 2^{t-1}$.

(ii) Para este caso tenemos

$$\begin{aligned} \Phi(\langle m\rangle) &= \Phi(\langle p\rangle^t) \\ &= (N(\langle p\rangle) - 1)N(\langle p\rangle)^{t-1} \\ &= (p^2-1)p^{2t-2}. \end{aligned}$$

De donde $h_{\mathcal{O}_m} = \dfrac{(p^2-1)p^{2t-2}}{2(p-1)p^{t-1}} 1 = \left(\frac{p+1}{2}\right) p^{t-1}$.

(iii) Por último,

$$\begin{aligned} \Phi(\langle m\rangle) &= \Phi(\langle a+bi\rangle^t \langle a-bi\rangle^t) \\ &= \Phi(\langle a+bi\rangle^t)\Phi(\langle a-bi\rangle^t) \\ &= (N(\langle a+bi\rangle) - 1)N(\langle a+bi\rangle)^{t-1}(N(\langle a-bi\rangle) - 1)N(\langle a-bi\rangle)^{t-1} \\ &= (p-1)p^{t-1}(p-1)p^{t-1} = (p-1)^2 p^{2t-2}. \end{aligned}$$

Por tanto, $h_{\mathcal{O}_m} = \dfrac{(p-1)^2 p^{2t-2}}{2(p-1)p^{t-1}} = \left(\frac{p-1}{2}\right) p^{t-1}$. □

Antes de ver el siguiente corolario, veamos un ejemplo particular en $\mathcal{O}_F$ el anillo de enteros del campo $F = \mathbb{Q}(\sqrt{-3})$.

Ejemplo 2.56. *Sea* $\mathcal{O}_F = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ *el anillo de enteros del campo de números* $F = \mathbb{Q}(\sqrt{-3})$. *Vamos a calcular el número de clases de* $\mathcal{O}_3 = \mathbb{Z} + 3\mathcal{O}_F$.

DEMOSTRACIÓN. Del teorema 2.53 se tiene $h_{\mathcal{O}_3} = \frac{\Phi(\langle 3\rangle)}{e\phi(3)}h$, pero sabemos que $h_F = 1$, $e = 3$ y $\phi(3) = 2$. Sólo nos falta calcular $\Phi(\langle 3\rangle)$. Dado que $3|\delta_F = -3$, por la proposición 1.69, $\langle 3\rangle = \langle 3, \sqrt{-3}\rangle^2$. Así,

$$\begin{aligned}\Phi(\langle 3\rangle) &= \Phi(\langle 3, \sqrt{-3}\rangle^2)\\ &= (N(\langle 3, \sqrt{-3}\rangle) - 1)N(\langle 3, \sqrt{-3}\rangle)\\ &= (3-1)3 = 6.\end{aligned}$$

Por lo tanto, $h_{\mathcal{O}_3} = \frac{6}{3\cdot 2}1 = 1$. □

La razón por la que se vio este ejemplo en particular es que en $\mathcal{O}_F = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$, 3 es el único primo racional que se ramifica totalmente.

Corolario 2.57. *Sean* $\mathcal{O}_F = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ *el anillo de enteros del campo de números* $F = \mathbb{Q}(\sqrt{-3})$ *y* $\mathcal{O}_m$ *el orden de índice* m.

(i) *Si* $m = p^t$, *con* $t \in \mathbb{N}$ *y* $\langle p\rangle$ *un ideal primo en* $\mathcal{O}_F$, *entonces* $h_{\mathcal{O}_m} = \left(\frac{p+1}{3}\right)p^{t-1}$.

(ii) *Si* $m = p^t$, *con* $t \in \mathbb{N}$ *y* $\langle p\rangle = \langle p, a+\sqrt{-3}\rangle\langle p, a-\sqrt{-3}\rangle$, *entonces* $h_{\mathcal{O}_m} = \left(\frac{p-1}{3}\right)p^{t-1}$.

(iii) *Si* $m = 3^t$, *con* $t \in \mathbb{N}$, *entonces* $h_{\mathcal{O}_m} = 3^{2t-2}$.

DEMOSTRACIÓN. Para todos los casos sabemos que $h_F = 1$, $e = 3$ y si p es un primo racional, entonces $\phi(p^t) = (p-1)p^{t-1}$. Sólo falta calcular $\Phi(\langle m\rangle)$ en cada caso.

(i) Para este caso

$$\begin{aligned}\Phi(\langle m\rangle) &= \Phi(\langle p\rangle^t)\\ &= (N(\langle p\rangle) - 1)(N(\langle p\rangle)^{t-1})\\ &= (p^2-1)(p^2)^{t-1} = (p^2-1)p^{2t-2},\end{aligned}$$

de donde $h_{\mathcal{O}_m} = \frac{(p^2-1)p^{2t-2}}{3(p-1)p^{t-1}}1 = \frac{p+1}{3}p^{t-1}$.

(ii) Ahora tenemos

$$\begin{aligned}\Phi(\langle m\rangle) &= \Phi(\langle p\rangle^t)\\ &= \Phi(\langle p, a+\sqrt{-3}\rangle^t)\Phi(\langle p, a-\sqrt{-3}\rangle^t)\\ &= (N(\langle p, a+\sqrt{-3}\rangle) - 1)^2(N(\langle p, a+\sqrt{-3}\rangle)^{t-1})^2\\ &= (p-1)^2p^{2t-2},\end{aligned}$$

así $h_{\mathcal{O}_m} = \frac{(p-1)^2p^{2t-2}}{3(p-1)p^{t-1}}1 = \frac{p-1}{3}p^{t-1}$.

(iii) Por último,

$$\begin{aligned}\Phi(\langle m\rangle) &= \Phi(\langle 3\rangle^t)\\ &= \Phi(\langle 3,\sqrt{-3}\rangle^{2t})\\ &= (N(\langle 3,\sqrt{-3}\rangle)-1)(N(\langle 3,\sqrt{-3}\rangle)^{2t-1})\\ &= (3-1)3^{2t-1},\end{aligned}$$

por tanto $h_{\mathcal{O}_m} = \dfrac{(2)3^{2t-1}}{3(2)3^{t-1}}1 = 3^{t-1}$. □

El corolario anterior es muy importante ya que de los incisos (i) y (ii) podemos obtener más información.

En el anillo $\mathcal{O}_F = \mathbb{Z}\left[\dfrac{-1+\sqrt{-3}}{2}\right]$ los primos racionales de la forma $p \equiv 2 \pmod 3$ siguen siendo primos en $\mathcal{O}_F$, mientras que los primos racionales de la forma $p \equiv 1 \pmod 3$ dejan de ser primos en $\mathcal{O}_F$.

Ahora veremos qué pasa en el resto de los campos cuadráticos imaginarios.

Corolario 2.58. *Sean $F = \mathbb{Q}(\sqrt{d})$ con $d < 0$ libre de cuadrados y $d \neq -1, -3$, con anillo de enteros $\mathcal{O}_F$ y $\mathcal{O}_m$ el orden de índice m en F. Para $m \neq 2$ tenemos*

(i) *Si $m = p^t$ con $t \in \mathbb{N}$ y p un primo racional tal que $\langle p\rangle$ es un ideal primo en $\mathcal{O}_F$, entonces $h_{\mathcal{O}_m} = (p+1)p^{t-1}h_F$.*

(ii) *Si $m = p^t$ con $t \in \mathbb{N}$ y p un primo racional tal que $\langle p\rangle = \langle p, a+\sqrt{d}\rangle\langle p, a-\sqrt{d}\rangle$, entonces $h_{\mathcal{O}_m} = (p-1)p^{t-1}h_F$.*

(iii) *Si $m = p^t$ con $t \in \mathbb{N}$ y p un primo racional tal que $\langle p\rangle = \langle p, \sqrt{d}\rangle^2$, entonces $h_{\mathcal{O}_m} = p^t h_F$.*

Donde h_F es el número de clases de $\mathcal{O}_F$.

DEMOSTRACIÓN. Sabemos que $h_{\mathcal{O}_m} = \dfrac{\Phi(\langle m\rangle)}{e\phi(m)}h_F$, en todos los casos que estamos considerando $e = 1$.

Para (i)

$$\begin{aligned}\Phi(\langle m\rangle) &= \Phi(\langle p\rangle^t)\\ &= (N(\langle p\rangle)-1)(N(\langle p\rangle)^{t-1})\\ &= (p^2-1)p^{2t-2}.\end{aligned}$$

Así, $h_{\mathcal{O}_m} = \dfrac{(p^2-1)p^{2t-2}}{(p-1)p^{t-1}}h_F = (p+1)p^{t-1}h_F$.

Para el siguiente caso

$$\begin{aligned}\Phi(\langle m\rangle) &= \Phi(\langle p, a+\sqrt{d}\rangle^t)\Phi(\langle p, a-\sqrt{d}\rangle^t)\\ &= (N(\langle p, a+\sqrt{d}\rangle)-1)^2(N(\langle p, a+\sqrt{d}\rangle)^{2t-2})\\ &= (p-1)^2p^{2t-2},\end{aligned}$$

entonces $h_{\mathcal{O}_m} = \dfrac{(p-1)^2p^{2t-2}}{(p-1)p^{t-1}}h_F = (p-1)p^{t-1}h_F$.

Para el último caso

$$\begin{aligned}\Phi(\langle m\rangle) &= \Phi(\langle p,\sqrt{d}\rangle^2)\\ &= (N(\langle p,\sqrt{d}\rangle)-1)(N(\langle p,\sqrt{d}\rangle)^{2t-1})\\ &= (p-1)p^{2t-1},\end{aligned}$$

por tanto, $h_{\mathcal{O}_m}=\dfrac{(p-1)p^{2t-1}}{(p-1)p^{t-1}}h_F=p^th_F$. □

Para calcular el número de clases del orden $\mathcal{O}_2=\mathbb{Z}+2\mathcal{O}_F$ hay que analizar dos casos: $d\equiv 2,3 \pmod 4$ y $d\equiv 1 \pmod 4$.

Corolario 2.59. *Sea $\mathcal{O}_F$ el anillo de enteros del campo de número $F=\mathbb{Q}(\sqrt{d})$ con $d\equiv 2,3 \pmod 4$, $d<0$ libre de cuadrados y $d\neq -1$. Entonces, si $m=2^t$, tenemos $h_{\mathcal{O}_m}=2^th_F$.*

DEMOSTRACIÓN.

Sólo hay que notar

$$\Phi(\langle m\rangle)=\Phi(\langle 2\rangle^t)=\Phi(\langle 2,\sqrt{d}\rangle^{2t})=(2-1)2^{2t-1}=2^{2t-1} \text{ si } d\equiv 2 \pmod 4$$

y también

$$\Phi(\langle m\rangle)=\Phi(\langle 2\rangle^t)=\Phi(\langle 2,1+\sqrt{d}\rangle^{2t})=(2-1)2^{2t-1}=2^{2t-1} \text{ si } d\equiv 2 \pmod 4.$$

Así, $h_{\mathcal{O}_m}=\dfrac{2^{2t-1}}{2^{t-1}}h_F=2^th_F$. □

Corolario 2.60. *Sea $\mathcal{O}_F$ el anillo de enteros del campo de número $F=\mathbb{Q}(\sqrt{d})$ con $d\equiv 1 \pmod 4$, $d<0$ libre de cuadrados y $d\neq -3$. Entonces*

(i) *Si $d\equiv 1 \pmod 8$ y $m=2^t$, entonces $h_{\mathcal{O}_m}=2^{t-1}h_F$.*
(ii) *Si $d\equiv 5 \pmod 8$ y $m=2^t$, entonces $h_{\mathcal{O}_m}=3\cdot 2^{t-1}h_F$.*

DEMOSTRACIÓN. Como en los casos anteriores sólo nos falta $\Phi(\langle m\rangle)$. Para el primer caso tenemos $\langle 2\rangle=\left\langle 2,\dfrac{1+\sqrt{d}}{2}\right\rangle\left\langle 2,\dfrac{1-\sqrt{d}}{2}\right\rangle$, de donde.

$$\begin{aligned}\Phi(\langle m\rangle) &= \Phi(\langle 2\rangle^t)\\ &= \Phi\left(\left\langle 2,\frac{1+\sqrt{d}}{2}\right\rangle^t\left\langle 2,\frac{1-\sqrt{d}}{2}\right\rangle^t\right)\\ &= \Phi\left(\left\langle 2,\frac{1+\sqrt{d}}{2}\right\rangle^t\right)\Phi\left(\left\langle 2,\frac{1-\sqrt{d}}{2}\right\rangle^t\right)\\ &= \left(N\left(\left\langle 2,\frac{1+\sqrt{d}}{2}\right\rangle\right)-1\right)^2\left(N\left(\left\langle 2,\frac{1+\sqrt{d}}{2}\right\rangle\right)\right)^{2t-2}\\ &= (2-1)(2)^{2t-2}=2^{2t-2}.\end{aligned}$$

Por tanto, $h_{\mathcal{O}_m}=\dfrac{2^{2t-2}}{2^{t-1}}h_F=2^{t-1}h_F$.

En el caso en que $d \equiv 5 \pmod 8$, tenemos $\langle 2 \rangle$ es un ideal primo en $\mathcal{O}_F$. De modo que

$$\begin{aligned} \Phi(\langle m \rangle) &= \Phi(\langle 2 \rangle^t) \\ &= (N(\langle 2 \rangle) - 1)(N(\langle 2 \rangle)^{t-1}) \\ &= (4-1)4^{t-1} = 3(2^{2t-2}). \end{aligned}$$

Así, $h_{\mathcal{O}_m} = \dfrac{3(2^{2t-2})}{2^{t-1}} h_F = 3 \cdot 2^{t-1} h_F$. □

Capítulo 3

Teorema de Furtwängler

En el capítulo anterior dimos la definición de orden, al cual se le asocia un conductor, el cual es uno de los principales actores en la teoría que desarrollamos. Este último resulta ser un ideal tanto del orden como del anillo de enteros. Una pregunta natural es: ¿Todo ideal no cero del anillo de enteros es conductor de algún orden? Justamente el teorema de Furtwängler publicado en 1919 (ver [**6**]), caracteriza a los ideales del anillo de enteros, para los cuales existe algún orden del cual ellos son conductores. En 2014 Prabpayak (ver [**10**] y [**14**]) da una prueba distinta, la cual es presentada en este capítulo.

3.1. Caracterización de los ideales conductor

Prabpayak resume el teorema de Furtwängler en dos partes, las cuales, como lo mencionamos anteriormente, se presentan en esta sección.

Lema 3.1. *Sean $\mathcal{O}_1$ y $\mathcal{O}_2$ órdenes en F con conductores $\mathfrak{f}_1$ y $\mathfrak{f}_2$ respectivamente.*
Si ŕm mcd$(\mathfrak{f}_1, \mathfrak{f}_2) = 1$, entonces $\mathcal{O}_1 \cap \mathcal{O}_2$ es un orden en F con conductor $\mathfrak{f}_1\mathfrak{f}_2$.

DEMOSTRACIÓN. Primero, $\mathcal{O}_1 \cap \mathcal{O}_2$ es un orden en F pues $(\mathcal{O}_1 \cap \mathcal{O}_2) \subseteq \mathcal{O}_1 \subseteq \mathcal{O}_F$ y también, $|\mathcal{O}_F/\mathcal{O}_1 \cap \mathcal{O}_2| = |\mathcal{O}_F/\mathcal{O}_1| \cdot |\mathcal{O}_1/\mathcal{O}_1 \cap \mathcal{O}_2| < \infty$, con $|\mathcal{O}_F/\mathcal{O}_1| < \infty$ ya que $\mathcal{O}_1$ es un orden en F. Por tanto, por el teorema 2.6, $\mathcal{O}_1 \cap \mathcal{O}_2$ es un orden en F.

Ahora veremos que $\mathfrak{f}_1\mathfrak{f}_2$ es el conductor de $\mathcal{O}_1 \cap \mathcal{O}_2$. Para ello, probaremos que $\mathfrak{f}_1\mathfrak{f}_2$ es el ideal de $\mathcal{O}_F$ más grande contenido en $\mathcal{O}_1 \cap \mathcal{O}_2$.

Claramente $\mathfrak{f}_1\mathfrak{f}_2 = \mathfrak{f}_1 \cap \mathfrak{f}_2$ pues mcd$(\mathfrak{f}_1, \mathfrak{f}_2) = 1$. Entonces $\mathfrak{f}_1\mathfrak{f}_2 = \mathfrak{f}_1 \cap \mathfrak{f}_2 \subseteq (\mathbb{Z} + (\mathfrak{f}_1 \cap \mathfrak{f}_2)) \subseteq ((\mathbb{Z}+\mathfrak{f}_1)\cap(\mathbb{Z}+\mathfrak{f}_2))$, como $\mathfrak{f}_i$ es el conductor de $\mathcal{O}_i$, tenemos $\mathbb{Z}+\mathfrak{f}_i \subseteq \mathcal{O}_i$, pues $\mathbb{Z}+\mathfrak{f}_i$ es el orden más chico que contiene a $\mathfrak{f}_i$, con $i = 1, 2$. De lo anterior, $((\mathbb{Z}+\mathfrak{f}_1)\cap(\mathbb{Z}+\mathfrak{f}_2)) \subseteq (\mathcal{O}_1 \cap \mathcal{O}_2)$. Así, $\mathfrak{f}_1\mathfrak{f}_2 \subseteq \mathcal{O}_1 \cap \mathcal{O}_2$.

Supongamos que $\mathfrak{f}$ es el conductor de $\mathcal{O}_1 \cap \mathcal{O}_2$. Entonces $\mathfrak{f} \subseteq \mathcal{O}_1 \cap \mathcal{O}_2$, de donde $\mathfrak{f} \subseteq \mathcal{O}_1$ y $\mathfrak{f} \subseteq \mathcal{O}_2$, por el lema 2.15 (ii), $\mathfrak{f} \subseteq \mathfrak{f}_1$ y $\mathfrak{f} \subseteq \mathfrak{f}_2$, es decir, $\mathfrak{f} \subseteq \mathfrak{f}_1 \cap \mathfrak{f}_2 = \mathfrak{f}_1\mathfrak{f}_2$. Por otro lado $\mathfrak{f}_1\mathfrak{f}_2$ es un ideal de $\mathcal{O}_F$ y $\mathfrak{f}_1\mathfrak{f}_2 \subseteq \mathcal{O}_1 \cap \mathcal{O}_2$, por el lema 2.15 (ii), $\mathfrak{f}_1\mathfrak{f}_2 \subseteq \mathfrak{f}$.

Por lo tanto, $\mathfrak{f} = \mathfrak{f}_1\mathfrak{f}_2$ es el conductor de $\mathcal{O}_1 \cap \mathcal{O}_2$. □

Lema 3.2. *Sea $\mathfrak{f} = \mathfrak{f}_1\mathfrak{f}_2$ con* mcd$(\mathfrak{f}_1, \mathfrak{f}_2) = 1$ *y supongamos que $\mathfrak{f}'_1, \mathfrak{f}'_2$ son ideales no cero de $\mathcal{O}_F$ tales que $\mathfrak{f}_1 \subseteq \mathfrak{f}'_1$, $\mathfrak{f}_2 \subseteq \mathfrak{f}'_2$ y $\mathfrak{f}' = \mathfrak{f}'_1\mathfrak{f}'_2$. Entonces $\psi(\mathfrak{f}'/\mathfrak{f}) = \mathfrak{f}'_1/\mathfrak{f}_1 \times \mathfrak{f}'_2/\mathfrak{f}_2$, donde $\psi : \mathcal{O}_F/\mathfrak{f} \to \mathcal{O}_F/\mathfrak{f}_1 \times \mathcal{O}_F/\mathfrak{f}_2$ es el isomorfismo dado por el teorema chino del residuo.*

DEMOSTRACIÓN. Sea $l + \mathfrak{f} \in \mathfrak{f}'/\mathfrak{f}$ un elemento cualquiera, con $l \in \mathfrak{f}'$. Dado que $\mathfrak{f}' = \mathfrak{f}'_1\mathfrak{f}'_2$, tenemos $l = l_1l_2$ con $l_1 \in \mathfrak{f}'_1$ y $l_2 \in \mathfrak{f}'_2$.

Aplicamos ψ al elemento $l + \mathfrak{f}$.

$$\begin{aligned} \psi(l + \mathfrak{f}) &= (l + \mathfrak{f}_1, l + \mathfrak{f}_2) \\ &= (l_1l_2 + \mathfrak{f}_1, l_1l_2 + \mathfrak{f}_2), \end{aligned}$$

como $\mathfrak{f}_1'$ y $\mathfrak{f}_2'$ son ideales, $l \in f_1'$ y $l \in \mathfrak{f}_2'$. Así, $\psi(\mathfrak{f}'/\mathfrak{f}) \subseteq \mathfrak{f}_1'/\mathfrak{f}_1 \times \mathfrak{f}_2'/\mathfrak{f}_2$.

Ahora sea $(l_1 + \mathfrak{f}_1, l_2 + \mathfrak{f}_2) \in \mathfrak{f}_1'/\mathfrak{f}_1 \times \mathfrak{f}_2'/\mathfrak{f}_2$, queremos ver que existe $\alpha \in \mathfrak{f}'$ tal que $\psi(\alpha + \mathfrak{f}) = (l_1 + \mathfrak{f}_1, l_2 + \mathfrak{f}_2)$.

Tenemos $\psi(\alpha + \mathfrak{f}) = (\alpha + \mathfrak{f}_1, \alpha + \mathfrak{f}_2)$ y necesitamos $(\alpha + \mathfrak{f}_1, \alpha + \mathfrak{f}_2) = (l_1 + \mathfrak{f}_1, l_2 + \mathfrak{f}_2)$, es decir, $\alpha + \mathfrak{f}_1 = l_1 + \mathfrak{f}_1$ y $\alpha + \mathfrak{f}_2 = l_2 + \mathfrak{f}_2$, de donde $\alpha - l_1 = \beta_1$ y $\alpha - l_2 = \beta_2$ con $\beta_1 \in \mathfrak{f}_1$ y $\beta_2 \in \mathfrak{f}_2$, de lo anterior $\alpha = l_1 + \beta_1 = l_2 + \beta_2 \in \mathfrak{f}_1' \cap \mathfrak{f}_2' = \mathfrak{f}'$. Así $\psi(\alpha + \mathfrak{f}) = (l_1 + \mathfrak{f}_1, l_2 + \mathfrak{f}_2)$, es decir $\mathfrak{f}_1'/\mathfrak{f}_1 \times \mathfrak{f}_2'/\mathfrak{f}_2 \subseteq \psi(\mathfrak{f}'/\mathfrak{f})$. □

Corolario 3.3. *Sea* $\mathfrak{f} = \mathfrak{f}_1\mathfrak{f}_2$ *con* $\text{mcd}(\mathfrak{f}_1, \mathfrak{f}_2) = 1$ *tal que* $\mathfrak{f} \subseteq \mathfrak{f}'$*, donde* $\mathfrak{f}'$ *es un ideal de* $\mathcal{O}_F$*. Entonces existen* $\mathfrak{f}_1', \mathfrak{f}_2'$ *ideales no cero de* $\mathcal{O}_F$ *tales que* $\mathfrak{f}_1 \subseteq \mathfrak{f}_1'$*,* $\mathfrak{f}_2 \subseteq \mathfrak{f}_2'$*,* $\mathfrak{f}' = \mathfrak{f}_1'\mathfrak{f}_2'$ *y* $\psi(\mathfrak{f}'/\mathfrak{f}) = \mathfrak{f}_1'/\mathfrak{f}_1 \times \mathfrak{f}_2'/\mathfrak{f}_2$.

DEMOSTRACIÓN. Sean $f_1' = \mathfrak{f}' + \mathfrak{f}_1$ y $f_2' = \mathfrak{f}' + \mathfrak{f}_2$, los cuales claramente son ideales de $\mathcal{O}_F$ y $\mathfrak{f}_1 \subseteq \mathfrak{f}_1'$, $\mathfrak{f}_2 \subseteq \mathfrak{f}_2'$.

Veremos que $\mathfrak{f}' = \mathfrak{f}_1'\mathfrak{f}_2'$. Como $\mathfrak{f}' \subseteq \mathfrak{f}_1'$ y $\mathfrak{f}' \subseteq \mathfrak{f}_2'$, se tiene $\mathfrak{f}' \subseteq \mathfrak{f}_1' \cap \mathfrak{f}_2' = \mathfrak{f}_1'\mathfrak{f}_2'$. Además, $\mathfrak{f}_1'\mathfrak{f}_2' = (\mathfrak{f}' + \mathfrak{f}_1)(\mathfrak{f}' + \mathfrak{f}_2) = \mathfrak{f}'\mathfrak{f}' + \mathfrak{f}'\mathfrak{f}_1 + \mathfrak{f}'\mathfrak{f}_2 + \mathfrak{f}_1\mathfrak{f}_2 \subseteq \mathfrak{f}'$.

Finalmente, $\psi(\mathfrak{f}'/\mathfrak{f}) = \mathfrak{f}_1'/\mathfrak{f}_1 \times \mathfrak{f}_2'/\mathfrak{f}_2$, se cumple por el lema anterior. □

Proposición 3.4. *Sean* $\mathfrak{f}_1, \mathfrak{f}_2$ *ideales no cero de* $\mathcal{O}_F$ *cuyas normas son primas relativas, es decir* $\text{mcd}(N(\mathfrak{f}_1), N(\mathfrak{f}_2)) = 1$ *y ponemos* $\mathfrak{f} = \mathfrak{f}_1\mathfrak{f}_2$*. Entonces:*

(i) *Existe algún orden* $\mathcal{O}$ *en* F *con conductor* $\mathfrak{f}$ *si y sólo si existen órdenes* $\mathcal{O}_1$ *y* $\mathcal{O}_2$ *con conductores* $\mathfrak{f}_1$ *y* $\mathfrak{f}_2$ *respectivamente.*

(ii) *Supongamos que* $\mathfrak{f}_1$ *y* $\mathfrak{f}_2$ *son ideales conductores y sean* $n_1, n_2 \in \mathbb{N}$ *el número de órdenes diferentes en* F *con conductores* $\mathfrak{f}_1$ *y* $\mathfrak{f}_2$ *respectivamente. Entonces existen* n_1n_2 *órdenes en* F *con conductor* $\mathfrak{f}$*.*

DEMOSTRACIÓN. (i) Para cada $i = 1, 2$, sean $e_i \in \mathcal{O}_F/\mathfrak{f}$ los idempotentes ortogonales con $\psi(e_1) = (1 + \mathfrak{f}_1, \mathfrak{f}_2)$ y $\psi(e_2) = (\mathfrak{f}_1, 1 + \mathfrak{f}_2)$. Como $\text{mcd}(N(\mathfrak{f}_1), N(\mathfrak{f}_2)) = 1$, existen $u_1, u_2 \in \mathbb{Z}$ tales que $1 = u_1N(\mathfrak{f}_1) + u_2N(\mathfrak{f}_2)$, de donde

$$e_i = 1 - u_iN(\mathfrak{f}_i) + \mathfrak{f} \in (\mathbb{Z} + \mathfrak{f})/\mathfrak{f}. \tag{7}$$

Usando el lema 1.60,

$$\begin{aligned} \psi(e_1) &= \psi(1 - u_1N(\mathfrak{f}_1) + \mathfrak{f}) \\ &= (1 - u_1N(\mathfrak{f}_1) + \mathfrak{f}_1, 1 - u_1N(\mathfrak{f}_1) + \mathfrak{f}_2) \\ &= (1 + (-u_1N(\mathfrak{f}_1)) + \mathfrak{f}_1, u_2N(\mathfrak{f}_2) + \mathfrak{f}_2) \\ &= (1 + \mathfrak{f}_1, \mathfrak{f}_2). \end{aligned}$$

Análogamente $\psi(e_2) = (\mathfrak{f}_1, 1 + \mathfrak{f}_2)$, es decir, e_1 y e_2 están bien definidos.

Ahora supongamos que $\mathcal{O}$ es un orden en F con conductor $\mathfrak{f}$, por el lema 2.15 (iii), $A = \mathcal{O}/\mathfrak{f}$ es un subanillo de $\mathcal{O}_F/\mathfrak{f}$ que contiene a $(\mathbb{Z} + \mathfrak{f})/\mathfrak{f}$ y, por (7), $e_1, e_2 \in \mathcal{O}/\mathfrak{f}$.

Notemos que $\psi(A) = \psi(e_1A) + \psi(e_2A)$, esto sucede pues si $l + \mathfrak{f} \in A$ con $l \in \mathcal{O}$ es cualquier elemento, se tiene

$$\psi(l + \mathfrak{f}) = (l + \mathfrak{f}_1, l + \mathfrak{f}_2)$$

y

$$\begin{aligned}\psi(e_1(l+\mathfrak{f}))+\psi(e_2(l+\mathfrak{f})) &= \psi(e_1l+\mathfrak{f})+\psi(e_2l+\mathfrak{f})\\ &= (e_1l+\mathfrak{f}_1, e_1l+\mathfrak{f}_2)+(e_2l+\mathfrak{f}_1, e_2l+\mathfrak{f}_2)\\ &= (l+\mathfrak{f}_1, \mathfrak{f}_2)+(\mathfrak{f}_1, l+\mathfrak{f}_2)\\ &= (l+\mathfrak{f}_1, l+\mathfrak{f}_2).\end{aligned}$$

Veremos que $\psi(e_1A)+\psi(e_2A)=\mathcal{O}_1/\mathfrak{f}_1\times\mathcal{O}_2/\mathfrak{f}_2$, con $\mathcal{O}_1=\mathcal{O}+\mathfrak{f}_1$ y $\mathcal{O}_2=\mathcal{O}+\mathfrak{f}_2$. Para $l+\mathfrak{f}\in A$, tenemos $\psi(e_1(l+\mathfrak{f}))+\psi(e_2(l+\mathfrak{f}))=(l+\mathfrak{f}_1, l+\mathfrak{f}_2)\in\mathcal{O}/\mathfrak{f}_1\times\mathcal{O}/\mathfrak{f}_2\subseteq\mathcal{O}_1/\mathfrak{f}_1\times\mathcal{O}_2/\mathfrak{f}_2$, es decir $\psi(e_1A)+\psi(e_2A)\subseteq\mathcal{O}_1/\mathfrak{f}_1\times\mathcal{O}_2/\mathfrak{f}_2$.

Sea $(m_1+\mathfrak{f}_1, m_2+\mathfrak{f}_2)\in\mathcal{O}_1/\mathfrak{f}_1\times\mathcal{O}_2/\mathfrak{f}_2$, veremos que existe $l\in\mathcal{O}$ tal que $\psi(e_1(l+\mathfrak{f}))+\psi(e_2(l+\mathfrak{f}))=(m_1+\mathfrak{f}_1, m_2+\mathfrak{f}_2)$. Necesitamos que $(l+\mathfrak{f}_1, l+\mathfrak{f}_2)=(m_1+\mathfrak{f}_1, m_2+\mathfrak{f}_2)$, lo anterior se cumple si y sólo si $m_1+\mathfrak{f}_1=l+\mathfrak{f}_1$ y $m_2+\mathfrak{f}_2=l+\mathfrak{f}_2$, de donde $m_1-l\in\mathfrak{f}_1$ y $m_2-l\in\mathfrak{f}_2$, luego $m_1-l=\beta_1$ con $\beta_1\in\mathfrak{f}_1$ y $m_2-l=\beta_2$ con $\beta_2\in\mathfrak{f}_2$, lo que implica $l=m_1-\beta_1=m_2-\beta_2$. Entonces, $\psi(e_1(l+\mathfrak{f}))+\psi(e_2(l+\mathfrak{f}))=(m_1+\mathfrak{f}_1, m_2+\mathfrak{f}_2)$, es decir, $\mathcal{O}_1/\mathfrak{f}_1\times\mathcal{O}_2/\mathfrak{f}_2\subseteq\psi(e_1A)+\psi(e_2A)$. Así, $\psi(\mathcal{O}/\mathfrak{f})=\mathcal{O}_1/\mathfrak{f}_1\times\mathcal{O}_2/\mathfrak{f}_2$ con $\mathcal{O}_1$ y $\mathcal{O}_2$ órdenes en F.

Probaremos que $\mathfrak{f}_i$ es el conductor de $\mathcal{O}_i$.

Supongamos que h_1 y h_2 son conductores de $\mathcal{O}_1$ y $\mathcal{O}_2$ respectivamente, notemos que $\mathfrak{f}_1\subseteq\mathcal{O}_1$ y $\mathfrak{f}_2\subseteq\mathcal{O}_2$, por el lema 2.15 (ii), $\mathfrak{f}_1\subseteq h_1$ y $\mathfrak{f}_2\subseteq h_2$. Por otro lado, $h_1+h_2=\mathcal{O}_F$ pues $\mathfrak{f}_1+\mathfrak{f}_2=\mathcal{O}_F$ y por el lema 3.1, $h_1h_2=\mathfrak{f}$, de donde $h_1h_2=\mathfrak{f}_1\mathfrak{f}_2$ y por la factorización única en $\mathcal{O}_F$, $h_1=\mathfrak{f}_1$ y $h_2=\mathfrak{f}_2$.

Inversamente, si $\mathcal{O}_1$ y $\mathcal{O}_2$ son órdenes en F con conductores $\mathfrak{f}_1$ y $\mathfrak{f}_2$ respectivamente, por el lema 3.1, existe un orden $\mathcal{O}=\mathcal{O}_1\cap\mathcal{O}_2$ con conductor $\mathfrak{f}=\mathfrak{f}_1\mathfrak{f}_2$.

(ii) Como $\psi(\mathcal{O}/\mathfrak{f})=\mathcal{O}_1/\mathfrak{f}_1\times\mathcal{O}_2/\mathfrak{f}_2$, existe una biyección entre órdenes con conductor $\mathfrak{f}$ y parejas de órdenes con conductores $\mathfrak{f}_1$ y $\mathfrak{f}_2$ respectivamente. Por lo tanto, si $\mathfrak{f}_1$ tiene n_1 órdenes distintos y $\mathfrak{f}_2$ tiene n_2 órdenes distintos, por el lema 3.1, $\mathfrak{f}$ tendrá n_1n_2 órdenes distintos. □

Teorema 3.5 (Furtwängler parte 1)**.** *Sea $\mathfrak{f}$ un ideal no cero de $\mathcal{O}_F$ con $\mathfrak{f}=\mathfrak{f}_1\mathfrak{f}_2\cdots\mathfrak{f}_m$ la factorización tal que $N(\mathfrak{f}_i)=p_i^{k_i}$, donde $k_i\in\mathbb{N}$ y $p_1,\ldots,p_m$ son primos racionales distintos dos a dos. Entonces, existe un orden $\mathcal{O}$ en F con conductor $\mathfrak{f}$ si y sólo si para todo $1\leq i\leq m$ existen órdenes $\mathcal{O}_i$ en F con conductores $\mathfrak{f}_i$.*

Más aún, si $n_i\in\mathbb{N}$ es el número de órdenes diferentes en F con conductor $\mathfrak{f}_i$, entonces existen exactamente $n_1n_2\cdots n_m$ órdenes distintos en F con conductor $\mathfrak{f}$.

DEMOSTRACIÓN. La demostración se hará por inducción sobre m. La base de inducción se cumple por la proposición 3.4.

Supongamos que el resultado se cumple hasta m. Veremos que también es válido para para $m+1$. Sea $\mathfrak{f}=\mathfrak{f}_1\mathfrak{f}_2\cdots\mathfrak{f}_m\mathfrak{f}_{m+1}$, con $\text{mcd}(\mathfrak{f}_i,\mathfrak{f}_j)=1$ para $i\neq j$. Claramente $\mathfrak{f}=h\mathfrak{f}_{m+1}$, con $h=\mathfrak{f}_1\mathfrak{f}_2\cdots\mathfrak{f}_m$, por el lema 1.62, tenemos $\mathfrak{f}_1\mathfrak{f}_2\cdots\mathfrak{f}_m+\mathfrak{f}_{m+1}=\mathcal{O}_F$, es decir, $\text{mcd}(h,\mathfrak{f}_{m+1})=1$. Ahora, si existe un orden $\mathcal{O}$ en F con conductor $\mathfrak{f}$, por la proposición 3.4 (i), existen órdenes $\mathcal{O}_1$ y $\mathcal{O}_2$ en F con conductores h y $\mathfrak{f}_{m+1}$ respectivamente. Por hipótesis de inducción existen órdenes $\mathcal{O}_1', \mathcal{O}_2', \ldots, \mathcal{O}_m'$ con conductores $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$ respectivamente y así existen órdenes $\mathcal{O}_1', \mathcal{O}_2', \ldots, \mathcal{O}_m', \mathcal{O}_2$ con conductores $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m, \mathfrak{f}_{m+1}$.

Ahora supongamos que existen órdenes $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m, \mathcal{O}_{m+1}$ en F con conductores $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m, \mathfrak{f}_{m+1}$ respectivamente. Por hipótesis de inducción, $\mathcal{O}'=\mathcal{O}_1\cap\mathcal{O}_2\cap\cdots\cap\mathcal{O}_m$

es un orden en F con conductor h y por el lema 3.1, $\mathcal{O}' \cap \mathcal{O}_{m+1}$ es un orden en F con conductor $\mathfrak{f}$.

Si n_i es el número de órdenes distintos en F con conductor $\mathfrak{f}_i$ para cada $1 \leq i \leq m+1$, entonces por hipótesis de inducción existen exactamente $n = n_1 n_2 \cdots n_m$ órdenes distintos con conductor h y, usando la proposición 3.4 (ii), existen exactamente nn_{m+1} órdenes distintos con conductor $\mathfrak{f}$. □

Lema 3.6. *Sea p un primo racional, tal que $\langle p \rangle = p\mathcal{O}_F = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$, con P_i un ideal primo con $N(P_i) = p^{f_i}$, para cada i. Entonces, si $i \in \{1, 2, \ldots, g\}$ y $k \in \mathbb{N}$, tenemos lo siguiente:*

(i) *El entero más chico $c \in \mathbb{N}$ con $p^c \in P_i^k$, está dado por $c = \left\lceil \frac{k}{e_i} \right\rceil$.*[2]

(ii) *Sea $c = \left\lceil \frac{k}{e_i} \right\rceil$. Entonces $(\mathbb{Z} + P_i^k)/P_i^k$ consiste de exactamente p^c elementos distintos de $\mathcal{O}_F/P_i^k$.*

(iii) *Si $k \equiv 1 \pmod{e_i}$, entonces P_i^{k-1}/P_i^k contiene exactamente p elementos de $(\mathbb{Z} + P_i^k)/P_i^k$.*
Si $k \not\equiv 1 \pmod{e_i}$, entonces P_i^{k-1}/P_i^k contiene sólo un elemento de $(\mathbb{Z}+P_i^k)/P_i^k$.

DEMOSTRACIÓN. (i) Dado que los P_i se encuentran por encima de p, tenemos $P_i^k \cap \mathbb{Z} = p^c\mathbb{Z}$ para algún $c \in \mathbb{N}$ y en particular $p^c =$mín$(P_i^k \cap \mathbb{N})$. Esto significa que p^c es la mínima potencia de p con $P_i^k | \langle p^c \rangle$, es decir p^c es la mínima potencia de p que hace que $\langle p^c \rangle \subseteq P_i^k$. Como $\langle p^c \rangle = P_1^{ce_1} P_2^{ce_2} \cdots P_g^{ce_g}$, se tiene $P_1^{ce_1} \cdots P_i^{ce_i} \cdots P_g^{ce_g} = P_i^k I$, con I un ideal no cero de $\mathcal{O}_F$, por tanto c es el entero más chico con $k \leq ce_i$, es decir $c = \left\lceil \frac{k}{e_i} \right\rceil$.

(ii) Sea $c = \left\lceil \frac{k}{e_i} \right\rceil$. Demostraremos que $(\mathbb{Z}+P_i^k)/P_i^k = \{P_i^k, 1+P_i^k, \ldots, (p^c-1)+P_i^k\}$.

Primero veremos que las anteriores son todas la clases. Si $d + P_i^k \in (\mathbb{Z} + P_i^k)/P_i^k$, entonces $d = a + b$ con $a \in \mathbb{Z}$ y $b \in P_i^k$, es decir $d + P_i^k = (a + b) + P_i^k = a + P_i^k$. Por el algoritmo de la división en $\mathbb{Z}$, tenemos $a = p^c t + r$, con $0 \leq r < p^c$. Así, $d + P_i^k = (p^c t + r) + P_i^k$ y dado que $p^c \in P_i^k$, se sigue $d + P_i^k = r + P_i^k$, con $0 \leq r < p^c$. Por lo tanto, $P_i^k, 1 + P_i^k, \ldots, (p^c - 1) + P_i^k$ son todas las clases.

Ahora probaremos que son clases distintas.

Sean $\alpha + P_i^k, \beta + P_i^k \in \{P_i^k, 1 + P_i^k, \ldots, (p^c - 1) + P_i^k\}$ con $0 \leq \alpha < \beta < p^c$ y supongamos que $\alpha + P_i^k = \beta + P_i^k$, entonces $\alpha - \beta \in P_i^k$, de donde $\alpha - \beta \equiv 0 \pmod{P_i^k}$, lo que implica $\alpha - \beta \equiv 0 \pmod{P_i}$, luego $\beta - \alpha \in P_i$ y como $\beta - \alpha \in \mathbb{Z}$, tenemos $\beta - \alpha \in P_i \cap \mathbb{Z} = p^c\mathbb{Z}$ y $0 \leq \beta - \alpha < p^c$, así $\alpha = \beta$.

(iii) Supongamos que $k \equiv 1 \pmod{e_i}$. Entonces existe $m \in \mathbb{Z}$ tal que $k = 1 + me_i$. Luego $m + 1 = \left\lceil \frac{k}{e_i} \right\rceil$ y, por la parte (ii),

$$(\mathbb{Z} + P_i^k)/P_i^k = \{P_i^k, 1 + P_i^k, \ldots, (p^{m+1} - 1) + P_i^k\}.$$

[2]Recordemos que $\lceil q \rceil$ es el entero más chico, mayor o igual que q, para $q \in \mathbb{R}$.

Dado que $m = \left\lceil \frac{k-1}{e_i} \right\rceil$, por la parte (i), se cumple $p^m =$mín$(P_i^{k-1} \cap \mathbb{N})$, es decir p^m es la mínima potencia de p tal que $p^m \in P_i^{k-1}$. Por tanto, P_i^{k-1}/P_i^k contiene exactamente p elementos de $(\mathbb{Z}+P_i^k)/P_i^k$ los cuales son $\{P_i^k, p^m+P_i^k, 2p^m+P_i^k, \ldots, (p-1)p^m+P_i^k\}$.

Supongamos que $k \not\equiv 1 \pmod{e_i}$. Entonces $\left\lceil \frac{k-1}{e_i} \right\rceil = \left\lceil \frac{k}{e_i} \right\rceil = n_0 \in \mathbb{N}$, usando un argumento similar, P_i^{k-1}/P_i^k contiene exactamente un elemento de $(\mathbb{Z}+P_i^k)/P_i^k$, el cual es P_i^k. □

Lema 3.7. *P_i^k es el conductor del orden $\mathbb{Z}+P_i^k$ si y sólo si $P_i^{k-1}/P_i^k \nsubseteq (\mathbb{Z}+P_i^k)/P_i^k$.*

DEMOSTRACIÓN. Supongamos que P_i^k es el conductor del orden $\mathbb{Z}+P_i^k$, dado que $P_i^{k-1} \nsubseteq P_i^k$, por el lema 2.15 (ii), $P_i^{k-1} \nsubseteq \mathbb{Z}+P_{i^k}$. Por tanto, $P_i^{k-1}/P_i^k \nsubseteq (\mathbb{Z}+P_i^k)/P_i^k$.

Ahora supongamos que $P_i^{k-1}/P_i^k \nsubseteq (\mathbb{Z}+P_i^k)/P_i^k$ (es decir, $P_i^{k-1} \nsubseteq \mathbb{Z}+P_i^k$) y sea h el conductor de $\mathbb{Z}+P_i^k$.

Notemos que $P_i^k \subseteq P_i^{k-1} \subseteq \cdots \subseteq P_i^2 \subseteq P_i$ son los únicos ideales que contienen a P_i^k. Como $P_i^k \subseteq \mathbb{Z}+P_i^k$, por el lema 2.15 (ii), $P_i^k \subseteq h$ pero $P_i^{k-1} \nsubseteq h$. Por lo tanto, $P_i^k = h$. □

Proposición 3.8. *Sea p un primo racional tal que $\langle p \rangle = P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}$ es su factorización en $\mathcal{O}_F$, con P_i un ideal primo tal que $N(P_i) = p^{f_i}$ para cada i. Si $i \in \{1,\ldots,g\}$ y $k \in \mathbb{N}$, entonces P_i^k es un ideal conductor si y sólo si se da una de las siguientes dos afirmaciones:*

(i) $f_i \geq 2$.
(ii) $f_i = 1$ y $k \not\equiv 1 \pmod{e_i}$.

DEMOSTRACIÓN. Supongamos que P_i^k es un ideal conductor y $f_i = 1$. Veremos que $k \not\equiv 1 \pmod{e_i}$.

Como P_i^k es el conductor del orden $\mathbb{Z}+P_i^k$, por el lema 3.7, $P_i^{k-1}/P_i^k \nsubseteq (\mathbb{Z}+P_i^k)/P_i^k$ y sabemos que P_i^{k-1}/P_i^k consiste de $N(P_i) = p^{f_i}$ elementos. Como $f_i = 1$, entonces P_i^{k-1}/P_i^k consiste de p elementos y, además, $P_i^{k-1}/P_i^k \nsubseteq (\mathbb{Z}+P_i^k)/P_i^k$, es decir, P_i^{k-1}/P_i^k no consiste de p elementos de $(\mathbb{Z}+P_i^k)/P_i^k$. Por el lema 3.6 (iii), $k \not\equiv 1 \pmod{e_i}$.

Ahora si $f_i = 1$ y $k \not\equiv 1 \pmod{e_i}$. Por el lema 3.6 (iii), $P_i^{k-1}/P_i^k \nsubseteq (\mathbb{Z}+P_i^k)/P_i^k$ y por el lema 3.7, P_i^k es el conductor del orden $\mathbb{Z}+P_i^k$. Por lo tanto, P_i^k es un ideal conductor.

Si $f_i \geq 2$, y dado que $|P_i^{k-1}/P_i^k| = p^{f_i}$, por lema 3.6 (iii), $P_i^{k-1}/P_i^k \nsubseteq (\mathbb{Z}+P_i^k)/P_i^k$ (en este caso no tiene relevancia si $k \equiv 1 \pmod{e_i}$ ó si $k \not\equiv 1 \pmod{e_i}$), por el lema 3.7, P_i^k es el conductor del orden $\mathbb{Z}+P_i^k$. Por lo tanto, P_i^k es un ideal conductor. □

Lema 3.9. *Sean $\mathfrak{f} = P_1^{k_1}P_2^{k_2}\cdots P_g^{k_g}$ donde los P_i son ideales primos distintos y $\mathcal{O} = \mathbb{Z}+\mathfrak{f}$. Entonces $\mathfrak{f}$ es conductor del orden $\mathcal{O}$ si y sólo si para todo $i \in \{1,2,\ldots,g\}$ con $k_i \geq 1$ se cumple que $\mathfrak{f}_i \nsubseteq \mathcal{O}$, donde $\mathfrak{f}_i = \mathfrak{f}P_i^{-1}$.*

DEMOSTRACIÓN. Supongamos que $\mathfrak{f}$ es el conductor de $\mathcal{O}$ y $\mathfrak{f}_i \subseteq \mathcal{O}$ para algún $i \in \{1,\ldots,g\}$. Por el lema 2.15 (ii), $\mathfrak{f}_i \subseteq \mathfrak{f}$ y notemos que $\mathfrak{f} \subseteq \mathfrak{f}_i$, entonces $\mathfrak{f} = \mathfrak{f}_i = \mathfrak{f}P_i^{-1}$, lo que implica $P_i = \mathcal{O}_F$, lo cual es una contradicción.

Supongamos que para todo $1 \leq i \leq g$, $\mathfrak{f}_i \nsubseteq \mathcal{O}$ y sea h el conductor de $\mathcal{O}$. Por el lema 2.15 (ii), $\mathfrak{f} \subseteq h$ y $\mathfrak{f}_i \nsubseteq h$. Notemos que por definición, $\mathfrak{f}_i$ es el ideal más chico que contiene a $\mathfrak{f}$, por tanto $h = \mathfrak{f}$. □

Lema 3.10. *Sean* $\mathfrak{f} = P_1^{k_1} P_2^{k_2} \cdots P_g^{k_g}$, $\mathfrak{f}_i = \mathfrak{f} P_i^{-1}$ *con los* P_i *ideales primos distintos y* $\psi : \mathcal{O}_F/\mathfrak{f} \to \mathcal{O}_F/P_1^{k_1} \times \cdots \times \mathcal{O}_F/P_g^{k_g}$ *el isomorfismo de anillos dado por el teorema chino del residuo, con* $k_i \geq 1$. *Entonces,*

$$\psi(\mathfrak{f}_i/\mathfrak{f}) = \{P_1^{k_1}\} \times \cdots \times \{P_{i-1}^{k_{i-1}}\} \times P_i^{k_i-1}/P_i^{k_i} \times \{P_{i+1}^{k_{i+1}}\} \times \cdots \times \{P_g^{k_g}\}.$$

DEMOSTRACIÓN.

Lo anterior se cumple ya que:

$$\begin{aligned} \psi(\mathfrak{f}_i/\mathfrak{f}) \quad &= \quad \mathfrak{f}_i/P_1^{k_1} \times \cdots \times \mathfrak{f}_i/P_{i-1}^{k_{i-1}} \times \mathfrak{f}_i/P_i^{k_i} \times \mathfrak{f}_i/P_{i+1}^{k_{i+1}} \times \cdots \times \mathfrak{f}_i/P_g^{k_g} \\ &\text{como} \quad \mathfrak{f}_j \subseteq P_j^{k_j} \text{ para } j \in \{1, 2, \ldots, i-1, i+1, \ldots, g\}, \\ &= \quad \{P_1^{k_1}\} \times \cdots \times \{P_{i-1}^{k_{i-1}}\} \times P_i^{k_i-1}/P_i^{k_i} \times \{P_{i+1}^{k_{i+1}}\} \times \cdots \times \{P_g^{k_g}\}. \end{aligned}$$

□

Proposición 3.11. *Sean* $\mathcal{O} = \mathbb{Z} + \mathfrak{f}$ *con* $\mathfrak{f} = P_1^{k_1} P_2^{k_2} \cdots P_g^{k_g}$ *donde los* P_i *son ideales distintos con* $N(P_i) = p^{f_i}$ *para cada* $i \in \{1, 2, \ldots, g\}$, $k_i \in \mathbb{N}$ *y* $\mathfrak{f}_i = \mathfrak{f} P_i^{-1}$. *Entonces* $\mathfrak{f}_i \subseteq \mathcal{O}$ *si y sólo si* $f_i = 1$, $k_i \equiv 1 \pmod{e_i}$ *y para todo* $j \in \{1, 2, \ldots, g\}$ *con* $j \neq i$, *tenemos* $\left\lceil \dfrac{k_j}{e_j} \right\rceil \leq \dfrac{k_i - 1}{e_i}$.

DEMOSTRACIÓN. Supongamos que $\mathfrak{f}_i \subseteq \mathcal{O}$, luego $\mathfrak{f}_i/\mathfrak{f} \subseteq \mathcal{O}/\mathfrak{f}$ y $\psi(\mathfrak{f}_i/\mathfrak{f}) \subseteq \psi(\mathcal{O}/\mathfrak{f})$. Por el lema 3.10, $P_i^{k_i-1}/P_i^{k_i} \subseteq (\mathbb{Z} + P_i^{k_i})/P_i^{k_i}$ pues $\psi(\mathcal{O}/\mathfrak{f}) = (\mathbb{Z} + P_1^{k_1})/P_1^{k_1} \times \cdots \times (\mathbb{Z} + P_i^{k_i})/P_i^{k_i} \times \cdots \times (\mathbb{Z} + P_g^{k_g})/P_g^{k_g}$. Entonces $P_i^{k_i-1} \subseteq \mathbb{Z} + P_i^{k_i}$, luego $P_i^{k_i}$ no es un ideal conductor. Por la proposición 3.8, $f_i = 1$ y $k_i \equiv 1 \pmod{e_i}$.

Sea $m = \dfrac{k_i - 1}{e_i} \in \mathbb{Z}$. De la prueba del lema 3.6 (iii), tenemos

$$P_i^{k_i-1}/P_i^{k_i} = \{P_i^{k_i}, p^m + P_i^{k_i}, \ldots, (p-1)p^m + P_i^{k_i}\}$$

y notemos que p^{m+1} es la mínima potencia de p tal que $p^{m+1} \in P_i^{k_i}$. Usando el lema 3.10, existe algún $a \in \mathbb{Z}$ de tal forma que $a + \mathfrak{f} \in \mathfrak{f}_i/\mathfrak{f}$ y $\psi(a + \mathfrak{f}) = (P_1^{k_1}, \ldots, P_{i-1}^{k_{i-1}}, p^m + P_i^{k_i}, P_{i+1}^{k_{i+1}}, \ldots, P_g^{k_g})$.

Dado que p^{m+1} es la mínima potencia de p tal que $p^{m+1} \in P_i^{k_i}$, tenemos $a \equiv p^m \pmod{p^{m+1}}$. Así, $a = p^m a_0$, con $a_0 = 1 + pt \in \mathbb{Z}$, $t \in \mathbb{Z}$ y $p \nmid a_0$. De lo anterior, para todo $0 \leq j < g$, con $j \neq i$, se cumple $a = p^m a_0 \in P_j^{k_j}$, lo que implica $\langle p^m a_0 \rangle \subseteq P_j^{k_j}$ y $P_j^{k_j} \mid \langle p^m \rangle \langle a_0 \rangle$. Como $p \nmid a_0$ se tiene que $\langle a_0 \rangle$ y $P_j^{k_j}$ son primos relativos y, por tanto, $\langle p^m \rangle \subseteq P_j^{k_j}$, es decir $p^m \in P_j^{k_j}$. Como $\left\lceil \dfrac{k_j}{e_j} \right\rceil$ es el entero más chico tal que $p^{\left\lceil \frac{k_j}{e_j} \right\rceil} \in P_j^{k_j}$, se tiene $\left\lceil \dfrac{k_j}{e_j} \right\rceil \leq m = \dfrac{k_i - 1}{e_i}$.

Inversamente, supongamos que $f_i = 1$, $k_i \equiv 1 \pmod{e_i}$ y para todo $j \in \{1, 2, \ldots, g\}$ con $j \neq i$, tenemos $\left\lceil \frac{k_j}{e_j} \right\rceil \leq \frac{k_i - 1}{e_i}$. Como $k_i \equiv 1 \pmod{e_i}$, tenemos $m = \frac{k_i - 1}{e_i}$, con $m \in \mathbb{Z}$, luego, $\left\lceil \frac{k_j}{e_j} \right\rceil \leq m$.

Veremos que $\psi(\{\nu p^m + \mathfrak{f} : 0 \leq \nu < p\}) = \psi(\mathfrak{f}_i/\mathfrak{f})$. Sea $\nu_0 p^m + \mathfrak{f}$ cualquier elemento de $\{\nu p^m + \mathfrak{f} : 0 \leq \nu < p\}$, entonces

$$\begin{aligned}\psi(\nu_0 p^m + \mathfrak{f}) &= (\nu_0 p^m + P_1^{k_1}, \ldots, \nu_0 p^m + P_{i-1}^{k_{i-1}}, \nu_0 p^m + P_i^{k_i}, \nu_0 p^m + P_{i+1}^{k_{i+1}}, \ldots, \nu_0 p^m + P_g^{k_g}) \\ &= (P_1^{k_1}, \ldots, P_{i-1}^{k_{i-1}}, \nu_0 p^m + P_i^{k_i}, P_{i+1}^{k_{i+1}}, \ldots, P_g^{k_g}),\end{aligned}$$

dado que $\left\lceil \frac{k_j}{e_j} \right\rceil \leq m$ para $j \neq i$. Así, $\psi(\{\nu p^m + \mathfrak{f} : 0 \leq \nu < p\}) = \{P_1^{k_1}\} \times \cdots \times \{P_{i-1}^{k_{i-1}}\} \times P_i^{k_i - 1}/P_i^{K_i} \times \{P_{i+1}^{k_{i+1}}\} \times \cdots \times \{P_g^{k_g}\}$ y, por el lema 3.10,

$$\psi(\{\nu p^m + \mathfrak{f} : 0 \leq \nu < p\}) = \psi(\mathfrak{f}_i/\mathfrak{f}).$$

Como $\{\nu p^m + \mathfrak{f} : 0 \leq \nu < p\} \subseteq (\mathbb{Z} + \mathfrak{f})/\mathfrak{f} \subseteq \mathcal{O}/\mathfrak{f}$, $\psi(\mathfrak{f}_i/\mathfrak{f}) \subseteq \psi(\mathcal{O}/\mathfrak{f})$. Por lo tanto, $\mathfrak{f}_i \subseteq \mathcal{O}$. □

Teorema 3.12 (Furtwängler parte 2)**.** *Sea p un primo racional que se factoriza en $\mathcal{O}_F$ como*

$$p\mathcal{O}_F = P_1^{e_1} \cdots P_g^{e_g},$$

donde los $P_1, \ldots, P_g$ son ideales primos distintos dos a dos, cuya norma es $N(P_i) = p^{f_i}$, y $e_i, f_i, g \in \mathbb{N}$. Sea $0 \leq k_i \in \mathbb{Z}$ y ponemos

$$\mathfrak{f} = P_1^{k_1} \cdots P_g^{k_g}.$$

Entonces $\mathfrak{f}$ es el conductor de algún orden en F si y sólo si para cada $1 \leq i \leq g$ con $k_i \geq 1$ tenemos: si $f_i = 1$ y $k_i \equiv 1 \pmod{e_i}$, entonces existe algún $j \in \{1, \ldots, g\} \setminus \{i\}$ con $k_j > \frac{k_i - 1}{e_i} e_j$.

DEMOSTRACIÓN. Supongamos que $\mathfrak{f}$ es conductor de algún orden $\mathcal{O}$ en F, por el lema 3.9, $\mathfrak{f}_i \not\subseteq \mathcal{O}$, donde $\mathfrak{f}_i = \mathfrak{f}P_i^{-1}$. Tomando la negación de la proposición 3.11, en el caso en que $f_i = 1$ y $k_i \equiv 1 \pmod{e_i}$, existe algún $j \in \{1, \ldots, g\} \setminus \{i\}$ con $\left\lceil \frac{k_j}{e_j} \right\rceil > \frac{k_i - 1}{e_i}$, es decir, $k_j > \frac{k_i - 1}{e_i} e_j$.

Ahora supongamos que para cada $1 \leq i \leq g$ con $k_i \geq 1$ tenemos: si $f_i = 1$ y $k_i \equiv 1 \pmod{e_i}$, entonces existe algún $j \in \{1, \ldots, g\} \setminus \{i\}$ con $k_j > \frac{k_i - 1}{e_i} e_j$. Por la proposición 3.11 , $\mathfrak{f}_i \not\subseteq \mathcal{O}$ y por el lema 3.9, $\mathfrak{f}$ es el conductor del orden $\mathcal{O} = \mathbb{Z} + \mathfrak{f}$ en F. □

Con el teorema de Furtwängler podemos ver si un ideal del anillo de enteros es o no un ideal conductor, procediendo de la siguiente manera:

Sea I un ideal de $\mathcal{O}_F$.

(i) Factorizamos a I como $I = P_1^{k_1} P_2^{k_2} \cdots P_g^{k_g}$, con $P_1, \ldots, P_g$ ideales primos distintos.

(ii) Agrupamos los factores por bloques, de tal manera que cada bloque este sobre un mismo primo racional, digamos que:

$$I = (P_1^{k_1} P_2^{k_2} \cdots P_l^{k_l})(P_{l+1}^{k_{l+1}} \cdots P_m^{k_m}) \cdots (P_r^{k_r} \cdots P_g^{k_g}),$$

$$\text{con } \langle p_1 \rangle = P_1^{e_1} P_2^{e_2} \cdots P_l^{e_l}, \langle p_2 \rangle = P_{l+1}^{e_{l+1}} \cdots P_m^{e_m}, \ldots, \langle p_t \rangle = P_r^{e_r} \cdots P_l^{e_l}.$$

(iii) Finalmente con el teorema de Furtwängler parte 1, I es un ideal conductor si y sólo si cada cada bloque es un ideal conductor. Y para saber si cada bloque es un ideal conductor, usamos el teorema de Furtwängler parte 2.

3.2. Caracterización de los ideales conductor en un campo de números cuadrático

Sea F un campo de números cuadrático. Por el teorema 3.5, es suficiente concentrarnos en ideales $\mathfrak{f}$ de $\mathcal{O}_F$ cuya norma es potencia de algún primo racional p.

La caracterización de estos ideales $\mathfrak{f}$ depende de cómo el ideal principal $\langle p \rangle$ se factoriza en $\mathcal{O}_F$, para lo cual tenemos tres posibilidades. Después utilizaremos la proposición 3.8 y el teorema 3.12 para encontrar todos los ideales conductores en cada caso.

Caso 1: p es inerte, es decir $\langle p \rangle = P_1$ ($e_1 = 1$ y $f_1 = 2$) con P_1 un ideal primo.

Sea $\mathfrak{f} = P_1^{k_1}$, con $k_1 \in \mathbb{N}$. Como $f_1 \geq 2$, por la proposición 3.8, $\mathfrak{f} = P_1^{k_1}$ es un conductor para todo $k_1 \in \mathbb{N}$.

Caso 2: p es totalmente ramificado, es decir $\langle p \rangle = P_1^2$ ($e_1 = 2$ y $f_1 = 1$) con p_1 un ideal primo.

Sea $\mathfrak{f} = P_1^{k_1}$,con $k_1 \in \mathbb{N}$. Por la proposición 3.8, $\mathfrak{f}$ es un conductor si y sólo si $k_1 \not\equiv 1 \pmod 2$, es decir $\mathfrak{f}$ es conductor si y sólo si $k_1 = 2d$, con $d \in \mathbb{N}$.

Así, $\mathfrak{f} = P_1^{2d}$ es un conductor para $d \in \mathbb{N}$.

Caso 3: p se descompone totalmente, es decir $\langle p \rangle = P_1 P_2$ ($e_1 = f_1 = 1$ y $e_2 = f_2 = 1$) con P_1 y P_2 ideales primos.

Sea $\mathfrak{f} = P_1^{k_1} P_2^{k_2}$, con $k_1, k_2 \in \mathbb{N}$. Usaremos el teorema 3.12 para ver las condiciones que deben cumplir k_1 y k_2 para que $\mathfrak{f}$ sea un conductor.

- Condiciones para k_1:
  Como $e_1 = 1$ y $f_1 = 1$, tenemos $k_1 \equiv 1 \pmod{e_1}$ siempre sucede. Por el teorema 3.12, necesitamos que $k_2 > \dfrac{k_1 - 1}{e_1} e_2 = k_1 - 1$, lo que implica $k_2 \geq k_1$.
- Condiciones para k_2:
  Como $e_2 = 1$ y $f_2 = 1$, entonces $k_2 \equiv 1 \pmod{e_2}$ siempre sucede, por el teorema 3.12, queremos $k_1 > \dfrac{k_2 - 1}{e_2} e_1 = k_2 - 1$, lo que implica $k_1 \geq k_2$.

Por nuestras condiciones anteriores necesitamos $k_1 = k_2$. Por lo tanto, $\mathfrak{f}$ es conductor si y sólo si $\mathfrak{f} = (P_1 P_2)^{k_1}$ para $k_1 \in \mathbb{N}$.

Lo anterior lo resumimos en la siguiente tabla.

Descomposición de p	Conductor
$\langle p \rangle = p\mathcal{O}_F$	$\mathfrak{f} = \langle p \rangle^t, t \in \mathbb{N}$
$\langle p \rangle = P^2$	$\mathfrak{f} = P^{2t}, t \in \mathbb{N}$
$\langle p \rangle = P_1 P_2$	$\mathfrak{f} = (P_1 P_2)^t, t \in \mathbb{N}$

Usando las proposiciones 1.69 y 1.70 tenemos las siguientes tablas, para ideales en $F = \mathbb{Q}(\sqrt{d})$, con d un entero libre de cuadrados.

Descomposición de $p \neq 2$	Conductor
$\langle p\rangle = p\mathcal{O}_F$	$\mathfrak{f} = \langle p\rangle^t, t \in \mathbb{N}$
$\langle p\rangle = \langle p, \sqrt{d}\rangle^2$	$\mathfrak{f} = \langle p, \sqrt{d}\rangle^{2t}, t \in \mathbb{N}$
$\langle p\rangle = \langle p, a+\sqrt{d}\rangle\langle p, a-\sqrt{d}\rangle$	$\mathfrak{f} = \langle p, a+\sqrt{d}\rangle^t\langle p, a-\sqrt{d}\rangle^t, t \in \mathbb{N}$

Descomposición de 2	Conductor
$\langle 2\rangle = 2\mathcal{O}_F$	$\mathfrak{f} = \langle p\rangle^t, t \in \mathbb{N}$
$\langle 2\rangle = \langle 2, 1+\sqrt{d}\rangle^2$	$\mathfrak{f} = \langle 2, 1+\sqrt{d}\rangle^{2t}, t \in \mathbb{N}$
$\langle 2\rangle = \left\langle 2, \frac{1+\sqrt{d}}{2}\right\rangle\left\langle 2, \frac{1-\sqrt{d}}{2}\right\rangle$	$\mathfrak{f} = \left\langle 2, \frac{1+\sqrt{d}}{2}\right\rangle^t\left\langle 2, \frac{1-\sqrt{d}}{2}\right\rangle^t, t \in \mathbb{N}$

Ejemplo 3.13. *Sea $F = \mathbb{Q}(i)$, con $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}i$. Veremos si el ideal*

$$I = \langle 13, 3-2i\rangle^2\langle 3\rangle^2\langle 5, 1-2i\rangle^3\langle 13, 3+2i\rangle^2\langle 5, 1+2i\rangle^3$$

es un ideal conductor.

Agrupamos los factores por bloques.

$$I = \langle 3\rangle^2(\langle 5, 1+2i\rangle^3\langle 5, 1-2i\rangle^3)(\langle 13, 3-2i\rangle^2\langle 13, 3+2i\rangle^2),$$

con $\langle 3\rangle$ ideal primo, $\langle 5\rangle = \langle 5, 1+2i\rangle\langle 5, 1-2i\rangle$ y $\langle 13\rangle = \langle 13, 3-2i\rangle\langle 13, 3+2i\rangle$.

Finalmente, por el teorema de Furtwängler parte 2, $\langle 3\rangle^2$, $(\langle 5, 1+2i\rangle^3\langle 5, 1-2i\rangle^3)$ y $(\langle 13, 3-2i\rangle^2\langle 13, 3+2i\rangle^2)$ son ideales conductor. Por lo tanto, por el teorema de Furtwängler parte 1, I es un ideal conductor.

3.3. Caracterización de los ideales conductor en un campo de números cúbico

Sea F un campo de números cubico. De manera análoga a la sección anterior veremos cuáles son los ideales conductores para este caso.

Caso 1: p es inerte, es decir $\langle p\rangle = P_1$ ($e_1 = 1$, $f_1 = 3$) con P_1 un ideal primo .

Sea $\mathfrak{f} = P_1^{k_1}$, con $k_1 \in \mathbb{N}$. Como $f_1 \geq 2$, por la proposición 3.8, $\mathfrak{f} = P_1^{k_1}$ es un conductor para todo $k_1 \in \mathbb{N}$.

Caso 2: p se descompone totalmente, es decir $\langle p\rangle = P_1P_2P_3$ ($e_1 = e_2 = e_3 = 1$ y $f_1 = f_2 = f_3 = 1$) con P_1, P_2 y P_3 ideales primos.

Sea $\mathfrak{f} = P_1^{k_1}P_2^{k_2}P_3^{k_3}$, con $k_1, k_2, k_3 \in \mathbb{N}$ y supongamos que $k_1 \leq k_2 \leq k_3$.

Ahora veamos qué condiciones deben cumplir k_1, k_2 y k_3 para que $\mathfrak{f}$ sea conductor.

- Condiciones para k_1:
  Como $f_1 = 1$ y $e_1 = 1$, tenemos $k_1 \equiv 1 \pmod{e_1}$ siempre sucede. Por el teorema 3.12, necesitamos algún $j \in \{2, 3\}$ tal que $k_j > \dfrac{k_1 - 1}{e_1}e_j = k_1 - 1$, lo que implica $k_j \geq k_1$ es decir, necesitamos que $k_2 \geq k_1$ ó $k_3 \geq k_1$.
  Por nuestra suposición, no necesitamos restricciones para k_1.

- Condiciones para k_2:
  Como $e_2 = 1$ y $f_2 = 1$, se tiene, igual que para k_1, $k_2 \equiv 1 \pmod{e_2}$. De la misma forma, necesitamos algún $j \in \{1, 3\}$ tal que $k_j > k_2 - 1$, lo que implica $k_1 \geq k_2$ ó $k_3 \geq k_2$, por lo que tampoco necesitamos restricciones para k_2.
- Condiciones para k_3:
  Para este caso, de forma análoga a los dos anteriores, necesitamos que $k_1 \geq k_3$ ó $k_2 \geq k_3$.

Así, tenemos sólo dos posibilidades: $k_1 = k_2 = k_3$ ó $k_1 < k_2 = k_3$.

Por lo tanto, todos los posibles ideales conductores son de la forma $\mathfrak{f} = (P_1P_2P_3)^{k_1}$ para $k_1 \in \mathbb{N}$ ó $\mathfrak{f} = P_1^{k_1}(P_2P_3)^{k_2}$ para $k_1 \in \mathbb{N}_0$, $k_2 \in \mathbb{N}$ y $k_1 < k_2$.

Caso 3: p es totalmente ramificado, es decir $\langle p \rangle = P_1^3$ ($e_1 = 3$ y $f_1 = 1$) con P_1 un ideal primo.

Sea $\mathfrak{f} = P_1^{k_1}$, con $k_1 \in \mathbb{N}$, entonces por la proposición 3.8, $\mathfrak{f}$ es conductor si y sólo si $k_1 \not\equiv 1 \pmod 3$ si y sólo si $k_1 = 3d$ ó $k_1 = 3d + 2$. Por lo tanto, los posibles ideales conductores son de la forma $\mathfrak{f} = P_1^{3d}$, con $d \in \mathbb{N}$ ó $\mathfrak{f} = P_1^{3d}P_1^2$, con $d \in \mathbb{N}_0$.

Caso 4: $\langle p \rangle = P_1P_2$ ($e_1 = 1, f_2 = 1$ y $e_2 = 1, f_2 = 2$) con P_1 y P_2 ideales primos.

Sea $\mathfrak{f} = P_1^{k_1}P_2^{k_2}$, con $k_1, k_2 \in \mathbb{N}$. Ahora veamos qué condiciones deben cumplir k_1 y k_2 para que $\mathfrak{f}$ sea un conductor.

- Condiciones para k_1:
  Como $e_1 = 1$ y $f_1 = 1$, entonces $k_1 \equiv 1 \pmod{e_1}$ siempre sucede. Por el teorema 3.12, necesitamos $k_2 > \dfrac{k_1 - 1}{e_1} e_2 = k_1 - 1$, de donde $k_2 \geq k_1$.
- Condiciones para k_2:
  Dado que $f_2 = 2$, no hay restricciones para k_2.

Por tanto, $\mathfrak{f} = P_1^{k_1}P_2^{k_2} = (P_1P_2)^{k_1}P_2^{k_2-k_1}$. En este caso $\mathfrak{f}$ es conductor si y sólo si $\mathfrak{f} = (P_1P_2)^dP_2^l$, con $d, l \in \mathbb{N}_0$ y $(d, l) \neq (0, 0)$.

Caso 5: $\langle p \rangle = P_1P_2^2$ ($e_1 = 1, f_1 = 1$ y $e_2 = 2, f_2 = 1$) con P_1 y P_2 ideales primos.

Sea $\mathfrak{f} = P_1^{k_1}P_2^{k_2}$, con $k_1, k_2 \in \mathbb{N}$. De nuevo, veamos qué condiciones deben cumplir k_1 y k_2 para que $\mathfrak{f}$ sea conductor.

- Condiciones para k_1:
  Como $e_1 = 1$ y $f_1 = 1$, entonces $k_1 \equiv 1 \pmod{e_1}$ siempre sucede. Por el teorema 3.12, necesitamos $k_2 > \dfrac{k_1 - 1}{e_1} e_2 = 2k_1 - 2$, esto implica $k_2 \geq 2k_1 - 1$.
- Condiciones para k_2:
  Como $e_2 = 2$ y $f_2 = 1$, tenemos.
  Si $k_2 \equiv 1 \pmod 2$ (es decir k_2 es un número impar), entonces por el teorema 3.12, necesitamos que $k_1 > \dfrac{k_2 - 1}{e_2} e_1 = \dfrac{k_2 - 1}{2}$, lo que implica $2k_1 \geq k_2$.
  Si $k_2 \not\equiv 1 \pmod 2$ (es decir k_2 es un número par), entonces por la proposición 3.8, no hay restricciones para k_2.

Si k_2 es impar, $2k_1 - 1 \leq k_2 \leq 2k_1$, lo cual implica $2k_1 - 1 = k_2$ es decir,

$$\mathfrak{f} = P_1^{k_1}P_2^{2k_1-1} = P_1^{k_1-1}P_2^{2k_1-2}P_1P_2 = (P_1P_2^2)^{k_1-1}P_1P_2.$$

Si k_2 es par, entonces $k_2 \geq 2k_1 - 1$ y si ponemos $k_2 = 2k_1 + 2m$ para algún $m \in \mathbb{N}_0$, tenemos que

$$\mathfrak{f} = P_1^{k_1} P_2^{k_2} = P_1^{k_1} P_2^{2k_1+2m} = (P_1 P_2^2)^{k_1} P_2^{2m}.$$

Por lo tanto, los posibles ideales conductores son de la forma: $\mathfrak{f} = (P_1 P_2^2)^d P_1 P_2$, con $d \in \mathbb{N}_0$ ó $\mathfrak{f} = (P_1 P_2^2)^d P_2^{2m}$ con $d, m \in \mathbb{N}_0$ y $(d, m) \neq (0, 0)$.

Dependiendo de la descomposición del primo racional p en ideales primos de $\mathcal{O}_F$, tenemos la siguiente tabla.

Descomposición de p	Conductor
$\langle p\rangle = p\mathcal{O}_F$	$\mathfrak{f} = \langle p\rangle^d$, $d \in \mathbb{N}$
$\langle p\rangle = P_1P_2P_3$	$\mathfrak{f} = \langle p\rangle^d (P_iP_j)^l$, $d, l \in \mathbb{N}_0$, $(d, l) \neq (0, 0)$
$\langle p\rangle = P_1P_2$, $N(P_2) = p^2$	$\mathfrak{f} = \langle p\rangle^d P_2^l$, $d, l \in \mathbb{N}_0$, $(d, l) \neq (0, 0)$
$\langle p\rangle = P^3$	$\mathfrak{f} = \langle p\rangle^d P^2$, $d \in \mathbb{N}_0$ ó $\mathfrak{f} = \langle p\rangle^d$, $d \in \mathbb{N}$
$\langle p\rangle = P_1P_2^2$	$\mathfrak{f} = \langle p\rangle^d P_1P_2$, $d \in \mathbb{N}_0$ ó $\mathfrak{f} = \langle p\rangle^d P_2^{2l}$, $d, l \in \mathbb{N}_0$, $(d, l) \neq (0, 0)$

Ejemplo 3.14. *Sea $F = \mathbb{Q}(\sqrt[3]{2})$, con $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}$. Veremos si el ideal*

$I = \langle 5, 4+3\sqrt[3]{2}+\sqrt[3]{4}\rangle^5 \langle 2, \sqrt[3]{2}\rangle^3 \langle 5, 2+\sqrt[3]{2}\rangle^5 \langle 11, 5+7\sqrt[3]{2}+\sqrt[3]{4}\rangle^8 \langle 3, 1+\sqrt[3]{2}\rangle^9 \langle 7\rangle^4 \langle 11, 4+\sqrt[3]{2}\rangle^8$

es un ideal conductor.

Agrupamos los factores por bloques.

$I = \langle 3, 1+\sqrt[3]{2}\rangle^9 (\langle 5, 4+3\sqrt[3]{2}+\sqrt[3]{4}\rangle^5 \langle 5, 2+\sqrt[3]{2}\rangle^5)(\langle 11, 5+7\sqrt[3]{2}+\sqrt[3]{4}\rangle^8 \langle 11, 4+\sqrt[3]{2}\rangle^8) \langle 2, \sqrt[3]{2}\rangle^3 \langle 7\rangle^4$,

con $\langle 7\rangle$ un ideal primo, $\langle 5\rangle = \langle 5, 4 + 3\sqrt[3]{2} + \sqrt[3]{4}\rangle\langle 5, 2 + \sqrt[3]{2}\rangle$, $\langle 2\rangle = \langle 2, \sqrt[3]{2}\rangle^3$, $\langle 3\rangle = \langle 3, 1 + \sqrt[3]{2}\rangle^3$ y $\langle 11\rangle = \langle 11, 5 + 7\sqrt[3]{2} + \sqrt[3]{4}\rangle\langle 11, 4 + \sqrt[3]{2}\rangle$.[3]

Finalmente, por el teorema de Furtwängler, I es un ideal conductor.

Ya sabemos que no todos los ideales del anillo de enteros son conductores de algún orden, a continuación presentamos algunos ideales que no son conductores.

Ejemplo 3.15. *Sea $F = \mathbb{Q}(i)$, por la proposición 1.70, $\langle 2\rangle = \langle 1 + i\rangle^2$ en $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}i$ y por el teorema de Furtwängler, algunos ideales de $\mathcal{O}_F$ que no son ideales conductores son:*

(i) $I_t = \langle 1 + i\rangle^{2t+1}$ *con* $t \in \mathbb{N}$.
(ii) $J = \langle 3\rangle^2 \langle 5, 1 + 2i\rangle^2 \langle 5, 1 - 2i\rangle^3 \langle 13, 3 + 2i\rangle^3 \langle 13, 3 - 2i\rangle^2$.

También tenemos el siguiente ejemplo.

Ejemplo 3.16. *Sea $F = \mathbb{Q}(\sqrt[3]{2})$ con anillo de enteros $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}$. Como $\langle 2\rangle = \langle 2, \sqrt[3]{2}\rangle^3$, por el teorema de Furtwängler, los siguientes ideales no son conductores de ningún orden. $I_t = \langle 2, \sqrt[3]{2}\rangle^{3t+1}$ con $t \in \mathbb{N}$.*

[3] La factorización de los ideales $\langle 2\rangle, \langle 3\rangle, \langle 5\rangle, \langle 7\rangle$ y $\langle 11\rangle$ las obtuvimos con ayuda del teorema de Dedekind (ver [**2**] teorema 10.3.1 pág. 249).

Bibliografía

[1] Aguilar Zavoznik, A., Pineda Ruelas, M. *Teoría de números: campos de números y campos de funciones*. Departamento de Matemáticas UAM-I (2014).

[2] Alaca, S., Williams, K. S., *Introductory Algebraic Number Theory*. Cambridge University Press, 2004.

[3] Atiyah, M. F., Macdonald, I. G. *Introducción al álgebra conmutativa*. Universidad de Oxford, 1980.

[4] Deitmar, A. *Class numbers of orders in cubic fields*. J. of Number Theory. 95 (2002).

[5] Deitmar, A., Pavey, M. *Class numbers of orders in complex quartic fields*. Math. Ann. 338 (2007).

[6] Furtwängler, Ph. *Über die Führer von Zahlringen*. Sitzungsberichte Akademie Wien 128 (1919), 239245.

[7] Irelan, K., Rosen, M., *A clasical introduction to modern number theory*. GTM 84, Springer Verlag (1982).

[8] Ivorra Castillo, C. *Teoría de Números*. Notas electrónicas disponibles en https://www.uv.es/ivorra/Libros/Libros.htm, consultadas en septiembre de 2016.

[9] Kovács, B., Pethö A. *Number systems in integral domains, especially in orders of algebraic number fields*. Acta Sci. Math. (Szeged) 55 (1991).

[10] Lettl, G., Prabpayak, C. *Conductor ideals of orders in algebraic number fields*. Arch. Math. (Basel) 103 (2014).

[11] Mollin, R. A. *Orders in quadratic fields*. IV. Proc. Japan Acad. Ser. A Math. Sci. 71 (1995).

[12] Neukirch, J. *Algebraic Number Theory*. Springer.

[13] Philipp, A. *A precise result on the arithmetic of non-principal orders in algebraic number fields*. Algebra Appl. 11 (2012).

[14] Prabpayak, C. *Orders in pure cubic number fields*, PhD-thesis, Univ. Graz. Grazer Math. Ber. 361 (2014).

[15] Ribenboim, P. *Classical Theory of Algebraic Numbers*, Springer- Verlag, New York, 2001.

[16] Smith, D., Gröbner, A. *Bases in orders of algebraic number fields*. J. Symbolic Comput. 33 (2002).

[17] Stewart, I., Tall, D. *Algebraic Number Theory and Fermat's Last Theorem.* Chapman and Hall, London, A Halsed Press Book, John Wiley and Sons, New York (1979).

[18] Wilson, P. M. H. *On blowing up conductor ideals*. Math. Proc. Cambridge Philos. Soc. 83 (1978).

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE EXAMEN DE GRADO

No. 00154
Matrícula: 2142800095

Órdenes en Campos de Números y el Teorema de Furtwängler

En la Ciudad de México, se presentaron a las 14:00 horas del día 3 del mes de marzo del año 2017 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. ROGELIO FERNANDEZ ALONSO GONZALEZ
DRA. MARTHA RZEDOWSKI CALDERON
DR. ALEJANDRO AGUILAR ZAVOZNIK

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron para proceder al Examen de Grado cuya denominación aparece al margen, para la obtención del grado de:

MAESTRO EN CIENCIAS (MATEMÁTICAS)

DE: JULIO PEREZ HERNANDEZ

y de acuerdo con el artículo 78 fracción III del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

JULIO PEREZ HERNANDEZ
ALUMNO

REVISÓ

LIC. JULIO CESAR DE LARA ISASSI
DIRECTOR DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JOSE GILBERTO CORDOBA HERRERA

PRESIDENTE

DR. ROGELIO FERNANDEZ ALONSO GONZALEZ

VOCAL

DRA. MARTHA RZEDOWSKI CALDERON

SECRETARIO

DR. ALEJANDRO AGUILAR ZAVOZNIK