Factorización única de ideales

Pedro Henar Navarro

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director: Javier Otal Cinca
11 de septiembre de 2019

Prólogo

En el siglo XIX Kummer intentó probar el Último Teorema de Fermat utilizando los números algebraicos y creando la teoría de los números ideales con el objetivo de abordar el error que cometió al asumir que la factorización única tenía cabida en los cuerpos de números albegraicos que había introducido. Sin embargo, fue Richard Dedekind quien llevo más lejos las ideas de Kummer. Abordó el problema de la factorización única de una forma nueva y original. Generalizó la teoría de números algebraicos de Kummer e introdujo los conceptos de cuerpo y anillo. Para conseguir la factorización única, en lugar de números ideales, consideró clases de números algebraicos, a las que llama ideales, en honor a Kummer.

El objetivo de este trabajo es probar que en ciertos dominios donde no hay factorización única de elementos como producto de primos, sí existe una factorización única de sus ideales como producto de ideales primos. En particular presentaremos los llamados anillos de enteros algebraicos de los cuerpos de números con los que trabajó Dedekind en los que encontraremos situaciones en las que no podemos asegurar la factorización única. A lo largo de los primeros capítulos estudiaremos las propiedades de dichos anillos, los cuales ejercen sobre sus cuerpos de números un papel similar al que desempeña $\mathbb{Z}$ en $\mathbb{Q}$. Estos anillos de enteros algebraicos forman parte de los llamados dominios de Dedekind. La propiedad característica que tienen estos dominios es que siempre aseguran la existencia de una factorización única de sus ideales en ideales primos y que pese a estar muy cerca de ser dominios de factorización única, no tienen por qué serlo. Esto nos permite definir conceptos y propiedades de los ideales de estos dominios similares a los que tienen los elementos en un dominio de factorización única, como por ejemplo el máximo común divisor de dos ideales. Este paso del elemento al ideal será explicado en el último capítulo, donde veremos además algunas propiedades de los dominios de Dedekind. Los dominios de Dedekind tienen aplicación en distintas áreas, por ejemplo se utilizan en el estudio de la función zeta, sin embargo no profundizaremos en las aplicaciones en este trabajo.

Para ejemplificar estos conceptos, a lo largo de la memoria estudiaremos en profundidad los anillos de enteros algebraicos de los denominados cuerpos cuadráticos, llegando a una caracterización de los mismos y viendo cómo se factorizan algunos ideales en dichos anillos.

Summary

The aim of this project is to investigate domains which are not unique factorization domains, but every ideal of them can be expressed uniquely as a product of prime ideals. This project focuses on the **ring of integers** of a **number field** in particular.

In the first chapter, we introduce the basic definitions and concepts of the number fields, which are subfields K of $\mathbb{C}$ such that $[K|\mathbb{Q}]$ is finite. By the primitive element theorem we can express any number field as $K = \mathbb{Q}(\alpha)$ with $\alpha \in K$; moreover we can choose α to be algebraic.

A complex number θ is an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. Let $\alpha \in K$ and algebric number, there is an algebraic integer θ such that $\alpha = c\theta$ $(c \in \mathbb{Z})$, so we can express any field as $K = \mathbb{Q}(\theta)$ with θ and algebraic integer. We will see other properties of albegraic integers in this chapter.

Algebraics integers form a subring of the field generated by algebraic numbers, this ring is denoted by $\mathbb{B}$. The intersection of $\mathbb{B}$ and a number field generate a ring called ring of integers of a number field and it is denoted by $\mathfrak{O}$.

The end of this chapter is dedicated to the study of **quadratic fields**. A quadratic field can be written as $K = \mathbb{Q}(\sqrt{d})$ with d a free square integer. We will show which are their algebraic integer rings.

In order to find good properties of the rings of integers, we will define new useful tools in the second chapter, such as the **norm** and the **trace** of an element in an extension F/K where F and K are number fields.

Let F and K number fields, if F/K is an extension of degree n, then there are only n distinct K-homomorphisms $\sigma_i : F \to \mathbb{C}$ $1 \leq i \leq n$. When we consider an extension of a number field K over $\mathbb{Q}$ of degree n, the $\sigma_i(\alpha)$ for $i = 1, \ldots, n$ will be denoted K-conjugates of α for each $\alpha \in K$. Let $B = \{\alpha_1, \ldots, \alpha_n\}$ a basis of a number field K, we define the **discriminant** of B as

$$\Delta[B] := (det\,[\sigma_i(\alpha_j)])^2 .$$

An **integral basis** of a number field K of degree n is a $\mathbb{Z}$-basis of the ring of integers of K $(\mathfrak{O})$, and it is simple to check that an integral basis of K is a basis of K. We will prove that integral basis exist for all number fields. Notice that integral basis exist is equivalent to the statement that $(\mathfrak{O}, +)$ is a free abelian group of rank n. However, there is not a general method to find it.

In order to research the concepts, we will continue the study of quadratic fields, showing integral basis of them and the discriminants of those basis.

In Chapter 3, we will see that the rings of integers are **noetherians**, it means that every ideal of these rings is finitely generated, which implies that the factorization into irreducibles is possible in every ring of integers of a number field. However, there are rings of integers where the factorization into irreducibles is not unique, for example, in $\mathbb{Z}(\sqrt{-5})$ which is the ring of integers of $\mathbb{Q}(\sqrt{-5})$, where six can be factorizated as $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Against this background, the central question that motivates this paper is the analysis of other properties of integer rings. In order to do this, in Chapter 4, we will define the concept of **Dedekind domain**. According to the definition, a Dedekin domain R is an integral domain such that:

1) R is noetherian.

2) R is integrally closed in its field of fractions.

3) Every nonzero prime ideal is a maximal ideal.

Despite the fact that a principal ideals domain is always a Dedekind domain, the converse is in general false. Furthermore, we will prove that a Dedekind domain is a principal ideals domain if and only if it is a unique factorizaction domain. However, any ideal of a Dedekind domain can be generated by two elements, it means that a Dedekind domain is near to be a principal ideals domain. We will see that a ring of integers is always a Dedekind domain. Although a Dedekind domain could not be a unique factorization domain, every ideal in a Dedekind domain is uniquely representable as a product of prime ideals. In this paper we will prove that the ring of integers of a number field has this property in particular.

In order to give examples of the factorization of ideals in a Dedekind domain, the end of the Chapter 4 is dedicated to study the factorization of some ideals in the ring of integers of a quadratic field. At the end of this section we will use some theorems of ramification theory (without demostration) to study those examples.

Índice general

Capítulo 1

Números y enteros algebraicos

Un número complejo α lo llamaremos **algebraico** si es algebraico sobre $\mathbb{Q}$ y denotaremos $\mathbb{A}$ al conjunto de todos ellos.

Proposición 1.1. *$\mathbb{A}$ es un cuerpo y una extensión infinita de $\mathbb{Q}$.*

Demostración. Sean $x, y \in \mathbb{A}, y \neq 0$. Como $\mathbb{Q}(x)$ y $\mathbb{Q}(y)$ son extensiones finitas de $\mathbb{Q}$ e y es algebraico sobre $\mathbb{Q}(x)$ (por serlo sobre $\mathbb{Q}$), $[\mathbb{Q}(x,y) : \mathbb{Q}]$ es finita, luego sus elementos son algebraicos sobre $\mathbb{Q}$. Pero $x \pm y$, xy, $x/y \in \mathbb{Q}(x,y)$, luego todos ellos son números algebraicos y se sigue que $\mathbb{A}$ es cuerpo.
Sea x tal que $[\mathbb{Q}(x) : \mathbb{Q}]$ es finito pero arbitrario. $\mathbb{Q}(x) \subseteq \mathbb{A}$, luego $\mathbb{A}/\mathbb{Q}$ no puede ser finito. □

Además $\mathbb{A}$ resulta ser la clausura algebraica de $\mathbb{Q}$. No obstante, no es el objetivo de este trabajo profundizar en este asunto, ya que resulta más interesante estudiar extensiones finitas por sus propiedades.

Definición. Se llamará *textbf cuerpodenmeros* (algebraicos) a cualquier extensión finita K de $\mathbb{Q}$.

Ejemplos:

1) El propio $\mathbb{Q}$;

2) Sea α solución de un polinomio $f \in \mathbb{Q}[X]$ irreducible de grado 2, entonces $\mathbb{Q}(\alpha)$ es un cuerpo de números algebraicos. Estos cuerpos se llamarán cuadráticos. En este caso $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

Evidentemente cualquier cuerpo de números está contenido en $\mathbb{A}$. Por el teorema del elemento primitivo se sigue la siguiente proposición.

Proposición 1.2. *Si K es un cuerpo de números entonces $K = \mathbb{Q}(\theta)$ para algún número algebraico θ.*

Demostración: ([ST], Teorema 2.2). □

Nuestro primer objetivo es, dado un cuerpo de números algebraicos K, definir un anillo de enteros $\mathfrak{O}$ que sea "muy parecido a $\mathbb{Z}$". Por ejemplo, si $K = \mathbb{Q}(\sqrt{d})$, se podría pensar en usar $\mathfrak{O} = \mathbb{Z}[\sqrt{d}]$, sin embargo veremos que no tiene porqué ser la mejor forma de definirlo.

Definición. Un número complejo α es un **entero algebraico** si existe un polinomio mónico con coeficientes enteros del que α es raíz. Denotaremos $\mathbb{B}$ al conjunto de todos ellos.

Este concepto se puede generalizar de la siguiente forma: sea un cuerpo K, R un subanillo de K y $\alpha \in K$, se dice que α es entero sobre R si es raíz de un polinomio mónico con coeficientes en R.

Proposición 1.3. *Un número algebraico α es entero algebraico si y solo si su polinomio mínimo sobre $\mathbb{Q}$ tiene los coeficientes en $\mathbb{Z}$.*

Demostración. Sea p el polinomio mínimo de α sobre $\mathbb{Q}$. Si $p \in \mathbb{Z}[X]$ entonces α es un entero algebraico. Por el otro lado, si α es un entero algebraico $q(\alpha) = 0$ para cierto $q \in \mathbb{Z}[X]$ mónico y por tanto $p|q$. Por el lema de Gauss, $\exists \lambda \in \mathbb{Q}$ tal que $\lambda p \in \mathbb{Z}[X]$ y $\lambda p|q$ como p y q son mónicos se sigue $\lambda = 1$. □

Lema 1.4. ***(proceso de linealización de Dedekind)*** *Un número complejo es un entero algebraico si y solo si el grupo aditivo generado por las potencias* $1, \theta, \theta^2, \ldots$ *es finitamente generado.*

Si θ es entero algebraico entonces, entonces para cierto $n \in \mathbb{N}$

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0 \tag{1.1}$$

con $a_i \in \mathbb{Z}\ \forall i \in (1,\ldots,n)$. Sea Γ el grupo generado por $1, \theta, \ldots, \theta^{n-1}$. Por la ecuación anterior es evidente que $\theta^n \in \Gamma$. Usando el método de inducción se sigue que todas las potencias de θ están en Γ: sea $m \geq n$, y $\theta^j \in \Gamma\ \forall j \in (1,\ldots,m)$ entonces

$$\theta^{m+1} = \theta^{m+1-n}\theta^n = \theta^{m+1-n}\left(-a_{n-1}\theta^{n-1} - \ldots - a_0\right) = -a_{n-1}\theta^m - \ldots - \theta^{m+1-n}a_0 \in \Gamma.$$

Veamos ahora la otra implicación, sea Γ el subgrupo de G generado por las potencias $1, \theta, \theta^2, \ldots$. y suponer que es finitamente generado. Sean $v_1, .., v_n$ una familia de generadores de Γ. Notar que cada v_i es un polinomio de $\mathbb{Z}[\theta](=\Gamma)$, evidentemente $\theta v_i \in \mathbb{Z}[\theta]$ y además $\exists\ b_{ij}$ tales que

$$\theta v_i = \sum_{j=1}^{n} b_{ij} v_j.$$

De esta forma obtenemos un sistema homogéneo de n ecuaciones con n incógnitas de la forma

$$\begin{aligned}
(b_{11} - \theta)X_1 + b_{12}X_2 + \ldots + b_{1n}X_n &= 0 \\
b_{21}X_1 + (b_{22} - \theta)X_2 + \ldots + b_{2n}X_n &= 0 \\
&\vdots \\
b_{n1}X_1 + b_{n2}X_2 + \ldots + (b_{nn} - \theta)X_n &= 0
\end{aligned}$$

que tiene solución $v_1, \ldots, v_n \in \mathbb{C}$ con algún $v_i \neq 0$, luego el determinante

$$\begin{vmatrix}
b_{11} - \theta & b_{12} & \ldots & b_{1n} \\
b_{21} & b_{22} - \theta & \ldots & b_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
b_{n1} & b_{n2} & \ldots & b_{nn} - \theta
\end{vmatrix}$$

es nulo. Mediante el cálculo del determinante obtenemos un polinomio mónico con coeficientes enteros del que θ es raíz. □

Teorema 1.5. $\mathbb{B}$ *es un subanillo de* $\mathbb{A}$.

Demostración. Sean $a, b \in \mathbb{B}$. Tenemos que demostrar que $a+b$ y $ab \in \mathbb{B}$. Todas las potencias de a y b se encuentran en los grupos generados por sus respectivas potencias que denotaremos por Γ_a y Γ_b respectivamente, siendo estos finitamente generados por el Lema 1.4. Notar que todas las potencias de $a+b$ y ab son combinaciones lineales de elementos $a^i b^j$ que están en $\Gamma_a\Gamma_b \subseteq \mathbb{C}$. Pero si Γ_a tiene generadores $v_1, \ldots, v_n$ y Γ_b tiene generadores $w_1, \ldots, w_m$, entonces $\Gamma_a\Gamma_b$ es un grupo (aditivo) abeliano generado por todos los $v_i w_j$ con $i \in (1,\ldots,n)$, $j \in (1\ldots,m)$. Como las potencias de $a+b$ y ab están en $\Gamma_a\Gamma_b$ abeliano finitamente generado, se sigue que el grupo generado por las potencias de $a+b$ y el generado por las de ab son también finitamente generados (recordar que todo subgrupo de un grupo abeliano finitamente generado es finitamente generado). Luego por el Lema 1.4 se tiene que $a+b$ y $ab \in \mathbb{B}$. Por tanto $\mathbb{B}$ es un subanillo de $\mathbb{A}$. □

Teorema 1.6. *Sea* θ *un número complejo raíz de un polinomio mónico cuyos coeficientes están en* $\mathbb{B}$*, entonces* $\theta \in \mathbb{B}$.

Demostración. Suponer

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0$$

con $a_0, \ldots, a_{n-1} \in \mathbb{B}$. Estos $\{a_i\}$ generan un subanillo Υ de $\mathbb{B}$. Por un argumento análogo al usado en el Lema 1.4 se puede ver que todas las potencias de θ están en un Υ-submódulo M de $\mathbb{C}$ finitamente generado por $1, \theta, \ldots, \theta^{n-1}$. Por el Teorema 1.5 cada a_i y todas sus potencias se encuentran en un grupo aditivo abeliano finitamente generado Γ_i. Luego se sigue que M se encuentra en el grupo aditivo abeliano generado por todos los generadores de cada grupo Γ_i y las potencias $1, \theta, \ldots, \theta^{n-1}$, luego M es un grupo finitamente generado y por el Lema 1.4 se sigue el resultado. □

Definición. Sea K un cuerpo de números, llamaremos **anillo de enteros** de K a

$$\mathfrak{O} = K \cap \mathbb{B}.$$

Ejemplo: $\mathbb{Q} \cap \mathbb{B} = \mathbb{Z}$.

Demostración. Por definición de entero algebraico se sigue $\mathbb{Z} \subseteq \mathbb{Q} \cap \mathbb{B}$. Sea $\alpha \in \mathbb{Q} \cap \mathbb{B}$ su polinomio mínimo sobre $\mathbb{Q}$ es $t - \alpha$. por el Lema 1.3 se sigue que $-\alpha \in \mathbb{Z}$, luego $\alpha \in \mathbb{Z}$. □

Lema 1.7. *Si $\alpha \in K$ entonces $c\alpha \in \mathfrak{O}$ para algún $c \in \mathbb{Z}$ no nulo.*

Demostración. Sea $f(X) = a_0 + a_1 X + \ldots + X^r$ el polinomio mínimo de α sobre $\mathbb{Q}$ y sea $c \in \mathbb{Z}$ múltiplo de los denominadores que aparecen en $f(X)$, entonces α es solución de la ecuación $c^r a_0 + c^r a_1 X + \ldots + c^r X^r = 0$. Notar que $c\alpha$ es raíz del polinomio $c^r a_0 + c^{r-1} a_1 X + \ldots + c a_{n-1} X^{r-1} + X^r \in \mathbb{Z}[X]$, luego $c\alpha \in \mathfrak{O}$. □

Colorario 1.8. *Si K es un cuerpo de números entonces $K = \mathbb{Q}(\theta)$ para algún entero algebraico θ.*

Demostración. Por la Proposición 1.2, $K = \mathbb{Q}(\alpha)$ para algún número algebraico α. Por el Lema 1.7, $c\alpha \in \mathfrak{O}$ para algún $c \in \mathbb{Z}$ no nulo. Tomando $\theta = c\alpha$ es evidente que $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha)$ luego se sigue el resultado. □

1.1. Enteros cuadráticos

Un **cuerpo cuadrático** K es un cuerpo de números de grado 2 sobre $\mathbb{Q}$. Por el Colorario 1.8 $K = \mathbb{Q}(\theta)$ para algún θ entero algebraico y, por ser de grado 2, es un cero de un polinomio de la forma

$$t^2 + at + b \quad (a,b) \in \mathbb{Z}.$$

Luego se sigue que

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2} = \frac{-a \pm r\sqrt{d}}{2}$$

siendo $r, d \in \mathbb{Z}$ y d libre de cuadrados tales que $a^2 - 4b = r^2 d$. Por tanto cualquier cuerpo cuadrático K se puede expresar de la forma $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$ con $d \in \mathbb{Z}$ libre de cuadrados.

Teorema 1.9. *Sea $d \in \mathbb{Z}$ libre de cuadrados. Entonces los enteros del cuerpo de números $K = \mathbb{Q}(\sqrt{d})$ son:*

a) $\mathbb{Z}\left[\sqrt{d}\right]$ *si* $d \not\equiv 1$ *(mod 4),*

b) $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right]$ *si* $d \equiv 1$ *(mod 4).*

Demostración: Todo elemento $\alpha \in \mathbb{Q}(\sqrt{d})$ es de la forma $\alpha = r + s\sqrt{d}$ para ciertos $r,s \in \mathbb{Q}$. Luego

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

donde $a,b,c \in \mathbb{Z}$, $c > 0$ y no tienen ningún divisor primo común. Notar que α es un entero algebraico si y solo si los coeficientes del polinomio mínimo

$$(X-\alpha)\left(X-\left(\frac{a-b\sqrt{d}}{c}\right)\right)$$

son enteros, es decir, si

$$\frac{a^2-b^2d}{c^2} \in \mathbb{Z}, \tag{1.2}$$

$$\frac{2a}{c} \in \mathbb{Z}. \tag{1.3}$$

Si c y a tienen un factor primo común p entonces por (1.2) como d es libre de cuadrados $p|b$, lo que contradice que a,b,c tengan un mismo divisor primo común. Luego c y a no tienen un factor primo común luego por (1.3) $c = 1$ ó $c = 2$. Si $c = 1$ es evidente que α es entero sobre K. En el caso de que $c = 2$, a tiene que ser impar para que no tenga ningún factor primo común con c, luego por (1.2) b es impar (pues en caso contrario $c^2|a^2$ y hemos supuesto que eso no pasaba) también y además

$$a^2 - b^2d \equiv 0 \pmod 4.$$

Ahora bien, un número impar $2k+1$ tiene cuadrado $4k^2+4k+1 \equiv 1 \pmod 4$, por tanto $a^2 \equiv 1 \equiv b^2 \pmod 4$, y esto implica $d \equiv 1 \pmod 4$. Por otro lado si $d \equiv 1 \pmod 4$, entonces para a y b impares se sigue que α es entero sobre K por cumplirse (1.2) y (1.3) (es una comprobación).

Si $d \not\equiv 1 \pmod 4$, entonces a y b no son impares luego $c = 1$ y es evidente que se cumple a). Sin embargo, si $d \equiv 1 \pmod 4$, c puede valer 1, pero también 2 si a y b son impares luego veamos que se cumple b): Tomar $d \equiv 1$ y sean a y b impares, en caso de que $c = 2$ tenemos que

$$\frac{a+b\sqrt{d}}{2} = \frac{a-b+b+b\sqrt{d}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$$

si $c = 1$ es evidente que $a+b\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right] \subseteq \mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$. Por otro lado es fácil de comprobar que cualquier elemento $r+s(\frac{1+\sqrt{d}}{2}) \in \mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$ se encuentra en uno de los dos casos anteriores en función de la paridad de s. □

Capítulo 2

Dependencia entera y herramientas

Sea una extensión finita F/K de cuerpos intermedios entre $\mathbb{Q}$ y $\mathbb{C}$, $\mathbb{Q} \leq K \leq F \leq \mathbb{C}$ tal que $[F/K] = n$, se buscarán funciones que a cada elemento de F se le asigne un elemento de K. Consideraremos la base $B = \{b_1, \ldots, b_n\}$ de F sobre K.

Sea $\alpha \in F$ no nulo. Consideremos la homotecia $\phi_\alpha : F \to F$ dada por $\phi_\alpha(a) = \alpha a \ \forall a \in F$. De forma que $\alpha b_i = \sum_{j=1}^{n} a_{ij} b_j \ \forall i \in (1, \ldots, n)$. Entonces la matriz de ϕ_α respecto de la base B es $M = (a_{ij})$. Si $B' = \{b'_1, \ldots, b'_n\}$ es otra base, llamamos C a la matriz de cambio de base de B' a B entonces la matriz de ϕ_α respecto de la base B' es $C^{-1}MC$.

Como F es cuerpo ϕ es biyectiva, por tanto M y $C^{-1}MC$ son invertibles. Luego su determinante y su traza dependen únicamente de sus valores propios, como son los mismos en ambas matrices tenemos que su determinante y su traza no dependen de la base escogida.

Definición. Sea $\alpha \in F$, la **norma** de α se define como $N_{F/K}(\alpha) := det(M)$ y la **traza** de α se define como $t_{F/K}(\alpha) := tr(M)$. Si no hay confusión lo denotaremos como $N(\alpha)$ y $t(\alpha)$ respectivamente.

Proposición 2.1. *Sean F y K cuerpos de números tales que F/K es una extensión finita de grado n, entonces $\forall \alpha, \beta \in F$ y $\forall a \in K$ se cumple:*

1) $N(\alpha\beta) = N(\alpha)N(\beta), \quad t(\alpha+\beta) = t(\alpha)+t(\beta).$

2) $N(\alpha\beta) = a^n N(\alpha)$ *y* $t(a\alpha) = at(\alpha).$

Demostración: ([IR] Capítulo 2, Sección 2). □

Teorema 2.2. *Sean F y K cuerpos de números. Si F/K es una extensión de grado n entre $\mathbb{Q}$ y $\mathbb{C}$, sólo hay n K-homomorfismos $\sigma_i : F \to \mathbb{C}$ $1 \leq i \leq n$.*

Demostración: F/K es una extensión de grado n, luego $\exists \theta \in F$ tal que $F = K(\theta)$ (esto es una extensión de la Proposición 1.2 y es consecuencia del Teorema del elemento primitivo). Sea $f(X)$ el polinomio mínimo de θ sobre K. $[F/K] = n$ luego $f(X)$ tiene exactamente n raíces distintas $\theta_1, \ldots, \theta_n$ que definen cada una un K-homomorfismo σ_i tal que $\sigma_i(\theta) = \theta_i \ \forall i \in (1, \ldots, n)$. Notar que si σ es K-homomorfismo, entonces necesariamente $f(\sigma(\theta)) = \sigma(f(\theta)) = 0$, luego hay exactamente n K-homomorfismos. □

Sea $\alpha \in F$ bajo las condiciones del teorema anterior, los $\sigma_i(\alpha)$ para $i = 1, \ldots, n$ los definiremos como (F/K)-conjugados de α. Cuando consideremos una extensión del tipo $K/\mathbb{Q}$ los llamaremos K-conjugados de α.

Teorema 2.3. *En las condiciones del Teorema 2.2, si $a \in F$ se tiene:*
$t(a) = \sum_{i=1}^{n} \sigma_i(a)$, $N(a) = \prod_{i=1}^{n} \sigma_i(a)$.

Demostración. ([DL], IV Lema 2.5) en este caso pide extensiones separables pero no hay problema por tratarse de cuerpos de números (cuerpos característica 0). □

Colorario 2.4. *Sea K un cuerpo de números y considerando la extensión $K/\mathbb{Q}$, entonces $N(\alpha), t(\alpha) \in \mathbb{Z}$ $\forall \alpha \in \mathfrak{O}$.*

Demostración. Sean $\alpha_1, \ldots, \alpha_n$ los conjugados de α en esta extensión, entonces son las raíces del polinomio mínimo $f(X)$ de α sobre $\mathbb{Q}$. Luego $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$. Sea $f(X) = X^n + \ldots + a_1 X + a_0$, notar que $a_0 = (-1)^n \prod_{i=1}^{n} \alpha_i = (-1)^n N(\alpha)$ y $a_{n-1} = \sum_{i=1}^{n}(-\alpha_i) = -t(\alpha)$
Por la Proposición 1.3 se sigue que $N(\alpha), t(\alpha) \in \mathbb{Z}$. □

Proposición 2.5. *Sea $\mathfrak{O}$ el anillo de enteros de un cuerpo de número K, y sean $x, y \in \mathfrak{O}$ entonces:*

a) x es unidad si y solo si $N(x) = \pm 1$.

b) Si x e y son asociados entonces $N(x) = \pm N(y)$.

c) Si $N(x)$ es primo (en $\mathbb{Z}$), entonces x es irreducible en $\mathfrak{O}$.

Demostración. ([ST] Proposición 4.10). □

Sea K un cuerpo de números de grado n (sobre $\mathbb{Q}$). Llamaremos base de K a una base de K como espacio vectorial sobre $\mathbb{Q}$ (una $\mathbb{Q}$-base de K).

Definición. Sean F y K cuerpos de números tales que F/K es una extensión finita, sean $\alpha_1, \ldots, \alpha_n \in F$. Llamaremos **discriminante** de $\alpha_1, \ldots, \alpha_n$ a:

$$\Delta[\alpha_1, \ldots, \alpha_n] := (det[\sigma_i(\alpha_j)])^2. \tag{2.1}$$

Definición. Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números de grado n sobre $\mathbb{Q}$ y $B = \{\alpha_1, \ldots, \alpha_n\}$ una base de K. Denotaremos al discriminante de esta base como:

$$\Delta[B] := (det[\sigma_i(\alpha_j)])^2. \tag{2.2}$$

Proposición 2.6. *Sea K un cuerpo de números. Suponer que $B = \{\alpha_1, \ldots, \alpha_n\}$ y $B' = \{\beta_1, \ldots, \beta_n\}$ son bases de K con $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$, $a_{ij} \in K$ $\forall\, i \in (1, \ldots, n)$. Entonces $\Delta[B] = (det(a_{ij}))^2 \Delta[B']$.*

Demostración: Es una simple comprobación usando la fórmula del producto de determinantes. □

En la demostración del siguiente teorema usaremos un resultado muy útil de los polinomios simétricos que veremos a continuación. Recordemos que un polinomio simétrico $f(X_1, \ldots, X_n)$ es aquel tal que $\tau(f) = f$ $\forall \tau \in S_n$ (grupo simétrico de permutaciones de n elementos).

Lema 2.7. *Sea K una extensión de un cuerpo L, $f \in L[X]$ de grado n y cuyos ceros $\theta_1, \ldots, \theta_n$ están en K. Si $g(X_1, \ldots, X_n) \in L[X_1, \ldots, X_n]$ es simétrico, entonces $g(\theta_1, \ldots, \theta_n) \in L$.*

Demostración: ([ST] Colorario 1.14). □

Teorema 2.8. *El discriminante de cualquier base de un cuerpo de números $K = \mathbb{Q}(\theta)$ es un número racional y no nulo. Si todos los K-conjugados de θ son reales entonces el discriminante de cualquier base es positivo.*

Demostración: Consideremos la base $B = \{1, \theta, \ldots, \theta^{n-1}\}$ y sean $\theta_1, \ldots, \theta_n$ a los K-conjugados de θ. Por definición

$$\Delta[B] = \left(det\,\theta_i^j\right)^2.$$

Notar que se trata de un determinante de una matriz de Vandermonde luego

$$\Delta[B] = \left(\prod_{1 \le i < j \le n} (\theta_i - \theta_j)\right)^2.$$

Consideremos $p(X_1,\ldots,X_n)=\prod_{1\leq i<j\leq n}(X_i-X_j)\in\mathbb{Q}[X_1,\ldots,X_n]$. Notar que $p^2(X_1,\ldots,X_n)$ es simétrico, luego por el lema anterior $\Delta[B]=p^2(\theta_1,\ldots,\theta_n)\in\mathbb{Q}$. Como los θ_i son distintos, $\Delta[B]\neq 0$.

Consideremos otra base B'. Entonces por la Proposición 2.6

$$\Delta[B']=(detc_{ik})^2\Delta[B]$$

para ciertos $c_{ik}\in\mathbb{Q}$ con $detc_{ik}\neq 0$, luego $\Delta[B']\in\mathbb{Q}\setminus 0$. Evidentemente si $\theta_i\in\mathbb{R}\ \forall 1\leq i\leq n$, $\Delta[B]$ es un número racional positivo y se sigue que $\Delta[B']$ también lo es. □

Dado un cuerpo de números $K=\mathbb{Q}(\theta)$ de grado n podemos encontrar fácilmente una base. Por ejemplo, podemos considerar $\left\{1,\theta,\ldots,\theta^{n-1}\right\}$, que de hecho es una base de K formada por enteros algebraicos. Dado que el anillo de enteros algebraicos de K (lo denotamos como $\mathfrak{O}$) es un grupo abeliano bajo la suma, llamaremos **base entera** de K (o de $\mathfrak{O}$) a una $\mathbb{Z}$-base de ($\mathfrak{O}$,+). Por el Lema 1.7 se sigue que una base entera de K es una base de K. Notar que $\left\{1,\theta,\ldots,\theta^{n-1}\right\}$ es una base formada por elementos de $\mathfrak{O}$ y no por ello tiene que ser una base entera, pues pueden existir enteros algebraicos que no pertenezcan a $\mathbb{Z}[\theta]$. Por ejemplo en $K=\mathbb{Q}[\sqrt{5}]$, el elemento $\frac{1}{2}+\frac{1}{2}\sqrt{5}$ es raíz del polinomio X^2-X-1 luego es entero algebraico, pero no pertenece a $\mathbb{Z}[\sqrt{5}]$. Veamos algún ejemplo de base entera y calculemos su discriminante.

Proposición 2.9. *Sea $d\in\mathbb{Q}$ libre de cuadrados, entonces*

a) Si $d\not\equiv 1$ (mod 4) entonces $\mathbb{Q}(\sqrt{d})$ tiene una base entera de la forma $\left\{1,\sqrt{d}\right\}$ y cuyo discriminante es $4d$.

b) Si $d\equiv 1$ (mod 4) entonces $\mathbb{Q}(\sqrt{d})$ tiene una base entera de la forma $\left\{1,\frac{1}{2}+\frac{1}{2}\sqrt{d}\right\}$ y cuyo discriminante es d.

Demostración: Las bases se obtienen del Teorema 1.9 y es evidente que son bases enteras. Los discriminantes los obtenemos mediante el cálculo directo:

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2=(-2\sqrt{d})^2=4d,$$

$$\begin{vmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{d} \end{vmatrix}^2=(-\sqrt{d})^2=d.$$

□

Ahora bien, ¿podemos asegurar que para todo cuerpo de números K existe una base entera? Esto equivale a probar que $(\mathfrak{O},+)$ es un grupo libre abeliano de rango $n<\infty$, veámoslo a continuación demostrando previamente un lema que usaremos.

Lema 2.10. *Sea $B=\{\theta_1,\ldots,\theta_n\}$ una base de K cuerpo de números tal que $\theta_i\in\mathfrak{O}\ \forall i\in(1,\ldots,n)$, entonces $\Delta[B]\in\mathbb{Z}\setminus\{0\}$.*

Demostración: Por el Teorema 2.8 $\Delta[B]\in\mathbb{Q}\setminus\{0\}$. Como $\theta_i\in\mathfrak{O}\ \forall i\in(1,\ldots,n)$, se sigue que $\Delta[B]\in\mathfrak{O}$. Luego $\Delta[B]\in\mathfrak{O}\cap(\mathbb{Q}\setminus\{0\})=\mathbb{Z}\setminus\{0\}$. □

Teorema 2.11. *Todo cuerpo de números $K=\mathbb{Q}(\theta)$ tiene una base entera, y el grupo ($\mathfrak{O}$,+) es libre abeliano de rango n igual al grado de K.*

Demostración: Sabemos que siempre existe una base de K formada por elementos de $\mathfrak{O}$, coger por ejemplo $\left\{1,\theta,\ldots,\theta^{n-1}\right\}$ pero esta puede no ser base entera. Por el Lema 2.10 el discriminante de una base de K formada por enteros algebraicos es un número entero no nulo. Consideremos la base $B=\{\omega_1,\ldots,\omega_n\}$ formada por enteros algebraicos cuyo discriminante es el menor posible en valor absoluto. Suponer que esta base no es un base entera y lleguemos a contradicción. Si no es base entera entonces $\exists\omega\in\mathfrak{O}$ tal que

$$\omega=a_1\omega_1+\ldots+a_n\omega_n.$$

Con $a_i \in \mathbb{Q}\ \forall i$ pero no todos los a_i en $\mathbb{Z}$. Suponer sin pérdida de generalidad $a_1 \notin \mathbb{Z}$. Entonces $a_1 = a + r$ con $a \in \mathbb{Z}$ y $0 < r < 1$. Definimos

$$\mu_1 := \omega - a\omega_1, \qquad \mu_i := \omega_i \quad (i = 2, \ldots, n).$$

Entonces $B' = \{\mu_1, \ldots, \mu_n\}$ es una base formada por enteros algebraicos. El determinante de la matriz de cambio de bases de B a B' es

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = r,$$

luego

$$\Delta[B] = r^2 \Delta[B'].$$

Como $0 < r < 1$, se contradice con la condición de minimalidad de $|\Delta[B]|$. Por tanto, B es una base entera, luego $(\mathfrak{O}, +)$ es libre abeliano de rango n. □

Pese a que hemos demostrado que para todo cuerpo de números existe una base entera, esto no quiere decir que siempre seamos capaces de encontrarla, de hecho el cálculo de una base entera puede complicarse mucho convirtiéndose en un reto para el Álgebra Computacional. No obstante en las condiciones apropiadas uno puede hallarla de forma sencilla como vimos en el caso concreto de los cuerpos cuadráticos.

Proposición 2.12. *Sea B una base de K cuerpo de números formada por elementos de $\mathfrak{O}$. Si $\Delta[B]$ es libre de cuadrados entonces B es base entera.*

Demostración: ([ST] Teorema 2.17). □

El discriminante de una base resulta ser una herramienta muy útil tanto para el cálculo de bases enteras como para estudiar otras propiedades de los anillos de enteros. Veamos pues otras formas de hallarlos.

Proposición 2.13. *Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números donde el polinomio mínimo de θ p tiene grado n. Entonces la base $B = \left\{1, \theta, \ldots, \theta^{n-1}\right\}$ tiene discriminante*

$$\Delta[B] = (-1)^{n(n-1)/2} N(p'(\theta))$$

Demostración: Sabemos por lo visto en la demostración del Teorema 2.8:

$$\Delta[B] = \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2,$$

siendo $\theta_1, \ldots, \theta_n$ los conjugados de θ, luego

$$p(X) = \prod_{i=1}^{n} (X - \theta_i), \qquad p'(X) = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \neq j}}^{n} (X - \theta_i), \qquad p'(\theta_j) = \prod_{\substack{i=1 \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

Multiplicando estas últimas ecuaciones para cada $j = 1, \ldots, n$ obtenemos la norma de $p'(\theta)$

$$N(p'(\theta)) = \prod_{j=1}^{n} p'(\theta_j) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (\theta_j - \theta_i).$$

Notar que en el segundo término cada factor $(\theta_i - \theta_j)$ para $i < j$ aparece dos veces, una como $(\theta_i - \theta_j)$ y otra como $(\theta_j - \theta_i)$, siendo el producto de ambos $-(\theta_i - \theta_j)^2$. Luego operando se sigue

$$N(p'(\theta)) = \Delta[B](-1)^{n(n-1)/2},$$

obteniéndose así el resultado. □

Este resultado se puede extender a extensiones de cuerpos de números F/K ([JO] Lema 3.5).

Proposición 2.14. *Sea $B = \{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Q}$-base de K cuerpo de números, entonces*

$$\Delta[B] = det(t(\alpha_i \alpha_j)).$$

Demostración: ([ST] Proposición 2.19). □

Capítulo 3

Factorización en irreducibles

La mayoría de las ventajas de trabajar en $\mathbb{Z}$ provienen de que es un dominio euclídeo. Los anillos de enteros de un cuerpo de números no tienen necesariamente esta propiedad. Por ejemplo, el anillo de enteros de $\mathbb{Q}(\sqrt{-5})$ es $\mathbb{Z}[\sqrt{-5}]$ que no es dominio de factorización única en irreducibles (DFU), ya que por ejemplo podemos factorizar el 6 de la siguiente forma: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ siendo $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ irreducibles y $\{2,3\}$ no asociados con $\{1+\sqrt{-5}, 1-\sqrt{-5}\}$. Veámoslo a continuación.

Notar que $\forall\ a+b\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$, su norma es $N(a+b\sqrt{-5}) = a^2+5b^2$. Si $2 = xy$ con $x, y \in \mathbb{Z}[\sqrt{-5}]$ no unidades, tomando la norma $4 = N(2) = N(x)N(y)$ como x e y son enteros algebraicos, por el Colorario 2.4 sus normas son números enteros. Por tanto, como x e y no son unidades,se sigue de la Proposición 2.5, $N(x) = N(y) = \pm 2$. De forma análoga los divisores no triviales de 3 tienen, si existen, norma ± 3, mientras que los de $1 \pm \sqrt{-5}$ tienen norma ± 2 ó ± 3. Como $N(a+b\sqrt{-5}) = a^2+5b^2$ $\forall a, b \in \mathbb{Z}$, si $|b| \geq 1$ tenemos que $|a^2+5b^2| \geq 5$, en cambio si $|b| = 0$ como $a \in \mathbb{Z}$ es imposible que $a^2 = \pm 2$ ó ± 3. Luego esos elementos son irreducibles. Nuevamente por la Proposición 2.5 dos elementos asociados tienen las misma norma salvo el signo, luego como $N(1 \pm \sqrt{-5}) = 6$, $N(2) = 4$, y $N(3) = 9$ se sigue que son factorizaciones en irreducibles distintas.

Definición. Diremos que un dominio D es **noetheriano** si todo ideal de D es finitamente generado.

Como ya vimos durante el grado, esta definición se puede caracterizar de las siguientes maneras.

Proposición 3.1. *Las siguientes condiciones son equivalentes para un dominio de integridad D*

a) D es noetheriano.

b) Dada una cadena ascendente de ideales de D:

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

entonces $\exists N$ tal que $I_n = I_N$ $\forall n > N$.

c) En todo conjunto no vacío de ideales de D existe algún ideal de dicho conjunto que no está contenido en ningún otro ideal del conjunto.

Demostración: ([ST] Proposición 4.6). □

Teorema 3.2. *Si un dominio D es noetheriano, la factorización en irreducibles es posible en D.*

Demostración: Sea D noetheriano, suponer que existe $x \neq 0$ no unidad en D que no puede ser expresado como un producto finito de irreducibles. Elijamos x tal que $\langle x \rangle$ sea el conjunto maximal bajo las condiciones impuestas al x, esto es posible por ser D noetheriano y usar la Proposición 3.1 c). Por definición, x es reducible, luego $x = yz$ con y, z, no unidades. Entonces $\langle y \rangle \supseteq \langle x \rangle$ y como z no es unidad entonces el contenido es estricto. Análogamente con z tendríamos $\langle z \rangle \supset \langle x \rangle$. Por maximalidad de $\langle x \rangle$:

$$y = p_1 \cdots p_r, \qquad z = q_1 \cdots q_s,$$

con cada p_i y p_j irreducible. Comos $x = yz$ llegamos a que x es producto finito de irreducibles llegando a contradicción. Luego si D es noetheriano la factorización en irreducibles es siempre posible. □

Teorema 3.3. *El anillo de los enteros $\mathfrak{O}$ de un cuerpo de números K es noetheriano.*

Demostración: Sea **a** ideal de $\mathfrak{O}$ Por el Teorema 2.11 $(\mathfrak{O},+)$ es un grupo abeliano libre de rango n (grado de extensión en K), como todo subgrupo de un grupo libre abeliano de rango n es libre de rango $s \leq n$ se sigue que $(a,+)$ es libre abeliano de rango $s \leq n$. Si $\{a_1,\ldots,a_n\}$ es una $\mathbb{Z}$-base de $(\mathbf{a},+)$, entonces es claro que $\langle a_1,\ldots,a_n\rangle = \mathbf{a}$, luego **a** es finitamente generado y por tanto $\mathfrak{O}$ es noetheriano.□

Luego la factorización en irreducibles es posible en $\mathfrak{O}$ pero como ya vimos en el caso de $\mathbb{Q}(\sqrt{-5})$ esta no tiene porque ser única. En el grado vimos el siguiente resultado que caracteriza la condición de ser DFU bajo la hipótesis de que la factorización en irreducibles es posible.

Teorema 3.4. *En un dominio en el que la factorización en irreducibles es posible, la factorización es única si y solo si todo irreducible es primo.*

Capítulo 4

Dominios de Dedekind

Definición. Sea D un dominio de integridad, se dice que D es **Dominio de Dedekind (DD)** si se cumple:

1) D es noetheriano;

2) D es íntegramente cerrado sobre su cuerpo de fracciones K, es decir, los elementos de K enteros sobre D, son los de D;

3) Todo ideal primo no nulo de D es maximal.

Teorema 4.1. *El anillo de los enteros $\mathfrak{O}$ de un cuerpo de números K es un Dominio de Dedekind.*

Demostración: Evidentemente $\mathfrak{O}$ se trata de un dominio sobre su cuerpo de fracciones K. Por el Teorema 3.3 es noetheriano.
El segundo punto de la definición de Dominio de Dedekind equivale a probar que si $\alpha \in K$ es raíz de un polinomio mónico con coeficientes en $\mathfrak{O}$, entonces $\alpha \in \mathfrak{O}$, lo cual se sigue del Teorema 1.6. Veamos que también cumple el último punto. Sea $\mathbf{p}$ un ideal primo de $\mathfrak{O}$ y $0 \neq \alpha \in \mathbf{p}$, entonces

$$N = N(\alpha) = \alpha_1 \cdots \alpha_n \in \mathbf{p}$$

(siendo α_i los conjugados de α y $\alpha_1 = \alpha$). $\langle N \rangle \subseteq p$, luego $\mathfrak{O}/\mathbf{p}$ es un anillo cociente de $\mathfrak{O}/N\mathfrak{O}$, que es un grupo abeliano finitamente generado y de torsión, luego es finito. $\mathfrak{O}/\mathbf{p}$ es finito y un dominio (pues $\mathbf{p}$ es un ideal primo), luego es un cuerpo y por tanto $\mathbf{p}$ es maximal. □

Veamos ahora como sería la aritmética (por así decirlo) de los ideales no nulos de $\mathfrak{O}$ especialmente con la multiplicación de ideales. Tenemos conmutatividad y asociatividad pero no tenemos elementos inversos necesariamente, luego descartamos una posible estructura de grupo. Notar que todo ideal de $\mathfrak{O}$ es un $\mathfrak{O}$-submódulo de $\mathfrak{O}$.
Todo $\mathfrak{O}$-submódulo $\mathbf{a}$ de K tal que existe $c \in \mathfrak{O}$ que cumple $c\mathbf{a} \subseteq \mathfrak{O}$ se llama ideal fraccionario de $\mathfrak{O}$. Notar que todo ideal es un ideal fraccionario y un ideal fracionario es ideal si y solo si está en $\mathfrak{O}$. El producto de ideales fraccionarios es fracionario, y la multiplicación de ideales fracionarios es asociativa y conmutativa siendo $\mathfrak{O}$ la identidad (es un semigrupo conmutativo).

Teorema 4.2. *Los ideales fraccionarios no nulos de $\mathfrak{O}$ forman un grupo abeliano bajo la multiplicación.*

este teorema lo probaremos junto al siguiente.

Teorema 4.3. *Todo ideal no nulo de $\mathfrak{O}$ puede ser escrito como un producto de ideales primos de forma única salvo el orden de los factores.*

Demostración: Dividiremos la demostración de estos teoremas en 9 pasos más sencillos:

1) Sea $\mathbf{a} \neq 0$ un ideal de $\mathfrak{O}$. entonces existen ideales primos $\mathbf{p}_1, \ldots, \mathbf{p}_r$ tales que $\mathbf{p}_1 \cdots \mathbf{p}_r \subseteq \mathbf{a}$.

2) Definición de lo que resultará ser el inverso de un ideal.

3) Si $\mathbf{a}$ es un ideal propio, entonces $\mathbf{a}^{-1} \supset \mathfrak{O}$.

4) Si $\mathbf{a}$ es un ideal no nulo y $\mathbf{a}S \subseteq \mathbf{a}$ para todo subconjunto $S \subseteq K$, entonces $S \subseteq \mathfrak{O}$.

5) Si $\mathbf{p}$ es un ideal maximal, entonces $\mathbf{p}\mathbf{p}^{-1} = \mathfrak{O}$.

6) Para todo ideal $\mathbf{a} \neq 0$, $\mathbf{a}\mathbf{a}^{-1} = \mathfrak{O}$.

7) Todo ideal fraccionario $\mathbf{a}$ tiene un inverso $\mathbf{d}$ tal que $\mathbf{a}\mathbf{d} = \mathfrak{O}$ (esto prueba 4.2).

8) Todo ideal no nulo $\mathbf{a}$ es un producto de ideales primos.

9) La factorización en ideales primos es única.

Demostraciones (1)-(9)

1) : Suponer que no es cierto. Por el Teorema 3.3, $\mathfrak{O}$ es noetheriano, luego por la Proposición 3.1 podemos elegir un ideal $\mathbf{a}$ contenido en el conjunto de ideales tales que no contienen productos de ideales primos, de forma que $\mathbf{a}$ no está contenido en ningún otro ideal de dicho conjunto. Evidentemente $\mathbf{a}$ no es primo, luego existen ideales $\mathbf{b}$, $\mathbf{c}$ de $\mathfrak{O}$ tales que $\mathbf{b}\mathbf{c} \subseteq \mathbf{a}$, $\mathbf{b} \nsubseteq \mathbf{a}$, $\mathbf{c} \nsubseteq \mathbf{a}$. Sean

$$\mathbf{a}_1 = \mathbf{a} + \mathbf{b},\ \mathbf{a}_2 = \mathbf{a} + \mathbf{c}.$$

Entonces $\mathbf{a}_1\mathbf{a}_2 \subseteq \mathbf{a},\ \mathbf{a}_1 \supset \mathbf{a},\ \mathbf{a}_2 \supset \mathbf{a}$. Por la maximalidad de $\mathbf{a}$ existen ideales primos $\mathbf{p}_1, \ldots, \mathbf{p}_s, \mathbf{p}_{s+1}, \ldots, \mathbf{p}_r$ tales que:

$$\mathbf{p}_1 \cdots \mathbf{p}_s \subseteq \mathbf{a}_1,\ \mathbf{p}_{s+1} \cdots \mathbf{p}_r \subseteq \mathbf{a}_2,$$

pero por lo anterior

$$\mathbf{p}_1 \cdots \mathbf{p}_r \subseteq \mathbf{a}_1\mathbf{a}_2 \subseteq \mathbf{a},$$

llegando a contradicción, luego se cumple 1).

2) : Para cada ideal $\mathbf{a}$ de $\mathfrak{O}$ definimos

$$\mathbf{a}^{-1} = \{x \in K | x\mathbf{a} \subseteq \mathfrak{O}\}$$

Está claro que $\mathbf{a}^{-1}$ es un $\mathfrak{O}$-submódulo de K. Si $\mathbf{a} \neq 0$ entonces $\forall c \in \mathbf{a}$ no nulo, se cumple $c\mathbf{a}^{-1} \in \mathfrak{O}$, asi que $\mathbf{a}^{-1}$ es un ideal fraccionario. Claramente $\mathfrak{O} \subseteq \mathbf{a}^{-1}$ así que $\mathbf{a} = \mathbf{a}\mathfrak{O} \subseteq \mathbf{a}\mathbf{a}^{-1}$. Luego el ideal fraccionario $\mathbf{a}\mathbf{a}^{-1}$ es un ideal de $\mathfrak{O}$.

3) : Notar que para $\mathbf{b},\ \mathbf{c}$ ideales cualesquiera tales que $\mathbf{b} \subseteq \mathbf{c}$ se cumple $\mathfrak{O} \subseteq \mathbf{c}^{-1} \subseteq \mathbf{b}^{-1}$. Como $\mathbf{a} \subseteq \mathbf{p}$ para algún ideal $\mathbf{p}$ maximal, es suficiente probar que $\mathfrak{O} \neq \mathbf{p}^{-1}$. Sea $d \in \mathbf{p}$, $d \neq 0$. Por 1) podemos elegir el r más pequeño tal que:

$$\mathbf{p}_1 \cdots \mathbf{p}_r \subseteq \langle d \rangle$$

Siendo $\mathbf{p}_1, \ldots, \mathbf{p}_r$ primos. Como $\mathbf{p}$ es primo por ser maximal y $\langle d \rangle \subseteq \mathbf{p}$, algún $\mathbf{p}_i \subseteq \mathbf{p}$. Suponemos sin pérdida de generalidad que $\mathbf{p}_1 \subseteq \mathbf{p}$. Como son ideales de $\mathfrak{O}$ que es un DD, los ideales primos son maximales y por tanto $\mathbf{p}_1 = \mathbf{p}$. Además por la minimalidad de r se sigue

$$\mathbf{p}_2 \cdots \mathbf{p}_r \nsubseteq \langle d \rangle$$

Sea $b \in \mathbf{p}_2 \cdots \mathbf{p}_r \setminus \langle d \rangle$, entonces $b\mathbf{p} \subseteq \langle d \rangle$ luego $bd^{-1}\mathbf{p} \subseteq \mathfrak{O}$ y $bd^{-1} \in \mathbf{p}^{-1}$. Como $b \notin d\mathfrak{O}$ se sigue $\mathbf{p}^{-1} \neq \mathfrak{O}$.

4) : Veamos que si $\mathbf{a}\theta \subseteq \mathbf{a}$ con $\theta \in S$, entonces $\theta \in \mathfrak{O}$. $\mathfrak{O}$ noetheriano luego $\mathbf{a} = \langle a_1, \ldots, a_m \rangle$ con algún a_i no nulo. Entonces $\mathbf{a}\theta \subseteq \mathbf{a}$ implica que

$$a_1\theta = b_{11}a_1 + \ldots + b_{1m}a_m,$$
$$\vdots$$
$$a_m\theta = b_{m1}a_1 + \ldots + b_{mm}a_m,$$

para ciertos $b_{ij} \in \mathfrak{O}$, luego las ecuaciones

$$(b_{11}-\theta)X_1+\ldots+b_{1m}X_m=0$$
$$\vdots$$
$$b_{m1}X_1+\ldots+(b_{mm}-\theta)X_m=0$$

tienen solución no nula $X_1=a_1,\ldots,X_m=a_m$, así que, como en la demostración del Lema 1.4 se sigue que el determinante es nulo y tenemos un polinomio mónico con coeficientes en $\mathfrak{O}$ del que θ es raíz, luego por el Teorema 1.6, $\theta \in \mathfrak{O}$.

5) : Por la definición del inverso de un ideal, $\mathbf{pp}^{-1}$ es un ideal tal que $\mathbf{p} \subseteq \mathbf{pp}^{-1} \subseteq \mathfrak{O}$ Si $\mathbf{p}$ es maximal, $\mathbf{pp}^{-1}$ es igual a $\mathbf{p}$ o a $\mathfrak{O}$. Si $\mathbf{pp}^{-1}=\mathbf{p}$, entonces por 4) $\mathbf{p}^{-1} \subseteq \mathfrak{O}$ lo cual contradice 3). Por tanto $\mathbf{pp}^{-1}=\mathfrak{O}$.

6) : Suponer que es falso. Por el Teorema 3.3, $\mathfrak{O}$ es noetheriano, luego por la Proposición 3.1 podemos elegir un ideal $\mathbf{a}$ contenido en el conjunto de ideales tales que $\mathbf{bb}^{-1} \neq \mathfrak{O}$ $\forall \mathbf{b}$ ideal del conjunto, de forma que $\mathbf{a}$ no está contenido en ningún otro ideal de dicho conjunto. Entonces $\mathbf{a} \subseteq \mathbf{p}$ donde $\mathbf{p}$ es maximal. Luego $\mathfrak{O} \subseteq \mathbf{p}^{-1} \subseteq \mathbf{a}^{-1}$, tal que por la definición de ideal inverso $\mathbf{a} \subseteq \mathbf{ap}^{-1} \subseteq \mathbf{aa}^{-1} \subseteq \mathfrak{O}$.

En particular $\mathbf{ap}^{-1}$ es un ideal. Notar que $\mathbf{ap}^{-1} \neq \mathbf{a}$ pues en caso contrario por 4) $\mathbf{p}^{-1} \subseteq \mathfrak{O}$ y contradice 3). Luego $\mathbf{a} \subset \mathbf{ap}^{-1}$ y por la maximalidad de $\mathbf{a}$ (en el conjunto definido antes)

$$\mathbf{ap}^{-1}\left(\mathbf{ap}^{-1}\right)^{-1}=\mathfrak{O}.$$

Por la definición del inverso de un ideal $\mathbf{p}^{-1}\left(\mathbf{ap}^{-1}\right)^{-1} \subseteq \mathbf{a}^{-1}$. Luego

$$\mathfrak{O}=\mathbf{ap}^{-1}\left(\mathbf{ap}^{-1}\right)^{-1} \subseteq \mathbf{aa}^{-1} \subseteq \mathfrak{O}$$

llegando a contradicción, luego se sigue el resultado.

7) : Sea $\mathfrak{F}$ el conjunto de ideales fraccionarios de $\mathfrak{O}$ y dado $\mathbf{a} \in \mathfrak{F}$, como $\mathfrak{F}$ es un semigrupo conmutativo, basta con encontrar un $\mathbf{a'} \in \mathfrak{F}$ tal que $\mathbf{aa'}=\mathfrak{O}$. Por ser $\mathbf{a} \in \mathfrak{F}, \exists \mathbf{b}$ ideal de $\mathfrak{O}$ y $c \in \mathfrak{O}$ no nulo tal que $c\mathbf{a}=\mathbf{b}$, tomando $\mathbf{a'}=c\mathbf{b}^{-1}$ se sigue de 6) que $\mathbf{aa'}=\mathfrak{O}$ luego tomando $\mathbf{d}=\mathbf{a'}$ tenemos lo que queríamos.

8) : Suponer que no es cierto y lleguemos a contradicción. Como en 1) podemos elegir $\mathbf{a}$ ideal maximal en el conjunto de ideales que no son producto de ideales primos. $\mathbf{a}$ no puede ser primo y como todo ideal primo es maximal en $\mathfrak{O}$ por ser DD, $\exists \mathbf{p}$ maximal tal que $\mathbf{a} \subseteq \mathbf{p}$, como en 6),

$$\mathbf{a} \subset \mathbf{ap}^{-1} \subseteq \mathfrak{O}$$

por la maximalidad de $\mathbf{a}$, $\mathbf{ap}^{-1}=\mathbf{p}_1\cdots\mathbf{p}_r$ para ciertos ideales primos $\mathbf{p}_i$. Pero entonces tenemos

$$\mathbf{a}=\mathbf{pp}_1\cdots\mathbf{p}_r,$$

llegando a contradicción.

9) : Dados dos ideales $\mathbf{a}$ y $\mathbf{b}$, diremos que $\mathbf{a}$ divide a $\mathbf{b}$ ($\mathbf{a}|\mathbf{b}$) si existe un ideal $\mathbf{c}$ tal que $\mathbf{b}=\mathbf{ac}$. Esto equivale a que $\mathbf{b} \subseteq \mathbf{a}$, además podemos tomar $\mathbf{c}=\mathbf{a}^{-1}\mathbf{b}$. Sea $\mathbf{p}$ ideal primo tenemos que si $\mathbf{p}|\mathbf{ab}$ entonces $\mathbf{p}|\mathbf{a}$ o $\mathbf{p}|\mathbf{b}$. Si tenemos una serie de ideales primos $\mathbf{p}_1,\ldots,\mathbf{p}_r,\mathbf{q}_1,\ldots,\mathbf{q}_s$ tales que

$$\mathbf{p}_1\cdots\mathbf{p}_r=\mathbf{q}_1\cdots\mathbf{q}_s,$$

entonces $\mathbf{p}_1|\mathbf{q}_i$ para algún i, y como estamos en un DD por maximalidad $\mathbf{p}_1=\mathbf{q}_i$. Multiplicando ahora por $\mathbf{p}_1^{-1}$ y por inducción se llega a la factorización única salvo por el orden de los factores. □

Este resultado se puede extender a cualquier DD ([DM] Capitulo 3, Teorema 16), y análogamente a como vimos en la demostración del apartado 9), podemos definir la propiedad de ser divisor de un ideal.

Definición. Sean **a** y **b** ideales de un DD, diremos que

$$\mathbf{a}|\mathbf{b} \text{ si y solo si } \mathbf{a} \supseteq \mathbf{b}.$$

Luego en un DD los factores de un ideal **b** son precisamente los ideales que contienen a **b**. Además la definición de un ideal primo **p** se traduce en una notación análoga a la de un elemento primo:

$$\mathbf{p}|\mathbf{ab} \text{ implica que } \mathbf{p}|\mathbf{a} \text{ ó } \mathbf{p}|\mathbf{b}.$$

Dados dos ideales **a** y **b** en un DD, podemos definir el máximo común divisor (mcd) y el mínimo común múltiplo (mcm) de dos ideales. Considerando la descomposición en primos de **a** y **b**: $\mathbf{a} = \prod \mathbf{p}_i^{e_i}$, $\mathbf{b} = \prod \mathbf{p}_i^{f_i}$.

$$mcd(\mathbf{a},\mathbf{b}) = \prod \mathbf{p}_i^{min(e_i,f_i)}, \quad mcm(\mathbf{a},\mathbf{b}) = \prod \mathbf{p}_i^{máx(e_i,f_i)}.$$

Lema 4.4. *Si **a** y **b** son ideales de un DD entonces: $mcd(\boldsymbol{a},\boldsymbol{b}) = \boldsymbol{a}+\boldsymbol{b}$, $mcm(\boldsymbol{a},\boldsymbol{b}) = \boldsymbol{a}\cap\boldsymbol{b}$.*

Demostración. Es una comprobación. □

Proposición 4.5. *Todo Dominio de ideales principales (DIP) es DD.*

Demostración: Veamos que un DIP cumple las tres condiciones de la definición de DD. Las condiciones 1) y 3) son fáciles de probar y se vieron durante el curso. Para ver que es íntegramente cerrado sobre su cuerpo de fracciones, demostremos que todo DFU cumple esta propiedad y como todo DIP es DFU quedará demostrada la condición 2). Sea K el cuerpo de fracciones de un DFU R, sea $z \in K$ entero sobre R. Sin pérdida de generalidad, consideramos b, c coprimos en R tales que $z = b/c$. Luego para ciertos $a_i \in R$, $i \in (0,\dots,n-1)$ tenemos que

$$(b/c)^n + a_{n-1}(b/c)^{n-1} + \cdots + a_1(b/c) + a_0 = 0,$$

luego

$$-b^n = c(a_{n-1}b^{n-1} + \cdots + a_1 bc^{n-2} + a_0 c^{n-1}).$$

Como R es DFU, algún factor primo de c divide b, pero hemos supuesto que estos eran coprimos, luego c es unidad y por tanto $z \in R$, luego es R es íntegramente cerrado sobre K como queríamos demostrar.□

Un DIP es un DD y todo DIP es un DFU, pero los recíprocos no tienen por qué cumplirse. Nuestro problema ahora es que un anillo de enteros algebraicos no tiene porque ser DFU.

Proposición 4.6. *Sea R un DD, entonces R es DFU si y solo si es DIP.*

Demostración. El recíproco es inmediato pues ya vimos en el grado que todo DIP es DFU.

Para ver la otra implicación, por el Teorema 4.3 basta ver que todo ideal primo **p** es principal. Sea $a \in \mathbf{p}$, por ser un DFU $a = up_1 \cdots p_n$ para ciertos p_i primos y u unidad, luego $\exists p_i$ con $i \in (1,\dots,n)$ tal que $p_i \in \mathbf{p}$. Por ser DD **p** es maximal, luego $\mathbf{p} = \langle p_i \rangle$, pues $\langle p_i \rangle \subseteq I \ \forall I$ ideal de R tal que $p_i \in I$. □

Para demostrar la siguiente proposición, haremos uso del siguiente lema y de una versión del teorema chino de los restos para ideales.

Lema 4.7. *Si I y J son ideales en un anillo conmutativo R tales que $I+J=R$, entonces $I^n+J^m=R$ $\forall m,n \in \mathbb{N}$.*

Demostración. Basta probar que $1 \in I^n + J^m = R \ \forall m,n$. Sean $a \in I, b \in J$ tales que $1 = a+b$, elevando ambos términos a nm y operando llegamos en el término de la derecha a una suma de elementos que están en $I^n + J^m$. □

Teorema 4.8. *Sean $I_1,\dots,I_n$ ideales de un anillo R tales que $I_i + I_j = R \ \forall i \neq j$. Entonces*

$$R/\bigcap_{i=1}^{n} I_i \to R/I_1 \times \cdots \times R/I_n$$

es un isomorfismo.

Demostración. ([DM] Apéndice 1, pág. 253). □

Proposición 4.9. *Un ideal I de un DD R puede ser generado por dos elementos.*

Demostración. Sea $0 \neq a \in I$, basta encontrar $b \in R$ tal que $I = mcd(\langle a \rangle, \langle b \rangle)$. Por estar en un DD. sea $\mathbf{p}_1^{n_1}, \ldots, \mathbf{p}_n^{n_n}$ la descomposición en ideales primos de I, donde cada $\mathbf{p}_i$ es distinto. Entonces $\langle a \rangle$ es divisible por cada $\mathbf{p}_i^{n_i}$ ($\langle a \rangle \subseteq I \subseteq \mathbf{p}_i^{n_i}$). Sean $\mathbf{q}_1, \ldots, \mathbf{q}_s$ los restantes primos (si los hay) que dividen a $\langle a \rangle$. Vamos a encontrar un b tal que ningún $\mathbf{q}_j$ divida a $\langle b \rangle$, y para cada i, $\mathbf{p}_i^{n_i}$ sea la potencia exacta de $\mathbf{p}_i$ que divida a $\langle b \rangle$. Es decir,

$$b \in \bigcap_{i=1}^{r} (\mathbf{p}_i^{n_i} - \mathbf{p}_i^{n_{i+1}}) \cap \bigcap_{j=1}^{s} (R - \mathbf{q}_j).$$

Sea $b_i \in \mathbf{p}_i^{n_i} - \mathbf{p}_i^{n_{i+1}}$ (este existe pues es un DFU y $\mathbf{p}_i^{n_i} - \mathbf{p}_i^{n_{i+1}} \neq \emptyset$). Como $\mathbf{p}_i, \mathbf{q}_j$ son maximales y distintos para todos los i, j se sigue que la suma de cualquiera de ellos es R luego por el Lema 4.7 podemos aplicar el Teorema 4.8 a los ideales $\mathbf{p}_1^{n_1}, \ldots, \mathbf{p}_r^{n_r}, \mathbf{q}_1, \ldots, \mathbf{q}_s$, de forma que existe b satisfaciendo las congruencias:

$$b \equiv b_i (mod\, \mathbf{p}_i^{n_i+1}), \quad i = 1, \ldots, r;$$
$$b \equiv 1 (mod\, \mathbf{q}_j), \quad j = 1, \ldots, s.$$

Luego tenemos el b buscado. □

4.1. Ejemplos de factorización en ideales primos

A título de ejemplo en esta subsección describimos sin demostraciones algunos resultados de teoría de ramificación. Consideremos K y L cuerpos de números con $L \subset K$, siendo $\mathfrak{O}$ y $\mathfrak{S}$ sus anillos de enteros algebraicos respectivos.

Teorema 4.10. *Sean $\boldsymbol{q}$ ideal primo de $\mathfrak{O}$ y $\boldsymbol{p}$ ideal primo de $\mathfrak{S}$. Las siguientes condiciones son equivalentes.*

1) $\boldsymbol{q} | \boldsymbol{p}\mathfrak{O}$.
2) $\boldsymbol{q} \supset \boldsymbol{p}\mathfrak{O}$.
3) $\boldsymbol{q} \supset \boldsymbol{p}$.
4) $\boldsymbol{q} \cap \mathfrak{S} = \boldsymbol{p}$.
5) $\boldsymbol{q} \cap L = \boldsymbol{p}$.

Demostración: Son sencillas comprobaciones. ([DM] Cap 3 T.19). □

Cuando para $\mathbf{q}$ y $\mathbf{p}$ se cumplen las condiciones del teorema anterior diremos que $\mathbf{q}$ está sobre $\mathbf{p}$, o que $\mathbf{p}$ está bajo $\mathbf{q}$.

Teorema 4.11. *Todo ideal primo $\boldsymbol{q}$ de $\mathfrak{O}$ está sobre un único $\boldsymbol{p}$ primo de $\mathfrak{S}$. Todo ideal primo $\boldsymbol{p}$ de $\mathfrak{S}$ está bajo al menos un primo $\boldsymbol{q}$ de $\mathfrak{O}$.*

Demostración: ([DM] Capítulo 3 Teorema 20). □

Notar que los primos que están sobre $\mathbf{p}$ son precisamente los que se encuentran en la descomposición de ideales primos de $\mathbf{p}\mathfrak{O}$ (en el anillo $\mathfrak{O}$ que es un DD). Los exponentes que aparecen en la descomposición de primos de $\mathbf{p}\mathfrak{O}$ los llamaremos **índices de ramificación**, es decir si $\mathbf{p}\mathfrak{O} = \prod_{i=1}^{r} \mathbf{q}_i^{r_i}$ con los $\mathbf{q}_i$ primos, el índice de ramificación de $\mathbf{q}_i$ sobre $\mathbf{p}$ es $e(\mathbf{q}_i|\mathbf{p}) = r_i$.

Por otro lado, sean $\mathbf{p}$ y $\mathbf{q}$ como en el Teorema 4.10, notar que ambos ideales son maximales en sus respectivos anillos (pues son DD), luego $\mathfrak{O}/\mathbf{q}$ y $\mathfrak{S}/\mathbf{p}$ son cuerpos y de hecho el segundo es un subcuerpo del primero. Denotaremos por $f(\mathbf{q}|\mathbf{p})$ al grado de extensión de $\mathfrak{O}/\mathbf{q}$ sobre $\mathfrak{S}/\mathbf{p}$ y lo llamaremos **índice de inercia** asociado a $\mathbf{p}$ y $\mathbf{q}$.

Teorema 4.12. *Sea n el grado de extensión de K sobre L y sean $\mathbf{q}_1,\dots,\mathbf{q}_r$ primos de $\mathfrak{O}$ que están sobre un primo $\mathbf{p}$ de $\mathfrak{S}$. Denotando por $e_1,\dots,e_r$ y $f_1,\dots,f_r$ a los correspondientes índices de ramificación y de inercia. Entonces*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Demostración: ([DM] Capítulo 3 Teorema 21). □

Veamos ahora un ejemplo de factorización en ideales primos en un cuerpo de números cuadrático. Notar que si tomamos $K=\mathbb{Q}(\sqrt{d})$ y $L=\mathbb{Q}$, aplicando el Teorema 4.12 y teniendo en cuenta que $[K|\mathbb{Q}]=2$, para todo primo $p\in\mathbb{Z}$ (recordar que los ideales primos en $\mathbb{Z}$ son los generados por elementos primos) el ideal $p\mathfrak{O}$ se puede solo puede factorizarse de una de las siguientes formas.

$$p\mathfrak{O}=\begin{cases}\mathbf{q}^2, & f(\mathbf{q}|p\mathbb{Z})=1\\ \mathbf{q}, & f(\mathbf{q}|p\mathbb{Z})=2\\ \mathbf{q}\mathbf{q}_1, & f(\mathbf{q}|p\mathbb{Z})=f(\mathbf{q}_1|p\mathbb{Z})=1\end{cases}$$

siendo $\mathbf{q}$ y $\mathbf{q}_1$ ideales primos con $p\in\mathbf{q}$.

Para el siguiente teorema tomaremos las bases integrales y discriminantes correspondientes que vimos en la Proposición 2.9 (denotaremos por Δ al discriminante de la base en la que estemos).

Teorema 4.13. *Sea $K=\mathbb{Q}(\sqrt{d})$ con $d\in\mathbb{Z}$ libre de cuadrados y $d\neq 1$. Sea $p\in\mathbb{Z}$ primo. Entonces $\langle p\rangle := p\mathfrak{O}$ se factoriza en ideales primos en $\mathfrak{O}$ de la siguiente manera:*

a) Suponer que p es impar

- *(i) Si $p\not|\Delta$ y $a^2\equiv d\ (mod\ p)$ para algún $a\in\mathbb{Z}$ entonces $\langle p\rangle=\langle p,a+\sqrt{d}\rangle\langle p,a-\sqrt{d}\rangle$ siendo estos dos últimos ideales distintos.*
- *(ii) Si $p\not|\Delta$ y $X^2\equiv d\ (mod\ p)$ no tiene solución en $\mathbb{Z}$ entonces $\langle p\rangle$ es primo.*
- *(iii) Si $p|\Delta$ entonces $\langle p\rangle=\langle p,\sqrt{d}\rangle^2$.*

b) Suponer que p es 2

- *(i) Si $2\not|\Delta$ y $d\equiv 1\ (mod\ 8)$ entonces $\langle 2\rangle=\langle 2,\frac{1}{2}+\frac{1}{2}\sqrt{d}\rangle\langle 2,\frac{1}{2}-\frac{1}{2}\sqrt{d}\rangle$ siendo estos dos últimos ideales distintos.*
- *(ii) Si $2\not|\Delta$ y $d\equiv 5\ (mod\ 8)$ entonces $\langle 2\rangle$ es primo.*
- *(iii) Si $2|\Delta$ y $d\equiv 2\ (mod\ 4)$ entonces $\langle 2\rangle=\langle 2,\sqrt{d}\rangle^2$.*
- *(iv) Si $2|\Delta$ y $d\equiv 3\ (mod\ 4)$ entonces $\langle 2\rangle=\langle 2,1+\sqrt{d}\rangle^2$.*

(notar que no hay más casos posibles, esto se sigue fácilmente tras revisar la forma del discriminante en la Proposición 2.9).

Demostración:

a).(i): Sea a como en el enunciado, notar que $\langle p\rangle=\langle p,a+\sqrt{d}\rangle\langle p,a-\sqrt{d}\rangle=\langle p\rangle\langle p,a+\sqrt{d},a-\sqrt{d},(a^2-d)/p\rangle$, veamos que este último ideal es $\mathfrak{O}$. Como por hipótesis $a^2\equiv d$ (mod p), se sigue $\exists q\in\mathbb{Q}$ tal que $q(a^2-d)/p=p$ luego p pertenece al ideal. Además es evidente que $2a$ pertenece al ideal, como p y $2a$ son primos relativos, se sigue del Teorema de Bezout que 1 está en el ideal, luego ese ideal es $\mathfrak{O}$. Para ver que $\langle p,a+\sqrt{d}\rangle\neq\langle p,a-\sqrt{d}\rangle$, notar que en caso contrario $a-\sqrt{d}\in\langle p,a+\sqrt{d}\rangle$, luego se sigue que $2a,p\in\langle p,a+\sqrt{d}\rangle$ y tendríamos que $\langle p,a+\sqrt{d}\rangle^2=\langle p\rangle=\mathfrak{O}$ llegando a contradicción.

a).(ii): Sea $\mathbf{p}$ un ideal primo que contiene a p, veamos que este tiene índice de inercia 2 sobre $\mathbb{Z}_p$ de forma que aplicando el Teorema 4.12 se seguirá que $\mathbf{p}=\langle p\rangle$. Para ello basta ver que no tiene índice 1, luego es suficiente con demostrar que $\mathfrak{O}/\mathbf{p}$ no es isomorfo a $\mathbb{Z}_p$. Como p es impar y $p\not|\Delta$ se sigue de la Proposición 2.9 que $p\not|d$. Como además d es libre de cuadrados, considerando el polinomio X^2-d

observamos que no tiene raíces en $\mathbb{Z}_p$ pero si las tiene en $\mathfrak{O}$ y, por tanto, también tiene raíces en $\mathfrak{O}/\mathbf{p}$, luego no son isomorfos y se sigue el resultado.

a).(iii) Notar que $\langle p, \sqrt{d}\rangle^2 = \langle p\rangle\langle p, \sqrt{d}, d/p\rangle$, veamos que este último ideal es $\mathfrak{O}$. Como p es impar y $p|\Delta$, se sigue de la Proposición 2.9 que $p|d$. Además al ser d es libre de cuadrados se tiene que p y d/p son primos relativos, luego se sigue el resultado como en a).(i).

Los apartados b).(i), b).(iii), b).(iv) se demuestran de forma similar a los apartados a).(i) y a).(iii), mientras que b).(ii) se demuestra de forma análoga al apartado a).(ii) considerando el polinomio $X^2 - X + \frac{1-d}{4}$. ([IR] Proposición 13.1.4). □

Finalicemos el trabajo con un ejemplo concreto. Consideremos el anillos de enteros cuadráticos $\mathbb{Z}[\sqrt{-5}]$ del cuerpo de números $\mathbb{Q}(\sqrt{-5})$ y factoricemos el ideal $\langle 6\rangle$ en ideales primos. Es evidente que $\langle 6\rangle = \langle 2\rangle\langle 3\rangle$ y aplicando el teorema anterior tenemos que

$$\langle 2\rangle = \langle 2, 1+\sqrt{-5}\rangle^2, \qquad \langle 3\rangle = \langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle.$$

Luego llegamos a que

$$\langle 6\rangle = \langle 2, 1+\sqrt{-5}\rangle^2\langle 3, 1+\sqrt{-5}\rangle\langle 3, 1-\sqrt{-5}\rangle.$$

Bibliografía

[SG] S. GUTIÉRREZ, (Noviembre 2010,pp. 95-98), Kummer: los números ideales camino del teorema de Fermat, *Suma*, https://revistasuma.es/IMG/pdf/65/095-098.pdf.

[IR] K. IRELAND, M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer, 1990 (second edition).

[CI] C. IVORRA CASTILLO, *Apuntes Teoría Algebraica de Números*, https://www.uv.es/ivorra/Libros/Numeros2.pdf.

[DL] D. LORENZINI, *An Invitation to Arithmetic Geometry-American Mathematical Society (1996)*, Graduate Studies in Mathematics.

[DM] D. A. MARCUS, *Number Fields (1977, Springer-Verlag New York)*.

[JO] J. OTAL, *Curso de teoría algebraica de números*, Pre-print, Universidad de Zaragoza, Zaragoza 1991.

[ST] I. STEWART, D. TALL, *Algebraic number theory and Fermat's last theorem (2016, CRC Press)*.

[MS] M. SUÁREZ ÁLVAREZ, *Apuntes Dominios de Dedekind*, https://docplayer.es/2824256-Dominios-de-dedekind.html.