UNIVERSIDAD DE MURCIA

Facultad de Matemáticas

Trabajo Fin de Grado

Anillos de Enteros de Cuerpos de Números

Jesús Hernández Gil

Junio 2013

Índice general

Introduction

The fact that the ring of integers is a unique factorization domain (UFD), ie all non-zero element and non-unit decomposes as a product of primes uniquely except order and associates, is a very useful tool when solving some of the Diophantine equations. A good example is the determination of all primitive Pythagorean triads (no common factors integer solutions of Pythagorean equation $x^2 + y^2 = z^2$) as triads (x, y, z) of integer the form $x = \pm(m^2 - n^2)$, $y = \pm 2mn$, $z = \pm(m^2 + n^2)$ with m and n relatively prime and not both odd.

However, the method used to get to this result, which is to consider a specific decomposition expression, $x^2 = (z + y)(z - y)$ integer, it can't be applied to other types of equations that have a suitable decomposition in the ring of integer. In such cases, the commonly used method consists of considering a particular extension of the ring of integer numbers in which expression can be decomposed and in which we suppose suitable conditions of factorization. Let us see an example.

Fermat claimed that the only integer solutions of the equation $y^2 + 2 = x^3$ are precisely $y = \pm 5$, $x = 3$.

To prove this result, since this term doesn't have a decomposition in the ring of integer, it can be convenient to work in the ring

$$\mathbb{Z}[\sqrt{-2}] = \{\, a + b\sqrt{-2} \,|\, a, b \in \mathbb{Z}\}$$

in which

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2})$$

assuming, a priori, that in this ring certain factoring properties similar to those which occur in integers are verified. Properties, as discussed in memory, actually occur.

Thus, given a solution x, y of this equation, y obviously can't be even, and if $2|y$, then $2|x$ and therefore, $2^3|x^3 = y^2 + 2$ and should $2^2|x^3 - y^2$, which is a contradiction.

Once we have taken this into account, and using the function norm $N(a + b\sqrt{-2}) = a^2 + 2b^2$, we can see that $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ have no common factors in the ring $\mathbb{Z}[\sqrt{-2}]$ except ± 1. But, as the product $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$ is a cube, each of them is a cube and, therefore,

$$y + \sqrt{-2} = (m + n\sqrt{-2})^3 = (m^3 - 6mn^2) + (3m^2n - 2n^3)\sqrt{-2},$$

where, matching coefficients are obtained

$$y = m^3 - 6mn^2 \ \ , \ 1 = (3m^2 - 2n^2)n.$$

The only integer solutions of the last equation are $m = \pm 1$ and $n = 1$ which correspond, as claimed by Fermat, to $y \pm 5$, $x = 3$.

The results are not always so satisfactory. By analogy with the previous case, one might think that to solve the equation $y^2 + 11 = x^3$ it can be useful to work on this occasion with the ring $\mathbb{Z}[\sqrt{-11}] = \{a + b\sqrt{-11} \mid a, b \in \mathbb{Z}\}$. Indeed, considering that y may not be divisible by 11 and using standard function in this ring, $N(a+b\sqrt{-11}) = a^2+11b^2$, also comes to the conclusion that $(y+\sqrt{-11})$ and $(y - \sqrt{-11})$ both common factors have to be a cube and that the only solutions of this equation is $y = \pm 58$, $x = 15$ that indeed are solutions, but not unique since, as it can be seen easily, so are $y = \pm 4$, $x = 3$ that have not been obtained.

These solutions are found, together with those already obtained, if instead of working in ring $\mathbb{Z}[\sqrt{-11}]$ the ring considered is

$$\mathbb{Z}[\frac{1+\sqrt{-11}}{2}] = \{a + b(\frac{1+\sqrt{-11}}{2}) \mid a, b \in \mathbb{Z}\} \ = \ \{\frac{a+b\sqrt{-11}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \text{ (mód 2) }\}$$

containing the former and,as it will be discussed in this report, it is also a domain of unique factorization. It would therefore be appropriate to consider an extension of the ring of integers which provides good conditions of factorization.

Arguably Gauss was the first to feel the need to formalize factorization properties in an extension of the integers. Between 1808 and 1832, he developed a theory of prime factorization of what are now called **Gaussian integer**, the numbers of the form $a + bi$ with $a, b \in \mathbb{Z}$, and showed that the decomposition into primes in this ring was unique.

The study of such a property would also be very important in the historical development of the so called Fermat's Last Theorem, a result recently shown by Wiles.

It is well known that the origin of this problem is an annotation by Pierre de Fermat (1601-1665) made around 1630, in the margins of their *A*rithmetic by Diophantus. It indicated that it was impossible to express a cube as the sum of two cubes or generally, any higher-order power as sum of two powers of the same order, a fact for which he claimed to have an extraordinary demonstration but found that the margins were too narrow to include it.

Fermat himself, using the method of descent, had shown the result for $n = 4$, thus reducing the problem to remaining exponent considered odd primes.

If there is a solution of the equation $x^p + y^p = z^p$ it can be considered a factorization of the form

$$z^p = (x + y)(x + \xi y) \cdots (x + \xi^{p-1} y)$$

in the ring $\mathbb{Z}[\xi] = \{a_0 + a_1\xi + \cdots + a_r\xi^r \ \mid \ a_j \in \mathbb{Z}\}$, with $\xi = e^{2\pi i/p}$ a p-th root of unity, to study, use in this ring of a divisibility reasoning from unique factorization. This way Euler and Gauss got a demonstration for $p = 3$ and Dirichlet for $p = 5$.

In 1847, Lamé announced a demonstration of the Fermat's Last Theorem. His idea was that if x and y didn't have common factors, the above factors didn't have them either and each of them had to be a p-th power, from which Lamé deduced a contradiction. Liouville told him that his deduction supposed uniqueness of decomposition and, in fact, Kummer had demonstrated three years before that the uniqueness of the decomposition failed in some cases, the first one for $n = 23$.

Although this type of rings, the rings of integers, needn't have a theory of unique factorization of elements, the works developed by Kummer and Dedekind show that there is a good theory of factorization of ideals.

These are precisely the issues we want to study in this report: the introduction of the rings of integers of number fields, their identification in individual cases and determine, in such cases, if unique factorization conditions are given or not, using the ideal class-group and class-number of a ring of integers.

In the first chapter, the concepts and basic properties of the theory of field extensions are recalled, necessary for the development of the theory. Basically following the line marked in [5], define the concepts as algebraic integer, ring of integers and integral basis of a number field, main object of our study. We demonstrate the existence of integral bases in the rings of numbers, and the special integer basis Theorem can be found in [3], although it is unusual to appear in the bibliography. This theorem gives us a integer basis of a very concrete way, but not always easy to calculate. Definitions of norm, trace and discriminant are introduced and their properties are studied. These concepts are especially helpful for practical calculations.

In the second chapter the rings of integers of certain numbers field are identified: quadratic fields, cyclotomic fields, biquadratic fields and pure cubic extensions. Although quadratic and cyclotomic fields (when it comes to p-th root of the unit with p prime) is becoming common in the literature, biquadratic fields and pure cubic extensions aren't common, which, for example, in [3] appears as exercises and whose proof we have included.

In the third chapter, we develop the theory corresponding to the factorization of a domain irreducible in elements. The importance of taking integer ring of number fields in our study is checked, because these rings are Noetherian and therefore factorization in them is possible. However, this unique factorization doesn't always happen, and in this chapter several such situations are included. We show that this factorization is unique if and only if every irreducible element is prime and that all principal ideal domain, and therefore all Euclidean domain has unique factorization.

In the fourth chapter, following the theories of Kummer and Dedekind, it is proved that even in the rings of integers the unique factorization into irreducible elements doesn't always happen, there is a unique factorization of ideals as a product of prime ideals. The concept of norm of an ideal is introduced, with the importance of its multiplicative property. It is determined how to factorize on certain integer rings ideals primes generated by prime numbers and therefore those generated by any integer number, based on the decomposition of certain polynomials over finite fields and it is shown that a ring of integer is a unique factorization domain if and only if it is a principal ideal domain. In general, it shown that although we don't have unique factorization in irreducible elements on a ring of integer of a number field, all non-zero ideal is generated at most by two elements.

The fifth chapter deals with the development of tools to study whether there is unique factorization in certain rings of integers. On the one hand, a geometric sense is provided to the ring of integer of number fields as lattices of $\mathbb{R}^n$. Furthermore, we define an equivalence relation in the set of fractional ideals which allows us to obtain an Abelian group, called the class-group, and its cardinal called class-number, which will be one just as the ring of integers is a unique factorization domain. The application of Minkowski's Theorem to the correspondent lattice allows to obtain a bound for the norm of a representative of each of the classes of ideals and the finiteness of the class-number. We

finish the chapter by showing some examples of application of these techniques.

In the memory Annex we include a table that lists the relevant data (discriminant class-group, class-number, factorization of ideals generated by prime numbers, etc.) corresponding to the results we have obtained to calculate effectively the class-group and the class-number of certain rings of integers.

Tema 1

Enteros algebraicos

1.1. Números algebraicos

En lo que sigue cuando hablemos de un anillo $\mathbf{R}$, siempre nos referiremos a un anillo conmutativo con elemento unidad ($1 \neq 0$). Si tal anillo no tiene divisores de cero (es decir, $a \neq 0$ y $b \neq 0$ implica $ab \neq 0$) se dirá que $\mathbf{R}$ es un dominio.

Usaremos la notación standard $\mathbb{N}$ para el conjunto de los naturales, $\mathbb{Z}$ para los enteros , $\mathbb{Q}$ para los racionales, $\mathbb{R}$ para los reales y $\mathbb{C}$ para los complejos.

Empezamos recordando algunos conceptos relativos a la teoría de extensiones de cuerpos, que serán utilizados en toda la memoria y cuyas demostraciones pueden encontrarse, por ejemplo, en [4] y [1].

Dado $L \subset K$, con L y K cuerpos, si la dimensión de K como espacio vectorial sobre L es finita, digamos n, entonces diremos que K es una ***extensión finita de grado*** n ***sobre*** L y denotaremos el grado de la extensión por $[K : L] := dim_L K$.

Definición 1.1. *Un número complejo α se dice que es un **número algebraico** si es algebraico sobre el cuerpo $\mathbb{Q}$ de los números racionales; es decir, si es raíz de un polinomio no nulo con coeficientes en $\mathbb{Q}$ o, equivalentemente, con coeficientes en $\mathbb{Z}$.*

Proposición 1.2. *Un numero complejo α es un número algebraico si y sólo si la extensión $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ es una extensión finita y, en este caso se verifican:*

*i) Existe un polinomio mónico irreducible $f(t) \in \mathbb{Q}[t]$, único, tal que $f(\alpha) = 0$. A este polinomio se le denominará **polinomio mínimo** (o polinomio irreducible) de α, sobre $\mathbb{Q}$, y se le denotará por $Irr(\alpha, \mathbb{Q})$.*

ii) Si $g(t) \in \mathbb{Q}[t]$ y $g(\alpha) = 0$, entonces $Irr(\alpha, \mathbb{Q})|g(t)$.

iii) Todo elemento de $\mathbb{Q}(\alpha)$ se escribe de forma única como $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ con los $a_i \in \mathbb{Q}$; es decir, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espacio vectorial; una $\mathbb{Q}$-base.

iv) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n = \partial(Irr(\alpha, \mathbb{Q}))$.

Definición 1.3. *Si α es un número algebraico, a las raíces de $Irr(\alpha, \mathbb{Q})$ en $\mathbb{C}$, que son todas distintas, se les denomina $\mathbb{Q}$-**conjugados** de α.*

A partir de estos resultados y del carácter multiplicativo del grado de una extensión se obtiene:

Teorema 1.4. *El conjunto $\mathcal{A}$ de los números algebraicos es un subcuerpo de $\mathbb{C}$.*

Como consecuencia de la existencia de polinomios irreducibles en $\mathbb{Q}[t]$ de grado tan grande como se quiera (los de la forma $t^n - 2$ o los ciclotómicos, por ejemplo) se tiene el resultado siguiente.

Proposición 1.5. *La extensión $\mathbb{Q} \subset \mathcal{A}$ es una extensión infinita.*

Los cuerpos que estudiaremos son subcuerpos de este cuerpo $\mathcal{A}$ finitamente generados sobre $\mathbb{Q}$.

Definición 1.6. *Se llama **cuerpo de números** a todo subcuerpo de $\mathbb{C}$ de dimensión finita sobre $\mathbb{Q}$; es decir, a toda extensión finita de $\mathbb{Q}$.*

Si K es un cuerpo de números entonces todo elemento de K es algebraico y, por tanto, $K \subset \mathcal{A}$.

Ejemplos 1.7. *Ejemplos de cuerpos de números:*

- $\mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ no cuadrado perfecto (*Cuerpos cuadráticos*).
- $\mathbb{Q}(\xi)$ con $\xi = e^{2\pi i/n}$ (*Cuerpos ciclotómicos*).
- Más generalmente, si α es un número algebraico $\mathbb{Q}(\alpha)$ es un cuerpo de números.

Este último caso es el arquetipo de cuerpo de números pues, como consecuencia del teorema del elemento primitivo, se tiene el siguiente resultado:

Teorema 1.8. *Si K es un cuerpo de números, entonces $K = \mathbb{Q}(\alpha)$ para algún número algebraico α.*

1.2. Discriminantes

Si $K = \mathbb{Q}(\theta)$ es un cuerpo de números, existen en general distintos $\mathbb{Q}$-homomorfismos $\sigma : K \longrightarrow \mathbb{C}$, es decir, homomorfismos inyectivos que dejan fijo a $\mathbb{Q}$, que de hecho solo hay una cantidad finita para un cuerpo de números:

Teorema 1.9. *Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números de grado n sobre $\mathbb{Q}$. Entonces hay exactamente n $\mathbb{Q}$-homomorfismos distintos $\sigma_i : K \longrightarrow \mathbb{C}\,(i = 1, \ldots, n)$. Los elementos $\sigma_i(\theta) = \theta_i$ son los distintos $\mathbb{Q}$-conjugados de θ.*

Demostración. Sean $\theta_1, \ldots, \theta_n$ los $\mathbb{Q}$-conjugados de θ. Entonces cada θ_i, también tiene por polinomio mínimo a p. Por lo tanto, hay un único isomorfismo de cuerpos $\sigma_i : \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta_i)$ tal que $\sigma_i(\theta) = \theta_i$. De hecho, si $\alpha \in \mathbb{Q}(\theta)$, como $\alpha = r(\theta)$ para un $r \in \mathbb{Q}[t]$ con $\partial r < n$, debe tenerse $\sigma_i(\alpha) = r(\theta_i)$ ([2] Corolario 2 hasta Teorema 7.4, pág. 66). Recíprocamente si $\sigma : K \longrightarrow \mathbb{C}$ es un $\mathbb{Q}$-homomorfismo,

entonces σ deja invariante a $\mathbb{Q}$ y, por tanto, $0 = \sigma(p(\theta)) = p(\sigma(\theta))$, por lo que $\sigma(\theta)$ es uno de los θ_i y σ es uno de los σ_i. □

Con la notación anterior, para cada $\alpha \in K = \mathbb{Q}(\theta)$ se define el *polinomio de cuerpo* de α sobre K como

$$f_\alpha(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha)).$$

En principio es un polinomio de $K[t]$, pero, más concretamente, se tiene:

Teorema 1.10. $f_\alpha(t) \in \mathbb{Q}[t]$.

Demostración. $\alpha = r(\theta)$ para un $r \in \mathbb{Q}[t]$, $\partial r < n$. Ahora el polinomio de cuerpo es de la forma

$$f_\alpha(t) = \prod_{i=1}^{n}(t - r(\theta_i))$$

donde los θ_i son los ceros del polinomio mínimo p de θ, cuyos coeficientes están en $\mathbb{Q}$. Es fácil ver que los coeficientes de $f_\alpha(t)$ son de la forma

$$h(\theta_1, \ldots, \theta_n)$$

donde $h(t_1, \ldots, t_n)$ es un polinomio simétrico en $\mathbb{Q}[t_1, \ldots, t_n]$ y el resultado se obtiene como consecuencia de [5] Corolario 1.14, pág. 25. □

A los elementos $\sigma_i(\alpha)$, para $i = 1, \ldots, n$, se les denomina los $\mathbb{Q}$-*conjugados de* α.

Teorema 1.11. *Con la anterior notación,*

(a) el polinomio de cuerpo f_α es una potencia del polinomio mínimo $p_\alpha = Irr(\alpha, \mathbb{Q})$,

(b) los K-conjugados de α son los ceros de p_α en $\mathbb{C}$, repetidos n/m veces donde $m = \partial p_\alpha$ es un divisor de n,

(c) el elemento $\alpha \in \mathbb{Q}$ si y sólo si todos sus K-conjugados son iguales,

(d) $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ si y sólo si todos los K-conjugados de α son distintos.

Demostración. Ver [5] Teorema 2.6, pág. 40. □

Atención: Nótese que los K-conjugados de α no son necesariamente elementos de K.

Definición 1.12. *Sea K=$\mathbb{Q}(\theta)$ un extensión de grado n y $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Q}$-base de K. Se define el discriminante de dicha base como*

$$\Delta[\alpha_1, \ldots, \alpha_n] = (det[\sigma_i(\alpha_j)])^2.$$

Si $\{\beta_1, \ldots, \beta_n\}$ es otra base, entonces

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i \text{ con los } c_i \in \mathbb{Q}$$

para $k = 1, \ldots, n$, y $det(c_{ik}) \neq 0$. Por la fórmula del determinante y el hecho de que los σ_i son $\mathbb{Q}$-homomorfismos, se puede ver fácilmente que

$$\Delta[\beta_1, \ldots, \beta_n] = (det[c_{ik}])^2 \Delta[\alpha_1, \ldots, \alpha_n].$$

Teorema 1.13. *El discriminante de cualquier base de $K = \mathbb{Q}(\theta)$ es un número racional no nulo. Si, además, todos los K-conjugados de θ son números reales, entonces el discriminante de cualquier base es positivo.*

Demostración. Consideremos primero la $\mathbb{Q}$-base de K $\{1, \theta, \ldots, \theta^{n-1}\}$. Si los K-conjugados de θ son $\theta_1, \ldots, \theta_n$, entonces

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (det[\theta_i^j])^2.$$

El determinante $det[\theta_i^j]$ es el determinante de *Vandermonde* de $\theta_1, \ldots, \theta_n$ y su valor viene dado por

$$\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)$$

por lo tanto se tiene que

$$\Delta = \Delta[1, \theta, \ldots, \theta^{n-1}] = [\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)]^2.$$

Como D es antisimétrico en los θ_i, D^2 es simétrico y, por [5] Corolario 1.14, pág. 25, Δ es un número racional. Si ahora $\{\beta_1, \ldots, \beta_n\}$ es otra base, entonces

$$\Delta[\beta_1, \ldots, \beta_n] = (det[c_{ik}])^2 \Delta$$

para ciertos números racionales c_{ik} con $det(c_{ik}) \neq 0$ por lo que

$$\Delta[\beta_1, \ldots, \beta_n] \neq 0$$

y también es un número racional. Evidentemente, si todos los θ_i son reales, entonces Δ es un real positivo, y por tanto también lo es

$$\Delta[\beta_1, \ldots, \beta_n].$$

□

1.3. Enteros algebraicos

Definición 1.14. *Un número complejo θ se dice que es un entero algebraico si existe un polinomio mónico con coeficientes enteros tal que $p(\theta) = 0$. Es decir, si*

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

donde $a_i \in \mathbb{Z}$ para todo i.

Por ejemplo $\theta = \sqrt{2}$ es un entero algebraico, ya que $\theta^2 - 2 = 0$. También $\tau = \frac{1}{2}(1 + \sqrt{5})$ lo es, ya que $\tau^2 - \tau - 1 = 0$. Pero $\frac{1}{2}$ no lo es ya que no es raíz de ningún polinomio mónico con coeficientes enteros.

Se denotará por $\mathcal{B}$ el conjunto de los enteros algebraicos.

De la definición de entero algebraico es fácil deducir el siguiente resultado:

Lema 1.15. *Un número complejo θ es un entero algebraico si y sólo si el grupo aditivo generado por todas las potencias $1, \theta, \theta^2, \ldots$ es finitamente generado.*

□

Teorema 1.16. *El conjunto $\mathcal{B}$ de los enteros algebraicos es un subanillo del cuerpo $\mathcal{A}$ de los números algebraicos.*

Demostración. Sean $\theta, \phi \in \mathcal{B}$ tenemos que probar que $\theta + \phi$ y $\theta\phi \in \mathcal{B}$. Por el lema anterior, todas las potencia de θ están en un subgrupo aditivo finitamente generado Γ_θ de $\mathbb{C}$, y todas las potencias de ϕ en un subgrupo aditivo finitamente generado Γ_ϕ. Pero ahora todas las potencias de $\theta + \phi$ y de $\theta\phi$ son combinaciones lineales enteras de los elementos $\theta^i\phi^j$ que están en $\Gamma_\theta\Gamma_\phi \subseteq \mathbb{C}$. Pero si Γ_θ tiene generadores $v_1, \ldots, v_n$ y Γ_ϕ tiene generadores $w_1, \ldots, w_m$, entonces $\Gamma_\theta\Gamma_\phi$ es el grupo aditivo generado por los $v_i w_j$ con $1 \leq i \leq n,\ 1 \leq j \leq m$. Por lo tanto todas las potencias de $\theta + \phi$ y de $\theta\phi$ están en un subgrupo aditivo finitamente generado de $\mathbb{C}$, así que por el anterior lema $\theta + \phi$ y $\theta\phi$ son enteros algebraicos. Por lo tanto $\mathcal{B}$ es un subanillo de $\mathcal{A}$. □

Una aplicación de este teorema nos da una gran herramienta para encontrar nuevos enteros algebraicos:

Teorema 1.17. *Sea θ un número complejo cero de un polinomio mónico cuyos coeficientes son enteros algebraicos. Entonces θ es un entero algebraico.*

Demostración. Supongamos que

$$\theta^n + \phi_{n-1}\theta^{n-1} + \cdots \ldots + \phi_0 = 0$$

donde $\phi_0, \ldots, \phi_{n-1} \in \mathcal{B}$. Esos elementos generan un subanillo Φ de $\mathcal{B}$. El argumento del lema muestra que todas las potencia de θ están en un Φ-submódulo finitamente generado M de $\mathbb{C}$, generado por $1, \theta, \ldots, \theta^{n-1}$. Por el anterior teorema, cada ϕ_i y todas sus potencias están en un subgrupo aditivo finitamente generado Γ_i con generadores γ_{ij} $(1 \leq j \leq n_i)$. Se sigue que M está dentro del subgrupo aditivo generado por los elementos

$$\gamma_{1,j_i}, \gamma_{2,j_2}, \ldots, \gamma_{n-1,j_{n-1}}\theta^k$$

$(1 \leq j_i \leq n_i,\ 0 \leq i \leq n-1,\ 0 \leq k \leq n-1)$, que es finitamente generado. Así que M es finitamente generado y es un grupo aditivo. Por tanto θ es un entero algebraico. □

Los dos teoremas anteriores nos permiten obtener nuevos casos de enteros algebraicos; como $\sqrt{5}$ y $\sqrt{7}$ son enteros algebraicos también lo son $\sqrt{5}+3\sqrt{7}$ y $(\sqrt{5}-4)^2(\sqrt{7})^5$, y no sólo esos, sino que también son enteros algebraicos las raíces del polinomio

$$t^{53}+(\sqrt{5}-4)^2t^{15}-(\sqrt{5}+3\sqrt{7})t^4.$$

Definición 1.18. *Si K es un cuerpo de números se define el anillo de enteros de K, que representaremos por $\mathfrak{O}_K$, como*

$$\mathfrak{O}_K = K \cap \mathcal{B}.$$

A veces escribiremos simplemente $\mathfrak{O}$ cuando no de lugar a confusión. Fijémonos en el hecho de que K y $\mathcal{B}$ son subanillos de $\mathbb{C}$ por lo que también lo es $\mathfrak{O}$. Además, $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ y $\mathbb{Z} \subseteq \mathcal{B}$ así que $\mathbb{Z} \subseteq \mathfrak{O}$. Los siguientes resultados son fáciles de probar.

Lema 1.19. *Si $\alpha \in K$ entonces para algún elemento no nulo $c \in \mathbb{Z}$ se tiene $c\alpha \in \mathfrak{O}$.*

Corolario 1.20. *Si K es un cuerpo de números entonces $K= \mathbb{Q}(\theta)$ para algún entero algebraico θ.*

El siguiente resultado es un criterio muy útil para ver cuándo un número algebraico es un entero algebraico:

Teorema 1.21. *Un número algebraico α es un entero algebraico si y sólo si su polinomio mínimo sobre $\mathbb{Q}$ tiene coeficientes en $\mathbb{Z}$.*

Demostración. Sea p el polinomio mínimo de α sobre $\mathbb{Q}$, que es un polinomio mónico irreducible en $\mathbb{Q}[t]$. Si $p\in \mathbb{Z}[t]$ entonces α es un entero algebraico.
Recíprocamente, si α es un entero algebraico entonces $q(\alpha)=0$ para algún polinomio mónico $q \in \mathbb{Z}[t]$ y $p|q$. Por el lema de Gauss ([5] Lema 1.7, pág. 18) se sigue que $p \in \mathbb{Z}[t]$ porque algún múltiplo racional λp está en $\mathbb{Z}$ y divide a q, y por la monicidad de p y q se tiene que $\lambda = 1$. □

Lema 1.22. *Un entero algebraico es un número racional si y sólo si es un número entero. Es decir $\mathcal{B} \cap \mathbb{Q} = \mathbb{Z}$.*

Demostración. Claramente $\mathbb{Z} \subseteq \mathcal{B} \cap \mathbb{Q}$. Sea $\alpha \in \mathcal{B} \cap \mathbb{Q}$; como $\alpha \in \mathbb{Q}$ su polinomio mínimo sobre $\mathbb{Q}$ es $t-\alpha$. Por el teorema 1.21 los coeficientes de este están en $\mathbb{Z}$ así que $-\alpha \in \mathbb{Z}$ y entonces $\alpha \in \mathbb{Z}$. □

1.4. Bases enteras

Sea K un cuerpo de números de grado n sobre $\mathbb{Q}$. Como hemos visto en el corolario 1.20,
$K = \mathbb{Q}(\theta)$ con θ un entero algebraico, y se sigue que el polinomio mínimo p de θ tiene grado n y que $\{1, \theta, \ldots, \theta^{n-1}\}$ es una base para K.
El anillo $\mathfrak{O}$ de enteros de K, con la suma, es un grupo abeliano.

Definición 1.23. *En las condiciones anteriores se denomina base entera de K(o de $\mathfrak{O}$) a cualquier $\mathbb{Z}$-base de $(\mathfrak{O}, +)$.*

Es decir, un conjunto de enteros algebraicos $\{\alpha_1, \ldots, \alpha_m\}$ será una base entera si y sólo si todo elemento de $\mathfrak{O}$ se expresa de manera única de la forma

$$a_1\alpha_1 + \cdots + a_m\alpha_m$$

con $a_1, \ldots, a_m \in \mathbb{Z}$. Del lema 1.19, se sigue que cualquier base entera para K es una $\mathbb{Q}$-base de K. En particular $m = n$. Tenemos que probar que existen las bases enteras. Una vez visto eso, podemos pensar en cómo pueden ser las bases enteras, puediendo ser estas distintas de lo que se puede esperar en principio.
Por ejemplo, si $K = \mathbb{Q}(\sqrt{5})$ al ser $\sqrt{5}$ un entero algebraico, se tiene que $\mathbb{Z}[\sqrt{5}] \subseteq \mathfrak{O}$ sin embargo, en este caso, tenemos que el elemento $\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ es un entero algebraico, pues es cero del polinomio $f(t) = t^2 - t + 1$ y sin embargo $\frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$.

Vamos por lo tanto a demostrar que las bases enteras existen, que es equivalente a probar que $(\mathfrak{O}, +)$ es un grupo abeliano libre de rango n.

Lema 1.24. *Si $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Q}$-base de K con $\alpha_1, \ldots, \alpha_n$ enteros algebraicos entonces el discriminante $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z}$ y es distinto de cero.*

Demostración. Sabemos que $\Delta = \Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q}$ por el teorema 1.13, y es entero, ya que α_i lo son, por lo que $\Delta \in \mathbb{Z}$. Por el teorema 1.13 $\Delta \neq 0$. □

Teorema 1.25. *Todo cuerpo de números K tiene una base entera, y el grupo aditivo $\mathfrak{O}$ es libre abeliano de rango n igual al grado de K.*

Demostración. Como $K = \mathbb{Q}(\theta)$ para un entero algebraico θ, existen $\mathbb{Q}$-bases de K formadas por enteros algebraicos; por ejemplo $\{1, \theta, \ldots, \theta^{n-1}\}$. Sin embargo estas $\mathbb{Q}$-bases no tienen por qué ser bases enteras. Sin embargo el discriminante de las $\mathbb{Q}$-bases formadas por enteros algebraicos es siempre un número entero (lema 1.24). Por lo tanto, podemos elegir la $\mathbb{Q}$-base formada por enteros algebraicos $w_1, \ldots, w_n$ que haga mínimo $|\Delta[w_1, \ldots, w_n]|$. Vamos a probar que es una base entera.
Si no lo fuera, existiría un elemento $w \in \mathfrak{O}$ tal que

$$w = a_1w_1 + \cdots, a_nw_n$$

para $a_i \in \mathbb{Q}$ no todos en $\mathbb{Z}$. Puedo elegirlos de tal manera que $a_1 \notin \mathbb{Z}$. Entonces $a_1 = a + r$ donde $a \in \mathbb{Z}$ y $0 < r < 1$. Si se definen

$$\psi_1 = w - aw_1, \qquad \psi_i = w_i \qquad (i = 2, \ldots, n),$$

entonces $\{\psi_1, \ldots, \psi_n\}$ es una $\mathbb{Q}$-base formada de enteros.
El determinante del cambio de base $\{w_1, \ldots, w_n\}$ a $\{\psi_1, \ldots, \psi_n\}$ es

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

y por lo tanto

$$\Delta[\psi_1, \ldots, \psi_n] = r^2 \Delta[w_1, \ldots, w_n].$$

Como $0 < r < 1$ esto contradice la elección de $\{w_1, \ldots, w_n\}$ haciendo $|\Delta[w_1, \ldots, w_n]|$ minimal. □

Teorema 1.26. *Supongamos $\alpha_1, \ldots, \alpha_n \in \mathfrak{O}$ forman una $\mathbb{Q}$-base de K. Si $\Delta[\alpha_1, \ldots, \alpha_n]$ es libre de cuadrados, entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera.*

Demostración. Sea $\{\beta_1, \ldots, \beta_n\}$ una base entera. Entonces existen números enteros c_{ij} tales que $\alpha_i = \sum c_{ij}\beta_j$ y, por tanto,

$$\Delta[\alpha_1, \ldots, \alpha_n] = (det[c_{ij}])^2 \Delta[\beta_1, \ldots, \beta_n].$$

Como $det[c_{ij}] \in \mathbb{Z}$ y $\Delta[\alpha_1, \ldots, \alpha_n]$ es libre de cuadrados, hemos de tener que $det[c_{ij}] = \pm 1$, así que (c_{ij}) es unimodular; por lo que el cambio de base es biyectivo y se tiene lo pedido. □

Como aplicación de este resultado, podemos calcular algunas bases enteras con facilidad. Por ejemplo en $\mathbb{Q}(\sqrt{5})$ como hemos visto anteriormente $\frac{1+\sqrt{5}}{2}$ es un entero algebraico, y $\{1, \frac{1+\sqrt{5}}{2}\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{5})$. Además los monomorfismos de la extensión son los dados por $\sigma_1(\sqrt{5}) = \sqrt{5}$ y $\sigma_2(\sqrt{5}) = -\sqrt{5}$, por lo que el discrimintante de la base es

$$\Delta[1, \frac{1+\sqrt{5}}{2}] = \begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{vmatrix}^2 = 5$$

que es libre de cuadrados, por lo que el teorema 1.26 nos asegura que $\{1, \frac{1+\sqrt{5}}{2}\}$ es una base entera.

Si $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ son dos bases enteras de un cuerpo de números K, entonces existen coeficientes $c_{ij} \in \mathbb{Z}$ tal que $\alpha_i = \sum c_{ij}\beta_j$ y además, al ser el cambio de base biyectivo se tiene $det[c_{ij}] = \pm 1$, y se tiene que

$$\Delta[\alpha_1, \ldots, \alpha_n] = (det[c_{ij}])^2 \Delta[\beta_1, \ldots, \beta_n] = \Delta[\beta_1, \ldots, \beta_n].$$

Por lo que el discriminante de todas las bases enteras de K es el mismo, y en adelante llamaremos *discriminante* de K, denotado por Δ_K o Δ cuando no haya lugar a confusión, como el discriminante de cualquier base entera.

Pero tenemos un resultado más importante aún, y es que siempre hay una base entera de una forma determinada. Antes de ello empezamos unos resultados previos:

Teorema 1.27. *Sean K y L dos cuerpos de números con grados, sobre $\mathbb{Q}$, m y n respectivamente y*

$$d = m.c.d(\Delta_K, \Delta_L).$$

Si $[KL : \mathbb{Q}] = mn$, entonces

$$\mathfrak{O}_{KL} \subset \frac{1}{d}\mathfrak{O}_K\mathfrak{O}_L.$$

En particular, si $[KL : \mathbb{Q}] = mn$ y $d = 1$ entonces $\mathfrak{O}_{KL} = \mathfrak{O}_K\mathfrak{O}_L$.

Demostración. Si $\{\alpha_1, \ldots, \alpha_m\}$ y $\{\beta_1, \ldots, \beta_n\}$ son dos bases enteras de los anillos de números $\mathfrak{O}_K$ y $\mathfrak{O}_L$ respectivamente, entonces $\{\alpha_i\beta_j\}_{\{(i,j)\}}$ es una $\mathbb{Q}$-base de KL y, también, una $\mathbb{Z}$-base de $\mathfrak{O}_K\mathfrak{O}_L$. Por tanto, si $\alpha \in \mathfrak{O}_{KL}$, existirán $r, m_{ij} \in \mathbb{Z}$, para $1 \leq i \leq m$ y $1 \leq j \leq n$, con $m.c.d(r, \{m_{ij}\}) = 1$ tales que

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r}\sigma(\alpha_i)\beta_j.$$

Veamos que, en estas condiciones, $r|d = m.c.d(\Delta_K, \Delta_L)$. Para ello bastará, por simetría, probar que $r|\Delta_K$.

Cada $\mathbb{Q}$-homomorfismo $\sigma : K \longrightarrow \mathbb{C}$ se extiende a un único KL-homomorfismo de KL a $\mathbb{C}$ que deja invariante a L, que también lo denotaremos por σ, por lo que

$$\sigma(\alpha) = \sum_{i,j} \frac{m_{ij}}{r}\sigma(\alpha_i)\beta_j.$$

Si, para cada $i = 1, \ldots, m$, consideramos

$$x_i = \sum_{j=1}^{n} \frac{m_{ij}}{r}\beta_j,$$

se tiene que, para cada K-homomorfismo de K en $\mathbb{C}$,

$$\sum_{i=1}^{m} \sigma(\alpha_i)x_i = \sigma(\alpha).$$

Extendida esta igualdad a todos los K-homomorfismos, se obtiene un sistema de ecuaciones lineales y, al resolverlo por Cramer, se obtiene que

$$x_i = \frac{\gamma_i}{\delta},$$

donde, como es bien sabido, δ es el determinante de la matriz $(\sigma_j(\alpha_i))$ de los coeficientes y cada γ_j se obtiene calculando el determinante de la matriz resultante de reemplazar la columna j-ésima de la matriz $(\sigma_j(\alpha_i))$ por los $\sigma_j(\alpha)$; por lo que los γ_j y los δ son enteros algebraicos, y $\delta^2 = \Delta_K$. Si $e = \Delta_K$, entonces

$$ex_i = \sum_{j=1}^{n} \frac{em_{ij}}{r}\beta_j = \gamma_i\delta \in L \cap \mathcal{B} = \mathfrak{O}_L$$

y, como los $\{\beta_j\}$ forman una base entera de $\mathfrak{O}_L$,

$$\frac{em_{ij}}{r} \in \mathbb{Z},$$

luego $r|em_{ij}$ para cada i, j y, por tanto, $r|e(m.c.d(\{m_{ij}\}))$; pero como r es primo con $m.c.d(\{m_{ij}\})$, entonces $r|e$. □

Lema 1.28. *Si $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Q}$-base de un cuerpo de números K formada por enteros algebraicos y $d = \Delta[\alpha_1, \ldots, \alpha_n]$, entonces cada entero algebraico $\alpha \in \mathfrak{O}$ 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 $\alpha \in \mathfrak{O}$, existirán $x_1, \ldots, x_n \in \mathbb{Q}$ tales que $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$.

Si $\sigma_1, \ldots, \sigma_n$ son los monomorfismos de K en $\mathbb{C}$, se tiene el sistema de ecuaciones lineales

$$\begin{cases} \sigma_1(\alpha) &= x_1\sigma_1(\alpha_1) + x_2\sigma_1(\alpha_2) + \cdots + x_n\sigma_1(\alpha_n) \\ \cdots & \cdots \\ \sigma_n(\alpha) &= x_1\sigma_n(\alpha_1) + x_2\sigma_n(\alpha_2) + \cdots + x_n\sigma_n(\alpha_n) \end{cases}$$

que puede ser resuelto usando Cramer, esto da lugar a

$$x_j = \frac{\gamma_j}{\delta} \qquad \text{para} \quad j = 1, \ldots, n$$

donde recordemos que δ es el determinante de la matriz $det[\sigma_j(\alpha_i)]$ y cada γ_j es el determinante de esa matriz cambiando la j-ésima columna por el vector columna $\sigma_i(\alpha)$, por lo que γ_j y δ son enteros algebraicos y $\delta^2 = d$. Como $\delta^2 = d$, se tiene que $dx_j = \delta\gamma_j$ es un entero algebraico y racional, por lo que $dx_j = m_j \in \mathbb{Z}$. Bastará probar ahora que $d|m_j^2$ para cada $j = 1, \ldots, n$. Pero

$$\frac{m_j^2}{d} = \frac{(d\gamma_j)^2}{d} = \gamma_j^2 \in \mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$$

luego $d|m_j^2$. □

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

$$\mathfrak{O} \subseteq \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}$$

Teorema 1.29. *(Teorema de la base entera especial) Si α es un entero algebraico de grado n sobre $\mathbb{Q}$, entonces existe una base entera de $\mathfrak{O}_{\mathbb{Q}(\alpha)} = \mathcal{B} \cap \mathbb{Q}(\alpha)$ de la forma*

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

donde los $d_i \in \mathbb{Z}$ con $d_1|d_2|\cdots|d_{n-1}$, los f_j son polinomios mónicos con coeficientes enteros y cada f_j tiene grado j. Los d_j están determinados unívocamente.

Demostración. Si α es un número algebraico de grado n sobre $\mathbb{Q}$, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$, luego si $d = \Delta(\alpha) = \Delta[1, \alpha, \ldots, \alpha^{n-1}]$ y K=$\mathbb{Q}(\alpha)$, se tiene por el lema anterior que

$$\mathfrak{O} \subset \mathbb{Z}\frac{1}{d} \oplus \mathbb{Z}\frac{\alpha}{d} \cdots \oplus \mathbb{Z}\frac{\alpha^{n-1}}{d}.$$

Sea para cada i, $0 \leq i \leq n$,

$$F_i \subset \mathbb{Z}\frac{1}{d} \oplus \mathbb{Z}\frac{\alpha}{d} \cdots \oplus \mathbb{Z}\frac{\alpha^{i-1}}{d} \cong \mathbb{Z}^i \quad \text{y} \quad R_i = \mathfrak{O} \cap F_i.$$

Entonces

$$R_1 = \mathbb{Z}\frac{1}{d} \cap \mathfrak{O} \subset \mathbb{Q} \cap \mathfrak{O} = \mathbb{Z} \subset R_1$$

luego $R_1 = \mathbb{Z}$. Además como

$$\mathfrak{O} \subset \mathbb{Z}\frac{1}{d} \oplus \mathbb{Z}\frac{\alpha}{d} \cdots \oplus \mathbb{Z}\frac{\alpha^{n-1}}{d}$$

entonces $R_n = \mathfrak{O}$. Obtendremos la existencia de la base por recurrencia 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_j están en $\mathbb{Z}$ con $d_1|d_2| \cdots |d_{i-1}$ y los f_j son polinomios mónicos de grado j.

Sea

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

la proyección canónica.

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

y $\pi(R_{i+1}) \neq 0$ pues contiene a α^i; por lo tanto será un grupo abeliano libre de rango 1 y existirá un $\beta \in R_{i+1}$ tal que $\pi(R_{i+1}) = \mathbb{Z}\pi(\beta)$. En estas condiciones,

$$\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{i-1}(\alpha)}{d_{i-1}}, \beta\}$$

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

En efecto, son generadores porque si $\gamma \in R_{i+1}$, $\pi(\gamma) = m\pi(\beta)$, se tiene que

$$\gamma - m\beta \in \ker(\pi) \cap \mathfrak{O} = F_i \cap \mathfrak{O} = R_i,$$

luego

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

Además son linealmente independientes, ya que si

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

como $m_0, m_1, \ldots, m_{i-1}, m \in \mathbb{Z}$, entonces

$$0 = \pi(m\beta) = m\pi(\beta) \Rightarrow m = 0 \Rightarrow m_0 = m_1 = \ldots = m_{i-1} = 0$$

Veamos que β se puede tomar de la forma deseada. Como $\alpha \in \mathfrak{O}$ y

$$\frac{f_{i-1}(\alpha)}{d_{i-1}} \in R_i = \mathfrak{O} \cap \left(\mathbb{Z}\frac{1}{d} \oplus \mathbb{Z}\frac{\alpha}{d} \cdots \oplus \mathbb{Z}\frac{\alpha^{i-1}}{d}\right),$$

resulta que

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

Mas concretamente, si

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

se tiene que

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

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

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

de donde

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

Si

$$\beta=\frac{1}{d}(b_0+b1\alpha+\cdots+b_{i-1}\alpha^{i-1}+b_i\alpha^i),\qquad\frac{b_i}{d}=\frac{1}{d_i},\ b_id_i=d$$

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

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

mónico de grado i.

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

y

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

luego

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

y

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

Por lo que $\gamma\in\mathfrak{O}\cap F_i=R_i$ y, por consiguiente, existen $a_0,a_1,\ldots,a_{i-1}\in\mathbb{Z}$ con

$$\gamma=a_01+a_1\frac{f_1(\alpha)}{d_1}+\cdots+a_{i-1}\frac{f_{i-1}(\alpha)}{d_{i-1}}=\frac{g(\alpha)}{d_{i-1}}$$

con $g\in\mathbb{Z}[t]$ y $\partial g<i$ y, como $\{1,\alpha,\ldots,\alpha^{n-1}\}$ son linealmente independientes sobre $\mathbb{Q}$, entonces $f_i(t)-tf_{i-1}(t)=g(t)$ de lo que se deduce que $f_i(t)=g(t)+tf_{i-1}(t)\in\mathbb{Z}[t]$ y se tiene la base deseada de R_{i+1}.

La unicidad de los d_i es consecuencia de que, en esas condiciones, son los menores enteros positivos m tales que $mR_{i+1}\subset\mathbb{Z}[\alpha]$. □

Observación 1.30.

- *Los polinomios mónicos f_i pueden ser sustituidos por otros polinomios mónicos $g_i(t)\in\mathbb{Z}[t]$ tales que, para cada i, $\partial g_i=i$ y $g_i(\alpha)/d_i$ sea entero algebraico.*
- $\Delta[1,\alpha,\ldots,\alpha^n]=\Delta[1,f_1(\alpha),\ldots,f_{n-1}(\alpha)]=(d_1\cdots d_{n-1})^2\Delta_{Q(\alpha)}$.

- *Si* $1 \leq i, j \leq n-1$ *con* $i+j \leq n-1$ *entonces* $d_i d_j | d_{i+j}$*, ya que tal y como se ha construido la base entera especial,*

$$\frac{f_i(\alpha)}{d_i}\,\frac{f_k(\alpha)}{d_j} \in \mathfrak{O} \cap F_{i+j} = R_{i+i} \text{ y } \frac{\alpha^i \alpha^j}{d_i d_j} = m\frac{\alpha^{i+j}}{d_{i+j}} \quad \textit{luego} \quad d_i d_j | d_{i+j}.$$

- *Teniendo en cuenta los dos puntos anteriores* $d_1^{n(n-1)} | \Delta[1, \alpha, \ldots, \alpha^{n-1}]$.

1.5. Normas y trazas

En esta sección se definen los conceptos de traza y la norma de un elemento, que resultarán muy útiles para determinar los enteros algebraicos. Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números de grado n, y sean $\sigma_1, \ldots, \sigma_n$ los n $\mathbb{Q}$-homomorfismos de K a $\mathbb{C}$. Por el Teorema 1.21 se tiene que un elemento $\alpha \in K$ es un entero algebraico si y sólo si el polinomio de cuerpo de ese elemento tiene coeficientes enteros.

Para cada $\alpha \in K$ se define la *norma*

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

y la *traza*

$$T_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Cuando esté claro sobre qué cuerpo tomamos la norma, abreviaremos la notación de la norma y la traza de α a $N(\alpha)$ y $T(\alpha)$ respectivamente. Como el polinomio de cuerpo de α

$$f_\alpha(t) = \prod_{i=1}^{n} (t - \sigma_i(\alpha))$$

es una potencia del polinomio mínimo de α, se sigue que *si* α *es entero algebraico entonces la norma y la traza de* α *son números enteros.* Como los σ_i son monomorfismos, se tiene que

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

y si $\alpha \neq 0$ entonces $N(\alpha) \neq 0$. Si p, q son números racionales, entonces

$$T(p\alpha + q\beta) = pT(\alpha) + qT(\beta).$$

Para un caso más general, cuanto tengamos dos cuerpos de números K y L, con $K \subset L$ y $n = [L : K]$, tendremos entonces n K-homomorfismos $\sigma_i : L \longrightarrow \mathbb{C}$ (y cada uno de los σ_i deja invariante K). Entonces escribiremos

$$T_K^L(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

$$N_K^L(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Veamos ahora algunas simplificaciones para calcular el discriminante a través de la norma y la traza:

Proposición 1.31. *Sea K= $\mathbb{Q}(\theta)$ un cuerpo de números, donde θ tiene polinomio mínimo p de grado n. La $\mathbb{Q}$-base $\{1, \theta, \ldots, \theta^{n-1}\}$ tiene discriminante*

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(Dp(\theta))$$

donde Dp es la derivada formal de p.

Demostración. Por la prueba del teorema 1.13 tenemos

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

donde $\theta_1, \ldots, \theta_n$ son los K-conjugados de θ. Ahora

$$p(t) = \prod_{i=1}^{n} (t - \theta_i)$$

así que

$$Dp(t) = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \neq j}}^{n} (t - \theta_i)$$

y por lo tanto

$$Dp(\theta_j) = \prod_{\substack{i=1 \\ i \neq j}}^{n} (\theta_j - \theta_i)$$

multiplicando todas esas ecuaciones para $j = 1, \ldots, n$ obtenemos

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

El término de la izquierda es $N(Dp(\theta))$; en el de la derecha, cada factor $(\theta_i - \theta_j)$ para $i < j$ aparece dos veces, una como $(\theta_i - \theta_j)$ y otra como $(\theta_j - \theta_i)$. El producto de esos dos factores es $-(\theta_i - \theta_j)^2$; por lo que el término de la derecha ese $(-1)^s \Delta$ $s = \frac{1}{2} n(n-1)$ es el número de pares (i, j) con $1 \leq i < j \leq n$. □

Proposición 1.32. *Si $\{\alpha_1, \ldots, \alpha_n\}$ es cualquier $\mathbb{Q}$-base de K, entonces*

$$\Delta[\alpha_1, \ldots, \alpha_n] = det[T(\alpha_i \alpha_j)].$$

Demostración. $T(\alpha_i \alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i) \sigma_r(\alpha_j)$; por lo tanto

$$\Delta[\alpha_1, \ldots, \alpha_n] = (det[\sigma_i(\alpha_j)])^2 = (det[\sigma_j(\alpha_i)])(det[\sigma_i(\alpha_j)]) = det[\sum_{r=1}^{n} \sigma_r(\alpha_i) \sigma_r(\alpha_j)] = det[T(\alpha_i \alpha_j)].$$

□

Tema 2

Anillo de enteros de algunos cuerpos de números

En este capítulo vamos a estudiar el anillo de enteros de algunos cuerpos de números: cuerpos cuadráticos, cuerpos ciclotómicos, extensiones bicuadráticas y extensiones cúbicas puras. Centrándonos únicamente en este tipo de cuerpos dado que la dificultad aumenta sustancialmente al incrementar el grado de la extensión. Obtendremos sus bases enteras y sus discriminantes.

2.1. Cuerpos cuadráticos

Un *cuerpo cuadrático* es un cuerpo de números K de grado 2 sobre $\mathbb{Q}$; por lo que $K=\mathbb{Q}(\theta)$ donde θ es un entero algebraico, y θ es raíz de un polinomio de la forma t^2+at+b con $a,b\in\mathbb{Z}$. Así que

$$\theta=\frac{-a\pm\sqrt{(a^2-4b)}}{2}.$$

Si $a^2-4b=r^2d$ donde $r,d\in\mathbb{Z}$ y d es libre de cuadrados, entonces

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

por lo que $\mathbb{Q}(\theta)=\mathbb{Q}(\sqrt{d})$. Hemos probado que:

Proposición 2.1. *Los cuerpos cuadráticos son precisamente aquellos de la forma $\mathbb{Q}(\sqrt{d})$ para d un entero libre de cuadrados.*

Vamos ahora a dar explícitamente cómo son los anillos enteros de los cuerpos cuadráticos:

Teorema 2.2. *Sea d un entero libre de cuadrados. Entonces el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es:*

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

(b) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ *si* $d\equiv 1\,(mód\ 4)$

Demostración. Todo elemento $\alpha\in\mathbb{Q}(\sqrt{d})$ es de la forma $\alpha=r+s\sqrt{d}$ para $r,s\in\mathbb{Q}$. Por lo tanto podemos escribir

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

con $a, b, c \in \mathbb{Z},\ c > 0$, y ningún primo divide a todos a, b, c. Ahora α es entero si y sólo si su polinomio mínimo tiene coeficientes enteros

$$\left(t - \left(\frac{a + b\sqrt{d}}{c}\right)\right)\left(t - \left(\frac{a - b\sqrt{d}}{c}\right)\right).$$

Así que

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}, \tag{1}$$

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

Si c y a tienen un factor primo común p, entonces (1) implica que p divide a b (ya que d es libre de cuadrados) lo que contradice nuestras premisas. Por lo tanto por (2) tenemos $c = 1$ ó 2. Si $c = 1$ entonces α es un entero de K en cualquier caso, nos centramos en el caso $c = 2$. Ahora a y b deben ser ambos impares, y $(a^2 - b^2 d)/4 \in \mathbb{Z}$. Por lo tanto

$$a^2 - b^2 d \equiv 0 \text{ (mód 4)}.$$

Ahora un número impar $2k+1$ tiene cuadrado $4k^2 + 4k + 1 \equiv 1$ (mód 4), por lo que $a^2 \equiv 1 \equiv b^2$ (mód 4), y esto implica que $d \equiv 1$ (mód 4). Recíprocamente, si $d \equiv 1$ (mód 4) entonces para impares a, b tenemos que α es entero algebraico por (1) y (2).

Para terminar, si $d \equiv 1$ (mód 4) entonces $c = 1$ y así que se tiene (a); si ahora $d \equiv 1$ (mód 4) podemos tener también $c = 2$ y a, b impares, por lo tanto también se tiene (b). □

Si $K = \mathbb{Q}(\sqrt{d})$ con d libre de cuadrados es un cuerpo cuadrático, entonces los $\mathbb{Q}$-homomorfismos $K \longrightarrow \mathbb{C}$ vienen dados por

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d} \text{ y } \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$$

Teorema 2.3. *Si $d \not\equiv 1$ (mód 4) entonces $\mathbb{Q}(\sqrt{d})$ tiene una base entera de la forma $\{1, \sqrt{d}\}$ y discriminante $4d$. Si $d \equiv 1$ (mód 4) entonces $\mathbb{Q}(\sqrt{d})$ tiene una base entera de la forma $\{1, \frac{1+\sqrt{d}}{2}\}$ y discriminante d.*

Demostración. La afirmación sobre las bases enteras se deduce del teorema 2.2; para los discriminantes, por el inciso anterior sobre los $\mathbb{Q}$-homomorfismos de los cuerpos cuadráticos tenemos, según sea el caso,

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & \sqrt{d} \end{vmatrix}^2 = 4d, \text{ y } \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d.$$

□

Con esto, ya tenemos caracterizados los discriminantes, bases enteras y anillos de enteros de todos los cuerpos cuadráticos, y no nos es difícil el comprobar que

$$N(r + s\sqrt{d}) = r^2 - ds^2 \text{ y } T(r + s\sqrt{d}) = 2r.$$

Un cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$ se dirá *real* si d es positivo, o se dirá *imaginario* si d es negativo.

2.2. Cuerpos ciclotómicos

Para esta sección puede tomarse como apoyo el capítulo 9 de [1] cuya notación y terminología seguiremos. $\xi = e^{2\pi i/m}$ es una raíz m-ésima primitiva de la unidad (raíz de la unidad con orden multiplicativo m). Como ξ es raíz del polinomio $f(t) = t^m - 1$, cuyas raíces son todas de la forma ξ^k para $1 \leq k \leq m$, $Irr(\xi, \mathbb{Q})|f$ y los $\mathbb{Q}(\xi)$-conjugados de ξ son de dicha forma donde, además, $m.c.d.(k, m) = 1$ ya que cada $\mathbb{Q}(\xi)$-conjugado de ξ es de la forma $\sigma(\xi)$ para algún $\mathbb{Q}$-homomorfismo $\sigma : \mathbb{Q}(\xi) \longrightarrow \mathbb{C}$ y, por tanto, será también una raíz m-ésima primitiva de la unidad; pero, por [1] Proposición 9.1.7, ξ^k es una raíz m-ésima primitiva de la únidad precisamente cuando se cumple dicha condición. Teniendo en cuenta esto y [1] Corolario 9.2.4, se tiene el siguiente resultado:

Teorema 2.4. *Los $\mathbb{Q}(\xi)$-conjugados de ξ son precisamente los ξ^k con $1 \leq k \leq m$, $m.c.d.(k, m) = 1$ y $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(m)$ donde ϕ es la función de euler.*

A $\mathbb{Q}(\xi)$ se le denomina m-ésimo cuerpo ciclotómico.

Observación 2.5.

- *Si $\xi = e^{2\pi i/m}$ y m es par, entonces las únicas raíces de la unidad en $\mathbb{Q}(\xi)$ son las raíces m-ésismas de la únidad. Si m es impar, las raíces de la unidad en $\mathbb{Q}(\xi)$ son las raíces $2m$-ésimas de la unidad.*
- *Los m-ésimos cuerpos ciclotómicos para m par son todos distintos, y de hecho, son no isomorfos dos a dos.*
- *Sean, ahora p un número primo impar, $\xi = e^{2\pi i/p}$ y $K = \mathbb{Q}(\xi)$. Usando el criterio de Eisenstein se puede ver que*

$$f(t) = Irr(\xi, \mathbb{Q}) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} \cdots + t + 1 = \prod_{i=1}^{p-1}(t - \xi^i)$$

y, por tanto, $[K : \mathbb{Q}] = p - 1$.

Como $t^p - 1 = f(t)(t - 1)$, derivando resulta que $pt^{p-1} = f(t) + (t - 1)f'(t)$ y

$$f'(\xi) = \frac{p\xi^{p-1}}{\xi - 1} = \frac{p}{\xi(\xi - 1)}$$

como $N(\xi) = 1$, y $N(\xi - 1) = \prod_{i=1}^{p-1}((\xi^i - 1)) = f(1) = p$, tenemos que

$$\Delta[1, \xi, \ldots, \xi^{p-2}] = (-1)^{(p-1)(p-2)/2}N(f'(t)) = (-1)^{(p-1)/2}\frac{N(p)}{N(\xi)N(\xi - 1)} =$$

$$= (-1)^{(p-1)/2}\frac{p^{p-1}}{p} = (-1)^{(p-1)/2}p^{p-2}.$$

En general, si $\xi = e^{2\pi i/m}$ y $f(t) = Irr(\xi, \mathbb{Q})$, sabemos que $t^m - 1 = f(t)g(t)$ con $g(t) \in \mathbb{Z}[t]$; por lo que $mt^{m-1} = f'(t)g(t) + f(t)g(t)$ y $m\xi^{m-1} = f'(\xi)g(\xi)$ y al tomar normas, se tiene

$$m^{\phi(m)} = \pm\Delta[1, \xi, \ldots, \xi^{\phi(m)-1}]N(\xi g(\xi)),$$

con $N(\xi g(\xi)) \in \mathbb{Z}$ pues es un entero algebraico. Es decir, $\Delta[1, \xi, \ldots, \xi^{p-2}]|m^{\phi(m)}$.

Demostraremos que si $\xi = e^{2\pi i/m}$, entonces el anillo de enteros de $\mathbb{Q}(\xi)$ es precisamente $\mathbb{Z}(\xi)$.

Lema 2.6. *Sea* $\xi = e^{2\pi i/m}$ *con* $m \geq 3$*, entonces* $\mathbb{Z}[1-\xi] = \mathbb{Z}[\xi]$ *y, además,* $\Delta[1,(1-\xi),\ldots,(1-\xi)^{\phi(m)-1}] = \Delta[1,\xi,\ldots,\xi^{\phi(m)-1}]$.

Lema 2.7. *Si* $\xi = e^{2\pi i/m}$*, con* $m = p^r$ *y* p *primo, entonces*

$$N(1-\xi) = \prod_{k,\, 1\leq k\leq m, p\nmid k} (1-\xi^k) = p.$$

Demostración. Si

$$f(t) = Irr(\xi, \mathbb{Q}) = \Phi_{p^r}(t) = \Phi_p(t^{p^{r-1}}),$$

donde Φ_s es el polinomio irreducible de $e^{2\pi i/s}$ sobre $\mathbb{Q}$. Por tanto, se tiene que

$$\prod_{k,\, 1\leq k\leq m, p\nmid k} (1-\xi^k) = f(1) = p.$$

□

Teorema 2.8. *Si* $\xi = e^{2\pi i/m}$*, entonces el anillo de enteros de* $\mathbb{Q}(\xi)$ *es* $\mathbb{Z}[\xi]$*, es decir:*

$$\mathfrak{O}_{\mathbb{Q}(\xi)} = \mathbb{Q}(\xi) \cap \mathcal{B} = \mathbb{Z}[\xi].$$

Demostración. Veámoslo primero cuando m es potencia de un primo. Sea $\xi = e^{2\pi i/m}$ donde $m = p^r$ y p es primo. Si $R = \mathfrak{O}_{\mathbb{Q}(\xi)}$ y $n = \phi(m) = p^{r-1}(p-1)$; como $\{1, 1-\xi, \ldots, (1-\xi)^{n-1}\}$ es una base formada por enteros algebraicos, sabemos por el Lema 1.28 que todo $\alpha \in R$ es de la forma

$$\alpha = \frac{m_1 + m_2(1-\xi) + \cdots + m_n(1-\xi)^{n-1}}{d}$$

donde los $m_i \in \mathbb{Z}$, $d = \Delta[1,\xi,\ldots,\xi^{n-1}] = \Delta[1,(1-\xi),\ldots,(1-\xi)^{n-1}] | m^{\phi(m)}$, que es una potencia de p, y además, d es un divisor de cada m_i^2.

Si $R \neq \mathbb{Z}[\xi] = \mathbb{Z}[1-\xi]$, considerando un elemento de la forma $p^s\alpha \in R$ para un determinado s, R tendrá algún elemento de la forma

$$\beta = \frac{m_i(1-\xi)^{i-1} + m_{i+1}(1-\xi)^i + \cdots + m_n(1-\xi)^{n-1}}{p},$$

para algún $i < n$, enteros m_j (para $i \leq j < n$) y con m_i no divisible por p.

Por otra parte, como

$$\frac{1-\xi^k}{1-\xi} = 1 + \xi + \cdots + \xi^{k-1} \in \mathbb{Z}[\xi],$$

por el tercer punto de la observación 2.5, tenemos que

$$\frac{p}{(1-\xi)^n} = \prod_{k,\, 1\leq k\leq m,\, p\nmid k} \frac{1-\xi^k}{1-\xi} \in \mathbb{Z}[\xi]$$

y, por tanto, también

$$\frac{p}{(1-\xi)^i} = (1-\xi)^{n-i}\frac{p}{(1-\xi)^n} \in \mathbb{Z}[\xi],$$

por lo que

$$\beta\frac{p}{(1-\xi)^i} \in R$$

y resulta que

$$\frac{m_i}{1-\xi} \in R,$$

por lo que

$$p = (1-\xi)|N(m_i) = m_i^n$$

lo que supone una contradicción. Procedamos por inducción para el caso general. Si suponemos el resultado cierto para los enteros menores que m y m no es una potencia de un primo, m se podrá escribir de la forma $m = k_1k_2$, con k_1 y k_2 primos entre sí y $k_1, k_2 > 1$, por lo que el resultado será cierto para ambos.

Si $\xi_1 = e^{2\pi i/k_1}$, $\xi_2 = e^{2\pi i/k_2}$, $K_1 = \mathbb{Q}(\xi_1)$, $K_2 = \mathbb{Q}(\xi_2)$, entonces $R_i = \mathfrak{O}_{K_i} = \mathbb{Z}[\xi_i]$. Además, $K_1K_2 = \mathbb{Q}(\xi)$, $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(m) = \phi(k_1)\phi(k_2) = [\mathbb{Q}(\xi_1) : \mathbb{Q}][\mathbb{Q}(\xi_2) : \mathbb{Q}]$ y $m.c.d(\Delta_{R_1}, \Delta_{R_2}) = m.c.d(\Delta[1, \xi_1, \ldots, \xi_1^{\phi(k_1)-1}], \Delta[1, \xi_2, \ldots, \xi_2^{\phi(k_1)-1}])$ (véase [1] Proposición 9.2.6). Con esto y por el Teorema 1.27 resulta que

$$\mathfrak{O}_{\mathbb{Q}(\xi)} = R_1R_2 = \mathbb{Z}[\xi_1]\mathbb{Z}[\xi_2] = \mathbb{Z}[\xi].$$

□

2.3. Cuerpos bicuadráticos

En esta sección demostramos cuál es el anillo de enteros de un cuerpo bicuadrático; es decir un cuerpo K de grado 4 sobre los racionales de la forma $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ que al igual que con los cuadráticos, podemos suponer que m, n son libres de cuadrados.

De aquí en adelante consideraremos $k = \dfrac{mn}{m.c.d(m,\, n)^2}$, que desempeñará un papel importante en las sucesivas demostraciones. Asimismo, cuando nos refiramos a K, siempre será $K = \mathbb{Q}(\sqrt{m},\, \sqrt{n})$.

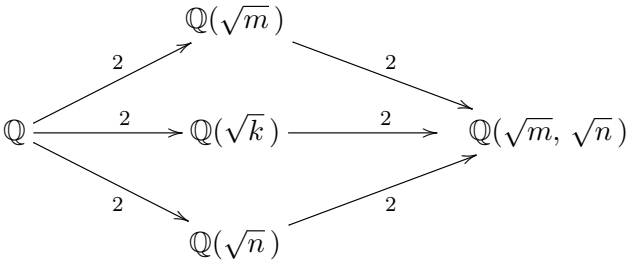
Lema 2.9. *El cuerpo bicuadrático K contiene a $\mathbb{Q}(k)$.*

Demostración. Basta probar que $\sqrt{k} \in K$. Pero

$$\sqrt{k} = \sqrt{\frac{mn}{m.c.d(m,\, n)^2}} = \frac{\sqrt{mn}}{m.c.d(m,\, n)} = \frac{\sqrt{m}}{m.c.d(m,\, n)}\sqrt{n} \in K.$$

□

El diagrama que tenemos es:



donde el número en la flecha indica el grado de la extensión. Utilizaremos este diagrama para apoyarnos en extensiones de grado dos para calcular el anillo de enteros.
El siguiente resultado generaliza el hecho de que la traza y la norma de un entero algebraico sean números enteros.

Teorema 2.10. *Sean S y L cuerpos de números con $S \subset L$ y $n = [\,L : S]$. Si $\alpha \in \mathfrak{O}_L = \mathcal{B} \cap L$ es un entero alebraico, entonces $T_S^L(\alpha)$, $N_S^L(\alpha) \in \mathfrak{O}_S = \mathcal{B} \cap S$.*

Demostración. Si $\alpha \in L$ es un entero algebraico y σ es un S-homomorfismo de L en $\mathbb{C}$, se verifica que $\sigma(\alpha)$ es también un entero algebraico pues es raíz de $Irr(\alpha,\, S) \in S[t]$ y, por tanto $T_S^L(\alpha)$ y $N_S^L(\alpha)$, que son suma y producto de elementos de este tipo son también enteros algebraicos de S. □

Proposición 2.11. *Un elemento $\alpha \in K$ es entero algebraico si y sólo si se tiene que $T^K_{\mathbb{Q}(\sqrt{m})}(\alpha)$ y $N^K_{\mathbb{Q}(\sqrt{m})}(\alpha) \in \mathfrak{O}_{Q(\sqrt{m})}$.*

Demostración. Por el Teorema 2.10, si α es un entero algebraico, entonces $T^K_{\mathbb{Q}(\sqrt{m})}(\alpha)$ y $N^K_{\mathbb{Q}(\sqrt{m})}(\alpha) \in \mathfrak{O}_{Q(\sqrt{m})}$. Recíprocamente, si $T^K_{\mathbb{Q}(\sqrt{m})}(\alpha)$ y $N^K_{\mathbb{Q}(\sqrt{m})}(\alpha) \in \mathfrak{O}_{Q(\sqrt{m})}$, entonces α es raíz del polinomio

$$f(t) = X^2 - T^K_{\mathbb{Q}(\sqrt{m})}(\alpha)t + N^K_{\mathbb{Q}(\sqrt{m})}(\alpha)$$

que tiene por coeficientes enteros algebraicos y por el Teorema 1.16, se tiene que α es entero algebraico. □

Apoyandonos en este resultado, podemos calcular ya el anillo de enteros de los cuerpos bicuadráticos según los casos:

Teorema 2.12. *Si $m \equiv 3\,(mód\ 4)$ y $n \equiv k \equiv 2\,(mód\ 4)$, entonces todo elemento de $\mathfrak{O}_K$ se puede expresar de la forma*

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2} \text{ con } a,\, b,\, c,\, d \in \mathbb{Z} \text{ } a,b \text{ pares y } c \equiv d\,(mód 2),$$

una base entera para $\mathfrak{O}_K$ viene dada por

$$\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{k}}{2}\}$$

y su discriminante es $\Delta = 64mnk$.

Demostración. Veamos que todo elemento de $\mathfrak{O}_K$ se puede expresar de la forma

$$\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}$$

con a, b, c, $d \in \mathbb{Z}$.

Como $\{1,\, \sqrt{m},\, \sqrt{n},\, \sqrt{k}\}$ es una $\mathbb{Q}$-base de K, cada elemento de K se expresa de forma única como

$$\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \qquad \text{con } a,\, b,\, c,\, d \in \mathbb{Q}$$

Ahora, si suponemos que $\alpha \in \mathfrak{O}_K$, por el Teorema 2.10, se tiene

$$T^K_{\mathbb{Q}(\sqrt{m})}(\alpha) = 2a + 2b\sqrt{m} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\sqrt{m}] \quad \text{luego} \quad 2a,\, 2b \in \mathbb{Z},$$

$$T^K_{\mathbb{Q}(\sqrt{n})}(\alpha) = 2a + 2c\sqrt{n} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}] \quad \text{luego} \quad 2c \in \mathbb{Z},$$

$$T^K_{\mathbb{Q}(\sqrt{k})}(\alpha) = 2a + 2d\sqrt{k} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{k})} = \mathbb{Z}[\sqrt{k}] \quad \text{luego} \quad 2d \in \mathbb{Z},$$

y así

$$a = \frac{a'}{2} \qquad b = \frac{b'}{2} \qquad c = \frac{c'}{2} \qquad d = \frac{d'}{2}$$

con a', b', c', $d' \in \mathbb{Z}$. Y α se expresa de la forma indicada. Calculando la norma sobre uno de los cuerpos intermedios

$$N^K_{\mathbb{Q}(\sqrt{m})}(\alpha) = \left(\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}\right)\left(\frac{a + b\sqrt{m} - c\sqrt{n} - d\sqrt{k}}{2}\right)$$

$$= \frac{a^2 + b^2m - c^2n - d^2k}{4} + \frac{2ab - 2cd\frac{n}{m.c.d(m,\,n)}}{4}\sqrt{m} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\sqrt{m}],$$

por lo que

$$a^2 + 3b^2 - 2c^2 - 2d^2 \equiv 0\,(\text{mód}\,4), \tag{1}$$

$$ab + cd\frac{n}{m.c.d(m,\,n)} \equiv 0\,(\text{mód}\,2). \tag{2}$$

Como n es par y m es impar, $m.c.d(m,\,n)$ es impar y $n/m.c.d(m,\,n)$ es par. Por lo que (2) es equivalente a $ab \equiv 0\,(mód\,2)$ que se da si y sólo si a o b es par. Pero si alguno de los dos es par, supongamos por ejemplo que es a, entonces (1) se transforma en

$$3b^2 - 2c^2 - 2d^2 \equiv 0\,(\text{mód}\,4), \quad \text{equivalente a} \quad b^2 \equiv 0\,(\text{mód}\,2)$$

es decir, b es par. El otro caso (b par) se resuelve análogamente y se tiene que a y b son pares. Esto nos lleva a que la fórmula (1) queda finalmente de la forma

$$2c^2 \equiv -2d^2\,(\text{mód}\,4), \quad \text{que es equivalente a} \quad c \equiv d\,(\text{mód}\,2).$$

Se tiene entonces que

$$\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{m} + \left(\frac{c-d}{2}\right)\sqrt{n} + d(\frac{\sqrt{n}+\sqrt{k}}{2})$$

y, por tanto, $\{1,\, \sqrt{m},\, \sqrt{n},\, \frac{\sqrt{n}+\sqrt{k}}{2}\}$ es una base entera de $\mathfrak{O}_K$. □

Teorema 2.13. *Si $m \equiv 1\,(mód\ 4)$ y $n \equiv k \equiv 2, 3\,(mód\ 4)$. Entonces todo elemento de $\mathfrak{O}_K$ se puede expresar de la forma*

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2} \text{ con } a,\, b,\, c,\, d \in \mathbb{Z}\ ,\ \ a \equiv b\,(mód 2) \text{ y } c \equiv d\,(mód 2),$$

una base entera para $\mathfrak{O}_K$ viene dada por

$$\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\}$$

y su discriminante es $\Delta = 16mnk$.

Demostración. Haremos el mismo procedimiento que en el anterior teorema tomando un elemento $\alpha \in \mathfrak{O}_K$ de la forma $\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}$ con $a, b, c, d \in \mathbb{Q}$.

$$T^K_{\mathbb{Q}(\sqrt{n})}(\alpha) = 2(a + c\sqrt{n}) \in \mathfrak{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}] \quad \text{luego} \quad a = \frac{a'}{2},\, c = \frac{c'}{2} \quad \text{con} \;\; a', b' \in \mathbb{Z},$$

$$T^K_{\mathbb{Q}(\sqrt{k})}(\alpha) = 2(a + d\sqrt{k}) \in \mathfrak{O}_{\mathbb{Q}(\sqrt{k})} = \mathbb{Z}[\sqrt{m}] \quad \text{luego} \quad d = \frac{d'}{2} \quad \text{con} \;\; d' \in \mathbb{Z},$$

$$T^K_{\mathbb{Q}(\sqrt{m})}(\alpha) = 2(a + b\sqrt{m}) \in \mathfrak{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \;\text{ luego} \quad 2a + 2b\sqrt{m} = \frac{x + y\sqrt{m}}{2} \quad \text{con } x, y \in \mathbb{Z},$$

$x \equiv y \,(\text{mód}\, 2)$, pero entonces $2a = a' = \frac{x}{2} \in \mathbb{Z}$; es decir, x es par, lo que implica que y es par y $2b = \frac{y}{2} \in \mathbb{Z}$, $b = \frac{b'}{2}$ con $b' \in \mathbb{Z}$. Ahora, calculando la norma sobre uno de los cuerpos intermedios, si $l = m.c.d(m,\, n)$, se tiene

$$N^K_{\mathbb{Q}(\sqrt{n})}(\alpha) = \frac{a^2 - b^2 m + c^2 n - d^2 k}{4} + \frac{ac - bd\frac{m}{l}}{2}\sqrt{n} \in \mathfrak{O}_{Q(\sqrt{n})} = \mathbb{Z}[\sqrt{n}]\ .$$

Y estudiamos los distintos casos.

(1) Si $n \equiv \; k \equiv 2 \,(\text{mód}\, 4)$ entonces

$$a^2 - b^2 \equiv 2d^2 - 2c^2 \,(\text{mód}\, 4) \Rightarrow a^2 - b^2 \equiv 0 \,(\text{mód}\, 2) \Rightarrow (a+b)(a-b) \equiv 0 \,(\text{mód}\, 2) \Rightarrow a \equiv b \,(\text{mód}\, 2)$$

y como $a^2 - b^2 \equiv 0 \,(\text{mód}\, 4)$

$$2c^2 - 2d^2 \equiv 0 \,(\text{mód}\, 4) \Rightarrow c^2 - d^2 \equiv 0 \,(\text{mód}\, 2) \Rightarrow c \equiv d \,(\text{mód}\, 2).$$

(2) si $n \equiv k \equiv 3 \,(\text{mód}\, 4)$ (por definición de k esta es la última de las posibilidades), nos apoyamos también en la norma sobre $\mathbb{Q}(\sqrt{k})$

$$N^K_{\mathbb{Q}(\sqrt{k})}(\alpha) = \frac{a^2 - b^2 m - c^2 n + d^2 k}{4} + \frac{ad - bcl}{2}\sqrt{k} \in \mathfrak{O}_{Q(\sqrt{k})} = \mathbb{Z}[\sqrt{k}]\ .$$

de donde

$$a^2 - b^2 + c^2 - d^2 \equiv 0 \,(\text{mód}\, 4)$$

y sumando con la congruencia obtenida con la norma sobre $\mathbb{Q}(\sqrt{n})$ que es $a^2 - b^2 - c^2 + d^2 \equiv 0 \,(\text{mód}\, 4)$ nos queda

$$2a^2 - 2b^2 \equiv 0 \,(\text{mód}\, 4) \Rightarrow a^2 - b^2 \equiv 0 \,(\text{mód}\, 2) \Rightarrow a \equiv b \,(\text{mód}\, 2)$$

y si en vez de sumar, ahora restamos las congruencias

$$-2c^2 + 2d^2 \equiv 0 \,(\text{mód}\, 4) \Rightarrow c \equiv d \,(\text{mód}\, 2).$$

Y una vez visto esto, podemos poner α de la forma

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

y por tanto $\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\}$ es una base entera de K. □

Teorema 2.14. *Si $m \equiv n \equiv k \equiv 1 \,(mód\, 4)$, entonces una base entera para $\mathfrak{O}_K$ viene dada por*

$$\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\}$$

y su discriminante es $\Delta = mnk$.

Demostración. Como siempre, tenemos $\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}$, y nos apoyamos en las trazas sobre los distintos cuerpos intermedios

$$T^K_{\mathbb{Q}(\sqrt{m})}(\alpha) = 2(a+b\sqrt{m}) = \frac{a' + b'\sqrt{m}}{2} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \quad \text{luego} \quad a = \frac{a'}{4}, b = \frac{b'}{2}, \quad \text{con} \quad a', b' \in \mathbb{Z},$$

$$T^K_{\mathbb{Q}(\sqrt{n})}(\alpha) = 2(a + c\sqrt{n}) = \frac{a' + c'\sqrt{n}}{2} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\frac{1+\sqrt{n}}{2}] \quad \text{luego} \quad b = \frac{b'}{4}, \quad \text{con} \quad b' \in \mathbb{Z},$$

$$T^K_{\mathbb{Q}(\sqrt{k})}(\alpha) = 2(a + d\sqrt{k}) = \frac{a' + d'\sqrt{k}}{2} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{k})} = \mathbb{Z}[\frac{1+\sqrt{k}}{2}] \quad \text{luego} \quad d = \frac{b'}{4}, \quad \text{con} \quad d' \in \mathbb{Z},$$

además se tiene $a' \equiv b' \equiv c' \equiv d' \,(\text{mód}\, 2)$. Y entonces podemos expresar cada elemento de $\mathfrak{O}_K$ de la forma

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{4} \quad \text{con} \quad a, b, c, d \in \mathbb{Z} \quad a \equiv b \equiv c \equiv d \,(\text{mód}\, 2).$$

Dicho elemento es entero algebraico si y sólo si lo es el siguiente (por restarle un múltiplo entero de un entero algebraico)

$$\alpha - d\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right) = \frac{(a-d) + (b-d)\sqrt{m} + (c - d\frac{m}{l})\sqrt{n}}{4} = \frac{r + s\sqrt{m} + t\sqrt{n}}{2} = \beta$$

con $r, s, t \in \mathbb{Z}$. Donde la última igualdad es posible al tener que $a \equiv b \equiv c \equiv d \,(\text{mód}\, 2)$. Si ahora calculamos la norma sobre $\mathbb{Q}(\sqrt{m})$ a β

$$N^K_{\mathbb{Q}(\sqrt{m})}(\beta) = \frac{r^2 + s^2 m - t^2 n}{4} + \frac{sr}{2}\sqrt{m} \in \mathfrak{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\frac{1+\sqrt{m}}{2}],$$

luego ha de tenerse $r^2 + s^2 + t^2 \equiv 0 \,(\text{mód}\, 2)$ o equivalentemente $r + s + t \equiv 0 \,(\text{mód}\, 2)$. Entonces todo elemento de $\mathfrak{O}_K$ puede ponerse de la forma (siguiendo la notación del teorema)

$$\alpha = \left(\frac{a - b - c + d\frac{m}{l}}{4}\right) + \frac{b-d}{2}\left(\frac{1+\sqrt{m}}{2}\right) + \frac{c-d}{2}\left(\frac{1+\sqrt{n}}{2}\right) + d\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)$$

y la del enunciado es una base entera para $\mathfrak{O}_K$. □

2.4. Extensiones cúbicas puras

Consideremos, ahora, el caso de una extensión cúbica pura, es decir, aquellas de la forma $K = \mathbb{Q}(\alpha)$, con $\alpha = \sqrt[3]{m}$ donde m es 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 $m = hk^2$, con h, $k \in \mathbb{Z}$, $m.c.d(h, k) = 1$ y libres de cuadrados. En estas condiciones se tiene el siguiente resultado:

Teorema 2.15. *Sea $K = \mathbb{Q}(\alpha)$ la extensión cúbica en las condiciones anteriores, entonces el anillo $R = \mathfrak{O}_K$ de enteros algebraicos de K tiene una base entera de la forma*

$$\mathcal{B} = \begin{cases} \{1, \alpha, \dfrac{\alpha^2}{k}\} \ \textit{si } m \not\equiv \pm 1 \ (\ \textit{mód } 9) \\ \{1, \alpha, \dfrac{\alpha^2 + k^2\alpha + k^2}{3k}\} \ \textit{si } m \equiv 1 \ (\ \textit{mód } 9) \\ \{1, \alpha, \dfrac{\alpha^2 - k^2\alpha + k^2}{3k}\} \ \textit{si } m \equiv -1 \ (\ \textit{mód } 9) \end{cases}$$

Demostración. Por el teorema de la base entera especial, sabemos que R tiene una base entera de la forma

$$\{1, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}\}$$

con cada $f_i \in \mathbb{Z}[t]$ 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

$$(d_1 d_2)^2 | \Delta(\alpha) = -27\, m^2 = (-1)\, 3^3\, h^2\, k^4,$$

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

Por otro lado, si $d_1 = 3$ y $f_1(t) = t + a \in \mathbb{Z}[t]$, se tendría que $\beta = \dfrac{\alpha + a}{3} \in R$, por lo que $\beta^3 \in R$ y $T(\beta^3) \in \mathbb{Z}$; pero

$$T(\beta^3) = \frac{1}{27}(T(\alpha^3 + 3a\alpha^2 + 3a^2\alpha + a^3)) = \frac{1}{27}(T(m) + 3aT(\alpha^2) + 3a^2T(\alpha) + T(a^3))$$

y, como $T(\alpha) = 0$ y $T(\alpha^2) = 0$, se tiene que

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

pero como en este caso $9|m$, resulta que $9|a^3$ y, por tanto $3|a$ por lo que se tendría que

$$\frac{\alpha}{3} = \beta - \frac{a}{3} \in R$$

que no puede ser ya que $Irr\left(\dfrac{\alpha}{3}, \mathbb{Q}\right) = t^3 - \dfrac{m}{27} \notin \mathbb{Z}[t]$.

En resumen, se ha demostrado que, en cualquier caso, $d_1 = 1$ y, por las observaciones posteriores al teorema de la base entera especial, se puede considerar $f_1(t) = t$; por lo que el segundo término de la base entera puede ser, 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.

$Irr\left(\dfrac{\alpha^2}{k}, \mathbb{Q}\right) = t^3 - h^2k \in \mathbb{Z}[t]$, por lo que, en general, $\dfrac{\alpha^2}{k} \in R$ y, por consiguiente, $k|d_2$.

Además, si $m \equiv 1$ (mód 9), es fácil comprobar que

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

por lo que

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

y, por tanto, $3k|d_2$.

De forma análoga, si $m \equiv -1$ (mód 9), considerando ahora el elemento $\dfrac{(\alpha+1)^2}{3}$, se puede comprobar que

$$\frac{\alpha^2 - k^2\alpha + k^2}{3k} \in R$$

y, por tanto, también en este caso, $3k|d_2$.

Para terminar la demostración bastará probar que $d_2 = k$ cuando $m \not\equiv \pm 1$ (mód 9) y que $d_2 = 3k$ cuando $m \equiv \pm 1$ (mód 9). Como se sabe que, en general, $k|d_2$ y que si $m \equiv \pm 1$ (mód 9) se tiene que $3k|d_2$; para probar dichas afirmaciones bastará demostrar que d_2 no puede ser, en cada caso, mayor que dichos valores.

Supongamos a partir de ahora que $f_2(t) = t^2 + at + b$ con $a, b \in \mathbb{Z}$.

Como $d_2^2|27\,m^2 = 3^3\,m^2$ y m es libre de cubos, $d_2|3m$ y 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 $p \neq 3$ con $p|m$ y supongamos que $p \not| k$ ($p^2 \not| m$), veamos que $p \not| d_2$.

Si $p|d_2$, entonces

$$\frac{\alpha^2 + a\alpha + b}{p} = \frac{d_2}{p}\frac{\alpha^2 + a\alpha + b}{d_2} \in R$$

por lo que $\dfrac{3b}{p} = T(\frac{\alpha^2+a\alpha+b}{p}) \in \mathbb{Z}$ y, por tanto, $p|b$; pero entonces,

$$\frac{\alpha^2 + a\alpha}{p} = \frac{\alpha^2 + a\alpha + b}{p} - \frac{b}{p} \in R$$

y, por consiguiente, $\left(\dfrac{\alpha^2 + a\alpha}{p}\right)^3 \in R$, de donde $T\left(\left(\dfrac{\alpha^2 + a\alpha}{p}\right)^3\right) \in \mathbb{Z}$; pero como

$$\left(\frac{\alpha^2 + a\alpha}{p}\right)^3 = \frac{1}{p^3}(\alpha^3(\alpha+a)^3) = \frac{1}{p^3}(m(\alpha^3 + 3a\alpha^2 + 3a^2\alpha + a^3)) =$$

$$= \frac{m}{p^3}(3a\alpha^2 + 3a^2\alpha + (m + a^3)),$$

$T\left(\left(\dfrac{\alpha^2 + a\alpha}{p}\right)^3\right) = \dfrac{m}{p^3}(3(m + a^3))$ y, por tanto, $p^3|3m(m + a^3)$ y, como $p^2 \not| m$, $p^2|m + a^3$, por lo que $p|a$, en cuyo caso,

$$\frac{\alpha^2}{p} = \frac{\alpha^2 + a\alpha}{p} - \frac{a\alpha}{p} \in R$$

lo cual no puede darse pues

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

Los únicos factores primos distintos de 3 que dividen a d_2 son los que dividen a k. Si p es uno de ellos, como k es libre de cuadrados, $p^2\not| k$ y, de forma similar a la anterior, se puede demostrar que también se tiene que $p^2\not| d_2$.

Si $p^2|d_2$, entonces

$$\frac{\alpha^2+a\alpha+b}{p^2}=\frac{d_2}{p^2}\frac{\alpha^2+a\alpha+b}{d_2}\in R$$

por lo que $\frac{3b}{p^2}=T(\frac{\alpha^2+a\alpha+b}{p^2})\in\mathbb{Z}$ y, por tanto, $p^2|b$; pero entonces tenemos que, $\left(\frac{\alpha^2+a\alpha}{p^2}\right)\in R$ y $T\left(\left(\frac{\alpha^2+a\alpha}{p}\right)^3\right)\in\mathbb{Z}$ y utilizando, como en el caso anterior, la traza se tendría que $p^6|3m(m+a^3)$ y, como $p^3\not| m$, resulta que $p^4|m+a^3$; pero, como en este caso $p^2|m$ se tiene que $p^2|a^3$, $p|a$, $p^3|a^3$ y, por tanto, $p^3|m$ que no puede ser.

Para terminar, bastará considerar las potencias de 3 que dividen a d_2.

Si $3\not| m$, como $d_2|3m$, $9\not| d_2$; por lo que para $m\equiv\pm1$ (mód 9) se ha completado el resultado ya que, en ambos casos, se tenía que $3k|d_2$.

Para el resto de los casos a considerar haremos uso de que, como

$$\left(\frac{f_2(\alpha)}{d_2}\right)^2\in R=\mathbb{Z}1\oplus\mathbb{Z}\alpha\oplus\mathbb{Z}\frac{f_2(\alpha)}{d_2}$$

y

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

se tiene que $d_2|a^2+2b$, $m+2ab$, $2am+b^2$.

Supongamos ahora que $3\not| m$ y $m\not\equiv\pm1$ (mód 9), veamos que $3\not| d_2$.

Si $3|d_2$, $2ab\equiv-m\not\equiv0$(mód 3) por lo que $1\equiv a^2\equiv-2b\equiv b\equiv1$(mód 3) y, por tanto, $a\equiv-2a\equiv-2ab\equiv m$(mód 3) y, por otro lado

$$\frac{(\alpha^2+a\alpha+b)}{3}=\frac{d_2}{3}\frac{(\alpha^2+a\alpha+b)}{d_2}\in R$$

por lo que

$$\frac{(\alpha^2+m\alpha+1)}{3}=\frac{(\alpha^2+a\alpha+b)}{3}-r\alpha-s\in R.$$

En cuyo caso, si $m\equiv a\equiv-2$(mód 3), entonces

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

y elevando a la cuarta potencia y tomando trazas se llega a que $3^2|m-1$ y $m\equiv1$(mód 9) que no puede ser.

Si, por el contrario, $m \equiv a \equiv 2(\text{ mód } 3)$

$$\frac{(\alpha+1)^2}{3} = \frac{\alpha^2+2\alpha+1}{3} = \frac{\alpha^2+a\alpha+1}{3} + t \in R$$

y elevando, también en este caso, a la cuarta potencia y tomando trazas se llega a que $3^2|m+1$ y $m \equiv -1(\text{ mód } 9)$ que tampoco puede ser.

Supongamos, ahora, que $3 \not| k$ ($9 \not| m$) y veamos que $3 \not| d_2$. Si $3|d_2$, se tiene que $3|a^2+2b$, $m+2ab$, b^2+2am, por lo $3|a^2+2b$, $2ab$, b^2, de donde $3|a,b$ por lo que

$$\frac{\alpha^2}{3} = \frac{\alpha^2+a\alpha+b}{3} - \frac{a}{3}\alpha - \frac{b}{3} \in R$$

que no es cierto ya que $Irr\left(\frac{\alpha^2}{3}, \mathbb{Q}\right) = t^3 - \frac{m^2}{3^3} \notin \mathbb{Z}[t]$ pues $9 \not| m$.

Por último, si $3|k$ ($9|m$) y suponemos $9|d_2$, se tendría que $9|a^2+2b$, $m+2ab$, b^2+2am, por lo $9|a^2+2b$, $2ab$, b^2, de donde $9|b^2$, a^2, $2b$ y $9|b$, por lo que

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

y, por tanto,

$$(\frac{\alpha^2+a\alpha}{9})^3 \in R$$

lo que, al tomar trazas, lleva a que $3^3|m$ que es imposible.

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

Tema 3

Factorización en irreducibles

En este capítulo vamos a dar las definiciones de elemento irreducible y primo. Asimismo veremos cuando es posible la factorización en irreducibles y por último estudiar cuando dicha factorización es única. Todo esto, será posteriormente utilizado para demostrar cuándo el anillo de enteros de un cuerpo de números tiene factorización única en irreducibles.

3.1. Introducción a la irreducibilidad

Proposición 3.1. *El conjunto formado por las unidades $U(R)$ de un anillo R es un grupo con la multiplicación.*

Es fácil de ver que $U(\mathbb{Q}) = \mathbb{Q}\setminus\{0\}$ que $U(\mathbb{Z}) = \pm 1$, y tomando normas se puede ver que si $R{=}\ \mathbb{Z}[i]$ que las unidades son $\{1, -1, i, -i\}$.

Dos elementos a y b de un dominio D se dicen *asociados* si existe una unidad $u \in D$ tal que $b = ua$.

Un elemento p, no nulo ni unidad, de un dominio D se dirá *primo* si $p|ab$ implica que $p|a$ o $p|b$.

Con este concepto puede haber alguna confusión, pues la definición usual de número primo es que no se pueda expresar como producto de dos elementos sin que uno de ellos fuera unidad. En $\mathbb{Z}$ ambos conceptos coinciden, pero esto no se da en general. Esta última condición corresponde a otro concepto, el de elemento irreducible.

Un elemento b, no nulo ni unidad, de un dominio D se dice que es *irreducible* si $b = cd$ implica que c o d es unidad. Un elemento que no es irreducible diremos que es *reducible*.

Todo elemento reducible admite una factorización de la forma $x = ab$ con a y b no unidades. Si alguno de los elementos que aparecen en dicha factorización son reducibles, podemos seguir avanzando en la factorización escribiendo

$$x = a_1 a_2 \cdots a_n$$

donde esperamos que los factores en algún momento lleguen a ser irreducibles y el proceso finalice; pero hay que tener en cuenta que esta factorización no tiene porqué ser un proceso finito, nada nos asegura el que nos aparezcan continuamente elementos reducibles.

Proposición 3.2. *Para un dominio D se verifican las siguientes propiedades,*

(a) x es unidad si y sólo si $x \mid 1$,

(b) cualesquiera dos unidades son asociadas y cualquier asociado a una unidad es una unidad,

(c) x, y son asociados si y sólo si $x \mid y$ e $y \mid x$,

(d) x es irreducible si y sólo si todo divisor de x es un asociado de x o una unidad,

(e) un asociado de un irreducible es irreducible.

Proposición 3.3. *Sea D un dominio, x e y elementos no nulos de D, entonces*

(a) $x|y$ si y sólo si $\langle y\rangle \subseteq \langle x\rangle$,

(b) x e y son asociados si y sólo si $\langle x\rangle = \langle y\rangle$,

(c) x es unidad si y sólo si $\langle x\rangle = D$,

(d) x es irreducible si y sólo si $\langle x\rangle$ es maximal entre los ideales principales propios de D.

Demostración. (a) Si $x|y$ entonces $y = xc$ para algún $c \in D$ y entonces $y \in \langle x\rangle$ y entonces $\langle y\rangle \subseteq \langle x\rangle$. Recíprocamente, si $\langle y\rangle \subseteq \langle x\rangle$ entonces $y = xc$ para algún $c \in D$. (b) es inmediato a partir de (a). (c) es trivial. (d) Supongamos que x es irreducible, con $\langle x\rangle \subsetneqq \langle y\rangle \subsetneqq D$. Entonces $y|x$, pero no es ni unidad ni un asociado de x, contradiciendo la proposición 3.2(d). Recíprocamente si tal y no existe entonces todo divisor de x es o unidad o un asociado, así que x es irreducible. □

3.2. Factorización en irreducibles

Como habíamos indicado anteriormente, un elemento se dice reducible, si lo podemos expresar como producto de dos no unidades. Y siguiendo con el procedimiento de descomposición esperamos encontrar una factorización en elementos irreducibles. Decimos que *la factorización en irreducibles* es *posible* en D, si todo $0 \neq x \in D$ no unidad es producto de un número finito de irreducibles. En general esto no es posible. Por ejemplo, sea $\mathcal{B}$ el anillo formado por los enteros algebraicos de $\mathbb{C}$. Si $\alpha \in \mathcal{B}$ es no nulo y no unidad entonces α es reducible, pues $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ y α es un entero algebraico, además $\sqrt{\alpha}$ no es unidad y esto muestra que no hay irreducibles en B. Esta es la razón de tomar cuerpos de números para estudiar la factorización única, ya que la clave de poder factorizar está en que la extensión sobre el cuerpo de los racionales sea finita.

Definición 3.4. *Un dominio D se dirá noetheriano si todo ideal de D es finitamente generado.*

Condición de la cadena ascendente. Diremos que un dominio D satisface la condición de la cadena ascendente para cada cadena de ideales de D

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

existe algún N tal que $I_n = I_N$ para todo $n \geq N$.

Condición maximal. Diremos que un dominio D satisface la condición maximal si todo conjunto no vacío de ideales de D tiene un elemento maximal, que es un elemento no contenido propiamente en ningún ideal de dicho conjunto.

A partir del Axioma de Elección se puede demostrar el siguiente resultado:

Proposición 3.5. *Las siguientes condiciones son equivalentes para un dominio integral D:*

(a) D es noetheriano,

(b) D satisface la condición de la cadena ascendente,

(c) D satisface la condición maximal.

Teorema 3.6. *Si D es un dominio noetheriano, entonces la factorización en irreducibles es posible en D.*

Demostración. Supongamos que D es noetheriano, pero que existe un $x \neq 0$ no unidad en D que no puede ser expresado como producto de un número finito de irreducibles. Elegimos x tal que $\langle x \rangle$ es maximal entre los que cumplen esa condición, que es posible por la condición de maximalidad en conjuntos no vacíos. Por definición x no puede ser irreducible, así que $x = ab$ donde a y b son no unidades. Entonces $\langle x \rangle \subseteq \langle a \rangle$ por la proposición 3.3 (a). Si $\langle x \rangle = \langle a \rangle$ entonces x y a son asociados por la proposición 3.3(b) y esto no puede ser por que implicaría que c es unidad. Así que $\langle x \rangle \subsetneq \langle a \rangle$, y por lo mismo $\langle x \rangle \subseteq \langle b \rangle$. Por la maximalidad de $\langle x \rangle$ se debe tener

$$a = p_1 \cdots p_r$$
$$b = q_1 \cdots q_s$$

donde cada p_i y q_i son irreducibles. Multiplicando las anteriores expresiones, expresamos a x como producto finito de irreducibles, lo que contradice que existan elementos no nulos y no unidades que no se expresen como producto de un número finito de irreducibles. □

Teorema 3.7. *El anillo de enteros $\mathfrak{O}$ de un cuerpo de números K es noetheriano.*

Demostración. Probaremos que todo ideal I de $\mathfrak{O}$ es finitamente generado. Como $(\mathfrak{O}, +)$ es libre abeliano de rango n igual al grado de K por el teorema 1.25. Por lo tanto $(I, +)$ es libre abeliano de rango $s \leq n$ ([5] Teorema 1.16, pág. 28). Si $\{x_1, \ldots, x_s\}$ es una $\mathbb{Z}$-base de $(I, +)$, entonces claramente $\langle x_1, \ldots x_s \rangle = I$. Así que I es finitamente generado y $\mathfrak{O}$ es noetheriano. □

Corolario 3.8. *La factorización en irreducibles es posible en el anillo de enteros de un cuerpo de números.*

Proposición 3.9. *Sea $\mathfrak{O}$ el anillo de enteros de un cuerpo de números K, y sean $x, y \in \mathfrak{O}$. Entonces:*

(a) x es unidad si y sólo si $N(x) = \pm 1$,

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

(c) si N(x) es un número entero primo, entonces x es irreducible en $\mathfrak{O}$.

3.3. Ejemplos de factorización no única en irreducibles

Definición 3.10. *Diremos que la factorización en un dominio D es única, y se llamará a D* ***dominio de factorización única (DFU)*** *si siempre que tengamos*

$$p_1 \cdots p_r = q_1 \cdots q_s$$

donde los p_i y q_i son irreducibles en D, se tiene que

(a) $r = s$,

(b) existe una permutación π de $\{1, \ldots, r\}$ tal que p_i y $q_{\pi(i)}$ son asociados para todo $i = 1, \ldots, r$.

Teorema 3.11. *La factorización en irreducibles no es única en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ para al menos los siguientes valores de d:-5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30.*

Demostración. En $\mathbb{Q}(\sqrt{-6})$ tenemos las factorizaciones

$$6 = 2 \cdot 3 = (\sqrt{-6})(-\sqrt{-6})$$

Vamos a ver que $2, 3, \sqrt{-6}$ y $-\sqrt{-6}$ son irreducibles en $\mathfrak{O}_{\mathbb{Q}(\sqrt{-6})}$. En este anillo de enteros, la norma de un elemento $\alpha = a + b\sqrt{-6}$ viene dada por

$$N(\alpha) = a^2 + 6b^2,$$

por lo que se puede ver fácilmente que no hay elementos de norma 2 o 3. Siguiendo con la propiedad de la norma, tenemos que $4 = N(2) = N(x)N(y)$ lo que implica que x o y es unidad, por tanto 2 irreducible (porque no hay elementos de norma 2). Análogamente pasa con $3, \sqrt{-6}$ y $-\sqrt{-6}$. Sin embargo ni 2 ni 3 son asociados a ninguno de los $\sqrt{-6}$ ó $-\sqrt{-6}$, ya que $2(c + d\sqrt{-6}) = 2c + 2d\sqrt{-6}$ con $c, d \in \mathbb{Z}$. Por lo que la factorización no es única en dicho anillo de enteros. Se pueden comprobar para los distintos valores de d lo que propone el teorema. Aquí simplemente se deja el ejemplo que demuestra lo dicho:

$$\begin{array}{rcrcrcl}
\mathbb{Q}(\sqrt{-5}) & : & 6 & = & 2 \cdot 3 & = & (1+\sqrt{-5}) \cdot (1-\sqrt{-5}) \\
\mathbb{Q}(\sqrt{-10}) & : & 14 & = & 2 \cdot 7 & = & (2+\sqrt{-10}) \cdot (2-\sqrt{-10}) \\
\mathbb{Q}(\sqrt{-13}) & : & 14 & = & 2 \cdot 7 & = & (1+\sqrt{-13}) \cdot (1-\sqrt{-13}) \\
\mathbb{Q}(\sqrt{-14}) & : & 15 & = & 3 \cdot 5 & = & (1+\sqrt{-14}) \cdot (1-\sqrt{-14}) \\
\mathbb{Q}(\sqrt{-15}) & : & 4 & = & 2 \cdot 2 & = & (\frac{1+\sqrt{-15}}{2}) \cdot (\frac{1-\sqrt{-15}}{2}) \\
\mathbb{Q}(\sqrt{-17}) & : & 18 & = & 2 \cdot 3 \cdot 3 & = & (1+\sqrt{-17}) \cdot (1-\sqrt{-17}) \\
\mathbb{Q}(\sqrt{-21}) & : & 22 & = & 2 \cdot 11 & = & (1+\sqrt{-21}) \cdot (1-\sqrt{-21}) \\
\mathbb{Q}(\sqrt{-22}) & : & 26 & = & 2 \cdot 13 & = & (2+\sqrt{-22}) \cdot (2-\sqrt{-22}) \\
\mathbb{Q}(\sqrt{-23}) & : & 6 & = & 2 \cdot 3 & = & (\frac{1+\sqrt{-23}}{2}) \cdot (\frac{1-\sqrt{-23}}{2}) \\
\mathbb{Q}(\sqrt{-26}) & : & 27 & = & 3 \cdot 3 \cdot 3 & = & (1+\sqrt{-26}) \cdot (1-\sqrt{-26}) \\
\mathbb{Q}(\sqrt{-29}) & : & 30 & = & 2 \cdot 3 \cdot 5 & = & (1+\sqrt{-29}) \cdot (1-\sqrt{-29}) \\
\mathbb{Q}(\sqrt{-30}) & : & 34 & = & 2 \cdot 17 & = & (2+\sqrt{-30}) \cdot (2-\sqrt{-30})
\end{array}$$

□

3.4. Factorización prima

Hemos notado ya que un irreducible en $\mathbb{Z}$ satisface la condición adicional

$$p|mn \quad \text{implica} \quad p|m \text{ o } p|n.$$

En esta sección vamos a demostrar que esa propiedad caracteriza la factorización única. Recordemos que la definición de primo es exactamente la anterior.

Proposición 3.12. *Los primos en un dominio D son irreducibles.*

Demostración. Supongamos que D es un dominio, $x \in D$ es primo, y $x = ab$. Entonces $x|ab$ por lo que $x|a$ o $x|b$, podemos suponer sin pérdida de generalidad que $p|a$, entonces existe un elemento $c \in D$ tal que $a = xc$, entonces

$$x = ab = xcb$$

y entonces cancelando

$$1 = cb$$

y b es unidad. De la misma manera, si $x|b$ entonces a es unidad. □

El recíproco de lo que dice la proposición no es cierto, como hemos podido ver en todos los anteriores casos donde no había factorización única.

Teorema 3.13. *En un dominio D en el cual la factorización única es posible, la factorización en irreducibles es única si y sólo si todo irreducible es primo.*

Demostración. Sea D un dominio, y tomemos un elemento $x \in D$ que por hipótesis es factorizable en un número finito de irreducibles

$$x = up_1 \cdots p_r$$

donde u es unidad y $p_1 \cdots p_r$ son irreducibles. Cuando $r = 0$ entonces $x = u$ es unidad y si $r \geq 1$ entonces up_1 es irreducible, así que x es producto de los irreducibles $up_1, p_2, \ldots, p_r$.
Supongamos ahora que la factorización es única y p es un irreducible y lo que debemos a probar es que p es primo.

$$\text{Si } p|ab, \text{ entonces } pc = ab \ (c \in D).$$

Necesitamos considerar solo los casos donde $a \neq 0$, $b \neq 0$ lo que implica que $c \neq 0$ también.
Factorizamos a, b, c en irreducibles:

$$\begin{aligned} a &= u_1 p_1 \cdots p_r \\ b &= u_2 q_1 \cdots q_m \\ c &= u_3 r_1 \cdots r_s \end{aligned}$$

donde cada u_i es unidad y p_i, q_i y r_i son irreducibles. Entonces

$$p(u_3 r_1 \cdots r_s) = (u_1 p_1 \cdots p_r)(u_2 q_1 \cdots q_m),$$

y la factorización única implica que p es un asociado (y por lo tanto divide) a uno de los p_i o q_j así que divide a o b. Y por lo tanto p es primo.

Recíprocamente, supongamos que todo irreducible es primo. Demostraremos que si

$$u_1 p_1 \cdots p_m = u_2 q_1 \cdots q_n \tag{1}$$

donde u_1, u_2 son unidades y p_i, q_k son irreducibles, entonces $m = n$ y existe una permutación π de $\{1, \ldots, m\}$ tal que p_i y $q_{\pi(i)}$ son asociados para todo $i = 1, \ldots m$.
Si $m = 0$ esto se cumple trivialmente. Para $m \geq 1$ si se tiene (1), entonces $p_m | u_2 q_1 \cdots q_n$. Pero p_m es primo así que (por inducción en n), $p_m | u_2$ o $p_m | q_j$ para algún j. La primera de las posibilidades implicaría que p_m es unidad, así que se tiene que $p_m | q_j$. Podemos renumerar si hiciese falta y suponer que $p_m | q_n$, entonces $q_n = p_m u$ donde u es unidad. Así que

$$u_1 p_1 \cdots p_m = u_2 q_1 \cdots u p_m$$

y cancelando p_m,

$$u_1 p_1 \cdots p_{m-1} = (u_2 u) q_1 \cdots q_{n-1}.$$

Por inducción tenemos que $m-1 = n-1$ y hay una permutación de $\{1, \ldots, m-1\}$ tal que p_i, $q_{\pi(i)}$ son asociados ($1 \leq i \leq m-1$). Esa permutación la podemos extender a $\{1, \ldots, m\}$ definiendo $\pi(m) = m$ que nos da el resultado. □

De manera seguida, con la factorización única podemos generalizar conceptos como el de máximo común divisor y mínimo común múltiplo. Si a, $b \in D$ entonces el máximo común múltiplo de a y b se define como el único elemento salvo asociados, que cumple

(i) $h|a$ y $h|b$,

(ii) si $h'|a$, $h'|b$ entonces $h'|h$.

Si $a, b \neq 0$ en un dominio de factorización única, y sus factorizaciones en irreducibles son

$$\begin{aligned} a &= u_1 p_1^{e_1} \cdots p_n^{e_n} \\ b &= u_2 p_1^{f_1} \cdots p_n^{f_n} \end{aligned}$$

donde u_1, u_2 son unidades y los p_i son todos distintos y no asociados, entonces si $m_i = min\{e_i, f_i\}$ se tiene que el máximo común divisor de a y b viene dado por

$$h = p_1^{m_1} \cdots p_n^{m_n}$$

y equivalentemente, el mínimo común multiplo vendría con la misma expresión cambiando los valores de m_i por $m_i = max\{e_i, f_i\}$. Cabe decir que sin la factorización única no podemos garantizar la existencia del mínimo común múltiplo o del máximo común divisor.

Ahora vamos a definir un especial tipo de dominio en donde vamos a garantizar que existe la factorización única. Sea un dominio D, se dirá que el dominio es *euclídeo* si posee una función $\phi : D\backslash\{0\} \longrightarrow \mathbb{N}$, llamada *función euclídea* tal que

(i) si a, $b \in D\backslash\{0\}$ y $a|b$ entonces $\phi(a) \leq \phi(b)$,

(ii) si $a, b \in D\backslash\{0\}$ entonces existen $q, r \in D$ tal que $a = bq+r$ donde o bien $r = 0$ o bien $\phi(r) < \phi(b)$.

Por ejemplo, en $\mathbb{Z}$ la función $\phi(n) = |n|$ y en $K[t]$ $\phi(g) = \partial g$ son funciones euclídeas. Un dominio D se dice de *dominio de ideales principales* si todo ideal de D es principal, esto es generado por un solo elemento. Es decir, si $I \leq D$, entonces $I = aD = \langle a \rangle$ para algún $a \in D$.

Considerando, para cada ideal, el elemento de nulo sobre el que la función euclídea toma valor mínimo, se demuestra:

Teorema 3.14. *Todo dominio euclídeo es un dominio de ideales principales.*

Teorema 3.15. *Todo dominio de ideales principales es dominio de factorización única.*

Demostración. Sea D un dominio de ideales principales. Evidentemente esto implica que D es noetheriano, porque todos los ideales son finitamente generados, así que la factorización en irreducibles es posible en D por el teorema 3.6, así que para probar la factorización única resta ver que todo irreducible es primo. Supongamos que p es irreducible, entonces $\langle p \rangle$ es maximal entre los ideales principales de D por el teorema 3.3(d), pero todo ideal es principal por lo que $\langle p \rangle$ es maximal en D. Supongamos que $p|ab$ pero $p \not| a$. El hecho de que $p \not| a$ implica $\langle p \rangle \subsetneq \langle p, a \rangle$, y por la maximalidad de $\langle p \rangle$ implica que $\langle p, a \rangle = D$. Entonces $1 \in \langle p, a \rangle$. Así que

$$1 = cp + da \qquad (c, d \in D).$$

Multiplicando por b

$$b = cpb + dab$$

y como $p|ab$, encontramos que $p|(cap + dab)$ y entonces $p|b$. Y entonces p es primo, lo que completa la prueba. □

Teorema 3.16. *Todo dominio euclídeo es un dominio de factorización única.*

Tema 4

Ideales

En este capítulo, abordaremos la teoría de ideales en anillos de enteros de cuerpos de números, fijándonos en la factorización de elementos. Como hemos visto en el capítulo anterior, la factorización única en irreducibles no se tiene en todos los anillos de enteros de cuerpos de números, por ejemplos como $6 = 3 \cdot 2 = (\sqrt{-6}) \cdot (-\sqrt{-6})$ en $\mathbb{Z}[\sqrt{-6}]$ anillo de enteros de $\mathbb{Q}(\sqrt{-6})$ no es dominio de factorización única. Sin embargo, la genial idea de Kummer fue estudiar si hay factorización única en ideales primos, y esto se consigue en dominios de Dedekind, donde el propio Dedekind probó su veracidad, dando una definición bastante lógica de divisivilidad.

Vamos a recordar otro ejemplo de no factorización única y al final del tema vamos a ver su factorización única en ideales. Estudiamos, más adelante, el caso de $\mathbb{Z}[\sqrt{-26}]$

$$27 = 3 \cdot 3 \cdot 3 = (1 + \sqrt{-26}) \cdot (1 - \sqrt{-26}).$$

4.1. Factorización prima de ideales

Como siempre, $\mathfrak{O}$ será el anillo de enteros de un cuerpo de números K de grado n. Escribiremos de aquí en adelante los ideales con letras góticas minúsculas ($\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{p}, \mathfrak{m}, \ldots$). Aquí estudiaremos especialmente dos tipos de ideales:

Definición 4.1. *Sea R un anillo y $\mathfrak{a}$ un ideal de R, se dirá que $\mathfrak{a}$ es **maximal**, si es propio y no hay ideales propios extrictamente entre $\mathfrak{a}$ y R.*

Definición 4.2. *Sea R un anillo. Un ideal de R $\mathfrak{a} \neq R$ se dirá **primo** si para cualesquiera ideales $\mathfrak{b}, \mathfrak{c}$ de R, si se tiene $\mathfrak{bc} \subseteq \mathfrak{a}$ entonces se tiene $\mathfrak{b} \subseteq \mathfrak{a}$ o $\mathfrak{c} \subseteq \mathfrak{a}$.*

Veamos que si $\mathfrak{a} = \langle a \rangle$, $\mathfrak{b} = \langle b \rangle$, $\mathfrak{c} = \langle c \rangle$ como $\langle x \rangle \subseteq \langle y \rangle$ implica $y|x$ el que $\mathfrak{a}$ sea un ideal primo se traduce a

$$a|bc \text{ implica que } a|b \text{ o } a|c.$$

Si R es un dominino de integridad, entonces el ideal cero es un ideal primo.

Lema 4.3. *Sea R un anillo y $\mathfrak{a}$ un ideal de R. Entonces*

(a) $\mathfrak{a}$ *es maximal si y sólo si* $R/\mathfrak{a}$ *es un cuerpo,*

(b) $\mathfrak{a}$ *es primo si y sólo si* $R/\mathfrak{a}$ *es un dominio.*

Corolario 4.4. *Todo ideal maximal es primo.*

Lema 4.5. *Si* I *es un ideal no nulo de un anillo de números* $\mathfrak{O}$*, entonces* $(I,+)$ *es también un grupo abeliano libre de rango* $n=[K,\mathbb{Q}]$ *y, por tanto,* $|\mathfrak{O}/I|$ *es finito.*

Demostración. Si $\{\alpha_1,\ldots,\alpha_n\}$ es una base entera de $\mathfrak{O}$ y $\alpha\in I$, $\alpha\neq 0$, entonces

$$\langle\alpha\rangle\subset I\subset\mathfrak{O}$$

con $\langle\alpha\rangle$ y $\mathfrak{O}$ grupos abelianos libres de rango n pues

$$\langle\alpha\rangle=\mathfrak{O}\alpha=\mathbb{Z}(\alpha_1\alpha)\oplus\cdots\oplus\mathbb{Z}(\alpha_n\alpha)$$

por tanto I es también grupo abeliano de rango n y $|\mathfrak{O}/I|$ es finito. □

En el siguiente teorema se recogen unas importantes propiedades del anillo de enteros de un cuerpo de números:

Teorema 4.6. *El anillo de enteros* $\mathfrak{O}$ *de un cuerpo de números* K *tiene las siguientes propiedades:*

(a) Es un dominio, con cuerpo de fracciones K*,*

(b) es noetheriano,

(c) si $\alpha\in K$ *es cero de un polinomio mónico con coeficientes en* $\mathfrak{O}$ *entonces* $\alpha\in\mathfrak{O}$*,*

(d) todo ideal primo no nulo de $\mathfrak{O}$ *es maximal.*

Demostración. La parte (a) es obvia. Para (b) por el teorema 1.25 el grupo $(\mathfrak{O},+)$ es libre abeliano de rango n, y como $(\mathfrak{a},+)$ es un subgrupo de éste, ([5] Teorema 1.16, pág. 28) se tiene que $(\mathfrak{a},+)$ es libre abeliano de rango $\leq n$, y por tanto $\mathfrak{a}$ es finitamente generado sobre $\mathbb{Z}$. La parte (c) se tiene inmediatamente del teorema 1.17. (d) Sea $\mathfrak{p}$ un ideal primo, entonces $|\mathfrak{O}/\mathfrak{p}|$ es finito por el lema 4.5, y por ser $\mathfrak{p}$ primo se tiene $\mathfrak{O}/\mathfrak{p}$ es dominio y como su cardinal es finito es un cuerpo, que a su vez implica que $\mathfrak{p}$ es maximal en $\mathfrak{O}$. □

Para probar la factorización única en ideales primos, estudiaremos el comportamiento de los ideales de $\mathfrak{O}$ bajo la multiplicación. Para ello nos ayudamos de los *ideales fraccionales*:

Definición 4.7. *Un* $\mathfrak{O}$*-submódulo* $\mathfrak{a}$ *de* K *se dirá* ***ideal fraccional****, si existe* $c\in\mathfrak{O}$ *tal que* $\mathfrak{b}=c\mathfrak{a}\subseteq\mathfrak{O}$*.*

No es difícil de ver que $\mathfrak{b}$ es un ideal. Además, los ideales fraccionales los podemos caracterizar por ser de la forma $\mathfrak{a}=c^{-1}\mathfrak{b}$ con $c\in\mathfrak{O}$ y $\mathfrak{b}$ un ideal de $\mathfrak{O}$.

Por ejemplo, los ideales fraccionales de $\mathbb{Z}$ de la forma $r\mathbb{Z}$ donde $r\in\mathbb{Q}$.

En general, un ideal $\mathfrak{a}$ de $\mathfrak{O}$ es un ideal fraccional, y recíprocamente, un ideal fraccional $\mathfrak{a}$ es fraccional si y sólo si $\mathfrak{a}\subseteq\mathfrak{O}$. El producto de dos ideales fraccionales es un ideal fraccional, por que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales fraccionales, entonces $\mathfrak{a}=c^{-1}\mathfrak{a}_1$, $\mathfrak{b}=d^{-1}\mathfrak{b}_1$ para $c,d\in\mathfrak{O}$ y $\mathfrak{a}_1,\mathfrak{b}_1$ ideales. Con esta notación tenemos $\mathfrak{ab}=(c^{-1}\mathfrak{a}_1)(d^{-1}\mathfrak{b}_1)=(cd)^{-1}\mathfrak{a}_1\mathfrak{b}_1$

Lo que queremos demostrar a partir de ahora son los siguientes resultados:

Teorema 4.8. *Los ideales fraccionales de $\mathfrak{O}$ forman un grupo abeliano bajo la multiplicación.*

Teorema 4.9. *Todo ideal no nulo de $\mathfrak{O}$ puede ser escrito como producto finito de ideales primos, de manera única salvo orden de los factores.*

Demostración. Demostraremos los anteriores teoremas en una serie de pasos.

(i) Sea $\mathfrak{a} \neq 0$ un ideal de $\mathfrak{O}$. Entonces existen un número finito de ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tal que $\mathfrak{p}_1, \cdots, \mathfrak{p}_r \subseteq \mathfrak{a}$.
Lo haremos por reducción al absurdo. Si suponemos que no es cierto (i) entonces por ser $\mathfrak{O}$ noetheriano podemos elegir $\mathfrak{a}$ maximal entre los que no contienen a un producto finito de primos. En particular $\mathfrak{a}$ no es primo, así que existen un par de ideales $\mathfrak{b}$, $\mathfrak{c}$ de $\mathfrak{O}$ con $\mathfrak{bc} \subseteq \mathfrak{a}$, $\mathfrak{b} \nsubseteq \mathfrak{a}$, $\mathfrak{c} \nsubseteq \mathfrak{a}$. Sean

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

Entonces $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$, $\mathfrak{a} \subsetneqq \mathfrak{a}_1$, $\mathfrak{a} \subsetneqq \mathfrak{a}_2$. Por la maximalidad de $\mathfrak{a}$ existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, $\mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$ tal que

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

Por lo tanto

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$$

contradiciendo la elección de $\mathfrak{a}$.

(ii) Definición de inverso de un ideal.

Para cada ideal $\mathfrak{a}$ de $\mathfrak{O}$ se define

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

Está claro que $\mathfrak{a}^{-1}$ es un $\mathfrak{O}$-submódulo. Si $\mathfrak{a} \neq 0$ entonces para cualquier $c \in \mathfrak{a}$, $c \neq 0$ tenemos que $c\mathfrak{a}^{-1} \subseteq \mathfrak{O}$, así que $\mathfrak{a}^{-1}$ es un ideal fraccional. Claramente $\mathfrak{O} \subseteq \mathfrak{a}^{-1}$, por consiguiente $\mathfrak{a} = \mathfrak{a}\mathfrak{O} \subseteq \mathfrak{a}\mathfrak{a}^{-1}$. De la definición tenemos que

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{O}.$$

Esto significa que el ideal fraccional $\mathfrak{a}\mathfrak{a}^{-1}$ es de hecho un ideal. Lo que queremos probar es que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$. Una propiedad que nos servirá es que si $\mathfrak{a}$, $\mathfrak{p}$ son ideales con $\mathfrak{a} \subseteq \mathfrak{p}$, entonces se tiene que $\mathfrak{O} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$.

(iii) Si $\mathfrak{a}$ es un ideal propio, entonces $\mathfrak{O} \subsetneqq \mathfrak{a}$.

Como $\mathfrak{a} \subseteq \mathfrak{p}$ para algún ideal maximal $\mathfrak{p}$, donde $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, basta probar $\mathfrak{p} \neq \mathfrak{O}$ para $\mathfrak{p}$ maximal. Debemos buscar entonces un elemento en $\mathfrak{p}$ que no sea entero algebraico. Empezamos con cualquier $a \in \mathfrak{p}$, $a \neq 0$. Usando (i) elegimos el menor r tal que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle a \rangle$$

para $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideales primos. Como $\langle a \rangle \subseteq \mathfrak{p}$ y $\mathfrak{p}$ es primo, entonces algún $\mathfrak{p}_i \subseteq \mathfrak{p}$. Sin pérdida de generalidad $\mathfrak{p}_1 \subseteq \mathfrak{p}$ y por tanto $\mathfrak{p}_1 = \mathfrak{p}$ por ser ideales primos y por tanto maximales. Además

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq \langle a \rangle$$

por la minimalidad de r. Por lo tanto podemos encontrar $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \backslash \langle a \rangle$. Pero $b\mathfrak{p} \subseteq \langle a \rangle$. Así que $ba^{-1}\mathfrak{p} \subseteq \mathfrak{O}$ y $ba^{-1} \in \mathfrak{p}^{-1}$. Pero $b \notin a\mathfrak{O}$ así que $ba^{-1} \notin \mathfrak{O}$, por lo que $\mathfrak{p}^{-1} \neq \mathfrak{O}$.

(iv) Si $\mathfrak{a}$ es un ideal no nulo y $\mathfrak{a}S \subseteq \mathfrak{a}$ para cualquier subconjunto $S \subseteq K$, entonces $S \subseteq \mathfrak{O}$.

Veamos que si $a\theta \subseteq \mathfrak{a}$ para $\theta \in S$, entonces $\theta \in \mathfrak{O}$. Como $\mathfrak{O}$ es noetheriano, $\mathfrak{a} = \langle a_1, \ldots, a_m \rangle$, donde no todos los a_i son cero. Entonces $\mathfrak{a}\theta \subseteq \mathfrak{a}$ implica

$$\begin{array}{rcll} a_1\theta & = & b_{11}a_1 + \cdots + b_{1m}a_m & \\ \cdots & & \cdots & (b_{ij} \in \mathfrak{O}) \\ a_m\theta & = & b_{m1}a_1 + \cdots + b_{mm}a_m & \end{array}$$

Y entonces las ecuaciones

$$\begin{array}{rcl} (b_{11} - \theta)x_1 + \cdots + b_{1m}x_m & = & 0 \\ & \cdots & \\ b_{m1}x_1 + \cdots + (b_{mm} - \theta)x_m & = & 0 \end{array}$$

tienen una solución no nula $x_1 = a_1, \ldots, x_m = a_m$. Como resultado, el determinante de la matriz asociada a dicho sistema vale cero, que precisamente es un polinomio mónico con coeficientes en $\mathfrak{O}$ y por lo tanto $\theta \in \mathfrak{O}$ por el teorema 4.6(c).

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

De *(ii)*, elegimos $\mathfrak{p}\mathfrak{p}^{-1}$ es un ideal donde $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$. Como $\mathfrak{p}$ es maximal, $\mathfrak{p}\mathfrak{p}^{-1}$ es igual a $\mathfrak{p}$ o a $\mathfrak{O}$. Pero si $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ entonces *(iv)* implicaría $\mathfrak{p}^{-1} \subseteq \mathfrak{O}$, contradiciendo *(iii)*. Así que $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}$. Extendemos ahora esta propiedad a cualquier ideal $\mathfrak{a}$:

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

Si no fuese cierto, elegimos $\mathfrak{a}$ maximal entre los que $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathfrak{O}$. Entonces $\mathfrak{a} \subseteq \mathfrak{p}$ donde $\mathfrak{p}$ es maximal. De *(ii)*, $\mathfrak{O} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, así que

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}.$$

En particular, $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$ implica $\mathfrak{a}\mathfrak{p}^{-1}$ es un ideal. Ahora no puede ser que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, que implicaría que $\mathfrak{p}^{-1} \subseteq \mathfrak{O}$ por *(iv)*, contradiciendo *(iii)*. Así que $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ y la maximalidad de la condición de $\mathfrak{a}$ implica que el ideal $\mathfrak{a}\mathfrak{p}^{-1}$ satisface

$$\mathfrak{a}\mathfrak{p}(\mathfrak{a}\mathfrak{p})^{-1} = \mathfrak{O}$$

pero por la definición de $\mathfrak{a}^{-1}$ esto significa

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}.$$

Así que

$$\mathfrak{O} = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}$$

de donde se tiene que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$.

(vii) Todo ideal fraccional $\mathfrak{a}$ tiene un inverso $\mathfrak{a}^{-1}$ tal que $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$.

El conjunto $\mathcal{F}$ de los ideales fraccionales es un un grupo conmutativo. Dado un ideal fraccional $\mathfrak{a}$ entonces para encontrar el inverso, solo debemos encontrar encontrar un ideal fraccional $\mathfrak{a}'$ tal que $\mathfrak{a}\mathfrak{a}' = \mathfrak{O}$. Pero existe un ideal $\mathfrak{b}$ y un elemento $c \in \mathfrak{O}$ tal que $\mathfrak{a} = c^{-1}\mathfrak{b}$. Es fácil ver que $\mathfrak{a}^{-1} = \mathfrak{a}' = c\mathfrak{b}^{-1}$. Hasta aquí hemos probado el teorema 4.8.

(viii) Todo ideal $\mathfrak{a}$ no nulo es producto de ideales primos.

Si no, sea $\mathfrak{a}$ maximal entre los que no son producto de ideales primos. Entonces $\mathfrak{a}$ no es primo, pero tendremos que $\mathfrak{a} \subseteq \mathfrak{p}$ para algún ideal maximal (por tanto primo), y como en (vi),

$$\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{O}.$$

Por la maximalidad de la condición en $\mathfrak{a}$,

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$$

para ideales primos $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, y entonces

$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

(ix) La factorización en ideales primos es única.

Por analogía con la factorización en elementos, para ideales $\mathfrak{a}$, $\mathfrak{b}$ diremos que $\mathfrak{a}$ divide a $\mathfrak{b}$ y escribiremos $\mathfrak{a}|\mathfrak{b}$ si existe un ideal $\mathfrak{c}$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Esta condición es equivalente a $\mathfrak{b} \subseteq \mathfrak{a}$ ya que podemos ver que en este caso $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$. La definición de que $\mathfrak{p}$ sea ideal primo en esta notación se traduce a, si $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$ implica $\mathfrak{p}|\mathfrak{a}$ o $\mathfrak{p}|\mathfrak{b}$. Si tenemos ahora ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ con

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

entonces $\mathfrak{p}_1$ divide a algún $\mathfrak{q}_i$, y por la maximalidad entonces $\mathfrak{p}_1 = \mathfrak{q}_i$. Multiplicando por $\mathfrak{p}^{-1}$ y usando inducción obtenemos la factorización única en ideales primos, salvo el orden de los factores. Y esto prueba finalmente el teorema 4.9. □

Proposición 4.10. *Para ideales $\mathfrak{a}$, $\mathfrak{b}$ de $\mathfrak{O}$,*

$$\mathfrak{a}|\mathfrak{b} \text{ si y sólo si } \mathfrak{a} \supseteq \mathfrak{b}$$

Recordemos que cuando tenemos factorización única en irreducibles sobre elementos, tenemos asegurada la existencia del mínimo común múltiplo y el máximo común divisor, y demostrada ya la factorización única en ideales primos tenemos su analogía en ideales. Dados ideales $\mathfrak{a}$ y $\mathfrak{b}$ tenemos que el máximo común divisor $\mathfrak{g}$ y el mínimo común múltiplo $\mathfrak{l}$ de $\mathfrak{a}$ y $\mathfrak{b}$ son los que cumplen las siguientes propiedades:

$$\mathfrak{g}|\mathfrak{a},\ \mathfrak{g}|\mathfrak{b} \text{ y si } \mathfrak{g}' \text{ tiene las mismas propiedades entonces } \mathfrak{g}'|\mathfrak{g},$$
$$\mathfrak{a}|\mathfrak{l},\ \mathfrak{b}|\mathfrak{l} \text{ y si } \mathfrak{l}' \text{ tiene las mismas propiedades entonces } \mathfrak{l}|\mathfrak{l}'.$$

De hecho, suponiendo que la factorización en ideales primos de $\mathfrak{a}$ y de $\mathfrak{b}$ es

$$\prod \mathfrak{p}_i^{e_i}, \quad \prod \mathfrak{p}_i^{f_i}.$$

Entonces $\mathfrak{g}$ y $\mathfrak{l}$ vienen dados por

$$\mathfrak{g} = \prod \mathfrak{p}_i^{min\{e_i,f_i\}} \qquad \mathfrak{l} = \prod \mathfrak{p}_i^{max\{e_i,f_i\}}.$$

También tenemos otras útiles expresiones de $\mathfrak{g}$ y de $\mathfrak{l}$

Proposición 4.11. *Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales de $\mathfrak{O}$, y $\mathfrak{g}$, $\mathfrak{l}$ son el máximo común divisor y mínimo común múltiplo respectivamente, de $\mathfrak{a}$ y $\mathfrak{b}$, entonces*

$$\mathfrak{g} = \mathfrak{a} + \mathfrak{b}, \qquad \mathfrak{l} = \mathfrak{a} \cap \mathfrak{b}.$$

Demostración. Sabemos que $\mathfrak{r}|\mathfrak{a}$ si y sólo si $\mathfrak{a} \subseteq \mathfrak{r}$ (Proposición 4.7). Entonces $\mathfrak{g}$ es el ideal más pequeño que contenga a $\mathfrak{a}$ y $\mathfrak{b}$. Por lo mismo, $\mathfrak{l}$ es el ideal más grande contenido en $\mathfrak{a}$ y $\mathfrak{b}$. □

4.2. Norma de un ideal

Como anteriormente se ha visto, si $\mathfrak{a}$ es un ideal de $\mathfrak{O}$, entonces $|\mathfrak{O}/\mathfrak{a}|$ es finito, y lo llamaremos *norma* de un ideal:

Definición 4.12. *Sea $\mathfrak{a}$ un ideal de $\mathfrak{O}$. Se define la **norma** de $\mathfrak{a}$, y se denota por $N(\mathfrak{a})$ al valor $N(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}|$.*

Esta definición es fundamental en la práctica por sus múltiples propiedades que veremos a continuación. Como es evidente, la norma de un ideal siempre es un entero positivo.

Teorema 4.13. *(a) Todo ideal $\mathfrak{a}$ de $\mathfrak{O}$ con $\mathfrak{a} \neq 0$ tiene una $\mathbb{Z}$-base $\{\alpha_1, \ldots, \alpha_n\}$ donde n es el grado de K.*

(b) Se tiene que

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{1/2}$$

donde Δ es el discriminante de K.

Demostración. Para (a), por el Lema 4.5, $(\mathfrak{a}, +)$ es libre abeliano de rango n y por tanto, tiene una base de esa forma. Para (b) sea $\{\omega_1, \ldots, \omega_n\}$ una $\mathbb{Z}$-base de $\mathfrak{O}$, y supongamos que $\alpha_i = \sum c_{ij}\omega_j$. Entonces por [5] Teorema 1.17, pág. 30

$$N(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}| = |det[c_{ij}]|.$$

Y por la fórmula

$$\begin{aligned} \Delta[\alpha_1, \ldots, \alpha_n] &= (det[c_{ij}])^2 \Delta[\omega_1, \ldots, \omega_n] \\ &= (N(\mathfrak{a}))^2 \Delta. \end{aligned}$$

Tomando raíces y recordando que $N(\mathfrak{a})$ es un número positivo, obtenemos lo deseado. □

Corolario 4.14. *Si* $\mathfrak{a} = \langle a \rangle$ *es un ideal principal entonces* $N(\mathfrak{a}) = |N(a)|$.

Demostración. Con la notación anterior, una $\mathbb{Z}$-base de $\mathfrak{a}$ sería $\{a\omega_1, \ldots, a\omega_n\}$. Y el resultado se tiene de la definicion de $\Delta[\alpha_1, \ldots, \alpha_n]$ y del teorema 4.13(b). □

Una de las propiedades muy útiles de la norma de un ideal es su propiedad multiplicativa.

Teorema 4.15. *Si* $\mathfrak{a}$ *y* $\mathfrak{b}$ *son ideales no nulos de* $\mathfrak{O}$*, entonces*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Demostración. Por la factorización única en ideales primos, basta probar

$$N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p}) \tag{1}$$

donde $\mathfrak{p}$ es un ideal primo. Veamos que

$$|\mathfrak{O}/\mathfrak{ap}| = |\mathfrak{O}/\mathfrak{a}|\,|\mathfrak{a}/\mathfrak{ap}| \tag{2}$$

y que

$$|\mathfrak{a}/\mathfrak{ap}| = |\mathfrak{O}/\mathfrak{p}|. \tag{3}$$

La ecuación (1) se obtiene directamente de (2) junto con (3). Dicha ecuación (2) es conscuencia del primer teorema de isomorfía para anillos, y el homomorfismo suprayectivo $\phi : \mathfrak{O}/\mathfrak{ap} \longrightarrow \mathfrak{O}/\mathfrak{a}$ dado por

$$\phi(x + \mathfrak{ap}) = x + \mathfrak{a}$$

que tiene núcleo $\ker(\phi) = \mathfrak{a}/\mathfrak{ap}$. Y aplicando el Teorema de Lagrange (aplicación a grupos aditivos) nos da (2).
Para probar la ecuación (3), primero notemos que la factorización única implica que $\mathfrak{a} \neq \mathfrak{ap}$, así que $\mathfrak{ap} \subsetneqq \mathfrak{a}$. Ahora probaremos que no hay ideales estrictamente contenidos entre $\mathfrak{a}$ y $\mathfrak{ap}$, pues si

$$\mathfrak{ap} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$$

entonces, como ideales fraccionales

$$\mathfrak{a}^{-1}\mathfrak{ap} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a}$$

así que

$$\mathfrak{p} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{O}.$$

Entonces $\mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{O}$, que de hecho es un ideal, y contiene a $\mathfrak{p}$ que es maximal, por lo que

$$\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{O} \quad \text{o} \quad \mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{p}$$

luego

$$\mathfrak{b} = \mathfrak{a} \quad \text{o} \quad \mathfrak{b} = \mathfrak{ap}.$$

Esto significa que para cada elemento $a \in \mathfrak{a} \backslash \mathfrak{ap}$, se tiene

$$\mathfrak{ap} + \langle a \rangle = \mathfrak{a}. \tag{4}$$

Fijamos a con esa propiedad, y definimos el homomorfismo de $\mathfrak{O}$-módulos $\varphi : \mathfrak{O} \longrightarrow \mathfrak{a}/\mathfrak{ap}$, dado por

$$\varphi(x) = ax + \mathfrak{ap},$$

suprayectivo por (4), con $\mathfrak{p} \subseteq \ker(\varphi)$. Ahora $\ker(\varphi) \neq \emptyset$ (que significaría que $\mathfrak{a}/\mathfrak{ap} \cong \mathfrak{O}/\ker(\varphi) = 0$, que contradice $\mathfrak{a} \neq \mathfrak{ap}$), y $\mathfrak{p}$ es maximal, así que

$$\ker(\varphi) = \mathfrak{p}.$$

Por lo tanto $\mathfrak{O}/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$ (como $\mathfrak{O}$-módulos), que demuestra la ecuación (3) y completa la prueba. □

Vamos ahora a introducir para mayor comodidad una notación para la divisividad. Hasta ahora, si $\mathfrak{a}$ es un ideal y $b \in \mathfrak{O}$, tiene sentido decir que $\mathfrak{a}|\langle b\rangle$ que partir de ahora, para ideales principales simplificaremos diciendo que $\mathfrak{a}|b$. Por ejemplo, si $\mathfrak{p}$ es un ideal primo, $a, b \in \mathfrak{O}$, y se tiene $\mathfrak{p}|\langle a\rangle\langle b\rangle$ implica $\mathfrak{p}|\langle a\rangle$ o $\mathfrak{p}|\langle b\rangle$, y esto se traduce a

$$\mathfrak{p}|ab \quad \text{implica} \quad \mathfrak{p}|a \text{ o } \mathfrak{p}|b.$$

Teorema 4.16. *Sea $\mathfrak{a}$ un ideal no nulo de $\mathfrak{O}$,*

(a) si $N(\mathfrak{a})$ es un número primo, entonces $\mathfrak{a}$ es un ideal primo.

(b) $N(\mathfrak{a})$ es un elemento de $\mathfrak{a}$, o equivalentemente $\mathfrak{a}|N(\mathfrak{a})$.

(c) si $\mathfrak{a}$ es un ideal primo, entonces divide exactamente a un número primo p, y

$$N(\mathfrak{a}) = p^m$$

donde $m \leq n$, el grado de K.

Demostración. Para la parte (a), $\mathfrak{a}$ se descompone en ideales primos y se igualan las normas (teniendo en cuenta que por la definición de norma de un ideal, el único ideal $\mathfrak{b}$ tal que $N(\mathfrak{b}) = 1$ es $\mathfrak{b} = \mathfrak{O}$). Para (b) como $N(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}|$ se sigue que para cualquier $x \in \mathfrak{O}$ se tiene $N(\mathfrak{a})x \in \mathfrak{a}$. Entonces tomando $x = 1$ se tiene $N(\mathfrak{a}) \in \mathfrak{a}$. Para (c) notemos que por la parte (b)

$$\mathfrak{a}|N(\mathfrak{a}) = p_1^{m_1} \cdots p_r^{m_r}$$

considerando ideales principales en lugar de los p_i tenemos que $\mathfrak{a}\,|p_i$ para algún número primo p_i. Si p y q son distintos números primos, ambos divisibles por $\mathfrak{a}$, entonces podríamos encontrar enteros u, v tal que $up + vq = 1$, de donde se deduce que $\mathfrak{a}\,|1$, que implica que $\mathfrak{a} = \mathfrak{O}$ que es una contradicción. Entonces

$$N(\mathfrak{a})|N(\langle p\rangle) = p^n$$

así que $N(\mathfrak{a}) = p^m$ para algún $m \leq n$. □

Teorema 4.17. *(a) Todo ideal no nulo de $\mathfrak{O}$ tiene un número finito de divisores.*

(b) Un número entero pertenece sólo a un número finito de ideales de $\mathfrak{O}$.

(c) Dado un número entero s, sólo un número finito tienen de norma s.

Demostración. La parte (a) es consecuencia directa de la factorización prima, (b) es un caso particular de (a), y (c) se sigue directamente de (b). □

El siguiente es un resultado muy útil y será fundamental su aplicación en el cálculo de ideales primos.

Teorema 4.18. *Sea K un cuerpo de números de grado n con anillo de enteros $\mathfrak{O} = \mathbb{Z}[\theta]$ generado por $\theta \in \mathfrak{O}$. Dado un número primo p. Supongamos que el polinomio mínimo de θ sobre $\mathbb{Q}$ es f, que da lugar la factorización en irreducibles sobre $\mathbb{Z}_p$:*

$$\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r}$$

donde las barras denotan la proyección natural $\mathbb{Z}[t] \longrightarrow \mathbb{Z}_p[t]$. Entonces, si $f_i \in \mathbb{Z}[t]$ es cualquier polinomio mónico que vía la anterior proyección es $\bar{f}_i$, el ideal

$$\mathfrak{p}_i = \langle p\,,\, f_i(\theta)\rangle$$

es primo y la factorización en primos de $\langle p\rangle$ en $\mathfrak{O}$ es

$$\langle p\rangle = \mathfrak{p}_i^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Demostración. Sea θ_i una raíz de $\bar{f}_i$ en $\mathbb{Z}_p[\theta_i] \cong \mathbb{Z}_p[t]/\langle \bar{f}_i\rangle$. Hacemos uso de la aplicación natural $\nu_i : \mathbb{Z}[\theta] \longrightarrow \mathbb{Z}_p[\theta_i]$ dada por

$$\nu_i(p(\theta)) = \bar{p}(\theta_i).$$

La imagen de ν_i es $\mathbb{Z}_p[\theta_i]$, que es un cuerpo, así que $\ker(\nu_i)$ es un ideal primo de $\mathbb{Z}[\theta] = \mathfrak{O}$. Claramente

$$\langle p\,, f_i(\theta)\rangle \subseteq \ker(\nu_i).$$

Pero si $g(\theta) \in \ker(\nu_i)$, entonces $\bar{g}(\theta_i) = 0$, así que $\bar{g} = \bar{f}_i\bar{h}$ para algún $\bar{h} \in \mathbb{Z}_p[t]$; lo que significa que $g - f_i h \in \mathbb{Z}[t]$ tiene coeficientes divisibles por p. Por lo tanto

$$g(\theta) = (g(\theta) - f_i(\theta)h(\theta)) + f_i(\theta)h(\theta) \in \langle p,\, f_i(\theta)\rangle,$$

demostrando que

$$\ker(\nu_i) = \langle p\,,\, f_i(\theta)\rangle.$$

Sean

$$\mathfrak{p}_i = \langle p\,,\, f_i(\theta)\rangle,$$

entonces para cada $\bar{f}_i$ el ideal $\mathfrak{p}_i$ es primo y satisface $\langle p\rangle \subseteq \mathfrak{p}_i$, es decir $\mathfrak{p}_i | \langle p\rangle$. Para cualesquiera ideales $\mathfrak{a}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$ se tiene que

$$(\mathfrak{a} + \mathfrak{b}_1)(\mathfrak{a} + \mathfrak{b}_2) \subseteq \mathfrak{a} + \mathfrak{b}_1\mathfrak{b}_2,$$

así que por inducción

$$\begin{aligned} \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} &\subseteq \langle p\rangle + \langle f_1(\theta)^{e_1} \cdots f_r(\theta)^{e_r}\rangle \\ &\subseteq \langle p\,,\, f(\theta)\rangle \\ &= \langle p\rangle. \end{aligned}$$

Entonces $\langle p\rangle|\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$, y los únicos factores de $\langle p\rangle$ son $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$, por lo que

$$\langle p\rangle = \mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r} \tag{1}$$

donde $0 < k_i \leq e_i$ para $i = 1,\ldots,r$. La norma de $\mathfrak{p}_i$ es por definición $|\mathfrak{O}/\mathfrak{p}_i|$ y usuando los isomorfismos

$$\mathfrak{O}/\mathfrak{p}_i = \mathbb{Z}[\theta]/\mathfrak{p}_i \cong \mathbb{Z}_p[\theta_i]$$

y entonces

$$N(\mathfrak{p}_i) = |\mathbb{Z}_p[\theta_i]| = p^{d_i}$$

donde $d_i = \partial\bar{f}_i = \partial f_i$. También

$$N(\langle p\rangle) = N(p) = p^n,$$

así que tomando normas en (1), tenemos que

$$p^n = N(\langle p\rangle) = N(\mathfrak{p}_1)^{k_1}\cdots N(\mathfrak{p}_r)^{k_r},$$

y entonces se tiene la igualdad

$$d_1k_1 + \cdots + d_rk_r = n = d_1e_1 + \cdots + d_re_r$$

que por ser $k_i \leq e_i$ para $i = 1,\ldots,r$ implica que $k_i = e_i$ para todo i, y esto completa la prueba. □

Con este teorema, sabemos descomponer cualquier $\langle m\rangle$ con $m \in \mathbb{Z}$, en ideales primos, pues si $m = p_1^{n_1}\cdots p_s^{n_s}$ es su factorización en irreducibles, entonces $\langle m\rangle = \langle p_1\rangle^{n_1}\cdots\langle p_s\rangle^{n_s}$. Y estamos ya en condiciones de demostrar y explicar los casos de factorización no única, aquí vamos a desarrollar el ejemplo de factorización no única en el anillo de enteros de $\mathbb{Q}(\sqrt{-26})$ que es $\mathbb{Z}[\sqrt{-26}]$ donde recordemos que el ejemplo de que no hay factorización única es

$$27 = 3\cdot 3\cdot 3 = (1+\sqrt{-26})\cdot(1-\sqrt{-26})$$

que visto en ideales queda como

$$\langle 27\rangle = \langle 3\rangle\langle 3\rangle\langle 3\rangle = \langle 1+\sqrt{-26}\rangle\langle 1-\sqrt{-26}\rangle.$$

Utilizando el teorema 4.18 descompondremos $\langle 3\rangle$ en primos. Lo primero es buscar el irreducible, que en este caso queda como $f(t) = Irr(\sqrt{-26},\mathbb{Q}) = t^2+26$ y pasamos a irreducibles en $\mathbb{Z}_3[t]$

$$\overline{f(t)} = \overline{(t^2-1)} = \overline{(t+1)}\cdot\overline{(t-1)}$$

luego si $f_1(t) = t+1$ y $f_2(t) = t-1$, entonces por el teorema 4.18

$$\langle 3\rangle = \langle 3\,,\, f_1(\sqrt{-26})\rangle\langle 3\,,\, f_2(\sqrt{-26})\rangle = \langle 3\,,\, 1+\sqrt{-26}\rangle\langle 3\,,\, 1-\sqrt{-26}\rangle,$$

llamamos $\mathfrak{p}_1 = \langle 3\,,\, 1+\sqrt{-26}\rangle$ y $\mathfrak{p}_2 = \langle 3\,,\, 1-\sqrt{-26}\rangle$. Por la factorización única, y usando normas $N(\langle 1+\sqrt{-26}\rangle) = N(\langle 1-\sqrt{-26}\rangle) = 27$, se tiene que

$$\langle 1+\sqrt{-26}\rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \qquad \text{con } e_1+e_2 = 3.$$

Por tanto, probemos con $\mathfrak{p}_1^3$:

$$\begin{aligned}\mathfrak{p}_1^2 &= \langle 3\,,\, 1+\sqrt{-26}\rangle\langle 3\,,\, 1+\sqrt{-26}\rangle \\ &= \langle 9\,,\, 3+3\sqrt{-26}\,,\, -25+2\sqrt{-26}\rangle \\ &= \langle 9\,,\, 3+3\sqrt{-26}\,,\, 2+2\sqrt{-26}\rangle \\ &= \langle 9\,,\, 1+\sqrt{-26}\rangle.\end{aligned}$$

$$\begin{aligned}\mathfrak{p}_1^3 &= \langle 3\,,\, 1+\sqrt{-26}\rangle\langle 9\,,\, 1+\sqrt{-26}\rangle \\ &= \langle 27\,,\, 9+9\sqrt{-26}\,,\, 3+3\sqrt{-26}\,,\, -25+2\sqrt{-26}\rangle \\ &= \langle 27\,,\, 3+3\sqrt{-26}\,,\, 2+2\sqrt{-26}\rangle \\ &= \langle 27\,,\, 1+\sqrt{-26}\rangle \\ &= \langle 1+\sqrt{-26}\rangle.\end{aligned}$$

Y por tanto $\mathfrak{p}_1^3 = \langle 1+\sqrt{-26}\rangle$, que por la factorización única nos da que $\mathfrak{p}_2^3 = \langle 1-\sqrt{-26}\rangle$. Y tenemos

$$\langle 3\rangle\langle 3\rangle\langle 3\rangle = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_1\mathfrak{p}_2) = (\mathfrak{p}_1^3)(\mathfrak{p}_2^3) = \langle 1+\sqrt{-26}\rangle\langle 1-\sqrt{-26}\rangle.$$

Sabemos que todo ideal de $\mathfrak{O}$ es finitamente generado, por ser el anillo notheriano, de hecho probaremos que todo ideal es generado por dos elementos:

Teorema 4.19. *Si $\mathfrak{a}$ y $\mathfrak{b}$ son dos ideales no nulos de $\mathfrak{O}$ entonces existe $\alpha \in \mathfrak{a}$ tal que*

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathfrak{O}.$$

Demostración. Primero, ver que si $\alpha \in \mathfrak{a}$ entonces $\mathfrak{a}\,|\alpha$. Así que $\alpha\mathfrak{a}^1$ es un ideal y no sólo un ideal fraccional. Ahora $\alpha\mathfrak{a}^{-1}+\mathfrak{b}$ es el mínimo común múltiplo de $\alpha\mathfrak{a}^{-1}$ y $\mathfrak{b}$, así que es suficiente elegir $\alpha \in \mathfrak{a}$ tal que

$$\alpha\mathfrak{a}^{-1} + \mathfrak{p}_i \quad (i = 1, \ldots, r)$$

donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son los distintos primos que dividen a $\mathfrak{b}$. Esto se seguirá si

$$\mathfrak{p}_i \not| \alpha\mathfrak{a}^{-1}$$

ya que $\mathfrak{p}_i$ es un ideal maximal. Así que es suficiente elegir $\alpha \in \mathfrak{a}\backslash\mathfrak{a}\,\mathfrak{p}_i$ para todo $i = 1, \ldots, r$. Si $r = 1$ es sencillo por la factorización única, que implica $a \neq \mathfrak{a}\,\mathfrak{p}_i$. Para $r > 1$ sea

$$\mathfrak{a}_i = \mathfrak{a}\,\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_r.$$

Por el caso $r = 1$ puedo elegir

$$\alpha_i \in \mathfrak{a}_i\backslash\mathfrak{a}_i\,\mathfrak{p}_i.$$

Definimos

$$\alpha = \alpha_1 + \cdots + \alpha_r.$$

Entonces, cada $\alpha_i \in \mathfrak{a}_i \subseteq \mathfrak{a}$, por consiguiente $\alpha \in \mathfrak{a}$. Supongamos que es posible que $\alpha \in \mathfrak{a}\,\mathfrak{p}_i$.
Si $j \neq i$, $\alpha_j \in \mathfrak{a}_j \subseteq \mathfrak{a}\,\mathfrak{p}_i$. Así que se sigue que

$$\alpha_i = \alpha - \alpha_1 - \ldots - \alpha_{i-1} - \alpha_{i+1} - \ldots \alpha_r \in \mathfrak{a}\,\mathfrak{p}_i.$$

Por lo tanto $\mathfrak{a}\,\mathfrak{p}_i|\langle\alpha_i\rangle$. Y por otra parte $\mathfrak{a}_i|\langle\alpha_i\rangle$. Entonces $\mathfrak{a}_i\,\mathfrak{p}_i|\langle\alpha_i\rangle$. Lo que contradice la elección de α_i. □

Teorema 4.20. *Sea $\mathfrak{a} \neq 0$ un ideal de $\mathfrak{O}$, y $0 \neq \beta \in \mathfrak{a}$. Entonces existe $\alpha \in \mathfrak{a}$ tal que $\mathfrak{a} = \langle \alpha\,,\, \beta \rangle$.*

Demostración. Sea $\mathfrak{b} = \beta\mathfrak{a}^{-1}$. Por el lema 4.19 existe $\alpha \in \mathfrak{a}$ tal que

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = \alpha\mathfrak{a}^{-1} + \beta\mathfrak{a}^{-1} = \mathfrak{O}$$

por lo que

$$(\langle \alpha \rangle + \langle \beta \rangle)\mathfrak{a}^{-1} = \mathfrak{O}$$

y así

$$\mathfrak{a} = \langle \alpha \rangle + \langle \beta \rangle = \langle \alpha\,,\, \beta \rangle.$$

Este teorema muestra algo que ya hemos utilizado en el ejemplo anterior de la factorización en $\mathbb{Z}[\sqrt{-26}]$, donde siempre hemos sido capaces de expresar un ideal con solo dos generadores. Estamos ahora en condiciones de caracterizar cuando un anillo de enteros de un cuerpo de números es un dominio de factorización única.

Teorema 4.21. *La factorización en elementos de $\mathfrak{O}$ en irreducibles es única si y sólo si todo ideal de $\mathfrak{O}$ es principal.*

Demostración. Si todo ideal es principal, entonces la factorización única de elementos se sigue del teorema 3.15. Recíprocamente, si la factorización de elementos es única, entonces por la factorización única en ideales primos, bastará probar que todo ideal primo es principal. Sea $\mathfrak{p} \neq 0$ un ideal primo de $\mathfrak{O}$. Por el teorema 4.16(b) existe un entero $N = N(\mathfrak{p})$ tal que $\mathfrak{p}|N$. Podemos factorizar N como producto de irreducibles en $\mathfrak{O}$, digamos

$$N = \pi_1 \cdots \pi_s.$$

Como $\mathfrak{p}|N$ y $\mathfrak{p}$ es un ideal primo, se sigue que $\mathfrak{p}|\pi_i$ para algún i, o equivalentemente $\mathfrak{p}|\langle \pi_i \rangle$. Pero por ser la factorización única en $\mathfrak{O}$, y π_i un elemento irreducible, π_i es primo por el teorema 3.13 y entonces el ideal $\langle \pi_i \rangle$ es primo. Así que $\mathfrak{p}|\langle \pi_i \rangle$, y como ambos $\mathfrak{p}$, $\langle \pi_i \rangle$ son primos, por la factorización única en ideales primos se tiene

$$\mathfrak{p} = \langle \pi_i \rangle,$$

así que $\mathfrak{p}$ es principal. □

Tema 5

El grupo de clases y el número de clases

5.1. El Teorema de Minkowski

En este capítulo, estudiamos la representación como retículos de $\mathbb{R}^n$ de los ideales del anillo de enteros de un cuerpo de números de grado n que, como sabemos, son grupos libres abelianos de rango n.

Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números de grado n, donde θ es un entero algebraico. Sean $\sigma_1, \ldots, \sigma_n$ los n $\mathbb{Q}$-homomorfismos, $\sigma_i : K \longrightarrow \mathbb{C}$. Si $\sigma_i(K) \subseteq \mathbb{R}$, lo que ocurre si y sólo si $\sigma_i(\theta) \in \mathbb{R}$, decimos que σ_i es *real*, en otro caso, decimos que σ_i es *complejo*. Está claro, que si σ_i es complejo, entonces $\sigma_i(\theta)$ es una raíz del polinomio mínimo de θ sobre $\mathbb{Q}$, y no sólo eso, sino que $\overline{\sigma_i(\theta)}$ es también una raíz de dicho polinomio. Definiendo

$$\overline{\sigma_i}(\alpha) = \overline{(\sigma_i(\alpha))}$$

podemos decir que existe $j \neq i$ tal que $\sigma_j = \overline{\sigma_i}$, y entonces, los $\mathbb{Q}$-homomorfismos vienen a pares, y existirán un número s de $\mathbb{Q}$-homomorfismos reales, y un número $2t$ de $\mathbb{Q}$-homomorfismos complejos y tal que $n = s + 2t$.

Sean ahora $\sigma_1, \ldots, \sigma_s$ los $\mathbb{Q}$-homomorfismos reales, y $\sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ los $\mathbb{Q}$-homomorfismos complejos. Definiremos la aplicación $\sigma : K \longrightarrow \mathbb{R}^n$ dada por

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), Re(\sigma_{s+1}(\alpha)), Im(\sigma_{s+1}(\alpha)), \ldots, Re(\sigma_{s+t}(\alpha)), Im(\sigma_{s+t}(\alpha)))$$

donde Re y Im denotan a la parte real e imaginaria del número complejo. Es fácil ver que la aplicación es un homomorfismo aditivo con $\ker(\sigma) = \phi$ y, por lo tanto, podemos ver K contenido en $\mathbb{R}^n$ (considerando la estructura aditiva).

Definición 5.1. *Si $e_1, \ldots, e_n$ son vectores linealmente independientes en $\mathbb{R}^n$, entonces el subgrupo aditivo de $(\mathbb{R}^n, +)$ generado por $e_1, \ldots, e_n$ se dice que es un retículo n-dimensional generado por $e_1, \ldots, e_n$. Si L es un retículo n-dimensional generado por $e_1, \ldots, e_n$ definimos su dominio fundamental T formado por todos los puntos de $\mathbb{R}^n$ de la forma $\sum a_i e_i$ con $a_i \in [0, 1)$ para $i = 1, \ldots, n$.*

Lo que vamos a ver ahora es que $\sigma(\mathfrak{O}_K)$ es un retículo n-dimensional. Para empezar, tomamos $\alpha_1, \ldots, \alpha_n$ una base entera y nos preguntamos si los vectores de $\mathbb{R}^n$ $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ son linealmente independientes sobre $\mathbb{R}$, esto es equivalente a que

$$D = \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_s(\alpha_1) & Re(\sigma_{s+1}(\alpha_1)) & Im(\sigma_{s+1}(\alpha_1)) & \cdots & Re(\sigma_{s+t}(\alpha_1)) & Im(\sigma_{s+t}(\alpha_1)) \\ \cdots & & \cdots & \cdots & \cdots & & \cdots & \cdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_s(\alpha_n) & Re(\sigma_{s+1}(\alpha_n)) & Im(\sigma_{s+1}(\alpha_n)) & \cdots & Re(\sigma_{s+t}(\alpha_n)) & Im(\sigma_{s+t}(\alpha_n)) \end{vmatrix} \neq 0$$

pero lo anterior es equivalente multiplicando por $-2i$ algunas columnas y haciendo transformaciones elementales columna a

$$E = \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_s(\alpha_1) & Re(\sigma_{s+1}(\alpha_1)) + iIm(\sigma_{s+1}(\alpha_1)) & Re(\sigma_{s+1}(\alpha_1)) - iIm(\sigma_{s+1}(\alpha_1)) & \cdots \\ \cdots & & \cdots & \cdots & \cdots & \\ \sigma_1(\alpha_n) & \cdots & \sigma_s(\alpha_n) & Re(\sigma_{s+1}(\alpha_n)) + iIm(\sigma_{s+1}(\alpha_n)) & Re(\sigma_{s+1}(\alpha_n)) - iIm(\sigma_{s+1}(\alpha_n)) & \cdots \end{vmatrix}$$

$$= \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}}(\alpha_1) & \cdots & \sigma_{s+t}(\alpha_1) & \overline{\sigma_{s+t}}(\alpha_1) \\ \cdots & & \cdots & \cdots & \cdots & & \cdots & \cdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}}(\alpha_n) & \cdots & \sigma_{s+t}(\alpha_n) & \overline{\sigma_{s+t}}(\alpha_n) \end{vmatrix}.$$

Pero

$$E^2 = \Delta[\alpha_1, \ldots, \alpha_n] \neq 0$$

y por las transformaciones que hemos hecho en D para llegar a E se tiene que

$$E = (-2i)^t D$$

por lo que, $D \neq 0$ y entonces, $\sigma(\mathfrak{O}_K)$ es un retículo n-dimensional de $\mathbb{R}$. Además es bien sabido que el volumen del dominio fundamental de un retículo n-dimensional generado por los vectores $e_1, \ldots, e_n$ coincide precisamente con el valor absoluto del determinante formado por dichos vectores. En nuestro caso, el volumen del dominio fundamental del retículo generado por el anillo de enteros coincide (siguiendo con la notación anterior) con el valor de $|D|$, y por tanto

$$vol(T) = |D| = \frac{1}{2^t}\sqrt{|\Delta|}.$$

Definición 5.2. *Un subconjunto $X \subseteq \mathbb{R}^n$ es convexo si para cualesquiera $x, y \in X$ se tiene que el segmento de recta que los une está contenido en X, es decir, si para todo $\lambda \in [0, 1]$*

$$\lambda x + (1 - \lambda)y \in X.$$

Definición 5.3. *Un subconjunto $X \subseteq \mathbb{R}^n$ se dice simétricamente centrado si $x \in X$ implica $-x \in X$.*

El siguiente es un hecho muy geométrico y que será muy importante en nuestro estudio de la factorización única:

Teorema 5.4. *(Teorema de Minkowski) Sea L un retículo n-dimensional generado por $\{e_1, \ldots, e_n\}$ contenido en $\mathbb{R}^n$ con dominio fundamental T, y sea $E \subseteq \mathbb{R}^n$ un subconjunto convexo, simétricamente centrado y medible Lebesgue. Si*

$$vol(E) > 2^n vol(T)$$

entonces, E contiene un punto no nulo de L. Si E es también compacto, la desiguadad estricta puede ser reemplazada por $\geq$.

Demostración. $\mathbb{R}^n$ es la unión disjunta de los subconjuntos $x+T$ con $x \in L$. Se sigue que

$$\frac{1}{2}E = \bigcup_{x \in L} ((\frac{1}{2}E) \cap (x+T)) \qquad \text{(unión disjunta)}$$

donde con tE, con $t \in \mathbb{R}$, nos referimos a $\{te : e \in E\}$. Por lo tanto, asumiendo la desigualdad del enunciado, tenemos

$$vol(T) < \frac{1}{2^n} vol(E) = vol(\frac{1}{2}E) = \sum_{x \in L} vol(\frac{1}{2}E \cap (x+T))$$

$$= \sum_{x \in L} vol(((\frac{1}{2}E) - x) \cap T)$$

la última igualdad se mantiene por que el ser medible Lebesgue es invariante bajo traslaciones. Lo anterior muestra que los conjuntos $((\frac{1}{2}E) - x) \cap T$ no pueden ser disjuntos a pares. Fijados dos puntos cualesquiera x, $y \in L$ tales que $((\frac{1}{2}E) - x)$ y $((\frac{1}{2}E) - y)$ se intersecan; entonces $x - y$ es un punto no nulo de L y de la convexidad y las propiedades simétricas de E fácilmente vemos que $x - y \in E$. Ahora supongamos que E es compacto (que en $\mathbb{R}^n$ significa cerrado y acotado) y cambiemos la desigualdad estricta por $\geq$. Para cada $m = 1, 2, \ldots$, la primera parte del teorema muestra que el conjunto $(1 + \frac{1}{m})E$ contiene algún punto no nulo x_m de L. Los x_m están acotados como $m \to \infty$ ya que todos están en $2E$, y todos x_m están en L; Se sigue que solo hay un número finito de puntos distintos x_m. Entonces alguno de ellos está en $(1 + \frac{1}{m})E$ y por que m tiende a infinito, entonces esta en la clausura $\overline{E}$, que es E. □

Se define ahora en $\mathbb{R}^n$ una norma, que depende de los parámetros s y t. Dado un elemento $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ y $n = s + 2t$, se define la norma como

$$N(x) = x_1 \cdots x_s (x_{s+1}^2 + x_{s+2}^2) \cdots (x_{n-1}^2 + x_n^2)$$

que por supuesto es una norma, además es fácil notar que si $\alpha \in \mathfrak{O}_K$, entonces $N(\alpha) = N(\sigma(\alpha))$.

Corolario 5.5. *Supongamos que A es un subconjunto compacto, convexo, simétricamente centrado con $vol(a) > 0$, y la propiedad*

$$a \in A \text{ implica } N(a) \leq 1.$$

Entonces todo retículo n-dimensional L contiene un punto no nulo x con

$$|N(x)| \leq \frac{2^n}{vol(A)} vol(T)$$

siendo T el dominio fundamental del retículo L.

Demostración. Aplicamos el Teorema de Minkowski con $E = tA$, donde

$$t^n = \frac{2^n}{vol(A)}\, vol(L).$$

□

Teorema 5.6. *Con la norma N sobre $\mathbb{R}^n$ definida anteriormente, todo retículo n-dimensional L en $\mathbb{R}^n$ contiene un punto no nulo x con*

$$|N(x)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^t vol(T)$$

siendo T el dominio fundamental de L.

Demostración. Si consideremos el conjunto A determinado por las desigualdades

$$|x_1| \leq 1, \ldots, |x_s| \leq 1, x_{s+1}^2 + x_{s+2}^2 \leq 1, \ldots, x_{n-1}^2 + x_n^2 \leq 1.$$

Entonces $vol(A) = 2^s \pi^t$ y obtenemos que todo retículo L contiene un elemento no nulo x con

$$|N(x)| \leq \left(\frac{4}{\pi}\right)^t vol(T).$$

Sin embargo, para mejorar la cota, puede ser conveniente otra elección de A. Consideremos, ahora, el conjunto A determinado por

$$|x_1| + \cdots + |x_s| + 2\left(\sqrt{x_{s+1}^2 + x_{s+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n,$$

no es difícil ver que A es convexo, y la condición $a \in A$ implica $|N(a)| \leq 1$, esto se obtiene de la desigualdad

$$\frac{y_1 + \cdots + y_n}{n} \geq \sqrt[n]{y_1 \cdots y_n}$$

con $y_1, \ldots, y_n \in \mathbb{R}^+$. Probaremos ahora que

$$vol(A) = \frac{n^n}{n!} 2^s \left(\frac{\pi}{2}\right)^t,$$

que probará el teorema. En general, sea $V_{s,\,t}(m)$ el valor del volumen del subconjunto de $\mathbb{R}^{s+2t}$ determinado por

$$|x_1| + \cdots + |x_s| + 2\left(\sqrt{x_{s+1}^2 + x_{s+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq m$$

entonces

$$V_{s,\,t}(m) = m^{s+2t} V_{s,\,t}(1).$$

Vamos a ver ahora que

$$V_{s,\,t}(1) = \frac{1}{(s+2t)!} 2^s \left(\frac{\pi}{2}\right)^t.$$

Si $r > 0$ tenemos

$$V_{s,\,t}(1) = 2\int_0^1 V_{s-1,\,t}(1-x)dx = 2\int_0^1 (1-x)^{s-1+2t} V_{s-1,\,t}(1) = \frac{2}{s+2t} V_{s-1,\,t}(1).$$

Aplicando esto repetidas veces obtenemos

$$V_{s,\,t}(1) = \frac{2^s}{(s+2t)(s+2t-1)\cdots(2t+1)} V_{0,\,t}(1).$$

Cuando $t = 0$, lo que tenemos es un cubo s-dimensional de lado 2. Veamos ahora el valor de $V_{s,\,0}\,(1)$ para $s > 0$. Tenemos

$$V_{0,\,t}\,(1) = \int\int V_{0,\,s-1}\,(1 - 2\sqrt{x^2 + y^2})dx\;dy$$

con la integral tomada sobre la región circular $x^2 + y^2 < 1/4$. Transformando a coordenadas polares, obtenemos

$$\begin{aligned} V_{,\,t}\,(1) &= \int_0^{2\pi}\int_0^{1/2} V_{0,\,t-1}\,(1-2\rho)\rho\;d\rho\;d\theta = 2\pi V_{0,\,t-1}\,(1)\int_0^{1/2}(1-2\rho)^{2(t-1)}\rho\;d\rho \\ &= \frac{\pi}{2}V_{0,\,t-1}\,(1)\int_0^1 u^{2(t-1)}(1-u)du = \frac{\pi}{2}V_{0,\,t-1}\,(1)(\frac{1}{2t-1} - \frac{1}{2t}) = \frac{\pi}{2}\,\frac{V_{0,\,t-1}\,(1)}{(2t)(2t-1)}\,. \end{aligned}$$

Así, iterando, obtenemos

$$V_{0,\,t}\,(1) = \left(\frac{\pi}{2}\right)^t\,\frac{1}{(2s)!}\,.$$

Juntando los valores obtenidos, y utilizando la desigualdad proporcionada por el Corolario 5.7 obtenemos que todo retículo contiene un punto x no nulo, tal que

$$|N(x)| \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^t vol(T).$$

□

Corolario 5.7. *Sea K un cuerpo de números con anillo de enteros $\mathfrak{O}$, entonces todo ideal no nulo I de $\mathfrak{O}$ contiene un elemento α tal que*

$$N_{\mathbb{Q}}^K(\alpha) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t N(I)\sqrt{|\Delta|}.$$

Demostración. Como anteriormente se ha comentado, la imagen de un ideal de $\mathfrak{O}$ por σ es un subretículo M del retículo L imagen de $\mathfrak{O}$ por σ, además el volumen del dominio fundamental N de M, viene dado por

$$vol(N) = vol(\mathbb{R}^n/M) = vol(\mathbb{R}^n/L)|L/M| = vol(T)N(I) = \frac{1}{2^t}\sqrt{|\Delta|}N(I)$$

siendo T el dominio fundamental de L. El resultado se sigue de este resultado y el teorema anterior. □

Denotaremos de aquí en adelante la denominada *constante de Minkowski* que depende de los parámetros s y t con $n = s + 2t$ como

$$M_{s,\,t} = \left(\frac{4}{\pi}\right)^t\,\frac{(s+2t)!}{(s+2t)^{s+2t}}.$$

5.2. El grupo de clases

Como siempre, K será un cuerpo de números de grado n, con anillo de enteros $\mathfrak{O}$. Como vimos en el capítulo anterior, en los anillos de enteros en general no se da la factorización única en elementos, sin embargo siempre teníamos la factorización única en ideales primos, y observamos que la factorización única en elementos se daba si y sólo si $\mathfrak{O}$ es un dominio de ideales principales. Este resultado, junto con el Teorema 4.5 que nos asegura que el conjunto de los ideales fraccionales forma un grupo aditivo bajo la multiplicación, será nuestro punto de partida.

Denotamos por $\mathcal{F}$ el grupo de los ideales fraccionales. No es difícil comprobar que el subconjunto de $\mathcal{F}$ formado por los ideales fraccionales principales es un subgrupo de $\mathcal{F}$, denotado por $\mathcal{P}$, donde con ideales fraccionales principales, nos referimos a los que son de la forma $\mathfrak{b} = c^{-1}\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal principal de $\mathfrak{O}$ y $c \in \mathfrak{O}$. Una pequeña observación es que los ideales principales de $\mathfrak{O}$ son ideales fraccionales principales tomando $c = 1$.

Definición 5.8. *En las condiciones anteriores, se define entonces el* ***grupo de clases*** *de $\mathfrak{O}$ y lo denotamos por $\mathcal{H}$, como el cociente*

$$\mathcal{H} = \mathcal{F}/\mathcal{P} \ .$$

Se define también el ***número de clases*** *como $h = |\mathcal{H}|$.*

Como $\mathcal{F}$ y $\mathcal{P}$ son grupos infinitos, no podemos señalar de manera obvia la finitud de h, que veremos es cierta. Diremos que dos ideales fraccionales $\mathfrak{a}$ y $\mathfrak{b}$ son equivalentes si pertenecen a la misma clase en dicho cociente y escribiremos

$$\mathfrak{a} \sim \mathfrak{b}$$

y si $\mathfrak{a}$ y $\mathfrak{b}$ son equivalentes, usaremos $\overline{\mathfrak{a}}$ para denotar a la clase de equivalencia de $\mathfrak{a}$. Si $\mathfrak{a}$ es un ideal fraccional, entonces $\mathfrak{a} = c^{-1}\mathfrak{b}$ donde $c \in \mathfrak{O}$ y $\mathfrak{b}$ es un ideal de $\mathfrak{O}$. Por lo tanto

$$\mathfrak{b} = c\mathfrak{a} = \langle c \rangle \mathfrak{a}$$

y como $\langle c \rangle \in \mathcal{P}$, entonces $\mathfrak{a} \sim \mathfrak{b}$. En otras palabras, toda clase de equivalencia contiene al menos un ideal. Sean ahora $\mathfrak{a}$ y $\mathfrak{b}$ ideales equivalentes. Entonces $\mathfrak{a} = \mathfrak{c}\mathfrak{b}$ donde $\mathfrak{c}$ es un ideal fraccional principal, digamos $c = d^{-1}\mathfrak{h}$ para $d \in \mathfrak{O}$, $\mathfrak{h}$ un ideal principal. Por lo tanto

$$\mathfrak{a}\langle d \rangle = \mathfrak{b}\mathfrak{h}.$$

Recíprocamente, si $\mathfrak{c}\mathfrak{a} = \mathfrak{d}\mathfrak{b}$ donde $\mathfrak{c}$ y $\mathfrak{d}$ son ideales principales, entonces $\mathfrak{a} \sim \mathfrak{b}$. Por lo que tenemos que $\mathfrak{a} \sim \mathfrak{b}$, si y sólo si existen dos ideales principales $\mathfrak{c}$, $\mathfrak{d}$ tales que $\mathfrak{c}\mathfrak{a} = \mathfrak{d}\mathfrak{b}$. El conjunto $\mathcal{H}$ es un grupo junto con la operación en las clases de equivalencia

$$\overline{\mathfrak{a}}\,\overline{\mathfrak{b}} = \overline{\mathfrak{a}\mathfrak{b}}$$

de ahí su denominación. Con las definiciones introducidas, podemos caracterizar de otro modo, que computacionalmente será el adecuado, la factorización única en un anillo de enteros.

Teorema 5.9. *La factorización en $\mathfrak{O}$ es única si y sólo si el grupo de clases tiene orden uno, o equivalentemente el número de clases es uno.*

Demostración. La factorización es única si y sólo si todo ideal de $\mathfrak{O}$ es principal, que es cierto si y sólo si todos los ideales fraccionales son principales, es decir $\mathcal{F} = \mathcal{P}$, y por tanto $h = 1$. □

Pasamos ahora a estudiar la finitud del número de clases:

Teorema 5.10. *Todo ideal fraccional no nulo $\mathfrak{a}$ es equivalente a un ideal $\mathfrak{b}$ tal que*

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

Demostración. La clase de ideales fraccionales equivalentes a $\mathfrak{a}^{-1}$ contiene un ideal $\mathfrak{c}$, así que $\mathfrak{ac} \sim \mathfrak{O}$. Usando el Corolario 5.7 pordemos encontrar un entero algebraico $\gamma \in \mathfrak{c}$ tal que

$$|N(\gamma)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} N(\mathfrak{c})\sqrt{|\Delta|}.$$

Como $\mathfrak{c}|\gamma$ tenemos

$$\langle\gamma\rangle = \mathfrak{cb}$$

para algún ideal $\mathfrak{b}$. Como $N(\mathfrak{b})N(\mathfrak{c}) = N(\mathfrak{bc}) = N(\langle\gamma\rangle) = |N(\gamma)|$ tenemos

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}.$$

Y solo falta ver que $\mathfrak{b} \sim \mathfrak{a}$. Pero esto está claro ya que $\mathfrak{c} \sim \mathfrak{a}^{-1}$ y $\mathfrak{b} \sim \mathfrak{c}^{-1}$. □

Estamos ahora en condiciones de demostrar la finitud del número de clases:

Teorema 5.11. *El grupo de clases de un cuerpo de números es un grupo abeliano finito. El número de clases h es finito.*

Demostración. Sea K un cuerpo de números, con discriminante Δ, y grado $n = s + 2t$. Sabemos que el grupo de clases $\mathcal{H}$ es abeliano, así que falta probar que es finito, lo que es cierto si y sólo si el número de clases de equivalencia distintas es finito. Sea $\bar{\mathfrak{c}}$ una clase de equivalencia. Como hemos visto en el Teorema 5.10, dicha clase contiene un ideal $\mathfrak{a}$ con $N(a) \leq M_{s,\,t}\sqrt{|\Delta|}$ que es un valor finito y fijo. Sólo hay un número finito de ideales que tienen una norma fija (Teorema 4.17(c)). Entonces por la finitud de números enteros menores que la constante $M_{s,\,t}\sqrt{|\Delta|}$ y por la finitud de ideales de norma fija, se tiene la finitud del orden del grupo de clases, esto es $|\mathcal{H}| = h$ es finito. □

5.3. Cálculo de grupo de clases y número de clases

En general, en el cálculo de número de clases se pueden usar teoría elemental de grupos abelianos, como que el orden de un elemento divide al orden del grupo. También nos serviremos de resultados más precisos, como por ejemplo el Teorema 4.18 que nos muestra cual es la descomposición de los ideales generados por números primos, y el siguiente resultado:

Teorema 5.12. *Sea $\mathfrak{O}$ el anillo de enteros de un cuerpo de números K de grado $n = s+2t$. Supongamos que para todo primo $p \in \mathbb{Z}$ con*

$$p \leq M_{s,\,t}\sqrt{|\Delta|}$$

(siendo Δ el discriminante de K), que todo ideal primo dividiendo a $\langle p\rangle$ es principal. Entonces $\mathfrak{O}$ tiene número de clase $h = 1$.

Demostración. Toda clase de ideales fraccionales contiene un ideal $\mathfrak{a}$ con $N(\mathfrak{a}) \leq M_{s,\,t}\sqrt{|\Delta|}$. Ahora

$$N(\mathfrak{a}) = p_1 \cdots p_k$$

donde $p_1 \ldots, p_k \in \mathbb{Z}$ y $p_i \leq M_{s,\,t}\sqrt{|\Delta|}$; y $\mathfrak{a}|N(\mathfrak{a})$, así que $\mathfrak{a}$ es producto de ideales primos, cada uno de ellos dividiendo a algún p_i. Por hipótesis estos ideales son principales, así que $\mathfrak{a}$ es principal. Por lo que todas las clases de ideales fraccionales son iguales a $\overline{\mathfrak{O}}$, y $h = 1$. □

Este resultado, de manera práctica, es útil para determinar cuando un anillo de enteros de un cuerpo de números es un dominio de factorización única. Caso de no serlo, también estamos ya en condiciones de calcular el grupo de clases de alguno de los tipos de cuerpos de números que hemos utilizado a lo largo de la memoria. En el Anexo se muestra una tabla donde se recogen, de forma resumida, los cálculos correspondientes a diversos anillos de enteros. A continuación, desarrollamos algunos casos de especial relevancia:

Ejemplo 5.13. $\mathbb{Q}(\sqrt{-26})$.

Al ser $-26 \equiv 2\,(\text{mód}\,4)$ tenemos que $\mathfrak{O}_{\mathbb{Q}(\sqrt{-26})} = \mathbb{Z}[\sqrt{-26}]$. Por tanto una base entera es $\{1,\, \sqrt{-26}\}$ y el discriminante vale $\Delta = 4d = 4(-26) = -104$. Los distintos $\mathbb{Q}$-homomorfismos de $\mathbb{Q}(\sqrt{-26})$ son complejos y entonces $s = 0$ y $t = 1$.

$$\left(\frac{4}{\pi}\right)\frac{2!}{2^2}M_{01}\sqrt{|-104|} < 7.$$

El Teorema 5.10, nos dice que todo ideal fraccional no nulo es equivalente a un ideal de norma menor que 7. Pasamos a la descomposición en primos de los ideales generados por $2, 3$ y 5 (usando el Teorema 4.18). Como el anillo de enteros está generado por $\theta = \sqrt{-26}$, el teorema requiere del polinomio irreducible de θ sobre $\mathbb{Q}$, que es

$$f(t) = Irr(\sqrt{-26}, \mathbb{Q}) = t^2 - T(\sqrt{-26})t + N(\sqrt{-26}) = t^2 + 26.$$

Ahora descomponemos en irreducibles el polinomio en los distintos $\mathbb{Z}_p[t]$:

$\mathbb{Z}_2[t]:$ $\quad \overline{f(t)} = \overline{t^2} = \bar{t}^2$ $\quad$ luego $\quad \langle 2\rangle = \langle 2,\, \sqrt{-26}\rangle^2 = \mathfrak{p}^2$

$\mathbb{Z}_3[t]:$ $\quad \overline{f(t)} = \overline{t^2 - 1} = \overline{(t+1)}\,\overline{(t-1)}$ $\quad$ luego $\quad \langle 3\rangle = \langle 3,\, 1 + \sqrt{-26}\rangle\langle 3,\, 1 - \sqrt{-26}\rangle = \mathfrak{q}_1\mathfrak{q}_2$

$\mathbb{Z}_5[t]:$ $\quad \overline{f(t)} = \overline{t^2 + 1} = \overline{(t+2)}\,\overline{(t-2)}$ $\quad$ luego $\quad \langle 5\rangle = \langle 5,\, 2 + \sqrt{-26}\rangle\langle 5,\, 2 - \sqrt{-26}\rangle = \mathfrak{r}_1\mathfrak{r}_2$

Además, el único ideal primo que contiene a 2 es $\mathfrak{p}$, ya que si otro ideal $\mathfrak{a}$ contiene a 2, entonces $\mathfrak{a}\,|2$ pero esto es $\mathfrak{a}\,|\mathfrak{p}^2$ con lo que $\mathfrak{a} = \mathfrak{p}$. Lo mismo pasa con 2 y 5. Entonces todo ideal es equivalente a alguno de los siguientes,

$$\overline{1}, \overline{\mathfrak{p}}, \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_2}, \overline{\mathfrak{r}_1}, \overline{\mathfrak{r}_2}, \overline{\mathfrak{p}\mathfrak{q}_1}, \overline{\mathfrak{p}\mathfrak{q}_2}.$$

Es decir $h \leq 8$. Un hecho fundamental, es que $N(\mathfrak{p}) = 2$, ya que divide a $N(\mathfrak{p})^2 = N(\langle 2\rangle) = 4$. Fijemonos que los ideales que son equivalentes a uno de norma cuatro, necesariamente lo son a $\mathfrak{p}^2 = \langle 2\rangle$, y esto nos dice $\overline{\mathfrak{p}}^2 = \overline{\mathfrak{p}^2} = \overline{1}$. En $\mathbb{Z}[\sqrt{-26}]$ la norma de un elemento $\alpha = a + b\sqrt{-26}$ viene dada por $N(\alpha) = a^2 + 26b^2$, y lo que nos preguntamos ahora es si alguno de los ideales anteriores es principal. Para ello nos facilitamos la tarea con el Corolario 4.14 que nos dice

$$N(\langle\gamma\rangle) = |N(\gamma)|,$$

y como los coeficientes $a, b \in \mathbb{Z}$, entonces no hay elementos de norma 2,3,5 ni 6 en $\mathbb{Z}[\sqrt{-26}]$, y por tanto

$$\overline{\mathfrak{p}}, \overline{\mathfrak{q}_1}, \overline{\mathfrak{q}_2}, \overline{\mathfrak{r}_1}, \overline{\mathfrak{r}_2}, \overline{\mathfrak{p}\mathfrak{q}_1}, \overline{\mathfrak{p}\mathfrak{q}_2} \neq \overline{1}$$

es decir $h \geq 2$. Además como $\overline{\mathfrak{p}} \neq \overline{1}$ y $\overline{p}^2 = \overline{1}$, entonces por propiedades elementales de grupos (el orden de un elemento divide al orden del grupo) tenemos que $2|h$.
En $\mathbb{Z}[\sqrt{-26}]$ tampoco hay elementos de norma 6, por lo que el ideal $\mathfrak{p}\mathfrak{q}_1$ no puede ser principal, es decir $\overline{\mathfrak{p}\mathfrak{q}_1} \neq \overline{1}$, y como el inverso de $\overline{\mathfrak{p}}$ es el mismo, tenemos que $\overline{\mathfrak{q}_1} \neq \overline{\mathfrak{p}}$ y entonces $h \geq 3$, al ser h múltiplo de 2, tenemos que $h \geq 4$. Veamos ahora cual es el orden de $\overline{\mathfrak{q}_1}$. En $\mathbb{Z}[\sqrt{-26}]$ los únicos elementos de norma 9 que hay son ± 3, y $\mathfrak{q}_1^2 \neq \mathfrak{q}_1\mathfrak{q}_2 = \langle 3\rangle$, así que $\overline{\mathfrak{q}_1^2} \neq \overline{1}$.

$$\begin{aligned}\mathfrak{q}_1^2 &= \langle 3,\, 1+\sqrt{-26}\rangle\langle 3,\, 1+\sqrt{-26}\rangle = \langle 9,\, 3+3\sqrt{-26},\, -25+2\sqrt{-26}\rangle \\ &= \langle 9,\, 3+3\sqrt{-26},\, 2+2\sqrt{-26}\rangle = \langle 9,\, 1+\sqrt{-26}\rangle.\end{aligned}$$

$$\begin{aligned}\mathfrak{q}_1^3 &= \langle 3,\, 1+\sqrt{-26}\rangle\langle 9,\, 1+\sqrt{-26}\rangle = \langle 27,\, 3+3\sqrt{-26},\, -25+2\sqrt{-26}\rangle \\ &= \langle 27,\, 3+3\sqrt{-26},\, 2+2\sqrt{-26}\rangle = \langle 27,\, 1+\sqrt{-26}\rangle = \langle 1+\sqrt{-26}\rangle.\end{aligned}$$

Luego el orden de $\mathfrak{q}_1$ es 3. Tenemos las siguientes condiciones para h, $4 \leq h \leq 8$, $2, 3|h$ por tanto $h = 6$ y entonces $\mathcal{H} \cong \mathbb{Z}_6$. Además tenemos identificados un elemento de norma 2 y un elemento de norma 3, por lo que conocemos enteramente el grupo $\mathcal{H}$

$$\mathcal{H} = \{\overline{1}, \overline{\mathfrak{p}\mathfrak{q}_1}, \overline{\mathfrak{q}_1^2}, \overline{\mathfrak{p}}, \overline{\mathfrak{q}_1}, \overline{\mathfrak{p}\mathfrak{q}_1^2}\}$$

□

Ejemplo 5.14. $\mathbb{Q}(\sqrt{17})$.

Como $17 \equiv 1 \,(\text{mód}\, 4)$, entonces $\mathfrak{O}_{\mathbb{Q}(\sqrt{17})} = \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ y una base entera es $\{1, \frac{1+\sqrt{17}}{2}\}$, con discriminante $\Delta = d = 17$.
Los dos $\mathbb{Q}$-homomorfismos son reales, por lo que $s = 2$ y $t = 0$.

$$\left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2} M_{20}\sqrt{17} < 3$$

El Teorema 5.10, nos dice que todo ideal fraccional no nulo es equivalente a un ideal de norma menor que 3. Por tanto sólo tenemos que calcular los primos de norma dos que hay en $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ y para ello usamos el Teorema 4.18. En este caso el generador del anillo de enteros es $\theta = \frac{1+\sqrt{17}}{2}$, y su irreducible viene dado por

$$f(t) = Irr(\frac{1+\sqrt{17}}{2}, \mathbb{Q}) = t^2 - T(\frac{1+\sqrt{17}}{2})t + N(\frac{1+\sqrt{17}}{2}) = t^2 - t - 4.$$

Pasamos a irreducibles en $\mathbb{Z}_2[t]$:

$$\overline{f(t)} = \overline{(t^3+t)} = \bar{t}\,\overline{(t+1)} \qquad \text{luego} \qquad \langle 2\rangle = \langle 2,\ \frac{1+\sqrt{17}}{2}\rangle\langle 2,\ \frac{3+\sqrt{17}}{2}\rangle = \mathfrak{pq}.$$

Luego todo ideal es equivalente a uno de los siguientes

$$\overline{1}, \overline{\mathfrak{p}}, \overline{\mathfrak{q}}$$

y $h \leq 3$. Nos preguntamos ahora si $\mathfrak{p}$ o $\mathfrak{q}$ son principales. Un elemento $\alpha = \frac{a+b\sqrt{17}}{2} \in \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ tiene norma

$$N(\alpha) = \frac{a^2 - 17b^2}{4},$$

y la norma de un ideal principal viene dada por $N(\langle\gamma\rangle) = |N(\gamma)|$, luego buscamos $a, b \in \mathbb{Z}$ tales que $\frac{a^2-17b^2}{4} = \pm 2$. Observamos que $N(\frac{3+\sqrt{17}}{2}) = -2$, luego

$$\mathfrak{q} = \langle \frac{3+\sqrt{17}}{2}\rangle$$

y $\overline{\mathfrak{q}} = \overline{1}$. Además Luego $h = 1$ y $\mathcal{H} = \{1\}$. Siendo $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ dominio de ideales principales y por el Teorema 5.9 un dominio de factorización única.

$$\overline{\mathfrak{p}} = \overline{\mathfrak{p}}\,\overline{1} = \overline{\mathfrak{p}}\,\overline{\mathfrak{q}} = \overline{\mathfrak{pq}} = \overline{1}.$$

□

Ejemplo 5.15. $\mathbb{Q}(e^{2\pi i/7})$.

Para simplificar la notación, llamaremos $\xi = e^{2\pi i/7}$. Por el Teorema 2.8, $\mathfrak{O}_{\mathbb{Q}(\xi)} = \mathbb{Z}[\xi]$, por lo que una base entera es $\{1, \xi, \ldots, \xi^6\}$. El discriminante lo calculamos utilizando la fórmula:

$$\Delta = (-1)^{(p-1)/2} p = p - 2 = (-1)^{6/2}\, 7^{(7-2)} = -7^5.$$

Y considerando los distintos $\mathbb{Q}$-homomorfismos, se puede ver que $s = 0$ y $t = 3$, por lo que

$$\left(\frac{4}{\pi}\right)^3 \frac{6!}{6^6} M_{03} \sqrt{|-7^5|} < 5.$$

Por el Teorema 5.10, todo ideal fraccional es equivalente a un ideal de norma menor o igual a 5.
El irreducible de ξ sobre $\mathbb{Q}$ es

$$f(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t^1 + 1.$$

Pasamos a descomponer f en irreducibles sobre $\mathbb{Z}_p[t]$ para $p = 2, 3$:

$$\begin{array}{lll} \mathbb{Z}_2[t]: & \overline{f(t)} = \overline{(t^3+t^2+1)}\,\overline{(t^3+t+1)} & \text{luego} \quad \langle 2\rangle = \langle 2, \xi^3+\xi^2+1\rangle\langle 2,\ \xi^3+\xi+1\rangle = \mathfrak{pq} \\ \mathbb{Z}_3[T]: & \overline{f(t)} \text{ es irreducible en } \mathbb{Z}_3[t] & \text{luego} \quad \langle 3\rangle \text{ es primo} \end{array}$$

Todo ideal de $\mathbb{Z}[\xi]$ es equivalente a uno de los siguientes

$$1, \mathfrak{p}, \mathfrak{q}$$

Luego $h \leq 3$.
Operando sobre $\mathbb{Z}[t]$ tenemos

$$f(t) = (t^3 + t^2 + 1)(t^3 + t + 1) - 2t^3$$

de donde sacamos la igualdad

$$(\xi^3 + \xi^2 + 1)(\xi^3 + \xi + 1) = 2\xi^3.$$

De la anterior expresión, tenemos que

$$2 = 2\xi^3\xi^3 = \xi^3(\xi^3 + \xi^2 + 1)(\xi^3 + \xi + 1),$$

por lo que

$$2 \in \langle \xi^3 + \xi^2 + 1 \rangle \qquad \text{y} \qquad 2 \in \langle \xi^3 + \xi + 1 \rangle,$$

lo que implica que

$$\mathfrak{p} = \langle \xi^3 + \xi^2 + 1 \rangle \qquad \text{y} \qquad \mathfrak{q} = \langle \xi^3 + \xi + 1 \rangle.$$

Como resultado, tenemos que $\overline{\mathfrak{p}} = \overline{\mathfrak{q}} = \overline{1}$, y que $h = 1$ y $\mathcal{H} = \{1\}$. Siendo entonces $\mathbb{Z}[\xi]$ un dominio de ideales principales y por tanto un dominio de factorización única.

Anexo

Cuerpo	$\mathfrak{O}_K$	Δ	s	t	$M_{st}\sqrt{\lvert\Delta\rvert}<$	Factorización de los $\langle p\rangle$	$\mathcal{H}$	h
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Z}[\sqrt{-1}]$	4	0	1	2		$\{1\}$	1
$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Z}[\sqrt{-2}]$	-8	0	1	3	$\langle 2\rangle = \langle 2, \sqrt{-2}\rangle^2$	$\{1\}$	1
$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$	-3	0	1	2		$\{1\}$	1
$\mathbb{Q}(\sqrt{-5})$	$\mathbb{Z}[\sqrt{-5}]$	-20	0	1	4	$\langle 2\rangle = \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle$ $\langle 3\rangle$ es primo	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{-6})$	$\mathbb{Z}[\sqrt{-6}]$	-24	0	1	4	$\langle 2\rangle = \langle 2, \sqrt{-6}\rangle^2$, $\langle 3\rangle = \langle 3, \sqrt{-6}\rangle^2$	$\mathbb{Z}_2$	1
$\mathbb{Q}(\sqrt{-7})$	$\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$	-7	0	1	2		$\{1\}$	1
$\mathbb{Q}(\sqrt{-10})$	$\mathbb{Z}[\sqrt{-10}]$	-40	0	1	6	$\langle 2\rangle = \langle 2, \sqrt{-10}\rangle^2$, $\langle 3\rangle$ es primo, $\langle 5\rangle = \langle 5, \sqrt{-10}\rangle^2$	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{-11})$	$\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$	-11	0	1	3	$\langle 2\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Z}[\sqrt{-13}]$	-52	0	1	5	$\langle 2\rangle = \langle 2, 1+\sqrt{-13}\rangle^2$, $\langle 3\rangle$ es primo	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{-14})$	$\mathbb{Z}[\sqrt{-14}]$	-56	0	1	5	$\langle 2\rangle = \langle 2, \sqrt{-14}\rangle^2$, $\langle 3\rangle = \langle 3, 1+\sqrt{-14}\rangle\langle 3, 1-\sqrt{-14}\rangle$	$\mathbb{Z}_4$	4
$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$	-15	0	1	3	$\langle 2\rangle = \langle 2, \frac{1+\sqrt{-15}}{2}\rangle\langle 2, \frac{1-\sqrt{-15}}{2}\rangle$	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{-17})$	$\mathbb{Z}[\sqrt{-17}]$	-68	0	1	6	$\langle 2\rangle = \langle 2, 1+\sqrt{-17}\rangle^2$, $\langle 3\rangle = \langle 3, 1+\sqrt{-17}\rangle\langle 3, 1-\sqrt{-17}\rangle$, $\langle 5\rangle$ es primo	$\mathbb{Z}_4$	4
$\mathbb{Q}(\sqrt{-19})$	$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$	-19	0	1	3	$\langle 2\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{-21})$	$\mathbb{Z}[\sqrt{-21}]$	-84	0	1	6	$\langle 2\rangle = \langle 2, 1+\sqrt{-21}\rangle^2$, $\langle 3\rangle = \langle 3, \sqrt{-21}\rangle^2$, $\langle 5\rangle = \langle 5, 2+\sqrt{-21}\rangle\langle 5, 2-\sqrt{-21}\rangle$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
$\mathbb{Q}(\sqrt{-22})$	$\mathbb{Z}[\sqrt{-22}]$	-88	0	1	6	$\langle 2\rangle = \langle 2, \sqrt{-22}\rangle^2$, $\langle 3\rangle$ es primo, $\langle 5\rangle$ es primo	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{-23})$	$\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$	-23	0	1	4	$\langle 2\rangle = \langle 2, \frac{1+\sqrt{-15}}{2}\rangle\langle 2, \frac{1-\sqrt{-15}}{2}\rangle$, $\langle 3\rangle = \langle 3, \frac{1+\sqrt{-15}}{2}\rangle\langle 3, \frac{1-\sqrt{-15}}{2}\rangle$	$\mathbb{Z}_3$	3
$\mathbb{Q}(\sqrt{-26})$	$\mathbb{Z}[\sqrt{-26}]$	-104	0	1	7	$\langle 2\rangle = \langle 2, \sqrt{-26}\rangle$, $\langle 3\rangle = \langle 3, 1+\sqrt{-26}\rangle\langle 3, 1-\sqrt{-26}\rangle$, $\langle 5\rangle = \langle 5, 2+\sqrt{-26}\rangle\langle 5, 2-\sqrt{-26}\rangle$	$\mathbb{Z}_6$	6

Cuerpo	$\mathfrak{O}_K$	Δ	s	t	$M_{st}\sqrt{\lvert\Delta\rvert} <$	Factorización de los $\langle p\rangle$	$\mathcal{H}$	h
$\mathbb{Q}(\sqrt{-29})$	$\mathbb{Z}[\sqrt{-29}]$	-116	0	1	7	$\langle 2\rangle = \langle 2,\ 1+\sqrt{-29}\rangle^2$, $\langle 3\rangle = \langle 3,\ 1+\sqrt{-29}\rangle\langle 3,\ 1-\sqrt{-29}\rangle$, $\langle 5\rangle = \langle 5,\ 1+\sqrt{-29}\rangle\langle 5,\ 1-\sqrt{-29}\rangle$	$\mathbb{Z}_6$	6
$\mathbb{Q}(\sqrt{-30})$	$\mathbb{Z}[\sqrt{-30}]$	-120	0	1	7	$\langle 2\rangle = \langle 2,\ \sqrt{-30}\rangle^2$, $\langle 3\rangle = \langle 3, \sqrt{-30}\rangle^2$, $\langle 5\rangle = \langle 5, \sqrt{-30}\rangle^2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
$\mathbb{Q}(\sqrt{2})$	$\mathbb{Z}[\sqrt{2}]$	8	2	0	2		$\{1\}$	1
$\mathbb{Q}(\sqrt{3})$	$\mathbb{Z}[\sqrt{3}]$	12	2	0	2		$\{1\}$	1
$\mathbb{Q}(\sqrt{5})$	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	5	2	0	2		$\{1\}$	1
$\mathbb{Q}(\sqrt{6})$	$\mathbb{Z}[\sqrt{6}]$	24	2	0	3	$\langle 2\rangle = \langle 2,\ \sqrt{6}\rangle^2$	$\{1\}$	1
$\mathbb{Q}(\sqrt{7})$	$\mathbb{Z}[\sqrt{7}]$	28	2	0	3	$\langle 2\rangle = \langle 2,\ 1+\sqrt{7}\rangle^2$	$\{1\}$	1
$\mathbb{Q}(\sqrt{10})$	$\mathbb{Z}[\sqrt{10}]$	40	2	0	4	$\langle 2\rangle = \langle 2,\ \sqrt{10}\rangle^2$, $\langle 3\rangle = \langle 3,\ 1+\sqrt{10}\rangle\langle 3,\ 1-\sqrt{10}\rangle$	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{11})$	$\mathbb{Z}[\sqrt{11}]$	44	2	0	4	$\langle 2\rangle = \langle 2,\ 1+\sqrt{11}\rangle^2$, $\langle 3\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{13})$	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	13	2	0	2		$\{1\}$	1
$\mathbb{Q}(\sqrt{14})$	$\mathbb{Z}[\sqrt{14}]$	56	2	0	4	$\langle 2\rangle = \langle 2,\ \sqrt{14}\rangle^2$, $\langle 3\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{15})$	$\mathbb{Z}[\sqrt{15}]$	60	2	0	4	$\langle 2\rangle = \langle 2,\ 1+\sqrt{15}\rangle^2$ $\langle 3\rangle = \langle 3,\ \sqrt{15}\rangle^2$	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{17})$	$\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$	17	2	0	3	$\langle 2\rangle = \langle 2,\ \frac{1+\sqrt{17}}{2}\rangle\langle 2,\ \frac{1-\sqrt{17}}{2}\rangle$	$\{1\}$	1
$\mathbb{Q}(\sqrt{19})$	$\mathbb{Z}[\sqrt{19}]$	76	2	0	5	$\langle 2\rangle = \langle 2,\ 1+\sqrt{19}\rangle^2$, $\langle 3\rangle = \langle 3,\ 1+\sqrt{19}\rangle\langle 3,\ 1-\sqrt{19}\rangle$	$\{1\}$	1
$\mathbb{Q}(\sqrt{21})$	$\mathbb{Z}[\frac{1+\sqrt{21}}{2}]$	21	2	0	3	$\langle 2\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{22})$	$\mathbb{Z}[\sqrt{22}]$	88	2	0	5	$\langle 2\rangle = \langle 2,\ \sqrt{22}\rangle^2$, $\langle 3\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{23})$	$\mathbb{Z}[\sqrt{23}]$	92	2	0	5	$\langle 2\rangle = \langle 2,\ 1+\sqrt{22}\rangle^2$ $\langle 3\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{26})$	$\mathbb{Z}[\sqrt{26}]$	104	2	0	6	$\langle 2\rangle = \langle 2,\ \sqrt{26}\rangle^2$, $\langle 3\rangle$ es primo, $\langle 5\rangle = \langle 5,\ 1+\sqrt{26}\rangle\langle 5,\ 1-\sqrt{26}\rangle$	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{29})$	$\mathbb{Z}[\frac{1+\sqrt{29}}{2}]$	29	2	0	3	$\langle 2\rangle$ es primo	$\{1\}$	1
$\mathbb{Q}(\sqrt{30})$	$\mathbb{Z}[\sqrt{30}]$	120	2	0	6	$\langle 2\rangle = \langle 2,\ \sqrt{30}\rangle^2$, $\langle 3\rangle = \langle 3,\ \sqrt{30}\rangle^2$, $\langle 5\rangle = \langle 5,\ \sqrt{30}\rangle^2$	$\mathbb{Z}_2$	2
$\mathbb{Q}(\sqrt{22})$	$\mathbb{Z}[\sqrt{22}]$	88	2	0	5	$\langle 2\rangle = \langle 2,\ 1+\sqrt{7}\rangle^2$	$\{1\}$	1
$\mathbb{Q}(e^{2\pi i/3})$	$\mathbb{Z}[e^{2\pi i/3}]$	-9	0	1	2		$\{1\}$	1
$\mathbb{Q}(e^{2\pi i/5})$	$\mathbb{Z}[e^{2\pi i/5}]$	125	0	2	2		$\{1\}$	1
$\mathbb{Q}(e^{2\pi i/7})$	$\mathbb{Z}[e^{2\pi i/7}]$	7^5	0	3	5	Si $\xi = e^{2\pi i/7}$, $\langle 2\rangle = \langle \xi^3+\xi+1\rangle\langle \xi^3+\xi^2+1\rangle$, $\langle 3\rangle$ es primo	$\{1\}$	1

Cuerpo	$\mathfrak{O}_K$	Δ	s	t	$M_{st}\sqrt{\lvert\Delta\rvert} <$	Factorización de los $\langle p\rangle$	$\mathcal{H}$	h
$\mathbb{Q}(\sqrt{5},\sqrt{-3})$	-	-225	2	1	2		$\{1\}$	1
$\mathbb{Q}(\sqrt[3]{2})$	$\mathbb{Z}[\sqrt[3]{2}]$	-108	1	1	3	$\langle 2\rangle = \langle\sqrt[3]{2}\rangle^3$	$\{1\}$	1

Bibliografía

[1] Asensio Mayor, José; Caruncho Castro, José Ramón y Martínez Hernández, Juan: *Ecuaciones Algebraicas*. ICE, Universidad de Murcia - Diego Marín, 2002.

[2] Garling, D.J.H.: *A Course in Galois Theory*. Cambridge University Press, Cambridge, 1986.

[3] Marcus A.: *Number Fields*. Springer-Velag, New York, 1987.

[4] Stewart, Ian: *Galois Theory*. Chapman and Hall, London, 1973.

[5] Stewart, Ian y Tall, David: *Algebraic Number Theory and Fermat's Last Theorem*. (3ª Ed.) A K Peters, Massachusetts, 1994.