El teorema de las unidades de Dirichlet

Andrés Bernal Sisamón

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza
Curso 2017/2018

Director del trabajo: Javier Otal Cinca

Prólogo

El objetivo de este trabajo es dar la demostración de uno de los más destacados resultados en *Teoría Algebraica de Números* atribuido al prolífico matemático alemán Peter Dirichlet (1805-1859), conocido como *El Teorema de las unidades* y cuyo enunciado es el resultado siguiente.

Teorema A *El grupo abeliano formado por las unidades del anillo de enteros de un cuerpo de números está finitamente generado.*

A continuación presentamos una breve descripción de los términos involucrados en el resultado que permitan situarlo y comprenderlo.

Un cuerpo de números es una extensión finita K del cuerpo racional $\mathbb{Q}$. Todo elemento de K es raíz de un polinomio $p(X) \in \mathbb{Q}[X]$, luego K se trata de una *extensión algebraica* y sus elementos son *números algebraicos*. Se demuestra que para todo $\alpha \in K$ existe un único polinomio irreducible $m_\alpha(X) \in \mathbb{Q}[X]$, denominado *polinomio minimo de* α. Se dice que α *es un entero algebraico* (sobre $\mathbb{Q}$) si $m_\alpha(X) \in \mathbb{Z}[X]$ y es mónico.

Los enteros algebraicos del cuerpo de números K forman un anillo $\mathcal{O}_K$ (conmutativo y con unidad) que se puede demostrar que es un grupo abeliano libre cuyo rango es el grado $[K:\mathbb{Q}] = n$. Por el teorema del elemento primitivo, una extensión finita del cuerpo $\mathbb{Q}$ puede escribirse de la forma $K = \mathbb{Q}(\theta)$ con $\theta \in K$; de hecho se puede elegir θ de modo que sea un entero algebraico. Para dicho θ, el polinomio $m_\theta(X)$ tiene n raíces distintas en $\mathbb{C}$, conformadas por r raíces reales y $2s$ raíces complejas (ya que deben ser conjugadas dos a dos) tal que $n = r + 2s$. En función de estos parámetros el *Teorema de las unidades de Dirichlet* se puede enunciar de manera explícita como sigue.

Teorema B *El grupo abeliano $\mathcal{O}_K^*$ de las unidades del anillo de enteros $\mathcal{O}_K$ del cuerpo de números K está finitamente generado y es de la forma*

$$\mathcal{O}_K^* = L_K \times T_K,$$

donde L_K es un grupo abeliano libre de rango $r+s-1$ y T_K es un grupo cíclico finito de orden par formado por las raíces de la unidad que pertenecen a K.

La demostración del Teorema B constituye el objetivo de este trabajo. Indicamos concisamente la organización de su contenido.

El Capítulo 1 tiene carácter introductorio y en él se definen los elementos esenciales del teorema: un *cuerpo de números* y su *anillo de enteros*. Describimos brevemente estas estructuras así como sus propiedades mas relevantes para nuestro estudio (han sido estudiadas ampliamente en asignaturas del grado). Para una mejor comprensión de los objetivos de este trabajo, estudiamos el caso mas sencillo por pequeño, esto es, los *cuerpos cuadráticos* (extensiones de grado 2).

El Capítulo 2 es auxiliar y detalla la técnica a través de la cual se apoya la demostración del teorema de las unidades en la mayoría de los textos que se dedican a ello, sino en todos ellos, al menos en los que hemos usado. Básicamente consiste en representar geométricamente un cuerpo de números por medio de lo que se denomina *espacio logarítmico*. Para ello juegan un papel muy destacado los $\mathbb{Q}$–homomorfismos (que son incrustaciones) del cuerpo de números en el cuerpo complejo determinados por las raíces del polinomio mínimo del elemento generador del cuerpo de números. Se trata pues de una

incursión en la *Teoría Geométrica de Números* que no tiene carácter exhaustivo sino que únicamente busca dotarse de los resultados técnicos necesarios para la demostración del Teorema.

Ésta se lleva a cabo en el Capítulo 3, que constituye el núcleo central del trabajo ya que en él se procede a la demostración detallada del *Teorema de las unidades*.

Summary

The aim of this paper is to demonstrate the *Dirichlet´s unit theorem* . The demonstration that we expose here requires, at least in general terms, basic knowledge in *algebraic number theory* and *geometric number theory*. We study these results in the first and second chapters. The third (and last) chapter is dedicated entirely to the *unit theorem demonstration*.

The first chapter has an introductory and auxiliary nature. We have thought for this study review, in an immersive way, the algebraic structures that take part in the *unit theorem*.

A *group* is no more than a non-empty set G endowed with a binary operation $(\cdot) : G \times G \to G; (a,b) \to a \cdot b$, wich is *associative*, has a *neutral element* (denoted by 1) and an *inverse element* for any $a \in G$ denoted by a^{-1}, such that $a \cdot a^{-1} = 1$. For this survey we will consider the groups with $(\cdot)$ *commutative*, called *abelian groups*. *Finitely generated groups* ($G = \langle S \rangle$, $S \leq G$) and *cyclic groups* ($G = \langle x \rangle$, $x \in G$) will also have a significant presence in our work.

If G is a finitely generated abelian group, then $G = L(G) \oplus T(G)$, where $L(G)$ y $T(G)$ are the *free torsion part* and the *torsion part* of G respectively. Remember that a group H is said to be *torsion group* if $\forall a \in H \ \exists n \in \mathbb{N}$ such that $a^n = 1$ (n is called the *order of* a), while H is said to be *torsion free* if all its elements have infinite order.

In addition, we can descompose $L(G)$ as direct sum of infinite cyclic groups and $T(G)$ as direct sum of finite cyclic groups. These results determine the structure of *finitely generated abelian groups* and will have an important rol in the *unit theorem demonstration*.

A *ring* is a non-empty set A endowed with a sum operation $(+) : A \times A \to A, (a,b) \to a+b$ and a product operation $(\cdot) : A \times A \to A, (a,b) \to a \cdot b$, such that $(A,+)$ is an abelian group and $(\cdot)$ is associative and distributive respect to the $(+)$. In this survey we work with *commutative rings with identity*, that is, $a \cdot b = b \cdot a \ \ (\forall a,b \in A)$ and there exists a *nuetral element* for $(\cdot)$ denoted by 1 such that $a \cdot 1 = a \ \ (\forall a \in A)$. An element $u \in A$ is a *unit* if there is only one $v \in A$ verifying $u \cdot v = 1$; v is called the *inverse* of u and is denoted by $v = u^{-1}$. The unit set of a ring A is denoted by A^* and has group structure with the multiplication.

A *field* is basically a ring K whose multiplicative group $K^* = K \setminus \{0\}$ is formed by all its non-zero elements. A field L is said to be an *extension of* K if $K \subseteq L$, we will write it as L/K. In this work we focus in *number fields*, which are *finite extensions* over the rational field $\mathbb{Q}$. Then, a *number field extension* $K/\mathbb{Q}$ is said to be *algebraic* since $\forall \alpha \in K$ exists a polynomial $p(X) \in K[X]$ such that $p(\alpha) = 0$, and any element of K is said to be *algebraic*. If $p(X)$ is monic and with the least degree, then it is the *minimal polyomial of* α *over* $\mathbb{Q}$.

By the *primitive element theorem* we can express any *number field* as $K = \mathbb{Q}(\alpha)$ with $\alpha \in K$; moreover we can choose α to be algebraic. Let $p_\alpha(X)$ be the minimal polynomial of α of degree n, then there are n distinct homomorphisms $\sigma_i : K \to \mathbb{C}$. These maps are called the *n-embeddings* of K in $\mathbb{C}$ and are determined by the n distinct roots (real or complex) of $p_\alpha(X)$ in $\mathbb{C}$.

A complex number θ is an *algebraic integer* if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. There is an algebraic number ϕ such that $\phi = c\alpha \ \ (c \in \mathbb{Z})$, so we can express any field as $K = \mathbb{Q}(\alpha)$ with α algebraic integer. We proof that the subset of the algebraic integers of K has a ring structure and

is denoted by $\mathcal{O}_K$. In adittion, we write $\mathcal{O}_K^*$ for the unit subgroup of $\mathcal{O}_K$.

The end of Chapter 1 is dedicated to the study of *quadratic fields*. A *quadratic field* can be write as $K = \mathbb{Q}\left(\sqrt{d}\right)$ with d a *free square integer*. We will show results about which are their algebraic integer rings $\mathcal{O}_K$ and its unit subgroups $\mathcal{O}_K^*$.

In the second chapter we make a brief but complete entrance into *geometric number theory*. The purpose of this chapter is to provide us with the necessary tools to be able to demonstrate the central theorem in Chapter 3.

A *lattice L of degree m* in $\mathbb{R}^n$ $(m \leq n)$ is a mathematical structure generated additively by a family of vectors $\{e_1, \ldots, e_m\}$ linearly independent in $\mathbb{R}^n$. It is clear that a lattice has an *abelian free group structure*, so for any $e \in L$ there is only one tuple $(a_1, \ldots, a_m)$ in $\mathbb{Z}^m$ such that $e = a_1 e_1 + \cdots + a_m e_m$; so there is an isomorphism between L and $\mathbb{Z}^n$.

We will proof that an additive subgroup of $\mathbb{R}^m$ is a *lattice* if and only if it is *discrete*. Remember that a set is said to be *discrete* if intersects in a finite set with all closed ball centered in the origin (note that this result matchs abelian group theory and lattice theory).

Let $K = \mathbb{Q}(\theta)$ be a field with θ algebraic integer and let $p(X)$ be its minimal polynomial. If $p(X)$ has s real roots and t conjugated pairs of complex roots, then the associated reticulated space for K is:

$$\mathbb{L}^{st} = \mathbb{R}^s \times \mathbb{C}^t$$

Any element of $\mathbb{L}^{st}$ is given by one tuple like $(x_1, \cdots, x_s, y_1 + iz_1, \cdots, y_t + iz_t)$ with $x_i, y_i, z_i \in \mathbb{R}$.

Now we can define for any field K an *standard map* $\sigma : K \to \mathbb{L}^{st}$, which assigns for each element of K its value in the n-embeddings $K \to \mathbb{C}$, that is, in the space $\mathbb{L}^{st}$.

The end of the Chapter 2 is dedicated to define the logarithmic space associated to a field K and to describe the method that links K to that space. Consider the n-embeddings that define K with the descomposition $n = s + 2t$, then the logarithmic space of K is the vector space $\mathbb{R}^{s+t}$.

Now, we define:

$$\begin{gathered} l : \mathbb{L}^{st} \longrightarrow \mathbb{R}^{s+t} \\ x \longmapsto (l_1(x), \cdots, l_s(x), l_{s+1}(x), \cdots, l_{s+t}(x)) \end{gathered}$$

such that for any $x = (x_1, \cdots, x_s, x_{s+1}, \cdots, x_{s+t}) \in \mathbb{L}^{st}$, each component of l is given by:

$$l_k(x) = \begin{cases} log\,|x_k| & for \text{ k=1,...,s} \\ log|x_k|^2 & for \text{ k=s+1,...,s+t} \end{cases}$$

The next step is to establish a bijective correspondence between any field K and the space $\mathbb{L}^{st}$ throught its *standard map* σ. We identify any $\alpha \in K$ with the $s + 2t$ homomorphisms that define K for that α:

$$\alpha = \sigma(\alpha) = \underbrace{\sigma_1(\alpha), \cdots, \sigma_s(\alpha)}_{\mathbb{R}}, \underbrace{\sigma_{s+1}(\alpha), \cdots, \sigma_{s+t}(\alpha)}_{\mathbb{C}}$$

Applying this identification, we redefine the map l as follows:

$$\begin{gathered} l : K \longrightarrow \mathbb{L}^{st} \longrightarrow \mathbb{R}^{s+t} \\ l(\alpha) \longmapsto l(\sigma(\alpha)) \longmapsto \left(log\,|\sigma_1(\alpha)|, \ldots, log\,|\sigma_s(\alpha)|, log|\sigma_{s+1}(\alpha)|^2, \ldots, log|\sigma_{s+t}(\alpha)|^2\right) \end{gathered} \tag{1}$$

The map (1) is said to be the *logarithmic representation* of K in $\mathbb{R}^{s+t}$.

The third (and last) chapter begins with the restriction of the logarithmic representation of any field K to the unit subgroup $\mathscr{O}_K^*$.

$$l : \mathscr{O}_K^* \longrightarrow \mathbb{R}^{s+t}$$

The *Dirichlet's unit theorem* includes a set of previous results that are essential for its demonstration, so we can consider them as part of it. We enumerate them in order to clarify the strategy that we are going to follow:

1. *The kernel W of $l : \mathscr{O}_K^* \longrightarrow \mathbb{R}^{s+t}$ is a finite cyclic group of even order formed by the set of all roots of unity belonging to $\mathscr{O}_K$.*

2. *The image E of $\mathscr{O}_K^*$ by l in $\mathbb{R}^{s+t}$ is a lattice of dimension $\leq s+t-1$.*

3. *A lattice L in $\mathbb{R}^m$ has dimension m if and only if there exists a bounded subset B of $\mathbb{R}^m$ such that:*

$$\mathbb{R}^m = \bigcup_{l \in L} l + B$$

4. *Let $y \in \mathbb{L}^{st}$ and let $\lambda_y : \mathbb{L}^{st} \longrightarrow \mathbb{L}^{st}$ defined as $\lambda_y(x) = yx$. Then λ_y is a linear map and $det(\lambda_y) = N(y)$, being $N(\cdot)$ the norm map in $\mathbb{L}^{st}$.* (This result is merely auxiliar for the next one).

5. *The image E of $\mathscr{O}_K^*$ in $\mathbb{R}^{s+t}$ is a lattice of dimension $s+t-1$.*

This compendium of results support the demonstration of the theorem that motivates this final degree project, let's remember it:

Theorem: *The abelian group $\mathscr{O}_K^*$ formed by the units of the integer ring $\mathscr{O}_K$ of the field K in finitely generated and is given by*

$$\mathscr{O}_K^* = L_K \times T_K,$$

where L_K is a free abelian group of rank $r+s-1$ and T_K is a finite cyclic group of even order formed by the roots of unity belonging to K.

Índice general

Capítulo 1

El anillo de enteros de un cuerpo de números

Este primer capítulo es de carácter introductorio ya que tiene como objetivo asentar (a modo de recordatorio) la base de teoría algebraica necesaria en la demostracion del *Teorema de las unidades*. Comenzamos describiendo de forma sencilla y clara las estructuras algebraicas que toman parte en el teorema (*grupos, anillos, cuerpos*) así como sus propiedades más relevantes para este estudio.

Describiremos los *números* y *enteros algebraicos*. Se demostrará que el subconjunto de los *enteros algebraicos* de cualquier *cuerpo de números* tiene estructura de anillo. También veremos que todo *cuerpo de números K* puede ser expresado como $K = \mathbb{Q}(\theta)$ con θ *entero algebraico*.

Por último, para una mejor comprensión del lector, trataremos de llevar los objetivos de este trabajo al caso práctico de los *cuerpos cuadráticos*. Veremos resultados acerca de sus anillos de enteros e intentaremos deducir las *unidades* de éstos cuando sea posible.

1.1. Generalidades

Esta sección la dedicamos a repasar los conceptos básicos de carácter algebraico en los que se apoya el trabajo y que suponemos conocidos ya que corresponden a temas desarrollados en las asignaturas obligatorias del Grado de Matemáticas.

1.1.1. Grupos abelianos finitamente generados

Un grupo es un conjunto no vacía G dotado con una operación binaria:

$$(\cdot) : G \times G \to G,\ (x,y) \to x \cdot y\ (= xy) \tag{1.1}$$

usualmente llamada propiedad multiplicativa y que satisface las siguinetes propiedades:

- La operación $(\cdot)$ es *asociativa*, es decir, $x(yz) = (xy)z\ \ \forall x,y,z \in G$.
- Existe un *elemento neutro* $e \in G$ tal que $xe = x = ex\ \ \forall x \in G$. Este elemento e es único y suele denotarse como 1.
- Para todo elemento x de G existe un único $x' \in G$, denotado por $x' = x^{-1}$ y llamado *el elemento inverso de* x, tal que $xx' = x'x = 1$.

Además, para dos grupos G_1 y G_2, su *producto cartesiano* $G_1 \times G_2$ dado por

$$(a,b) \times (a',b') \to (a \cdot a', b \cdot b')\ \ \left(a,a' \in G_1, b,b' \in G_2\right) \tag{1.2}$$

es también grupo y se dice que es el *el producto directo* de G_1 y G_2.

Si la operación $(\cdot)$ es además conmutativa ($xy = yx\ \forall x, y \in G$) se dice que G es un *grupo abeliano*. Salvo mención en sentido contrario, *grupo* significará *grupo abeliano*. En este caso es conveniente reemplazar la notación multiplicativa por la aditiva. Los principales cambios son:

Concepto	Multiplicativa	Aditiva
Operación	xy	$x+y$
Elemento neutro	1	0
Elemento inverso	x^{-1}	$-x$
Potencia	x^n	nx
Producto directo	$G_1 \otimes G_2$	$G_1 \oplus G_2$

Por ejemplo, con estos cambios se tiene

$$\mathbb{Z} = \langle 1 \rangle = \{n = n1 \mid n \in \mathbb{Z}\},\ \mathbb{Z}_n = \left\langle \overline{1} \right\rangle = \{\overline{a} \mid 0 \leq a \leq n-1\},$$

lo que da la descripción de los grupos aditivos de los enteros y de los enteros módulo n; Un grupo infinito el primero y finito de orden n el segundo.

Sea H un subconjunto no vacío de G, se dice que H es un *subgrupo de* G si para cualquier $x, y \in H$, xy y x^{-1} pertenecen a H (se denota como $H \leq G$). La forma de construir subgrupos en este trabajo se deduce de las ideas siguientes: Dados un grupo G y un elemento $x \in G$, por la asociatividad de $(\cdot)$ es muy sencillo definir las potencias $x^n,\ n \in \mathbb{Z}$. Entonces, como $x^n x^m = x^{n+m}$, $x^0 = 1$ y $x^{-n} = (x^n)^{-1}$, es inmediato ver que el subconjunto

$$\langle x \rangle := \{x^n \mid n \in \mathbb{Z}\}$$

es un subgrupo de G.
Dado un grupo G, se dice que el *cardinal* $n = |G|$ es el *orden de* G; si n es finito se dirá que G es de tipo finito. Analogamente, se dice que un elemento $x \in G$ tiene *orden finito* si $n = |\langle x \rangle|$ es finito; es claro que n es el menor entero positivo tal que $x^n = 1$ (en caso contrario diremos que el *orden de x es infinito*). El ejemplo clásico de elemento con orden finito es la raíz n-sima primitiva de la unidad ($x = e^{\frac{2\pi i}{n}}$), que tiene orden n; se sigue que el grupo $\langle x \rangle$ contiene a todas las raíces n-simas de la unidad.

Se dice que el grupo G es de *torsión* si todo elemento tiene orden finito y que es *libre de torsión* o simplemente *libre* si su elemento neutro 0 es el único que tiene orden finito ($|\langle 0 \rangle| = 1$ en cualquier grupo). Por ejemplo, $\mathbb{Z}$ es libre mientras que $\mathbb{Z}_n$ es de torsión, también se puede dar el caso de un grupo que no sea ni lo uno ni otro, como ocurre con $\mathbb{Z} \times \mathbb{Z}_n$.
Si G es un grupo (abeliano) y $x_1, \cdots, x_s \in G$, es inmediato que el conjunto

$$\langle x_1, \cdots, x_s \rangle := \{n_1 x_1 + \cdots + n_s x_s \mid n_1, \cdots, n_s \in \mathbb{Z}\} \tag{1.3}$$

es un subgrupo de G. Si $G = \langle x_1, \cdots, x_s \rangle$ diremos que G es *un grupo finitamente generado* por sus elementos $x_1, \cdots, x_s$. Si $s = 1$, $G = \langle x_1 \rangle$ se dice *cíclico* y se recupera lo dicho anteriormente: $\mathbb{Z}$ es un grupo cíclico infinito y libre de torsión y $\mathbb{Z}_n$ es un grupo cíclico de torsión porque es finito. Para grupos G finitamente generados, éstas son las piezas que los describen como se va a ver a continuación.

Lema 1.1. *Un subgrupo de un grupo abeliano finitamente generado está finitamente generado.*

Teorema 1.2. *Si G es un grupo abeliano finitamente generado, entonces*

$$G = L(G) \oplus T(G), \tag{1.4}$$

donde $L(G)$ es libre de torsión y $T(G)$ es de torsión.

Notemos que, por el Lema 1.1, ambos sumandos están finitamente generados.

Teorema 1.3. *Sea G un grupo abeliano finitamente generado.*

(1) Si G es libre de torsión entonces es libre, es decir existen $y_1, \cdots, y_r \in G$ tales que todo $x \in G$ se escribe de modo único en la forma $x = n_1 y_1 + \cdots + n_r y_r$. El entero $r \geq 1$ está determinado por G y se llama rango de G. Como cada sumando está unívocamente determinado por la suma y al variar el coeficiente describe un grupo cíclico infinito, se escribe $G = \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{r}$.

(2) Si G es de torsión es finito y se puede escribir de modo único como suma directa de grupos cíclicos finitos en la forma $G = \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_t}$ donde $a_1 \mid \cdots \mid a_t$. Los enteros positivos $a_1, \cdots, a_t$ son únicos y se denominan los factores invariantes de G. Notemos que a_t es el mínimo común múltiplo de los órdenes de los elementos de G. Se le llama exponente de G.

La combinación de los dos teoremas anteriores constituye *el teorema de estructura de un grupo abeliano finitamente generado*, fundamental para los objetivos de este trabajo. Tal grupo es suma directa de un número finito de grupos cíclicos infinitos (*su parte libre*) y grupos cíclicos finitos (*su parte de torsión*), cuyos invariantes se atribuyen al grupo total.

1.1.2. Anillos y unidades

Un anillo es una estructura matemática A dotada de dos operaciones internas

$$(+) : A \times A \to A \quad (a,b) \to a+b$$
$$(\cdot) : A \times A \to A \quad (a,b) \to ab$$

que satisfacen las propiedades siguientes:

- $(A,+)$ *es un grupo abeliano.*
- $(\cdot)$ *es asociativa*, esto es, $a(bc) = (ab)c \quad \forall a,b,c \in A$.
- $(\cdot)$ *es distributiva respecto de* $(+)$, luego será $a(b+c) = ab+ac \quad \forall a,b,c \in A$.

Los anillos considerados para este estudio serán *anillos conmutativos con identidad*, es decir satisfaciendo las condiciones adicionales siguientes:

- $(\cdot)$ *es conmutativa*: $ab = ba \quad \forall a,b \in A$.
- *Existencia de elemento neutro para el producto* $(\cdot)$; existirá un (único) elemento denotado por $1 \in A$ tal que $a \cdot 1 = a \quad \forall a \in A$.

Un elemento $a \in A$ es una *unidad* si tiene *elemento inverso*, es decir, si existe un $0 \neq b \in A$ tal que $ab = 1 = ba$. El elemento b es único y lo denotamos $b = a^{-1}$; se sigue que b también es unidad y su elemento inverso es precisamente $b^{-1} = a$. El subconjunto de las unidades del anillo A se denota por A^* y es un grupo con respecto a la multiplicación ya que $(ab)^{-1} = b^{-1}a^{-1} \ (\forall a,b \in A^*)$. Ejemplos típicos de subgrupos de unidades son: $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{Z}_n^* = \{\overline{a} \mid mcd(a,n) = 1\}$, etc

Un cuerpo es un anillo K cuyo grupo multiplicativo $K^* = K \setminus \{0\}$ esta formado por todos sus elementos no nulos. Cuerpos conocidos son $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$; también es cuerpo $\mathbb{Z}_p$ con p primo. Más adelante veremos que todo cuerpo K contiene al cuerpo de los racionales $\mathbb{Q}$ y definiremos *grado de K* a partir de $\mathbb{Q}$. De hecho el primer ejemplo no trivial es el *cuerpo racional Gaussiano* $\mathbb{Q}(i) = \{a+bi | a,b \in \mathbb{Q}\}$.
La estructura aditiva de un cuerpo K es análoga a la de un espacio vectorial, mientras que la multiplicativa viene dada por el siguiente resultado.

Lema 1.4. *Un subgrupo finito G del grupo multiplicativo de un cuerpo K es cíclico.*

Demostración. Sea n el exponente de G; la existencia de n está asegurada por el Teorema 1.3. Además existe $g \in G$ cuyo orden $|\langle g \rangle| = n$. Por definición de exponente todo elemento de G es raíz del polinomio $x^n - 1 \in K[x]$. Como éste tiene a lo sumo n raíces en K se sigue que $|G| \leq n$. Trivialmente $n = |\langle g \rangle| \leq |G|$. Luego $|G| = n$ y $G = \langle g \rangle$ es cíclico. □

1.2. Números y enteros algebraicos

Antes de estudiar los números y enteros algebraicos, comenzamos esta sección repasando algunos conceptos básicos de teoría de cuerpos; no nos vamos a extender demasiado ya que son conceptos que se dan por conocidos.

Sean K y L cuerpos tal que $K \subseteq L$, se dice que L *es una extensión de* K y se denota como L/K. Notar que L tiene estructura de espacio vectorial sobre K, de hecho, se dice que la dimensión de este espacio vectorial es el *grado de la extensión* L/K y se denota $[L:K]$. Si $[L:K]$ es finito se dice que L es una extensión finita de K.
Sean $H \subseteq K \subseteq L$ cuerpos, se tiene la siguiente propiedad multiplicativa:

$$[L:H] = [L:K]\,[K:H]$$

Una extensión L/K se dice *algebraica* si $\forall \alpha \in L$ existe un polinomio $p(X) \in K[X]$ tal que $p(\alpha) = 0$; se dice que α es *algebraico sobre* K. Además existe un único polinomio mónico e irreducible $m_\alpha(X)$ con coeficientes en K tal que $m_\alpha(\alpha) = 0$; se dice que m_α es el *polinomio mínimo de* α *sobre* K. Con esto damos paso a la siguiente definición.

Un número complejo se dice *algebraico sobre* $\mathbb{Q}$ ó simplemente *algebraico* si es solución de una ecuación polinómica con coeficientes en $\mathbb{Q}$. Equivalentemente (quitando denominadores), podemos asumir que los coeficientes están en $\mathbb{Z}$ y sería resolver:

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_o = 0 \quad (a_n \neq 0, a_1, \cdots, a_n \in \mathbb{Z}) \tag{1.5}$$

Comentarios al respecto:

- La suma, diferencia, producto y cociente de dos números algebraicos es algebraico, luego el conjunto de los números algebraicos constituyen un grupo abeliano para la suma, un anillo con unidad y un cuerpo. Por lo tanto, el conjunto de los números algebraicos es un subcuerpo de $\mathbb{C}$.

- Siguiendo la definición, es claro que todos los números racionales son algebraicos ya que si $r = \frac{a}{b} \in \mathbb{Q}$ $(a, b \in \mathbb{Z})$, entonces r es solución de $bx - a = 0$. Es más, el conjunto de los números algebraicos es el cuerpo algebraicamente cerrado más pequeño que contiene a $\mathbb{Q}$, es decir, es la clausura algebraica de $\mathbb{Q}$. Es razonable entonces denotar al conjunto de los números algebraicos como $\overline{\mathbb{Q}}$.

- Si nos fijamos en los irracionales hay muchos números algebraicos, por ejemplo $\sqrt{2}$ y $\frac{\sqrt[3]{3}}{2}$, que son solución de $x^2 - 2 = 0$ y $8x^3 - 3 = 0$ respectivamente; pero también hay irracionales como π, e ó $2^{\sqrt{2}}$ que no son son solución de ninguna ecuación del tipo (1.5) (son los llamados *números trascendentes*).

Volviendo a los cuerpos de números, notar que cualquier cuerpo K es un subcuerpo del cuerpo complejo $\mathbb{C}$ tal que $[K:\mathbb{Q}]$ es finito, es decir, todo cuerpo K es una extensión finita de $\mathbb{Q}$. Esto implica que todo elemento de K es algebraico. Además, se sigue por el *teorema del elemento primitivo* que K es una *extensión simple* de $\mathbb{Q}$, es decir, existe un elemento $\alpha \in K$ llamado *elemento primitivo de* K tal que

$$K = \mathbb{Q}(\alpha) \tag{1.6}$$

De hecho se puede elegir α para que sea algebraico.

Teorema 1.5. *Sea* $K = \mathbb{Q}(\theta)$ *como en (1.6) de grado n, hay exactamente n monomorfismos* $\sigma_i : K \to \mathbb{C}$ $(i = 1, \ldots, n)$. *Además los elementos* $\sigma_i(\theta) = \theta_i$ *son los distintos ceros en* $\mathbb{C}$ *del polinomio minimo de* θ *sobre* $\mathbb{Q}$.

Demostración. Se sabe por teoría de cuerpos que un polinomio irreducible sobre un cuerpo K no tiene ceros repetidos en $\mathbb{C}$, luego el polinomio minimo $p(X)$ de θ tendrá $\theta_1, \cdots, \theta_n$ raíces distintas en $\mathbb{C}$. Notar que cada θ_i también debe tener polinomio mínimo $p(X)$ en $\mathbb{C}$ (el polinomio minimo de θ_i debe dividir a $p(X)$ y $p(X)$ es irreducible, luego ha de ser $p(X)$, de modo que hay un único monomorfismo $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ tal que $\sigma_i(\theta) = \theta_i$. Y es claro que $\mathbb{Q}(\theta_i) \subseteq \mathbb{C}$, luego efectivamente tenemos n monomorfismos distintos $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{C}$ como en el enunciado. □

Decimos que los monomorfismos $\sigma_i (i = 1, \cdots, n)$ son las *n-incrustaciones* de K en $\mathbb{C}$. Además, nos referiremos a ellos simplemente como homomorfismos, ya que un homomorfismo de dominio un cuerpo K siempre es inyectivo por ser su núcleo un ideal de K.

Veamos uno de los ejemplos más sencillos: Sea $K = \mathbb{Q}(i) = \{x + iy | x, y \in \mathbb{Q}\}$, tenemos efectivamente que i algebraico con polinomio mínimo $x^2 + 1$ de grado 2 sobre $\mathbb{Q}$; luego habrá 2 homomorfismos $\sigma_i : K \to \mathbb{C} (i = 1, 2)$ tal que:

$$\sigma_1(x + iy) = x + iy$$
$$\sigma_2(x + iy) = x - iy$$

Ahora, para cada $\alpha \in K = \mathbb{Q}(\theta)$ se define el *polinomio de cuerpo* para α como:

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

Se tiene de lo anterior que el polinomio de cuerpo $f_\alpha(X)$ es una potencia del polinomio mínimo $p_\alpha(X)$, $\forall \alpha \in K$.

Un número complejo θ se dice *entero algebraico* si es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$, es decir, si satisface una ecuación de la forma:

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_o = 0 \quad (a_i \in \mathbb{Z})$$

Un ejemplo clásico de enteros algebraicos son las raíces de los polinomios de segundo grado $X^2 + bX + c$ $(b, c \in \mathbb{Z})$, es decir, los elementos $X = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$ $(b, c \in \mathbb{Z})$, denominados *enteros cuadráticos*. Por ejemplo, $\frac{1-\sqrt{5}}{2}$ es entero algebraico por ser raíz de $X^2 - X - 2$.

Denotamos como E al conjunto de los enteros algebraicos. Para evitar confusiones, hablaremos de *enteros racionales* para referirnos a los elementos de $\mathbb{Z}$. Asimismo, definimos los *enteros libres de cuadrados* como los elementos de $\mathbb{Z}$ que no son divisibles por ningún primo al cuadrado (les daremos uso en la siguiente sección).

Lema 1.6. *Un número complejo θ es un entero algebraico si y solo si el anillo de valores de θ, $\mathbb{Z}[\theta] = \{f(\theta) | f \in \mathbb{Z}[X]\}$, está finitamente generado.*

Demostración. Podemos desarrollar el anillo de valores de θ como

$$\mathbb{Z}[\theta] = \left\{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_r\theta^r \mid r \in \mathbb{N},\ a_1, \cdots, a_r \in \mathbb{Z}\right\}$$

Es decir, $\mathbb{Z}[\theta]$ está generado de forma aditiva por las potencias $\left\{1, \theta, \theta^2, \cdots, \theta^r, \cdots\right\}$.
Ahora bien, si suponemos θ entero algebraico, entonces para algún n finito será:

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_o = 0 \quad (a_i \in \mathbb{Z}) \tag{1.7}$$

Denotando como Γ_θ al grupo aditivo generado por $\left\{1, \theta, \theta^2, \cdots, \theta^{n-1}\right\}$, vamos a tratar de probar por inducción que toda potencia de θ está en Γ_θ. Es claro que θ^n está en Γ_θ por ser combinacion lineal de los $\left(1, \theta, \theta^2, \cdots, \theta^{n-1}\right)$ (1.7).

Entonces, suponiéndolo cierto para θ^m con $m \geq n$, veamos si se cumple para θ^{m+1}:

$$\theta^{m+1} = \theta^{m+1-n}\theta^n = \theta^{m+1-n}\left(a_{n-1}\theta^{n-1} - \cdots - a_1\theta - a_o\right) \in \Gamma_\theta$$

Efectivamente, toda potencia de θ está en Γ_θ y se tiene que $\mathbb{Z}[\theta]$ está finitamente generado.

Para la implicación inversa, supongamos que $\mathbb{Z}[\theta]$ está finitamente generado, es decir, toda potencia de θ está en un grupo G finitamente generado. Entonces el subgrupo Γ_θ también debe estar finitamente generado por el Lema 1.1. Sean $v_1, \cdots, v_n$ los generadores de Γ_θ , cada v_i es un polinomio en θ con coeficientes enteros, de modo que los polinomios θv_i también están en θ y tienen coeficientes en $\mathbb{Z}$. Existirán enteros b_i tal que:

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

Teniendo en cuenta todos los v_i llegamos a un sistema de ecuaciones homogéneo como sigue

$$\begin{array}{rcl} (b_{11}-\theta)\,v_1 + b_{12}v_2 + \cdots + b_{1n}v_n &=& 0 \\ b_{21}v_1 + (b_{22}-\theta)\,vv_2 + \cdots + b_{1n}v_n &=& 0 \\ \cdots & \cdots & \cdots \\ b_{n1}v_1 + b_{n2}v_2 + \cdots + (b_{nn}-\theta)\,v_n &=& 0 \end{array} \tag{1.8}$$

Al ser un sistema homogéneo existirá una única solución no nula en $\mathbb{C}$, de modo que su determinante asociado será:

$$\begin{vmatrix} b_{11}-\theta & b_{12} & \cdots & b_{1n} \\ b_{11} & b_{22}-\theta & \cdots & b_{12n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn}-\theta \end{vmatrix} = 0$$

Desarrollando el determinante vemos que θ es raíz de un polinomio mónico con coeficientes enteros, es decir, θ entero algebraico.

□

Teorema 1.7. *El conjunto de los enteros algebraicos E forman un subanillo del cuerpo de números algebraicos $\overline{Q}$.*

Demostración. Sean $\theta, \phi \in E$, para ver que E es un subanillo de $\overline{Q}$ tenemos que probar que $\theta+\phi, \theta\phi \in E$. Sabemos por el teorema anterior que las potencias de θ están en el grupo aditivo Γ_θ y las potencias de ϕ en el grupo aditivo Γ_ϕ, ambos finitamente generados; por lo que todas las potencias de $\theta+\phi$ y de $\theta\phi$ son combinaciones lineales de elementos de la forma $\theta^i\phi^j$ (i,j finitos), luego es claro que estarán en $\Gamma_\theta\Gamma_\phi \subseteq \mathbb{C}$. Pero si Γ_θ tiene generadores $v_1, \cdots, v_n$ y Γ_ϕ tiene generadores $w_1, \cdots, w_m$ entonces $\Gamma_\theta\Gamma_\phi$ es el grupo aditivo generado por elementos de la forma $v_i w_j\,(1 \leq i \leq n, 1 \leq j \leq m)$. Los v_i y los w_j son polinomios en θ y ϕ respectivamente y con coeficientes enteros. Por lo tanto todas las potencias de $\theta+\phi$ y $\theta\phi$ están en un subgrupo de $\mathbb{C}$ finitamente generado. Se sigue del lema anterior que $\theta+\phi$ y $\theta\phi$ son enteros algebraicos. □

Entonces, para cualquier cuerpo de números K, se tiene que el subconjunto de sus enteros algebraicos tiene estructura de anillo y lo denotamos como $\mathcal{O}_K$; equivalentemente podemos escribir:

$$\mathcal{O}_K = K \cap E$$

Sea $\mathcal{O}_K$ el anillo de enteros algebraicos de un cuerpo K de grado n, se demuestra la existencia de una $\mathbb{Z}$-base para $(\mathcal{O}_K, +)$, es decir, una familia de elementos $\{\alpha_1, \cdots, \alpha_n\}$ con $\alpha_i \in \mathcal{O}_K$ tal que todo elemento $e \in \mathcal{O}_K$ viene expresado de forma unívoca como:

$$e = a_1\alpha_1 + \cdots + a_n\alpha_n \;\; (a_i \in \mathbb{Z})$$

Se dice que esta $\mathbb{Z}$-base es una *base entera* de $\mathscr{O}_K$ (o de K).

Asimismo, denotamos por $\mathscr{O}_K^*$ al subconjunto de las unidades de $\mathscr{O}_K$. Se demuestra sin mayor dificultad que $\mathscr{O}_K^*$ tiene estructura de grupo con la multiplicación ya que $\forall a,b \in \mathscr{O}_K^*$ tenemos que $(ab)^{-1} = b^{-1}a^{-1} \in \mathscr{O}_K^*$. Nos referiremos a $\mathscr{O}_K^*$ como el *subgrupo de las unidades de* $\mathscr{O}_K$.

Comentario: Dado un cuerpo cualquiera, el lector puede hacerse la evidente pregunta: ¿Cúal es su anillo de enteros algebraicos? Bien, no hay una respuesta unificada que abarque todos los casos. La mayoría de las veces, encontrar estos anillos supone cálculos muy pesados y procedimientos muy engorrosos que no vamos a citar aquí, ya que se exceden de lo que necesitamos para nuestro estudio. Tampoco entraremos en hallar bases enteras para estos anillos; encontrarlas no es algo trivial y su cometido aquí es secundario. No obstante, para hacernos una idea, en la siguiente sección veremos cuáles son los anillos de enteros en el caso particular de cuerpos cuadráticos.

Lema 1.8. *Si $\alpha \in K$ entonces existe un elemento no nulo $c \in \mathbb{Z}$ tal que $c\alpha \in \mathscr{O}_K$.*

Corolario 1.9. *Si K es un cuerpo de números entonces $K = \mathbb{Q}(\theta)$ para un entero algebraico θ.*

Demostración. Sabemos que $K = \mathbb{Q}(\phi)$ para un número algebraico ϕ. Por el Lema anterior existirá un entero algebraico θ tal que $\theta = c\phi$ con $0 \neq c \in \mathbb{Z}$. Luego claramente es $\mathbb{Q}(\phi) = \mathbb{Q}(\theta)$ y tenemos efectivamente que $K = \mathbb{Q}(\theta)$ con θ entero algebraico. □

Teorema 1.10. *Un número algebraico α es un entero algebraico si y solo si su polinomio mínimo sobre $\mathbb{Q}$ tiene coeficientes en $\mathbb{Z}$.*

Demostración. Sea $p(X)$ el polinomio mínimo de α sobre $\mathbb{Q}$, recordar que $p(X)$ es mónico e irreducible en $\mathbb{Q}[X]$. Si α es un entero algebraico entonces existe un polinomio mónico $q(X) \in \mathbb{Z}[X]$ tal que $q(\alpha) = 0$, luego será $p|q$; entonces, por el Lema de Gauss se sigue que existirá un $\lambda \in \mathbb{Q}$ tal que $\lambda p(X) \in \mathbb{Z}[X]$ y $\lambda p|q$. Y como $p(X)$ y $q(X)$ son mónicos, ha de ser $\lambda = 1$. Luego efectivamente, $p(X) \in \mathbb{Z}[X]$. La implicación inversa es inmediata. □

Con la notación usual, sea K cuerpo de grado n con $\sigma_1, \cdots, \sigma_n$ las n-incrustaciones $K \to \mathbb{C}$. Para todo $\alpha \in K$ se define la *norma en un cuerpo* como la aplicación:

$$N_K : K \to \mathbb{C} \ , \ \alpha \mapsto N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \tag{1.9}$$

Si no hay lugar a confusión omitiremos el subíndice que determina el cuerpo y nos referiremos a la norma simplemente como $N(\cdot)$.
Ahora, sea $\alpha \in K$, sabemos que su polinomio de cuerpo $f_\alpha(X)$ es una potencia del polinomio mínimo $m_\alpha(X)$. Si además α es entero algebraico, se tiene por el Teorema 1.10 que $m_\alpha(X) \in \mathbb{Z}[X]$. Luego, si $\alpha \in \mathscr{O}_K$ será:

$$f_\alpha(X) \in \mathbb{Z}[X]$$

Notar que el término independiente de $f_\alpha(X)$ es de la forma:

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

Por consiguiente es inmediato que $N(\alpha) \in \mathbb{Z}$. Además, como los σ_i son homomorfismos, $\forall \alpha, \beta \in K$ será:

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

1.3. Enteros cuadráticos

Dentro del amplio espectro de los cuerpos de números, vamos a centrarnos por un momento en el caso particular de las *extensiones cuadráticas*, quizás el más familiar y de más fácil uso y visualización.

Un cuerpo K se dice *cuerpo cuadrático* si es de grado 2 sobre $\mathbb{Q}$, es decir, si $[K:\mathbb{Q}]=2$. Además, por el Corolario 1.9, $K=\mathbb{Q}(\theta)$ con θ entero algebraico, de modo que θ es raiz de un polinomio de la forma

$$X^2+aX+b \quad (a,b\in\mathbb{Z})$$

Deducimos de lo anterior que

$$\theta=\frac{-a\pm\sqrt{a^2-4b}}{2} \quad (a,b\in\mathbb{Z}) \tag{1.10}$$

Como $a^2-4b\in\mathbb{Z}$, podemos afirmar por factorización por primos en $\mathbb{Z}$ que $a^2-4b=r^2d$ con $r,d\in\mathbb{Z}$ y d *entero libre de cuadrados*.
Sustituyendo en (1.10) queda:

$$\theta=\frac{-a\pm\sqrt{a^2-4b}}{2}=\frac{-a\pm r\sqrt{d}}{2} \quad (a,r,d\in\mathbb{Z})$$

Luego, una definición alternativa de cuerpo cuadrático es decir que $K=\mathbb{Q}(\sqrt{d})$ con d entero libre de cuadrados. Asímismo, decimos que K es un *cuerpo cuadrático real* si d es positivo e *imaginario* si d es negativo.

Sea $K=\mathbb{Q}(\sqrt{d})$ como hemos definido y sea $\alpha=a+b\sqrt{d}\in K$ $(a,b\in\mathbb{Q})$, se definen 2 homomorfismos $K\to\mathbb{C}$ de la siguiente forma:

$$\begin{array}{l} a+b\sqrt{d}\to a+b\sqrt{d} \\ a+b\sqrt{d}\to a-b\sqrt{d} \end{array} \tag{1.11}$$

Se dice que $\overline{\alpha}=a-b\sqrt{d}$ es el *conjugado de* α *en* $\mathbb{Q}(\sqrt{d})$. Si $d<0$, $\overline{\alpha}$ coincide con el complejo conjugado de α. Además el polinomio mínimo de α en $\mathbb{Q}[t]$ viene dado por:

$$m_\alpha(X)=(X-\alpha)(X-\overline{\alpha})=X^2-2aX+\left(a^2-db^2\right)$$

Teorema 1.11. *Sea d un cuadrado libre, entonces, el anillo de enteros de* $K=\mathbb{Q}(\sqrt{d})$ *es:*

1. $\mathcal{O}_K=\mathbb{Z}[\sqrt{d}]$ *si* $d\not\equiv 1$ *(mod 4).*
2. $\mathcal{O}_K=\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{d}]$ *si* $d\equiv 1$ *(mod 4).*

Demostración. Sea $\alpha\in K=\mathbb{Q}(\sqrt{d})$, podemos escribir $\alpha=\dfrac{a+b\sqrt{d}}{c}$ con $a,b,c\in\mathbb{Z}$ y coprimos entre sí. Por (1.11) su polinomio mínimo es:

$$p_\alpha(X)=(X-\alpha)(X-\bar{\alpha})=\left(X-\frac{a+b\sqrt{d}}{c}\right)\left(X-\frac{a-b\sqrt{d}}{c}\right)=X^2-\frac{2a}{c}X+\frac{a^2-db^2}{c^2}$$

Entonces, para que $\alpha\in\mathcal{O}_K$ tendrá que verificarse:

$$(1):\frac{2a}{c}\in\mathbb{Z};\quad (2):\frac{a^2-db^2}{c^2}\in\mathbb{Z}$$

Como $\mathrm{mcd}(a,c)=1$ por ser coprimos, para que se verifique (1) ha de ser $c=1$ ó $c=2$.

- Si $c=1$ tenemos que $\alpha=a+b\sqrt{d}$ con $a,b\in\mathbb{Z}$; es decir, $\alpha\in\mathbb{Z}[\sqrt{d}]$.

- Si $c = 2$ tenemos que a y b no pueden ser pares ya que tendrían el 2 en común y recordemos que son coprimos; tampoco pueden ser uno par y otro impar ya que si uno de ellos es par, por (2) el otro ha de ser también par, lo cual es una contradicción. Luego, la única posibilidad es que a y b sean impares.

  Y ahora, como el cuadrado de un numero impar es congruente con 1 en módulo 4 y siendo por (2) $4|a^2 - db^2$, será:

  $$a^2 - db^2 \equiv 1 - d \ (mod\ 4) \equiv 0 \ (mod\ 4)$$

  Es decir, $n \equiv 1 \pmod 4$. Además, teniendo en cuenta que $(a-b)$ par por ser a, b impares, descomponemos α tal que:

  $$\alpha = \frac{a + b\sqrt{d}}{2} = \underbrace{\frac{a-b}{2}}_{\mathbb{Z}} + b\left(\frac{1+\sqrt{d}}{2}\right)$$

  Luego es claro que $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

Resumiendo lo anterior:

$$Si\ d \not\equiv 1 \ (mod\ 4) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$$
$$Si\ d \equiv 1 \ (mod\ 4) \Rightarrow \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

□

1.4. Unidades en el anillo de enteros de un cuerpo cuadrático

Recordando el enunciado del *Teorema de las unidades*, tenemos que el objetivo principal que nos atañe y que abordaremos con generalidad en el último Capítulo es describir el grupo de las unidades $\mathcal{O}_K^*$ del anillo de enteros $\mathcal{O}_K$ de un cuerpo K cualquiera. El siguiente resultado describe $\mathcal{O}_K^*$ para cuerpos cuadráticos imaginarios.

Teorema 1.12. *Dado un cuerpo de números cuadrático $K = \mathbb{Q}(\sqrt{d})$ con $d < 0$ entero libre de cuadrados, el grupo de las unidades $\mathcal{O}_K^*$ es:*

a) Si $d = -1 \ \rightarrow \ \mathcal{O}_K^* = \{\pm 1 \pm i\}$

b) Si $d = -3 \ \rightarrow \ \mathcal{O}_K^* = \left\{\pm 1, \overset{+}{-}\omega, \overset{+}{-}\omega^2\right\}$ donde $\omega = e^{2\pi i/3}$.

c) Para el resto de $d < 0 \quad {O_K}^* = \{\pm 1\}$

Demostración. Suponer que α es una unidad del anillo de enteros de $\mathbb{Q}(\sqrt{d})$ con elemento inverso β de modo que $\alpha\beta = 1$. Entonces, tomando normas como en (1.9) tenemos:

$$N(\alpha)N(\beta) = 1$$

Como $N(\alpha), N(\beta) \in \mathbb{Z}$, tendrá que ser $N(\alpha) = \pm 1$. Si denotamos $\alpha = a + b\sqrt{d} \ \ (a, b \in \mathbb{Q})$ y teniendo en cuenta los dos homomorfismos que genera un cuerpo cuadrático

$$N(\alpha) = \sigma_1(\alpha)\,\sigma_2(\alpha) = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - db^2$$

Y como estamos trabajando con con $d < 0$ ha de ser $N(\alpha) = +1$. Por tanto, nuestro problema se reduce a calcular, fijado un d negativo, qué valores $a, b \in \mathbb{Q}$ verifican la ecuación $a^2 - db^2 = 1$. Para ello tenemos que tener en cuenta cúal es el anillo de enteros en cada caso, dependiendo de si $d \equiv 1 \ (mod\ 4)$ o $d \not\equiv 1 \ (mod\ 4)$.

a) $\boxed{d=-1}$
Como $-1 \not\equiv 1 \ (mod\ 4)$, el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es $\mathbb{Z}[\sqrt{d}]$; entonces la ecuación a resolver es $a^2+b^2=1$ con $a,b\in\mathbb{Z}$, que tiene como únicas soluciones $\{a=\pm1,b=0\}$ y $\{a=0,b=\pm1\}$. Luego el grupo de las unidades en este caso será efectivamente $\mathscr{O}_K^*=\{\pm1,\pm i\}$

b) $\boxed{d=-3}$
Ahora, como $-3\equiv 1 \ (mod\ 4)$ tenemos que el grupo de las unidades estará en el anillo de enteros $\mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{-3}\right]$. Luego los enteros serán de la forma:

$$\alpha=\lambda+\mu\left(\tfrac{1}{2}+\tfrac{1}{2}\sqrt{-3}\right)=\underbrace{\frac{2\lambda+\mu}{2}}_{\text{a}}+\underbrace{\frac{\mu}{2}}_{\text{b}}\sqrt{-3}\ (\lambda,\mu\in\mathbb{Z})$$

Tenemos que resolver la ecuación $a^2+3b^2=1$ $(a,b\in\mathbb{Q})$. Notar que si μ es par entonces $a,b\in\mathbb{Z}$ y las únicas soluciónes son $\{a=\pm1,b=0\}$. Para μ impar tenemos $a=\frac{A}{2},\ b=\frac{B}{2}$ con A,B enteros pares. Entonces la ecuación a resolver es $A^2+3B^2=4$, que tiene como soluciones las 4 variantes de combinar $\{A=\pm1,B=\pm1\}$. El caso $\{A=1,B=1\}$ da:

$$\alpha=\tfrac{1}{2}\left(1+\sqrt{3}\right)=e^{2\pi i/3}\quad \text{(lo denotamos } \omega\text{)}.$$

El resto de las soluciones son $-\omega,\omega^2,-\omega^2$. Por tanto el grupo de las unidades es efectivamente $\mathscr{O}_K^*=\left\{\pm1,\pm\omega,\pm\omega^2\right\}$.

c) $\boxed{d<-3, d\neq -1,-3}$
Remitiéndonos al apartado anterior y a partir de la ecuación $A^2-dB^2=4$ deducimos que ha de ser $B=0$, ya que como d es negativo y B entero racional nos excederíamos de 4 para cualquier valor de A que tomásemos. Por tanto la única posibilidad es $\{A=\pm2,B=0\}$, es decir $\{a=\pm1,b=0\}$. Luego será $\mathscr{O}_K^*=\{\pm1\}$.

□

Hemos obtenido, con un razonamiento deductivo, cúal es el subgrupo de las unidades del anillo de enteros de un cuerpo cuadrático imaginario cualquiera. Sin embargo, para cuerpos cuadráticos reales no tenemos una información tan precisa.
Si tomamos un $d>0$, por ejemplo $K=\mathbb{Q}(\sqrt{3})$, como $3\not\equiv 1\ (mod 4)$ su anillo de enteros es $\mathbb{Z}[\sqrt{3}]$. Ahora, de la primera parte de la demostración anterior tenemos que un elemento $\alpha\in\mathbb{Z}[\sqrt{3}]$ de la forma $\alpha=a+b\sqrt{3}$ $(a,b\in\mathbb{Z})$ será unidad si y solo si $N(\alpha)=\pm1$, o lo que es lo mismo, si y solo si $a^2-3b^2=\pm1$. A primera vista encontramos valores de a y b que verifican dicha ecuación:

$$\{a=\pm1,b=0\}\to\alpha=\pm1$$
$$\{a=\pm2,b=\pm1\}\to\alpha=\pm2\pm\sqrt{3}$$

Hemos encontrado 6 unidades del anillo de enteros del cuerpo $K=\mathbb{Q}(\sqrt{3})$, pero a diferencia del caso imaginario, ahora no podemos asegurar que éstas sean las únicas unidades de $\mathscr{O}_K$. De hecho, intuitivamente podemos pensar por la forma de la ecuación que existen mas valores a,b que la verifican. Abordaremos y trataremos de responder a estos interrogantes mas adeante, cuando afrontemos el *Teorema de las unidades* en el caso general. Será entonces cuando razonaremos la finitud de $\mathscr{O}_K^*$ (para cualquier cuerpo) y podamos describirlo genéricamente.

Capítulo 2

Representación geométrica de un cuerpo de números

El objetivo de este capítulo es establecer una correspondencia bien definida entre un *cuerpo de números* cualquiera y su *espacio logarítmico asociado* (describiremos este espacio en la última sección). Buscamos esta correlación por el simple hecho de que el grupo de las unidades de un cuerpo, que es el que nos interesa, es multiplicativo; y el espacio logarítmico, como su propio nombre indica, nos permite trabajar aditivamente debido a la propiedad aditiva del logaritmo.

Para ello necesitaremos describir detalladamente qué es un *retículo* (algebraicamente hablando), así como definir para cualquier cuerpo K su *espacio reticular asociado*. Recordemos que podemos expresar un cuerpo K de grado n como $K = \mathbb{Q}(\theta)$ con θ entero algebraico y que hay exactamente n homomorfismos $\sigma_i : K \to \mathbb{C}$ distintos.

2.1. Retículos

Sea $(e_1, \ldots, e_m)$ una familia de vectores linealmente independientes en $\mathbb{R}^n$ ($m \leq n$). Diremos que el subgrupo aditivo de $(\mathbb{R}^n, +)$ generado por $(e_1, \ldots, e_m)$ es un *retículo* de dimension m generado por $(e_1, \ldots, e_m)$.

Siguiendo la definición anterior, podemos ver un retículo como un $\mathbb{Z}$-módulo del conjunto de puntos $\{e_1, \ldots, e_m\}$. Graficamente es muy intuitivo identificar un retículo por su estructura en el espacio. Veámoslo con dos sencillos ejemplos:

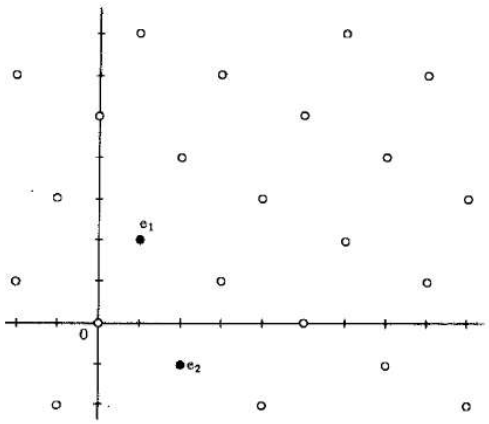

Figura 2.1: Retículo en $\mathbb{R}^2$ generado por $e_1\,(1,2)$ y $e_2\,(2,-1)$

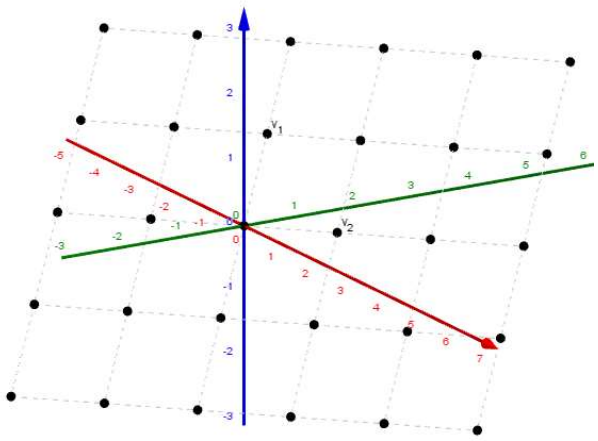

Figura 2.2: Retículo en $\mathbb{R}^3$ generado por $v_1\,(-1,1,1)$ y $v_2\,(1,1,0)$.

Notar que un retículo de dimensión m tal como está definido es precisamente un grupo libre abeliano de rango m, por lo que podemos aplicar terminología y teoría de grupos libres abelianos a retículos. Recordar que un grupo libre abeliano es un grupo abeliano dotado de una base en la que cualquier elemento puede expresarse de forma unívoca como combinación lineal de los elementos de la base.

Sea el subconjunto $X \subseteq \mathbb{R}^n$ y sea $B_r\,[0]$ la bola de radio $r \in \mathbb{R}^+$ y centro el origen, diremos que X es un *conjunto discreto* si y solo si la intersección de X con $B_r\,[0]$ es finita.

Teorema 2.1. *Un subgrupo aditivo de $\mathbb{R}^n$ es un retículo $\Longleftrightarrow$ es discreto.*

Demostración. Suponer que L es un retículo en $\mathbb{R}^n$ de dimensión n con generadores $\{e_1,\cdots,e_n\}$. Para probar la primera implicación tenemos que ver que la intersección de L con cualquier bola $B_r\,[0]$ resulta un conjunto finito. Si pasamos al subespacio extendido por L tenemos que la familia de vectores $\{e_1,\cdots,e_n\}$ es una base de $\mathbb{R}^n$. Entonces, para cada $v \in \mathbb{R}^n$ podemos poner de forma unívoca:

$$v = \lambda_1 e_1 + \cdots + \lambda_n e_n \quad (\lambda_i \in \mathbb{R})$$

Definimos la aplicación $f : \mathbb{R} \to \mathbb{R}$ dada por $f\,(\lambda_1 e_1 \cdots + \lambda_n e_n) = (\lambda_1,\cdots,\lambda_n)$, de modo que el conjunto de los puntos de $B_r\,[0]$ está acotado por f ya que:

$$\|f\,(v)\| = \|(\lambda_1,\cdots,\lambda_n)\| \leq K \quad (\forall v \in B_r\,[0]\,, K < \infty)$$

Si consideramos los puntos $\sum_{i=1}^{n} \mu_i e_i \in B_r\,[0]$ con $\mu_i \in \mathbb{Z}$ tenemos la intersección $L \cap B_r\,[0]$. Sabemos además que:

$$|\mu_i| \leq \|(\mu_1,\cdots,\mu_n)\| \leq K \tag{2.1}$$

Como el número de $\mu_i \in \mathbb{Z}$ verificando (2.1) es finito, $L \cap B_r\,[0]$ también será finito, por ser un subconjunto de las soluciones de (2.1). Por tanto, L es discreto.

La segunda implicación, que un subgrupo discreto G de $\mathbb{R}^n$ es un retículo, la probamos de forma inductiva sobre n. Es trivial ver que un subgrupo aditivo discreto de $\mathbb{R}$ es un retículo, luego tenemos que se cumple para $n = 1$.
Si tomamos un subconjunto maximal de G generado por $\{g_1,\cdots,g_m\}$ y considerando el subespacio V extendido por $\{g_1,\cdots,g_{m-1}\}$, tenemos que el subgrupo $G_o = G \cap V$ es discreto. Entonces, por inducción, suponemos que G_o es un retículo, de modo que existen elementos $h_1,\cdots,h_t$ linealmente independientes que generan G_o. Pero como $g_1,\cdots,g_{m-1} \in G_o$ ha de ser $m-1 = t$, por lo que podemos asumir que

todo elemento de G_o es una combinación $\mathbb{Z}$-lineal de $\{g_1, \cdots, g_{m-1}\}$. Ahora, sea T el suconjunto de G formado por los elementos $x = a_1 g_1 + \cdots + a_m g_m$ con los a_i verificando:

$$\begin{array}{l} 0 \leq a_i < 1 \quad (i = 1, \cdots, m-1) \\ 0 \leq a_m \leq 1 \end{array}$$

(Notar que T está acotado por ser G discreto).
Se demuestra que existe un $x' \in T$ de la forma $x' = b_1 g_1 + \cdots + b_m g_m$ con b_m el coeficiente a_m no nulo mas pequeño, de modo que $\{g_1, \cdots, g_{m-1}, x'\}$ es una familia linealmente independiente que genera G. Por tanto, por inducción, G es un retículo. □

Sea L el retículo generado por la familia de vectores $\{e_1, \ldots, e_n\}$, definimos el *dominio fundamental* de L como el conjunto:

$$\mathbb{T} = \left\{ \sum_{i=1}^{n} a_i e_i | 0 \leq a_i < 1, a_i \in \mathbb{R} \right\}$$

Observar que $\mathbb{T}$ depende de la elección de los generadores $\{e_i\}_{i \in \mathbb{N}}$.

Lema 2.2. *Sea $\mathbb{T}$ un dominio fundamental del retículo L, todo elemento de $\mathbb{R}^n$ está en uno de los conjuntos $\mathbb{T} + l$, $l \in L$.*

Demostración. Probamos este resultado desde un punto de vista más intuitivo. Dado un retículo L en $\mathbb{R}^n$ generado por $\{e_1, \ldots, e_n\}$, su dominio fundamental en este caso es el politopo (poliedro n-dimensional) de vértices el origen, los puntos e_i y los puntos resultantes de sumar los e_i entre ellos; Podemos desplazar este dominio fundamental mediante traslaciones con elementos de L y así abarcar cualquier punto de $\mathbb{R}^n$.
La siguienete figura acalara perfectamente el concepto de *dominio fundamental* de un *retículo* y la traslación $\mathbb{T} + l$:

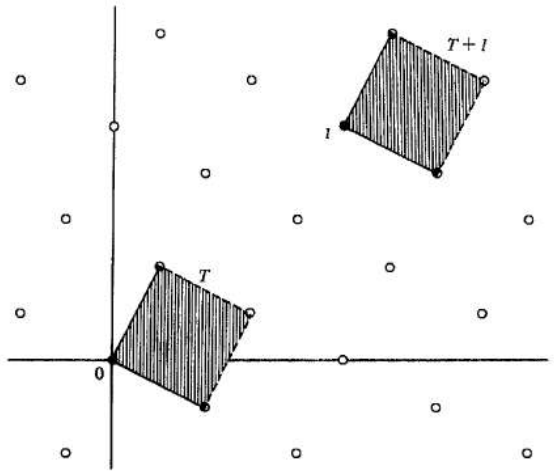

Figura 2.3: Dominio fundamental en $\mathbb{R}^2$ para el retículo de la figura 2.1 y la traslación $\mathbb{T} + l$.

□

Dado un subconjunto $X \subseteq \mathbb{R}^m$, se define el *volumen* de X como:

$$v(X) = \int_X dx_1 \cdots dx_n$$

donde $(x_1 \cdots x_n)$ son coordenadas de $\mathbb{R}^n$. Como el *dominio fundamental* $\mathbb{T}$ de un retículo L de dimensión m es un subconjunto de $\mathbb{R}^n$, podemos expresar su *volumen* como:

$$v(\mathbb{T}) = \int_{\mathbb{T}} dx_1 \cdots dx_m$$

Lema 2.3. *Sea L un retículo n-dimensional en $\mathbb{R}^n$ con base $\{e_1, \cdots, e_n\}$ y suponer $e_i = (a_{1i}, \cdots, a_{ni})$. Entonces el volumen del dominio fundamental $\mathbb{T}$ de L es $v(\mathbb{T}) = \left|det\,(a_{ij})\right|$.*

Demostración. Sabemos por definición de volumen que

$$v(\mathbb{T}) = \int_{\mathbb{T}} dx_1 \cdots dx_m \quad ((x_1 \cdots x_n) \text{ coordenadas de } \mathbb{R}^n)$$

Hacemos el cambio de variable:

$$x_i = \sum_{j=1}^{n} a_{ij} y_j$$

El jacobiano de esta transformación es $det\,(a_{ij})$. Entonces, aplicando el cambio en la integral y por teoría de cambio de variable en integración múltiple tenemos:

$$v(T) = \int_{\mathbb{T}} \left|det\,(a_{ij})\right| dy_1 \cdots dy_n = \left|det\,(a_{ij})\right| \int_0^1 dy_1 \cdots \int_0^1 dy_n = \left|det\,(a_{ij})\right|$$

□

Observación: Un *retículo* admite distintas $\mathbb{Z}$-bases generadoras, las cuales estan relacionadas por una matriz unimodular (módulo del determinante es 1). Entonces, por el lema anterior, los distintos *dominios fundamentales* generados por cada una de las $\mathbb{Z}$-bases tienen el mismo volumen.

2.2. Espacios reticulados asociados a un cuerpo de números

En esta sección, dado un cuerpo K, vamos a construir y describir su espacio asociado $\mathbb{L}^{st}$, el cual nos será de gran utilidad para poder desarrollar un método que nos lleve de K a un espacio vectorial real.

Recordando el Teorema 1.5 del Capítulo 1, sabemos que un cuerpo $K = \mathbb{Q}(\theta)$ (θ algebraico) de grado n genera n homomorfismos $\sigma_i : K \to \mathbb{C}$ distintos. Pueden suceder dos cosas:

1. $\sigma_i(K) \subseteq \mathbb{R} \Longleftrightarrow \sigma_i(\theta) = \theta_i \in \mathbb{R}$
2. $\sigma_i(K) \nsubseteq \mathbb{R}$. Es decir $\sigma_i(K) \subseteq \mathbb{C} \Longleftrightarrow \sigma_i(\theta) = \theta_i \in \mathbb{C}$.

En este segundo caso, como la conjugación compleja es un automorfismo en $\mathbb{C}$, tenemos que al ser $\sigma_i : K \longrightarrow \mathbb{C}$ un homomorfismo, $\overline{\sigma}_i : K \longrightarrow \mathbb{C}$ también lo será; de modo que $\overline{\sigma}_i = \sigma_j$ para algún $j \in (i, \ldots, n), j \neq i$.
Es decir, los homomorfismos complejos vienen dados en pares conjugados. Por lo tanto, para K cuerpo de grado n tendremos s homomorfismos reales y $2t$ homomorfismos complejos ($n = s + 2t$)

$$\underbrace{\sigma_1, \cdots, \sigma_s}_{\text{reales}}, \underbrace{\sigma_{s+1}, \overline{\sigma}_{s+1}, \sigma_{s+2}, \overline{\sigma}_{s+2}, \cdots, \sigma_{s+t}, \overline{\sigma}_{s+t}}_{\text{imaginarios}}$$

Sea K un cuerpo de grado n como hasta ahora, definimos su *espacio* $\mathbb{L}^{st}$ como:

$$\mathbb{L}^{st} = \mathbb{R}^s x \mathbb{C}^t$$

siendo los parámetros s y t el número de homomorfismos reales y complejos (pares conjugados) construidos a partir de K. Es decir, $\mathbb{L}^{st}$ es el conjunto de las $(s+t)$-tuplas:

$$(x_1,\cdots,x_s,y_1+iz_1,\cdots,y_t+iz_t) \quad x_i,y_i,z_i\in\mathbb{R} \tag{2.2}$$

Notar que podemos ver $\mathbb{L}^{st}$ como un espacio vectorial de dimensión n sobre $\mathbb{R}$; en este sentido, la base usual es:

$$\begin{cases} (1,0,\cdots,0;0,\cdots,0)\\ (0,1,\cdots,0;0,\cdots,0)\\ \cdots\\ (0,0,\cdots,1;0,\cdots,0)\\ (0,0,\cdots,0;1,0,\cdots,0)\\ (0,0,\cdots,0;i,0,\cdots,0)\\ \cdots\\ (0,0,\cdots,0;0,0,\cdots,1)\\ (0,0,\cdots,0;0,0,\cdots,i) \end{cases} \tag{2.3}$$

Con respecto a esta base, los elementos de la forma (2.2) tienen coordenadas:

$$(x_1,\cdots,x_s,y_1,z_1,\cdots,y_t,z_t)$$

Observar que $\mathbb{L}^{st}$ también tiene estructura de anillo con las operaciones asociadas, de tal manera que:

- $(\cdot):\mathbb{L}^{st}\times\mathbb{L}^{st}\to\mathbb{L}^{st}, \quad (x,x')\to(x_1+x_1',\cdots,x_s+x_s',(y_1+y_1')+i(z_1+z_1'),\cdots,(y_t+y_t')+i(z_t+z_t'))$
- $(+):\mathbb{L}^{st}\times\mathbb{L}^{st}\to\mathbb{L}^{st}, \quad (x,x')\to(x_1x_1',\cdots,x_sx_s',(y_1y_1'-z_1z_1')+i(y_1z_1'+y_1'z_1),\cdots,(y_ty_t'-z_tz_t')+i(y_tz_t'+y_t'z_t))$

Ahora, para un cierto cuerpo K, conocidos los homomorfismos σ_i que genera y su espacio $\mathbb{L}^{st}$, definimos la *aplicación estándar* $\sigma:K\longrightarrow\mathbb{L}^{st}$ dada por:

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

Es claro que σ es un homomorfismo entre anillos, luego $\forall\alpha,\beta\in K$ será:

$$\begin{gathered}\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)\\ \sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)\end{gathered}$$

Sea $x=(x_1,\cdots,x_s,y_1+iz_1,\cdots,y_t+iz_t)\in\mathbb{L}^{st}$ como antes, se define la *norma en* $\mathbb{L}^{st}$ como la aplicación $N:\mathbb{L}^{st}\to\mathbb{R}$ dada por:

$$x\mapsto x_1\cdots x_s|y_1+iz_1|^2\cdots|y_t+iz_t|^2=x_1\cdots x_s\left(y_1^2+z_1^2\right)\cdots\left(y_t^2+z_t^2\right)$$

Se deduce inmediatamente que $N(xy)=N(x)N(y)\,(\forall x,y\in L^{st})$.

Teorema 2.4. *Si $\alpha_1,\ldots,\alpha_n$ es una base de K respecto de $\mathbb{Q}$ entonces $\sigma(\alpha_1),\ldots,\sigma(\alpha_n)$ es una familia de vectores linealmente independientes respecto de $\mathbb{R}$.*

Idea de la demostración: La independencia de los α_i sobre $\mathbb{Q}$ es inmediata debido a que σ es inyectiva. Para verlo sobre $\mathbb{R}$ se necesita un resultado mas fuerte. Escribimos

$$\begin{aligned}\sigma_i(\alpha_l)&=x_i^{(l)} && (i=1,\cdots,s)\\ \sigma_{s+j}(\alpha_l)&=y_j^{(l)}+z_j^{(l)} && (j=1,\cdots,t)\end{aligned}$$

con $x_i^{(l)}, y_i^{(l)}, z_i^{(l)}$ reales y $l \in (1, \cdots, n)$. Para cada elemento de la base α_l será:

$$\sigma(\alpha_l) = \left(x_1^{(l)}, \cdots, x_s^{(l)}, y_1^{(l)} + iz_1^{(l)}, \cdots, y_t^{(l)} + iz_t^{(l)}\right)$$

De modo que si:

$$D = \begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \cdots & y_t^{(1)} & z_t^{(1)} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \cdots & y_t^{(n)} & z_t^{(n)} \end{vmatrix} \neq 0$$

probaremos el enunciado. Se demuestra por métodos constructivos que $(-2i)^t D = det(\sigma_i(\alpha_j)) \neq 0$ ya que la matriz $(\sigma_i(\alpha_j))(i, j = 1, \cdots, n)$ es una matriz de tipo Vandermonde. Luego efectivamente $D \neq 0$.

Corolario 2.5. *Si G es un subgrupo de $(K, +)$ finitamente generado con $\mathbb{Z}$-base $(\alpha_1, \ldots, \alpha_n)$, entonces la imagen de G por σ en $\mathbb{L}^{st}$ es un retículo con generadores $(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$.*

Observación Con lo visto hasta ahora es claro que σ dota a K de una *representación geométrica* en $\mathbb{L}^{st}$. Aunque no tenemos espacio para profundizar, mencionar que cuando trabajamos en $\mathbb{L}^{st}$ como espacio vectorial, la base (2.3) es la utilizada en el cálculo de distancias entre elementos de $\mathbb{L}^{st}$, ya que $\mathbb{L}^{st}$ como espacio vectorial es isomorfo a $\mathbb{R}^{s+2t}$, por lo que podemos trasladar la métrica euclídea usual de un espacio a otro.

Por último, exponemos el siguiente enunciado referido a retículos y volúmenes en $\mathbb{L}^{s+t}$. Es un resultado muy concreto que se excede de lo que hemos visto hasta ahora y que por tanto no vamos a demostrar. Sin embargo nos será de gran ayuda en el Capítulo 3, ya que llegado el momento lo necesitaremos de forma auxiliar para demostrar el *Teorema de las Unidades de Dirichlet*.

Lema 2.6. *Sea L un retículo en $\mathbb{L}^{s+t}$ de dimensión $s+2t$ con un dominio fundmental de volumen V. Sean $c_1 \cdots c_{s+t}$ números reales positivos cuyo producto cumple:*

$$c_1 \cdots c_{s+t} > \left(\frac{4}{\pi}\right)^t V \tag{2.4}$$

entonces existe en L un elemento no nulo $x = (x_1 \cdots x_{s+t})$ tal que:

$$\begin{aligned} |x_k| &< c_k \qquad (k = 1, \cdots, s) \\ |x_{s+j}|^2 &< c_{s+j} \quad (j = 1, \cdots, t) \end{aligned}$$

2.3. Espacio logarítmico asociado a un cuerpo de números

En la última parte de este capítulo vamos a determinar, para un cuerpo de números K, qué y cuál es su *espacio logarítmico*.

Sean $K = \mathbb{Q}(\theta)$ cuerpo de grado n y el espacio $\mathbb{L}^{st}$ como hasta ahora. Definimos como *espacio logarítmico asociado a K* al espacio $\mathbb{R}^{s+t}$, donde los parámetros s y t corresponden a las $s+2t$ $\mathbb{Q}$-*incrustaciones* de K en $\mathbb{C}$. Llegados a este punto describimos el método que nos lleva cada elemento de K a su correspondiente en el *espacio logarítmico* $\mathbb{R}^{s+t}$.

1. Definimos la aplicación:

$$\begin{aligned} l : \mathbb{L}^{st} &\longrightarrow \mathbb{R}^{s+t} \\ x &\longmapsto (l_1(x), \cdots, l_s(x), l_{s+1}(x), \cdots, l_{s+t}(x)) \end{aligned}$$

De modo que para un $x=(x_1,\cdots,x_s,x_{s+1},\cdots,x_{s+t})\in\mathbb{L}^{st}$, l está definida como:

$$l_k(x)=\begin{cases} log\,|x_k| & para\ \text{k=1,...,s} \\ log|x_k|^2 & para\ \text{k=s+1,...,s+t} \end{cases}$$

De la propiedad aditiva del logaritmo tenemos la propiedad inmediata para l:

$$l(xy)=l(x)+l(y) \quad \left(\forall x,y\in\mathbb{L}^{st}\right)$$

Además, de la norma definida en la sección anterior tenemos :

$$\sum_{k=1}^{s+t} l_k(x)=log\,|N(x)| \quad \left(\forall x\in\mathbb{L}^{st}\right)$$

Observación: Los $x\in\mathbb{L}^{st}$ con todas las componentes no nulas forman un grupo bajo multiplicación, de modo que l define un homomorfismo entre este grupo y $\mathbb{R}^{s+t}$.

2. Establecemos una correspondencia biyectiva entre cualquier elemento de K y la *aplicación estándar* σ.
   Es decir, identificamos cualquier $\alpha\in K$ con los $n=s+2t$ homomorfismos que define K para ese α, esto es:
   $$\alpha=\sigma(\alpha)=\underbrace{\sigma_1(\alpha),\cdots,\sigma_s(\alpha)}_{\mathbb{R}},\underbrace{\sigma_{s+1}(\alpha),\cdots,\sigma_{s+t}(\alpha)}_{\mathbb{C}}$$

3. Por último, vamos a incorporar la identificación $\alpha=\sigma(\alpha)$ del apartado 2 en la aplicación l del apartado anterior, redefiniéndola como sigue:
   $$l:K\longrightarrow\mathbb{L}^{st}\longrightarrow\mathbb{R}^{s+t}$$
   $$l(\alpha)\longmapsto l(\sigma(\alpha))\longmapsto\left(log\,|\sigma_1(\alpha)|,\ldots,log\,|\sigma_s(\alpha)|,log|\sigma_{s+1}(\alpha)|^2,\ldots,log|\sigma_{s+t}(\alpha)|^2\right) \quad (2.5)$$
   Se sigue como antes que $l(\alpha\beta)=l(\alpha)+l(\beta),\forall\alpha,\beta\in K$. Es decir, l es un homomorfismo entre el grupo multiplicativo $K^*=K\setminus\{0\}$ y el grupo aditivo de $\mathbb{R}^{s+t}$.
   Además, como $l(\alpha)=l(\sigma(\alpha))$ será:
   $$\sum_{k=1}^{s+t} l_k(\alpha)=log\,|N(\alpha)|$$

Se dice que la aplicación $l:K\longrightarrow\mathbb{R}^{s+t}$ es la *representación logarítimica de K*.

Capítulo 3

El teorema de las unidades de Dirichlet

Este capítulo se dedica esencialmente a la demostración del Teorema que motiva este trabajo fin de grado, recordémoslo:

Teorema. *El grupo de las unidades $\mathscr{O}_K^*$ del anillo de enteros algebraicos $\mathscr{O}_K$ de un cuerpo K es de tipo finito y puede describirse como:*

$$\mathscr{O}_K^* \cong L_K \times T_K$$

donde L_K (parte libre) es un grupo abeliano de rango $s+t-1$ y T_K (parte de torsión) es un grupo abeliano cíclico finito de orden par formado por las raíces de la unidad de K.

Su demostración es extensa y sigue una disposición escalonada; es decir, no probamos el teorema de una vez, sino que vamos demostrando una serie de resultados que desembocan en el *Teorema de las unidades*. Asimismo, este capítulo justifica en cierta forma los capítulos anteriores, ya que nos serviremos de muchos de los resultados vistos en ellos.

Encajamiento del grupo unidad en el espacio logarítmico: Con la notación usual, sea K un cuerpo de números cualquiera y $\mathscr{O}_K^*$ el grupo de las unidades del anillo de enteros $\mathscr{O}_K$, restringimos la representación logarítmica de K (2.5) al grupo de las unidades $\mathscr{O}_K^*$:

$$l : \mathscr{O}_K^* \longrightarrow \mathbb{R}^{s+t}$$

Esta aplicación relaciona el grupo de las unidades, que es multiplicativo, con el espacio logarítmico, que es aditivo. Notar además que l es un homomorfismo no inyectivo.

Lema 3.1. *El núcleo W de $l : \mathscr{O}_K^* \longrightarrow \mathbb{R}^{s+t}$ es el conjunto de todas las raíces de la unidad pertenecientes a $\mathscr{O}_K^*$. Además, se trata de un grupo cíclico finito de orden par.*

Demostración. Por definición de núcleo, $W = \{X \in \mathscr{O}_K^* |\ l(X) = 0\}$ y es claro que:

$$l(X) = 0 \Longleftrightarrow |\sigma_i(X)| = 1 \ \ (\forall i \in (1,\ldots,s+t))$$

Sea $\alpha \in \mathscr{O}_K^*$, por el Teorema 1.10 su polinomio mínimo $m_\alpha(X)$ tiene coeficientes en $\mathbb{Z}$ por ser α entero algebraico. Sabemos además, por lo visto en el Capítulo 1, que el polinomio de cuerpo $f_\alpha(X)$ es potencia de $m_\alpha(X)$. Luego será:

$$f_\alpha(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha)) \in \mathbb{Z}[X]$$

Llegados a este punto, precisamos del siguiente resultado teórico (no lo demostraremos): *"Dado un polinomio mónico p con coeficientes en $\mathbb{Z}$, los ceros de p que en $\mathbb{C}$ tengan valor absoluto 1 serán raíces de la unidad"*

Como $f_\alpha(X) \in \mathbb{Z}[X]$ cumple las condiciones del enunciado anterior y todas sus raices son $\sigma_i(\alpha) \in \mathbb{C}$ con $|\sigma_i(\alpha)| = 1$, es claro que $\sigma_i(\alpha)$ es una raíz de la unidad $\forall i \in (1,\dots,n)$. Con esto queda probada la primera parte.
Veamos que W es un grupo cíclico finito de orden par. Tenemos que $\mathscr{O}_K$ es un subgrupo aditivo finitamente generado y que además está dotado de una $\mathbb{Z}$-base, entonces por el Corolario 2.5 la imagen de $\mathscr{O}_K$ por σ en $\mathbb{L}^{st}$ es un retículo. Se sigue, por el Teorema 2.1, que el subgrupo $(\sigma(\mathscr{O}_K),+)$ es discreto. Por tanto, si tomamos el círculo unidad en $\mathbb{C}$ tenemos que σ nos lleva a un subconjunto acotado en $\mathbb{L}^{st}$, de lo cual se sigue que $\mathscr{O}_K$ contiene sólo un número finito de raíces de la unidad, luego efectívamente W es finito.
Por el Lema 1.4 sabemos que cualquier subgrupo finito de K^* es cíclico, luego W es cíclico (notar que $0 \notin W$). Finalmente, como $-1 \in W$ tiene orden 2, tenemos que W tiene orden par. □

Lema 3.2. *La imagen E de $\mathscr{O}_K^*$ por l en $\mathbb{R}^{s+t}$ es un retículo de dimensión $\leq s+t-1$.*

Demostración. En primer lugar tenemos que para toda unidad ε, su norma es ± 1. Luego será:

$$\sum_{k=1}^{s+t} l_k(\varepsilon) = log\,|N(\varepsilon)| = log\,|\pm 1| = 0 \ \ (\forall \varepsilon \in \mathscr{O}_K^*)$$

Por lo tanto, todos los elementos de E están en el subespacio de $\mathbb{R}^{s+t}$ cuyos elementos $(x_1,\dots,x_{s+t})$ satisfacen:

$$x_1 + \cdots + x_{s+t} = 0$$

Llamamos a este subespacio V. Es claro que V tiene dimension $s+t-1$. Y como $E \leq V$ es claro que $dim(E) \leq s+t-1$.
Ahora nos falta ver que E es un retículo. Para ello es suficiente con probar que E es discreto por el Teorema 2.1.
Consideremos la aplicación distancia $\|\cdot\|$ en $\mathbb{R}^{s+t}$ y supongamos $\|l(\varepsilon)\| < r$ $(0 < r \in \mathbb{R})$ y $\varepsilon \in \mathscr{O}_K^*$. Como $|l_k(\varepsilon)| \leq \|l(\varepsilon)\| < r$ se deduce que:

$$|\sigma_k(\varepsilon)| < e^r \ \ para \ \ (k = 1,\cdots,s)$$
$$\left|\sigma_{s+j}(\varepsilon)\right|^2 < e^r \ \ para \ \ (k = s,\cdots,t)$$

Por tanto, el conjunto de puntos $\sigma(\varepsilon)$ de $\mathbb{L}^{st}$ correspondientes por l a las unidades con $\|l(\varepsilon)\| < r$ está acotado, luego es finito por el Corolario 2.5.
Por tanto, la intersección de E con cualquier bola cerrada $B_r[0]$ en $\mathbb{R}^{s+t}$ es un conjunto finito, es decir, E es discreto. Por consiguiente, E es un retículo. □

Lema 3.3. *Sea L un retículo en $\mathbb{R}^m$. Entonces L tiene dimensión m si y solo si existe un subconjunto acotado B de $\mathbb{R}^m$ tal que:*

$$\mathbb{R}^m = \bigcup_{l \in L} l + B$$

Demostración. Sea L un retículo de dimension m en $\mathbb{R}^m$ y sea $\mathbb{T}$ un dominio fundamental de L (da igual la base generadora de L), por el Lema 2.2 todo elemento de $\mathbb{R}^m$ está en uno de los conjuntos $\mathbb{T}+l$, es decir:

$$\forall x \in \mathbb{R}^m \ \exists l \in L \ tal \ que \ x \in \mathbb{T} + l$$

Luego, si renombramos como B al dominio fundamental de nuestro retículo L y generalizando para cualquier $x \in \mathbb{R}^m$ tenemos precisamente:

$$\mathbb{R}^m = \bigcup_{l \in L} l + B$$

Para la implicación inversa, supongamos que B es un subconjunto acotado de $\mathbb{R}^m$ tal que $\mathbb{R}^m = \bigcup_{x \in L} x + B$. Vamos a probarlo por reducción al absurdo. Supongamos que L tiene dimensión $d < m$ y consideremos el subespacio V de $\mathbb{R}^m$ extendido por L. Como $dim(L) < m$, entonces $dim(V) < dim(\mathbb{R}^m)$; Podemos encontrar un complemento ortogonal V' de V tal que:

$$\mathbb{R}^m = V' \oplus V$$

Considerando la identificación ya mencionada de L con el subespacio V se tiene por hipótesis que

$$\mathbb{R}^m = \bigcup_{v\in V} v + B$$

Ahora, bajo la aplicación proyección $\pi : R^m \longrightarrow V'$ tenemos que V' es la imagen de B por π. Y como π preserva la distancia entonces $V' = \pi(B)$ está acotado por ser B un conjunto acotado. Entramos en contradicción ya que V' no está acotado, por tanto ha de ser $dim(L) = m$. □

Lema 3.4. *Sea $y \in \mathbb{L}^{st}$ y sea $\lambda_y : \mathbb{L}^{st} \longrightarrow \mathbb{L}^{st}$ definida como $\lambda_y(x) = yx$. Entonces λ_y es una aplicación lineal y $det(\lambda_y) = N(y)$.*

Demostración. Es claro que λ_y es lineal. Para calcular $det(\lambda_y)$ usamos la base usual de $\mathbb{L}^{st}$ que vimos en (2.3). Entonces, sea $y = (x_1, \cdots, x_s, y_1 + iz_1, \cdots, y_t + iz_t) \in \mathbb{L}^{st}$, obtenemos para el $det(\lambda_y)$ la expresión:

$$det(\lambda_y) = \begin{vmatrix} x_1 & & & & & & & & \\ & \ddots & & & & & 0 & & \\ & & x_s & & & & & & \\ & & & y_1 & -z_1 & & & & \\ & & & z_1 & y_1 & & & & \\ & & & & & \ddots & & & \\ & 0 & & & & & y_t & -z_t \\ & & & & & & z_t & y_t \end{vmatrix} = x_1 \cdots x_s \left(y_1^2 + z_1^2\right) \cdots \left(y_t^2 + z_t^2\right) = N(y)$$

□

Teorema 3.5. *La imagen E de $\mathscr{O}_K^*$ en $\mathbb{R}^{s+t}$ es un retículo de dimensión $s+t-1$.*

Demostración. La parte de que E es un retículo ya ha sido demostrada en el Lema 3.2, veamos que tiene dimension $s+t-1$. Sea V la extensión de E como subespacio vectorial de $\mathbb{R}^{s+t}$, recordemos que sus elementos satisfacían:

$$x_1 + \cdots + x_{s+t} = 0$$

Luego es claro que $dim(V) = s+t-1$. Para ver que $dim(E) = dim(V)$ tenemos que aplicar el Lema 3.3, pero ahora en vez de considerar el espacio $\mathbb{R}^{s+t}$ trabajaremos con el subespacio V. Como E es un retículo contenido en V y $dim(V) = s+t-1$, si encontramos un subconjunto acotado B de V tal que:

$$V = \bigcup_{e\in E} e + B \tag{3.1}$$

tendremos el resultado, es decir, que $dim(E) = s+t-1$. Buscamos entonces un B adecuado que verifique lo anterior.
Todo punto en V es la imagen bajo l de algun punto en $\mathbb{L}^{st}$, es más:

$$l(x) \in V \Longleftrightarrow |N(x)| = 1 \ \left(\forall x \in \mathbb{L}^{st}\right)$$

Luego si definimos el conjunto:

$$S = \left\{x \in \mathbb{L}^{st} \,|\, |N(x)| = 1\right\} \longrightarrow \ l(S) = V$$

Ahora, notar que si un conjunto X_o está acotado, entonces también lo está $l(X_o)$ ya que l preserva la distancia. Asimsmo, los $x = \sigma(\varepsilon)$ con ε unidad son elementos de S, luego los elementos $\sigma(\varepsilon)X_o$ también están en S.
La idea entonces es encontrar un conjunto acotado X_o contenido en S que verifique:

$$S = \bigcup_{\varepsilon\in\mathscr{O}_K^*} \sigma(\varepsilon)X_o \tag{3.2}$$

Operando con l y teniendo en cuenta que $l(xy) = l(x) + l(y)$ y $l\left(\bigcup_{x\in X} x\right) = \bigcup_{x\in X} l(x)$ desarrollamos como sigue:

$$V = l(S) = l\left(\bigcup_{\varepsilon\in\mathscr{O}_K^*} \sigma(\varepsilon)X_o\right) = \bigcup_{\varepsilon\in\mathscr{O}_K^*} l(\sigma(\varepsilon)) + l(X_o) = \bigcup_{e\in E} e + B$$

Resumiendo, tenemos que encontrar un X_o que verifique (3.2) ya que en ese caso habremos encontrado un conjunto acotado B en V que verifique (3.1) y se cumplirá el enunciado del teorema.

Sea M el retículo en $\mathbb{L}^{st}$ corrrespondiente a $\mathscr{O}_K$ bajo σ ($\mathscr{O}_K$ anillo de enteros algebraicos de K). Si tomamos un $y \in S$ y consideramos la transformación lineal del Lema 3.4 tenemos que $det(\lambda_y) = N(y) = \pm 1$, es decir, λ_y es unimodular; luego las bases de los retículos M e $yM = \lambda_y(M)$ están relacionadas por una matriz unimodular. Entonces, se sigue por la observación posterior al Lema 2.3 que el volumen del dominio fundamental de M es igual al volumen del dominio fundamental de yM $(\forall y \in S)$. Llamamos a dicho volumen v. Ahora, fijado v, elegimos números reales c_i $(i = 1, \cdots, s+t)$ tal que:

$$c_1 \cdots c_{s+t} = Q > \left(\frac{4}{\pi}\right)^t v \tag{3.3}$$

Determinamos un conjunto X, formado por los $x \in \mathbb{L}^{st}$ que cumplen:

$$\begin{cases} |x_k| < c_k & (k = 1, \cdots, s) \\ |x_{s+j}|^2 < c_{s+j} & (j = 1, \cdots, t) \end{cases} \tag{3.4}$$

Entonces, como se verifican las condiciones del Lema 2.6. existirá en yM un elemento $0 \neq x \in X$, de modo que podemos escribir:

$$x = y\sigma(\alpha) \quad (0 \neq \alpha \in \mathfrak{D}) \tag{3.5}$$

Si aplicamos la norma a ambos lados tenemos:

$$N(x) = N(y)N(\sigma(\alpha)) =^+_- N(\alpha) \quad (0 \neq \alpha \in \mathfrak{D})$$

Se sigue por (3.3) y (3.4) que $|N(\alpha)| < Q$.

Se puede demostrar que solo un número finito de ideales del anillo de enteros tienen norma dada. Por tanto, el número de ideales de $\mathscr{O}_K$ con norma $< Q$ es finito. Considerando los ideales principales y recordando que sus generadores son ambiguos hasta múltiplos de la unidad, se sigue que en $\mathscr{O}_K$ existe un número finito de elementos $\sigma_1 \ldots \sigma_N$ asociados dos a dos, cuyas normas son $< Q$ en valor absoluto. Así, para algún $i \in (1, \cdots, N)$ podemos poner $\alpha\varepsilon = \alpha_i$ con $\varepsilon \in \mathscr{O}_K^*$ unidad. Si despejamos $y \in S$ de la expresión (3.5) y combinamos con lo anterior teniendo en cuenta que $\alpha = \alpha_i\varepsilon^{-1}$ y que σ es un homomorfismo:

$$y = x\sigma^{-1}(\alpha) = x\sigma\left(\alpha^{-1}\right) = x\sigma\left(\left(\alpha_i\varepsilon^{-1}\right)^{-1}\right) = x\sigma\left(\alpha_i^{-1}\varepsilon\right) = x\sigma\left(\alpha_i^{-1}\right)\sigma(\varepsilon) \tag{3.6}$$

Definimos:

$$X_o = S \cap \left(\bigcup_{i=1}^{N} \sigma\left(\alpha_i^-\right)X\right)$$

Como X está acotado (por definición) también lo estarán los conjuntos $\sigma\left(\alpha_i^{-1}\right)X$, y como N es un número finito, X_o está acotado, luego está bien definido. Notar que el conjunto X_o no depende de la elección del $y \in S$.
Si nos fijamos en la expresión (3.6) tenemos que $y = x\sigma\left(\alpha_i^{-1}\right)\sigma(\varepsilon)$ con $y \in S$ y $\sigma(\varepsilon) \in S$, entonces $x\sigma\left(\alpha_i^{-1}\right) \in S$. Luego, por definición de X_o será $x\sigma\left(\alpha_i^{-1}\right) \in X_o$.

Con todo lo recabado hasta ahora es momento de comprobar si X_o verifica la expresión:

$$S = \bigcup_{\varepsilon \in \mathscr{O}_K^*} \sigma(\varepsilon) X_o$$

$\Rightarrow$) Tenemos que $y = \sigma(\varepsilon) x \sigma\left(\alpha_i^{-1}\right)$ con $x\sigma\left(\alpha_i^{-1}\right) \in X_o \quad \rightarrow \quad y \in \sigma(\varepsilon) X_o \quad \rightarrow \quad S \subseteq \bigcup_{\varepsilon \in \mathscr{O}_K^*} \sigma(\varepsilon) X_o$
$\Leftarrow$) Es claro que se cumple por ser $X_o \in S$ por definición y $\sigma(\varepsilon) \in S \; \forall \varepsilon \in \mathscr{O}_K^*$, luego es evidente que $\bigcup_{\varepsilon \in \mathscr{O}_K^*} \sigma(\varepsilon) X_o \subseteq S$.

Por tanto, hemos encontrado un conjunto acotado $X_o \in S$ que verifica (3.2) y por consiguiente hemos encontrado en V un conjunto acotado $B = l(X_o)$ tal que $V = \bigcup_{e \in E} e + B$. □

Teorema 3.6. *Para un cuerpo de números K el grupo de las unidades de $\mathscr{O}_K$ es isomorfo a:*

$$W \times \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{s+t-1}$$

Demostración. Por el teorema anterior tenemos que la imágen de $\mathscr{O}_K^*$ por l es un retículo E de dimensión $s+t-1$. Sea W el núcelo de l como en el Lema 3.1, por el primer teorema del isomorfismo será

$$\frac{\mathscr{O}_K^*}{W} \cong E$$

Pero recordar que un retículo tiene estructura de $\mathbb{Z}$-módulo; luego en nuestro caso, como $dim(E) = s+t-1$ entonces E es isomorfo al $\mathbb{Z}^{s+t-1}$. Sustituyendo queda:

$$\frac{\mathscr{O}_K^*}{W} \cong \mathbb{Z}^{s+t-1} \tag{3.7}$$

Habíamos visto que W es un grupo abeliano cíclico de tipo finito, de donde se sigue que $\mathscr{O}_K^*$ es un grupo abeliano finitamente generado. Entonces por el Teorema 1.2 podemos descomponer $\mathscr{O}_K^*$ en parte libre y parte de torsión:

$$\mathscr{O}_K^* = L(\mathscr{O}_K^*) \otimes T(\mathscr{O}_K^*)$$

Por la descripción de parte de torsión y parte libre en el Teorema 1.3 tenemos que $\mathscr{O}_K^*$ es isomorfo al producto directo de grupos cíclicos. Ahora, como W es finito por ser todos sus elementos de orden finito (raíces de la unidad) y $\dfrac{\mathscr{O}_K^*}{W}$ un grupo abeliano libre de torsión, se sigue que W es la parte de torsión de $\mathscr{O}_K^*$. Luego, W es el producto de todos los factores cíclicos finitos en la descomposición directa. El resto de factores son todos cíclicos de orden infinitoy corresponden a la parte libre de $\mathscr{O}_K^*$; fijándonos en (3.7) vemos que hay exactamente $s+t-1$ de ellos. Luego efectivamente será

$$\mathscr{O}_K^* \cong W \times \mathbb{Z}^{s+t-1} \tag{3.8}$$

con $T(\mathscr{O}_K^*) = W$ y $L(\mathscr{O}_K^*) = \mathbb{Z}^{s+t-1}$. □

3.1. Comentarios y conclusiones

Sea K un cuerpo de números con la notación usual, se sabe por lo anterior que la parte libre del subgrupo de las unidades ${O_K}^*$ viene dada por $L({O_K}^*) \cong \mathbb{Z}^{s+t-1}$, equivalentemente, el rango de ${O_K}^*$ es $s+t-1$. Recordar que s hace referencia al número de $\mathbb{Q}$-incrustaciones de K en $\mathbb{R}$ y t a los pares (conjugados) de $\mathbb{Q}$-incrustaciones de K en $\mathbb{C}$, de modo que el grado de K es $n = s+2t$. Supongamos el caso particular en el que el subgrupo de las unidades ${O_K}^*$ tiene rango $s+t-1=1$, es decir, su parte libre de torsión es un grupo cíclico infinito de la forma $L({O_K}^*) \cong \mathbb{Z}$. Es claro por (3.8) que:

$$ {O_K}^* \cong W \times \mathbb{Z} $$

y toda unidad de O_K será de la forma

$$ \zeta \cdot \eta^r \tag{3.9} $$

donde ζ es una raíz de la unidad de K y $r \in \mathbb{Z}$. Se puede demostrar que existe un único elemento generador minimal $\eta > 1$; se dice entonces que η es la *unidad fundamental* de ${O_K}^*$.

Para el *Teorema de las unidades* en el caso general, $s+t-1 \geq 1$, tenemos que $L({O_K}^*) \cong \mathbb{Z}^{s+t-1}$, de modo que existe una base de $s+t-1$ elementos generadores

$$ \eta_1, \cdots, \eta_{s+t-1} $$

llamado *sistema de unidades fundamentales* tal que toda unidad de O_K se descompone de forma única como:

$$ \zeta \cdot {\eta_1}^{r_1} \cdots {\eta_{s+t-1}}^{r_{s+t-1}} \tag{3.10} $$

donde ζ es una raíz de la unidad de K y $r_1, \cdots, r_{s+t-1} \in \mathbb{Z}$.

Nota: Es claro que para saber numericamente cuáles son las unidades de ${O_K}^*$ hay que conocer el *sistema de unidades fundamentales* según el caso. El *Teorema de las unidades* no nos permite hallar estos elementos ya que se limita a detallar la estructura de ${O_K}^*$ e inidicar si es de tipo finito ($s+t-1=0$) o infinito ($s+t-1 \geq 1$). Hallar *unidades fundamentales* requiere, en la mayoría de los casos, procedimientos muy pesados y ajenos a la naturaleza de este estudio, y que por tanto no veremos aquí.

Veamos el caso singular de que ${O_K}^*$ sea finito ($s+t-1=0$), es decir, que sea solo grupo de torsión (${O_K}^* \cong W$). Hay dos posibilidades:

1. $(s=1,\ t=0) \to K$ es de grado 1 sobre $\mathbb{Q}$, o lo que es lo mismo $K=\mathbb{Q}$. En este caso, como $\mathbb{Q} \subseteq \mathbb{R}$ y las únicas raicés de la unidad en $\mathbb{R}$ son ± 1, será ${O_K}^* = \{\pm 1\}$

2. $(s=0,\ t=1) \to K$ es de grado 2 con dos $\mathbb{Q}$-incrustaciones en $\mathbb{C}$ (la identidad y el conjugado), es decir, K es una *extensión cuadrática de tipo imaginario*. Tenemos por lo estudiado en las útimas secciones del Capítulo 1 que podemos expresar estos cuerpos como $K = \mathbb{Q}\left(\sqrt{d}\right)$ con $d<0$ un *entero libre de cuadrados*. Recordar que habíamos encontrado, con métodos deductivos, el subgrupo ${O_K}^*$ para cada $d<0$ (Teorema 1.12); ${O_K}^*$ era finito y estaba formado efectivamente por las raíces de la unidad de K.

Por último, estudiamos el subgrupo de las unidades para el caso $(s=2,\ t=0)$, es decir, para *cuerpos cuadráticos reales*. Escribíamos $K = \mathbb{Q}\left(\sqrt{d}\right)$ con $d>0$. Los métodos deductivos usados en el Capítulo 1 para hallar ${O_K}^*$ en el caso imaginario no nos servían para *cuerpos cuadráticos reales*. El *Teorema de las unidades* nos permite solventar esta problemática. Por (3.9) y teniendo en cuenta que las raíces de la unidad de $\mathbb{Q}\left(\sqrt{d}\right)$ son ± 1 por ser $\mathbb{Q}\left(\sqrt{d}\right) \subseteq \mathbb{R}$, será:

$$ {O_K}^* = \{\pm \eta^r |\ \eta \ unidad\ fundamental,\ r \in \mathbb{Z}\} $$

Luego existen infinitas unidades en O_K y vienen dadas por ${O_K}^* = \langle -1, \eta \rangle$.

Veamos un resultado práctico de aplicar el Teorema de las unidades en extensiones cuadráticas reales. Sabemos por el Teorema 1.11 que el anillo de enteros de $K = \mathbb{Q}(\sqrt{d})$ es:

$$O_K = \mathbb{Z}[\sqrt{d}] \text{ si } d \not\equiv 1 \ (mod\ 4) \ \wedge \ O_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \text{ si } d \equiv 1 \ (mod\ 4).$$

Entonces, sea $\alpha \in O_K$ tenemos que $\alpha \in {O_K}^*$ si y solo si existe elemento inverso β tal que $\alpha\beta = 1$. Aplicando normas tenemos $N(\alpha)N(\beta) = 1$, y como $N(\alpha), N(\beta) \in \mathbb{Z}$ ha de ser $N(\alpha) = \pm 1$. Distinguiendo según el valor de d:

- $d \not\equiv 1 \ (mod\ 4)$: Sea $\alpha = a + b\sqrt{d} \in O_K \ \ (a,b \in \mathbb{Z})$, entonces $\alpha \in {O_K}^* \Leftrightarrow N(\alpha) = \pm 1 \Leftrightarrow \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) \Leftrightarrow a^2 - db^2 = \pm 1$
- $d \equiv 1 \ (mod\ 4)$: Sea $\alpha = \frac{a+b\sqrt{d}}{2} \in O_K \ \ (a,b \in \mathbb{Z})$, entonces $\alpha \in {O_K}^* \Leftrightarrow N(\alpha) = \pm 1 \Leftrightarrow \left(\frac{a+b\sqrt{d}}{2}\right)\left(\frac{a-b\sqrt{d}}{2}\right) \Leftrightarrow a^2 - db^2 = \pm 4$

Por tanto, el *Teorema de las unidades* asegura la existencia de infinitas soluciones enteras x, y para las ecuaciones

$$(1)\ x^2 - dy^2 = 1 \qquad (2)\ x^2 - dy^2 = -1$$
$$(3)\ x^2 - dy^2 = 4 \qquad (4)\ x^2 - dy^2 = -4$$

con d entero libre de cuadrados positivo. A la ecuación (1) se la conoce como *ecuación de Pell*.

Bibliografía

[1] I. STEWART, *Algebraic Number Theory and Fermat´s Last Theorem*, University of Warwick, Mathematics Institute, 2002.

[2] R. B. ASH, *A course in Algebraic Number Theory, Chapter 6 (The Dirichlet Unit Theorem)*, Department of Mathematics, University of Illinois, https://faculty.math.illinois.edu/~r-ash/Ant/AntChapter6.pdf

[3] H. GANGL, *Number Theory Lecture Notes*, University of Durham, http://www.maths.dur.ac.uk/~dma0hg/lectures08.pdf

[4] A. ELDUQUE, *course notes Introduction to Algebra*, Universidad de Zaragoza, http://www.unizar.es/matematicas/algebra/elduque/files/IAElduqueRef.pdf,

[5] A. ELDUQUE, *course notes Algebra (Groups and Galois Theory)*, Universidad de Zaragoza, http://www.unizar.es/matematicas/algebra/elduque/files/GroupsGalois.pdf

[6] J. B. FRALEIGH, *A first course in abstract algebra*, Addison-Wesley, Reading MA, 1989.

[7] K. CONRAD, *Dirichlet´s Unit Theorem*, Department of Mathematics, University of Connecticut, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/unittheorem.pdf

[8] M. BAKER, *Algebraic number theory course notes*, School of Mathematics, Georgia Institute of Technology, http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf

[9] J. NEUKIRCH, *Algebraic number theory*, University of Regensburg, http://www.cimat.mx/~luis/seminarios/Teoria-de-Numeros/Neukirch_Algebraic_number_theory.pdf

[10] P. L. CLARK, *Pell equation notes*, University of Georgia, http://math.uga.edu/~pete/4400pellnotes.pdf

Índice alfabético