ARITMÉTICA EN CUERPOS DE NÚMEROS

INÉS PACHARONI

RESUMEN. Un cuerpo de números algebraico es un subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{Q}$ y que como $\mathbb{Q}$-espacio vectorial es de dimensión finita. El objetivo general de este curso es estudiar aritmética en el anillo de enteros de estos cuerpos, o sea estudiar números primos, divisibilidad de enteros, unidades, etc.

Nos concentraremos en particular en los cuerpos cuadráticos $\mathbb{Q}(\sqrt{m})$ y veremos cuáles de ellos admiten un algoritmo de Euclides en el anillo de enteros y en cuales es válido el Teorema Fundamental de la Aritmética, que dice que todo entero (no nulo y no una unidad) se descompone como producto de primos de manera esencialmente única.

Como consecuencia del estudio de la aritmética en los enteros de Gauss, probaremos un clásico teorema que caracteriza los números naturales que se pueden escribir como suma de dos cuadrados. Este teorema fue enunciado por Fermat alrededor del año 1640 y probado por Euler en 1793.

ÍNDICE

1. CUERPOS DE NÚMEROS ALGEBRAICOS

1.1. Números algebraicos.

Definición 1.1. Un número complejo α se dice *algebraico* si es raíz de un polinomio

$$a_n x^n + \cdots + a_0$$

donde los coeficientes $a_0, a_1, \ldots, a_n$ son números racionales no todos nulos.
Un número complejo α se dice *trascendente* si no es algebraico.

Dado α un número algebraico consideramos el conjunto

$$\mathcal{A} = \{f \in \mathbb{Q}[x] : f(\alpha) = 0\}.$$

Claramente $\mathcal{A}$ es un ideal en $\mathbb{Q}[x]$ y por lo tanto está generado por un polinomio p no constante, que podemos suponer mónico. Este polinomio es irreducible pues si $p = qr$ con $0 < \deg q < \deg p$ y $0 < \deg r < \deg p$, a partir de $0 = p(\alpha) = q(\alpha)r(\alpha)$ obtenemos que q o r están en $\mathcal{A}$ lo que contradice el hecho que p genera $\mathcal{A}$. El polinomio p se denomina el *polinomio minimal* de α. Si p es de grado n decimos que el número algebraico α es de grado n.

Ejemplo 1.2.

1. Todo número racional q es un número algebraico de grado 1 y su polinomio minimal es $x - q$.
2. El número $\sqrt{2}$ es algebraico de grado 2 y su polinomio minimal es $x^2 - 2$.
3. El número $\sqrt{-5}$ es algebraico de grado 2 y su polinomio minimal es $x^2 + 5$.
4. Si α es una raíz n-ésima primitiva de la unidad entonces α es un número algebraico de grado n, cuyo polinomio minimal es $x^n - 1$.

Dado α un número algebraico, sea $\mathbb{Q}(\alpha)$ el menor subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{Q}$ y a α. Es fácil ver que $\mathbb{Q}(\alpha)$ consiste de todos los elementos de la forma $f(\alpha)/g(\alpha)$, con f, g polinomios con coeficientes en $\mathbb{Q}$ y $g(\alpha) \neq 0$.

Proposición 1.3. *Dado α un número algebraico consideramos el siguiente subanillo de $\mathbb{C}$:*

$$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_m\alpha^m : \, a_i \in \mathbb{Q}\}\,.$$

Entonces $\mathbb{Q}[\alpha]$ es un cuerpo. Mas aún $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

Demostración. La aplicación $\mathbb{Q}[x] \longrightarrow \mathbb{Q}[\alpha]$ dada por $\sum_{i=0}^m a_i x^i \mapsto \sum_{i=0}^m a_i \alpha^i$ es un homomorfismo de anillos, cuyo núcleo está generado por f, el polinomio minimal de α. Entonces $Q[\alpha]$ es isomorfo a $\mathbb{Q}[x]/(f)$.

Sea $g \in \mathbb{Q}[x]$ tal que $g(\alpha) \neq 0$, o lo que es lo mismo tal que f no divide a g. El ideal generado por f y g en $\mathbb{Q}[x]$ es un ideal principal (h). Luego $f = ch$, para algún $c \in \mathbb{Q}[x]$, como f es irreducible entonces $c \in \mathbb{Q}^*$ o $h \in \mathbb{Q}^*$. El primer caso es imposible porque h divide a g y f no. Entonces $h \in \mathbb{Q}^*$ o sea $(h) = \mathbb{Q}[x]$ y por lo tanto existen $k, \ell \in \mathbb{Q}[x]$ tales que $kf + \ell g = 1$. Luego g es inversible módulo f lo que prueba que $\mathbb{Q}[x]/(f) = \mathbb{Q}[\alpha]$ es un cuerpo.

□

Definición 1.4. Un subcuerpo $K \subset \mathbb{C}$ se dice un *cuerpo de números algebraico* si su dimensión, como $\mathbb{Q}$ espacio vectorial, es finita. La dimensión de K sobre $\mathbb{Q}$ se llama el *grado* del cuerpo K y se denota $[K : \mathbb{Q}]$.

Ejemplo 1.5. $\mathbb{Q}$ y $\mathbb{Q}(\sqrt{2})$ son cuerpos algebraicos de números de grado 1 y 2 respectivamente.

Es fácil ver que si α es algebraico de grado n entonces $\mathbb{Q}(\alpha)$ es un cuerpo algebraico de grado n. Además todo elemento de un cuerpo de números algebraico es un número algebraico, pues si $[K : \mathbb{Q}] = n$ entonces $1, \alpha, \alpha^2, \ldots \alpha^n$ son necesariamente linealmente dependientes sobre $\mathbb{Q}$.

Todo polinomio mónico irreducible en $\mathbb{Q}[x]$ es el polinomio minimal de sus raíces.

Proposición 1.6. *Sea K un cuerpo de números algebraico de grado n. Entonces existe un número algebraico $\theta \in K$ tal que $K = \mathbb{Q}[\theta]$.*

Demostración. Ver por ejemplo [3], pag. 33. □

Lema 1.7. *Sean α y β dos números algebraicos con el mismo polinomio minimal. Entonces la aplicación $\phi : \mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}[\beta]$ definida por $\phi(\sum a_i\alpha^i) = \sum a_i\beta^i$ es un isomorfismo de cuerpos, que es la identidad en $\mathbb{Q}$ y $\phi(\alpha) = \beta$.*

Recíprocamente si ϕ es cualquier morfismo inyectivo de $\mathbb{Q}[\alpha]$ en $\mathbb{C}$ tal que ϕ es la identidad en $\mathbb{Q}$ entonces $\phi(\alpha)$ es raíz del polinomio minimal de α.

Definición 1.8. Dos números algebraicos α y β se dicen *conjugados* si tienen el mismo polinomio minimal.

Proposición 1.9. *Sea K un cuerpo algebraico de grado n. Entonces, existen exactamente n morfismos inyectivos σ_1, $\sigma_2, \ldots, \sigma_n$ de K en $\mathbb{C}$ que son la identidad en $\mathbb{Q}$.*

Demostración. Si $K = \mathbb{Q}[\alpha]$ y $\alpha_1(= \alpha), \alpha_2, \ldots, \alpha_n$ son las raíces (distintas) del polinomio minimal de α, entonces, por Lema 1.7, para cada $j = 1, \ldots, n$ existe un isomorfismo σ_j de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}(\alpha_j)$ definido por $\sigma_j(\sum a_i\alpha^i) = \sum a_i\alpha_j^i$. Por definición $\sigma_j(a) = a$ para todo $a \in \mathbb{Q}$ y σ_1 es la identidad de K. Como $\alpha_i \neq \alpha_j$ para $i \neq j$ los isomorfismos $\sigma_1, \sigma_2, \ldots, \sigma_n$ son todos distintos. Por otra parte si σ es un morfismo inyectivo de $K = \mathbb{Q}(\alpha)$ en $\mathbb{C}$ que es la identidad en $\mathbb{Q}$ entonces, por Lema 1.7, $\sigma(\alpha_1) = \alpha_j$ para algún j. Por lo tanto tenemos que $\sigma = \sigma_j$. □

Sea K un cuerpo de números algebraico de grado n y sean $\sigma_1, \sigma_2, \ldots, \sigma_n$ los n isomorfismos distintos de K en $\mathbb{C}$. Denotaremos $K^{(i)}$ a la imagen $\sigma_i(K)$. De manera similar si $\alpha \in K$ denotamos $\alpha^{(i)} = \sigma_i(\alpha)$.

Como cada σ_i es un isomorfismo que es la identidad en $\mathbb{Q}$ resulta que $K^{(1)}, K^{(2)}, \ldots, K^{(n)}$ son cuerpos de números algebraicos de grado n. Mas aún si $K = \mathbb{Q}(\alpha)$ y $\alpha_1(= \alpha), \alpha_2, \ldots, \alpha_n$ son las raíces del polinomio minimal de α, entonces $K^{(i)} = \mathbb{Q}(\alpha_i)$.
Los cuerpos $K^{(i)}$ son llamados los *conjugados* de K. Si $K^{(i)} \subset \mathbb{R}$ decimos que es un *conjugado real* de K y si $K^{(i)} \not\subset \mathbb{R}$ decimos que es un *conjugado complejo*. Como los coeficientes del polinomio minimal de α son racionales, si una raíz α_i no es real entonces el conjugado complejo $\bar{\alpha}_i$ también es raíz del polinomio minimal.
Si r_1 es el número de conjugados reales de K y s es el número de conjugados complejos de K entonces $s = 2r_2$ para algún $r_2 \in \mathbb{N}$. Por lo tanto tenemos que $n = r_1 + 2r_2$.

1.2. Norma y traza. Sea K un cuerpo de números algebraico de grado n. Para $\alpha \in K$, la aplicación multiplicar por α: $x \mapsto \alpha x$, es $\mathbb{Q}$-lineal en K. Definimos la *traza* $\mathrm{Tr}(\alpha) = \mathrm{Tr}_K(\alpha)$ y la *norma* $N(\alpha) = N_K(\alpha)$ del elemento α como la traza y el determinante de esta aplicación lineal. Calculando la matriz A de esta transformación lineal en la base $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ vemos que

$$\begin{aligned} \mathrm{Tr}_K(\alpha) &= \alpha^{(1)} + \cdots + \alpha^{(n)}, \\ N_K(\alpha) &= \alpha^{(1)} \ldots \alpha^{(n)}. \end{aligned} \tag{1.1}$$

Además es fácil probar que si $\alpha, \beta \in K$ entonces

$$\mathrm{Tr}_K(\alpha + \beta) = \mathrm{Tr}_K(\alpha) + \mathrm{Tr}_K(\beta), \qquad N_K(\alpha\beta) = N_K(\alpha)N\,\mathrm{Tr}_K(\beta) \tag{1.2}$$

1.3. Enteros algebraicos.

Definición 1.10. Un número complejo α es dice un *entero algebraico* si α es raz de un polinomio mónico con coeficientes enteros.

Notemos las siguientes propiedades básicas de los enteros algebraicos:

1. Todo entero algebraico es un número algebraico.
2. Todo número entero (perteneciente a $\mathbb{Z}$) es un entero algebraico.
3. Si $\alpha \in \mathbb{Q}$ es un entero algebraico entonces $\alpha \in \mathbb{Z}$.

4. Dado un número algebraico α existe un $m \in \mathbb{Z}$, $m \neq 0$, tal que $m\alpha$ es un entero algebraico.

Definición 1.11. Un polinomio $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ se dice *primitivo* si el mximo común divisor de los coeficientes $a_0, a_1, \ldots, a_n$ es 1.

En particular todo polinomio mónico en $\mathbb{Z}[x]$ es primitivo. Cualquier polinomio $f \in \mathbb{Z}[x]$ se puede escribir en la forma $f = cg$ con $c \in \mathbb{Z}$ y g primitivo. Además todo polinomio $f \in \mathbb{Q}[x]$ es de la forma $f = \frac{a}{b}g$, con g un polinomio primitivo y a, b enteros coprimos.

Lema 1.12. (Gauss) *El producto de dos polinomios primitivos en $\mathbb{Z}[x]$ es primitivo.*

Proposición 1.13. *Las siguientes afirmaciones son equivalentes:*

i) *α es un entero algebraico.*
ii) *El polinomio minimal de α es un polinomio (nónico) en $\mathbb{Z}[x]$.*
iii) *$\mathbb{Z}[\alpha]$ es un $\mathbb{Z}$-módulo finitamente generado.*
iv) *Existe un $\mathbb{Z}$-módulo finitamente generado $M \neq \{0\}$ de $\mathbb{C}$ tal que $\alpha M \subset M$.*

Demostración. i) $\Rightarrow$ ii). Sea $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, con $a_i \in \mathbb{Z}$ y $\phi = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Sea f el polinomio minimal de α en $\mathbb{Q}[x]$. Por definición $\phi = f\psi$, con $\psi \in \mathbb{Q}[x]$. Podemos escribir $f = (a/b)f_1$ y $\psi = (c/d)\psi_1$ con f_1 y ψ_1 polinomios primitivos y $a, b, c, d \in \mathbb{Z}$ tales que $(a, b) = 1$, $(c, d) = 1$. Entonces $bd\phi = acf_1\psi_1$. El polinomios ϕ es primitivo por ser mónico y $f_1\psi_1$ es primitivo, por el lema de Gauss. Entonces comparando el máximo común divisor de los coeficientes en ambos miembros obtenemos que $ac = \pm bd$. Luego $\phi = \pm f_1\psi_1$. Comparando ahora los coeficientes directores vemos que el coeficiente director de f_1 es ± 1. Como $f_1(\alpha) = 0$ y f es el polinomio minimal de α, se sigue que $f = \pm f_1$. Por lo tanto $f \in \mathbb{Z}[x]$.

ii) $\Rightarrow$ iii). Sea $\phi = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ un polinomio tal que $\phi(\alpha) = 0$. Es claro que $\mathbb{Z}[\alpha]$ está generado, sobre $\mathbb{Z}$ por $1, \alpha, \ldots, \alpha^{n-1}$.

iii) $\Rightarrow$ iv). Es obvio que $\alpha\mathbb{Z}[\alpha] \subset \mathbb{Z}[\alpha]$, por lo tanto tomamos $M = \mathbb{Z}[\alpha]$.

iv) $\Rightarrow$ i). Sea $M = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n \subset \mathbb{C}$ un $\mathbb{Z}$-módulo finitamente generado tal que $\alpha M \subset M$. Entonces $\alpha v_i = \sum_{j=1}^n a_{ij}v_j$ $(i = 1, \ldots n)$, con $a_{ij} \in \mathbb{Z}$. Sean $A = (a_{ij})$, $B = \alpha I_n - A = (b_{ij})$, en particular $\sum_{j=1}^n a_{ij}v_j = 0$. Sea V un espacio vectorial de dimensión n sobre $\mathbb{C}$ y sea $\{e_1, \ldots, e_n\}$ una base de V. La aplicación lineal de $\phi : V \longrightarrow V$, $e_j \mapsto \sum_{j=1}^n b_{ij}e_i$ $(j = 1, \ldots n)$ manda el elemento no nulo $\sum_{j=1}^n v_j e_j$ a 0. Entonces $0 = \det\phi = \det B = \det(\alpha I_n - A)$. Expandiendo el determinante vemos que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ con $a_0, a_1, \ldots a_n \in \mathbb{Z}$, es decir α es un entero algebraico. □

Definición 1.14. Dado K un cuerpo de números algebraico definimos

$$\mathfrak{O} = \mathfrak{O}_K = \{\text{enteros algebraicos en } K\}.$$

Proposición 1.15. *Sea K un cuerpo de números entonces $\mathfrak{O}_K$ es un anillo y K es el cuerpo cociente de $\mathfrak{O}_K$.*

Demostración. Si $\alpha, \beta \in \mathfrak{O}$ entonces $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ son $\mathbb{Z}$-módulos finitamente generados. Entonces el anillo $M = \mathbb{Z}[\alpha, \beta]$ también es un $\mathbb{Z}$-módulo finitamente generado. Si γ es $\alpha + \beta$, $\alpha - \beta$ o $\alpha\beta$ entonces $\gamma M \subset M$. Luego, por Proposición 1.13 tenemos que $\alpha + \beta$, $\alpha - \beta$ y $\alpha\beta$ son enteros algebraicos. Por lo tanto $\mathfrak{O}$ es un anillo.
La última afirmación sigue del hecho que si α es algebraico existe un entero $m \in \mathbb{Z}$ tal que $m\alpha$ es entero algebraico. □

Teorema 1.16. *Sean K un cuerpo de números de grado n y $\mathfrak{O}$ el anillo de enteros algebraicos en K. Entonces existe una $\mathbb{Q}$-base $\{w_1, w_2, \ldots, w_n\}$ de K tal que $w_i \in \mathfrak{O}$ y*

$$\mathfrak{O} = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n.$$

Definición 1.17. Una base $\{w_1, w_2, \ldots, w_n\}$ de K como en el Teorema 1.16 se llama una *base entera* de K.

1.4. Unidades y primos.

Definición 1.18. Sea K un cuerpo cuadrático.

1. Decimos que $\epsilon \in \mathfrak{O}$ es una *unidad* si ϵ es inversible en $\mathfrak{O}$, es decir si $\epsilon^{-1} \in \mathfrak{O}$.
2. Dos enteros $\alpha, \beta \in \mathfrak{O}$ se dicen *asociados* si existe una unidad $\epsilon \in \mathfrak{O}$ tal que $\alpha = \epsilon\beta$.
3. Un entero $\gamma \in \mathfrak{O}$, $\gamma \neq 0$, se dice *primo* si no es una unidad y cualquier factorización de la forma $\gamma = \alpha\beta$ en $\mathfrak{O}$ implica que α o β son unidades.
4. Dados $\alpha, \beta \in \mathfrak{O}$, $\beta \neq 0$, decimos que α es *divisible* por β (o que β divide a α) si existe un entero $\gamma \in \mathfrak{O}$ tal que $\alpha = \beta\gamma$.

Notemos que si ϵ es una unidad entonces $N(\epsilon) = \pm 1$, en efecto ϵ y ϵ^{-1} son enteros algebraicos por lo que $N(\epsilon), N(\epsilon^{-1}) \in \mathbb{Z}$, además $1 = N(\epsilon\epsilon^{-1}) = N(\epsilon)N(\epsilon^{-1})$. Recíprocamente si $\epsilon \in \mathfrak{O}$ es un entero cuya norma es ± 1 entonces ϵ es una unidad, pues $\pm 1 = \epsilon\epsilon'$ implica que $\epsilon^{-1} = \pm\epsilon' \in \mathfrak{O}$. Por lo tanto tenemos

Lema 1.19. *Un entero ϵ en K es una unidad si y sólo si $N_K(\epsilon) = \pm 1$.*

Una raíz de la unidad es un número complejo α tal que $\alpha^n = 1$, para algún $m \in \mathbb{Z}$, $m \neq 0$. Toda raíz de la unidad en K es una unidad, pero no recíprocamente. Por ejemplo en $K = \mathbb{Q}(\sqrt{2})$, $1 + \sqrt{2}$ es una unidad y no es una raíz de la unidad.

El conjunto de las unidades del anillo de enteros $\mathfrak{O}$ es un grupo abeliano, pues si α y β son unidades entonces también lo son $\alpha\beta$ y α^{-1}. La estructura de este grupo será descripta en la Subseccin 1.5.

Proposición 1.20. *Si $\alpha \in \mathfrak{O}$ satisface que $N(\alpha)$ es un primo en $\mathbb{Z}$ entonces α es un elemento primo en $\mathfrak{O}$.*

Demostración. Supongamos que $\alpha = \beta\gamma$ y $N(\alpha) = p$ primo en $\mathbb{Z}$. Entonces tomando norma tenemos que

$$p = N(\alpha) = N(\beta)N(\gamma).$$

Entonces $N(\beta) = \pm 1$ o $N(\gamma) = \pm 1$, de donde obtenemos que β o γ es una unidad y por lo tanto α es un primo en $\mathfrak{O}$. □

Por ejemplo, en $\mathbb{Z}[i]$ el número $2 + i$ es primo pues $N(2 + i) = 5$.

Observación 1.21. La recíproca de la Proposición 1.20 no es cierta: En $\mathbb{Z}[i]$ el número 3 es primo y tiene norma $N(3) = 9$: En efecto si $3 = (a + ib)(c + id)$ entonces tomando norma a ambos miembros tenemos que

$$9 = (a^2 + b^2)(c^2 + d^2),$$

entonces tenemos que, o bien $a^2 + b^2 = 3$ y $c^2 + d^2 = 3$ lo que es imposible porque 3 no es suma de dos cuadrados, o bien que $a^2 + b^2 = 1$ o $c^2 + d^2 = 1$, lo que nos dice que $a + ib$ o $c + id$ son unidades y por lo tanto 3 es primo.

Proposición 1.22. *Todo entero en $\mathfrak{O}_K$, distinto de cero y de las unidades, es divisible por un primo.*

Demostración. Si γ es un entero que no es primo entonces $\gamma = \alpha_1\beta_1$ con $|N(\alpha_1)|, |N(\beta)| > 1$. Adems, como $N(\gamma) = N(\alpha_1)N(\beta_1)$, tenemos que $1 < |N(\alpha_1)| < |N(\gamma)|$. Si α_1 no es primo, podemos escribir $\alpha_1 = \alpha_2\beta_2$ con $1 < |N(\alpha_2)| < |N(\alpha_2)|$. Siguiendo con este proceso, obtenemos una sucesión decreciente de números naturales, $|N(\gamma)|, |N(\alpha_1)|, |N(\alpha_2)|, \ldots$, por lo tanto en

algún momento $|N(\alpha_r)|$ deberá ser un número primo y por la Proposición 1.20 obtenemos que α_r es un primo en $\mathfrak{O}$. Además

$$\gamma = \beta_1\alpha_1 = \beta_1\beta_2\alpha_2 = \cdots \beta_1\beta_2 \ldots \beta_r\alpha_r,$$

lo cual implica que α_r divide a γ. □

Teorema 1.23. *Todo entero en $\mathfrak{O}_K$, distinto de cero y de un unidad, puede ser factorizado como producto de primos en $\mathfrak{O}_K$.*

Observación 1.24. Notar que no hacemos ninguna afirmación respecto a la unicidad de tal descomposión.

Demostración. Si γ no es cero ni es una unidad, entonces es divisible por un primo α_1. Entonces

$$\gamma = \alpha_1\gamma_1, \quad \text{con} \quad |N(\gamma_1)| < |N(\gamma)|.$$

Luego, o γ_1 es una unidad o

$$\gamma_1 = \alpha_2\gamma_2, \quad \text{con} \quad |N(\gamma_2)| < |N(\gamma_1)|.$$

Siguiendo con este proceso obtenemos que $|N(\gamma)|, |N(\gamma_1)|, |N(\gamma_2)|, \ldots$ es una sucesión decreciente de números naturales. Entonces $N(\gamma_r) = 1$ para algún r y γ_r es una unidad. Por lo tanto tenemos que

$$\gamma = \alpha_1\alpha_2 \ldots \alpha_r\gamma_r = \alpha_1\alpha_2 \ldots \alpha_r'$$

donde $\alpha_r' = \alpha_r\gamma_r$ también es un primo. Esto completa la demostración del teorema. □

1.5. El grupo de unidades. Es claro que el conjunto de unidades del cuerpo K forman un grupo abeliano (con la multiplicación) y el conjunto de las raíces de la unidad en K forman un subgrupo.

Lema 1.25. *Las raíces de la unidad en un cuerpo K forman un grupo cíclico finito.*

Denotamos el orden de este grupo por w.

Teorema 1.26. (Dirichlet) *Sea K un cuerpo de números. Sea r_1 el número de conjugados reales de K y $2r_2$ el número de conjugados complejos. Sea $r = r_1 + r_2 - 1$. Entonces existen ζ una raíz de la unidad en K y $\epsilon_1, \ldots \epsilon_r$ unidades en K tales que toda unidad en K se puede escribir de manera única en la forma*

$$\varepsilon = \zeta^k \epsilon_1^{k_1} \ldots \epsilon_r^{k_r},$$

donde $k_1, \ldots, k_r \in \mathbb{Z}$ y $k \in \{0, 1, \ldots, w\}$.

El grupo de unidades es un grupo abeliano finitamente generado que tiene una parte de torsión, que es exactamente el grupo de raíces de la unidad que están en K y una parte libre con exactamente $r = r_1 + r_2 - 1$ generadores.

2. Cuerpos cuadráticos

2.1. Generalidades.

Definición 2.1. Un *cuerpo cuadrático* es un cuerpo de números algebraico de grado 2.

Notemos que si K es un cuerpo cuadrático podemos suponer que es de la forma $K = \mathbb{Q}(\sqrt{m})$ con m un entero libre de cuadrados. En efecto como $[K : \mathbb{Q}] = 2$ entonces para todo $0 \neq \alpha \in K$ tenemos que $1, \alpha, \alpha^2$ son linealmente dependientes sobre $\mathbb{Q}$. Es decir todo número $\alpha \in K$ es raíz de un polinomio en $\mathbb{Q}[x]$ de grado a lo mas 2. Pero K debe contener algún elemento β cuyo polinomio minimal sea de grado 2, pues sino tendríamos que $K = \mathbb{Q}$. Entonces $\{1, \beta\}$ es una $\mathbb{Q}$-base de K, es decir $K = \mathbb{Q}(\beta)$. Podemos suponer que $a_2\beta^2 + a_1\beta + a_0 = 0$ con $a_0, a_1, a_2 \in \mathbb{Z}$ y $a_2 \neq 0$. Completando cuadrados obtenemos que $\gamma = 2a_2\beta + a_1$ satisface $\gamma^2 = m$, con $m = a_1^2 - 4a_0a_2$. Por lo tanto $K = \mathbb{Q}(\gamma)$. Además podemos suponer que m es libre de cuadrados.

Definición 2.2. Un cuerpo cuadrático se dice *real* si $K \subset \mathbb{R}$ y *complejo* en caso contrario.

Un cuerpo cuadrático K es real si y sólo si $K = \mathbb{Q}(\sqrt{m})$ con m un número natural mayor que 1, libre de cuadrados. Notemos también que si un cuerpo K es cuadrático imaginario entonces $K \cap \mathbb{R} = \mathbb{Q}$.

Todo elemento α en el cuerpo K es de la forma $\alpha = p + q\sqrt{m}$ con $p, q \in \mathbb{Q}$. Definimos $\alpha' = p - q\sqrt{m}$. Como α es raíz del polinomio

$$(x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha\alpha' = x^2 - 2px + p^2 - q^2 \in \mathbb{Q}[x], \tag{2.1}$$

tenemos que α' es el conjugado de α.

Consideremos en K la aplicación dada por multiplicar por el elemento $\alpha \in K$, es decir $x \mapsto \alpha x$. Esta aplicación es $\mathbb{Q}$-lineal y su matriz en la base $\{1, \sqrt{m}\}$ es $A = \begin{pmatrix} p & qm \\ q & p \end{pmatrix}$. Notemos que el polinomio caracterísitico de A es justamente $(x-\alpha)(x-\alpha')$. Por lo tanto para $\alpha = p+q\sqrt{m}$ tenemos que

$$\begin{aligned} \mathrm{Tr}_K(\alpha) &= \mathrm{Tr}(A) = 2p = \alpha + \alpha' \in \mathbb{Q} \\ N_K(\alpha) &= \det(A) = p^2 - mq^2 = \alpha\alpha' \in \mathbb{Q} \end{aligned}$$

Tenemos la siguiente caracterización de los enteros algebraicos en el cuerpo K.

Proposición 2.3. *Sea $\alpha \in K$. Entonces α es un entero algebraico si y sólo si $\mathrm{Tr}_K(\alpha)$ y $N_K(\alpha) \in \mathbb{Z}$.*

Demostración. Sea $\alpha = p + q\sqrt{m} \in \mathfrak{O}$. Si el polinomio minimal de α es de grado uno entonces es de la forma $x - a$ con $a \in \mathbb{Z}$, por lo tanto $p = a$ y $q = 0$. Luego $\mathrm{Tr}_K(\alpha) = 2a \in \mathbb{Z}$ y $N_K(\alpha) = \alpha\alpha' = a^2 \in \mathbb{Z}$. Si el polinomio minimal de α es de grado 2, digamos $x^2 + cx + d$ con $c, d \in \mathbb{Z}$. Como α y α' son raíces del polinomio minimal entonces $-c = 2p = \alpha + \alpha' = \mathrm{Tr}_K(\alpha)$ y $d = p^2 - mq^2 = \alpha\alpha' = N_K(\alpha)$.
Recícrocamente si un elemento $\alpha = p + q\sqrt{m}$ en K satisface que $\alpha + \alpha' \in \mathbb{Z}$ y $\alpha\alpha' \in \mathbb{Z}$ entonces por (2.1) el polinomio minimal de α es mónico y de coeficientes enteros, luego α es un entero algebraico. □

Usaremos el resultado anterior para construir explícitamente una base entera de $\mathbb{Q}(\sqrt{m})$

Teorema 2.4. *Los enteros algebraicos de $\mathbb{Q}(\sqrt{m})$ son de la forma*

$$\begin{aligned} a + b\sqrt{m} \qquad & \text{si } m \equiv 2, 3 \pmod 4 \\ a + b\tfrac{(1+\sqrt{m})}{2} \qquad & \text{si } m \equiv 1 \pmod 4 \end{aligned}$$

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

Observación 2.5. Notemos que como m es libre de cuadrados, el caso $m \equiv 0 \pmod 4$ no es posible.

Demostración. Sea $\alpha = p + q\sqrt{m}$ un entero algebraico en K, $p, q \in \mathbb{Q}$. Entonces $a = 2p$, $b = p^2 - q^2 m$ pertenecen a $\mathbb{Z}$ lo que implica que $\frac{a^2-4q^2m}{4} \in \mathbb{Z}$. En particular $4q^2m \in \mathbb{Z}$. Como m es libre de cuadrado se sigue que $q = f/2$ para algún $f \in \mathbb{Z}$ y que $a^2 - f^2 m \equiv 0 (\mathrm{mod}\ 4)$.

Si $m \equiv 1 \,(\mathrm{mod}\ 4)$ entonces $a^2 \equiv f^2 \,(\mathrm{mod}\ 4)$, en particular a y f tienen la misma paridad (o sea que $(a - f)/2 \in \mathbb{Z}$). Luego α es de la forma

$$\alpha = p + q\sqrt{m} = \tfrac{a}{2} + \tfrac{f}{2}\sqrt{m} = \tfrac{a-f}{2} + f\tfrac{(1+\sqrt{m})}{2}.$$

Notemos que si $m \equiv 1 \,(\mathrm{mod}\ 4)$ entonces $\frac{1+\sqrt{m}}{2} \in \mathfrak{O}$.

Si $m \equiv 2, 3 \,(\mathrm{mod}\ 4)$ entonces $a^2 - f^2 m \equiv 0 (\mathrm{mod}\ 4)$ si y sólo si a y f son ambos pares. Entonces p, $q \in \mathbb{Z}$. Esto completa la demostración del teorema. □

Corolario 2.6. *Si $m \equiv 2, 3 \,(\mathrm{mod}\ 4)$ entonces $\{1, \sqrt{m}\}$ es una base entera de $\mathbb{Q}(\sqrt{m})$.*
Si $m \equiv 1 \,(\mathrm{mod}\ 4)$ entonces $\{1, \frac{1+\sqrt{m}}{2}\}$ es una base entera de $\mathbb{Q}(\sqrt{m})$.

Si $\{w_1, w_2\}$ es un base entera de $K = \mathbb{Q}(\sqrt{m})$ definimos el *discriminante* del cuerpo K como el cuadrado del determinante de la matriz $\begin{pmatrix} w_1 & w_2 \\ w_1' & w_2' \end{pmatrix}$. Si $\{v_1, v_2\}$ es otra base entera de K entonces $v_1 = pw_1 + qw_2$ y $v_1 = rw_1 + sw_2$ con $p, q, r, s \in \mathbb{Z}$. Si $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ tenemos que $\det P = \pm 1$. Por lo tanto la definición de discriminante de un cuerpo es independiente de la base elegida. Usando el Teorema 2.4 obtenemos que el discriminante de un cuerpo cuadrático $\mathbb{Q}(\sqrt{m})$ es

$$d = \begin{cases} m & \text{si } m \equiv 1 \,(\mathrm{mod}\ 4) \\ 4m & \text{si } m \equiv 2, 3 \,(\mathrm{mod}\ 4) \end{cases} \tag{2.2}$$

Notemos que el discriminante de un cuerpo cuadrático siempre es congruente a 0 o a 1 módulo 4.
Además podemos que hemos probado lo siguiente:

Proposición 2.7. *Sea K un cuerpo cuadrático K con discriminante d. Entonces $K = \mathbb{Q}(\sqrt{d})$ y $\{1, \frac{d+\sqrt{d}}{2}\}$ es una base entera del anillo $\mathfrak{O}$ de enteros algebraicos en K.*

Ejemplo 2.8.

1. $K = \mathbb{Q}(i)$ es un cuerpo de discriminante $d = -4$. Su anillo de enteros es $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ y se denomina el anillo de *enteros de Gauss*.
2. Si $K = \mathbb{Q}(\sqrt{-3})$, sea $\rho = \frac{-1+i\sqrt{3}}{2}$ entonces $\rho \in \mathfrak{O}_K$ y $\{1, \rho\}$ es una base entera de K. Notemos que ρ es una raíz cúbica de la unidad y que $K = \mathbb{Q}(\rho)$. Su discriminante es $d = -3$.

2.2. Ejemplo: Los enteros de Gauss. Repasemos algunos de los conceptos vistos hasta el momento en el caso de cuerpo $\mathbb{Q}(i)$.

Su anillo de enteros es $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ pues $-1 \equiv 3 \pmod 4$. Si $\alpha = a + ib \in \mathbb{Q}(i)$ entonces el conjugado de α es $\alpha' = a - ib$ (notar que coincide con el conjugado complejo del número α). Además la norma de α es $N(\alpha) = a^2 + b^2 \geq 0$.

Las unidades de $\mathbb{Q}(i)$ son $\{1, i, -1, -i\}$, pues son las únicas soluciones de $a^2 + b^2 = \pm 1$. O sea en este caso el grupo de unidades es un grupo finito isomorfo a $\mathbb{Z}_4$. Se sigue de esto que si α es un entero de Gauss, los asociados de α son $\alpha, i\alpha, -\alpha, -i\alpha$.

Proposición 2.9. *Sean $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Entonces existen $\delta, \gamma \in \mathbb{Z}[i]$ tales que $\alpha = \beta\gamma + \delta$ y $N(\delta) < N(\beta)$.*

Demostración. Como $\beta \neq 0$ podemos escribir el número complejo

$$\frac{\alpha}{\beta} = x + iy, \qquad (x, y \in \mathbb{R}).$$

Sean $m, n \in \mathbb{Z}$ tales que $|x - m| \leq \frac{1}{2}$ y $|y - n| \leq \frac{1}{2}$. Definimos $\gamma = m + ni \in \mathbb{Z}[i]$ y $\delta = \beta(x - m + i(y - n))$. Claramente $\frac{\alpha}{\beta} = \gamma + \frac{\delta}{\beta}$, de donde vemos que $\delta \in \mathbb{Z}[i]$. Adems, como

$$N(\tfrac{\delta}{\beta}) = (x - m)^2 + (y - n)^2 \leq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}$$

obtenemos que $N(\delta) \leq \frac{1}{2}N(\beta) < N(\beta)$. □

Definición 2.10. Sean $\alpha, \beta \in \mathbb{Z}[i]$. Decimos que $\delta \in \mathbb{Z}[i]$ es el *máximo común divisor* de α y β si δ divide a α y a β y si cada vez que un elemento γ divide a α y a β entonces también divide a δ. Denotamos $\delta = (\alpha, \beta)$.

Es claro que el máximo común divisor de α y a β, si existe, es único excepto por la ambigedad entre elementos asociados. Si (α, β) es una unidad, decimos que α y β son *coprimos* y tomamos $(\alpha, \beta) = 1$.

Proposición 2.11. *Si $\alpha, \beta \in \mathbb{Z}[i]$ son no nulos entonces existe el máximo común divisor $(\alpha, \beta) \in \mathbb{Z}[i]$. Mas aún existen $\gamma, \delta \in \mathbb{Z}[i]$ tales que $(\alpha, \beta) = \alpha\gamma + \beta\delta$.*

Demostración. Sea $I = \{\alpha\gamma + \beta\delta : \gamma, \delta \in \mathbb{Z}[i]\}$. Es fácil ver que I es un ideal en el anillo $\mathbb{Z}[i]$. Sea $\lambda_0 = \alpha\gamma_0 + \beta\delta_0$ un elemento de norma mínima en I. Por Proposición 2.9 existen $\sigma, \tau \in \mathbb{Z}[i]$ tales que $\alpha = \sigma\lambda_0 + \tau$, con $N(\tau) < N(\lambda_0)$. Entonces $\tau = \alpha - \sigma\lambda_0 \in I$ y por la minimalidad de $N(\lambda_0)$ obtenemos que $\tau = 0$, es decir que λ_0 divide a β. Como $\lambda_0 = \alpha\gamma_0 + \beta\delta_0$, todo divisor común de α y β debe dividir a λ_0. Por lo tanto λ_0 es el máximo común divisor de α y β y se cumple la relación $(\alpha, \beta) = \alpha\gamma_0 + \beta\delta_0$. □

Proposición 2.12. *Sea $\alpha \in \mathbb{Z}[i]$ un número primo. Entonces si α divide al producto $\beta\gamma$ $(\alpha, \beta \in \mathbb{Z}[i])$, implica que α divide a β o a γ.*

Demostración. Si α divide a $\beta\gamma$ entonces $\beta\gamma = \alpha\sigma$ para algún $\sigma \in \mathbb{Z}[i]$. Podemos asumir que α no divide a β y probar que α debe dividir a γ. El máximo común divisor (α, β) divide a α que es primo, por lo tanto $(\alpha, \beta) = 1$. Por proposición anterior tenemos que $1 = \alpha\rho + \beta\delta$, para algún $\rho, \delta \in \mathbb{Z}[i]$. Luego

$$\gamma = \alpha\gamma\rho + \beta\gamma\delta = \alpha\gamma\rho + \alpha\sigma\delta = \alpha(\gamma\rho + \sigma\delta),$$

lo que muestra que α divide a γ. □

Teorema 2.13. (Teorema fundamental de la aritmética para enteros de Gauss)
Todo elemento no nulo en $\mathbb{Z}[i]$ se escribe como producto de primos en forma (esencialmente) única. Mas precisamente si $\alpha \in \mathbb{Z}[i]$, $\alpha \neq 0$ entonces $\alpha = \pi_1 \dots \pi_r$ para algunos primos $\pi_1, \dots, \pi_r \in \mathbb{Z}[i]$. Además si $\alpha = \pi_1 \dots \pi_r = \sigma_1 \dots \sigma_s$ son dos factorizaciones de α como producto de primos entonces $r = s$ y, despus de una permutación de índices, π_i es asociado a σ_i, para $1 \leq i \leq r$.

Demostración. La existencia de tal descomposición fue probada en general para cualquier cuerpo en el Teorema 1.23. Para probar la unicidad supongamos que $\alpha = \pi_1 \dots \pi_r = \sigma_1 \dots \sigma_s$ son dos factorizaciones de α como producto de primos. Podemos suponer $r \leq s$. Como π_1 divide al producto $\sigma_1 \dots \sigma_s$ y π_1 es primo, por Proposición 2.12, π_1 divide a algún σ_i, digamos a σ_1. Entonces $\sigma_1 = \epsilon_1\pi_1$, con $\epsilon_1 \in \mathbb{Z}[i]$. Como σ_1 es primo entonces ϵ_1 es una unidad. Ahora cancelamos π_1 en ambas factorizaciones y nos queda $\pi_2 \dots \pi_r = \epsilon_1\sigma_2 \dots \sigma_s$. Continuamos con este proceso hasta que en el lado izquierdo nos quede un 1. Si tuviramos que $r < s$ entonces obtenemos $1 = \epsilon_1 \dots \epsilon_r\sigma_{k+1} \dots \sigma_s$ y tomando normas llegamos a una contradicción. Por lo tanto concluimos que $r = s$ y que cada π_i es asociado a σ_i. □

2.3. Cuerpos en los cuales el teorema fundamental es falso. El teorema fundamental de la aritmética, es verdadero en los cuerpos $\mathbb{Q}$ y $\mathbb{Q}(i)$, lo que dice que el anillo de enteros de estos cuerpos son dominios de factorización única. Pero esto no es cierto para todo cuerpo de números. Los ejemplos mas simples son $\mathbb{Q}(\sqrt{m})$ con $m = -5$ (cuerpo complejo) y $m = 10$ (cuerpo real).

2.3.1. El cuerpo $\mathbb{Q}(\sqrt{-5})$. Como $-5 \equiv 3 \pmod 4$ el anillo de enteros de $\mathbb{Q}(\sqrt{-5})$ es $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5} : a, \in \mathbb{Z}\}$. Veamos que el entero $1 + \sqrt{-5}$ es un primo en $\mathbb{Z}[\sqrt{-5}]$: Si

$$1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5}),$$

entonces tomando norma a ambos miembros obtenemos que

$$6 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Si ninguno de los factores en la descomposición de $1 + \sqrt{-5}$ es una unidad entonces $(a^2 + 5b^2)$ debe ser 2 o 3, lo cual es un absurdo, por lo tanto $1 + \sqrt{-5}$ es primo.

Del mismo modo podemos ver que los números $2, 3, 1 - \sqrt{-5}$ también son primos. Entonces el número 6 tiene dos descomposiciones distintas en primos:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

La falsedad del teorema fundamental de la aritmética en estos cuerpos se debe a la falsedad de otros teoremas centrales in la aritmética de $\mathbb{Z}$. Por ejemplo si α y β son enteros en $\mathbb{Z}$ sin factores comunes existen enteros λ, μ tales que

$$1 = \alpha\lambda + \beta\mu.$$

Este teorema es falso en $\mathbb{Q}(\sqrt{-5})$, por ejemplo 3 y $1 + \sqrt{-5}$ son primos y si tuviramos que

$$1 = 3(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5})$$

entonces

$$3a + c - 5d = 1 \qquad 3b + c + d = 0,$$

lo que implica que $3a - 3b - 6d = 1$, lo cual es imposible.

2.3.2. El cuerpo $\mathbb{Q}(\sqrt{10})$. Como $10 \equiv 2 \pmod 4$ el anillo de enteros de $\mathbb{Q}(\sqrt{10})$ es $\mathbb{Z}[\sqrt{10}] = \{a + \sqrt{10} : a, \in \mathbb{Z}\}$. En este caso tenemos que

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

Es sencillo ver que 2,3, $(4 + \sqrt{10})$ y $(4 - \sqrt{10})$ son primos en $\mathbb{Z}[\sqrt{10}]$. Por ejemplo si $2 = (a + b\sqrt{10})(c + d\sqrt{10})$ entonces tomando norma a ambos miembros tenemos que

$$4 = (a^2 - 10b^2)(c^2 - 10d^2).$$

Si ninguno de los factores es una unidad entonces $(a^2 - 10b^2)$ debe ser ± 2. Pero esto es imposible porque ni 2 ni -2 son residuos cuadráticos módulo 10. Por lo tanto 2 es primo en $\mathbb{Z}[\sqrt{10}]$.

2.4. Cuerpos Euclídeos. La aritmética en aquellos cuerpos donde el teorema fundamental es verdadero es muy similar a la aritmética de $\mathbb{Z}$. El problema de determinar en cuales cuerpos es válido este teorema no es sencillo. A continuación daremos algunos resultados en esta dirección.

Para $\mathbb{Z}[i]$ probamos este teorema a partir de un análogo del algoritmo de Euclides. Supongamos que la siguiente afirmación es cierta en $K = \mathbb{Q}(\sqrt{m})$:

(2.3) Si $0 \neq \gamma_1, \gamma \in \mathfrak{O}_K$ existen $\kappa, \gamma_2 \in \mathfrak{O}_K$ tales que $\gamma = \kappa\gamma_1 + \gamma_2$ con $|N(\gamma_2)| < |N(\gamma_1)|$.

En este caso decimos que *existe un algoritmo de Euclides* en $\mathbb{Q}(\sqrt{m})$ o que el cuerpo es *Euclídeo*. Siguiendo el mismo procedimiento que para $\mathbb{Z}[i]$, obtenemos el siguiente resultado:

Teorema 2.14. *El teorema fundamental de la aritmética es verdadero en todo cuerpo Euclídeo.*

Observación 2.15. La recíproca no es cierta ya que $\mathbb{Q}(\sqrt{-19})$ y $\mathbb{Q}(\sqrt{-43})$ son cuerpos en los que el anillo de enteros es un dominio de factorización única pero no admiten un algoritmo de Euclides.

La condición (2.3) es equivalente a

(2.4) Dados cualquier δ en $\mathbb{Q}(\sqrt{m})$, existe κ entero tal que $|N(\delta-\kappa)|<1$.

En efecto veamos que (2.3) implica (2.4): dado $\delta \in K$ existe $c \in \mathbb{Z}$ tal que $c\delta$ es un entero en K, luego, por (2.3), existen κ y γ enteros tales que $c\delta = c\kappa+\gamma$ con $|N(\gamma)|<|N(c)|$. Entonces $|N(\gamma)| = |N(c)N(\delta-\kappa)| < |N(c)|$, lo cual implica que $|N(\delta-\kappa)|<1$.

Recíprocamente veamos que (2.4) implica (2.3): Dados $\gamma, \gamma_1 \in \mathfrak{O}$, $\gamma_1 \neq 0$, entonces existe $\kappa \in \mathfrak{O}$ tal que $|N(\frac{\gamma}{\gamma_1})-\kappa|<1$. Ahora $\gamma = k\gamma_1 + (\gamma - k\gamma_1)$ y $|N(\gamma - k\gamma_1)| < |N(\gamma_1)|$.

Tenemos la siguiente caracterización de los cuerpos cuadráticos complejos que son Eucldeos. Si $m=-\mu<0$ es fácil determinar los cuerpos en los cuales se cumple la condición (2.4).

Teorema 2.16. *Hay exactamente cinco cuerpos cuadráticos Eucldeos complejos $\mathbb{Q}(\sqrt{m})$ y son los que tienen*

$$m = -1, -2, -3, -7, -11.$$

Demostración. Vamos a separar dos casos:

i) Sea $m \not\equiv 1 \pmod 4$. La condición en (2.4) para $\delta = \frac{1}{2}+\frac{1}{2}\sqrt{m}$ es

$$(x-\tfrac{1}{2})^2 + \mu(y-\tfrac{1}{2})^2 < 1,$$

para algún $x, y \in \mathbb{Z}$ y $m=-\mu<0$. Como $(y-\frac{1}{2})^2 \geq \frac{1}{2}$ y $(x-\frac{1}{2})^2 \geq \frac{1}{2}$ entonces $\frac{1}{4}+\frac{1}{4}\mu<1$ y por lo tanto μ debe ser $\mu=1$ o 2. En ambos casos la condición (2.4) se cumple para todo $\delta = r+s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, con $\kappa = x+y\sqrt{m}$, donde x e y son los enteros mas prximos a r y s respectivamente.

ii) Si $m \equiv 1 \pmod 4$, los enteros de $\mathbb{Q}(\sqrt{m})$ son de la forma $x+y\frac{(1+\sqrt{m})}{2}$ con $x, y \in \mathbb{Z}$. Una condición necesaria para que se cumpla (2.4) para $\delta = \frac{1}{4}+\frac{1}{4}\sqrt{m}$ es que $\frac{1}{16}+\frac{1}{16}\mu<1$. Como además $\mu = -m \equiv 3 \pmod 4$ los únicos posibles valores de μ son 3,7,11.
Dado $\delta = r+s\sqrt{m}$ tomamos $x, y \in \mathbb{Z}$ tales que $|2s-y| \leq \frac{1}{2}$ y $|r-x-\frac{1}{2}y| \leq \frac{1}{2}$. Poniendo $\kappa = x+y\frac{(1+\sqrt{m})}{2}$ obtenemos

$$|N(\delta-\kappa)| = |(r-x-\tfrac{1}{2}y)^2 + u(s-\tfrac{1}{2}y)| \leq \tfrac{1}{4}+\tfrac{11}{16} = \tfrac{15}{16} < 1.$$

□

Incluimos los siguiente teoremas para completar el estudio de estos temas, pero las demostraciones escapan al alcance de estas notas.

Teorema 2.17. *Hay exactamente nueve cuerpos cuadráticos complejos $\mathbb{Q}(\sqrt{m})$ en los que vale el teorema fundamental de la aritmética. Son los que tienen*

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Los cuerpos cuadráticos reales que admite un algoritmo de Euclides son mas numerosos.

Teorema 2.18. *Si $m>0$ el cuerpo $\mathbb{Q}(\sqrt{m})$ es Euclídeo si y sólo si*

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

2.5. Suma de dos cuadrados. Como una aplicación de la aritmética de $\mathbb{Z}[i]$ daremos una caracterización de los números naturales que son suma de dos cuadrados. Este resultado fue enunciado por Fermat alrededor del año 1640 y probado por Euler en 1793.

Denotaremos $\mathbb{F}_q$ el cuerpo finito de q elementos y $\mathbb{F}_q^\times$ el grupo multiplicativo de los elementos no nulos en $\mathbb{F}_q$.

Teorema 2.19. *Sea $p \in \mathbb{N}$ un primo impar. Las siguientes condiciones son equivalentes.*

1) $p \equiv 1 \pmod 4$.
2) -1 *es un cuadrado en* $\mathbb{F}_p$*, es decir la congruencia* $x^2 \equiv -1 \pmod p$ *tiene una solución en* $\mathbb{Z}$.
3) p *es suma de 2 cuadrados.*

Demostración. 1) $\Leftrightarrow$ 2). Para cada $y \in \mathbb{F}_p^\times$ definimos el conjunto

$$P_y = \{y, -y, y^{-1}, -y^{-1}\}.$$

Es fácil ver que estos conjuntos definen una partición en $\mathbb{F}_p^\times$. Genéricamente este conjunto tiene 4 elementos pero podría tener menos elementos. Por ejemplo, podríamos tener que $y = y^{-1}$: esto sucede exactamente cuando $y = \pm 1$, en cuyo caso $P_y = \{1, -1\}$. Además podría suceder que $y = -y^{-1}$: esto ocurre exactamente cuando -1 es un cuadrado módulo p, en cuyo caso el correspondiente conjunto P_y tiene 2 elementos. La situación $y = -y$ nunca es posible porque y es inversible y p es impar. Resumiendo, hemos construido una partición de $\mathbb{F}_p^\times$ (que tiene $p-1$ elementos) en clases de 4 elementos, con a lo más 2 excepciones, que tienen 2 elementos cada una. Notemos que la clase excepcional P_1 siempre está presente.

Entonces si $p \equiv 1 \pmod 4$ debe haber dos clases con 2 elementos, es decir que -1 es un cuadrado módulo p. Si $p \equiv 3 \pmod 4$, hay una sola clase con dos elementos y por lo tanto -1 no es un cuadrado módulo p.

2) $\Rightarrow$ 3). Supongamos que -1 es un cuadrado módulo p. Entonces existe $x \in \mathbb{Z}$ tal que p divide a $x^2 + 1 = (x - i)(x + i)$ en $\mathbb{Z}[i]$. Si p fuese primo en $\mathbb{Z}[i]$ entonces debería dividir a $x + i$ o a $x - i$, pero esto no es cierto porque los números $\frac{x \pm i}{p}$ no son enteros en $\mathbb{Q}(i)$. Por lo tanto p no es primo en $\mathbb{Z}[i]$. Entonces podemos factorizar $p = \alpha\beta$ con $N(\alpha) > 1$ y $N(\beta) > 1$. Tomando normas obtenemos que $p^2 = N(p) = N(\alpha)N(\beta)$. Esto implica que $p = N(\alpha) = N(\beta)$ y luego p es suma de dos cuadrados.

3) $\Rightarrow$ 2). Si p es suma de dos cuadrados, digamos $p = a^2 + b^2$ entonces a y b son inversibles módulo p. Sea $c \in \mathbb{Z}$ tal que $bc \equiv 1 \pmod p$. Entonces $pc^2 = (ac)^2 + (bc)^2$, de donde se sigue que $0 \equiv (ac)^2 + 1 \pmod p$, o sea -1 es un cuadrado módulo p. □

Corolario 2.20. *Un entero $n \geq 2$ es suma de 2 cuadrados si y sólo si todo número primo $p \equiv 3 \pmod 4$ aparece con exponente par en la factorización en primos del número n.*

Demostración. Sea $n = a^2 + b^2$ y sea p un primo impar que divida a n. Sea p^k la máxima potencia de p que divide a a y a b, si denotamos $x = \frac{a}{p^k}$, $y = \frac{b}{p^k}$ tenemos que $\frac{n}{p^{2k}} = x^2 + y^2$. Supongamos que p divide a $x^2 + y^2$, como p no divide a x o a y. Del mismo modo que en la prueba de 3) $\Rightarrow$ 2) del Teorema 2.19, podemos deducir que -1 es un cuadrado módulo p lo que es equivalente a que $p \equiv 1 \pmod 4$. Por lo tanto tenemos que los primos $p \equiv 3 \pmod 4$ aparecen con exponente par en la factorización de n.

La prueba de la recíproca se deja como ejercicio para el lector. □

2.6. Primos en $\mathbb{Z}[i]$. Empezamos viendo un criterio para decidir cuando un entero de Gauss es coprimo con un número natural.

Lema 2.21. *Sea $m \in \mathbb{Z}$ y $\alpha \in \mathbb{Z}[i]$. Entonces $(m, \alpha) = 1$ si y sólo si $(m, N(\alpha)) = 1$.*

Demostración. Si $(m, \alpha) = 1$ entonces existen $\gamma, \delta \in \mathbb{Z}[i]$ tal que $1 = m\gamma + \alpha\delta$. Entonces

$$N(\alpha)N(\delta) = N(1 - m\gamma) = (1 - m\gamma)(1 - m\overline{\gamma}) = 1 - (\gamma + \overline{\gamma})m + N(\gamma)m^2,$$

equivalentemente $N(\alpha)N(\delta) + (\gamma + \overline{\gamma})m - N(\gamma)m^2 = 1$. Notar que $\gamma + \overline{\gamma}$ y $N(\gamma)$ pertenecen a $\mathbb{Z}$. Por lo tanto si $\beta \in \mathbb{Z}[i]$ divide a m y a $N(\alpha)$ entonces divide a 1, lo que muestra que β es una unidad.

Recíprocamente supongamos que $(m, N(\alpha)) = 1$. Si $\delta \in \mathbb{Z}[i]$ divide a m y a α, como $N(\alpha) = \alpha\overline{\alpha}$ entonces δ divide a 1 y por lo tanto es una unidad. □

Proposición 2.22. *Un entero de Gauss $\pi \in \mathbb{Z}[i]$ es primo si y sólo si se cumple una de las siguientes condiciones:*

1. $N(\pi) = 2$ *(en este caso π es asociado a $1 + i$, es decir $\pi \in \{1 \pm i, -1 \pm i\}$).*
2. $N(\pi) = p$, *donde p es un primo en $\mathbb{Z}$, $p \equiv 1 \pmod 4$.*
3. *π es asociado a q, con q un primo en $\mathbb{Z}$, $q \equiv 3 \pmod 4$.*

Demostración. Supongamos que π es un primo en $\mathbb{Z}[i]$ y sea p un primo en $\mathbb{Z}$ que divida a $N(\pi)$. Sea $\delta = (p, \pi)$. Por el Lema 2.21, δ no es una unidad y como π es primo, δ es asociado a π, por lo que podemos asumir que $\delta = \pi$. Luego $p = \pi\gamma$, para algún $\gamma \in \mathbb{Z}[i]$. Tomando normas tenemos que $p^2 = N(\pi)N(\gamma)$, o equivalentemente

$$p = \frac{N(\pi)}{p} N(\gamma).$$

Tenemos dos situaciones posibles:

a) $\frac{N(\pi)}{p} = 1$, dice que $N(\pi) = p$. Luego p es suma de dos cuadrados y por el Teorema 2.19 tenemos que $p = 2$ o $p \equiv 1 \pmod 4$.

b) $N(\gamma) = 1$, en tal caso π es asociado a p y p es un primo en $\mathbb{Z}[i]$. Por lo tanto p no es suma de dos cuadrados, es decir $p \equiv 3 \pmod 4$.

Veamos ahora la recíproca. Por Proposición 1.20 sabemos que si $N(\pi)$ es primo en $\mathbb{Z}$ entonces π es primo en $\mathbb{Z}[i]$. Por lo tanto si $N(\pi) = 2$ o $N(\pi) = p$ con $p \equiv 1 \pmod 4$ entonces π es primo en $\mathbb{Z}[i]$. Por otra parte, si q es un primo en $\mathbb{Z}$, $q \equiv 3 \pmod 4$ entonces q sigue siendo primo en $\mathbb{Z}[i]$: en efecto, si $q = \alpha\beta$ para algún $\alpha, \beta \in \mathbb{Z}[i]$ entonces, tomando normas obtenemos que $q^2 = N(\alpha)N(\beta)$. Como q no es suma de dos cuadrados no puede suceder que $q = N(\alpha) = N(\beta)$, por lo tanto α o β es una unidad en $\mathbb{Z}[i]$. □

Referencias

[1] G. Hardy, E. Wright *An introduction to the Theory of Numbers*, Oxford Science Publications. (1978).

[2] E. Hecke, *Lectures on the theory of Algebraic Numbers*, Graduate texts in mathematics, **77**. Springer Verlag. (1981).

[3] R. Narasimhan, S. Raghavan, S. Rangachari, S. Lal *Algebraic Number Theory.* Lecture Notes of Tata Institute of Fundamental Research. Bombay. (1966).

CIEM-FaMAF, Universidad Nacional de Córdoba, Córdoba 5000, Argentina

E-mail address: pacharon@mate.uncor.edu