10

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS

EL TOEREMA DE LAS UNIDADES DE DIRICHLET

T E S I S

QUE PARA OBTENER EL TITULO DE

MATEMATICO

P R E S E N T A :

Rafael Gutiérrez **Estrada.**

DIR. DE TESIS:

Armando Reyes Rodríguez.

México D. F. 1996

TESIS CON
FALLA DE ORIGEN

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

"EL TEOREMA DE LAS UNIDADES DE DIRICHLET"

Comunicamos a usted que hemos revisado el trabajo de Tesis:

realizado por RAFAEL GUTIERREZ ESTRADA.

con número de cuenta 8212940-0 , pasante de la carrera de MATEMATICAS.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	M. EN C. ARMANDO REYES RODRIGUEZ.
Propietario	DR. FELIX RECILLAS JUAREZ.
Propietario	M. EN C. MARIO PINEDA RUELAS.
Suplente	DR. RAYMUNDO BAUTISTA RAMOS.
Suplente	DR. JUAN MORALES RODRIGUEZ.

Consejo Departamental de Matemáticas
M. EN C. ALEJANDRO BRAVO MOJICA.

A MIS PADRES, ESPOSA E HIJOS

Deseo manifestar mi agradecimiento a varios revisores, quienes leyeron este trabajo y me hicieron muchas sugerencias utiles para la presentación final del mismo. Expreso también mi gratitud a todos aquellos profesores, a quienes les robe parte de su preciado tiempo al exponerles parte del material que conforma este trabajo. Por último quiero agradecer muy en especial a Armando Reyes Rodriguez, por su paciencia al haberme escuchado tantas y tantas horas y por cuidar y procurar que mi tesis tuviera el mejor fin posible.

Rafael Gutiérrez E.

Introducción.

Uno de los grandes temas de la Aritmética (o Teoría de Números) es la solución de ecuaciones polinomiales de la forma

$$p(x_1, \ldots, x_n) = 0 \tag{1}$$

donde se requiere que las soluciones sean *enteros*. En general también se requiere que los coeficientes del polinomio (1) también estén en $\mathbb{Z}$. Problemas de este tipo, englobados en el tema de problemas diofantinos, han estado en la Matemática desde sus inicios. La dificultad de este tipo de problemas es ilustrada en forma dramática por la ecuación

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

El último teorema de Fermat que afirma que la ecuacion anterior, para $n \geq 3$, no tiene soluciones no triviales. De hecho gran parte de la Teoría de Números Algebraicos fue desarrollada con los intentos, por Kummer y sus contemporaneos, por resolver este problema.

Es bien sabido que muchos matemáticos brillantísimos, creyeron haber probado parcialmente lo que afirmó Fermat, sin embargo tales pruebas fueron en su mayoria erroneas. El error que cometieron en general fue el haber supuesto que en ciertos anillos se daba la factorización única en irreducibles. Por ejemplo en 1874 el frances Lamé anunció una prueba del último teorema de Fermat. En su prueba Lamé trabajo con el anillo $\mathbf{Z}[\xi]$, donde ξ es una raíz p-ésima primitiva de la unidad, p primo impar. Su prueba estaba entre comillas bien hecha, sin embargo Liouville, estudiando tal prueba se dio cuenta que era necesario asumir factorización única en $\mathbf{Z}[\xi]$; pero no mucho tiempo después Kummer se dio cuenta que la factorización única falla en algunos casos, el primer valor de estos es $n = 23$.

Por otro lado Kummer trabajando con números llamados *números ideales*, probó el último teorema de Fermat para un gran rango de números primos p, a saber con aquellos primos p que no dividen al número de clase del campo $\mathbf{Q}(\xi)$, en donde ξ es como antes definido. Tales números primos son llamados *primos regulares*.

Kummer en su prueba hace uso de muchos resultados, la mayoria de estos propuestos y probados por él mismo. El resultado más importante (quizás) en vías de la demostración del último teorema de Fermat en el caso que p es primo regular, es el *Lema de Kummer* el cual nos dice en forma precisa cómo son *las unidades* en el anillo de enteros $\mathbf{Z}[\xi]$ del campo de números $\mathbf{Q}(\xi)$.

Aunque la prueba parcial del último teorema de Fermat hecha por Kummer no se dá en este trabajo, con lo desarrollado en el capítulo 3 del presente, fácilmente se puede probar que

$$x^p + y^p = z^p \quad (p \text{ primo regular impar})$$

no tiene soluciones $x, y, z \in \mathbb{Z}$ no triviales tales que $p \nmid x, p \nmid y, p \nmid z$.

Problemas como el último teorema de Fermat, así como también muchos otros problemas diofantinos, no serían tan complicados en su resolución si en los anillos de enteros que surgen de manera natural se diera la factorización única en irreducibles. Lamentablemente lo anterior no ocurre.

Como podemos ver el problema de la factorización única es de vital importancia en el estudio de las ecuaciones diofantinas. La factorización única involura al importantísimo concepto de *unidad*. Cuando en un anillo son conocidas sus unidades, es menos complicada (pero aún muy difícil) la averiguación de la factorización única en irreducibles.

Una forma alternativa para saber si un dominio entero $\mathbf{D}$, donde se dá la factorización en irreducibles , tiene la propiedad de la factorización única, es tratar de hacer que $\mathbf{D}$ sea un dominio Euclideano, mediante la introducción de una función Euclideana $\phi : \mathbf{D} \to \mathbf{N} \cup \{0\}$.

Lamentablemente, el camino anterior no es del todo fácil, y es a veces un camino infructuoso ya que quizás no exista tal función ϕ y $\mathbf{D}$ sea sin embargo un dominio de factorización única. Por ejemplo cuando se trabaja con los campos cuadraticos $\mathbb{Q}(\sqrt{d})$, (d un entero libre de cuadrados) para $d = -5, -6, -10$ ó $d < -11$ el correspondiente anillo de enteros no es Euclideano [ver Teorema 2.26 pag. 46 del presente]. Pero para $d = -19, -43, -67, -163$, el correspondiente anillo de enteros si es un dominio de factorización única.

Una prueba de que el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ no es un dominio Euclideano para los valores de d antes mencionados (la cual se dá en este trabajo) se basa primordialmente en el conocimiento de las *unidades* del anillo en cuestión.

Como podemos apreciar el estudio de las unidades de un dominio entero $\mathbf{D}$ es de suma importancia ya que al tratar de resolver problemas diofantinos, de alguna u otra manera hay que saber quienes o de que forma son las unidades de $\mathbf{D}$.

La razón de ser de este trabajo es justamente el estudiar las *unidades* de dominios enteros muy particulares; a saber, de las unidades del anillo

de enteros $\mathcal{O}_K$ de un campo de números **K** (Un campo de números es una extensión finita de $\mathbb{Q}$).

Aunque los anillos de enteros son un caso muy particular de un dominio entero, al trabajar con problemas diofantinos, la mayoría de éstos en algún momento se reducen a un problema de factorización en algún anillo de enteros $\mathcal{O}_K$, y así es como entran en juego las unidades y **Dirichlet** habla.

El Teorema de las unidades de Dirichlet, nos da en forma precisa la estructura que tiene el conjunto de todas las unidades del anillo de enteros $\mathcal{O}_K$ de un campo de números **K**.

INDICE

Capítulo 1

Números algebraicos

En este capítulo se verán la mayoria de los conceptos algebraicos a trabajar en el transcurso de este trabajo.

En este capítulo se estudia la estructura que tiene el conjunto de los números algebraicos, y más aún se demuestra que cualquier campo de números es una extensión simple de $\mathbf{Q}$.

Después se definen y demuestran resultados relativos a los importantísimos conceptos de conjugados, polinomio de campo y discriminantes.

Posteriormente se define lo que es un entero algebraico y se demuestra que el conjunto de enteros algebraicos $\mathbf{B}$ tiene estructura de anillo. Enseguida se define el anillo de enteros $\mathcal{O}_\mathbf{K}$ de un campo de números $\mathbf{K}$. También se define lo que es una base entera y se demuestra la existencia de dichas bases.

Después se ve lo que es la norma de un elemento de un campo de números, el cual es uno de los conceptos más fructiferos en el desarrollo de este trabajo.

Finalmente, se trabaja con dos campos de números muy particulares, a saber, con los campos cuadráticos y con los campos ciclotómicos.

1.1 Números algebraicos

Definición 1.1 *Un número complejo α se llama algebraico sobre $\mathbf{Q}$, si α es raíz de un polinomio no nulo con coeficientes en $\mathbf{Q}$.*

Teorema 1.2 *El conjunto $\mathbf{A}$ de números algebraicos es un subcampo de $\mathbb{C}$.*

Demostración: Sean $\alpha, \beta \in \mathbf{A}$. Como β es algebraico sobre $\mathbf{Q}$, entonces también β es algebraico sobre $\mathbf{Q}(\alpha)$ pues $\mathbf{Q} \subseteq \mathbf{Q}(\alpha)$. Además $[\mathbf{Q}(\alpha) : \mathbf{Q}]$

es finita pues α es algebraico sobre $\mathbb{Q}$, [ver teorema A.18 del apéndice]. Análogamente $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)]$ es finita pues β es algebraico sobre $\mathbb{Q}(\alpha)$. Ahora como $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, entonces $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}]$ es finita y por lo tanto algebraica [ver corolario A.20 del apéndice].

Finalmente como $\mathbb{Q}(\alpha,\beta)$ es un campo

$$\alpha+\beta\ ,\ \alpha-\beta\ ,\ \alpha\,\beta\ ,\ \frac{\alpha}{\beta}\quad (\beta\neq 0)\in\mathbb{Q}(\alpha,\beta)\subseteq \mathbf{A}.$$

□

Notemos que $[\mathbf{A} : \mathbb{Q}]$ es infinita. En efecto, supongamos que $[\mathbf{A} : \mathbb{Q}] = n$, $n < \infty$. Sea p un primo tal que $p-1 > n$, entonces $f(x) = x^{p-1}+x^{p-2}+\cdots+x+1 \in \mathbb{Z}[\mathbf{x}]$ es irreducible en $\mathbb{Q}[\mathbf{x}]$ [ver ejemplos vistos enseguida del teorema A.12 del apéndice]. Ahora si $\omega \in \mathbb{C}$ es tal que $f(\omega) = 0$, entonces $\omega \in \mathbf{A}$. Finalmente $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 > n = [\mathbf{A} : \mathbb{Q}]$ [ver teorema A.18 del apéndice] lo cual es absurdo ya que $\mathbb{Q}(\omega) \subseteq \mathbf{A}$.

Definición 1.3 *Un campo de números es un subcampo* $\mathbf{K}$ *de* $\mathbb{C}$ *tal que* $[\mathbf{K} : \mathbb{Q}]$ *es finito. Se sigue de la definición que todo elemento de* $\mathbf{K}$ *es algebraico sobre* $\mathbb{Q}$*, entonces* $\mathbf{K} \subset \mathbf{A}$.

Teorema 1.4 *Si* $\mathbf{K}$ *es un campo de números, entonces* $\mathbf{K} = \mathbb{Q}(\theta)$ *para algún* θ *algebraico.*

Demostración: Como $\mathbf{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_1, \ldots, \alpha_n$ son algebraicos [ver teorema A.21 del apéndice], por inducción bastará probar que si $\mathbf{K} = \mathbf{K_1}(\lambda, \delta)$, entonces $\mathbf{K} = \mathbf{K_1}(\theta)$ (α, δ y θ algebraicos y $\mathbf{K_1}$ un subcampo de $\mathbf{K}$), pues si esto sucede entonces

$$\begin{aligned}
\mathbb{Q}(\alpha_1) &= \mathbb{Q}(\theta_1)\\
\mathbb{Q}(\alpha_1,\alpha_2) &= \mathbb{Q}(\theta_2)\\
\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) &= \mathbb{Q}(\theta_2,\alpha_3) = \mathbb{Q}(\theta_3)\\
\vdots &= \quad\vdots\\
\mathbf{K} = \mathbb{Q}(\alpha_1,\ldots,\alpha_n) &= \mathbb{Q}(\theta_{n-1},\alpha_n) = \mathbb{Q}(\theta_n) = \mathbb{Q}(\theta)
\end{aligned}$$

en donde α_i, θ_i son algebraicos sobre $\mathbb{Q}$ para toda i $(1 \leq i \leq n)$.

Probemos entonces lo anterior.

Sean p y q los polinomios *mínimos* de λ, δ sobre $\mathbf{K_1}$. Como $\mathbb{C}$ es un campo algebraicamente cerrado, estos dos polinomios se pueden factorizar como:

$$\begin{aligned}
p(x) &= (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_m)\\
q(x) &= (x-\delta_1)(x-\delta_2)\cdots(x-\delta_n)\ ,
\end{aligned}$$

en donde los λ_i, δ_j $(1 \leq i \leq m\ ;\ 1 \leq j \leq n)$ son distintos pues $p(x)$ y $q(x)$ son irreducibles [ver corolario A.14 del apéndice].

Consideremos $\lambda_1 = \lambda$ y $\delta_1 = \delta$. Para cada pareja (i,j) la ecuación

$$\lambda_i + y\delta_j = \lambda_1 + y\delta_1 \quad ; \quad j \neq 1\,, \tag{1.1}$$

tiene una solución única y, en donde y puede o no pertenecer a $\mathbf{K_1}$. Por lo tanto para cada i y para cada $j \neq 1$, existe a lo más un elemento $y \in \mathbf{K_1}$ que satisface la ecuación 1.1. Por lo tanto podemos elegir $c \neq 0 \in K_1$ tal que $\lambda_i + c\delta_j \neq \lambda_1 + c\delta_1$ $(1 \leq 1 \leq m\ ,\ 1 \leq j \leq n)$. Si definimos $\theta = \lambda + c\delta$, probaremos que $\mathbf{K_1}(\theta) = \mathbf{K_1}(\lambda, \delta)$.

Obviamente $\mathbf{K_1}(\theta) \subseteq \mathbf{K_1}(\lambda, \delta)$ y sólo nos resta probar que $\mathbf{K_1}(\lambda, \delta) \subseteq \mathbf{K_1}(\theta)$; pero para esto es suficiente probar que $\delta \in \mathbf{K_1}(\theta)$ pues si esto sucede, entonces $\lambda = \theta - c\delta$ también estará en $\mathbf{K_1}(\theta)$ y terminaremos la prueba.

Probemos pues entonces que $\delta \in \mathbf{K_1}(\theta)$. Para esto notemos que

$$p(\theta - c\delta) = p(\lambda) = 0\,.$$

Por lo tanto si definimos

$$r(x) = p(\theta - cx) \quad \in \mathbf{K_1}(\theta)[\mathbf{x}]\,,$$

δ es una raíz tanto de q como de r y q, r son ambos polinomios con coeficientes en $\mathbf{K_1}(\theta)$. Además q y r no tienen otro cero en común, ya que si $q(\xi) = r(\xi) = 0$, entonces ξ sería uno de los δ_j $(1 \leq j \leq n)$ y $\theta - c\xi$ sería uno de los λ_i $(1 \leq i \leq m)$; de lo cual se concluye que $\theta - c\delta_j = \lambda_i$, pero como también $\theta = \lambda_1 + c\delta_1$, entonces $\lambda_1 + c\delta_1 - c\delta_j = \lambda_i$ ó $\lambda_i + c\delta_j = \lambda_1 + c\delta_1$. Pero por la elección de c_i esta última igualdad sólo se puede dar si $i = j = 1$ y por lo tanto $\xi = \delta_1 = \delta$.

Por otro lado si $h(x)$ es el polinomio mínimo de δ sobre $\mathbf{K_1}(\theta)$, entonces $h(x)$ divide a $q(x)$ y a $r(x)$ [ver lema A.17 b) del apéndice]. Más aún $h(x)$ es un polinomio de grado 1. En efecto, ya que toda raíz de $h(x)$ también lo es de $q(x)$ y $r(x)$ pues $h(x)$ los divide. Por otro lado, todas las raíces de $h(x)$ son distintas pues $h(x)$ es irreducible; por lo tanto si η es cualquier raíz de $h(x)$, entonces η tiene que ser δ, pues $q(x)$ y $r(x)$ sólo tienen una raíz en común que es δ, de donde concluimos que el grado de $h(x)$ es 1.

Por lo tanto $\quad h(x) = x - \delta \ \in \mathbf{K_1}(\theta)$; de donde finalmente obtenemos que $\delta \in \mathbf{K_1}(\theta)$.

□

1.2 Conjugados y discriminantes

Si $\mathbf{K} = \mathbb{Q}(\theta)$ es un campo de números, existen en general varios monomorfismos distintos $\sigma : \mathbf{K} \to \mathbb{C}$.

En el siguiente teorema veremos cúal es el número exacto de estos monomorfismos y más aún, se verá cual es la regla de correspondencia de cada uno de ellos.

Teorema 1.5 *Sea $\mathbf{K} = \mathbb{Q}(\theta)$ un campo de números de grado n sobre $\mathbb{Q}$. Entonces existen exactamente n distintos monomorfismos $\sigma_i : \mathbf{K} \to \mathbb{C}$ $(i = 1, 2, \ldots, n)$, en donde los elementos $\sigma_i(\theta) = \theta_i$ son los distintos ceros en $\mathbb{C}$ del polinomio mínimo de θ sobre $\mathbb{Q}$.*

Demostración : Antes que nada recordemos que si $\sigma : \mathbf{K} \to \mathbb{C}$ es un homomòrfismo no trivial, entonces σ es un monomorfismo. Más aún tenemos que $\sigma(1) = 1$, y con ésto fácilmente se comprueba que $\sigma|_{\mathbb{Q}} = Id$ (σ restringida a $\mathbb{Q}$ es la identidad). También, como $1, \theta, \ldots, \theta^{n-1}$ es una base de $\mathbf{K}$ sobre $\mathbb{Q}$, si $\alpha \in \mathbf{K}, \alpha$ se expresa de manera única como $\alpha = r(\theta)$, en donde $r(x) \in \mathbb{Q}[\mathbf{x}]$ y $\partial(r) < n$ ($\partial(r)$ denota el grado del polinomio $r(x)$), y así :

$$\sigma(\alpha) = \sigma(r(\theta)) = r(\sigma(\theta)) \ .$$

Esto es, que si $\sigma : \mathbf{K} \to \mathbb{C}$ es un homomorfismo no trivial, basta que sepamos a quien es igual $\sigma(\theta)$ para tener completamente determinada la regla de correspondencia de σ.

Por otro lado, si el polinomio mínimo de θ es $p(x) \in \mathbb{Q}[\mathbf{x}]$, entonces

$$0 = \sigma(p(\theta)) = p(\sigma(\theta)) \quad , \tag{1.2}$$

por lo tanto $\sigma(\theta)$ es alguna de las n raíces distintas $(\theta_1, \ldots, \theta_n \in \mathbb{C})$ de $p(x)$.

Todo lo anterior parece indicarnos que los isomorfismos que buscamos son precisamente $\sigma_i : \mathbf{K} \to \mathbb{C}$ en donde $\sigma_i(\theta) = \theta_i$ $(i = 1, \ldots, n)$. Lo anterior es cierto ya que si nos fijamos en los campos $\mathbf{K} = \mathbb{Q}(\theta)$ y en $\mathbb{Q}(\theta_i)$ $(1 \leq i \leq n)$, cuyas respectivas bases sobre $\mathbb{Q}$ son $1, \theta, \ldots, \theta^{n-1}$ y $1, \theta_i, \ldots, \theta_i^{n-1}$ (puesto que $p(x)$ es el polinomio mínimo de θ y de θ_i), entonces existe un único isomorfismo de campos $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ tal que $\sigma_i(\theta) = \theta_i$. En efecto, ya que si $\alpha = r(\theta) \in \mathbb{Q}(\theta)$, entonces

$$\begin{aligned} \sigma_i(\alpha) &= r(\theta_i) \\ &= q(\theta_i) \end{aligned}$$

donde $r(x) = p(x)h(x) + q(x)$; $q(x) = 0$ ó $\partial(q) < n$.

σ_i es un homomorfismo, pues si $\alpha = r(\theta), \beta = s(\theta) \in \mathbb{Q}(\theta)$, claramente

$$\sigma_i(\alpha + \beta) = \sigma_i(\alpha) + \sigma_i(\beta) \ ,$$

además

$$\sigma_i(\alpha\beta) = r(\theta_i)s(\theta_i) = q(\theta_i)t(\theta_i) = \sigma_i(\alpha)\sigma_i(\beta)$$

$$\text{donde } s(x) = p(x)q(x) + t(x) \;\; ; \;\; t(x) = 0 \quad \text{ó} \quad \partial(t) < n \; .$$

Que σ_i es suprayectivo es inmediato. Por lo tanto σ_i es un isomorfismo. Claramente σ_i es único.

Todos los isomorfismos $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ $(1 \leq i \leq n)$ son distintos. Finalmente, por la igualdad 1.2 éstos son todos los isomorfismos posibles.

□

Definición 1.6 *Sea* $\mathbf{K} = \mathbb{Q}(\theta)$ *un campo de números de grado* n, *y* $\sigma_1, \ldots, \sigma_n$ *el conjunto de todos los distintos monomorfismos* $\mathbf{K} \to \mathbb{C}$. *Si* $\sigma_i(\mathbf{K}) \subseteq \mathbb{R}$, *lo cual ocurre si y sólo si* $\sigma_i(\theta) \in \mathbb{R}$, *se dice que* σ_i *es real, en otro caso* σ_i *es complejo.*

Recordemos que si $z \in \mathbb{C}$, el complejo conjugado de z se denota por $\overline{z}$. Si definimos $\overline{\sigma_i}(\alpha) = \overline{\sigma_i(\alpha)}$, en donde $\sigma_i : \mathbf{K} \to \mathbb{C}$, entonces $\overline{\sigma_i}$ también es un monomorfismo $\mathbf{K} \to \mathbb{C}$. En efecto, ya que $\varphi : \mathbb{C} \to \mathbb{C}$ dado por $\varphi(z) = \overline{z}$ es un monomorfismo y $\overline{\sigma_i} = \varphi \circ \sigma_i$. De lo anterior tenemos que $\overline{\sigma_i}$ es igual a σ_j para alguna j $(1 \leq j \leq n)$. Ahora como $\sigma_i = \overline{\sigma_i}$ si y sólo si σ_i es real, y $\overline{\overline{\sigma_i}} = \sigma_i$, entonces los monomorfismos complejos se dan en pares conjugados. Por lo tanto

$$n = s + 2t \; ,$$

en donde s es el número de monomorfismos reales y $2t$ el de complejos.

Definición 1.7 *Sea* $\mathbf{K}$ *un campo de números, y* $\alpha \in \mathbf{K}$. *Los elementos* $\sigma_i(\alpha)$ $(1 \leq i \leq n)$, *son llamados los* $\mathbf{K}$*-conjugados de* α.

Definición 1.8 *Con la notación anterior, si* $\alpha \in \mathbf{K} = \mathbb{Q}(\theta)$ *se define el polinomio de campo de* α *sobre* $\mathbf{K}$ *como*

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

Teorema 1.9 *Los coeficientes del polinomio de campo son números racionales, esto es,* $f_\alpha(x) \in \mathbb{Q}[\mathbf{x}]$.

Demostración : Si $\alpha \in \mathbf{K}$, entonces $\alpha = r(\theta)$, $r(x) \in \mathbb{Q}[\mathbf{x}]$ y $\partial(r) < n$. Entonces

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - \sigma_i(r(\theta))) = \prod_{i=1}^{n}(x - r(\theta_i)),$$

además

$$\sigma_i(\alpha\beta) = r(\theta_i)s(\theta_i) = q(\theta_i)t(\theta_i) = \sigma_i(\alpha)\sigma_i(\beta)$$

$$\text{donde } s(x) = p(x)g(x) + t(x) \ ; \ t(x) = 0 \quad \text{ó} \quad \partial(t) < n \ .$$

Que σ_i es suprayectivo es inmediato. Por lo tanto σ_i es un isomorfismo. Claramente σ_i es único.

Todos los isomorfismos $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ $(1 \leq i \leq n)$ son distintos. Finalmente, por la igualdad 1.2 éstos son todos los isomorfismos posibles.

□

Definición 1.6 *Sea* $\mathbf{K} = \mathbb{Q}(\theta)$ *un campo de números de grado* n, *y* $\sigma_1, \ldots, \sigma_n$ *el conjunto de todos los distintos monomorfismos* $\mathbf{K} \to \mathbb{C}$. *Si* $\sigma_i(\mathbf{K}) \subseteq \mathbb{R}$, *lo cual ocurre si y sólo si* $\sigma_i(\theta) \in \mathbb{R}$, *se dice que* σ_i *es real, en otro caso* σ_i *es complejo.*

Recordemos que si $z \in \mathbb{C}$, el complejo conjugado de z se denota por $\overline{z}$. Si definimos $\overline{\sigma_i}(\alpha) = \overline{\sigma_i(\alpha)}$, en donde $\sigma_i : \mathbf{K} \to \mathbb{C}$, entonces $\overline{\sigma_i}$ también es un monomorfismo $\mathbf{K} \to \mathbb{C}$. En efecto, ya que $\varphi : \mathbb{C} \to \mathbb{C}$ dado por $\varphi(z) = \overline{z}$ es un monomorfismo y $\overline{\sigma_i} = \varphi \circ \sigma_i$. De lo anterior tenemos que $\overline{\sigma_i}$ es igual a σ_j para alguna j $(1 \leq j \leq n)$. Ahora como $\sigma_i = \overline{\sigma_i}$ si y sólo si σ_i es real, y $\overline{\overline{\sigma_i}} = \sigma_i$, entonces los monomorfismos complejos se dan en pares conjugados. Por lo tanto

$$n = s + 2t \ ,$$

en donde s es el número de monomorfismos reales y $2t$ el de complejos.

Definición 1.7 *Sea* $\mathbf{K}$ *un campo de números, y* $\alpha \in \mathbf{K}$. *Los elementos* $\sigma_i(\alpha)$ $(1 \leq i \leq n)$, *son llamados los* $\mathbf{K}$*-conjugados de* α.

Definición 1.8 *Con la notación anterior, si* $\alpha \in \mathbf{K} = \mathbb{Q}(\theta)$ *se define el polinomio de campo de* α *sobre* $\mathbf{K}$ *como*

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

Teorema 1.9 *Los coeficientes del polinomio de campo son números racionales, esto es,* $f_\alpha(x) \in \mathbb{Q}[\mathbf{x}]$.

Demostración : Si $\alpha \in \mathbf{K}$, entonces $\alpha = r(\theta)$, $r(x) \in \mathbb{Q}[\mathbf{x}]$ y $\partial(r) < n$. Entonces

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = \prod_{i=1}^{n}(x - \sigma_i(r(\theta))) = \prod_{i=1}^{n}(x - r(\theta_i)),$$

desarrollando esto último tenemos que

$$f_\alpha(x) = x^n - h_1(\theta_1, \ldots, \theta_n)x^{n-1} + \cdots (-1)^n h_n(\theta_1, \ldots, \theta_n),$$

en donde*

$$\begin{aligned}
h_1(\theta_1, \ldots, \theta_n) &= r(\theta_1) + r(\theta_2) + \cdots + r(\theta_n) \\
h_2(\theta_1, \ldots, \theta_n) &= r(\theta_1)r(\theta_2) + r(\theta_1)r(\theta_3) + \ldots + \\
&\quad r(\theta_2)r(\theta_3) + \ldots + r(\theta_{n-1})r(\theta_n) \\
&\vdots \qquad\qquad \vdots \\
h_r(\theta_1, \ldots, \theta_n) &= \text{suma de todos los distintos productos} \\
&\quad \text{de } r \text{ distintas } h_i's \\
&\vdots \qquad\qquad \vdots \\
h_n(\theta_1, \ldots, \theta_n) &= r(\theta_1)r(\theta_2)\cdots r(\theta_n).
\end{aligned}$$

Los polinomios $h_i(x_1, \ldots, x_n) \in \mathbb{Q}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$ son simétricos $(1 \leq i \leq n)$ pues al efectuar cualquier permutación de $(x_1, \ldots, x_n)$ el polinomio h_i queda invariante.

Finalmente como $h_1, \ldots, h_n$ son simétricos y $\theta_1, \ldots, \theta_n$ son las raíces de $p(x) \in \mathbb{Q}[\mathbf{x}]$, entonces $h_i(\theta_1, \ldots, \theta_n) \in \mathbb{Q}\ \forall i = 1, 2, \ldots, n$ [ver teorema A.24 del apéndice]. Por lo tanto $f_\alpha(x) \in \mathbb{Q}[\mathbf{x}]$.

□

Si $\mathbf{K} = \mathbb{Q}(\theta)$ es un campo de números; como ya se vió los **K**-conjugados de θ son las raíces del polinomio mínimo de θ sobre $\mathbb{Q}$, las cuales son distintas; pero esto no siempre es cierto ya que por ejemplo $\sigma_i(1) = 1$ para toda i.

Algo más preciso se da en el siguiente.

Teorema 1.10 *Sea $\alpha \in \mathbf{K} = \mathbb{Q}(\theta)$. Con la notación anterior*

a) *El polinomio de campo f_α es una potencia del polinomio mínimo p_α.*
b) *Los **K**-conjugados de α son los ceros de p_α en $\mathbb{C}$, cada uno repetido $\frac{n}{m}$ veces en f_α, donde $m = \partial(p_\alpha)$ es un divisor de n.*
c) *$\alpha \in \mathbb{Q}$ si y sólo si todos sus **K**-conjugados son iguales.*
d) *$\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ si y sólo si los **K**-conjugados de α son distintos.*

Demostración : a) Sea p_α el polinomio mínimo de α sobre $\mathbb{Q}$ (p_α es irreducible y tiene raices distintas).

Claramente α es raíz de $f_\alpha(x)$ ya que $\sigma_i(\alpha) = \alpha$ para alguna i y por lo tanto $p_\alpha | f_\alpha$, esto es que $f_\alpha = p_\alpha h_1$. Sea s el mínimo entero positivo tal que $p_\alpha^s | f_\alpha$ y $p_\alpha^{s+1} \nmid f_\alpha$, entonces $f_\alpha = p_\alpha^s h$ donde p_α y h son primos relativos y mónicos. Para terminar basta probar que $h(x)$ es una constante $(h(x) = 1)$.

Si $h(x)$ no es una constante, sea β una raíz de $h(x)$, entonces también es una raíz de $f_\alpha(x)$ pues $f_\alpha(x) = p_\alpha^s(x)h(x)$; de hecho β es una de las $\sigma_i(\alpha)$, y como $\alpha = r(\theta)$, entonces $\beta = \sigma_i(\alpha) = r(\theta_i)$. Definamos $g(x) = h(r(x)) \in \mathbb{Q}[\mathbf{x}]$, entonces $g(\theta_i) = h(r(\theta_i)) = h(\beta) = 0$, es decir, θ_i es raíz de $g(x)$, pero también θ_i es raíz de $p(x)$ (el polinomio mínimo de θ sobre $\mathbb{Q}$), entonces $p|g$ y por lo tanto $g(\theta_j) = 0$ $(1 \leq j \leq n)$ en especial $g(\theta) = 0$. Por lo tanto $h(\alpha) = h(r(\theta)) = g(\theta) = 0$, esto último implica que $p_\alpha|h$ lo cual es una contradicción. Finalmente concluimos que $h(x) = 1$ y que $f_\alpha = p_\alpha^s$.

b) Supongamos que p_α, el polinomio mínimo de α sobre $\mathbb{Q}$, tiene grado m. La igualdad $f_\alpha = p_\alpha^s$ muestra que f_α y p_α tienen las mismas raíces, cada una repetida $s = \dfrac{n}{m}$ veces en $f_\alpha(x)$ ya que $n = \partial(f_\alpha) = \partial(p_\alpha^s) = sm$.

c) $\Rightarrow$) Si $\alpha \in \mathbb{Q}$ claramente $\sigma_i(\alpha) = \alpha \in \mathbb{Q}$.

$\Leftarrow$) Si todos los $\sigma_i(\alpha)$ son iguales. Por inciso a) tenemos que: $s = n = \dfrac{n}{m}$ de donde se tiene que $m = 1 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ y de aquí que $\alpha \in \mathbb{Q}$.

d) $\Rightarrow$) Si $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$, entonces $[Q(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}] = n$, lo cual implica que el grado de $p_\alpha(x)$ es n, y por lo tanto los $\sigma_i(\alpha)$ son distintos pues son las raíces de $p_\alpha(x)$.

$\Leftarrow$) Si todos los **K**-conjugados de α son distintos, entonces el grado de $p_\alpha(x)$ es n y de aquí que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}] = n$. Por otro lado como $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\theta)$, entonces se tiene que

$$n = [\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

de donde se concluye que $[\mathbb{Q}(\theta) : \mathbb{Q}(\alpha)] = 1$, y por lo tanto $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha)$.

□

Observemos que los **K**-conjugados de α no necesariamente son elementos de **K**, ya que por ejemplo si α es la raíz cubica real de 2, entonces $\mathbf{K} = \mathbb{Q}(\alpha)$ es un subcampo de $\mathbb{R}$. Pero los **K**-conjugados de α son $\alpha, \alpha\omega, \alpha\omega^2$, donde

$$\omega = \frac{-1 + \sqrt{3}i}{2}$$

es decir que $\alpha\omega, \alpha\omega^2$ no están en $\mathbb{Q}(\alpha)$.

Definición 1.11 *Si* **K** *es un campo de números de grado n sobre* $\mathbb{Q}$ *y si* $\{\alpha_1, \ldots, \alpha_n\}$ *es una base de* **K** *sobre* $\mathbb{Q}$, *entonces el discriminante de esta*

base (denotádo por $\Delta[\alpha_1,\ldots,\alpha_n]$) se define como

$$\Delta[\alpha_1,\ldots,\alpha_n] = \{\det[\sigma_i(\alpha_j)]\}^2 = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2$$

Si $\{\beta_1,\ldots,\beta_n\}$ es cualquier otra base de $\mathbf{K}$ sobre $\mathbb{Q}$, entonces $\beta_i = \sum_{j=1}^n c_{ij}\alpha_j$. Matricialmente tenemos $B = CA$, donde

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad ; \quad B = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

y la matriz $C = (c_{ij})$ tiene entradas racionales, y es la traspuesta de la matriz de cambio de base ($\det C \neq 0$).
Claramente $\Delta[\beta_1,\ldots,\beta_n] = [\det C]^2\Delta[\alpha_1,\ldots,\alpha_n]$. En efecto,n ya que

$$\begin{aligned}
\Delta[\beta_1,\ldots,\beta_n] &= \begin{vmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \cdots & \sigma_2(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{vmatrix}^2 \\
&= \begin{vmatrix} \sigma_1(\sum_{i=1}^n c_{i1}\alpha_i) & \cdots & \sigma_1(\sum_{i=1}^n c_{in}\alpha_i) \\ \sigma_2(\sum_{i=1}^n c_{i1}\alpha_i) & \cdots & \sigma_2(\sum_{i=1}^n c_{in}\alpha_i) \\ \vdots & \ddots & \vdots \\ \sigma_n(\sum_{i=1}^n c_{i1}\alpha_i) & \cdots & \sigma_n(\sum_{i=1}^n c_{in}\alpha_i) \end{vmatrix}^2 \\
&= \begin{vmatrix} \sum_{i=1}^n c_{i1}\sigma_1(\alpha_i) & \cdots & \sum_{i=1}^n c_{in}\sigma_1(\alpha_i) \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n c_{i1}\sigma_n(\alpha_i) & \cdots & \sum_{i=1}^n c_{in}\sigma_n(\alpha_i) \end{vmatrix}^2 \\
&= \left| \begin{pmatrix} c_{11} & \cdots & c_{n1} \\ \vdots & \ddots & \vdots \\ c_{1n} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \right|^2,
\end{aligned}$$

de donde se sigue lo afirmado

Teorema 1.12 *El discriminante de cualquier base de* $\mathbf{K} = \mathbb{Q}(\theta)$ *es un número racional distinto de cero. Si todos los* $\mathbf{K}$*-conjugados son reales, entonces el discriminante de cualquier base es positivo.*

Demostración : Se sabe que una base de K es $\{1, \theta, \ldots, \theta^{n-1}\}$. Ahora si los $\mathbf{K}$-conjugados de θ son $\theta_1, \ldots, \theta_n$, y $\Delta[1, \theta, \ldots, \theta_{n-1}] = D_n^2$, entonces

$$D_n^2 = \begin{vmatrix} \sigma_1(1) & \cdots & \sigma_1(\theta^{n-1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(1) & \cdots & \sigma_n(\theta^{n-1}) \end{vmatrix}^2$$

$$D_n^2 = \begin{vmatrix} 1 & \cdots & \theta_1^{n-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & \theta_n^{n-1} \end{vmatrix}^2$$

en donde a D_n se le conoce como el determinante de Vandermonde.

Si reemplazamos a θ_n por una variable x, entonces el determinante D_n se transforma en un polinomio $D_n(x)$ de grado $n-1$, en donde $x = \theta_1, \theta_2, \ldots, \theta_{n-1}$ son sus raíces. En efecto, ya que $D_n(\theta_i)$ es un determinante con dos filas iguales para cada $i = 1, 2, \ldots, n-1$. Por lo tanto

$$D_n(x) = a(x - \theta_1)(x - \theta_2) \cdots (x - \theta_{n-1})$$

donde a es el coeficiente del término de mayor grado de $D_n(x)$, esto es que

$$a = D_{n-1} = \begin{vmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_{n-1} & \cdots & \theta_{n-1}^{n-2} \end{vmatrix}$$

Con todo lo anterior tenemos que

$$D_n(\theta_n) = D_{n-1}(\theta_n - \theta_1) \ldots (\theta_n - \theta_1)$$

Ahora como D_{n-1} es un determinante del mismo tipo que D_n, se puede tratar de igual forma.

En resumen tenemos que

$$\begin{aligned} D_n^2 = {} & (\theta_n - \theta_1)^2 \cdots (\theta_n - \theta_{n-1})^2 \\ & (\theta_{n-1} - \theta_1)^2 \cdots (\theta_{n-1} - \theta_{n-2})^2 \\ & \vdots \\ & (\theta_3 - \theta_2)^2 (\theta_3 - \theta_1)^2 \\ & (\theta_2 - \theta_1)^2 \end{aligned}$$

esto es que

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

Claramente $D_n = \prod(\theta_j - \theta_i)$ es de la forma $h(\theta_1, \ldots, \theta_n)$ en donde $h(x_1, \ldots, x_n) \in \mathbb{Q}[\mathbf{x}_1, \ldots, \mathbf{x}_n]$, por otro lado $h(x_1, \ldots, x_n)$ es antisimétrico pues al efectuar cualquier permutación de $(x_1, \ldots, x_n)$, el polinomio queda igual ó quizas cambia de signo dependiendo de la permutación hecha, esto se debe a que el intercambio de dos variables, corresponde al intercambio de 2 filas en el determinante de Vandermonde

$$D = \prod_{1\le i<j\le n} (x_j - x_i) = h(x_1, \ldots, x_n).$$

Como $D = h(x_1, \ldots, x_n)$ es antisimétrico, $D^2 = [h(x_1, \ldots, x_n)]^2$ es simétrico y tiene coeficientes racionales. Finalmente como $p(x) \in \mathbb{Q}[\mathbf{x}]$, y sus raíces $\theta_1, \ldots, \theta_n$ son distintas, entonces

$$\Delta = D_n^2 = [h(x_1, \ldots, x_n)]^2 \in \mathbb{Q} \quad , \quad \Delta \neq 0$$

Por otro lado si $\{\beta_1, \ldots, \beta_n\}$ es cualquier otra base de $\mathbf{K}$, entonces

$$\Delta[\beta_1, \ldots, \beta_n] = [\det C]^2 \Delta$$

en donde $C = (c_{ij})$ es la matriz de cambio de base $(\det C \neq 0; \det C \in \mathbb{Q})$. Por lo tanto $0 \neq \Delta[\beta_1, \ldots \beta_n] \in \mathbb{Q}$. Para finalizar observemos que si todos los θ_i son reales, entonces $\Delta > 0$, y por lo tanto $\Delta[\beta_1, \ldots, \beta_n] > 0$.

□

1.3 Enteros algebraicos

Definición 1.13 *Un número $\theta \in \mathbb{C}$ se dice que es un entero algebraico si es raíz de algún polinomio mónico $p(x)$ con coeficientes enteros.*

Ejemplos :

a) $\theta = \sqrt{-2}$ es un entero algebraico ya que θ es raíz de $p(x) = x^2 + 2 \in \mathbf{Z}[\mathbf{x}]$

b) $\tau = \dfrac{1+\sqrt{5}}{2}$ es un entero algebraico ya que τ es raíz de $f(x) = x^2 - x - 1 \in \mathbf{Z}[\mathbf{x}]$

c) $\alpha \in \mathbf{Z}$ es un entero algebraico ya que α es raíz de $g(x) = x - \alpha \in \mathbf{Z}[\mathbf{x}]$

Lema 1.14 *Sea $\alpha \in \mathbb{C}$. Son equivalentes:*

a) *α es un entero algebraico.*
b) *El grupo aditivo del anillo $\mathbb{Z}[\alpha]$ es finitamente generado.*
c) *α es miembro de algún subanillo de $\mathbb{C}$ que tiene un grupo aditivo finitamente generado.*
d) *$\alpha A \subseteq A$ para algún grupo aditivo finitamente generado $A \subseteq \mathbb{C}$.*

Demostración : a) $\Rightarrow$b) Si α es un entero algebraico, entonces para alguna $n \in \mathbb{N}$

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \, , \, a_i \in \mathbb{Z} \, ,$$

de lo cuál se obtiene

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0 \tag{1.3}$$

De lo anterior se infiere que el grupo aditivo de $\mathbb{Z}[\alpha]$ esta generado por $S = \{1, \alpha, \ldots, \alpha^{n-1}\}$. En efecto, ya que procediendo inductivamente, si $m \geq n$ y $\alpha^m \in \langle S \rangle$, entonces usando la igualdad 1.3, α^{m+1} se puede escribir como

$$\begin{aligned} \alpha^{m+1-n+n} &= \alpha^{m+1-n}(-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0) \\ &= -a_{n-1}\alpha^m - a_{n-2}\alpha^{m-1} - \cdots - a_0\alpha^{m+1-n} \quad \in \langle S \rangle \end{aligned}$$

Por lo tanto todas las potencias de $\alpha \in \langle S \rangle$, esto es que $\mathbb{Z}[\alpha]$ es finitamente generado como grupo aditivo.

b) $\Rightarrow$c) Tómese el subanillo como $\mathbb{Z}[\alpha]$.

c) $\Rightarrow$d) Sea A finitamente generado, $\alpha A = \{\alpha x \, : \, x \in A\}$. Claramente $\alpha A \subseteq A$ pues $\alpha \in A$ y A es un anillo.

d) $\Rightarrow$a) Si $\{a_1, \ldots, a_n\}$ generan a A, entonces como $\alpha A \subseteq A$ se tiene que

$$\begin{aligned} \alpha a_1 &= m_{11}a_1 + m_{12}a_2 + \cdots + m_{1n}a_n \\ \alpha a_2 &= m_{21}a_1 + m_{22}a_2 + \cdots + m_{2n}a_n \qquad m_{ij} \in \mathbb{Z} \\ &\vdots \qquad\qquad\qquad \vdots \\ \alpha a_n &= m_{n1}a_1 + m_{n2}a_2 + \cdots + m_{nn}a_n \end{aligned}$$

Matricialmente nos queda

$$(\alpha I - M) \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

en donde I, M son ambas matrices cuadradas de tamaño $n \times n$, $M = (m_{ij})$ e I es la matriz identidad. Ahora como no todos los a_i son ceros, entonces el sistema de ecuaciones anterior tiene solución no trivial , por lo cuál

$$\det(\alpha I - M) = 0$$

desarrollando este determinante se obtiene

$$\alpha^n + \text{ terminos de grado menor } = 0$$

es decir que α es raíz de un polinomio mónico con coeficintes enteros. Por lo tanto α es un entero algebraico.

□

Teorema 1.15 *El conjunto* **B** *de enteros algebraicos es un subanillo de* **A** *(***A** *el conjunto de números algebraicos)*

Demostración : Si $\alpha, \beta \in \mathbf{B}$. Por el lema previo $\mathbf{Z}[\alpha]$ y $\mathbf{Z}[\beta]$ tienen grupos aditivos finitamente generados, entonces el anillo $\mathbf{Z}[\alpha, \beta]$ también visto como grupo aditivo es finitamente generado pues si $\{\alpha_1, \ldots, \alpha_m\}$ genera a $\mathbf{Z}[\alpha]$ y $\{\beta_1, \ldots, \beta_n\}$ genera a $\mathbf{Z}[\beta]$, mediante un cálculo muy sencillo se puede probar que los elementos $\alpha_i\beta_j$ $(1 \leq i \leq m\ 1 \leq j \leq n)$ generan a $\mathbf{Z}[\alpha, \beta]$.

Finalmente $\mathbf{Z}[\alpha, \beta]$ contiene a $\alpha + \beta$ y $\alpha\beta$, y como el grupo aditivo de $\mathbf{Z}[\alpha, \beta]$ es finitamente generado, entonces $\alpha + \beta$, $\alpha\beta \in \mathbf{B}$.

□

Teorema 1.16 *Si* $\theta \in \mathbf{C}$ *y* $p(\theta) = 0$, *en donde* $p(x)$ *es un polinomio mónico con coeficientes en* **B**, *entonces* $\theta \in \mathbf{B}$.

Demostración : Si $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbf{B}[\mathbf{x}]$, entonces

$$a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} + \theta^n = 0$$

de aquí que

$$\theta^n = -a_0 - a_1\theta - \cdots - a_{n-1}\theta^{n-1} \tag{1.4}$$

Por otro lado afirmamos que el anillo $\mathbf{Z}[a_0, \ldots, a_{n-1}, \theta]$ tiene grupo aditivo finitamente generado. En efecto ya que si consideramos los productos

$$a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \theta^m \tag{1.5}$$

Usando la igualdad 1.4 y razonando igual que en el lema 1.14 (a) $\Rightarrow$ (b), se tiene que cualquier potencia de θ y en particular θ^m es de la forma

$$-a_0\theta^{s_0} - a_1\theta^{s_1} - \cdots - a_{n-1}\theta^{s_{n-1}} \quad , \quad 0 \leq s_i \leq n-1$$

Por otro lado como $a_0, \ldots, a_{n-1} \in \mathbf{B}$, entonces los anillos

$$\mathbf{Z}[a_0], \ldots, \mathbf{Z}[a_{n-1}]$$

tienen grupos aditivos finitamente generados. Con todo lo anterior se tiene que sólo valores finitos para los exponentes de la expresión 1.5 son necesarios y por lo tanto $\mathbf{Z}[a_0, \ldots, a_{n-1}, \theta]$ tiene grupo aditivo finitamente generado. Finalmente por el lema 1.14 (c) $\Rightarrow$ (a) se concluye que $\theta \in \mathbf{B}$.

□

Definición 1.17 *Sea* $\mathbf{K}$ *un campo de números. El anillo de enteros de* $\mathbf{K}$, *denotado por* $\mathcal{O}_\mathbf{K}$, *es la intersección de* $\mathbf{K}$ *con el anillo de enteros* $\mathbf{B}$, *es decir que* $\mathcal{O}_\mathbf{K} = \mathbf{K} \cap \mathbf{B}$.

Lema 1.18 *Si* $\alpha \in \mathbf{K}$, *entonces* $c\alpha \in \mathcal{O}_\mathbf{K}$ *para algún* $0 \neq c \in \mathbf{Z}$.

Demostración : Sea $f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m \in \mathbf{Q}[\mathbf{x}]$ el polinomio mínimo de α sobre $\mathbf{Q}$, y c el mínimo entero positivo tal que $cf(x) \in \mathbf{Z}[\mathbf{x}]$, entonces $c\alpha \in \mathcal{O}_\mathbf{K}$. En efecto, ya que

$$\begin{aligned} 0 \;=\; c^m f(\alpha) \;&=\; c^m a_o + c^m a_1 \alpha + \cdots + c^m \alpha^m \\ &=\; c^m a_0 + c^{m-1} a_1 (c\alpha) + \cdots + (c\alpha)^m \end{aligned}$$

esto es que $c\alpha$ es raíz del polinomio

$$g(x) = c^m a_0 + c^{m-1} a_1 x + \cdots + c a_{m-1} x^{m-1} + x^m \quad \in \mathbf{Z}[\mathbf{x}]$$

□

Corolario 1.19 *Cualquier ideal* $\mathcal{I}$ *no nulo de* $\mathcal{O}_\mathbf{K}$ *contiene una base de* $\mathbf{K}$.

Demostración : Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $\mathbf{K}$, entonces por el lema 1.18, existen $c_1, \ldots, c_n \in \mathbf{Z}, c_i \neq 0$ tales que $c_1\alpha_1, \ldots, c_n\alpha_n \in \mathcal{O}_\mathbf{K}$. Ahora si $0 \neq \beta \in \mathcal{I}$, entonces $c_1\alpha_1\beta, \ldots, c_n\alpha_n\beta \in \mathcal{I}$ y fácilmente se checa que estos conforman una base de $\mathbf{K}$.

□

Corolario 1.20 *Si* $\mathbf{K}$ *es un campo de números, entonces* $\mathbf{K} = \mathbb{Q}(\Theta)$ *para algún entero algebraico* Θ

Demostración : Sabemos que $\mathbf{K} = \mathbb{Q}(\theta)$, en donde θ es un número algebraico. Por otro lado en virtud del lema previo se tiene que $c\theta = \Theta \in \mathcal{O}_{\mathbf{K}}$ para algún $0 \neq c \in \mathbb{Z}$ y , entonces $\mathbb{Q}(\theta) = \mathbb{Q}(\Theta)$. En efecto ya que claramente $\Theta \in \mathbb{Q}(\theta)$ y de aquí que $\mathbb{Q}(\Theta) \subseteq \mathbb{Q}(\theta)$, por otro lado como $\theta = \Theta/c$, entonces $\theta \in \mathbb{Q}(\Theta)$ y de aquí que $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\Theta)$.

□

Observación : Si $\mathbf{K} = \mathbb{Q}(\theta)$ donde θ es un entero algebraico, no necesariamente $\mathcal{O}_{\mathbf{K}}$ es igual a $\mathbb{Z}[\theta]$. Lo que siempre es cierto es que $\mathbb{Z}[\theta] \subseteq \mathcal{O}_{\mathbf{K}}$. En efecto, pues $p(\theta) \in \mathcal{O}_{\mathbf{K}}\ \forall\ p(x) \in \mathbb{Z}[\mathbf{x}]$. Para ver que la otra contención no siempre es cierta, notemos que $\mathbb{Q}(\sqrt{5})$ es un campo de números y que $\sqrt{5}$ es un entero algebraico ya que es raíz del polinomio $f(x) = x^2 - 5$, también $\alpha = \dfrac{1+\sqrt{5}}{2}$ es un entero algebraico pues es un cero de $f(x) = x^2 - x - 1$. Claramente $\alpha \in \mathcal{O}_{\mathbf{K}}$ y sin embargo $\alpha \notin \mathbb{Z}[\sqrt{5}]$.

Existe un criterio muy usado, en terminos del polinomio mínimo para que un número sea un entero algebraico.

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

Demostración : $\Rightarrow$) Si α, es un entero algebraico, entonces $q(\alpha) = 0$ para algún $q(x) \in \mathbb{Z}[\mathbf{x}]$, $q(x)$ mónico . Por lo tanto si $p(x)$ es el polinomio mínimo de α sobre $\mathbb{Q}$, entonces $q = ph$, $h(x) \in \mathbb{Q}[\mathbf{x}]$ y por el Lema de Gauss [ver teorema A.10 del apéndice], existe $\lambda \in \mathbb{Q}, \lambda \neq 0$ tal que $q = (\lambda p)(\lambda^{-1}h)$ en donde $\lambda p, \lambda^{-1}h \in \mathbb{Z}[\mathbf{x}]$. Pero como $p(x)$ y $q(x)$ son mónicos, entonces $\lambda = 1$ y $p(x) \in \mathbb{Z}[\mathbf{x}]$.

$\Leftarrow$) Esto se sigue inmediatamente de la definición de polinomio mínimo.

□

De ahora en adelante a los enteros algebraicos les llamaremos *enteros* simplemente y a los enteros usuales $\mathbb{Z}$ les llamaremos *enteros racionales.*

Lema 1.22 *Un entero es un número racional si y sólo si este es un entero racional. Equivalentemente* $\mathbf{B} \cap \mathbb{Q} = \mathbb{Z}$

Demostración : $\Rightarrow$) Sea α un entero ($\alpha \in \mathbf{B}$) y α racional ($\alpha \in \mathbb{Q}$). Por el lema 1.21 el polinomio mínimo de α sobre $\mathbb{Q}$ tiene coeficientes en $\mathbb{Z}$, pero su polinomio mínimo es $f(x) = x - \alpha$. Por lo tanto $\alpha \in \mathbb{Z}$ y $\mathbf{B} \cap \mathbb{Q} \subseteq \mathbb{Z}$.

$\Leftarrow$) Esto es inmediato ya que todo $\alpha \in \mathbf{Z}$ es un número racional y tambien un entero (ver ejemplos vistos enseguida de la definición 1.13). Por lo tanto $\mathbf{Z} \subseteq \mathbf{B} \cap \mathbf{Q}$.

□

1.4 Bases enteras

Si $\mathbf{K} = \mathbb{Q}(\theta)$ es un campo de números de grado n sobre $\mathbb{Q}$, entonces

$$\{1, \theta, \ldots, \theta^{n-1}\}$$

es una base de $\mathbf{K}$ sobre $\mathbb{Q}$. En el caso en que θ es un entero la anterior base consta de puros enteros.

Por otro lado se sabe que $\mathcal{O}_\mathbf{K}$ (el anillo de enteros de $\mathbf{K}$) es un grupo abeliano bajo la adición.

Definición 1.23 *Una $\mathbf{Z}$-base de $(\mathcal{O}_\mathbf{K}, +)$ es llamada una base entera de $\mathbf{K}$. Esto es que $\{\alpha_1, \ldots, \alpha_s\}$ es una base entera si y sólo si $\alpha_i \in \mathcal{O}_\mathbf{K}$ $\forall i$ y cualquier elemento de $\mathcal{O}_\mathbf{K}$ se expresa de manera única como $a_1\alpha_1 + \cdots + a_s\alpha_s$; $a_i \in \mathbf{Z}$*

Una pregunta muy natural que nos podemos hacer es: ?existen bases enteras?. Para contestar a ésto primero probaremos el siguiente lema del cual se desprenderá inmediatamente la respuesta.

Lema 1.24 *Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $\mathbf{K}$ consistente de puros enteros, entonces $0 \neq \Delta[\alpha_1, \ldots, \alpha_n] \in \mathbf{Z}$*

Demostración Por el teorema 1.12 tenemos que $0 \neq \Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q}$. Además $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbf{B}$ pues los $\mathbf{K}$-conjugados de α_i $(1 \leq i \leq n)$ son las raíces del polinomio mínimo p_{α_i} de α_i sobre $\mathbb{Q}$, el cuál tiene coeficientes enteros pues α_i es entero [ver lema 1.21].

Resumiendo tenemos que $0 \neq \Delta[\alpha_1, \ldots, \alpha_n] \in \mathbf{B} \cap \mathbb{Q} = \mathbf{Z}$.

□

Teorema 1.25 *Cualquier campo de números $\mathbf{K}$ de grado n sobre $\mathbb{Q}$ posee una base entera, y el grupo aditivo de $\mathcal{O}_\mathbf{K}$ es abeliano libre de rango n.*

Demostración Se sabe que si θ es un entero en $\mathbf{K}$, $\{1, \theta, \ldots, \theta^{n-1}\}$ es una base de $\mathbf{K}$ que consiste de puros enteros, la cual es una $\mathbb{Q}$-base pero no

necesariamente una $\mathbb{Z}$-base. También se sabe que el discriminante de una base que consiste de puros enteros es un entero racional.

Tomemos $\{w_1, \ldots, w_n\}$ una $\mathbb{Q}$-base de $\mathbf{K}$ formada por puros enteros de tal manera que $|\Delta[w_1, \ldots, w_n]|$ sea mínimo. Es de esperarse que $\{w_1, \ldots, w_n\}$ sea una $\mathbb{Z}$-base de $(\mathcal{O}_\mathbf{K}, +)$. En efecto, ya que si no lo fuera, entonces existiría un $w \in \mathcal{O}_\mathbf{K}$ tal que

$$w = a_1 w_1 + \cdots + a_n w_n \qquad a_i \in \mathbb{Q}\,, \quad \text{no todos en } \mathbb{Z}.$$

Sin pérdida de generalidad sea $a_1 \notin \mathbb{Z}$, entonces $a_1 = a + r$ en donde $a \in \mathbb{Z}$ y $0 < r < 1$ $(r \in \mathbb{Q} - \mathbb{Z})$. Si definimos

$$\psi_1 = w - a w_1 \quad , \quad \psi_i = w_i \qquad (i = 2, \ldots, n) \quad ,$$

$\{\psi_1, \ldots, \psi_n\}$ es una base de $\mathbf{K}$ consistente de enteros pues si

$$c_1\psi_1 + c_2\psi_2 + \cdots + c_n\psi_n = 0 \quad , \quad c_i \in \mathbb{Q} \quad ,$$

sustituyendo los valores de w y a en ψ_1 se tiene que

$$\begin{aligned} c_1(r w_1 + a_2 w_2 + \cdots + a_n w_n) + c_2 w_2 + \cdots + c_n w_n &= 0\,, \\ c_1 r w_1 + (c_1 a_2 + c_2) w_2 + (c_1 a_3 + c_3) w_3 + \cdots + (c_1 a_n + c_n) w_n &= 0\,, \end{aligned}$$

y como $\{w_1, \ldots, w_n\}$ es una base, entonces

$$c_1 r = 0\,,\ c_1 a_2 + c_2 = 0\,,\ \ldots\,,\ c_1 a_n + c_n = 0\,,$$

de donde se concluye que $c_1 = c_2 = \cdots = c_n = 0$. Por lo tanto $\{\psi_1, \ldots, \psi_n\}$ es linealmente independiente sobre $\mathbb{Q}$, y como $\mathbf{K}$ es de grado n, entonces $\{\psi_1, \ldots, \psi_n\}$ es una base de $\mathbf{K}$ claramente consistente de puros enteros algebraicos.

Por otro lado, tenemos que la matriz de cambio de base de $\{w_1, \ldots, w_n\}$ a la base $\{\psi_1, \ldots, \psi_n\}$ es

$$C = \begin{pmatrix} r & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

y de aquí que $0 < \det C = r < 1$. Con todo lo anterior se tiene que

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

lo cuál es una contradicción pues $|\Delta[w_1,\ldots,w_n]|$ era mínimo. Por lo tanto $\{w_1,\ldots,w_n\}$ es una base entera y $(\mathcal{O}_{\mathbf{K}},+)$ es un grupo abeliano libre de rango n.

□

La cuestión de encontrar bases enteras en campos de números $\mathbf{K}$ de grado 2 y en otros casos muy particulares se verá en las siguientes secciones. Por ejemplo se verá que si $\mathbf{K}=\mathbb{Q}(\sqrt{5})$, entonces el correspondiente anillo de enteros es $\mathcal{O}_{\mathbf{K}}=\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{5}]$ y una base entera es $\{1,\frac{1}{2}+\frac{1}{2}\sqrt{5}\}$.

Esto último también se puede probar por una ruta distinta usando el discriminante. En efecto, ya que claramente $\mathbb{Q}(\sqrt{5})=\mathbb{Q}(\frac{1}{2}+\frac{1}{2}\sqrt{5})$ y como los dos monomorfismos $\mathbb{Q}(\sqrt{5})\to\mathbb{C}$ están dados por

$$\begin{aligned}\sigma_1(p+q\sqrt{5}) &= p+q\sqrt{5}\\ \sigma_2(p+q\sqrt{5}) &= p-q\sqrt{5}\,,\end{aligned}$$

entonces

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

el cual es un entero racional libre de cuadrados, y así $\{1,\frac{1}{2}+\frac{1}{2}\sqrt{5}\}$ es una base entera como se afirma en el siguiente

Teorema 1.26 *Si $\{\alpha_1,\ldots,\alpha_n\}$ es una $\mathbb{Q}$-base de $\mathbf{K}$ consistente de puros enteros y $\Delta[\alpha_1,\ldots,\alpha_n]$ es libre de cuadrados, entonces $\{\alpha_1,\ldots,\alpha_n\}$ es una base entera.*

Demostración Sea $\{\beta_1,\ldots,\beta_n\}$ una base entera de $\mathbf{K}$. Entonces existen enteros racionales c_{ij} tales que $\alpha_i=\sum_{j=1}^n c_{ij}\beta_j$, y de aquí

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

pero como $\Delta[\alpha_1,\ldots,\alpha_n]$ es libre de cuadrados, entonces $[\det(c_{ij})]^2=1$ lo cual implica que $[\det(cij)]=\pm1$, es decir, la matriz $C=(c_{ij})$ es unimodular (una matriz cuyo determinante es 1 ó -1). Finalmente, en virtud del lema A.26 del apéndice concluimos que $\{\alpha_1,\ldots,\alpha_n\}$ es una base entera.

□

El recíproco del teorema anterior no es cierto. Por ejemplo, se verá más adelante que el campo $\mathbf{K}=\mathbb{Q}(\sqrt{7})$ tiene una $\mathbb{Q}$-base cuyo discriminante no es libre de cuadrados y que sin embargo es una base entera.

Notemos que para cualesquiera dos bases enteras $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ de un campo de números $\mathbf{K}$ se tiene

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\pm 1)^2 \Delta[\beta_1, \ldots, \beta_n] = \Delta[\beta_1, \ldots, \beta_n] ,$$

ésto es porque la matriz correspondiente al cambio de base es unimodular . Por lo tanto el discriminante de una base entera es independiente de la base entera elegida. Este valor común es llamado *el discriminante* de $\mathbf{K}$ (o de $\mathcal{O}_K$).

1.5 Normas

En esta sección se trabajará con un importantísimo concepto que a menudo sirve para transformar problemas acerca de enteros algebraicos en problemas acerca de enteros racionales.

Recordemos que si $\mathbf{K} = \mathbb{Q}(\theta)$ es un campo de números y $\alpha \in \mathbf{K}$, entonces el polinomio de campo de α sobre $\mathbf{K}$ es

$$f_\alpha(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) \in \mathbb{Q}[\mathbf{x}] .$$

Más aún, en virtud de los teoremas 1.10 a) , 1.21 y el Lema de Gauss se obtiene fácilmente que $\alpha \in \mathcal{O}_\mathbf{K}$ si y sólo si $f_\alpha(x) \in \mathbf{Z}[\mathbf{x}]$.

Definición 1.27 *Para cualquier $\alpha \in \mathbf{K}$ ($\mathbf{K}$ un campo de números de grado n) se define la norma de este como*

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

Gracias al desarrollo de la demostración del teorema 1.9 y a la reciente definición podemos notar que $N_K(\alpha)$ es igual a $\pm$ el termino independiente de $f_\alpha(x)$ ($+$ si n es par y $-$ si n es impar).

Con lo anterior tenemos que si $\alpha \in \mathcal{O}_\mathbf{K}$, entonces $N_K(\alpha) \in \mathbf{Z}$. Más aún, si $\alpha, \beta \in \mathbf{K}$ ($\alpha \neq 0$), y como σ_i es un monomorfismo ($1 \leq i \leq n$), entonces fácilmente se checa que

a) $N_K(\alpha) \neq 0$
b) $N_K(\alpha\beta) = N_K(\alpha) N_K(\beta)$

Para el caso particular en que $\mathbf{K} = \mathbb{Q}(\sqrt{7})$, los enteros de $\mathbf{K}$ son $\mathcal{O}_\mathbf{K} = \mathbf{Z}[\sqrt{7}]$ (ésto se probara en la siguiente sección), y los monomorfismos σ_i son

$$\begin{aligned}\sigma_1(p+q\sqrt{7}) &= p+q\sqrt{7}\\ \sigma_2(p+q\sqrt{7}) &= p-q\sqrt{7}\end{aligned}$$

Notemos que una $\mathbb{Q}$-base de $\mathbf{K}$ es $\{1,\sqrt{7}\}$, de aquí

$$\begin{aligned}N_K(p+q\sqrt{7}) &= p^2-7q^2\\ \Delta[1,\sqrt{7}] &= \begin{vmatrix}1 & \sqrt{7}\\ 1 & -\sqrt{7}\end{vmatrix}^2 = 28\,.\end{aligned}$$

Observemos que el discriminante de $\{1,\sqrt{7}\}$ no es libre de cuadrados, sin embargo esto no implica que $\{1,\sqrt{7}\}$ no sea una base entera (de hecho lo es como se verá en la siguiente sección).

Enseguida veremos la gran relacion que hay entre el discriminante de una base, la norma y la derivada formal de un polinomio.

Proposición 1.28 *Si $\mathbf{K}=\mathbb{Q}(\theta)$ es un campo de números de grado n, y $p(x)$ es el polinomio mínimo de θ sobre $\mathbb{Q}$ ($\partial(p)=n$), entonces la base $\{1,\theta,\ldots,\theta^{n-1}\}$ tiene discriminante*

$$\Delta[1,\theta,\ldots,\theta^{n-1}] = (-1)^{\frac{n(n-1)}{2}} N_K(p'(\theta))$$

en donde $p'(x)$ es la derivada formal del polinomio $p(x)$.

Demostración : Si $\theta_1,\ldots,\theta_n$ son los $\mathbf{K}$-conjugados de θ, entonces

$$p(x)=\prod_{i=1}^{n}(x-\theta_i)\,.$$

Derivando se tiene que

$$p'(x)=\sum_{j=1}^{n}\prod_{j\neq i=1}^{n}(x-\theta_i)$$

de donde

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

Por lo tanto

$$p'(\theta_1)\cdots p'(\theta_n)=\prod_{j=1}^{n}p'(\theta_j)=\prod_{1\leq i\neq j\leq n}(\theta_j-\theta_i)\,.$$

Por otro lado recordemos que

$$\begin{aligned}\Delta[1,\theta,\ldots,\theta^{n-1}] &= \prod_{1\le i<j\le n}(\theta_j-\theta_i)^2 \\ &= (-1)^{\frac{n(n-1)}{2}}\prod_{1\le i\ne j\le n}(\theta_j-\theta_i)\,.\end{aligned}$$

Reuniendo todo lo anterior se tiene que

$$\begin{aligned}\Delta[1,\theta,\ldots,\theta^{n-1}] &= (-1)^{\frac{n(n-1)}{2}}\prod_{j=1}^{n}p'(\theta_j) \\ &= (-1)^{\frac{n(n-1)}{2}}\prod_{j=1}^{n}p'(\sigma_j(\theta)) \\ &= (-1)^{\frac{n(n-1)}{2}}\prod_{j=1}^{n}\sigma_j(p'(\theta)) \\ &= (-1)^{\frac{n(n-1)}{2}}N_K(p'(\theta))\,.\end{aligned}$$

□

1.6 Campos cuadráticos

Definición 1.29 *Un campo cuadrático es un campo de números de grado 2 sobre* $\mathbb{Q}$.

Proposición 1.30 *Los campos cuadráticos son precisamente aquellos de la forma* $\mathbb{Q}(\sqrt{d})$ *para* $d \in \mathbb{Z}$, d *libre de cuadrados.*

Demostración : Por el corolario 1.20, $\mathbf{K} = \mathbb{Q}(\theta)$, en donde $\theta \in \mathcal{O}_{\mathbf{K}}$ y θ es raíz del polinomio irreducible $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$. Entonces

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

Claramente $a^2 - 4b$ no puede ser un cuadrado perfecto ya que si lo fuera, entonces $f(x)$ sería reducible en $\mathbb{Q}[x]$. Haciendo la factorización primaria de $a^2 - 4b$, este lo podemos expresar como $a^2 - 4b = r^2 d$ donde $r, d \in \mathbb{Z}$ y d es libre de cuadrados.

Por lo tanto

$$\mathbb{Q}(\theta) = \mathbb{Q}\left(\frac{-a \pm r\sqrt{d}}{2}\right) = \mathbb{Q}(\sqrt{d})\,.$$

□

Teorema 1.31 *Sea $d \in \mathbb{Z}$, d libre de cuadrados. Entonces los enteros de $\mathbb{Q}(\sqrt{d})$ son :*

a) $\mathbb{Z}[\sqrt{d}]$ *si* $d \not\equiv 1 \pmod 4$.
b) $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ *si* $d \equiv 1 \pmod 4$.

Demostración : Si $\alpha \in \mathbb{Q}(\sqrt{d})$ $(\alpha \notin \mathbb{Q})$, entonces $\alpha = r + s\sqrt{d}$, $r, s \in \mathbb{Q}(s \neq 0)$. Claramente si reducimos r y s a su mínima expresión, entonces α se pueden tomar de la siguiente manera

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

donde $a, b, c \in \mathbb{Z}$, $(b \neq 0$, $c > 0)$ y además a, b y c son primos relativos.

Ahora, $\alpha \in \mathcal{O}_K$ si y sólo si los coeficientes del polinomio mínimo

$$f(x) = \left(x - \left(\frac{a + b\sqrt{d}}{c}\right)\right)\left(x - \left(\frac{a - b\sqrt{d}}{c}\right)\right),$$

son enteros. Efectuando las operaciones lo anterior equivale a que

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z} \tag{1.6}$$

y

$$\frac{2a}{c} \in \mathbb{Z}. \tag{1.7}$$

Esto implica que $c|2$. En efecto, si suponemos que $c > 1$ podemos tomar un primo racional p que divida a c. Si $p|a$, entonces $p^2|b^2 d$. Como d es libre de cuadrados $p|b$. Esto no es posible, entonces si $c > 1, c = 2$.

Casos :

i) Si $c = 1$, entonces α es un entero en cualquier caso

ii) Si $c = 2;$, entonces a y b deben ser ambos impares, pues si alguno es par, por la expresión 1.6 el otro también resulta par. Sustituyendo el valor de c se tiene que $\frac{a^2 - b^2 d}{4} \in \mathbb{Z}$ y de aquí

$$a^2 - b^2 d \equiv 0 \pmod 4. \tag{1.8}$$

Ahora como todo número impar tiene cuadrado de la forma $4k^2 + 4k + 1$ $(k \in \mathbb{Z})$, $a^2 \equiv 1 \equiv b^2 \pmod 4$ y de aquí

$$\begin{aligned} a^2 &\equiv 1 \pmod 4, \\ -b^2 d &\equiv -d \pmod 4, \end{aligned}$$

sumando estas congruencias se obtiene

$$a^2 - b^2 d \equiv 1 - d \pmod 4,$$

pero por 1.8 se tiene entonces que $d \equiv 1 \pmod 4$.

Recíprocamente si $d \equiv 1 \pmod 4$ y a, b son impares, entonces se tiene que c es un entero ya que un análisis similar al anterior nos prueba que 1.6 y 1.7 se cumplen.

Resumiendo:
Si $d \not\equiv 1 \pmod 4$, entonces $c = 1$. Por lo tanto

$$\mathcal{O}_{\mathbf{K}} = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\} = \mathbf{Z}[\sqrt{d}]$$

pues $\mathbf{Z}[\sqrt{d}]$ está generado por $\{1, \sqrt{d}\}$ ($\mathbf{Z}[\sqrt{d}]$ visto como grupo aditivo).

Si $d \equiv 1 \pmod 4$, entonces $c = 1$ ($a, b \in \mathbf{Z}$) ó $c = 2$ ($a, b \in \mathbf{Z}$ impares). Por lo tanto

$$\mathcal{O}_{\mathbf{K}} = \left\{a + b\sqrt{d} : a, b \in \mathbf{Z}\right\} \cup \left\{\frac{a + b\sqrt{d}}{2} : a, b \in \mathbf{Z} \text{ impares}\right\}.$$

Lo anterior también se puede escribir como

$$\begin{aligned} \mathcal{O}_{\mathbf{K}} &= \left\{\frac{a + b\sqrt{d}}{2} : a, b \in \mathbf{Z} \text{ con la misma paridad}\right\} \\ &= \left\{\frac{a - b}{2} + b\left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right) : a, b \in \mathbf{Z} \text{ con la misma paridad}\right\}. \end{aligned}$$

Por lo tanto

$$\mathcal{O}_{\mathbf{K}} = \mathbf{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right]$$

pues $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\frac{1}{2} + \frac{1}{2}\sqrt{d})$ y $\mathbf{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ está generado por $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$. □

Teorema 1.32 *Si $\mathbf{K} = \mathbf{Q}(\sqrt{d})$, d libre de cuadrados, entonces*

(a) *$\mathbf{Q}(\sqrt{d})$ tiene una base entera de la forma $\{1, \sqrt{d}\}$ y discriminante $4d$ si $d \not\equiv 1 \pmod 4$.*

(b) *$\mathbf{Q}(\sqrt{d})$ tiene una base entera de la forma $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ y discriminante d si $d \equiv 1 \pmod 4$.*

Demostración : Los monomorfismos $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ están dados por

$$\begin{aligned} \sigma_1(r+s\sqrt{d}) &= r+s\sqrt{d} \quad r,s \in \mathbb{Q} \\ \sigma_1(r+s\sqrt{d}) &= r-s\sqrt{d} \quad r,s \in \mathbb{Q} \end{aligned}$$

(a) Por el teorema 1.31, $\{1, \sqrt{d}\}$ es una base entera pues es una $\mathbb{Z}$-base de $\mathcal{O}_{\mathbf{K}}$. Además

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

(b) Por el teorema 1.31 $\{1, \frac{1}{2}+\frac{1}{2}\sqrt{d}\}$ es una base entera pues es una $\mathbb{Z}$-base de $\mathcal{O}_{\mathbf{K}}$. Además

$$\begin{aligned} \Delta[1,\tfrac{1}{2}+\tfrac{1}{2}\sqrt{d}] &= \begin{vmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{d} \end{vmatrix}^2 \\ &= (\tfrac{1}{2}-\tfrac{1}{2}\sqrt{d}-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{d})^2 \\ &= (-\sqrt{d})^2 \\ &= d\,. \end{aligned}$$

□

Como campos de números isomorfos tienen el mismo discriminante, se sigue que para distintas d's libres de cuadrado los campos $\mathbb{Q}(\sqrt{d})$ no son isomorfos. Esto completa la clasificación de campos cuadráticos.

Un ejemplo de un campo cuadrático es el campo Gaussiano $\mathbf{K} = \mathbb{Q}(\sqrt{-1})$. En este caso $-1 \not\equiv 1 \pmod 4$, y por lo tanto el anillo de enteros es $\mathcal{O}_{\mathbf{K}} = \mathbf{Z}[\sqrt{-1}]$ (conocido como el anillo de los enteros Gaussianos) y el discriminante es -4 el cual no es libre de cuadrados. Esto último nos prueba que el recíproco del teorema 1.26 no es válido.

1.7 Campos ciclotómicos

Definición 1.33 *Un campo ciclotómico es un campo de la forma* $\mathbf{K} = \mathbb{Q}(\xi)$ *donde* $\xi = e^{2\pi i/m}$ *es una raíz* m*-ésima primitiva de la unidad.*

En el transcurso de este trabajo sólo se considerará el caso en que $m = p$ (p un primo racional).

Notemos que para $p = 2$, $\xi = -1$, y por lo tanto $\mathbb{Q}(\xi) = \mathbb{Q}$ por lo cual este caso lo evitaremos, y trabajaremos siempre con p primo impar a menos que se especifique lo contrario.

Lema 1.34 *El polinomio mínimo de* $\xi = e^{2\pi i/p}$ *sobre* $\mathbb{Q}$ *es*

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

y $[\mathbb{Q}(\xi) : \mathbb{Q}] = p - 1$.

Demostración : Se sabe que $\xi = e^{2\pi i/p}$ es raíz del polinomio $g(x) = x^p - 1$. Además

$$g(x) = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) \text{ , y como } \xi - 1 \neq 0 \text{ ,}$$

entonces ξ es raíz de $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, el cual es irreducible sobre $\mathbb{Q}$. Finalmente, como $f(x) \in \mathbb{Z}[\mathbf{x}]$, $\partial(f) = p - 1$ y f es mónico, entonces $\xi \in \mathcal{O}_{\mathbf{K}}$ y $[\mathbb{Q}(\xi) : \mathbb{Q}] = p - 1$.

□

Como ξ es raíz p-ésima primitiva de la unidad, entonces $\xi, \xi^2, \ldots, \xi^{p-1}$ son también raíces p-ésimas de la unidad ninguna de ellas igual a 1. De hecho $\xi, \xi^2, \ldots, \xi^{p-1}$ son los **K**-conjugados de ξ. Con todo lo anterior tenemos que

$$f(x) = x^{p-1} + \cdots + x + 1 = (x - \xi) \cdots (x - \xi^{p-1}) \tag{1.9}$$

y como todo elemento de $\mathbb{Q}(\xi)$ se escribe de manera única como $a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2}$, entonces los monomorfismos $\sigma_i : \mathbb{Q}(\xi) \to \mathbb{C}$ $(i = 1, 2, \ldots, p-1)$ estan dados por

$$\sigma_i(a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2}) = a_0 + a_1\xi^i + \cdots + a_{p-2}\xi^{i(p-2)} \text{ .}$$

Ahora recordemos que para $\alpha \in \mathbb{Q}(\xi)$, $N_K(\alpha) = \prod_{i=1}^{p-1} \sigma_i(\alpha)$. En particular

$$N_K(\xi) = \xi\xi^2 \cdots \xi^{p-1} = N_K(\xi^i) \quad , \quad i = 1, 2, \ldots, p-1$$

pues $\xi, \xi^2, \ldots, \xi^{p-1}$ son **K**-conjugados. Haciendo $x = 0$ en 1.9 se tiene que

$$1 = (-1)^{p-1}\xi\xi^2 \cdots \xi^{p-1} = N_K(\xi) = N_K(\xi^i) \text{ .}$$

Por lo tanto $N_K(\xi^i) = 1$, $i = 1, 2, \ldots, p-1$. Más aún, fácilmente se puede checar que $N_K(\xi^s) = 1 \quad \forall s \in \mathbb{Z}$. Para el caso en que α es un elemento

arbitrario en $\mathbb{Q}(\xi)$ es en general muy complicado el cálculo de la norma. Un caso muy especial es cuando $\alpha = 1 - \xi$, para el cual

$$N_K(1-\xi) = \prod_{i=1}^{p-1} \sigma_i(1-\xi) = \prod_{i=1}^{p-1}(1-\xi^i)$$

haciendo $x = 1$ en 1.9 se tiene que

$$N_K(1-\xi) = (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}) = p\,.$$

Teorema 1.35 *Sea* $\mathbf{K} = \mathbb{Q}(\xi)$, *donde* $\xi = e^{2\pi i/p}$. *El discriminante de la base* $\{1, \xi, \ldots, \xi^{p-2}\}$ *es* $(-1)^{\frac{p-1}{2}} p^{p-2}$.

Demostración : Se sabe por la proposición 1.28 que

$$\Delta[1, \xi, \ldots, \xi^{p-2}] = (-1)^{\frac{(p-1)(p-2)}{2}} N_K(f'(\xi))\,,$$

donde $f(x)$ es el polinomio mínimo de ξ sobre $\mathbb{Q}$. Ahora como p es impar

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

Por otro lado se sabe que el polinomio mínimo es

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}\,,$$

derivando se tiene

$$f'(x) = \frac{(x-1)px^{p-1} - (x^p - 1)}{(x-1)^2}\,,$$

evaluando en $x = \xi$

$$f'(\xi) = \frac{(\xi-1)p\xi^{p-1} - (\xi^p - 1)}{(\xi-1)^2} = \frac{p\xi^{p-1}}{\xi - 1} = \frac{-p\xi^{p-1}}{1-\xi}\,,$$

tomando normas

$$\begin{aligned} N_K(f'(\xi)) &= \frac{N_K(-p\xi^{p-1})}{N_K(1-\xi)} = \frac{N_K(-p)N_K(\xi^{p-1})}{N(1-\xi)} \\ &= \frac{(-p)^{p-1}(1)}{p} = \frac{p^{p-1}}{p} \\ &= p^{p-2}. \end{aligned}$$

Por lo tanto

$$\Delta[1, \xi, \ldots, \xi^{p-2}] = (-1)^{\frac{(p-1)}{2}} p^{p-2}\,.$$

□

Lema 1.36 *Si $\lambda = 1 - \xi$, entonces $\{1, \lambda, \ldots, \lambda^{p-2}\}$ es una base entera de $\mathbf{K} = \mathbb{Q}(\xi)$ ($\xi = e^{2\pi i/2}$, p primo racional impar).*

Demostración : Como $1, \xi$ son enteros, entonces λ es un entero y consecuentemente lo son también $\lambda^2, \ldots, \lambda^{p-2}$.

Ahora como $\{1, \xi, \ldots, \xi^{p-2}\}$ es una base de $\mathbf{K} = \mathbb{Q}(\xi)$, entonces

$$\lambda^i = \sum_{j=1}^{p-2} a_{ij}\xi^j \quad ; \quad i = 0, 1, 2, \ldots, p-2 \,,$$

en donde la matriz $A = (a_{ij})$ esta dada por

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & -2 & 1 & 0 & 0 & \cdots & 0 \\ 1 & -3 & 3 & -1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{p-2}{0} & -\binom{p-2}{1} & \cdots & \cdots & \cdots & \cdots & \binom{p-2}{p-2} \end{pmatrix}$$

es decir que A es una matriz triangular superior de $(p-1) \times (p-1)$, en donde los números en la diagonal son 1 y -1 alternandose estos. Claramente $\det A = \pm 1 \neq 0$, por lo que $\{1, \lambda, \ldots, \lambda^{p-2}\}$ es una base y además

$$\Delta[1, \lambda, \ldots, \lambda^{p-2}] = \Delta[1, \xi, \ldots, \xi^{p-2}] \tag{1.10}$$

y sólo nos resta probar que $\{1, \lambda, \ldots, \lambda^{p-2}\}$ es base entera. Para esto tomemos una base entera $\{w_1, \ldots, w_{p-1}\}$, entonces

$$\lambda^i = \sum_{j=1}^{p-1} c_{ij} w_j \,, \; c_{ij} \in \mathbf{Z} \quad , \quad i = 0, 1, 2, \ldots, p-2$$

Matricialmente lo anterior se puede expresar como $\Lambda = CW$ y de aquí que

$$\Delta[1, \lambda, \ldots, \lambda^{p-2}] = \left\{\det(c_{ij})\right\}^2 \Delta[w_1, \ldots, w_{p-1}]$$

pero por la ecuación 1.10 y el teorema 1.35 se tiene que

$$\Delta[1, \xi, \ldots, \xi^{p-2}] = \left\{\det(c_{ij})\right\}^2 \Delta[w_1, \ldots, w_{p-1}] \,,$$

en donde $\det(c_{ij}) = \pm p^r$ para alguna $r \in \mathbf{Z}$.

Ahora, de la forma matricial de $\Lambda = CW$ se tiene que

$$W = \frac{\tilde{C}}{detC}\Lambda\ ,$$

en donde $\tilde{C}$ es la matriz adjunta de C ($\tilde{C}$ tiene entradas enteras). Por lo tanto cualquier w_i $(i = 1, 2, \ldots, p-1)$ es de la forma

$$\frac{a_0 + a_1\lambda + \cdots + a_{p-2}\lambda^{p-2}}{p^r} \quad , \quad a_i \in \mathbb{Z}$$

pero como $\{w_1, \ldots, w_{p-1}\}$ es una base entera, entonces cualquier elemento de $\mathbb{Q}(\xi)$ es de esa forma. Si $\{1, \lambda, \ldots, \lambda^{p-2}\}$ no es base entera, entonces existe algún $w \in \mathcal{O}_{\mathbf{K}}$ de la forma

$$\frac{a_0 + a_1\lambda + \cdots + a_{p-2}\lambda^{p-2}}{p^r} \quad , \quad a_i \in \mathbb{Z}$$

donde p^r no divide a todos los a_i $(i = 0, 1, \ldots, p-2)$. Si esto pasa, entonces existe un entero de la forma

$$\frac{b_0 + b_1\lambda + \cdots + b_{p-2}\lambda^{p-2}}{p} \quad , \quad b_i \in \mathbb{Z}\ ,$$

donde p no divide a todos los b_i $(i = 0, 1, \ldots, p-2)$. Sea m el primer índice tal que p no divide a b_m $(m \leq p-2)$, entonces

$$\alpha = \frac{b_m\lambda^m + b_{m+1}\lambda^{m+1} + \cdots + b_{p-2}\lambda^{p-2}}{p} \quad \in \mathcal{O}_{\mathbf{K}} \qquad (1.11)$$

pero recordemos que

$$p = N_K(1-\xi) = \prod_{i=1}^{p-1}(1-\xi^i) = (1-\xi)^{p-1}\gamma_1 \quad , \gamma_1 \in \mathcal{O}_{\mathbf{K}}$$

y como $m+1 \leq p-1$, entonces $p = (1-\xi)^{m+1}\gamma = \lambda^{m+1}\gamma$, $\gamma \in \mathcal{O}_{\mathbf{K}}$. Sustituyendo esto último en la ecuación 1.11 se tiene

$$\lambda^{m+1}\gamma\alpha = b_m\lambda^m + b_{m+1}\lambda^{m+1} + \cdots + b_{p-2}\lambda^{p-2}\ ,$$

y de aquí que

$$b_m\lambda^m = \lambda^{m+1}\beta \quad , \quad \beta \in \mathcal{O}_{\mathbf{K}}\ ,$$

de donde $b_m = \lambda\beta$. Tomando normas

$$N_K(b_m) = b_m^{p-1} = ps = N_K(\lambda)N_K(\beta) \quad , \quad N_K(\beta) = s \in \mathbb{Z}\ .$$

Por lo tanto p divide a b_m^{p-1} y de aquí que p divide a b_m lo cual es una contradicción. Por lo tanto concluimos que $\{1, \lambda, \ldots, \lambda^{p-2}\}$ es una base entera.

□

Del anterior lema se desprende inmediatamente el siguiente

Teorema 1.37 *El anillo de enteros $\mathcal{O}_{\mathbf{K}}$, de $\mathbb{Q}(\xi)$ es $\mathbb{Z}[\xi]$.*

Demostración : Se vió en el lema 1.36 que

$$\lambda^i = \sum_{j=0}^{p-2} a_{ij}\xi^j \quad , \quad i = 0, 1, \ldots, p-2 \, ,$$

en donde a_{ij} son los coeficientes del desarrollo $(1-\xi)^i$, esto es que $a_{ij} \in \mathbb{Z}$. Ahora como $\{1, \lambda, \ldots, \lambda^{p-2}\}$ es una base entera de $\mathbb{Q}(\xi)$, entonces cualquier entero w se puede desarrollar como

$$w = \sum_{j=0}^{p-2} b_j \xi^j \quad , \quad b_j \in \mathbb{Z} \, .$$

Por lo tanto $\{1, \xi, \ldots, \xi^{p-2}\}$ es una base entera y $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\xi]$.

□

Por lo tanto p divide a b_m^{p-1} y de aquí que p divide a b_m lo cual es una contradicción. Por lo tanto concluimos que $\{1, \lambda, \ldots, \lambda^{p-2}\}$ es una base entera.

□

Del anterior lema se desprende inmediatamente el siguiente

Teorema 1.37 *El anillo de enteros $\mathcal{O}_K$, de $\mathbb{Q}(\xi)$ es $\mathbb{Z}[\xi]$.*

Demostración : Se vió en el lema 1.36 que

$$\lambda^i = \sum_{j=0}^{p-2} a_{ij}\xi^j \quad , \quad i = 0, 1, \ldots, p-2 \, ,$$

en donde a_{ij} son los coeficientes del desarrollo $(1-\xi)^i$, esto es que $a_{ij} \in \mathbb{Z}$. Ahora como $\{1, \lambda, \ldots, \lambda^{p-2}\}$ es una base entera de $\mathbb{Q}(\xi)$, entonces cualquier entero w se puede desarrollar como

$$w = \sum_{j=0}^{p-2} b_j \xi^j \quad , \quad b_j \in \mathbb{Z} \, .$$

Por lo tanto $\{1, \xi, \ldots, \xi^{p-2}\}$ es una base entera y $\mathcal{O}_K = \mathbb{Z}[\xi]$.

□

Capítulo 2

Factorización

En este capítulo se estudiará el problema de la factorización en cualquier dominio entero, y en particular en el anillo de enteros $\mathcal{O}_K$ de un campo de números K. Se probará que no todo $\mathcal{O}_K$ goza siempre de las mismas propiedades de factorización que $\mathbb{Z}$. En el capítulo 4 se verá que cuando $\mathcal{O}_K$ goza de las mismas propiedades de factorización que $\mathbb{Z}$, se desprenden inumerables aplicaciones en la solución de problemas sobre ecuaciones diofantinas.

En este capítulo también se verá que en cualquier anillo en donde es posible la factorización en irreducibles, todo número primo será irreducible, pero no todo irreducible es primo. De hecho se verá también que en los anillos en donde los elementos irreducibles coinciden con los primos se tendrá factorización única en irreducibles salvo el orden de los factores y la presencia de unidades.

En el trascurso de este capítulo también se dará parte de la clasificación de las unidades en el anillo de enteros de un campo de números cuadrático.

Posteriormente se extenderá la noción de ideal a lo que es un ideal fraccional y se verá que los ideales fraccionales son una importante herramienta para probar que cualquier ideal no nulo en el anillo de enteros $\mathcal{O}_K$ se puede factorizar como un producto de ideales primos de manera única salvo el orden de los factores.

Finalmente se verá lo que es la norma de un ideal y resultados importantes relativos a ésta.

2.1 Factorizaciones triviales

Definición 2.1 *Si* $\mathbf{R}$ *es un anillo, dos elementos* $x, y \in \mathbf{R}$ *se dice que*

son asociados si $x = uy$ *para una unidad* u.

Sin mucho esfuerzo se puede probar que la relación de ser asociados es una relación de equivalencia en $\mathbf{R}$.

Proposición 2.2 *Las unidades* $\mathbf{R}^*$ *de un anillo* $\mathbf{R}$ *forman un grupo bajo la multiplicación.*

Demostración : Primero que nada notemos que $\mathbf{R}^* \neq \emptyset$ pues $1 \in \mathbf{R}^*$.

i) Si $x, y \in \mathbf{R}^*$, entonces existen $z, w \in \mathbf{R}$ tales que $xz = 1$ y $yw = 1$ de aquí que

$$(xy)(zw) = (xz)(yw) = 1$$

esto es $xy \in \mathbf{R}^*$.

ii) La asociatividad se hereda de $\mathbf{R}$ pues $\mathbf{R}^* \subseteq \mathbf{R}$.

iii) El uno del anillo, el cual es una unidad, funge como el neutro multiplicativo.

iv) La existencia de los inversos multiplicativos se sigue inmediatamente de la definición de unidad.

□

Ejemplos :

a) Si $\mathbf{R} = \mathbb{Q}$, entonces $\mathbf{R}^* = \mathbb{Q} - \{0\}$, el cual es un grupo infinito.

b) Si $\mathbf{R} = \mathbb{Z}$, entonces $\mathbf{R}^* = \{-1, 1\}$, el cual es un grupo cíclico de orden 2.

c) Si $\mathbf{R} = \mathbb{Z}[\sqrt{-1}]$ (el anillo de enteros Gaussianos), entonces $\mathbf{R}^* = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$, el cual es un grupo cíclico de orden 4 (esto se probará en la siguiente proposición).

Proposición 2.3 *El grupo de unidades del anillo de enteros* $\mathcal{O}_\mathbf{K}$ *del campo de números* $\mathbb{Q}(\sqrt{d})$, *donde* d *es libre de cuadrados y* $d < 0$ *es como sigue :*

(a) *Para* $d = -1$, $\mathcal{O}_\mathbf{K}^* = \{\pm 1, \pm\sqrt{-1}\}$
(b) *Para* $d = -3$, $\mathcal{O}_\mathbf{K}^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ *donde* $\omega = e^{2\pi i/3}$
(c) *Para cualquier otra* $d < 0$, $\mathcal{O}_\mathbf{K}^* = \{\pm 1\}$

Demostración : Se sabe por el teorema 1.31 que si

$$d \not\equiv 1 \pmod 4 \;\Rightarrow\; \mathcal{O}_\mathbf{K} = \mathbb{Z}[\sqrt{d}]$$
$$d \equiv 1 \pmod 4 \;\Rightarrow\; \mathcal{O}_\mathbf{K} = \mathbb{Z}[\tfrac{1}{2} + \tfrac{1}{2}\sqrt{d}]$$

Por otro lado, si α es una unidad en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ con inverso β, entonces $\alpha\beta = 1$, tomando normas se tiene que: $N_K(\alpha)N_K(\beta) = 1$, $N_K(\alpha), N_K(\beta) \in \mathbb{Z}$. Por lo tanto $N_K(\alpha) = \pm 1$.

Casos:

1) $d \not\equiv 1 \pmod 4$

$\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Z}$ y

$$N_K(\alpha) = a^2 - db^2 \geq 0$$

pues $d < 0$, y así si α es una unidad

$$N_K(\alpha) = 1 = a^2 - db^2 .$$

Si $d = -1$, entonces $1 = a^2 + b^2$ lo cual sólo ocurre si $a = \pm 1, b = 0$ ó $a = 0, b = \pm 1$ y de aquí que $\mathcal{O}_K{}^* = \{\pm 1, \pm\sqrt{-1}\}$.

Si $d < -1$, entonces $1 = a^2 - db^2$ sólo ocurre si $a = \pm 1, b = 0$ y de aquí que $\mathcal{O}_K{}^* = \{\pm 1\}$.

2) $d \equiv 1 \pmod 4$

$$\alpha = a + b\left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right) \text{ , } a, b \in \mathbb{Z} \text{ , y}$$

$$N_K(\alpha) = \left(\frac{2a+b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 \geq 0$$

pues $d < 0$. Entonces

$$N_K(\alpha) = \frac{(2a+b)^2}{4} - \frac{db^2}{4} = 1$$

Si $d = -3$

$$\begin{aligned} \Rightarrow \quad (2a+b)^2 + 3b^2 &= 4 \\ \Rightarrow \quad 4a^2 + 4ab + b^2 + 3b^2 &= 4 \\ \Rightarrow \quad a^2 + ab + b^2 &= 1 \\ \Rightarrow \quad \left(a + \tfrac{b}{2}\right)^2 + \tfrac{3b^2}{4} &= \left(b + \tfrac{a}{2}\right)^2 + \tfrac{3a^2}{4} = 1 \end{aligned}$$

claramente de la última igualdad se tiene que $|\, a \,| < 2$ y $|\, b \,| < 2$ ya que de lo contrario se tendría que $a^2 + ab + b^2 > 1$. Por lo tanto la última igualdad sólo puede ocurrir si $a = \pm 1, b = 0$ ó $a = 0, b = \pm 1$ ó $a = 1, b = -1$ ó $a = -1, b = 1$, de donde se sigue que

$$\mathcal{O}_K{}^* = \left\{\pm 1, \pm\left(\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right), \pm\left(\frac{1}{2} - \frac{1}{2}\sqrt{-3}\right)\right\}.$$

Finalmente si $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3} = e^{2\pi i/3}$ se concluye que $\mathcal{O}_K{}^* = \{\pm 1, \pm\omega, \pm\omega^2\}$.

Si $d < -3$, entonces la igualdad $(2a+b)^2 - db^2 = 4$ sólo puede ocurrir si $a = \pm 1, b = 0$. Por lo tanto $\mathcal{O}_K{}^* = \{\pm 1\}$.

□

Cuando trabajamos con campos cuadráticos reales ($d > 0$), la situación se complica. Para ilustrar lo anterior tenemos los siguientes :

Lema 2.4 *El anillo de enteros de $\mathbb{Q}(\sqrt{2})$ no tiene unidades entre 1 y $1+\sqrt{2}$.*

Demostración : Si $\alpha = a + b\sqrt{2}$, $a, b \in \mathbb{Z}$ es una unidad en $\mathcal{O}_K$, esto es que $a^2 - 2b^2 = \pm 1$. Supongamos que $1 < \alpha < 1+\sqrt{2}$. Como $a - b\sqrt{2} = \frac{\pm 1}{a+b\sqrt{2}}$, entonces $-1 < a - b < 1$. Sumando las dos desigualdades se tiene que $0 < 2a < 2+\sqrt{2}$. Como $a \in \mathbb{Z}$, $a = 1$. Pero entonces $1 < 1 + b\sqrt{2} = \alpha < 1+\sqrt{2}$, lo cual es imposible para cualquier entero b.

□

Observemos que una solución de $a^2 - 2b^2 = \pm 1$ es $a = 1 = b$. Por lo tanto $\beta = 1+\sqrt{2}$ es una unidad.

Teorema 2.5 *El anillo de enteros de $\mathbb{Q}(\sqrt{2})$ tiene un número infinito unidades, las cuales están dadas por $\pm\beta^n$, $m \in \mathbb{Z}$.*

Demostración : Sea $\alpha \in \mathcal{O}_K{}^*$. Como $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, entonces α es un número real positivo o negativo.

Supongamos que $\alpha > 0$. Como $\beta = 1+\sqrt{2} > 1$ se puede encontrar un entero n tal que $\beta^n \leq \alpha < \beta^{n+1}$. Si $\beta^n < \alpha < \beta^{n+1}$, entonces $1 < \alpha\beta^{-n} < 1+\sqrt{2}$. Pero

$$N_K(\alpha\beta^{-n}) = \frac{N_K(\alpha)}{N_K(\beta)^n} = \pm 1 \,,$$

ya que α y β son unidades. Entonces $\alpha\beta^{-n}$ es unidad entre 1 y $1+\sqrt{2}$, contrario al lema 2.4 . Por lo tanto la única alternativa es que $\alpha = \beta^n$. Finalmente el teorema se sigue ya que α^{-1} y $-\alpha$ son unidades también.

□

El caso general de calcular las unidades del anillo de enteros $\mathcal{O}_K$ de cualquier campo de números $\mathbf{K}$ se pospone hasta el capítulo 5.

Definición 2.6 *Si $\mathbf{R}$ es un anilla, y $a \in \mathbf{R}$ no unidad, diremos que a es irreducible si este no tiene factores propios. Equivalentemente a es irreducible si siempre que $a = bc$, entonces b ó c es una unidad.*

Proposición 2.7 *Para un dominio entero* **D** *se cumple :*
(a) x *es una unidad si y sólo si* $x|1$
(b) *Cualesquiera dos unidades son asociados y cualquier asociado de una unidad es una unidad.*
(c) x, y *son asociados si y sólo si* $x|y$, $y|x$
(d) x *es irreducible si y sólo si cualquier divisor de* x *es un asociado de* x *o una unidad.*
(e) *Un asociado de un irreducible es irreducible.*

Demostración : Es trivial usando las definiciones de unidad, asociados e irreducibles, y de la proposición 2.2.

□

Proposición 2.8 *Sea* **D** *un dominio entero,* x, y *elementos no nulos de* **D**, *entonces*

(a) $x|y \Leftrightarrow \langle x \rangle \supseteq \langle y \rangle$
(b) x, y *son asociados* $\Leftrightarrow \langle x \rangle = \langle y \rangle$
(c) x *es una unidad* $\Leftrightarrow \langle x \rangle = \mathbf{D}$
(d) x *es irreducible* $\Leftrightarrow \langle x \rangle$ *es máximal entre los ideales principales propios de* **D**.

Demostración : Los incisos (a),(b) y (c) se demuestran fácilmente usando las definiciones de divisibilidad y asociados en combinación con la proposición 2.7.
(d) Si x es irreducible. Sea $\mathcal{J} = \langle z \rangle (z \in \mathbf{D})$ tal que $\langle x \rangle \subseteq \mathcal{J} \subseteq \mathbf{D}$, entonces hay que probar que $\langle x \rangle = \mathcal{J}$ ó $\mathbf{D} = \mathcal{J}$. Si $\langle x \rangle \neq \langle z \rangle = \mathcal{J}$, entonces según los incisos (b) y (a), z no es un asociado de x y $z|x$, pero como x es irreducible, lo anterior sólo puede ocurrir si z es una unidad y de aquí que $\mathbf{D} = \mathcal{J}$. Recíprocamente si $y|x$ por el inciso (a) tenemos que $\langle x \rangle \subseteq \langle y \rangle \subseteq \mathbf{D}$, pero como $\langle x \rangle$ es máximal entre los ideales principales, entonces $\langle x \rangle = \langle y \rangle$ ó $\langle y \rangle = \mathbf{D}$ de donde se concluye que y es asociado de x ó y es una unidad, y por lo tanto por la proposición 2.7 (d) x es irreducible.

□

2.2 Factorización en irreducibles

Definición 2.9 *En un dominio entero* **D** *se dice que es posible la factorización en irreducibles si para cada* x *en* **D** *no cero ni unidad,* x *se puede expresar como un producto de un número finito de irreducibles.*

Observación: No en cualquier dominio entero es posible la factorización en irreducibles. Por ejemplo en el anillo **B** de todos los enteros algebraicos ni siquiera hay elementos irreducibles pues, si $\alpha \in \mathbf{B}$ no es cero ni una unidad, y si $p(x) \in \mathbb{Z}[x]$ es un polinomio mónico tal que $p(\alpha) = 0$, entonces $\sqrt{\alpha}$ es raíz de $p(x^2)$ el cual tiene coeficientes enteros y es monico, es decir que $\sqrt{\alpha} \in \mathbf{B}$. Con todo lo anterior tenemos que

$$\alpha = \sqrt{\alpha}\sqrt{\alpha} \qquad ; \alpha \text{ es reducible}$$

Por lo tanto en **B** es imposible la factorización en irreducibles.

Afortunadamente en el anillo $\mathcal{O}_{\mathbf{K}}$ de enteros de un campo de números **K**, la factorización es siempre posible como se verá más adelante.

Proposición 2.10 *Sea $\mathcal{O}_{\mathbf{K}}$ el anillo de enteros de un campo de números* **K** *(de grado n) $x, y \in \mathcal{O}_{\mathbf{K}}$, entonces*

(a) *x es una unidad en $\mathcal{O}_{\mathbf{K}}$ si y sólo si $N_K(x) = \pm 1$.*
(b) *Si x, y son asociados, entonces $N_K(x) = \pm N_K(y)$.*
(c) *Si $N_K(x)$ es un primo racional, entonces x es irreducible en $\mathcal{O}_{\mathbf{K}}$.*

Demostración : (a) Si x es una unidad, existe $y \in \mathcal{O}_{\mathbf{K}}$ tal que $xy = 1$. Tomando normas $N_K(x)N_K(y) = 1 \quad , N(x)_K, N_K(y) \in \mathbf{Z}$, de donde concluimos que $N_K(x) = \pm 1$. Recíprocamente si $N_K(x) = \pm 1$, entonces

$$N_K(x) = \sigma_1(x)\sigma_2(x)\cdots\sigma_n(x) = \pm 1$$

en donde $\sigma_i \quad (i = 1, 2, \ldots, n)$ son los monomorfismos definidos en el capítulo 1. De los anteriores monomorfismos uno de ellos es la identidad, digamos que $\sigma_1(x) = x$, entonces

$$x\sigma_2(x)\sigma_3(x)\cdots\sigma_n(x) = \pm 1 \ .$$

Ahora, como los $\sigma_i(x)$ son las raíces del polinomio minímo de x, y x es un entero, entonces $\sigma_i(x) \in \mathbf{B}$ (**B** es el anillo de todos los enteros algebraicos).

Si hacemos $\pm y = \sigma_2(x)\sigma_3(x)\cdots\sigma_n(x) \in \mathbf{B}$, entonces se tiene que $xy = 1$ y de aquí que $y \in \mathbf{K}$.

Resumiendo, tenemos que $xy = 1$ en donde $y \in \mathbf{K} \cap \mathbf{B} = \mathcal{O}_{\mathbf{K}}$. Por lo tanto x es una unidad.

(b) Si $x = uy$, u una unidad, entonces $N_K(x) = N_K(u)N_K(y)$ y por el inciso (a) se concluye que $N_K(x) = \pm N_K(y)$

(c) Si $x = yz$, $y, z \in \mathcal{O}_{\mathbf{K}}$. Tomando normas $N_K(x) = N_K(y)N_K(z) = p$, (p un primo racional), entonces $N_K(y) = \pm p, N_K(y) = \pm 1$ ó $N_K(y) = \pm 1, N_K(z) = \pm p$ esto es que y ó z es una unidad. Por lo tanto x es irreducible.

□

El recíproco de (c) de la proposición 2.10, generalmente es falso. Por ejemplo en $\mathbb{Q}(\sqrt{-6})$, el número 2 es irreducible, y sin embargo $N_K(2) = 4$ como veremos en la siguiente sección.

Para probar que en el anillo de enteros $\mathcal{O}_{\mathbf{K}}$ de cualquier campo de números **K** es posible la factorización en irreducibles necesitamos introducir la siguiente:

Definición 2.11 *Si* **D** *es un dominio entero, se dice que* **D** *es noetheriano si cualquier ideal en* **D** *es finitamente generado.*

Dos propiedades que como veremos son equivalentes a la condición de ser noetheriano son

La condición de la cadena ascendente
Dada una cadena ascendente de ideales

$$\mathcal{I}_0 \subseteq \mathcal{I}_1 \subseteq \cdots \subseteq \mathcal{I}_n \subseteq \cdots$$

entonces existe algún N para el cual $\mathcal{I}_n = \mathcal{I}_N \quad \forall n \geq N$. Esto es que cualquier cadena ascendente se estaciona.

La condición máximal
Cualquier conjunto no vacío de ideales tiene un elemento máximal. Esto es, un ideal el cual no está contenido propiamente en cualquier otro ideal.

Proposición 2.12 *Las siguientes condiciones son equivalentes para un dominio entero* **D** *:*

(a) **D** *es noetheriano.*
(b) **D** *satisface la condición de la cadena ascendente.*
(c) **D** *satisface la condición máximal.*

Lo que nos afirma esta proposición es un resultado muy conocido que se demuestra en muchos libros de álgebra. Los detalles de la demostración también se pueden ver en [9] .

Teorema 2.13 *Si un dominio entero* **D** *es noetheriano, entonces en* **D** *es posible la factorización en irreducibles.*

Demostración : Supongamos que $\mathbf{D}$ es noetheriano, pero que existe un $0 \neq x \in \mathbf{D}$ no unidad que no puede ser expresado como un producto de un número finito de irreducibles. Sea X el conjunto de todos los elementos $d \in \mathbf{D}$ no cero y no unidades que no se pueden factorizar como un producto finito de irreducibles y sea

$$S = \{\langle d \rangle \ : \ d \in X\} \ .$$

Por la suposición $X \neq \emptyset$, y por lo tanto también $S \neq \emptyset$. Sea $\langle y \rangle$ un elemento máximal de S, lo cual es posible pues $\mathbf{D}$ es noetheriano y S es un conjunto no vacio de ideales de $\mathbf{D}$. Por definición $y \in X$ es reducible, por lo tanto $y = zw$ en donde $z, w \in \mathbf{D}$ no son unidades, entonces por la proposición 2.8 (a) se tiene que $\langle y \rangle \subseteq \langle z \rangle$. Más aún, $\langle y \rangle \subset \langle z \rangle$ pues y, z no son asociados. Similarmente $\langle y \rangle \subset \langle w \rangle$. Por la maximalidad de $\langle y \rangle$, se debe tener que

$$\begin{aligned} z &= p_1 \cdots p_r \\ w &= q_1 \cdots q_s \end{aligned}$$

donde los $p_i, q_j \quad (1 \leq i \leq r \ ; \ 1 \leq j \leq s)$, son irreducibles. Multiplicando estas dos últimas igualdades se tiene que

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

esto es que y es un producto de elementos irreducibles, lo cual es una contradicción. Por lo tanto la suposición de que existe un $0 \neq x \in \mathbf{D}$ no unidad el cual no se puede expresar como un producto finito de irreducibles es falsa. Por lo tanto la factorización en irreducibles es siempre posible en $\mathbf{D}$.

□

Pasemos ahora a demostrar que $\mathcal{O}_\mathbf{K}$ es noetheriano.

Teorema 2.14 *El anillo de enteros $\mathcal{O}_\mathbf{K}$ de un campo de números $\mathbf{K}$ es noetheriano.*

Demostración : Por el teorema 1.25 $(\mathcal{O}_\mathbf{K}, +)$ es un grupo abeliano libre de rango n (n es el grado de la extensión $\mathbf{K}$). Ahora como cualquier ideal $\mathcal{I}$ en $\mathcal{O}_\mathbf{K}$ es un subgrupo aditivo de $\mathcal{O}_\mathbf{K}$, entonces $(\mathcal{I}, +)$ es abeliano libre de rango $s \leq n$. Si $\{x_1, \ldots, x_s\}$ es una $\mathbb{Z}$-base de $(\mathcal{I}, +)$, entonces claramente $\mathcal{I} = \langle x_1, \ldots, x_s \rangle$. Por lo tanto $\mathcal{I}$ es finitamente generado y $\mathcal{O}_\mathbf{K}$ es noetheriano.

□

Corolario 2.15 *La factorización en irreducibles es posible en $\mathcal{O}_\mathbf{K}$.*

□

2.3 Ejemplos donde se dá la factorización en irreducibles pero no es única

Definición 2.16 *Si* **D** *es un dominio entero en donde es posible la factorización en irreducibles, se dice que esta es única si siempre que*

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

donde cada p_i, q_j *es irreducible en* **D**, *se tiene que*

(a) $r = s$,

y

(b) *existe una permutación* π *de* $\{1, 2, \ldots, r\}$ *tal que* p_i *y* $q_{\pi(i)}$ *son asociados* $\forall i = 1, \ldots, r$.

Aunque la factorización en irreducibles siempre es posible en el anillo de enteros $\mathcal{O}_K$ de cualquier campo de números **K**, esta factorización no siempre es única, desafortunadamente. Para mostrar esto tenemos el siguiente :

Teorema 2.17 *La factorización en irreducibles no es única en el anillo de enteros de* $\mathbb{Q}(\sqrt{d})$ *para (al menos) los siguientes valores de d:* -5,-6,-10, -13,-14,-15,-17,-21,-22,-23,-26,-29,-30 .

Demostración :

- Para $d = -6 \not\equiv 1 \pmod 4$.

El anillo de enteros de $\mathbb{Q}(\sqrt{-6})$ es: $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ y una base entera es $\{1, \sqrt{-6}\}$. Por lo tanto si $\alpha \in \mathcal{O}_K$, entonces $\alpha = a + b\sqrt{-6}$ $(a, b \in \mathbb{Z})$ y

$$N_K(\alpha) = a^2 + 6b^2 \tag{2.1}$$

Para checar que en $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ no se dá la factorización única en irreduciles trabajemos con el número $6 \in \mathcal{O}_K$ el cual se puede factorizar en $\mathcal{O}_K$ como

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

Afirmación: $2, 3, \sqrt{-6}$ y $-\sqrt{-6}$ son irreducibles y ningún factor de la primer factorización es asociado de alguno de los de la segunda. En efecto, según la igualdad 2.1, $N_K(2) = 4$,$N_K(3) = 9$ y $N_K(\pm\sqrt{-6}) = 6$, y como $4 \neq \pm 6$ y $9 \neq \pm 6$ tenemos probada ya la segunda parte de lo afirmado (ver proposición 2.10 (b)).

Por otro lado si $2, 3, \sqrt{-6}$ fuesen reducibles, es decir de la forma $\alpha\beta$ en donde α, β no son unidades y como la norma es multiplicativa, entonces tendríamos que $N_K(\alpha)N_K(\beta) = 4, 6$ ó 9 $(N_K(\alpha), N_K(\beta) \in \mathbb{Z})$ y de aquí que en $\mathcal{O}_K$

existirían elementos cuya norma es ± 2 ó ± 3. Pero por la igualdad 2.1 se tendría que existen enteros racionales a, b tales que

$$a^2 + 6b^2 = \pm 2 \text{ ó } \pm 3$$

Lo cual es imposible pues para $| b | \geq 1$, $a^2 + 6b^2 \geq 6$ y así b sólo podría admitir quizás el valor de cero. Pero si $b = 0$, entonces tendríamos que $a^2 = \pm 2$ ó ± 3 lo cual es imposible en $\mathbb{Z}$.

Por lo tanto $2, 3, \pm\sqrt{-6}$ son irreducibles y concluimos finalmente que en $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ no se dá la factorización única.

- Para $d = -23 \equiv 1 \pmod 4$.

El anillo de enteros de $\mathbb{Q}(\sqrt{-23})$ es

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{-23}\right]$$

y una base entera es

$$\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{-23}\right\}.$$

Si $\alpha \in \mathcal{O}_K$, $\alpha = a + b(1/2 + \sqrt{-23}/2)$ $(a, b \in \mathbb{Z})$ y

$$N_K(\alpha) = \left(\frac{2a+b}{2}\right)^2 + 23\left(\frac{b}{2}\right)^2 . \qquad (2.2)$$

Para checar que en $\mathcal{O}_K$ no se dá la factorización única en irreducibles trabajemos con el número $6 \in \mathcal{O}_K$ el cual se puede factorizar en $\mathcal{O}_K$ como

$$6 = 2 \cdot 3 = \left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right).$$

Afirmación:

$$2, 3, \left(\frac{1 \pm \sqrt{-23}}{2}\right) \quad \text{son irreducibles}$$

y ningún factor de la primera factorización es asociado de alguno de los de la segunda. En efecto ya que según la igualdad 2.2, $N_K(2) = 4$, $N_K(3) = 9$ y $N_K(\frac{1}{2} \pm \frac{1}{2}\sqrt{-23}) = 6$ y como $4 \neq \pm 6$ y $9 \neq \pm 6$ tenemos probada ya la segunda parte de lo afirmado.

Por otro lado si $2, 3, \frac{1}{2} \pm \frac{1}{2}\sqrt{-23}$ fuesen reducibles, entonces en $\mathcal{O}_K$ existirían elementos de norma ± 2 ó ± 3. Pero por la igualdad 2.2 se tendría que existen enteros racionales a, b tales que

$$\frac{(2a+b)^2 + 23b^2}{4} = \pm 2 \, , \, \pm 3$$

equivalentemente

$$(2a+b)^2+23b^2=\pm 8,\pm 12\ .$$

Lo cual es imposible pues para $\mid b \mid \geq 1$, $(2a+b)^2+23b^2 \geq 23$, y así b sólo podría admitir quizás el valor de cero. Pero si $b=0$, entonces tendríamos que $4a^2=\pm 8$ ó ± 12 equivalentemente tendríamos que $a^2=\pm 2$ ó ± 12 lo cual es imposible en $\mathbb{Z}$.

Para los demás valores de d se procede de igual manera apoyándonos en las siguientes factorizaciones.

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

□

Cuando trabajamos con campos cuadráticos reales ($d>0$) la cosa se complica bastante como se puede puede apreciar en el siguiente :

Teorema 2.18 *La factorización en irreducibles no es única en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ para (al menos) los siguientes valores de d:* 10,15,26,30.

Demostración :

- Para $d=10 \not\equiv 1 \pmod 4$.

El anillo de enteros de $\mathbb{Q}(\sqrt{10})$ es: $\mathcal{O}_K=\mathbb{Z}[\sqrt{10}]$ y $\{1,\sqrt{10}\}$ es una base entera. Por lo tanto, si $\alpha \in \mathcal{O}_K$, $\alpha=a+b\sqrt{10}$ $(a,b\in\mathbb{Z})$ y

$$N_K(\alpha)=a^2-10b^2 \qquad (2.3)$$

Para ver que en $\mathcal{O}_K=\mathbb{Z}[\sqrt{10}]$ no se dá la factorización única en irreducibles trabajemos con el número $6\in\mathcal{O}_K$ el cual se puede factorizar en $\mathcal{O}_K$ como

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

Ahora, por la igualdad 2.3 tenemos que

$$N_K(2) = 4$$
$$N_K(3) = 9$$
$$N_K(4 \pm \sqrt{10}) = 6$$

y como $4 \neq \pm 6$ y $9 \neq \pm 6$, entonces 2,3 no son asociados de ninguno de los elementos $4 \pm \sqrt{10}$.

Observemos ahora que en $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ no hay elementos cuya norma sea ± 2 ó ± 3. En efecto ya que si los hubiera, entonces por la igualdad 2.3 se tendría que

$$a^2 - 10b^2 = \pm 2 \text{ ó } \pm 3 \quad (a, b \in \mathbb{Z}), \tag{2.4}$$

notemos que en la ecuación 2.4, b podrín tomar bastantes valores, gracias a la presencia del signo menos, por lo cual la ecuación es un poco inaccesible en su resolución. Sin embargo démosle la vuelta al problema. Si existiesen $a, b \in \mathbb{Z}$ tales que 2.4 fuese cierta, entonces reduciendo dicha ecuación módulo 10 tendríamos que existe $a \in \mathbb{Z}$ tal que

$$a^2 \equiv \pm 2 \text{ ó } \pm 3 \pmod{10}$$

equivalentemente

$$a^2 \equiv 2, 3, 7 \text{ ó } 8 \pmod{10}$$

lo cual es imposible pues no existe ningun entero cuyo cuadrado se congruente con 2,3,7 ó 8 módulo 10.

Lo anterior nos dice claramente que $2, 3, 4 \pm \sqrt{10}$ son irreducibles, y por lo tanto en $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ no se dá la factorización única.

Algo similar se hace para los demás valores de d apoyándonos en las siguientes factorizaciones

$$\begin{aligned}
\mathbb{Q}(\sqrt{15}): \quad 10 &= 2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15}) \\
\mathbb{Q}(\sqrt{26}): \quad 10 &= 2 \cdot 5 = (6 + \sqrt{26})(6 - \sqrt{26}) \\
\mathbb{Q}(\sqrt{30}): \quad 6 &= 2 \cdot 3 = (6 + \sqrt{30})(6 - \sqrt{30})
\end{aligned}$$

□

Hasta el momento sólo hemos probado que en el anillo de enteros $\mathcal{O}_K$ de un campo cuadratico $\mathbb{Q}(\sqrt{d})$, la factorización no es única para ciertos valores de d. Pero no hemos exhibido ningún anillo de enteros (distinto de $\mathbb{Z}$) en donde se dé la factorización única en irreducibles. En la sección 2.6 veremos que en el campo cuadrático $\mathbb{Q}(\sqrt{d})$, el anillo de enteros es de factorización

única para $d = -1, -2, -3, -7$ y -11. Posteriormente en el capítulo 4 se probará que el anillo de enteros de $\mathbb{Q}(\sqrt{d})(d < 0)$ es de factorización única no sólo en los valores anteriores si no también para $d = -19, -43, -67$ y -163, de hecho en 1967 Stark probó que para $d < 0$ el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ tiene factorización única en irreducibles si y sólo si $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

Para el caso $d > 0$ se sabe que el anillo de enteros es de factorización única para muchos valores de d, pero en general la cosa es mucho más complicada y es hasta el momento, un problema abierto.

2.4 Factorización primaria

Recordemos que en un anillo $\mathbf{R}$, un elemento $0 \neq x$ se dice que es un primo si no es una unidad y siempre que x divide yz en $\mathbf{R}$, entonces x divide a y ó x divide a z.

Proposición 2.19 *Un primo en un dominio entero* $\mathbf{D}$ *es siempre irreducible.*

Demostración : Si $\mathbf{D}$ es un dominio entero, $x \in \mathbf{D}$ es un primo y $x = ab$, entonces $x|ab$ y de aquí que $x|a$ ó $x|b$. Si $x|a$, entonces $a = xc$, $c \in \mathbf{D}$, que sustituyendo en la primer igualdad nos dá $x = xcb$, finalmente cancelando a x se obtiene $1 = cb$, esto es que b es una unidad. De la misma forma si $x|b$, entonces a tiene que ser una unidad. Por lo tanto x es irreducible

□

El recíproco de la proposición 2.19 no siempre es cierto ya que por ejemplo en el anillo de enteros $\mathbf{Z}[\sqrt{-5}]$ del campo de números $\mathbb{Q}(\sqrt{-5})$ se tiene que

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

en donde $2, 3$ y $1 \pm \sqrt{-5}$ son irreducibles. Claramente se tiene que $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, y sin embargo $2 \nmid (1+\sqrt{-5})$ y $2 \nmid (1-\sqrt{-5})$, ya que si $2 \mid (1+\sqrt{-5})$, entonces existirían $a, b \in \mathbf{Z}$ tales que $1+\sqrt{-5} = 2(a+b\sqrt{-5})$ lo cual es absurdo. Análogamente si $2 \mid (1-\sqrt{-5})$ se llega a una contradicción. Por lo tanto 2 es irreducible pero no primo en $\mathbf{Z}[\sqrt{-5}]$.

Recordemos que en $\mathbf{Z}[\sqrt{-5}]$ no se dá la factorización única en irreducibles y por el previo ejemplo existen elementos en $\mathbf{Z}[\sqrt{-5}]$ que son irreducibles pero no primos.

En general como se verá en el siguiente teorema, en cualquier dominio entero $\mathbf{D}$ en donde no se dá la factorización en irreducibles en forma única, se tiene que en $\mathbf{D}$ hay elementos irreducibles que no son primos.

Teorema 2.20 *En un dominio entero* **D** *en el cual es posible la factorización en irreducibles, la factorización es única si y sólo si cualquier irreducible es primo.*

Demostración : Sea **D** un dominio entero en donde es posible la factorización en irreducibles. Si $0 \neq x \in \mathbf{D}$, nos será conveniente escribir

$$x = up_1p_2 \cdots p_r \qquad (u, p_1, p_2, \ldots, p_r \in \mathbf{D})$$

donde u es una unidad y $p_1, \ldots, p_r$ son irreducibles. Cuando $r = 0$ se puede interpretar como $x = u$ y si $r \geq 1$, entonces up_1 es un irreducible y por lo tanto x es el producto de los irreducibles $up_1, p_2, \ldots, p_r$.

$\Rightarrow$) Si $p \in \mathbf{D}$ es irreducible y si $p \mid ab$ $(a, b \in \mathbf{D})$.

Casos:
i) Si alguno de a ó b es cero. Claramente $p \mid a$ ó $p \mid b$
ii) Si $a \neq 0$, $b \neq 0$, entonces por ser **D** un dominio entero, existe $0 \neq c \in \mathbf{D}$ tal que $ab = pc$. Factorizando a, b, c en irreducibles

$$\begin{aligned} a &= u_1p_1 \cdots p_n \\ b &= u_2q_1 \cdots q_m \\ c &= u_3r_1 \cdots r_s \end{aligned}$$

en donde u_1, u_2, u_3 son unidades y p_i, q_j, r_k son irreducibles , entonces

$$p(u_3r_1 \cdots r_s) = (u_1p_1 \cdots p_n)(u_2q_1 \cdots q_m)$$

y por factorización única se tiene que p es asociado de uno de los p_i ó q_j por lo cual $p \mid a$ ó $p \mid b$, de donde concluimos que p es un primo.

$\Leftarrow$) Si $0 \neq x \in \mathbf{D}$ y éste se factoriza en irreducibles de las siguientes dos maneras

$$u_1p_1 \cdots p_m = x = u_2q_1 \cdots q_n \tag{2.5}$$

donde u_1, u_2 son unidades y los p_i, q_j son irreducibles.

Tratemos de probar que $m = n$ y que existe una permutación π de $\{1, \ldots, m\}$ tal que p_i y $q_{\pi(i)}$ son asociados $(1 \leq i \leq m)$.

Esto es trivialmente cierto si $m = 0$. Si $m \geq 1$ de la igualdad 2.5 se tiene que $p_1 \mid u_2q_1 \ldots q_n$, pero como p_1 es primo, entonces $p_1 \mid u_2$ ó $p_1 \mid q_j$ para alguna $j (1 \leq j \leq n)$. La primera de las posibilidades se descarta ya que si $p_1 \mid u_2$, entonces por la proposición 2.7 p_1 sería una unidad lo cual es absurdo. Por lo tanto $p_1 \mid q_j$. Si renombramos los indices, digamos que $j = 1$, entonces

$p_1 \mid q_1$, y así $q_1 = p_1 v_1$ donde v_1 es una unidad. Sustituyendo en la igualdad 2.5 se tiene

$$u_1 p_1 \cdots p_m = u_2 p_1 v_1 q_2 \cdots q_n \ ,$$

como **D** es un dominio entero, cancelamos a p_1 y obtenemos.

$$u_1 p_2 \cdots p_m = (u_2 v_1) q_2 \cdots q_n.$$

Procediendo en forma análoga, llegamos a que

$$\begin{array}{lll} q_2 & = & p_2 v_2 \\ q_3 & = & p_3 v_3 \\ \cdots & \cdots & \cdots \end{array}$$

Si m fuera menor que n, llegaríamos finalmente a una expresión de la forma

$$u = q_{m+1} \cdots q_n \ ,$$

lo cual es imposible. Análogamente, si $m > n$. Por lo tanto $m = n$, y como $q_i = p_i v_i$ (vía un renombramiento), entonces existe una permutación π de $\{1, \ldots, m\}$ tal que p_i y $q_{\pi(i)}$ son asociados $(1 \leq i \leq m)$.

□

2.5 Dominios Euclideanos

Si **F** es un campo. **F[x]** es un ejemplo de factorización única, y también un ejemplo de dominio Euclideano el cual se define enseguida.

Definición 2.21 *Sea* **D** *un dominio entero. Una función Euclideana en* **D** *es una función* $\phi : \mathbf{D} \to \mathbf{N} \cup \{0\}$ *, tal que.*

(a) *Si* $a, b \in \mathbf{D}$ *y* $a \mid b$, *entonces* $\phi(a) \leq \phi(b)$
(b) *Si* $a, b \in \mathbf{D}$ $(b \neq 0)$, *entonces existen* $q, r \in \mathbf{D}$ *tales que*

$$a = bq + r \quad \textit{donde} \quad r = 0 \quad \acute{o} \quad \phi(r) < \phi(b)$$

Si **D** es un dominio entero y ϕ es una función Euclideana para **D**, entonces *se dice que* **D** *es un dominio Euclideano.*

Teorema 2.22 *Cualquier dominio Euclideano es un dominio de ideales principales.*

Demostración : Sea **D** un dominio Euclideano e $\mathcal{I}$ un ideal de **D**. Claramente si $\mathcal{I} = \{0\}, \mathcal{I}$ es principal. Supongamos que $\mathcal{I} \neq \{0\}$, entonces por el principio del buen orden podemos elegir $0 \neq x \in \mathcal{I}$ tal que $\phi(x)$ sea mínimo. Ahora, si $y \in \mathcal{I}$, por el inciso (b) de la definición de dominio Euclideano se tiene que $y = qx + r$ donde $r = 0$ ó $\phi(r) < \phi(x)$. De lo anterior se tiene que $r = y - qx \in \mathcal{I}$, y por la minimalidad de x no se puede dar que $\phi(r) < \phi(x)$, entonces $r = 0$ y por lo cual $y = qx$. Por lo tanto $\mathcal{I} = \langle x \rangle$ es principal.

□

Teorema 2.23 *Cualquier dominio de ideales principales es un dominio de factorización única.*

Demostración : Si **D** un dominio de ideales principales, entonces **D** es noetheriano, y por lo tanto la factorización en irreducibles es posible en **D** (ver el corolario 2.15). Ahora, por el teorema 2.20 sólo nos resta probar que cualquier elemento irreducible de **D** es primo. Supongamos que p es irreducible, entonces $\langle p \rangle$ es maximal entre todos los ideales principales de **D** (ver proposición 2.8 (d)). Pero como en **D** cualquier ideal es principal, entonces $\langle p \rangle$ es maximal entre todos los ideales. Ahora, como cualquier ideal maximal es primo [ver teorema A.4 del apéndice], entonces $\langle p \rangle$ es un ideal primo y por la proposición A.9 del apéndice, p es primo.

□

Los dos teoremas anteriores nos prueban el

Teorema 2.24 *Un dominio Euclideano es un dominio de factorización única.*

□

2.6 Campos cuadráticos Euclideanos

Decir si un dominio entero **D** es o no un dominio Euclideano no es nada fácil.

Enseguida trabajaremos con dominios muy particulares, a saber con el anillo de enteros $\mathcal{O}_K$ de un campo de números cuadrático $\mathbb{Q}(\sqrt{d})$ en donde d es un entero racional libre de cuadrados.

Teorema 2.25 *El anillo de enteros* $\mathcal{O}_K$ *de* $\mathbb{Q}(\sqrt{d})$ *es Euclideano para* d= -1,-2,-3,-7 ,-11 , *con función Euclideana*

$$\phi(\alpha) = |\, N_K(\alpha) \,|$$

Demostración : Claramente $\phi : \mathcal{O}_K \to \mathbb{N} \cup \{0\}$ es una función, entonces sólo hace falta checar que si $\alpha, \beta \in \mathcal{O}_K$, ϕ satisface las condiciones de una función Euclideana.

(a) Si $\alpha \mid \beta$, entonces $\beta = \alpha\gamma$, $\gamma \in \mathcal{O}_K$. Aplicando ϕ se tiene

$$\mid N_K(\beta) \mid \;=\; \mid N_K(\alpha\gamma) \mid \;=\; \mid N_K(\alpha)N_K(\gamma) \mid \;=\; \mid N_K(\alpha) \mid\mid N_K(\gamma) \mid$$

pero como $\mid N_K(\gamma) \mid \geq 1$, entonces $\mid N_K(\alpha) \mid \leq \mid N_K(\beta) \mid$. Por lo tanto $\phi(\alpha) \leq \phi(\beta)$.

La condición (b) de la definición 2.21 es equivalente a:
(c) Para cualquier $\varepsilon \in \mathbb{Q}(\sqrt{d})$ existe $\kappa \in \mathcal{O}_K$ tal que

$$\mid N_K(\varepsilon - \kappa) \mid < 1$$

En efecto, (b) $\Rightarrow$ (c) Supongamos que (b) es cierto. Si $\varepsilon \in \mathbb{Q}(\sqrt{d})$; por el lema 1.18 existe $0 \neq c \in \mathbb{Z}$ tal que $c\varepsilon \in \mathcal{O}_K$. Si hacemos $\alpha = c\varepsilon, \beta = c$, entonces existen $\gamma, \delta \in \mathcal{O}_K$ tales que

$$c\varepsilon = c\gamma + \delta \quad ; \quad \delta = 0 \quad \text{ó} \quad \mid N_K(\delta) \mid < \mid N_K(c) \mid \; .$$

(i) Si $\delta = 0, c\varepsilon = c\gamma$, entonces $\varepsilon = \gamma \in \mathcal{O}_K$ y se puede tomar $\kappa = \varepsilon$.
(ii) Si $\mid N_K(\delta) \mid < \mid N_K(c) \mid$, como $c \neq 0$, entonces

$$\mid N_K(\delta/c) \mid < 1$$

lo cual es lo mismo que

$$\mid N_K(\varepsilon - \gamma) \mid < 1 \; .$$

Por lo tanto podemos tomar $\kappa = \gamma \in \mathcal{O}_K$. Con lo cual se concluye que (b) implica (c).

(c) $\Rightarrow$ (b) Sean $\alpha, \beta \in \mathcal{O}_K, \beta \neq 0$. Hagamos $\varepsilon = \alpha/\beta$, entonces existe $\kappa = \gamma \in \mathcal{O}_K$ tal que

$$\begin{aligned} \mid N_K(\alpha/\beta - \gamma) \mid < 1 \;\; &\Rightarrow \;\; \mid N_K(\tfrac{\alpha - \beta\gamma}{\beta}) \mid < 1 \\ &\Rightarrow \;\; \mid N_K(\alpha - \beta\gamma) \mid \; < \mid N_K(\beta) \mid \end{aligned}$$

claramente (b) se sigue si hacemos $\delta = \alpha - \beta\gamma$.
Probemos entonces que la condición (c) se satisface.

Sea $\varepsilon = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Si $d \not\equiv 1 \pmod 4$ $(d = -1, -2)$ se tiene que encontrar

$$\kappa = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \quad \text{tal que}$$

$$\mid N_K(\varepsilon - \kappa) \mid = \mid (r - x)^2 - d(s - y)^2 \mid < 1$$

para tal efecto tomemos $x, y \in \mathbb{Z}$ tales que $| r - x |, | s - y | \leq 1/2$ (lo cual es siempre posible ya que r, s son racionales y cualquier racional siempre está entre dos enteros), entonces

$$| (r-x)^2 - d(s-y)^2 | \leq | (\frac{1}{2})^2 + 2(\frac{1}{2})^2 | = \frac{3}{4} < 1 .$$

Si $d \equiv 1 \pmod 4$ $(d = -3, -7, -11)$ se tiene que encontrar

$$\kappa = x + y\left(\tfrac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\tfrac{1+\sqrt{d}}{2}\right] ,$$

tal que

$$| N_K(\varepsilon - \kappa) | = | (r - x - \tfrac{1}{2}y)^2 - d(s - \tfrac{1}{2}y)^2 | < 1$$

lo cual es lo mismo que

$$| (2r - 2x - y)^2 - d(2s - y)^2 | < 4 .$$

Para tal efecto tomemos $y \in \mathbb{Z}$ tal que $| 2s - y | \leq 1/2$, con esto podemos encontrar $x \in \mathbb{Z}$ tal que $| 2r - 2x - y | \leq 1$, porque entonces

$$| (2r - 2x - y)^2 - d(2s - y)^2 | \leq | 1^2 + 11(1/2)^2 | = \frac{15}{4} < 4$$

con lo cual queda probado el teorema.

□

Teorema 2.26 *Si d=-5,-6,-10 ó $d < -11$, entonces el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ no es Euclideano.*

Demostración : Sea $\mathcal{O}_K$ el anillo de enteros de $\mathbb{Q}(\sqrt{d})$. Supongamos que existe $\phi : \mathcal{O}_K \to \mathbb{N} \cup \{0\}$ función Euclideana. Elíjase $\beta \in \mathcal{O}_K$ no cero ni unidad tal que $\phi(\beta)$ es mínimo (esto es posible por el principio del buen orden en $\mathbb{N} \cup \{0\}$). Ahora, si tomamos $\alpha \in \mathcal{O}_K$, como ϕ es Euclideana existen $\gamma, \delta \in \mathcal{O}_K$ tales que

$$\alpha = \beta\gamma + \delta \quad \text{donde} \quad \delta = 0 \ \text{ó} \ \phi(\delta) < \phi(\beta),$$

pero por la elección de β, lo anterior implica que $\delta = 0$ ó δ es una unidad. Pero por la proposición 2.3 las unidades del anillo de enteros $\mathcal{O}_K$ para los valores de d del presente teorema son ± 1. Por lo tanto

$$\alpha = \beta\gamma \ , \ \alpha = \beta\gamma - 1 \ \text{ó} \ \alpha = \beta\gamma + 1$$

lo cual implica que $| \mathcal{O}_K/(\beta) | \leq 3$.

Casos:

(i) Si $d \not\equiv 1 \pmod 4$. Se sabe por el teorema 1.32 que una $\mathbb{Z}$-base de $\mathcal{O}_K$ es $\{1, \sqrt{d}\}$, de donde se puede verificar fácilmente que $\{\beta, \beta\sqrt{d}\}$ es una $\mathbb{Z}$-base de $\langle\beta\rangle$. Si $\beta = a + b\sqrt{d}$ $(a, b \in \mathbb{Z})$ la $\mathbb{Z}$-base para $\langle\beta\rangle$ es

$$\{a + b\sqrt{d}, db + a\sqrt{d}\} ,$$

entonces por el teorema A.28 del apéndice se tiene que

$$| \mathcal{O}_K/\langle\beta\rangle | = \left|\det \begin{pmatrix} a & b \\ bd & a \end{pmatrix}\right| = | a^2 - db^2 | = | N_K(\beta) | \leq 3 ,$$

pero para $d = -5, -6, -10$ y para $d < -11$ las únicas soluciones a la anterior desigualdad son $a = \pm 1, b = 0$. Por lo tanto

$$| N_K(\beta) | = 1 \Rightarrow N_K(\beta) = \pm 1 ,$$

esto es, que β es una unidad lo cual contradice la elección de β.

(ii) Si $d \equiv 1 \pmod 4$. Se sabe por el teorema 1.32 que una $\mathbb{Z}$-base de $\mathcal{O}_K$ es $\{1, (1+\sqrt{d})/2\}$, de donde se puede verificar fácilmente que $\{\beta, (\beta+\beta\sqrt{d})/2\}$ es una $\mathbb{Z}$-base de $\langle\beta\rangle$. Si $\beta = a+b(1/2+\sqrt{d}/2)$ $(a, b \in \mathbb{Z})$ la $\mathbb{Z}$-base para $\langle\beta\rangle$ es

$$\left\{a + b\left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right), \frac{bd}{4} - \frac{b}{4} + (a + b)\left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right)\right\} ,$$

entonces por el teorema A.28 del apéndice se tiene que

$$| \mathcal{O}_K/\langle\beta\rangle | = \left|\det \begin{pmatrix} a & b \\ \frac{bd}{4} - \frac{b}{4} & a + b \end{pmatrix}\right| = \left|\frac{(2a + b)^2}{4} - \frac{b^2 d}{4}\right|$$
$$= | N_K(\beta) | \leq 3$$

equivalentemente

$$| (2a + b)^2 - b^2 d | \leq 12$$

pero para $d < -11$ las únicas soluciones a la anterior desigualdad son $a = \pm 1, b = 0$. Por lo tanto al igual que en el inciso (i), β es una unidad lo cual contradice la elección de β.

Por lo tanto la suposición de que ϕ es una función Euclidea es falsa, con lo cual queda probado el teorema.

□

Los dos teoremas anteriores nos prueban que para d negativa y libre de cuadrados el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es Euclideano si y sólo si $d = -1, -2, -3, -7, -11$.

Si $\mathbf{K}$ es un campo de números, y $\mathcal{O}_{\mathbf{K}}$ (el anillo de enteros de $\mathbf{K}$) es Euclideano con función Euclidea el valor absoluto de la norma. Por brevedad diremos que $\mathbf{K}$ es un campo *norma-Euclideo*.

La determinación de los campos cuadráticos norma-Euclideos no es nada fácil con d positivo. Sin embargo se sabe que Chatland y Davenport en 1950, e Inkeri en 1949 probaron independientemente el siguiente teorema del cual no daremos la prueba.

Teorema 2.27 *El anillo de enteros de $\mathbb{Q}(\sqrt{d})$, para d positivo, es norma-Euclideo si y sólo si* d= 2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73.

□

Para ilustrar las complicaciones que se tienen al trabajar con d positiva probaremos un resultado parcial en la misma dirección del teorema 2.27.

Teorema 2.28 *El anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es norma-Euclideo para* d= 2,3,5,6,7,13,17,21,29.

Demostración : Procediendo igual que en el teorema 2.25. Si $\varepsilon = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, y trabajando simultaneamente con las dos posibilidades para $d \pmod 4$, si escribimos

$$\begin{array}{lll} \lambda = 0 & , & E = d \quad \left(d \not\equiv 1 \pmod 4\right) \\ \lambda = \frac{1}{2} & , & E = \frac{d}{4} \quad \left(d \equiv 1 \pmod 4\right). \end{array}$$

Entonces tenemos que probar que siempre existen $x, y \in \mathbf{Z}$ tales que

$$| (r - x - \lambda y)^2 - E(s - y)^2 | < 1 \tag{2.6}$$

Supongamos que $\mathbb{Q}(\sqrt{d})$ no es norma-Euclideano, entonces la desigualdad 2.6 es falsa para algunos $r, s \in \mathbb{Q}$ y para todo $x, y \in \mathbf{Z}$, esto es, que existen $r, s \in \mathbb{Q}$ tales que

$$| (r - x - \lambda y)^2 - E(s - y)^2 | \geq 1 \qquad \forall x, y \in \mathbf{Z}. \tag{2.7}$$

Afirmación: r, s se pueden tomar de tal manera que $0 \leq r, s \leq 1/2$. En efecto, ya que :

Si $d \not\equiv 1 \pmod 4$, podemos escribir $r = r_1 + m \quad (m \in \mathbb{Z}, r_1 \in \mathbb{Q}, 0 \leq r_1 < 1)$. Por lo tanto:

(i) Si $0 \leq r_1 \leq 1/2$. Claramente $r_1 = r - m, x - m, s, y$ satisfacen la desigualdad 2.7.

(ii) Si $1/2 < r_1 < 1$; $0 < 1 - r_1 = r_2 < 1/2$. Claramente

$$r_2 = 1 - r_1 = m - r + 1\ ,\ -x + m + 1\ ,\ s\ ,\ y\quad ,$$

satisfacen la desigualdad 2.7.

Por lo tanto se puede tomar $0 \leq r \leq 1/2$. Procediendo en forma análoga también se puede tomar $0 \leq s \leq 1/2$.

Si $d \equiv 1 \pmod 4$, procediendo como antes se pueden tomar r, x, s, y $(0 \leq r \leq 1/2)$ que satisfagan la desigualdad 2.7.

Ahora, si remplazamos

$$r \quad x \quad s \quad y$$

respectivamente por

$$\begin{array}{cccc} r & x - v & s + 2v & y + 2v \\ r & x + y & -s & -y \\ \frac{1}{2} - r & -x & 1 - s & 1 - y \end{array}$$

en donde $v \in \mathbb{Z}$, claramente los tres cuartetos anteriores satisfacen la desigualdad 2.7. El primero de ellos se usa para hacer $-1 \leq s \leq 1$; el segundo es necesario para hacer $0 \leq s \leq 1$. Si $s \leq 1/2$ terminamos; si no se usa el tercer cuarteto para hacer finalmente $0 \leq s \leq 1/2$.

Si $0 \leq r, s \leq 1/2$. Como estamos suponiendo que la desigualdad 2.7 es verdadera, entonces para toda $x, y \in \mathbb{Z}$ al menos una de las desigualdades

$$P(x,y): \qquad (r - x - \lambda y)^2 \geq 1 + E(s - y)^2, \qquad (2.8)$$

$$Q(x,y): \qquad E(s - y)^2 \geq 1 + (r - x - \lambda y)^2, \qquad (2.9)$$

es verdadera. Enseguida llegaremos a una contradicción trabajando con tres pares de desigualdades dando valores a x, y en 2.8 y en 2.9.

$$\begin{array}{llll} P(0,0): & r^2 \geq 1 + Es^2 & Q(0,0): & Es^2 \geq 1 + r^2 \\ P(1,0): & (1 - r)^2 \geq 1 + Es^2 & Q(1,0): & Es^2 \geq 1 + (1 - r)^2 \\ P(-1,0): & (1 + r)^2 \geq 1 + Es^2 & Q(-1,0): & Es^2 \geq 1 + (1 + r)^2. \end{array}$$

Como $0 \leq r \leq \frac{1}{2}$ y $E > 0$, claramente $P(0,0)$ y $P(1,0)$ son ambas falsas, por lo tanto $Q(0,0)$ y $Q(1,0)$ son ambas verdaderas. Si $P(-1,0)$ es verdadera entonces junto con $Q(1,0)$ se tiene que

$$(1+r)^2 \geq 1 + Es^2 \geq 2 + (1-r)^2 ,$$

de donde $r \geq \frac{1}{2}$. Pero por la forma en que se tomó r, entonces $r = \frac{1}{2}$ y de aquí que $Es^2 = \frac{5}{4}$. De la definición de E fácilmente se verifica que lo anterior es imposible. Por lo tanto $Q(-1,0)$ es verdadera. Entonces

$$Es^2 \geq 1 + (1+r)^2 \geq 2$$

y por lo tanto $E \geq 8$.

En resumen tenemos que $\mathbb{Q}(\sqrt{d})$ no norma-Euclideano implica $E \geq 8$. Por lo tanto si $E < 8$, entonces $\mathbb{Q}(\sqrt{d})$ es norma-Euclideano, tal como ocurre con los valores de d dados en el teorema.

□

2.7 Ideales

Aunque la factorización en irreducibles no es única en todo anillo de enteros $\mathcal{O}_{\mathbf{K}}$ de un campo de números $\mathbf{K}$, cuando trabajamos con ideales del anillo de enteros $\mathcal{O}_{\mathbf{K}}$ la factorización de ideales es única como se verá en esta sección.

En el transcurso de este capítulo como en los restantes de este trabajo, a los ideales (y los ideales fraccionales proximos a definir) de $\mathcal{O}_{\mathbf{K}}$ los denotaremos con letras caligraficas $\mathcal{A}, \mathcal{B}, \mathcal{C} \ldots$.

Recordemos que si $\mathbf{R}$ es un anillo, y x, y son elementos no nulos de $\mathbf{R}$, entonces $x|y$ si y sólo si $\langle y \rangle \subseteq \langle x \rangle$ (ver proposición 2.8 (a)). Por lo tanto, en el caso especial de que $\mathcal{A} = \langle a \rangle, \mathcal{B} = \langle b \rangle, \mathcal{C} = \langle c \rangle$, la afirmación

$$\mathcal{BC} \subseteq \mathcal{A} \text{ implica } \mathcal{B} \subseteq \mathcal{A} \text{ ó } \mathcal{C} \subseteq \mathcal{A},$$

trasladado nos dá

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

Más adelante veremos que cuando hablemos de divisibilidad entre ideales del anillo de enteros $\mathcal{O}_{\mathbf{K}}$, algo similar ocurrirá.

Teorema 2.29 *El anillo de enteros $\mathcal{O}_{\mathbf{K}}$ de un campo de números $\mathbf{K}$ tiene las siguientes propiedades.*

(a) *Este es un dominio entero con campo de cocientes $\mathbf{K}$.*
(b) *Este es noetheriano.*
(c) *Si $\alpha \in \mathbf{K}$ es raíz de un polinomio monico con coeficientes en $\mathcal{O}_{\mathbf{K}}$, entonces*

$\alpha \in \mathcal{O}_{\mathbf{K}}$.
(d) *Cualquier ideal primo no nulo de* $\mathcal{O}_{\mathbf{K}}$ *es maximal.*

Demostración : (a) Claramente $\mathcal{O}_{\mathbf{K}} \subseteq \mathbf{K}$. Ahora, si $\mathbf{F}$ es el campo de cocientes de $\mathcal{O}_{\mathbf{K}}$, entonces $\mathbf{F} \subseteq \mathbf{K}$ pues $\mathbf{F}$ es el mínimo campo que contiene a $\mathcal{O}_{\mathbf{K}}$. Por otro lado si $\alpha \in \mathbf{K}$, por el lema 1.18 existe $0 \neq c \in \mathbb{Z}$ tal que $c\alpha \in \mathcal{O}_{\mathbf{K}}$, entonces a α lo podemos reescribir como $\alpha = \frac{c\alpha}{c}$ (el cociente de dos números en $\mathcal{O}_{\mathbf{K}}$), por lo tanto $\alpha \in \mathbf{F}$ y se tiene que $\mathbf{K} \subseteq \mathbf{F}$ con lo cual se concluye finalmente que $\mathbf{K} = \mathbf{F}$.

Los incisos (*b*) y (*c*) ya se probaron en los teoremas 2.14 y 1.16 respectivamente.
(d) El corolario 1.19 nos afirma que cualquier ideal $\mathcal{I}$ no nulo de $\mathcal{O}_{\mathbf{K}}$ contiene una base de $\mathbf{K}$. Más aún si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $\mathbf{K}$ contenida en $\mathcal{I}$ tal que $\mid \Delta[\alpha_1, \ldots, \alpha_n] \mid \in \mathbb{N}$ es mínimo, entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de $\mathcal{I}$, esto es que *cualquier ideal* $\mathcal{I}$ *no nulo de* $\mathcal{O}_{\mathbf{K}}$ *es un grupo abeliano libre de rango n* (la prueba de esto último es identica a la dada en el teorema 1.25).

Con todo lo anterior tenemos que $\mid \mathcal{O}_{\mathbf{K}}/\mathcal{I} \mid$ es finito (ver teorema A.28 del apéndice) para cualquier ideal no nulo de $\mathcal{O}_{\mathbf{K}}$.

Para finalizar si $\mathcal{P}$ es un ideal primo, entonces $\mathcal{O}_{\mathbf{K}}/\mathcal{P}$ es un *dominio entero finito* y por lo tanto $\mathcal{O}_{\mathbf{K}}/\mathcal{P}$ es un campo [ver teoremas A.2 y A.4 del apéndice], de donde concluimos que $\mathcal{P}$ es maximal.

□

Un anillo que satisface las condiciones (a)-(d) del teorema 2.29 se llama un anillo de Dedekind. Aunque la factorización de ideales en un anillo de Dedekind es única en general, aquí sólo nos enfocaremos en el anillo de enteros $\mathcal{O}_{\mathbf{K}}$ de un campo de números $\mathbf{K}$.

Definiciones que serán de vital importancia para probar lo previamente dicho son.

Definición 2.30 *Si* $\mathcal{A}, \mathcal{B}$ *son ideales de* $\mathcal{O}_{\mathbf{K}}$, *se dice que* $\mathcal{A}$ *divide a* $\mathcal{B}$, *lo cual lo denotaremos por* $\mathcal{A}|\mathcal{B}$, *si existe un ideal* $\mathcal{C}$ *tal que* $\mathcal{B} = \mathcal{A}\mathcal{C}$.

Definición 2.31 *Un* $\mathcal{O}_{\mathbf{K}}$*-módulo* $\mathcal{I}$ *de* $\mathbf{K}$ *es llamado un ideal fraccional de* $\mathcal{O}_{\mathbf{K}}$ *si existe* $0 \neq \alpha \in \mathcal{O}_{\mathbf{K}}$ *tal que* $\alpha\mathcal{I} \subseteq \mathcal{O}_{\mathbf{K}}$. *En otras palabras que el conjunto* $\mathcal{J} = \alpha\mathcal{I}$ *es un ideal de* $\mathcal{O}_{\mathbf{K}}$.

Observemos que si $\mathcal{I}$ es un ideal, entonces éste es un ideal fraccional. El recíproco no siempre es cierto, sin embargo tenemos que un ideal fraccional $\mathcal{I}$ es un ideal si y sólo si $\mathcal{I} \subseteq \mathcal{O}_{\mathbf{K}}$.

Teorema 2.32 *Los ideales fraccionales no nulos de $\mathcal{O}_K$ forman un grupo abeliano bajo la multiplicación.*

Demostración : (i) Si $\mathcal{I}_1, \mathcal{I}_2$ son dos ideales fraccionales no nulos de $\mathcal{O}_K$, entonces existen $0 \neq \alpha_1, \alpha_2 \in \mathcal{O}_K$ e ideales no nulos $\mathcal{J}_1, \mathcal{J}_2$ de $\mathcal{O}_K$ tales que $\mathcal{I}_1 = \alpha_1^{-1}\mathcal{J}_1$ y $\mathcal{I}_2 = \alpha_2^{-1}\mathcal{J}_2$ y así

$$\mathcal{I}_1\mathcal{I}_2 = (\alpha_1^{-1}\mathcal{J}_1)(\alpha_2^{-1}\mathcal{J}_2) = (\alpha_1\alpha_2)^{-1}\mathcal{J}_1\mathcal{J}_2\,,$$

en donde $0 \neq \alpha_1\alpha_2 \in \mathcal{O}_K$ y $\mathcal{J}_1\mathcal{J}_2$ es un ideal no nulo de $\mathcal{O}_K$. Por lo tanto $\mathcal{I}_1\mathcal{I}_2$ es un ideal fraccional de $\mathcal{O}_K$.

(ii) Si $\mathcal{I}_1 = \alpha_1^{-1}\mathcal{J}_1$, $\mathcal{I}_2 = \alpha_2^{-1}\mathcal{J}_2$, $\mathcal{I}_3 = \alpha_3^{-1}\mathcal{J}_3$ son tres ideales fraccionales no nulos de $\mathcal{O}_K$ ($0 \neq \alpha_1, \alpha_2, \alpha_3 \in \mathcal{O}_K$ y $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ ideales no nulos de $\mathcal{O}_K$), entonces claramente se tiene que

$$(\mathcal{I}_1\mathcal{I}_2)\mathcal{I}_3 = \mathcal{I}_1(\mathcal{I}_2\mathcal{I}_3).$$

(iii) Si $\mathcal{I}_1, \mathcal{I}_2$ son dos ideales fraccionales de $\mathcal{O}_K$. Claramente $\mathcal{I}_1\mathcal{I}_2 = \mathcal{I}_2\mathcal{I}_1$.

(iv) Si $\mathcal{I} = \alpha^{-1}\mathcal{J}$ es un ideal fraccional no nulo de $\mathcal{O}_K$, entonces

$$\mathcal{I}\mathcal{O}_K = (\alpha^{-1}\mathcal{J})(1\mathcal{O}_K) = \alpha^{-1}\mathcal{J} = \mathcal{I}$$

es decir que $\mathcal{O}_K$ funge como el neutro multiplicativo.

(v) La existencia de los inversos multiplicativos se verá en el siguiente teorema.

□

Teorema 2.33 *Cualquier ideal no nulo de $\mathcal{O}_K$ puede ser escrito como un producto de ideales primos de manera única salvo el orden de los factores.*

Demostración : La demostración se hará siguiendo una serie de pasos.

(i) *Si $\mathcal{I}$ es un ideal no nulo de $\mathcal{O}_K$, entonces existen ideales primos $\mathcal{P}_1, \ldots, \mathcal{P}_r$ tales que $\mathcal{P}_1 \cdots \mathcal{P}_r \subseteq \mathcal{I}$.*

Supongamos que no existen tales ideales primos que cumplan que su producto está contenido en $\mathcal{I}$. Sea S el conjunto de ideales no nulos de $\mathcal{O}_K$ que no contienen a un producto de ideales primos. Claramente $S \neq \emptyset$ pues $\mathcal{I} \in S$. Ahora, como $\mathcal{O}_K$ es noetheriano y S es un conjunto de ideales de $\mathcal{O}_K$ no vacío, entonces S tiene un elemento maximal, digamos $\mathcal{M}$. Claramente $\mathcal{M}$ no es primo (pues si lo fuera $\mathcal{M} \subset \mathcal{M}$ y entonces $\mathcal{M} \notin S$), por lo tanto existen ideales $\mathcal{S}, \mathcal{T} \subseteq \mathcal{O}_K$ tales que $\mathcal{S}\mathcal{T} \subseteq \mathcal{M}$, $\mathcal{S} \nsubseteq \mathcal{M}$, $\mathcal{T} \nsubseteq \mathcal{M}$.

Consideremos ahora los siguientes ideales de $\mathcal{O}_K$.

$$\mathcal{J}_1 = \mathcal{M} + \mathcal{S} \quad \text{y} \quad \mathcal{J}_2 = \mathcal{M} + \mathcal{T}$$

entonces: $\mathcal{J}_1\mathcal{J}_2 \subseteq \mathcal{M}$, $\mathcal{M} \subset \mathcal{J}_1$, $\mathcal{M} \subset \mathcal{J}_2$. Por la máximilidad de $\mathcal{M}$ existen ideales primos $\mathcal{P}_1, \ldots \mathcal{P}_l, \mathcal{P}_{l+1}, \ldots \mathcal{P}_r$ tales que

$$\begin{aligned} \mathcal{P}_1 \cdots \mathcal{P}_l &\subseteq \mathcal{J}_1 \\ \mathcal{P}_{l+1} \cdots \mathcal{P}_r &\subseteq \mathcal{J}_2 \end{aligned}$$

De aquí que:

$$\mathcal{P}_1 \cdots \mathcal{P}_l \mathcal{P}_{l+1} \cdots \mathcal{P}_r \subseteq \mathcal{J}_1\mathcal{J}_2 \subseteq \mathcal{M}$$

lo cual es una contradicción. Por lo tanto para todo ideal $\mathcal{I}$ no nulo de $\mathcal{O}_\mathbf{K}$, existen ideales primos $\mathcal{P}_1, \ldots, \mathcal{P}_r$ tales que $\mathcal{P}_1 \cdots \mathcal{P}_r \subseteq \mathcal{I}$.
(ii) *Si $\mathcal{I}$ es un ideal no nulo de $\mathcal{O}_\mathbf{K}$, y se define el conjunto $\mathcal{I}^{-1}$ como*

$$\mathcal{I}^{-1} = \{x \in \mathbf{K} : x\mathcal{I} \subseteq \mathcal{O}_\mathbf{K}\},$$

entonces $\mathcal{I}\mathcal{I}^{-1}$ es un ideal de $\mathcal{O}_\mathbf{K}$.
Claramente $\mathcal{I}^{-1} \supseteq \mathcal{O}_\mathbf{K}$. También, un cálculo muy sencillo nos muestra que $\mathcal{I}^{-1}$ tiene estructura de $\mathcal{O}_\mathbf{K}$-módulo. Más aún $\forall \alpha \neq 0 \in \mathcal{I}$ se tiene que $\alpha\mathcal{I}^{-1} \subseteq \mathcal{O}_\mathbf{K}$, esto es que $\mathcal{I}^{-1}$ es un ideal fraccional de $\mathcal{O}_\mathbf{K}$.

Ahora, como $\mathcal{O}_\mathbf{K} \subseteq \mathcal{I}^{-1}$ se tiene que $\mathcal{I} = \mathcal{I}\mathcal{O}_\mathbf{K} \subseteq \mathcal{I}\mathcal{I}^{-1}$. Finalmente por la definición de $\mathcal{I}^{-1}$ y lo anterior se tiene que

$$\mathcal{I} \subseteq \mathcal{I}\mathcal{I}^{-1} = \mathcal{I}^{-1}\mathcal{I} \subseteq \mathcal{O}_\mathbf{K}$$

Esto significa que el ideal fraccional $\mathcal{I}\mathcal{I}^{-1}$ es en realidad un ideal.

(iii) *Si $\mathcal{I}$ es un ideal propio de $\mathcal{O}_\mathbf{K}$, entonces $\mathcal{O}_\mathbf{K} \subset \mathcal{I}^{-1}$.*

Como $\mathcal{I} \subseteq \mathcal{M}$ para algún ideal maximal $\mathcal{M}$, entonces $\mathcal{M}^{-1} \subseteq \mathcal{I}^{-1}$. En efecto ya que si $x \in \mathcal{M}^{-1}$, esto implica que $x\mathcal{M} \subseteq \mathcal{O}_\mathbf{K}$, es decir que $x\alpha \in \mathcal{O}_\mathbf{K}$ $\forall \alpha \in \mathcal{M}$ y como $\mathcal{I} \subseteq \mathcal{M}$, entonces $xi \in \mathcal{O}_\mathbf{K}$ $\forall i \in \mathcal{I}$, esto es que $x\mathcal{I} \subseteq \mathcal{O}_\mathbf{K}$ y por lo tanto $x \in \mathcal{I}^{-1}$.

Ahora por (ii) tenemos que $\mathcal{O}_\mathbf{K} \subseteq \mathcal{M}^{-1}$, y por lo tanto es suficiente probar que $\mathcal{M}^{-1} \neq \mathcal{O}_\mathbf{K}$ (pues si es así entonces $\mathcal{O}_\mathbf{K} \subset \mathcal{M}^{-1} \subseteq \mathcal{I}^{-1}$ y terminaríamos la prueba). Para probar lo anterior tomemos $a \neq 0 \in \mathcal{M}$. Usando (i) se elige el mínimo r tal que

$$\mathcal{P}_1 \cdots \mathcal{P}_r \subseteq (a) \quad , \quad \mathcal{P}_1, \ldots, \mathcal{P}_r \text{ ideales primos.}$$

Como $(a) \subseteq \mathcal{M}$ y $\mathcal{M}$ es primo (recordemos que según el teorema 2.29 (d) los ideales primos de $\mathcal{O}_\mathbf{K}$ coinciden con los maximales), algún $\mathcal{P}_i \subseteq \mathcal{M}$. Sin pérdida de generalidad sea $\mathcal{P}_1 \subseteq \mathcal{M}$; pero como los ideales primos coinciden con los maximales entonces $\mathcal{P}_1 = \mathcal{M}$

Ahora, por la minimalidad de r, tenemos que $\mathcal{P}_2\mathcal{P}_3 \cdots \mathcal{P}_r \not\subseteq (a)$, y entonces existe $b \in \mathcal{P}_2\mathcal{P}_3 \cdots \mathcal{P}_r - (a)$. Ahora, como $\mathcal{P}_1 = \mathcal{M}$, entonces $b\mathcal{M} \subseteq (a)$, lo

cual implica que $a^{-1}b\mathcal{M} \subseteq \mathcal{O}_K$, esto es que $a^{-1}b \in \mathcal{M}^{-1}$ (en estos pasos se esta usando que $(a) = a\mathcal{O}_K$).

Finalmente como $b \notin (a) = a\mathcal{O}_K$, entonces $a^{-1}b \notin \mathcal{O}_K$ concluyendose así que $\mathcal{M}^{-1} \neq \mathcal{O}_K$.

(iv) *Si $\mathcal{I}$ es un ideal no nulo de $\mathcal{O}_K$, y si $\mathcal{I}S \subseteq \mathcal{I}$ para algún subconjunto $S \subseteq K$, entonces $S \subseteq \mathcal{O}_K$*

Para demostrar esto basta checar que si $\mathcal{I}\theta \subseteq \mathcal{I}$ para $\theta \in S$, entonces $\theta \in \mathcal{O}_K$. Esto último se sigue inmediatamente si tomamos $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de $\mathcal{I}$ (ver teorema 2.29 (d)) y el mismo argumento usado en el lema 1.14 (d) $\Rightarrow$(a).

(v) *Si $\mathcal{P}$ es un ideal maximal (primo), entonces $\mathcal{P}\mathcal{P}^{-1} = \mathcal{O}_K$.*

De (ii) se tiene que $\mathcal{P} \subseteq \mathcal{P}\mathcal{P}^{-1} \subseteq \mathcal{O}_K$. Pero como $\mathcal{P}$ es maximal, entonces $\mathcal{P}\mathcal{P}^{-1} = \mathcal{P}$ ó $\mathcal{P}\mathcal{P}^{-1} = \mathcal{O}_K$. Si $\mathcal{P}\mathcal{P}^{-1} = \mathcal{P} \subseteq \mathcal{P}$, por (iv) se tendría que $\mathcal{P}^{-1} \subseteq \mathcal{O}_K$ lo cual contradice (iii). Por lo tanto $\mathcal{P}\mathcal{P}^{-1} = \mathcal{O}_K$.

(vi) *Para cualquier ideal $\mathcal{I}$ no nulo de $\mathcal{O}_K$, $\mathcal{I}\mathcal{I}^{-1} = \mathcal{O}_K$.*

Si no es cierto, elijamos $\mathcal{J}$ maximal tal que $\mathcal{J}\mathcal{J}^{-1} \neq \mathcal{O}_K$. Tomemos ahora un ideal maximal $\mathcal{P}$ tal que $\mathcal{J} \subseteq \mathcal{P}$, entonces por (ii) tenemos que $\mathcal{O}_K \subseteq \mathcal{P}^{-1} \subseteq \mathcal{J}^{-1}$, de donde se tiene que $\mathcal{J} \subseteq \mathcal{J}\mathcal{P}^{-1} \subseteq \mathcal{J}\mathcal{J}^{-1} \subseteq \mathcal{O}_K$. Como $\mathcal{J}\mathcal{P}^{-1} \subseteq \mathcal{O}_K$, entonces $\mathcal{J}\mathcal{P}^{-1}$ es un ideal. Ahora notemos que $\mathcal{J} \neq \mathcal{J}\mathcal{P}^{-1}$ pues de lo contrario por (iv) se tendría que $\mathcal{P}^{-1} \subseteq \mathcal{O}_K$ lo cual contradice (iii). Por lo tanto $\mathcal{J} \subset \mathcal{J}\mathcal{P}^{-1}$, y la condición de maximalidad sobre $\mathcal{J}$ implica que el ideal $\mathcal{J}\mathcal{P}^{-1}$ satisface

$$\mathcal{J}\mathcal{P}^{-1}\,(\mathcal{J}\mathcal{P}^{-1})^{-1} = \mathcal{O}_K$$

Pero por definición de $\mathcal{I}^{-1}$, esto significa que

$$\mathcal{P}^{-1}\,(\mathcal{J}\mathcal{P}^{-1})^{-1} \subseteq \mathcal{J}^{-1}$$

Por lo tanto

$$\mathcal{O}_K = \mathcal{J}\mathcal{P}^{-1}\,(\mathcal{J}\mathcal{P}^{-1})^{-1} \subseteq \mathcal{J}\mathcal{J}^{-1} \subseteq \mathcal{O}_K \quad \Rightarrow \quad \mathcal{J}\mathcal{J}^{-1} = \mathcal{O}_K$$

lo cual es una contradicción. Por lo tanto para cualquier ideal $\mathcal{I}$ no nulo, $\mathcal{I}\mathcal{I}^{-1} = \mathcal{O}_K$

(vii) *Cualquier ideal fraccional $\mathcal{I}$ no nulo tiene un inverso $\mathcal{I}^{-1}$ tal que $\mathcal{I}\mathcal{I}^{-1} = \mathcal{O}_K$*

Como $\mathcal{I}$ es un ideal fraccional no nulo, entonces existe $\alpha \neq 0$ y $\mathcal{J}$ ideal no nulo de $\mathcal{O}_K$ tal que $\mathcal{I} = \alpha^{-}\mathcal{J}$. Afirmación: el inverso multiplicativo de $\mathcal{I}$ es $\mathcal{I}^{-1} = \alpha\mathcal{J}^{-1}$ (el cual es un ideal fraccional pues $\mathcal{J}^{-1}$ lo es). En efecto, ya que

$$\mathcal{I}\mathcal{I}^{-1} = (\alpha^{-1}\mathcal{J})(\alpha\mathcal{J}^{-1}) = 1\mathcal{J}\mathcal{J}^{-1} = \mathcal{O}_K$$

Con la prueba de (vii) se concluye la demostración del teorema 2.32.

(viii) *Cualquier ideal $\mathcal{I}$ no nulo es un producto de ideales primos.*

Supongamos que no, y sea $\mathcal{J}$ maximal sujeto a esta condición (es decir

que $\mathcal{J}$ no es un producto de ideales primos), entonces $\mathcal{J}$ no es primo (no es maximal) y así existe $\mathcal{P}$ ideal maximal tal que $\mathcal{J} \subset \mathbf{P}$. Procediendo igual que en (vi) se tiene que

$$\mathcal{J} \subset \mathcal{J}\mathcal{P}^{-1} \subseteq \mathcal{O}_{\mathbf{K}} \quad (\mathcal{J}\mathcal{P}^{-1} \text{ es un ideal})$$

Por la condición de maximalidad sobre $\mathcal{J}$

$$\mathcal{J}\mathcal{P}^{-1} = \mathcal{P}_1 \cdots \mathcal{P}_r$$

en donde los ideales $\mathcal{P}_1, \ldots, \mathcal{P}_r$ son primos. Finalmente tenemos que

$$\mathcal{J} = \mathcal{P}\mathcal{P}_1 \cdots \mathcal{P}_r$$

lo cual es una contradicción. Por lo tanto cualquier ideal no nulo es un producto de ideales primos.

(ix) *La factorización en ideales primos es única.*

Si $\mathcal{I}$ es un ideal tal que

$$\mathcal{P}_1 \cdots \mathcal{P}_r = \mathcal{J}_1 \cdots \mathcal{J}_s$$

en donde los $\mathcal{P}_i, \mathcal{J}_k$ $(1 \leq i \leq r\ ,\ 1 \leq k \leq s)$ son ideales primos(maximales) , entonces $\mathcal{P}_1$ divide a algún $\mathcal{J}_k$ (esto se demostrará en la siguiente proposición). Pero como los ideales primos coinciden con los maximales entonces $\mathcal{P}_1 = \mathcal{J}_k$. Multiplicando por $\mathcal{P}_1^{-1}$ y procediendo igual que en el teorema 2.20 se obtiene que la factorización en ideales primos es única salvo el orden de los factores, con lo cual se le dá fin al teorema.

□

Proposición 2.34 *Para ideales $\mathcal{I}, \mathcal{J}$ de $\mathcal{O}_{\mathbf{K}}$, $\mathcal{I} \mid \mathcal{J}$ si y sólo si $\mathcal{I} \supseteq \mathcal{J}$.*

Demostración : $\Rightarrow$) Sea $x \in \mathcal{J}$. Como $\mathcal{J} = \mathcal{I}\mathcal{A}$, $\mathcal{A}$ algún ideal de $\mathcal{O}_{\mathbf{K}}$ e $\mathcal{I}\mathcal{A} \subseteq \mathcal{I}$, $x \in \mathcal{I}$. Esto es que $\mathcal{I} \supseteq \mathcal{J}$.

$\Leftarrow$) Si $\mathcal{I} \supseteq \mathcal{J}$, entonces $\mathcal{O}_{\mathbf{K}} = \mathcal{I}^{-1}\mathcal{I} \supseteq \mathcal{I}^{-1}\mathcal{J}$, es decir que $\mathcal{I}^{-1}\mathcal{J}$ es un ideal y claramente:

$$\mathcal{J} = \mathcal{I}\mathcal{I}^{-1}\mathcal{J} = \mathcal{I}\mathcal{A} \quad (\mathcal{I}^{-1}\mathcal{J} = \mathcal{A})$$

y por lo tanto $\mathcal{I} | \mathcal{J}$.

□

De esta proposición se desprende rápidamente que si $\mathcal{P}$ es un ideal primo y $\mathcal{A}, \mathcal{B}$ son ideales cualesquiera

$$\mathcal{P} \mid \mathcal{A}\mathcal{B} \quad \Rightarrow \quad \mathcal{P} \mid \mathcal{A} \text{ ó } \mathcal{P} \mid \mathcal{B}$$

pues si $\mathcal{P} | \mathcal{A}\mathcal{B}$, entonces $\mathcal{A}\mathcal{B} \subseteq \mathcal{P}$, pero como $\mathcal{P}$ es primo, entonces $\mathcal{A} \subseteq \mathcal{P}$ ó $\mathcal{B} \subseteq \mathcal{P}$ es decir $\mathcal{P} | \mathcal{A}$ ó $\mathcal{P} | \mathcal{B}$.

2.8 La norma de un ideal

El teorema de factorización única para ideales del anillo de enteros $\mathcal{O}_{\mathbf{K}}$ de un campo de números $\mathbf{K}$ tiene importantes concecuencias. En particular, cualesquiera dos ideales no nulos $\mathcal{A}$ y $\mathcal{B}$ tienen un máximo común divisor $\mathcal{G}$ y un mínimo común múltiplo $\mathcal{L}$ con las siguientes propiedades:

$$\begin{array}{ll} \mathcal{G}|\mathcal{A}\ ,\ \mathcal{G}|\mathcal{B}; & \text{y si } \mathcal{G}' \text{ tiene las mismas propiedades } \mathcal{G}'|\mathcal{G} \\ \mathcal{A}|\mathcal{L}\ ,\ \mathcal{B}|\mathcal{L}; & \text{y si } \mathcal{L}' \text{ tiene las mismas propiedades } \mathcal{L}|\mathcal{L}' \end{array}$$

Lema 2.35 *Si $\mathcal{A}, \mathcal{B}$ son dos ideales no nulos los cuales se factorizan en ideales primos como*

$$\mathcal{A} = \prod \mathcal{P}_i^{e_i} \quad , \quad \mathcal{B} = \prod \mathcal{P}_i^{f_i}$$

en donde los $\mathcal{P}_i$ son ideales primos distintos, entonces

$$\begin{aligned} \mathcal{G} &= \prod \mathcal{P}_i^{min(e_i,f_i)} \\ \mathcal{L} &= \prod \mathcal{P}_i^{max(e_i,f_i)} \end{aligned}$$

Demostración : Se sigue de la factorización única entre ideales.

□

Otra caracterización importante del máximo común divisor y del mínimo común múltiplo se da en el siguiente

Lema 2.36 *Si $\mathcal{A}, \mathcal{B}$ son dos ideales no nulos de $\mathcal{O}_{\mathbf{K}}$ y $\mathcal{G}, \mathcal{L}$ son el máximo común divisor y el mínimo común múltiplo respectivamente de $\mathcal{A}$ y $\mathcal{B}$, entonces*

$$\mathcal{G} = \mathcal{A} + \mathcal{B} \quad , \quad \mathcal{L} = \mathcal{A} \cap \mathcal{B}$$

Demostración : Por las propiedades de $\mathcal{G}$ y $\mathcal{L}$, tenemos que $\mathcal{G}$ es el más pequeño ideal que contiene a $\mathcal{A}$ y a $\mathcal{B}$, y $\mathcal{L}$ es el más grande ideal contenido en $\mathcal{A}$ y en $\mathcal{B}$, entonces $\mathcal{G} \subseteq \mathcal{A}+\mathcal{B}$ pues $(\mathcal{A}+\mathcal{B})|\mathcal{A}$ y $(\mathcal{A}+\mathcal{B})|\mathcal{B}$, análogamente $\mathcal{A}\cap\mathcal{B} \subseteq \mathcal{L}$ pues $\mathcal{A}|(\mathcal{A}\cap\mathcal{B})$ y $\mathbf{B}|(\mathcal{A}\cap\mathcal{B})$. Por otro lado si $x \in \mathcal{A}+\mathcal{B}$, entonces $x \in \mathcal{G}$ pues $\mathcal{A} \subseteq \mathcal{G}$ y $\mathcal{B} \subseteq \mathcal{G}$ de donde concluimos que $\mathcal{A}+\mathcal{B} \subseteq \mathcal{G}$ y por lo tanto $\mathcal{G} = \mathcal{A}+\mathcal{B}$. Similarmente si $y \in \mathcal{L}$, entonces $y \in \mathcal{A}$ pues $\mathcal{L} \subseteq \mathcal{A}$ y $y \in \mathcal{B}$ pues $\mathcal{L} \subseteq \mathcal{B}$ de donde concluimos que $\mathcal{L} \subseteq \mathcal{A} \cap \mathcal{B}$ y por lo tanto $\mathcal{L} = \mathcal{A} \cap \mathcal{B}$.

□

En la prueba del teorema 2.29 (d), se vió que si $0 \neq \mathcal{I}$ es un ideal de $\mathcal{O}_{\mathbf{K}}$, entonces el anillo coclente $\mathcal{O}_{\mathbf{K}}/\mathcal{I}$ es finito.

Definición 2.37 *Si $\mathcal{I}$ es un ideal no nulo de $\mathcal{O}_{\mathbf{K}}$. La norma de $\mathcal{I}$ se define como*

$$N(\mathcal{I}) = |\ \mathcal{O}_{\mathbf{K}}/\mathcal{I}\ |$$

En el siguiente teorema y su corolario veremos la analogía entre la norma de un elemento y de un ideal.

Teorema 2.38 *Si $\mathcal{I}$ es un ideal no nulo de $\mathcal{O}_{\mathbf{K}}$ y $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Z}$-base de $\mathcal{I}$, entonces*

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

en donde Δ es el discriminante de $\mathbf{K}$.

Demostración : Si $\{w_1, \ldots, w_n\}$ es una $\mathbb{Z}$-base de $\mathcal{O}_{\mathbf{K}}$, entonces existen enteros racionales c_{ij} tales que $\alpha_i = \sum c_{ij} w_i$ y por el teorema A.28 del apéndice se tiene que

$$N(\mathcal{I}) = |\ \mathcal{O}_{\mathbf{K}}/\mathcal{I}\ | = |\ \det(c_{ij})\ | \neq 0$$

Por otro lado se sabe que:

$$\Delta[\alpha_1 \ldots, \alpha_n] = [\det(c_{ij})]^2 \Delta[w_1, \ldots, w_n]$$

Por lo tanto tenemos que

$$\Delta[\alpha_1, \ldots, \alpha_n] = [N(\mathcal{I})]^2 \Delta$$

de donde se sigue inmediatamente el resultado.

□

Corolario 2.39 *Si $\mathcal{A} = \langle a \rangle$ es un ideal principal no nulo($a \neq 0$), entonces* $N(\mathcal{A}) = |\ N_K(a)\ |$.

Demostración : Si $\{w_1, \ldots, w_n\}$ es una $\mathbb{Z}$-base de $\mathcal{O}_{\mathbf{K}}$, entonces fácilmente se checa que $\{aw_1, \ldots, aw_n\}$ es una $\mathbb{Z}$-base de $\mathcal{A}$. Ahora como:

$$\Delta[aw_1,\ldots,aw_n] = \begin{vmatrix} \sigma_1(aw_1) & \sigma_1(aw_2) & \cdots & \sigma_1(aw_n) \\ \sigma_2(aw_1 & \sigma_2(aw_2) & \cdots & \sigma_2(aw_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(aw_1 & \sigma_n(aw_2) & \cdots & \sigma_n(aw_n) \end{vmatrix}^2$$

$$= \left(\sigma_1^2(a)\cdots\sigma_n^2(a)\right) \begin{vmatrix} \sigma_1(w_1 & \sigma_1(w_2) & \cdots & \sigma_1(w_n) \\ \sigma_2(w_1 & \sigma_2(w_2) & \cdots & \sigma_2(w_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(w_1 & \sigma_n(w_2) & \cdots & \sigma_n(w_n) \end{vmatrix}^2$$

$$= [N_K(a)]^2\Delta$$

Finalmente por el teorema previo tenemos que

$$N(\mathcal{A}) = \left|\frac{\Delta[aw_1,\ldots,aw_n]}{\Delta}\right|^{1/2} = \left|\frac{[N(a)]^2\Delta}{\Delta}\right| = \mid N_K(a) \mid$$

□

El siguiente teorema nos dice que la nueva norma es multiplicativa al igual que la norma de elementos de **K**.

Teorema 2.40 *Si $\mathcal{A},\mathcal{B}$ son ideales no nulos de $\mathcal{O}_{\mathbf{K}}$, entonces*

$$N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$$

Demostración : Por factorización única basta que probemos que

$$N(\mathcal{AP}) = N(\mathcal{A})N(\mathcal{P}) \tag{2.10}$$

donde $\mathcal{P}$ es un ideal primo. En efecto ya que si $\mathcal{B} = \mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_r$ (los $\mathcal{P}_i$ no necesariamente distintos), entonces $N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{P}_1)\cdots N(\mathcal{P}_r) = N(\mathcal{A})N(\mathcal{B})$.

Probemos entonces lo dado en 2.10. Para esto probaremos las siguientes dos cosas de las cuales se desprende inmediatamente el resultado:

$$\begin{array}{ll} \text{(i)} & \mid \mathcal{O}_{\mathbf{K}}/\mathcal{AP} \mid = \mid \mathcal{O}_{\mathbf{K}}/\mathcal{A} \mid\mid \mathcal{A}/\mathcal{AP} \mid . \\ \text{(ii)} & \mid \mathcal{A}/\mathcal{AP} \mid = \mid \mathcal{O}_{\mathbf{K}}/\mathcal{P} \mid . \end{array}$$

(i) $\mathcal{AP} \subseteq \mathcal{A} \subseteq \mathcal{O}_{\mathbf{K}}$, y de aquí que $\mathcal{O}_{\mathbf{K}}/\mathcal{A} \cong (\mathcal{O}_{\mathbf{K}}/\mathcal{AP})/(\mathcal{A}/\mathcal{AP})$ y por el teorema de Lagrange

$$|\mathcal{O}_K/\mathcal{A}| = \frac{|\mathcal{O}_K/\mathcal{AP}|}{|\mathcal{A}/\mathcal{AP}|}$$

de donde se concluye que $|\mathcal{O}_K/\mathcal{AP}| = |\mathcal{O}_K/\mathcal{A}|\,|\mathcal{A}/\mathcal{AP}|$.

(ii) La factorización única implica que $\mathcal{A} \neq \mathcal{AP}$, y de aquí que $\mathcal{AP}\mathcal{A}$. Más aún, no existe ningún ideal estrictamente entre $\mathcal{AP}$ y $\mathcal{A}$. En efecto, ya que si $\mathcal{J}$ es un ideal tal que

$$\mathcal{AP} \subseteq \mathcal{J} \subseteq \mathcal{A} \quad \Rightarrow \mathcal{A}^{-1}\mathcal{AP} \subseteq \mathcal{A}^{-1}\mathcal{J} \subseteq \mathcal{A}^{-1}\mathcal{A}$$

esto es que

$$\mathcal{P} \subseteq \mathcal{A}^{-1}\mathcal{J} \subseteq \mathcal{O}_K$$

pero como $\mathcal{P}$ es maximal pues es primo, entonces $\mathcal{A}^{-1}\mathcal{J} = \mathcal{P}$ ó $\mathcal{A}^{-1}\mathcal{J} = \mathcal{O}_K$ de donde se tiene que $\mathcal{J} = \mathcal{AP}$ ó $\mathcal{J} = \mathcal{A}$.

Lo anterior significa que para cualquier $a \in \mathcal{A} - \mathcal{AP}$ se tiene que

$$\mathcal{AP} + \langle a \rangle = \mathcal{A} \tag{2.11}$$

Con una a que satisfaga la ecuación 2.11 definamos

$$\Psi : \mathcal{O}_K \to \mathcal{A}/\mathcal{AP}$$

como

$$\Psi(x) = ax + \mathcal{AP}$$

Afirmación: Ψ es un epimorfismo entre $\mathcal{O}_K$-módulos. En efecto, ya que fácilmente se puede checar que Ψ es un homomorfismo. Por otro lado si $a_1 + \mathcal{AP} \in \mathcal{A}/\mathcal{AP}$, por la ecuación 2.11 se tiene que existen $r \in \mathcal{AP}$ y $x \in \mathcal{O}_K$ tales que $a_1 = r + ax$ y por lo tanto

$$\begin{aligned} \Psi(x) &= ax + \mathcal{AP} = (a_1 - r) + \mathcal{AP} \\ &= (a_1 + \mathcal{AP}) + (-r + \mathcal{AP}) \\ &= (a_1 + \mathcal{AP}) + \mathcal{AP} = a_1 + \mathcal{AP}\,, \end{aligned}$$

esto es que Ψ es suprayectiva.

Por otro lado el $\ker\Psi$ aparte de ser un $\mathcal{O}_K$-módulo, también es un ideal de $\mathcal{O}_K$ y claramente $\mathcal{P} \subseteq \ker\Psi$, además $\ker\Psi \neq \mathcal{O}_K$ (ya que de lo contrario

tendríamos que $\mathcal{A}/\mathcal{A}\mathcal{P} \cong \mathcal{O}_K/\mathcal{O}_K = 0$ lo cual contradice que $\mathcal{A} \neq \mathcal{A}\mathcal{P}$), y como $\mathcal{P}$ es maximal, entonces $\ker\Psi = \mathcal{P}$.

Finalmente $\mathcal{O}_K/\mathcal{P} \cong \mathcal{A}/\mathcal{A}\mathcal{P}$, de donde se concluye que

$$| \mathcal{A}/\mathcal{A}\mathcal{P} | = | \mathcal{O}_K/\mathcal{P} | \ .$$

□

Teorema 2.41 *Sea $\mathcal{A}$ un ideal de $\mathcal{O}_K$, $\mathcal{A} \neq 0$:* (a) *Si $N(\mathcal{A})$ es primo, entonces lo es también $\mathcal{A}$.*
(b) $N(\mathcal{A}) \in \mathcal{A}$.
(c) *Si $\mathcal{A}$ es primo, en $\mathcal{A}$ hay exactamente un primo racional p, y entonces*

$$N(\mathcal{A}) = p^m \ ,$$

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

Demostración : (a) Sea $\mathcal{A} = \mathcal{P}_1 \cdots \mathcal{P}_r$ la factorización en ideales primos de $\mathcal{A}$. Aplicando normas en ambos lados se tiene que:

$$N(\mathcal{A}) = N(\mathcal{P}_1) \cdots N(\mathcal{P}_r)$$

pero como $N(\mathcal{A})$ es primo racional, entonces todos los factores $N(\mathcal{P}_i)$ exepto uno de ellos valen 1, esto es que todos los ideales $\mathcal{P}_i$ exepto uno de ellos son iguales a $\mathcal{O}_\mathbf{K}$, de donde concluimos que $\mathcal{A}$ es un ideal primo.

(b) Como $\mathcal{O}_\mathbf{K}/\mathcal{A}$ es un grupo aditivo finito, por el teorema de Lagrange $N(\mathcal{A})(x+\mathcal{A}) = N(\mathcal{A})x + \mathcal{A} = \mathcal{A}\ \forall x \in \mathcal{O}_\mathbf{K}$, es decir que $N(\mathcal{A})x \in \mathcal{A}\ \forall x \in \mathcal{O}_\mathbf{K}$. Haciendo $x = 1$ se tiene entonces que $N(\mathcal{A}) \in \mathcal{A}$.

(c) Por el inciso (b) tenemos que si

$$N(\mathcal{A}) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \in \mathcal{A}$$

en donde $p_1, p_2, \ldots, p_r$ son primos racionales distintos , entonces $p = p_i \in \mathcal{A}$ para algún i pues $\mathcal{A}$ es un ideal primo. Mostraremos ahora que en $\mathcal{A}$ no hay dos primos racionales. Si p y q son primos racionales distintos y si ambos pertenecen a $\mathcal{A}$, entonces existen enteros racionales r, s tales que $pr + qs = 1$ y como $\mathcal{A}$ es un ideal entonces $1 \in \mathcal{A}$, y de aquí que $\mathcal{A} = \mathcal{O}_\mathbf{K}$, lo cual es una contradicción pues $\mathcal{A}$ es primo.

Finalmente como $(p) \subseteq \mathcal{A}$, entonces $\mathcal{A}|(p)$, y de aquí que: $N(\mathcal{A})|N((p))$, pero por el corolario 2.39, $N((p)) = | N_K(p) | = p^n$, en donde n es el grado de **K**. Por lo tanto

$$N(\mathcal{A}) = p^m \ , \ m \leq n \ .$$

□

Observemos que el inciso (c) de este teorema nos da la respuesta de si el recíproco del inciso (a) del mismo teorema es válido. Claramente la respuesta es no.

Ejemplo: Si $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$ (el anillo de enteros Gaussianos) y $\mathcal{A} = \langle 3 \rangle$. Afirmamos que el número 3 es irreducible en $\mathbb{Z}[\sqrt{-1}]$. En efecto ya que si $3 = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ y si ninguno de α, β es una unidad, tomando normas tendríamos que

$$9 = N_K(3) = N_K(\alpha) N_K(\beta)$$

de donde tendríamos que en $\mathbb{Z}[\sqrt{-1}]$ existirían elementos cuya norma es ± 3 lo cual es imposible pues la ecuación

$$a^2 + b^2 = \pm 3$$

no tiene solución en $\mathbb{Z}$. Por lo tanto 3 es irreducible. Ahora como $\mathbb{Z}[\sqrt{-1}]$ es un dominio de factorización única, 3 es primo y por lo tanto $\langle 3 \rangle$ es un ideal primo de $\mathbb{Z}[\sqrt{-1}]$. Sin embargo

$$N(\langle 3 \rangle) = \mid N_K(3) \mid = 3^2 \ .$$

Teorema 2.42 (a) *Cualquier ideal no nulo de $\mathcal{O}_K$ tiene un número finito de divisores.*
(b) *Un entero racional no nulo pertenece sólo a un número finito de ideales de $\mathcal{O}_K$.*
(c) *Sólo un numero finito de ideales tienen norma dada.*

Demostración : (a) Recordemos que según la proposición 2.34 los divisores de un ideal $0 \neq \mathcal{A}$ son aquellos ideales que contienen a $\mathcal{A}$. Por lo tanto el resultado se sigue inmediatamente del teorema de factorización única en ideales primos.
(b) Si $0 \neq r \in \mathbb{Z}$, entonces $0 \neq \langle r \rangle$ y por el inciso (a) sólo un número finito de ideales contienen al ideal $\langle r \rangle$ y así r sólo está en un número finito de ideales de $\mathcal{O}_K$.
(c) Si $n \in \mathbb{N}$, y

$$S = \{\mathcal{I} \subseteq \mathcal{O}_K \ / \ N(\mathcal{I}) = n\} \ ,$$

por el teorema 2.41 (b), $N(\mathcal{I}) \in \mathcal{I}$, y así n pertenece a todos los elementos de S. Pero por inciso (b) tenemos que n pertenece a sólo un número finito de ideales de $\mathcal{O}_K$. Por lo tanto $|\ S\ |$ es finito.

□

Recordemos que cualquier ideal de $\mathcal{O}_K$ es finitamente generado pues $\mathcal{O}_K$ es noetheriano. Más aún como veremos más adelante cualquier ideal de $\mathcal{O}_K$ está generado por a lo más dos elementos. Para probar tal resultado necesitaremos del siguiente

Lema 2.43 *Si $\mathcal{A}, \mathcal{B}$ son ideales no nulos de $\mathcal{O}_K$, entonces existe $0 \neq \alpha \in \mathcal{A}$ tal que*

$$\alpha\mathcal{A}^{-1} + \mathcal{B} = \mathcal{O}_K$$

Demostración : Como $\mathcal{A}\mathcal{A}^{-1} \subseteq \mathcal{O}_K$, entonces $\alpha\mathcal{A}^{-1} \subseteq \mathcal{O}_K\ \forall \alpha \in \mathcal{A}$. Esto es que $\alpha\mathcal{A}^{-1} (\alpha \neq 0)$ es un ideal y no solamente un ideal fraccional. Ahora según el lema 2.36 $\alpha\mathcal{A}^{-1} + \mathcal{B}$ es el máximo común divisor de $\alpha\mathcal{A}^{-1}$ y $\mathcal{B}$. Ahora notemos que es suficiente elegir $0 \neq \alpha \in \mathcal{A}$ tal que

$$\alpha\mathcal{A}^{-1} + \mathcal{P}_i = \mathcal{O}_K \quad (i = 1, 2, \ldots, r) \tag{2.12}$$

donde $\mathcal{P}_1, \ldots, \mathcal{P}_r$ son los distintos ideales primos que aparecen en la factorización primaria de $\mathcal{B}$. En efecto pues si 2.12 es cierto y suponiendo que $\mathcal{B} = \mathcal{P}_1^{m_1} \cdots \mathcal{P}_r^{m_r}$, entonces según la proposición A.5 del apéndice tenemos que

$$\mathcal{O}_K = (\alpha\mathcal{A}^{-1} + \mathcal{P}_1)^{m_1} \cdots (\alpha\mathcal{A}^{-1} + \mathcal{P}_r)^{m_r} \subseteq \alpha\mathcal{A}^{-1} + \mathcal{P}_1^{m_1} \cdots \mathcal{P}_r^{m_r} = \alpha\mathcal{A}^{-1} + \mathcal{B}$$

esto es que $\mathcal{O}_K \subseteq \alpha\mathcal{A}^{-1} + \mathcal{B}$, y así $\mathcal{O}_K = \alpha\mathcal{A}^{-1} + \mathcal{B}$.

Como $\mathcal{P}_i$ es maximal pues $\mathcal{P}_i$ es primo, entonces la igualdad 2.12 se sigue inmediatamente si demostramos que

$$\alpha\mathcal{A}^{-1} \not\subset \mathcal{P}_i \quad 0 \neq \alpha \in \mathcal{A} \quad (i = 1, \ldots, r) \tag{2.13}$$

pues si es así entonces $\mathcal{P}_i \subset \alpha\mathcal{A}^{-1} + \mathcal{P}_i \subseteq \mathcal{O}_K$, de donde se concluiría que $\alpha\mathcal{A}^{-1} + \mathcal{P}_i = \mathcal{O}_K$.

La expresión 2.13 se sigue si elegimos $\alpha \in \mathcal{A} - \mathcal{A}\mathcal{P}_i\ \forall i = 1, \ldots, r$. En efecto, ya que si tenemos tal α, entonces $\alpha\mathcal{A}^{-1} \neq \mathcal{P}_i\ \forall i$, porque de lo contrario se tendría que $\langle \alpha \rangle = \mathcal{A}\mathcal{P}_i$ lo cual es una contradicción con la elección de α.

Tratemos entonces de encontrar $\alpha \in \mathcal{A} - \mathcal{A}\mathcal{P}_i\ \ \forall i = 1, \ldots, r$.

Si $r = 1$, la factorización única de ideales implica que $\mathcal{A} \neq \mathcal{A}\mathcal{P}_i$ y se puede tomar $\alpha \in \mathcal{A} - \mathcal{A}\mathcal{P}_i$.

Si $r > 1$, sea

$$\mathcal{A}_i = \mathcal{A}\mathcal{P}_1 \cdots \mathcal{P}_{i-1}\mathcal{P}_{i+1} \cdots \mathcal{P}_r$$

Por el caso $r = 1$ se puede elegir

$$\alpha_i \in \mathcal{A}_i - \mathcal{A}_i\mathcal{P}_i$$

Definamos

$$\alpha = \alpha_1 + \cdots + \alpha_r \tag{2.14}$$

Como cada $\alpha_i \in \mathcal{A}_i \subseteq \mathcal{A}$, entonces $\alpha \in \mathcal{A}$, y sólo nos resta probar que $\alpha \notin \mathcal{A}\mathcal{P}_i \; \forall i = 1, \ldots, r$. Supongamos que $\alpha \in \mathcal{A}\mathcal{P}_i$ para alguna i. Ahora, si $j \neq i$, entonces $\alpha_j \in \mathcal{A}_j \subseteq \mathcal{A}\mathcal{P}_i$ es decir que $\alpha_j \in \mathcal{A}\mathcal{P}_i$, $j \neq i$, pero si es así entonces de 2.14 se tiene que

$$\alpha_i = \alpha - \alpha_1 - \cdots - \alpha_{i-1} - \alpha_{i+1} - \cdots - \alpha_r \; \in \mathcal{A}\mathcal{P}_i$$

como también $\alpha_i \in \mathcal{A}_i$, entonces $\alpha_i \in \mathcal{A}_i \bigcap \mathcal{A}\mathcal{P}_i$. Finalmente por los lemas 2.35 y 2.36 el mínimo común múltiplo de $\mathcal{A}_i$ y $\mathcal{A}\mathcal{P}_i$ es:

$$\mathcal{A}\mathcal{P}_i \cap \mathcal{A}_i = \mathcal{A}\mathcal{P}_1 \cdots \mathcal{P}_r = \mathcal{A}_i\mathcal{P}_i$$

Por lo tanto tenemos que $\alpha_i \in \mathcal{A}_i\mathcal{P}_i$ lo cual contradice la elección de α_i

□

Teorema 2.44 *Si $0 \neq \mathcal{A}$ es un ideal de $\mathcal{O}_K$ y $0 \neq \beta \in \mathcal{A}$, entonces existe $0 \neq \alpha \in \mathcal{A}$ tal que $\mathcal{A} = \langle \alpha, \beta \rangle$.*

Demostración : Sea $\mathcal{B} = \beta\mathcal{A}^{-1}$ el cual es un ideal no nulo de $\mathcal{O}_K$. Por el lema anterior existe $0 \neq \alpha \in \mathcal{A}$ tal que

$$\alpha\mathcal{A}^{-1} + \beta\mathcal{A}^{-1} = \mathcal{O}_K$$

de aquí que

$$(\langle \alpha \rangle + \langle \beta \rangle)\mathcal{A}^{-1} = \mathcal{O}_K$$

y como el conjunto de ideales fraccionales no nulos forma un grupo multiplicativo, entonces

$$\mathcal{A} = \langle \alpha \rangle + \langle \beta \rangle = \langle \alpha, \beta \rangle \ .$$

□

Con los resultados anteriores podemos caracterizar a los anillos de enteros $\mathcal{O}_{\mathbf{K}}$ de un campo de números $\mathbf{K}$, para los cuales la factorización de elementos en irreducibles es única.

Teorema 2.45 *La factorización de elementos de $\mathcal{O}_{\mathbf{K}}$ en irreducibles es única si y sólo si cualquier ideal de $\mathcal{O}_{\mathbf{K}}$ es principal.*

Demostración : $\Leftarrow$) Esto ya se probó en el teorema 2.23 .
$\Rightarrow$) Si en $\mathcal{O}_{\mathbf{K}}$ se da la factorización única en irreducibles, y si $\mathcal{A}$ es un ideal de $\mathcal{O}_{\mathbf{K}}$. Por factorización única de ideales $\mathcal{A} = \mathcal{P}_1 \cdots \mathcal{P}_r$, en donde los ideales $\mathcal{P}_1, \ldots, \mathcal{P}_r$ son primos. Ahora como el producto de ideales principales es un ideal principal, es suficiente probar que cualquier ideal primo es principal. Sea $\mathcal{P}$ un ideal primo de $\mathcal{O}_{\mathbf{K}}$, por el teorema 2.41 (b), $N(\mathcal{P}) = m \in \mathcal{P} \cap \mathbf{Z}$. Factorizando en elementos irreducibles a m se tiene que

$$m = \pi_1 \cdots \pi_s \quad (\pi_1, \ldots, \pi_s \quad \text{irreducibles})$$

como $m \in \mathcal{P}$ y $\mathcal{P}$ es primo, entonces algún $\pi_i \in \mathcal{P}$, esto implica que $\mathcal{P} | (\pi_i)$. Ahora como en $\mathcal{O}_{\mathbf{K}}$ se da la factorización única, entonces π_i es un primo y por lo tanto $\langle \pi_i \rangle$ es un ideal primo. Finalmente como $\mathcal{P} \mid \langle \pi_i \rangle$ y ambos ideales son maximales pues son primos, entonces

$$\mathcal{P} = \langle \pi_i \rangle$$

esto es que $\mathcal{P}$ es principal.

□

Capítulo 3

El lema de Kummer

En este capítulo se trabajará específicamente con sólo un tipo de campos de números, a saber con los campos ciclotómicos, esto es, con los campos $\mathbf{K} = \mathbb{Q}(\xi)$, en donde $\xi = e^{2\pi i/p}$ para p un primo racional impar.

En especial se probará el importante *lema de Kummer* el cual nos dice la forma que tiene cualquier unidad de $\mathbf{Z}[\xi]$ el anillo de enteros de $\mathbb{Q}(\xi)$.

3.1 El lema de Kummer

Como en el capítulo 1 , sea $\mathbf{K} = \mathbb{Q}(\xi)$; donde $\xi = e^{2\pi i/p}$ (p primo racional impar), definamos el siguiente ideal

$$\mathcal{L} = \langle 1 - \xi \rangle$$

en $\mathbf{Z}[\xi]$ el anillo de enteros de $\mathbf{K}$.

Algunas propiedades de $\mathcal{L}$ se dan en el siguiente:

Lema 3.1 (a) $\mathcal{L}^{p-1} = \langle p \rangle$
(b) $N(\mathcal{L}) = p$

Demostración : (a) En el capítulo 1 se vió que:

$$p = \prod_{j=1}^{p-1} (1 - \xi^j)$$

de aquí que

$$\langle p \rangle = \prod_{j=1}^{p-1} \langle 1 - \xi^j \rangle \,. \tag{3.1}$$

Claramente $1-\xi | 1-\xi^j$ para $j = 1, 2, \ldots, p-1$.

Por otro lado, tenemos que para cada $j = 1, 2, \ldots, p-1$ la congruencia

$$jx \equiv 1 \pmod{p}$$

tiene solución pues j, p son primos relativos. Entonces existe $t \in \mathbb{Z}$ tal que $jt \equiv 1 \pmod{p}$, esto es que

$$jt = 1 + ps \quad , \quad s \in \mathbb{Z}$$

entonces

$$1 - \xi = 1 - \xi\xi^{ps} = 1 - \xi^{jt} = 1 - (\xi^j)^t$$

lo cual implica que $1 - \xi^j \mid 1 - \xi$. Por lo tanto $1 - \xi$ es asociado de $1 - \xi^j$ para $j = 1, 2, \ldots, p-1$, y así por el teorema 2.8 (b) se tiene que

$$\langle 1 - \xi \rangle = \langle 1 - \xi^j \rangle .$$

Sustituyendo esto último en la ecuacion 3.1 se tiene que

$$\langle p \rangle = \prod_{j=1}^{p-1} \langle 1 - \xi^j \rangle = \langle 1 - \xi \rangle^{p-1} = \mathcal{L}^{p-1} .$$

(b) Como $\mathcal{L}^{p-1} = \langle p \rangle$, tomando normas y usando lo visto en el capítulo 2 sección 2.8 se tiene que

$$N(\mathcal{L}^{p-1}) = N(\langle p \rangle) \quad \Rightarrow \quad [N(\mathcal{L})]^{p-1} = N_K(p) = p^{p-1}$$

de donde concluimos que $N\langle \mathcal{L} \rangle = p$.

□

Observación : *Que* $N(\mathcal{L}) = | \mathbf{Z}[\xi]/\langle 1 - \xi \rangle | = p$, *nos dice que en* $\mathbf{Z}[\xi]$ *hay* p *distintas clases de equivalencia módulo* $\langle 1 - \xi \rangle$. *Ahora, como cualquier elemento de* $\mathbf{Z}[\xi]$ *es de la forma* $g(\xi)$, *en donde* $g(x) \in \mathbf{Z}[\mathbf{x}]$. *Por el algoritmo de la división*

$$g(x) = (1 - x)h(x) + r(x) \quad ; \quad en \ \ \mathbf{Z}[\mathbf{x}] ,$$

esto último es posible gracias a que $1 - x \in \mathbf{Z}[\mathbf{x}]$ *y sobre todo a que los coeficientes de* $1 - x$ *son* 1 *y* -1. *Con lo anterior tenemos que*

$$g(x) = (1 - x)h(x) + c \ , \ h(x) \in \mathbf{Z}[\mathbf{x}] \ , \ c \in \mathbf{Z} \subset \mathbf{Z}[\mathbf{x}]$$

evaluando en $x = \xi$ se tiene que

$$g(\xi) = (1-\xi)h(\xi) + c \quad \Rightarrow \quad g(\xi) - c = (1-\xi)h(\xi)\,.$$

Esto último nos dice que cualquier elemento de $\mathbb{Z}[\xi]$ es congruente módulo $\langle 1-\xi\rangle$ a algún entero racional.

Ahora, como $p = \prod_{j=1}^{p-1}(1-\xi^j)$, entonces todos los múltiplos de p (en $\mathbb{Z}$) estan en $\langle 1-\xi\rangle$. Además $n + \langle 1-\xi\rangle = (n+p) + \langle 1-\xi\rangle$ $\forall n \in \mathbb{Z}$ y como $N(\mathcal{L}) = p$, entonces cualquier elemento de $\mathbb{Z}[\xi]$ es congruente módulo $\mathcal{L} = \langle 1-\xi\rangle$ a uno de $0, 1, 2, \ldots, p-1$.

Lema 3.2 *Las únicas raíces de la unidad en $\mathbf{K} = \mathbb{Q}[\xi]$ son $\pm\xi^s$, $s \in \mathbb{Z}$*

Demostración : Primero que nada probaremos las siguientes tres cosas

(a) $i = \sqrt{-1} \notin \mathbf{K}$

Si $i \in \mathbf{K}$. Como i es raíz del polinomio $x^2 + 1$, entonces $i \in \mathbf{Z}[\xi]$ y más aún como $i(-i) = 1$, entonces i es una unidad. Por otro lado como $2 = i(1-i)^2$, entonces

$$\langle 2\rangle = \langle i\rangle\langle 1-i\rangle^2 = \mathbf{Z}[\xi]\langle 1-i\rangle^2 = \langle 1-i\rangle^2\,.$$

Esto es, que el ideal $\langle 2\rangle$ al ser factorizado en ideales primos en $\mathbf{Z}[\xi]$ tiene factores repetidos, y por lo tanto según el teorema 4.24 (el cual se probará en el capítulo 4), el polinomio $f(x) = (x^p-1)/(x-1)$ tiene un factor irreducible módulo 2 , de donde se deduce que también $x^p - 1$ tiene un factor irreducible módulo 2 . Con lo anterior y en combinación con el teorema A.13 del apéndice se tendría que el máximo común divisor de $x^p - 1$ y su derivada no es una unidad en $\mathbf{Z}_2[\mathbf{x}]$, lo cual es absurdo pues claramente la derivada de $x^p - 1$ que es $px^{p-1} = x^{p-1}$ (p es primo impar) es primo relativo con $x^p - 1$ en $\mathbf{Z}_2[\mathbf{x}]$. Por lo tanto $i \notin \mathbf{K}$.

Observemos que como $i = e^{2\pi i/4} \notin \mathbf{K}$, entonces claramente

$$e^{2\pi i/4a} \notin \mathbf{K} \quad \forall\, a \in \mathbf{Z}\,.$$

(b) *Si q es cualquier primo racional impar $q \neq p$, entonces $e^{2\pi i/q} \notin \mathbf{K}$.*
Sea $\eta = e^{2\pi i/q}$. Por el lema 3.1 (a), se tiene que

$$\langle q\rangle = \langle 1-\eta\rangle^{q-1}$$

y procediendo igual que en el inciso (a) se llega a que $e^{2\pi i/q} \notin \mathbf{K}$.

Observemos que como $e^{2\pi i/q} \notin \mathbf{K}$, entonces claramente

$$e^{2\pi i/qb} \notin \mathbf{K} \quad \forall\, b \in \mathbf{Z}$$

(c) $e^{2\pi i/p^2} \notin \mathbf{K}$

Supongamos que $e^{2\pi i/p^2} \in \mathbf{K}$. Claramente $e^{2\pi i/p^2}$ es raíz de $x^{p^2}-1$, pero no de x^p-1. Consideremos el siguiente polinomio

$$f(x) = \frac{x^{p^2}-1}{x^p-1} = \frac{(x^p)^p-1}{x^p-1} = \sum_{j=1}^{p-1} x^{jp} \quad \in \mathbb{Z}[\mathbf{x}] \subset \mathbb{Q}[x] \, .$$

Claramente $e^{2\pi i/p^2}$ es raíz de $f(x)$ y como $f(x)$ es irreducible (ver ejemplos vistos enseguida del teorema A.12 del apéndice), entonces

$$[\mathbb{Q}(e^{2\pi i/p^2}) : \mathbb{Q}] = p(p-1) > p-1 \, ,$$

lo cual es absurdo ya que $\mathbb{Q}(e^{2\pi i/p^2}) \subseteq \mathbb{Q}(e^{2\pi i/p}) = \mathbf{K}$. Por lo tanto $e^{2\pi i/p^2} \notin \mathbf{K}$

Observemos que como $e^{2\pi i/p^2} \notin \mathbf{K}$, entonces claramente

$$e^{2\pi i/p^{2c}} \notin \mathbf{K} \quad \forall\, c \in \mathbf{Z} \, .$$

Regresando ahora a la prueba del lema. Supongamos que la raíz de la unidad $e^{2\pi i/m}$ $(m \in \mathbf{N})$ está en $\mathbf{K}$. Por las observaciones hechas al final de los incisos (a) ,(b) y (c) tenemos que

$$4 \nmid m \quad , \quad q \nmid m \quad , \quad p^2 \nmid m \quad . \tag{3.2}$$

Ahora si $m = p_1^{s_1} \cdots p_r^{s_r}$, $s_1, \ldots, s_r \in \mathbf{Z}$ es la factorización primaria de m en $\mathbb{Z}$, entonces por 3.2 ningún primo impar que aparezca en esta factorización es distinto de p. Por lo tanto cualquier p_i es 2 ó es p. Más aún como $4 \nmid m$ y $p^2 \nmid m$, entonces la factorización primaria de m en $\mathbf{Z}$ tiene la forma

$$m = 2^{\alpha} p^{\beta} \quad , \quad \alpha, \beta \in \mathbf{Z} \quad 0 \leq \alpha, \beta \leq 1$$

de donde se deduce que $m|2p$. Ahora como $2p/m \in \mathbf{Z}$ y 2 , p son primos relativos, entonces existen $r, s \in \mathbf{Z}$ tales que

$$\frac{2p}{m} = 2s + pr \quad \Rightarrow \quad \frac{2\pi i}{m} = \frac{2\pi i s}{p} + \pi i r$$

de aquí que

$$e^{2\pi i/m} \;=\; e^{2\pi i s/p + \pi i r} \;=\; e^{r\pi i} \xi^s \;=\; \pm \xi^s \, .$$

□

Lema 3.3 *Para $\alpha \in \mathbb{Z}[\xi]$ existe $a \in \mathbf{Z}$ tal que $\alpha^p \equiv a \quad (\,mód\ \mathcal{L}^p\,)$*

Demostración : Por la observación hecha enseguida del lema 3.1 tenemos que para $\alpha \in \mathbb{Z}[\xi]$ existe $b \in \mathbb{Z}$ tal que $\alpha \equiv b \pmod{\mathcal{L}}$. Más aún, por la misma observación podemos tomar $b \neq 0$. Por otro lado como

$$x^p - 1 = (x-1)(x-\xi)(x-\xi^2)\cdots(x-\xi^{p-1})$$

evaluando en $x = \alpha/b$ se tiene que

$$\left(\frac{\alpha}{b}\right)^p - 1 = \left(\frac{\alpha}{b} - 1\right)\left(\frac{\alpha}{b} - \xi\right)\cdots\left(\frac{\alpha}{b} - \xi^{p-1}\right)$$

de donde se deduce que

$$\alpha^p - b^p = \prod_{j=0}^{p-1}(\alpha - \xi^j b)\,,$$

y como

$$(\alpha - \xi^j b) - (\alpha - b) = b(1-\xi^j) = b(1-\xi)(1+\xi+\cdots+\xi^{j-1})\,,$$

para $j = 1, 2, \ldots, p-1$ y también $(\alpha - b) - (\alpha - b) = 0 = (1-\xi)0$, entonces

$$(\alpha - \xi^j b) \equiv \alpha - b \equiv 0 \pmod{\mathcal{L}} \quad , \quad j = 0, 1, \ldots, p-1\,,$$

de donde multiplicando concluimos que

$$\alpha^p - b^p = \prod_{j=0}^{p-1}(\alpha - \xi^j b) \equiv 0 \pmod{\mathcal{L}^p}\,.$$

□

Un resultado curioso acerca de los ceros de un polinomio y las raíces de la unidad se da en el siguiente:

Lema 3.4 *Si $p(x) \in \mathbf{Z}[\mathbf{x}]$ es un polinomio mónico, con todos sus ceros en* **C** *de norma o magnitud igual a* 1 *, entonces cualquier cero es una raíz de la unidad.*

Demostración : Si $p(x)$ es un polinomio de grado r. Sean $\alpha_1, \ldots, \alpha_r$ los ceros de $p(x)$. Para cada entero racional $l > 0$ el siguiente polinomio

$$p_l(x) = (x - \alpha_1^l)(x - \alpha_2^l)\cdots(x - \alpha_r^l)$$

se puede escribir como

$$p_l(x) = x^r - a_{l,r-1}x^{r-1} + \cdots (-1)^{r-1}a_{l,1} + (-1)^r a_{l,0}\,,$$

en donde $a_{l,r-j}$ es igual a la suma de todos los distintos productos de j diferentes α_j^l $(j = 1, 2, \ldots, r)$. Igualmente que en el teorema 1.12 tenemos que los números $a_{l,r-j} \in \mathbb{Q}$ $(j = 1, 2, \ldots, r)$ y más aún como $\alpha_1, \ldots, \alpha_r$ son enteros algebraicos, entonces $a_{l,r-j} \in \mathbb{Z}$, y así $p_l(x) \in \mathbb{Z}[\mathbf{x}]$.

Ahora, con un poco de análisis combinatorio se tiene que el número de sumandos en $a_{l,r-j}$ es igual a

$$\binom{r}{j} = \frac{r!}{(r-j)!j!} \ ,$$

entonces

$$| a_{l,r-j} | \leq \binom{r}{j} \quad \text{ya que } | \alpha_1 | = \cdots = | \alpha_r | = 1 \ .$$

Notemos que lo previamente deducido es independiente de l. Por lo tanto sólo puede haber un número finito de polinomios distintos $p_l(x)$. Con lo anterior tenemos que existen $l, m \in \mathbb{Z}, l \neq m$ tales que

$$p_l(x) = p_m(x) \ .$$

De aquí que existe una permutación π de $\{1, \ldots, r\}$ tal que

$$\alpha_j^l = \alpha_{\pi(j)}^m \ ,$$

para $j = 1, \ldots, r$. Inductivamente se encuentra que

$$\alpha_j^{\frac{l^k}{m^{k-1}}} = \alpha_{\pi^k(j)}^m \ ,$$

pero como $\pi^k(j) = j$ para alguna $k \in \mathbb{N}$, entonces $\alpha_j^{l^k} = \alpha_j^{m^k}$. Finalmente como $l \neq m, l^k \neq m^k$, concluimos que α_j es una raíz de la unidad.

□

Ahora si estamos listos para probar el Lema de Kummer

Lema 3.5 ***(Lema de Kummer)*** *Cualquier unidad de* $\mathbb{Z}[\xi]$ *es de la forma* $r\xi^g$ *donde* r *es un real y* g *es un entero racional.*

Demostración : Sea u una unidad en $\mathbb{Z}[\xi]$. Como $\{1, \xi, \ldots \xi^{p-2}\}$ es una base entera de $\mathbb{Z}[\xi]$, entonces $u = e(\xi)$, donde $e(x) \in \mathbb{Z}[\mathbf{x}]$. Ahora para $s = 1, 2, \ldots, p-1$ se tiene que

$$\sigma_s(u) = \sigma_s(e(\xi)) = e(\sigma_s(\xi)) = e(\xi^s) = u_s \in \mathbb{Z}[\xi]$$

es conjugado de u. Ahora como $\pm N_K(u) = \pm u_1 u_2 \cdots u_{p-1} = 1$, se tiene que cada u_s es también una unidad. Por otro lado tenemos que

$$u_{p-s} = e(\xi^{p-s}) = e(\xi^{-s}) = e(\overline{\xi^s}) = \overline{e(\xi^s)} = \overline{u_s} .$$

Por lo tanto

$$u_s u_{p-s} = u_s \overline{u_s} = |\, u_s \,|^2 > 0 ,$$

y como hay $p-1$ u_s' ($p-1$ es par), multiplicando estos por parejas tenemos que

$$N_K(u) = \prod_{i=1}^{\frac{p-1}{2}} u_i u_{p-i} = (u_1 u_{p-1}) \cdots (u_{\frac{p-1}{2}} u_{\frac{p+1}{2}}) > 0$$

por lo tanto

$$N_K(u) = 1$$

Fijemonos ahora en los números u_s/u_{p-s} ($s = 1, \ldots, p-1$). Como el conjunto de todas las unidades conforman un grupo multiplicativo, cada u_s/u_{p-s} es una unidad y claramente tienen magnitud igual a 1. Usando ahora argumentos ya conocidos sobre polinomios simétricos se tiene que

$$f(x) = \prod_{s=1}^{p-1} \Big(x - \frac{u_s}{u_{p-s}} \Big)$$

es un polinomio con coeficientes en $\mathbb{Z}$, y por los lemas 3.2 y 3.4 se tiene que

$$\frac{u_s}{u_{p-s}} = \pm \xi^t \quad , \quad t \in \mathbb{Z}$$

en particular, si $s = 1$:

$$\frac{u}{u_{p-1}} = \pm \xi^t$$

Ahora como p es impar, alguno de t ó $t+p$ es par, y por lo tanto se puede tomar $0 < g \in \mathbb{Z}$ tal que

$$\frac{u}{u_{p-1}} = \pm \xi^{2g} . \tag{3.3}$$

Veamos que *el signo menos no tiene cabida.* Para esto recordemos que cualquier elemento de $\mathbb{Z}[\xi]$ es congruente a un entero racional módulo $\mathcal{L}$ y así para alguna $v \in \mathbb{Z}$, $\xi^{-g} u \equiv v \pmod{\mathcal{L}}$, esto es que

$$\xi^{-g} u - v = (1-\xi) f(\xi) \ , \ f(\xi) \in \mathbb{Z}[\xi] \tag{3.4}$$

tomando el complejo conjugado en ambos lados

$$\xi^g u_{p-1} - v = (1-\bar{\xi})f(\bar{\xi}) = (1-\xi^{p-1})f(\xi^{p-1}) \ , \ \ f(\xi^{p-1}) \in \mathbb{Z}[\xi]$$

pero como $1-\xi^{p-1}$ es un asociado de $1-\xi$, entonces

$$\xi^g u_{p-1} - v = (1-\xi)h(\xi) \ , \ h(\xi) \in \mathbb{Z}[\xi] \tag{3.5}$$

restando miembro a miembro la ecuación 3.4 de la ecuación 3.5 se tiene que

$$\xi^{-g} u - \xi^g u_{p-1} \equiv 0 \ (\text{mód } \mathcal{L}) \ ,$$

de donde

$$\frac{u}{u_{p-1}} \equiv \xi^{2g} \ (\text{mód } \mathcal{L}) \ . \tag{3.6}$$

Si tomamos el signo menos en la ecuación 3.3. Sustituyendo en la ecuación 3.6 se tendría que $2\xi^{2g} \equiv 0 \ \ (\text{mód } \ \mathcal{L})$, es decir que $2\xi^{2g} \in \mathcal{L}$ y de aquí que

$$\begin{aligned} \langle 2\xi^{2g} \rangle = \langle 2 \rangle \langle \xi \rangle^{2g} \subseteq \mathcal{L} \ \ &\Rightarrow \ \ \ \mathcal{L} \mid \langle 2 \rangle \langle \xi \rangle^{2g} \\ &\Rightarrow \ \ N(\mathcal{L}) \mid N(\langle 2 \rangle) N(\langle \xi \rangle)^{2g} \\ &\Rightarrow \ \ \ p \mid 2^{p-1} \ , \end{aligned}$$

lo cual es una contradicción pues p es un primo racional impar.

Por lo tanto $u = \xi^{2g} u_{p-1}$, y de aquí que $\xi^{-g} u = \xi^g u_{p-1}$. Finalmente conjugando: $\overline{\xi^{-g} u} = \overline{\xi^{-g}}\,\overline{u} = \xi^g u_{p-1} = \xi^{-g} u$, de donde se sigue que $\xi^{-g} u \in \mathbb{R}$.

□

Capítulo 4

Métodos analíticos

En este capítulo se definirá lo que es un retículo y se demostrarán importantes resultados relativos a estos, entre los que sobresalen, una caracterización topológica de los retículos. También se define lo que es un dominio fundamental Π asociado a un retículo Γ, y se ve una manera muy sencilla de calcular el volumen de éste.

En este capítulo también se demuestra *el teorema de Minkowski*, importante resultado como se verá en las siguientes secciones y capítulos.

Posteriormente se da una importantísima representación geométrica de los números algebraicos, la cual en combinación con el teorema de Minkowski serán de vital importancia en el capítulo 5.

Para terminar, en este capítulo se define el grupo de clases y se demuestran importantes teoremas que nos sirven para demostrar la finitud de éste. También en el final de este capítulo se le da fin a la clasificación de los campos cuadráticos norma-Euclideos para d negativo.

4.1 Retículos

Definición 4.1 *Si $S = \{v_1, \ldots, v_m\}$ es un conjunto de vectores $\mathbb{R}$-linealmente independientes en $\mathbb{R}^n$ $(m \leq n)$, el subgrupo aditivo de $(\mathbb{R}^n, +)$ generado por las $\mathbb{Z}$-combinaciones lineales de S es llamado un retículo de dimensión m.*

Ejemplo : En $\mathbb{R}^2$ sea $v_1 = (1,0)$ y $v_2 = (0,1)$. Claramente $\{v_1, v_2\}$ es un subconjunto $\mathbb{R}$-linealmente independiente de $\mathbb{R}^2$, entonces el retículo generado por v_1, v_2 es:

$$\Gamma = \{av_1 + bv_2 \ : \ a, b \in \mathbb{Z}\} \ = \ \{(a,0) + (0,b) \ : \ a, b \in \mathbb{Z}\}$$
$$= \ \{(a,b) \ : \ a, b \in \mathbb{Z}\} = \mathbb{Z} \times \mathbb{Z}$$

Claramente un retículo Γ de dimensión m es un grupo abeliano libre de rango m.

Enseguida daremos una caracterización topológica de los retículos. Para esto consideraremos a $\mathbb{R}^n$ como un espacio métrico con la métrica usual. En el transcurso de este capítulo se usará $B_r(x)$ para denotar a la bola abierta con centro en x y radio r, y $\overline{B_r(x)}$ para denotar a su cerradura.

°

Definición 4.2 *Un conjunto no vacío $M \subset \mathbb{R}^n$ se dice que es discreto si, para cualquier $x \in M$, existe $r_x > 0$ tal que $B_{r_x}(x) \cap M = \{x\}$.*

Proposición 4.3 *Para un módulo Γ en $\mathbb{R}^n$ se tiene*

$$\Gamma \text{ es discreto} \iff B_r(0) \cap \Gamma \text{ es finito para todo } r > 0.$$

Demostración : $\Leftarrow$) Si Γ no fuera discreto, entonces existiría $x \in \Gamma$ tal que para toda $r > 0$, $B_r(x) \cap \Gamma \neq \{x\}$, lo cual implica que existe $r_x > 0$ tal que $B_{r_x}(0) \cap \Gamma$ no es finito, lo cual es una contradicción.

$\Rightarrow$) Si Γ es discreto. Afirmamos que Γ es cerrado. En efecto, si Γ no es cerrado, entonces existe $x \in \bar{\Gamma} - \Gamma$ donde $\bar{\Gamma}$ denota la cerradura de Γ. Como se puede encontrar una sucesión $\{x_m\} \subset \Gamma$ tal que $\lim_{m\to\infty} x_m = x$, para cualquier $\epsilon > 0$, existe un entero positivo N tal que $|x_m - x_n| < \epsilon$ siempre que $m, n > N$. Pero como Γ es un módulo $x_m - x_n \in \Gamma$, y así de lo anterior se tiene que $\{0\} \subset B_\epsilon(0) \cap \Gamma$ para cualquier $\epsilon > 0$ lo cual es una contradicción ya que Γ es discreto. Por lo tanto el conjunto $\overline{B_r(0)} \cap \Gamma$ es discreto y compacto, es decir finito, y por lo tanto lo es también $B_r(0) \cap \Gamma$.

□

Teorema 4.4 *Un subgrupo aditivo de $\mathbb{R}^n$ es un retículo si y sólo si éste es discreto.*

Demostración : $\Rightarrow$) Tomemos un retículo Γ de dimensión $m \leq n$ y $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ una base de $\mathbb{R}^n$ tal que Γ esté generado por $\{v_1, \ldots, v_m\}$. Claramente Γ está contenido en el retículo Γ' generado por $\{v_1, \ldots, v_m, \ldots, v_n\}$ y como un subconjunto de un conjunto discreto es claramente discreto, es suficiente que probemos que Γ' es discreto.

Dado que cualquier $v \in \mathbb{R}^n$ tiene representación única como:

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n \quad (\lambda_i \in \mathbb{R}) ,$$

definamos: $f : \mathbb{R}^n \to \mathbb{R}^n$ como

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = (\lambda_1, \ldots, \lambda_n) .$$

Fácilmente se prueba que f es una función lineal, y por lo tanto f es continua en todo punto. Por otro lado sabemos que $\overline{B_r(0)}$ es compacto, y como las imagenes de conjuntos compactos bajo funciones continuas son compactos, entonces $f(\overline{B_r(0)})$ es compacto lo cual implica que $f(\overline{B_r(0)})$ es acotado, esto es que

$$\| f(v) \| \leq k \quad \forall v \in \overline{B_r(0)}, \quad k \in \mathbb{R}^+ .$$

Si $v = a_1 v_1 + \cdots + a_n v_n \in \Gamma' \cap \overline{B_r(0)}$, entonces:

$$\| f(v) \| = \| (a_1, \ldots, a_n) \| \leq k .$$

Esto implica

$$| a_i | \leq \| (a_1, \ldots, a_n) \| \leq k \quad (i = 1, \ldots, n) \tag{4.1}$$

Finalmente como el número de soluciones enteras de la desigualdad 4.1 es finito, entonces $\Gamma' \cap \overline{B_r(0)}$ es finito y por lo tanto Γ' es discreto.

$\Leftarrow$) Sea **G** un subgrupo aditivo discreto de $\mathbb{R}^n$ y $\{v_1, \ldots, v_m\}$ un subconjunto de **G** máximo $\mathbb{R}$-linealmente independiente. Sea Γ el retículo generado por $\{v_1, \ldots, v_m\}$.

Consideremos ahora el siguiente conjunto

$$\Pi = \left\{ v = \sum_{i=1}^{m} \alpha_i v_i \in \mathbb{R}^n \ : \ \alpha_i \in \mathbb{R} \ , \ 0 \leq \alpha_i < 1 \right\}$$

Claramente Π es acotado, y así $\Pi \subseteq B_r(0)$ para alguna $r > 0$.
Ahora por ser $\{v_1, \ldots, v_m\}$ un subconjunto máximo $\mathbb{R}$-linealmente independiente, cualquier $x \in \mathbf{G}$ se puede expresar como

$$x = \sum_{i=1}^{m} \lambda_i v_i \quad \lambda_i \in \mathbb{R} .$$

Si escribimos $\lambda_i = a_i + \alpha_i$ en donde $a_i \in \mathbb{Z}$ y $0 \leq \alpha_i < 1$, entonces

$$x = \sum_{i=1}^{m} a_i v_i + \sum_{i=1}^{m} \alpha_i v_i \in \Gamma + \Pi$$

y como $\Gamma \subseteq \mathbf{G}$ se tiene que

$$\sum_{i=1}^{m} \alpha_i v_i = x - \sum_{i=1}^{m} a_i v_i \in \mathbf{G} \cap \Pi \subseteq \mathbf{G} \cap B_r(0)$$

y como $\mathbf{G} \cap B_r(0)$ es finito porque $\mathbf{G}$ es discreto, existen sólo un número finito de estas sumas. Esto nos muestra que $\mathbf{G}/\Gamma$ es un grupo finito, digamos que $|\ \mathbf{G}/\Gamma\ | = N$, entonces por el teorema de Lagrange se tiene que para cualquier $x \in \mathbf{G}$, $N(x + \Gamma) = \Gamma$ y de aquí que $Nx \in \Gamma$. Con lo anterior se concluye que $\mathbf{G}$ está contenido en el reticulo Γ'' generado por $\{v_1/N, \ldots, v_m/N\}$.

Finalmente como Γ'' es un grupo abeliano libre de rango m, entonces $\mathbf{G}$ es un grupo abeliano libre de rango $l \leq m$. Pero como también $\Gamma \subseteq \mathbf{G}$ y Γ es abeliano libre de rango m, entonces $l = m$ es decir que $\mathbf{G}$ es un retículo de dimensión m.

□

En el transcurso de la demostración anterior se definió el conjunto Π al cual le llamaremos *un dominio fundamental* del retículo Γ de dimensión m generado por $\{v_1, \ldots, v_m\}$.

Lema 4.5 *Si Γ es un retículo de dimensión n, cualquier elemento de $\mathbb{R}^n$ está en exactamente uno de los conjuntos $l + \Pi$ para $l \in \Gamma$.*

Demostración : Si Γ está generado por $\{v_1, \ldots, v_n\}$ y $x \in \mathbb{R}^n$, entonces $x = \sum_{i=1}^{n} \lambda_i v_i$ $(\lambda_i \in \mathbb{R})$. Escribiendo $\lambda_i = a_i + \alpha_i$, $a_i \in \mathbb{Z}$, $0 \leq \alpha_i < 1$ se obtiene que $x = l + t$, $l \in \Gamma, t \in \Pi$. Por lo tanto $x \in l + \Pi$ para $l \in \Gamma$.

Para demostrar que x sólo está en un $l + \Pi$ es suficiente con que probemos que:

$$(r + \Pi) \cap (s + \Pi) = \emptyset\ ,\ r, s \in \Gamma, r \neq s\ .$$

Supongamos que $y \in (r + \Pi) \cap (s + \Pi)$, $r \neq s$, entonces existen $t_1, t_2 \in \Pi$ tales que $r + t_1 = s + t_2$ y de aquí que $r - s = t_2 - t_1 \in \Gamma$. Ahora si t_1, t_2 los escribimos como:

$$\begin{aligned} t_1 &= \textstyle\sum_{i=1}^{n} \alpha_i v_i \ \ ;\ \ 0 \leq \alpha_i < 1 \\ t_2 &= \textstyle\sum_{i=1}^{n} \beta_i v_i \ \ ;\ \ 0 \leq \beta_i < 1 \end{aligned}$$

entonces $\beta_i - \alpha_i \in \mathbb{Z}\ \forall i = 1, \ldots, n$ (esto último es porque $t_2 - t_1 \in \Gamma$). Por otro lado por la forma en que están definidos α_i y β_i se tiene que $|\ \beta_i - \alpha_i\ | < 1$, y así la única opción es que:

$$\beta_i - \alpha_i = 0 \Rightarrow \beta_i = \alpha_i \Rightarrow t_1 = t_2 \Rightarrow r = s$$

lo cual es una contradicción.

□

Un resultado que nos dice cuál es el volumen de un dominio fundamental Π de un retículo Γ se da en el siguiente:

Lema 4.6 *Sea Γ un retículo de dimensión n en $\mathbb{R}^n$ con base $\{v_1, \ldots, v_n\}$. Supongase que*

$$v_i = (a_{1i}, \ldots, a_{ni})$$

Entonces el volumen del dominio fundamental Π de Γ definido por esta base es

$$v(\Pi) = \mid \det(a_{ij}) \mid \ .$$

Demostración : El volumen de Π está dado por

$$v(\Pi) = \int_{\Pi} dx_1 \cdots dx_n \ .$$

Definamos $T : \mathbb{R}^n \to \mathbb{R}^n$ dada por el siguiente cambio de variables

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

El Jacobiano de esta transformación es

$$J = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \det(a_{ij})$$

y Π^* ($T(\Pi^*) = \Pi$) es el dominio fundamental asociado al retículo generado por la base canonica $\{e_1, \ldots, e_n\}$ en $\mathbb{R}^n$, esto es que

$$\Pi^* = \left\{ e = \sum_{i=1}^{n} \alpha_i e_i \in \mathbb{R}^n \ : \ \alpha_i \in \mathbb{R} \ , \ 0 \leq \alpha_i < 1 \right\} .$$

Por lo tanto

$$\begin{aligned} v(\Pi) &= \int_{\Pi^*} \mid \det(a_{ij}) \mid dy_1 \cdots dy_n \\ &= \mid \det(a_{ij}) \mid \int_0^1 dy_1 \cdots \int_0^1 dy_n \\ &= \mid \det(a_{ij}) \mid \ . \end{aligned}$$

□

Como para un retículo Γ existen diferentes $\mathbb{Z}$-bases, entonces existen distintos dominios fundamentales para Γ. Sin embargo, como distintas $\mathbb{Z}$-bases están relacionadas por una matriz unimodular [ver comentario hecho enseguida de la definición A.25 del apéndice], se sigue del lema 4.6 que los volúmenes de estos distintos dominios fundamentales son todos iguales.

4.2 Teorema de Minkowski

El teorema de Minkowski es uno de los resultados más ricos en lo que respecta a este trabajo ya que su poder de alcance en las aplicaciones es sorprendente, como se verá en las secciones y capítulos venideros.

Definición 4.7 *Un subconjunto $X \subseteq \mathbb{R}^n$ se dice que es centralmente simétrico si $-X = X$; es decir si $x \in X$, entonces $-x \in X$.*

Definición 4.8 *Un subconjunto $X \subseteq \mathbb{R}^n$ se dice que es convexo si siempre que $x, y \in X$, entonces $\lambda x + (1-\lambda)y \in X$, para todo número real $\lambda, 0 \leq \lambda \leq 1$.*

Teorema 4.9 ***(Teorema de Minkowski)*** *Sea Γ un retículo de dimensión n en $\mathbb{R}^n$ con dominio fundamental Π, y sea X un subconjunto acotado, convexo y centralmente simétrico de $\mathbb{R}^n$, tal que*

$$vol(X) > 2^n vol(\Pi) .$$

Entonces

$$X \cap (\Gamma - \{0\}) \neq \emptyset .$$

Demostración : Si X_0 es cualquier subconjunto acotado y centralmente simétrico de $\mathbb{R}^n$, entonces el conjunto

$$A = \{l \in \Gamma \ : \ X_0 \cap (\Pi + l) \neq \emptyset\}$$

es finito con un número par de elementos. En efecto, como X_0 y Π son acotados, existe $r > 0$ tal que $X_0 \subseteq B_r(0)$ y $\Pi \subseteq B_r(0)$ y así si tomamos $l \in A$, entonces $\emptyset \neq X_0 \cap (\Pi + l) \subseteq X_0$, por lo tanto existe $t \in \Pi$ tal que $r > \| t + l \| \geq \| l \| - \| t \|$; de aquí que $\| l \| < r + \| t \| < 2r$ de donde se concluye que A es finito y con un número par de elementos pues al ser X_0 centralmente simétrico si $X_0 \cap (\Pi + l) \neq \emptyset$, entonces $X_0 \cap (-\Pi - l) \neq \emptyset$, $-\Pi - l = \Pi + l'$, $l' \in \Gamma$.

Con lo anterior y usando el lema 4.5 tenemos que los conjuntos $X_0 \cap (\Pi + l), l \in A$, conforman una partición del conjunto X_0 y así

$$X_0 = \bigcup_{l \in A} X_0 \cap (\Pi + l)$$

de donde

$$vol(X_0) = \sum_{l \in A} vol(X_0 \cap (\Pi + l)) = \sum_{l \in A} vol((X_0 - l) \cap \Pi) .$$

Ahora, regresamos al conjunto acotado $X \subset \mathbb{R}^n$ el cual es centralmente simétrico y convexo. Poniendo $X_0 = \frac{1}{2}X$; mediante un cálculo muy sencillo se tiene que $vol(X_0) = 2^{-n} vol(X) > vol(\Pi)$. Se afirma que

$$(X_0 - l) \cap (X_0 - l') \neq \emptyset \qquad \text{para algunos } l, l' \in A . \tag{4.2}$$

En efecto, si $(X_0 - l) \cap (X_0 - l') = \emptyset \; \forall l, l' \in A$, entonces se tendría que

$$vol(X_0) = \sum_{l \in A} vol((X_0 - l) \cap \Pi) \leq vol(\Pi)$$

lo cual contradice el hecho que $vol(X_0) > vol(\Pi)$. Por lo tanto de 4.2 se sigue que existen $x, y \in X$ tales que $\frac{1}{2}x - l = \frac{1}{2}y - l'$ y, como $l - l' = \frac{1}{2}x - \frac{1}{2}y = \frac{1}{2}x + (1 - \frac{1}{2})(-y) \in X$, se tiene que $l - l' \in X \cap (\Gamma - \{0\})$.

□

4.3 Representación geométrica de números algebraicos

En esta sección veremos cómo un campo de números $\mathbf{K}$ se puede sumergir en un espacio vectorial de dimensión igual al grado de $\mathbf{K}$, de tal forma que los ideales en $\mathbf{K}$ son mapeados en los retículos de tal espacio vectorial.

Recordemos que en el capítulo 1 se vió que si $\mathbf{K}$ es un campo de números de grado n sobre $\mathbb{Q}$, entonces existen n distintos monomorfismos de $\mathbf{K} \to \mathbb{C}$. Más aún, se vió que s de tales monomorfismos eran reales y $2t$ complejos ($s + 2t = n$). Si el sistema de los n monomorfismos es

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$$

donde $\sigma_1, \ldots, \sigma_s$ son los monomorfismos reales y los restantes los complejos.

Definamos:

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

Fácilmente se puede verificar que $\mathbf{L}^{s,t}$ tiene estructura de espacio vectorial sobre $\mathbb{R}$ con la suma de vectores y el producto por escalares usuales. También $\mathbf{L}^{s,t}$ tiene estructura de anillo con las operaciones suma y producto coordenada a coordenada.

Como espacio vectorial sobre $\mathbb{R}$, $\mathbf{L}^{s,t}$ tiene dimensión $s + 2t = n$ ya que fácilmente se puede probar que una base esta dada por el siguiente conjunto

$$\left\{\begin{array}{rcl} e_1 &=& (1,0,\ldots,0,0,0,\ldots,0) \\ e_2 &=& (0,1,\ldots,0,0,0,\ldots,0) \\ & \vdots & \\ e_s &=& (0,0,\ldots,1,0,0,\ldots,0) \\ e_{s+1} &=& (0,0,\ldots,0,1,0,\ldots,0) \\ e_{s+2} &=& (0,0,\ldots,0,i,0,\ldots,0) \\ & \vdots & \\ e_{s+2t-1} &=& (0,0,\ldots,0,0,0,\ldots,1) \\ e_{s+2t} &=& (0,0,\ldots,0,0,0,\ldots,i) \end{array}\right\} \tag{4.3}$$

en donde $i = \sqrt{-1}$.

Definición 4.10 *Para $x = (x_1,\ldots,x_s,x_{s+1},\ldots,x_{s+t}) \in \mathbf{L}^{s,t}$ se define la norma de éste como*

$$N(x) = x_1\cdots x_s \parallel x_{s+1} \parallel^2 \cdots \parallel x_{s+t} \parallel^2 .$$

Dos propiedades de la norma acabada de definir y que son muy fáciles de verificar son

(a) $N(x) \in \mathbb{R} \quad \forall x \in \mathbf{L}^{s,t}$.

(b) $N(xy) = N(x)N(y) \quad \forall x,y \in \mathbf{L}^{s,t}$.

Definición 4.11 *Si $\mathbf{K}$ es un campo de números de grado n y*

$$\sigma_1,\ldots,\sigma_s,\sigma_{s+1},\ldots,\sigma_{s+t} ,$$

son $s+t$ monomorfismos de $\mathbf{K} \to \mathbf{C}$ como antes clasificados, definimos $\sigma : \mathbf{K} \to \mathbf{L}^{s,t}$ como

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

Claramente se tiene que $\forall\, \alpha,\beta \in \mathbf{K} : r \in \mathbf{Q}$

$$\begin{array}{rcl} \sigma(\alpha+\beta) &=& \sigma(\alpha)+\sigma(\beta) \\ \sigma(\alpha\beta) &=& \sigma(\alpha)\sigma(\beta) \\ \sigma(r\alpha) &=& r\sigma(\alpha) \end{array}$$

pues los σ_i son homomorfismos, es decir que σ es un homomorfismo entre los anillos $\mathbf{K}$ y $\mathbf{L}^{s,t}$, más aún σ es una $\mathbb{Q}$-transformación lineal entre los $\mathbb{Q}$-espacios vectoriales $\mathbf{K}$ y $\mathbf{L}^{s,t}$.

Ahora como el núcleo de σ es un ideal de $\mathbf{K}$ y $\mathbf{K}$ es un campo cuyos únicos ideales son $\mathbf{K}$ y $\{0\}$, entonces σ es identicamente *cero* ó σ es inyectiva, pero como

$$\begin{aligned}\sigma(1) &= (\sigma_1(1),\ldots,\sigma_s(1),\sigma_{s+1}(1),\ldots,\sigma_{s+t}(1)) \\ &= (1,\ldots,1,1,\ldots,1)\neq 0\,,\end{aligned}$$

por lo tanto σ *es inyectiva.*

Teorema 4.12 *Si* $\{\alpha_1,\ldots,\alpha_n\}$ *es una base de* $\mathbf{K}$ *sobre* $\mathbb{Q}$, *entonces* $\sigma(\alpha_1),\ldots,\sigma(\alpha_n)$ *son linealmente independientes sobre* $\mathbb{R}$.

Demostración : Consideremos la ecuación

$$\sum_{j=1}^{n}\lambda_j\sigma(\alpha_j)=0 \quad \lambda_j\in\mathbb{R} \quad (j=1,\ldots,n) \tag{4.4}$$

si denotamos

$$\sigma(\alpha_j)=(x_1^{(j)},\ldots,x_s^{(j)},y_1^{(j)}+iz_1^{(j)},\ldots,y_t^{(j)}+iz_t^{(j)})$$

en donde $i=\sqrt{-1}$ y sustituimos en la ecuación 4.4 se obtiene un sistema de n ecuaciones con n incognitas cuya representación matricial es

$$\begin{pmatrix} x_1^{(1)} & \ldots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \ldots & y_t^{(1)} & z_t^{(1)} \\ \ldots & & \ldots & & \ldots & & & \\ x_1^{(n)} & \ldots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \ldots & y_t^{(n)} & z_t^{(n)} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Este último sistema tiene unicamente la solución trivial si y sólo si el determinante

$$D=\begin{vmatrix} x_1^{(1)} & \ldots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \ldots & y_t^{(1)} & z_t^{(1)} \\ & \ldots & & \ldots & & \ldots & & \\ x_1^{(n)} & \ldots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \ldots & y_t^{(n)} & z_t^{(n)} \end{vmatrix}$$

es distinto de cero. Para probar que $D\neq 0$ apoyémonos en el siguiente determinante

$$E = \begin{vmatrix} x_1^{(1)} & \dots & x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & y_1^{(1)} - iz_1^{(1)} & \dots & y_t^{(1)} + iz_t^{(1)} & y_t^{(1)} - iz_t^{(1)} \\ \dots & & \dots & \dots & \dots & \dots & & \dots \\ x_1^{(n)} & \dots & x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & y_1^{(n)} - iz_1^{(n)} & \dots & y_t^{(n)} + iz_t^{(n)} & y_t^{(n)} - iz_t^{(n)} \end{vmatrix}$$

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

$$= \sqrt{\Delta[\alpha_1, \dots, \alpha_n]}.$$

Pero como se vio en el teorema 1.12 $\Delta[\alpha_1, \dots, \alpha_n] \neq 0$, entonces $E \neq 0$. Ahora por propiedades elementales de los determinantes tenemos que:

$$E = \begin{vmatrix} x_1^{(1)} & \dots & x_s^{(1)} & 2y_1^{(1)} & y_1^{(1)} - iz_1^{(1)} & \dots & 2y_t^{(1)} & y_t^{(1)} - iz_t^{(1)} \\ \dots & & \dots & \dots & \dots & \dots & & \dots \\ x_1^{(n)} & \dots & x_s^{(n)} & 2y_1^{(n)} & y_1^{(n)} - iz_1^{(n)} & \dots & 2y_t^{(n)} & y_t^{(n)} - iz_t^{(n)} \end{vmatrix}$$

$$= \begin{vmatrix} x_1^{(1)} & \dots & x_s^{(1)} & 2y_1^{(1)} & -iz_1^{(1)} & \dots & 2y_t^{(1)} & -iz_t^{(1)} \\ \dots & & \dots & \dots & \dots & \dots & & \dots \\ x_1^{(n)} & \dots & x_s^{(n)} & 2y_1^{(n)} & -iz_1^{(n)} & \dots & 2y_t^{(n)} & -iz_t^{(n)} \end{vmatrix}$$

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

De donde concluimos que $D \neq 0$. Por lo tanto $\lambda_1 = \dots = \lambda_n = 0$, y así $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ son linealmente independientes sobre $\mathbb{R}$.

□

Corolario 4.13 *Elementos* $\mathbb{Q}$*-linealmente independientes de* $\mathbf{K}$ *son mapeados bajo* σ *en elementos* $\mathbb{R}$*-linealmente independientes de* $\mathbf{L}^{s,t}$.

Demostración : Se sigue inmediatamente del hecho que cualquier subconjunto $\mathbb{Q}$-linealmente independiente de $\mathbf{K}$ es parte de una base de $\mathbf{K}$.

□

Corolario 4.14 *Si* $\mathbf{G}$ *es un subgrupo abeliano libre de* $(\mathbf{K}, +)$ *con* $\mathbb{Z}$*-base* $\{\alpha_1, \dots, \alpha_m\}$, *entonces la imagen bajo* σ *de* $\mathbf{G}$ *en* $\mathbf{L}^{s,t}$ *es un retículo de dimensión* m *con generadores* $\sigma(\alpha_1), \dots, \sigma(\alpha_m)$.

Demostración : Si $\mathbf{G}$ es un subgrupo abeliano libre de $(\mathbf{K}, +)$ con $\{\alpha_1, \ldots, \alpha_m\}$ una $\mathbb{Z}$-base de $\mathbf{G}$, entonces fácilmente se comprueba que $\{\alpha_1, \ldots, \alpha_m\}$ son $\mathbb{Q}$-linealmente independientes y por lo tanto por el corolario 4.13 , $\sigma(\alpha_1)$, $\ldots, \sigma(\alpha_m)$ son elementos $\mathbb{R}$-linealmente independientes de $\mathbf{L}^{s,t}$.

□

Observación : Como cualquier ideal $\mathcal{I}$ no nulo de $\mathcal{O}_\mathbf{K}$ es un subgrupo abeliano libre de rango n, entonces $\sigma(\mathcal{I})$ es un retículo en $\mathbf{L}^{s,t}$. Esto es que σ manda ideales de $\mathcal{O}_\mathbf{K}$ en retículos de $\mathbf{L}^{s,t}$.

Para ver el gran poder de alcance en las aplicaciones del teorema de Minkowski en combinación con la *representación geométrica* de $\mathbf{K}$ en $\mathbf{L}^{s,t}$ definida por σ es necesario tener la noción de *distancia* en $\mathbf{L}^{s,t}$. Como $\mathbf{L}^{s,t} \cong \mathbb{R}^{s+2t}$ (como $\mathbb{R}$-espacios vectoriales) la métrica Euclideana usual de $\mathbb{R}^{s+2t}$ la transferiremos a $\mathbf{L}^{s,t}$. Si trabajamos con la base dada en la ecuación 4.3, entonces con respecto a tal base el elemento

$$(x_1, \ldots, x_s, y_1 + iz_1, \ldots, y_t + iz_t) \in \mathbf{L}^{s,t}$$

tiene coordenadas

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

Cambiando un poco la notación, si tomamos

$$\begin{aligned} x &= (u_1, \ldots, u_{s+2t}) \\ y &= (w_1, \ldots, w_{s+2t}) \end{aligned}$$

con respecto a las nuevas coordenadas, entonces el producto interior es definido por

$$x \circ y = u_1 w_1 + \cdots + u_{s+2t} w_{s+2t}$$

La longitud de un vector x es entonces

$$\| x \| = \sqrt{x \circ x}$$

y la distancia entre x y y es $\| x - y \|$.

Regresando a las originales coordenadas de un elemento en $\mathbf{L}^{s,t}$ se tiene, para

$$x = (x_1, \ldots, x_s, y_1 + iz_1, \ldots, y_t + iz_t) ,$$

$$\| x \| = \sqrt{x_1^2 + \cdots + x_s^2 + y_1^2 + z_1^2 + \cdots + y_t^2 + z_t^2} .$$

Teorema 4.15 *Si $\mathbf{K}$ es un campo de números de grado $n = s + 2t$ con anillo de enteros $\mathcal{O}_\mathbf{K}$, y si $0 \neq \mathcal{I}$ es un ideal de $\mathcal{O}_\mathbf{K}$, entonces el volumen de un dominio fundamental de $\sigma(\mathcal{I})$ en $\mathbf{L}^{s,t}$ es igual a*

$$2^{-t} N(\mathcal{I}) \sqrt{|\Delta|}$$

donde Δ es el discriminante de $\mathbf{K}$.

Demostración : Si $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Z}$-base para $\mathcal{I}$, una $\mathbb{Z}$-base para $\sigma(\mathcal{I})$ en $\mathbf{L}^{s,t}$ es por corolario 4.14 $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$, la cual según la notación del teorema 4.12 y trabajando con la base dada en la ecuación 4.3 tienen coordenadas

$$\begin{array}{ccc} (x_1^{(1)}, \ldots, x_s^{(1)}, y_1^{(1)}, z_1^{(1)}, \ldots, y_t^{(1)}, z_t^{(1)}), \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ (x_1^{(n)}, \ldots, x_s^{(n)}, y_1^{(n)}, z_1^{(n)}, \ldots, y_t^{(n)}, z_t^{(n)}). \end{array}$$

Ahora por el lema 4.6 , si Π es un dominio fundamental para $\sigma(\mathcal{I})$, se tiene que

$$v(\Pi) = \mid D \mid$$

donde D es como en el teorema 4.12. Con la notación del teorema 4.12 se tiene que

$$D \;=\; (-2i)^{-t}E \quad \Rightarrow \quad \mid D \mid \;=\; 2^{-t} \mid E \mid .$$

Pero como $E^2 = \Delta[\alpha_1, \ldots, \alpha_n]$, y según el teorema 2.38 ,

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

Sustituyendo todo lo anterior se tiene

$$v(\Pi) = \mid D \mid = 2^{-t}E = 2^{-t}\sqrt{\mid \Delta[\alpha_1, \ldots, \alpha_n] \mid} = 2^{-t}N(\mathcal{I})\sqrt{\mid \Delta \mid} .$$

□

4.4 El grupo de clases

En la sección 0.14 del capítulo 2 se estudió un poco de ideales fraccionales. Se vió que el conjunto $\Im$ de todos los ideales fraccionales no nulos tiene estructura de grupo abeliano con respecto a la multiplicación.

Definición 4.16 *Un ideal fraccional $\mathcal{I} \neq 0$ de $\mathcal{O}_\mathbf{K}$ se dice que es principal si $\mathcal{I} = c^{-1}\mathcal{J}$ donde $\mathcal{J}$ es un ideal principal de $\mathcal{O}_\mathbf{K}$ y $0 \neq c \in \mathcal{O}_\mathbf{K}$.*

Fácilmente se puede probar que el conjunto $\wp$ de todos los ideales fraccionales principales no nulos de $\mathcal{O}_\mathbf{K}$ es un subgrupo de $\Im$.

Definición 4.17 *El grupo de clases h de $\mathcal{O}_K$ es el grupo cociente*

$$h = \Im/\wp = \{[\mathcal{A}] \ : \ \mathcal{A} \in \Im\} ,$$

donde $[\mathcal{A}]$ denota la clase de equivalencia de $\mathcal{A}$.

El orden de h (el cual es finito como se verá en las siguientes secciones) será de vital importancia en el capítulo 4. Para demostrar que h es finito necesitaremos de varias cosas. Primero que nada recordemos que las clases de equivalencia $[\mathcal{A}]$ conforman una partición de $\Im$. Ahora, si $\mathcal{A}$ es un ideal fraccional, entonces $\mathcal{A} = c^{-1}\mathcal{B}$ donde $c \in \mathcal{O}_K$ y $\mathcal{B}$ es un ideal de $\mathcal{O}_K$. De aquí que

$$\mathcal{B} = c\mathcal{A} = (c)\mathcal{A} ,$$

esto es que $\mathcal{A}$ y $\mathcal{B}$ están en el mismo elemento (lo cual lo denotaremos como $\mathcal{A} \equiv \mathcal{B}$) de h. En otras palabras, cualquier clase de equivalencia contiene un ideal de $\mathcal{O}_K$.

La importancia del grupo de clases de un anillo de enteros $\mathcal{O}_K$ es que éste guarda la información necesaria y suficiente para saber si en $\mathcal{O}_K$ se da o no la factorización única en irreducibles. En efecto, ya que entre más pequeño sea el orden del grupo de clases, entonces $\Im$ tiende a ser un grupo con puros ideales fraccionales principales, y por lo tanto $\mathcal{O}_K$ tiende a ser un dominio de ideales principales. En particular se tiene.

Teorema 4.18 *La factorización en $\mathcal{O}_K$ es única si y sólo si el grupo de clases h tiene orden 1.*

Demostración : Se sabe que la factorización en $\mathcal{O}_K$ es única si y sólo si cualquier ideal de $\mathcal{O}_K$ es principal (Teorema 2.45). También cualquier ideal de $\mathcal{O}_K$ es principal si y sólo si cualquier ideal fraccional de $\mathcal{O}_K$ es principal, lo cual es equivalente con $\Im = \wp$, lo cual a su vez es equivalente a que $| h | = 1$. □

4.5 Teoremas de existencia

En esta sección se demostrarán un Lema y un teorema de existencia los cuales serán de gran importancia en el siguiente capítulo y en especial en la siguiente sección donde se demostrará que el orden del grupo de clases es finito.

Lema 4.19 *Si M es un retículo en $\mathbf{L}^{s,t}$ de dimensión $s + 2t$ con dominio fundamental de volumen V, y si $c_1, \ldots, c_{s+t}$ son números reales positivos cuyo*

producto

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

entonces existe $0 \neq x = (x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+t})$ *en* M *tal que*

$$\begin{gathered} |\, x_1 \,| < c_1, \ldots, |\, x_s \,| < c_s; \\ |\, x_{s+1} \,|^2 < c_{s+1}, \ldots, |\, x_{s+t} \,|^2 < c_{s+t}. \end{gathered}$$

$x_1, \ldots, x_s \in \mathbb{R}$ *y* $x_{s+1}, \ldots, x_{s+t} \in \mathbb{C}$.

Demostración : Sea X el subconjunto de todos los puntos $x \in \mathbf{L}^{s,t}$ para los cuales la conclusión se sigue. Claramente X es acotado, simétrico y convexo pues X es el producto cartesiano de

$$\begin{aligned} (-c_1, c_1) \times \cdots \times (-c_s, c_s) \times \{y_1 + iz_1 \in \mathbb{C} \,:\, y_1^2 + z_1^2 < c_{s+1}\} \times \cdots \\ \cdots \{y_t + iz_t \in \mathbb{C} \,:\, y_t^2 + z_t^2 < c_{s+t}\} \end{aligned}$$

y el volumen de X es

$$\begin{aligned} v(X) &= \int_{-c_1}^{c_1} dx_1 \cdots \int_{-c_s}^{c_s} dx_s \\ &\quad \cdot \int\int_{y_1^2+z_1^2<c_{s+1}} dy_1 dz_1 \cdots \\ &\quad \cdot \int\int_{y_t^2+z_t^2<c_{s+t}} dy_t dz_t \\ &= 2c_1 \cdot 2c_2 \cdots 2c_s \cdot \pi c_{s+1} \cdots \pi c_{s+t} \\ &= 2^s \pi^t c_1 \cdots c_{s+t} . \end{aligned}$$

Por el teorema de Minkowski sólo tenemos que probar que $v(X) > 2^{s+2t}$ para garantizar la existencia de $0 \neq x \in M \cap X$. Esto último se sigue inmediatamente ya que por hipótesis

$$c_1 \cdots c_{s+t} \;>\; \left(\tfrac{4}{\pi}\right)^t V \;=\; \tfrac{2^{2t}}{\pi^t} V \;\Rightarrow\; v(X) > 2^{s+2t} V .$$

□

Teorema 4.20 *Sea* $\mathbf{K}$ *un campo de números de grado* n , $\mathcal{I}$ *un ideal no nulo de* $\mathcal{O}_{\mathbf{K}}$. *Entonces existe* $0 \neq \alpha \in \mathcal{I}$ *tal que*

$$|\, N_K(\alpha) \,| \leq \left(\frac{4}{\pi}\right)^t \left(\frac{n!}{n^n} \,|\, \Delta \,|^{1/2} \, N(\mathcal{I})\right) = M_{\mathbf{K}} N(\mathcal{I}) ,$$

donde Δ *es el discriminante y* $M_{\mathbf{K}} = (4/\pi)^t n! n^{-n} \,|\, \Delta \,|^{1/2}$ *es la constante de Minkowski de* $\mathbf{K}$.

Demostración : Consideremos el retículo $M = \sigma(\mathcal{I})$ en $\mathbf{L}^{s,t}$ [ver corolario 4.14]. Por el teorema 4.15 si Π es un dominio fundamental de M, entonces $v(\Pi) = 2^{-t}N(\mathcal{I}) \mid \Delta \mid^{1/2}$.

Por otro lado, sea $\rho > 0$ tal que

$$2^s(\pi/2)^t(1/n!)\rho^n = 2^n v(\Pi)\,. \tag{4.5}$$

Para cualquier $\epsilon > 0$, definamos

$$X_\epsilon = \{x \in \mathbf{L}^{s,t} : \mid x_1 \mid + \cdots + \mid x_s \mid + 2 \mid x_{s+1} \mid + \cdots + 2 \mid x_{s+t} \mid < \rho + \epsilon\}\,.$$

El volumen de este conjunto (ver [3], pag. 76) es:

$$v(X_\epsilon) = 2^s(\pi/2)^t(1/n!)(\rho+\epsilon)^n. \tag{4.6}$$

Ahora, de 4.5 y 4.6, se encuentra que

$$v(X_\epsilon) > 2^n v(\Pi)\,.$$

Como X_ϵ es acotado, centralmente simétrico y convexo (como fácilmente se puede verificar), entonces por el teorema de Minkowski existe $0 \neq x \in M \cap X_\epsilon$. Pero como $M = \sigma(\mathcal{I})$ y σ es inyectiva, entonces existe $0 \neq \alpha \in \mathcal{I}$ tal que

$$\mid \sigma_1(\alpha) \mid + \cdots + \mid \sigma_s(\alpha) \mid + 2 \mid \sigma_{s+1}(\alpha) \mid + \cdots + 2 \mid \sigma_{s+t}(\alpha) \mid < \rho + \epsilon\,. \tag{4.7}$$

Sea A_ϵ el conjunto de $0 \neq \alpha \in \mathcal{I}$ que satisfacen la desigualdad 4.7. Como $\sigma(\mathcal{I})$ es discreto y X_ϵ es acotado, entonces A_ϵ es finito y no vacío. Si tomamos $\epsilon < 1$, entonces A_ϵ es un subconjunto cerrado del conjunto compacto A_1. Por lo tanto $A = \bigcap_{\epsilon<1} A_\epsilon \neq \emptyset$. Si tomamos $\alpha \in A$, entonces

$$\mid \sigma_1(\alpha) \mid + \cdots + \mid \sigma_s(\alpha) \mid + 2 \mid \sigma_{s+1}(\alpha) \mid + \cdots + 2 \mid \sigma_{s+t}(\alpha) \mid \leq \rho\,.$$

Por otro lado para $\alpha \in A$ tenemos que

$$\begin{aligned}
\mid N_K(\alpha) \mid^{1/n} &= \mid \sigma_1(\alpha) \cdots \sigma_s(\alpha) \mid \sigma_{s+1}(\alpha) \mid^2 \cdots \mid \sigma_{s+t}(\alpha) \mid^2 \mid^{1/n} \\
&= (\mid \sigma_1(\alpha) \mid \cdots \mid \sigma_s(\alpha) \mid\mid \sigma_{s+1}(\alpha) \mid\mid \sigma_{s+1}(\alpha) \mid \cdots \\
&\qquad \cdots \mid \sigma_{s+t}(\alpha) \mid\mid \sigma_{s+t}(\alpha) \mid)^{1/n} \\
&\leq (1/n)(\mid \sigma_1(\alpha) + \cdots + \sigma_s(\alpha) + 2 \mid \sigma_{s+1}(\alpha) \mid + \cdots \\
&\qquad \cdots + 2 \mid \sigma_{s+t}(\alpha) \mid) \\
&\leq \rho/n\,,
\end{aligned}$$

de donde se tiene que $\mid N(\alpha) \mid \leq n^{-n}\rho^n$. Finalmente sustituyendo los valores de ρ^n de la igualdad 4.5 y el de $v(\Pi)$ se concluye que

$$| N_K(\alpha) | \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} | \Delta |^{1/2} N(\mathcal{I}) = M_{\mathbf{K}} N(\mathcal{I})$$

□

Corolario 4.21 *Cualquier clase de ideales fraccionales contiene un ideal $\mathcal{I}$ tal que $N(\mathcal{I}) \leq M_{\mathbf{K}}$ ($M_{\mathbf{K}}$ la constante de Minkowski).*

Demostración : Sea $[\mathcal{C}]$ cualquier clase de ideales fraccionales en $\Im/\wp$, y $\mathcal{J} \subseteq \mathcal{O}_{\mathbf{K}}$ un ideal en la clase $[\mathcal{C}]^{-1}$. Por el Teorema previo, existe $0 \neq \alpha \in \mathcal{J}$ tal que $| N(\alpha) | \leq N(\mathcal{J}) M_{\mathbf{K}}$. Ahora como $\mathcal{J} | (\alpha)$, entonces existe un ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbf{K}}$ tal que

$$(\alpha) = \mathcal{I}\mathcal{J} \ . \tag{4.8}$$

Tomando normas en la igualdad 4.8

$$N(\mathcal{I})N(\mathcal{J}) = N(\mathcal{I}\mathcal{J}) = N((\alpha)) = | N_K(\alpha) | \leq N(\mathcal{J}) M_{\mathbf{K}} \ \Rightarrow \ N(\mathcal{I}) \leq M_{\mathbf{K}}.$$

Afirmación: $\mathcal{I}$ es el ideal buscado. En efecto, ya que $\mathcal{J}^{-1} \in [\mathcal{C}]$, por 4.8 se tiene que $\mathcal{I}$ y $\mathcal{J}^{-1}$ están en la misma clase de equivalencia.

□

Observación : Si $M_{\mathbf{K}} < 2$ para un campo de números $\mathbf{K}$, cualquier clase de ideales fraccionales debe contener un ideal $\mathcal{I}$ en $\mathcal{O}_{\mathbf{K}}$ tal que $N(\mathcal{I}) = 1$, es decir que $\mathcal{I} = \mathcal{O}_{\mathbf{K}}$. Por lo tanto se tiene que $h = 1$.

Para referencias a futuro tenemos la siguiente tabla, tomada de [3], pag. 79

n	s	t	M_{st}
2	0	1	0.637
2	2	0	0.500
3	1	1	0.283
3	3	0	0.223
4	0	2	0.152
4	2	1	0.120
4	4	0	0.094
5	1	2	0.063
5	3	1	0.049
5	5	0	0.039

Donde

$$M_{st} = \left(\frac{4}{\pi}\right)^t \frac{(s+2t)!}{(s+2t)^{s+2t}}$$

está dado en la última columna en forma aproximada.

4.6 Finitud del grupo de clases

Teorema 4.22 *El grupo de clases de un campo de números* $\mathbf{K}$ *es un grupo abeliano finito.*

Demostración : Ya sabemos que el grupo de clases $\hbar = \Im/\wp$ es un grupo abeliano. Por lo tanto sólo resta probar que $\hbar$ es finito, lo cual es cierto si y sólo si el número de distintas clases de equivalencia de ideales fraccionales es finito. Sea $[\mathcal{C}]$ una clase de equivalencia, entonces por el corolario 4.21, $[\mathcal{C}]$ contiene un ideal $\mathcal{I}$ tal que $N(\mathcal{I}) \leq M_{\mathbf{K}}$ ($M_{\mathbf{K}}$ la constante de Minkowski). Pero como el Teorema 2.42 (c) nos dice que sólo un número finito de ideales tienen norma dada, entonces sólo un número finito de ideales tienen norma menor o igual que $M_{\mathbf{K}}$. Por lo tanto sólo existe un número finito de clases de equivalencia $[\mathcal{C}]$.

□

Al orden h del grupo de clases se le llama *el número de clase de* $\mathbf{K}$.

Proposición 4.23 *Sea* $\mathbf{K}$ *un campo de números con número de clase* h, *y sea* $\mathcal{I}$ *un ideal del anillo de enteros* $\mathcal{O}_{\mathbf{K}}$, *entonces*

(a) $\mathcal{I}^h$ *es principal,*
(b) Si q *es primo con* h, *e* $\mathcal{I}^q$ *es principal, entonces* $\mathcal{I}$ *es principal.*

Demostración : (a) Como $\mid \hbar \mid = h$, y $[\mathcal{O}_{\mathbf{K}}]$ es el neutro multiplicativo de $\hbar$, entonces por el teorema de Lagrange $[\mathcal{I}^h] = [\mathcal{I}]^h = [\mathcal{O}_{\mathbf{K}}]$, esto es que $\mathcal{I}^h \equiv \mathcal{O}_{\mathbf{K}}$, lo cual implica que $\mathcal{I}^h$ es principal.
(b) Como h y q son primos relativos, entonces existen $a, b \in \mathbf{Z}$ tales que $ah + bq = 1$. Ahora como $[\mathcal{I}]^q$ es principal, entonces $[\mathcal{I}]^q = [\mathcal{O}_{\mathbf{K}}]$, y así

$$\begin{aligned} [\mathcal{I}] &= [\mathcal{I}]^{ah+bq} \\ &= ([\mathcal{I}]^h)^a([\mathcal{I}]^q)^b \\ &= [\mathcal{O}_{\mathbf{K}}]^a[\mathcal{O}_{\mathbf{K}}]^b \\ &= [\mathcal{O}_{\mathbf{K}}] \end{aligned}$$

de donde concluimos que $\mathcal{I}$ es principal.

□

4.7 Factorización de un ideal principal generado por un primo racional

Si p es un primo racional, en general no es cierto que $\langle p\rangle$ es un ideal primo en el anillo de enteros $\mathcal{O}_{\mathbf{K}}$ de un campo de números $\mathbf{K}$. A continuación veremos que cuando tenemos un campo de números $\mathbf{K}$ con anillo de enteros generado (como grupo aditivo) por un sólo elemento (como los campos cuadráticos y ciclotómicos) el siguiente teorema debido a Dedekind es decisivo respecto a la primalidad de $\langle p\rangle$.

Teorema 4.24 *(Lema de Hensel). Sea* $\mathbf{K}$ *un campo de números de grado* n*, con anillo de enteros* $\mathcal{O}_{\mathbf{K}} = \mathbf{Z}[\theta]$ *generado por* θ*. Dado un primo racional* p*, supóngase que el polinomio mínimo* f *de* θ *sobre* $\mathbf{Q}$ *se factoriza en irreducibles sobre* $\mathbf{Z}_p$ *como*

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

donde las barras denotan el mapeo natural $\mathbf{Z}[\mathbf{x}] \to \mathbf{Z}_p[\mathbf{x}]$*. Entonces si* f_i *es cualquier polinomio irreducible que es mapeado en* $\bar{f}_i$*, el ideal*

$$\mathcal{P}_i = \langle p\rangle + \langle f_i(\theta)\rangle$$

es primo y la factorización en ideales primos de $\langle p\rangle$ *en* $\mathcal{O}_{\mathbf{K}}$ *es*

$$\langle p\rangle = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$$

Demostración : Sea θ_i una raíz de $\bar{f}_i(x)$ en $\mathbf{Z}_p[\mathbf{x}]$. Notemos que $\mathbf{Z}_p[\theta_i] \cong \mathbf{Z}_p[\mathbf{x}]/(\bar{f}_i)$. En efecto, ya que si definimos $\varphi : \mathbf{Z}_p[\mathbf{x}] \to \mathbf{Z}_p[\theta_i]$ como $\varphi(f(x)) = \varphi(f(\theta_i))$, fácilmente se verifica que φ es un homomorfismo de anillos suprayectivo con $\ker\varphi = \langle \bar{f}_i\rangle$, de donde se sigue lo afirmado. También $\mathbf{Z}_p[\theta_i]$ es un campo ya que al ser $\bar{f}_i$ irreducible, entonces $\mathbf{Z}_p[\mathbf{x}]/\langle \bar{f}_i\rangle$ es un campo.
Definamos ahora $v_i : \mathbf{Z}[\theta] \to \mathbf{Z}_p[\theta_i]$ dado por

$$v_i(g(\theta)) = \bar{g}(\theta_i) .$$

Fácilmente se verifica que v_i es un homomorfismo de anillos. Además claramente v_i es suprayectivo. Por lo tanto $\mathbf{Z}[\theta]/\ker v_i \cong \mathbf{Z}_p[\theta_i]$, pero como $\mathbf{Z}[\theta_i]$ es un campo, entonces $\ker v_i$ es un ideal primo de $\mathbf{Z}[\theta]$. Ahora afirmamos que

$$\ker v_i = \langle p\rangle + \langle f_i(\theta)\rangle.$$

En efecto, ya que si $g(\theta) \in \langle p\rangle + \langle f_i(\theta)\rangle$, entonces

$$\begin{aligned} g(\theta) = ph(\theta) + f_i(\theta)q(\theta) \quad &\Rightarrow \quad v_i(g(\theta)) = \overline{(ph)}(\theta_i) + \bar{f}_i(\theta_i)\bar{q}(\theta_i) = 0 \\ &\Rightarrow \quad \langle p\rangle + \langle f_i(\theta)\rangle \subseteq \ker v_i . \end{aligned}$$

Por otro lado si $g(\theta) \in \ker v_i$, entonces $\bar{g}(\theta_i) = 0$, pero como $\bar{f}_i(\theta_i) = 0$, y $\bar{f}_i$ es irreducible, entonces $\bar{g} = \bar{f}_i\bar{h}$ para algún $\bar{h} \in \mathbf{Z}_p[\mathbf{x}]$; esto significa que $g - f_i h \in \mathbf{Z}[\mathbf{x}]$ tiene coeficientes divisibles por p. Por lo tanto

$$g(\theta) = (g(\theta) - f_i(\theta)h(\theta)) + f_i(\theta)h(\theta) \in \langle p \rangle + \langle f_i(\theta) \rangle$$
$$\Rightarrow \ker v_i \subseteq \langle p \rangle + \langle f_i(\theta) \rangle .$$

Si llamamos $\mathcal{P}_i = \langle p \rangle + \langle f_i(\theta) \rangle$, entonces para cada $\bar{f}_i$ el ideal $\mathcal{P}_i$ es primo y satisface $\langle p \rangle \subseteq \mathcal{P}_i$, es decir que $\mathcal{P}_i | \langle p \rangle$.

Ahora por la proposición A.5 del apéndice tenemos que

$$\mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r} \subseteq \langle p \rangle + \langle f_1^{e_1}(\theta) \cdots f_r^{e_r}(\theta) \rangle \subseteq \langle p \rangle + \langle f(\theta) \rangle = \langle p \rangle .$$

Por lo tanto $\langle p \rangle | \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$. Ahora si $\mathcal{J}$ es un ideal primo tal que $\mathcal{J} | \langle p \rangle$, entonces $\mathcal{J}$ tiene que ser uno de los $\mathcal{P}_i$. En efecto, ya que

$$\mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r} = \langle p \rangle \mathcal{A} = \mathcal{J}\mathcal{B}\mathcal{A} \quad , \quad \mathcal{A}, \mathcal{B} \quad \text{ideales}$$

pero como $\mathcal{J}$ es primo, entonces $\mathcal{J}$ divide a alguno de los $\mathcal{P}_i$; pero como en $\mathcal{O}_\mathbf{K} = \mathbf{Z}[\theta]$ los ideales primos coinciden con los maximales, entonces $\mathcal{J} = \mathcal{P}_i$ para alguna $i = 1, \ldots, r$. Lo anterior muestra que los únicos factores primos de $\langle p \rangle$ son $\mathcal{P}_1, \ldots, \mathcal{P}_r$ y por lo tanto

$$\langle p \rangle = \mathcal{P}_1^{k_1} \cdots \mathcal{P}_r^{k_r} \ , \ 0 < k_i \leq e_i \quad (1 \leq i \leq r) . \tag{4.9}$$

Tomando normas en la anterior ecuación

$$N(\langle p \rangle) = N^{k_1}(\mathcal{P}_1) \cdots N^{k_r}(\mathcal{P}_r) .$$

Ahora como $\mathbf{Z}[\theta]/\mathcal{P}_i \cong \mathbf{Z}_p[\theta_i]$ y $N(\mathcal{P}_i) = | \mathcal{O}_\mathbf{K}/\mathcal{P}_i |$, entonces $N(\mathcal{P}_i) = | \mathbf{Z}_p[\theta_i] |$, donde

$$\mathbf{Z}_p[\theta_i] = \left\{ \sum_{j=0}^{d_i - 1} a_j \theta_i^j \ : \ a_j \in \mathbf{Z}_p \ , \ d_i = \partial(\bar{f}_i) = \partial(f_i) \right\} ,$$

esto es que $N(\mathcal{P}_i) = d_i$. También

$$N(\langle p \rangle) = | N(p) | = p^n .$$

Con todo lo anterior se tiene que

$$p^n = N(\langle p \rangle) = N^{k_1}(\mathcal{P}_1) \cdots N^{k_r}(\mathcal{P}_r) = p^{d_1 k_1 + \cdots + d_r k_r} ,$$

lo cual implica que

$$d_1 k_1 + \cdots + d_r k_r = n = d_1 e_1 + \cdots + d_r e_r ,$$

de aquí que

$$d_1(e_1 - k_1) + \cdots + d_r(e_r - k_r) = 0 , \tag{4.10}$$

pero de la ecuación 4.9 se tiene que $e_i - k_i \geq 0$, y así 4.10 sólo puede suceder si $e_i = k_i$ $(1 \leq i \leq r)$. Por lo tanto

$$\langle p \rangle = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r} .$$

□

Teorema 4.25 *Sea $\mathcal{O}_{\mathbf{K}}$ el anillo de enteros de un campo de números $\mathbf{K}$ de grado $n = s + 2t$. Supóngase que para cualquier primo $p \in \mathbb{Z}$ con*

$$p \leq M_{\mathbf{K}}$$

(Δ es el discriminante de $\mathbf{K}$ y $M_{\mathbf{K}}$ es la constante de Minkowski), cualquier ideal primo que divide a $\langle p \rangle$ es principal, entonces $\mathcal{O}_{\mathbf{K}}$ tiene número de clase $h = 1$.

Demostracion : Sea $[\mathcal{J}]$ cualquier clase de ideales fraccionales. Por el Corolario 4.21 en $[\mathcal{J}]$ existe un ideal $\mathcal{I}$ tal que $N(\mathcal{I}) \leq M_{\mathbf{K}}$. Ahora, como $N(\mathcal{I}) \in \mathbb{N}$, entonces.

$$N(\mathcal{I}) = p_1 \cdots p_k \leq M_{\mathbf{K}} ,$$

donde $p_1, \ldots, p_k \in \mathbb{Z}$ son primos racionales, y $p_i \leq M_{\mathbf{K}}$. Por otro lado como $N(\mathcal{I}) \in \mathcal{I}$, entonces

$$\mathcal{I} | (N(\mathcal{I})) = (p_1) \cdots (p_k) . \tag{4.11}$$

Si factorizamos en ideales primos a $\mathcal{I}$

$$\mathcal{I} = \mathcal{Q}_1 \cdots \mathcal{Q}_s \qquad \mathcal{Q}_i \text{ ideal primo } 1 \leq i \leq s ,$$

por la igualdad 4.11 tenemos que $\mathcal{Q}_i | \langle p_1 \rangle \cdots \langle p_k \rangle (1 \leq i \leq s)$, lo cual implica que $\mathcal{Q}_j$ divide a algún $\langle p_j \rangle$, entonces por hipótesis $\mathcal{Q}_j$ es un ideal principal, y por lo tanto lo es también $\mathcal{I}$.

Resumiendo, tenemos que cualquier clase de ideales fraccionales es igual a $[\mathcal{O}_{\mathbf{K}}]$.

□

4.8 Cálculo del número de clase en casos muy particulares

El teorema 4.24 en combinación con el teorema 4.25 nos provee de una muy buena técnica para calcular el número de clase para campos de números $\mathbf{K}$ de grado pequeño, con anillo de enteros $\mathcal{O}_{\mathbf{K}}$ de discriminante también pequeño.

En los siguientes ejemplos aparte de hacer uso de los teoremas ya mensionados, también se usarán los valores de M_{st} dados en la tabla que está al final de la sección 4.5. Notemos que la constante de Minkowski $M_{\mathbf{K}}$ es igual a $M_{st}\sqrt{|\Delta|}$.

Ejemplo 1. $\mathbf{K} = \mathbb{Q}(\sqrt{-19})$: El anillo de enteros es $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\theta]$ donde θ es un cero de

$$f(x) = x^2 - x + 5\,,$$

y el discriminante es 19. Entonces $M_{\mathbf{K}} \leq 0.637\sqrt{19}$, y así el único primo racional menor que $M_{\mathbf{K}}$ es 2. Ahora usando el teorema 4.25: módulo 2, $f(x)$ es irreducible, por lo tanto

$$\mathcal{P}_1 = \langle 2\rangle + \langle f(\theta)\rangle = \langle 2\rangle$$

es un ideal primo en $\mathcal{O}_{\mathbf{K}}$, de aquí que cualquier ideal primo que divida a $\langle 2\rangle$ es igual a $\langle 2\rangle$, el cual es principal. Por lo tanto $h = 1$.

Ejemplo 2. $\mathbf{K} = \mathbb{Q}(\sqrt{-43})$: Esto es similar, pero ahora

$$f(x) = x^2 - x + 11\,,$$

y $M_{\mathbf{K}} \leq 0.637\sqrt{-43}$, y así los únicos primos racionales menores que $M_{\mathbf{K}}$ son 2 y 3. Pero $f(x)$ es irreducible módulo 2 ó 3.

Ejemplo 3. $\mathbf{K} = \mathbb{Q}(\sqrt{-67})$: Para éste,

$$f(x) = x^2 - x + 17\,,$$

y $M_{\mathbf{K}} \leq 0.637\sqrt{67}$, por lo cual sólo hay que trabajar con los primos racionales ≤ 5. Pero $f(x)$ es irreducible módulo 2, 3 ó 5.

Ejemplo 4. $\mathbf{K} = \mathbb{Q}(\sqrt{-163})$: Para éste,

$$f(x) = x^2 - x + 41\,,$$

y $M_{\mathbf{K}} \leq 0.637\sqrt{163}$, por lo cual sólo hay que trabajar con los primos racionales ≤ 8. Pero $f(x)$ es irreducible módulo 2, 3, 5 ó 7.

Ejemplo 5. $\mathbf{K} = \mathbb{Q}(\sqrt{2})$: Para éste,

$$f(x) = x^2 - 2\,,$$

y $M_{\mathbf{K}} \leq 0.500\sqrt{8} < 2$. Por lo tanto $h = 1$ [ver observación hecha enseguida del corolario 4.21].

Ejemplo 6. $\mathbf{K} = \mathbb{Q}(\sqrt{3})$: Para éste,

$$f(x) = x^2 - 3\,,$$

y $M_{\mathbf{K}} \leq 0.500\sqrt{12} < 2$. Por lo tanto $h = 1$.

Ejemplo 7. $\mathbf{K} = \mathbb{Q}(\xi)$, donde $\xi^3 = 1$: Para éste caso tenemos que $\mathbf{K} = \mathbb{Q}(\sqrt{-3})$. Por lo tanto $h = 1$ [ver teorema 2.25].

Ejemplo 8. $\mathbf{K} = \mathbb{Q}(\xi)$, donde $\xi^5 = 1$: Para éste, ξ es raíz de

$$f(x) = x^4 + x^3 + x^2 + x + 1 \qquad \text{irreducible en } \mathbf{Z}[\mathbf{x}]$$

Aquí $n = 4, s = 0, t = 2$; y $\Delta = 125$ [ver teorema 1.35], además $M_{\mathbf{K}} \leq 0.152\sqrt{125} < 2$. Por lo tanto $h = 1$

Ejemplo 9. $\mathbf{K} = \mathbb{Q}(\xi)$, donde $\xi^7 = 1$: Para éste, ξ es raíz de

$$f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \qquad \text{irreducible en } \mathbf{Z}[\mathbf{x}]$$

Aquí $n = 6, s = 0, t = 3$; y $\Delta = -7^5$, además $M_{\mathbf{K}} \leq 3$, y así los únicos primos racionales menores o iguales que $M_{\mathbf{K}}$ son 2 y 3.

Módulo 2, $f(x)$ se factoriza como

$$(x^4 + x^2 + 1)(x^3 + x + 1)\,.$$

Por lo tanto $\langle 2\rangle = \mathcal{P}_1\mathcal{P}_2$ donde $\mathcal{P}_1, \mathcal{P}_2$ son ideales primos distintos [ver teorema 4.24]. Más aún, como

$$(\xi^3 + \xi^2 + 1)(\xi^3 + \xi + 1)\xi^4 = 2\,,$$

se tiene que

$$\langle 2\rangle = \langle \xi^3 + \xi^2 + 1\rangle\langle \xi^3 + \xi + 1\rangle$$

y por lo tanto $\mathcal{P}_1, \mathcal{P}_2$ son principales.

Módulo 3, $f(x)$ es irreducible, por lo tanto $\langle 3\rangle$ es primo, y así cualquier ideal primo que lo divida tiene que ser igual a $\langle 3\rangle$ que es principal.

Finalmente por el teorema 4.25 tenemos que $h = 1$.

Combinando lo obtenido en los ejemplos 1, 2, 3 y 4 con el teorema 2.25 se tiene.

Teorema 4.26 *El número de clase de* $\mathbb{Q}(\sqrt{d})$ *es igual a* 1 *para* d= -1,-2, -3,-5,-11,-19,-43,-67,-163.

□

En el capítulo 2 sección 2.3, se mencionó que para $d < 0$, el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ tiene factorización única en irreducibles o equivalentemente número de clase 1 si y sólo si d toma alguno de los valores dados en el teorema 4.26 . Por lo tanto, comparando el teorema previo con el teorema 2.26 obtenemos el interesante

Corolario 4.27 *Existen anillos de enteros en los cuales se dá la factorización única en irreducibles pero que no son Euclideanos; por ejemplo los anillos de enteros de* $\mathbb{Q}(\sqrt{d})$ *para* d= -19,-43,-67,-163 .

□

Capítulo 5

El teorema de las unidades de Dirichlet

5.1 El espacio logarítmico

Sea $\mathbf{K}$ un campo de números de grado n. Si $(\mathbf{L}^{s,t})^* = (\mathbb{R}^*)^s \times (\mathbb{C}^*)^t$ y $x = (x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+t}) \in (\mathbf{L}^{s,t})^*$, definimos $\ell : (\mathbf{L}^{s,t})^* \to \mathbb{R}^{s+t}$ como

$$\ell(x) = (\log \mid x_1 \mid, \ldots, \log \mid x_s \mid, \log \mid x_{s+1} \mid^2, \ldots, \log \mid x_{s+t} \mid^2)$$

Fácilmente se puede probar que $(\mathbf{L}^{s,t})^*$ es un grupo bajo la multiplicación coordenada a coordenada.

Teorema 5.1 *El mapeo ℓ definido previamente es un homomorfismo suprayectivo.*

Demostración : Es inmediata por las propiedades de las funciones logarítmicas

□

Ahora definamos $l : \mathbf{K}^* \to \mathbb{R}^{s+t}$ por

$$\alpha \to l(\alpha) = (\ell \circ \sigma)(\alpha) = \ell(\sigma(\alpha))$$

donde $\mathbf{K}^* = \mathbf{K} - \{0\}$ ($\mathbf{K}$ un campo de números de grado $n = s + 2t$), σ, ℓ son los mapeos definidos en el capítulo 4 sección 4.3 y al principio de esta sección respectivamente. Más explícitamente tenemos que

$$l(\alpha) = (\log \mid \sigma_1(\alpha) \mid, \ldots, \log \mid \sigma_s(\alpha) \mid, \log \mid \sigma_{s+1}(\alpha) \mid^2, \ldots, \log \mid \sigma_{s+t}(\alpha) \mid^2)$$

El mapeo l es llamado *la representación logarítmica* de $\mathbf{K}^*$ y $\mathbb{R}^{s+t}$ es llamado *el espacio logarítmico.*

Como σ y ℓ son homomorfismos, l es un homomorfismo entre el grupo multiplicativo $\mathbf{K}^*$ y el grupo aditivo $\mathbb{R}^{s+t}$.

Observemos que si hacemos

$$l_i(\alpha) = \begin{cases} \log | \sigma_i(\alpha) | & \text{si } i = 1, \ldots, s \\ \log | \sigma_i(\alpha) |^2 & \text{si } i = s+1, \ldots, s+t \end{cases} ,$$

entonces

$$\sum_{i=1}^{s+t} l_i(\alpha) = \log | N_K(\alpha) | \ . \tag{5.1}$$

5.2 Inyección del grupo de las unidades en el espacio logarítmico

Sea $\mathcal{O}_\mathbf{K}{}^*$ el grupo de las unidades de $\mathcal{O}_\mathbf{K}$, el anillo de enteros de $\mathbf{K}$. Si consideramos el mapeo $l : \mathbf{K}^* \to \mathbb{R}^{s+t}$ visto en la sección anterior y denotamos por $\mathcal{L}$ a la restricción de l sobre el subgrupo $\mathcal{O}_\mathbf{K}{}^*$ de $\mathbf{K}^*$, obtenemos el homomorfismo

$$\mathcal{L} : \mathcal{O}_\mathbf{K}{}^* \to \mathbb{R}^{s+t}$$

el cual no es inyectivo, pero su núcleo es fácilmente descrito en el siguiente

Lema 5.2 *El núcleo W de $\mathcal{L}$ es el conjunto de todas las raíces de la unidad que están en $\mathcal{O}_\mathbf{K}$. Además éste es un grupo cíclico finito de orden par.*

Demostración : Sea $W' = \{\alpha \in \mathcal{O}_\mathbf{K} \ : \ \alpha \text{ es raíz de la unidad}\}$.

Tratemos de probar entonces que $W = W'$.

Si $\alpha \in W'$, entonces $\alpha^m = 1$ para alguna $m \in \mathbb{N}$, y así

$$[\sigma_i(\alpha)]^m = \sigma_i(\alpha^m) = \sigma_i(1) = 1 \qquad \forall\, i = 1, \ldots, s+t$$

lo cual implica que

$$| \sigma_i(\alpha) | = 1 \quad , \quad 1 \leq i \leq s+t$$

de aquí que

$$\mathcal{L}(\alpha) = (\log | \sigma_1(\alpha) |, \ldots, \log | \sigma_s(\alpha) |, \log | \sigma_{s+1}(\alpha) |^2, \ldots, \log | \sigma_{s+t}(\alpha) |^2) = 0 \ .$$

Es decir que $\alpha \in \ker \mathcal{L}$. Por lo tanto $W' \subseteq W$.

Ahora, si $\alpha \in W$, entonces $\mid \sigma_i(\alpha) \mid = 1$, $(1 \leq i \leq s+2t)$. Como el polinomio de campo de α

$$f_\alpha(x) = \prod_{i=1}^{n=s+2t} (x - \sigma_i(\alpha))$$

está en $\mathbb{Z}[\mathbf{x}]$ [ver teorema 1.9 combinado con el lema 1.21 y el teorema 1,10 a)]. Se puede aplicar el lema 3.4, concluyéndose que todos los $\sigma_i(\alpha)$ son raíces de la unidad, pero como una de las σ_i es la función identidad, entonces α es raíz de la unidad. Por lo tanto $W \subseteq W'$.

Claramente W es un grupo ya que es el núcleo de un homomorfismo entre grupos. Ahora, como para cualquier $\alpha \in W$ se tiene que $\mid \sigma_i(\alpha) \mid = 1$ $(1 \leq i \leq s+t)$, entonces $\sigma(W)$ es un subconjunto acotado en $\mathbf{L}^{s,t}$. Como $\sigma(W) \subset \sigma(\mathcal{O}_\mathbf{K})$ y $\sigma(\mathcal{O}_\mathbf{K})$ es un retículo en $\mathbf{L}^{s,t}$ (ver corolario 4.14), si $0 < r \in \mathbb{R}$ es tal que $\sigma(W) \subset B_r(0)$, entonces $B_r(0) \cap \sigma(\mathcal{O}_\mathbf{K})$ es finito ya que $\sigma(\mathcal{O}_\mathbf{K})$ es discreto (teorema 4.3). Por lo tanto $\sigma(W)$ es finito, y como σ es inyectiva, entonces W es finito. Pero como cualquier subgrupo finito de $\mathbf{K}^*$ es cíclico (ver teorema A.30 del apéndice), W es cíclico (ver teorema A.30 del apéndice).

Finalmente como $\mathcal{L}(-1) = 0$, entonces $-1 \in W$ el cual tiene orden 2, por lo tanto por el teorema de Lagrange W tiene orden par.

□

El siguiente paso es dar una descripción de la imagen E de $\mathcal{O}_\mathbf{K}$ en $\mathbb{R}^{s,t}$ bajo $\mathcal{L}$.

Lema 5.3 *La imagen E de $\mathcal{O}_\mathbf{K}{}^*$ en $\mathbb{R}^{s+t}$ bajo $\mathcal{L}$ es un retículo de dimensión $\leq s+t-1$.*

Demostración : Se sabe que si α es una unidad ($\alpha \in \mathcal{O}_\mathbf{K}{}^*$), entonces $N_K(\alpha) = \pm 1$, y según la ecuación 5.1 se tiene que

$$\sum_{i=1}^{s+t} l_i(\alpha) = \log \mid N_K(\alpha) \mid = \log \mid \pm 1 \mid = 0 .$$

Por lo tanto los puntos de E están en el subespacio vectorial H de $\mathbb{R}^{s+t}$ definido como

$$H = \{(x_1, \ldots, x_{s+t}) \in \mathbb{R} \ : \ x_1 + \cdots + x_{s+t} = 0\}$$

el cual claramente tiene dimensión $s+t-1$. Ahora como $\mathcal{L}$ es un homomorfismo entre grupos y $\mathbb{R}^{s+t}$ es un grupo aditivo, entonces E es un subgrupo aditivo de $\mathbb{R}^{s+t}$ y gracias al teorema 4.4 solo necesitamos probar que E es discreto.

Supongamos que $0 < r \in \mathbb{R}$ y que $\mathcal{L}(\varepsilon) \in E \cap B_r(0)$, esto es que

$$\| \mathcal{L}(\varepsilon) \| < r$$

Como $\mathcal{L}(\varepsilon) = (l_1(\varepsilon), \ldots, l_{s+t}(\varepsilon))$, en donde $l_i(\varepsilon)$ es como lo previo a la igualdad 5.1, entonces

$$| l_i(\varepsilon) | \leq \| \mathcal{L}(\varepsilon) \| < r$$

de donde se obtiene que

$$\begin{array}{rcll} | \sigma_i(\varepsilon) | & < & e^r & (i = 1, \ldots, s) \\ | \sigma_i(\varepsilon) |^2 & < & e^r & (i = s+1, \ldots, s+t) \end{array}$$

de esto último se sigue que el conjunto $\sigma(R)$ es acotado, en donde

$$R = \{\varepsilon \in \mathcal{O}_K^* \ : \ \mathcal{L}(\varepsilon) \in E \cap B_r(0)\} = \mathcal{L}^{-1}(E \cap B_r(0)) \ .$$

Ahora como $\sigma(R) \subset \sigma(\mathcal{O}_K)$, y $\sigma(\mathcal{O}_K)$ es un retículo, razonando igual que en el lema 5.2 se tiene que $\sigma(R)$ es finito. Además como σ es inyectiva, entonces R es finito y de aquí que $E \cap B_r(0)$ también es finito. Por lo tanto finalmente E es discreto y así E es un retículo de dimensión $\leq s + t - 1$.

□

Observación : Con los dos lemas anteriores tenemos que $\mathcal{O}_K^*$ es finitamente generado. En efecto, ya que W es finito y $\mathcal{O}_K^*/W \cong E$ es un retículo (y por lo tanto un grupo abeliano libre de rango $\leq s + t - 1$), si $\{\alpha_1 W, \ldots, \alpha_k W\}$ $(k \leq s + t - 1)$ es una $\mathbb{Z}$-base de $\mathcal{O}_K^*/W$, fácilmente se puede verificar que $\{\alpha_1, \ldots, \alpha_k\} \cup W$ genera a $\mathcal{O}_K^*$. Todo lo que resta es encontrar el valor exacto de la dimensión del retículo E. De hecho éste es $s + t - 1$ como se probará en la siguiente sección.

5.3 El teorema de Dirichlet

Un resultado que será de vital importancia en la averiguación del valor exacto de la dimensión de E es

Lema 5.4 *Sea Γ un retículo en $\mathbb{R}^m$. Entonces Γ tiene dimensión m si y sólo si existe un subconjunto acotado B de $\mathbb{R}^m$ tal que*

$$\mathbb{R}^m = \bigcup_{x \in \Gamma} (x + B) \tag{5.2}$$

Demostración : $\Rightarrow$) Recordemos que si Π es un dominio fundamental del retículo Γ, entonces Π es acotado. Más aún, por el lema 4.5 cualquier elemento de $\mathbb{R}^m$ está en alguno de los conjuntos $x + \Pi$, $x \in \Gamma$. Por lo tanto $B = \Pi$ satisface la ecuación 5.2 .
$\Leftarrow$) Si $B \subset \mathbb{R}^m$ es acotado y satisface la ecuación 5.2. Hay que probar que la dimensión de Γ es igual a m.
Supongamos que $\dim \Gamma < m$. Sea V el espacio vectorial generado por Γ, entonces $\dim V < \dim \mathbb{R}^m$. Ahora tomemos $V^\perp$ el complemento ortogonal de V en $\mathbb{R}^m$ (es decir que $V^\perp$ es un subespacio vectorial de $\mathbb{R}^m$ tal que $\mathbb{R}^m = V \oplus V^\perp$ y además cualquier elemento de $V^\perp$ es ortogonal a todos los de V).

Como $\Gamma \subset V$ y $\mathbb{R}^m = \bigcup_{x \in \Gamma}(x + B)$, entonces claramente

$$\mathbb{R}^m = \bigcup_{v \in V}(v + B) . \tag{5.3}$$

Trabajando ahora con la transformación lineal $\pi : \mathbb{R}^m \to V^\perp$ (Proyección en $V^\perp$), fácilmente se puede verificar que la distancia entre cualesquiera dos puntos de $\mathbb{R}^m$ es mayor o igual que la distancia entre sus imágenes. Notemos también que $\pi(B) = V^\perp$. En efecto, ya que por definición $\pi(B) \subseteq V^\perp$. Por otro lado si $u \in V^\perp \subset \mathbb{R}^m$, entonces por 5.3 u está en algún conjunto $v + B$, $v \in V$, esto es que $u = v + b$ para ciertas $v \in V$ y $b \in B$, de donde se obtiene que $b = (-v) + u$ y sólo de esta forma ya que $\mathbb{R}^m = V \oplus V^\perp$, entonces $\pi(b) = u$ lo cual implica que $V^\perp \subseteq \pi(B)$. Ahora, como B es acotado existe $r > 0$ tal que

$$d(\pi(0), \pi(x)) = d(0, \pi(x)) \leq d(0, x) \leq r \quad \forall x \in B .$$

De lo último se sigue que $\pi(B) = V^\perp$ es acotado, lo cual es una contradicción. Por lo tanto Γ tiene dimensión m.

□

Lema 5.5 *Sea* $y \in (\mathbf{L}^{s,t})^*$ *y* $\lambda_y : \mathbf{L}^{s,t} \to \mathbf{L}^{s,t}$ *definida como*

$$\lambda_y(x) = yx.$$

Entonces λ_y *es lineal y el determinante de cualquier matriz asociada a* λ_y *es igual a* $N(y)$.

Demostración : Recordemos que $\mathbf{L}^{s,t}$ es un $\mathbb{R}$-espacio vectorial de dimensión $n = s + 2t$. Por otro lado, fácilmente se verifica que si $x, z \in \mathbf{L}^{s,t}$, $c \in \mathbb{R}$, entonces $\lambda_y(x + cz) = \lambda_y(x) + c\lambda_y(z)$, es decir que λ_y es una $\mathbb{R}$-transformación lineal.

Ahora, si $y = (x_1, \ldots, x_s, y_1 + iz_1, \ldots, y_t + iz_t)$, y trabajamos con la base de $\mathbf{L}^{s,t}$ vista en 4.3 se tiene que

$$\begin{array}{rcl}
\lambda_y(e_1) & = & x_1 e_1 \\
\vdots & & \vdots \\
\lambda_y(e_s) & = & x_s e_s \\
\lambda_y(e_{s+1}) & = & y_1 e_{s+1} + z_1 e_{s+2} \\
\lambda_y(e_{s+2}) & = & -z_1 e_{s+1} + y_1 e_{s+2} \\
\vdots & = & \vdots \\
\lambda_y(e_{s+2t-1}) & = & y_t e_{s+2t-1} + z_t e_{s+2t} \\
\lambda_y(e_{s+2t}) & = & -z_t e_{s+2t-1} + y_t e_{s+2t} \ ,
\end{array}$$

de donde se tiene que el determinante de la matriz asociada a λ_y está dado por

$$\begin{vmatrix}
x_1 & & & & & & & \\
 & \ddots & & & & & & \\
 & & x_s & & & & & \\
 & & & y_1 & -z_1 & & & \\
 & & & z_1 & y_1 & & & \\
 & & & & & \ddots & & \\
 & & & & & & y_t & -z_t \\
 & & & & & & z_t & y_t
\end{vmatrix}$$

el cual es igual a

$$x_1 \cdots x_s (y_1^2 + z_1^2) \cdots (y_t^2 + z_t^2) = N(y) \ .$$

Si se hubiera trabajado con otra base el resultado sería exactamente el mismo ya que las matrices asociadas son equivalentes.

□

Pasemos ahora a calcular el valor exacto de la dimensión del retículo E.

Teorema 5.6 *La imagen E de $\mathcal{O}_K^*$ en $\mathbb{R}^{s+t}$ bajo $\mathcal{L}$ es un retículo de dimensión $s+t-1$.*

Demostración : En el lema 5.3 se probó que E es un retículo de dimensión $\leq s+t-1$. En ese mismo lema se vió que $E \subset H \subset \mathbb{R}^{s+t}$, en donde

$$H = \{(x_1, \ldots, x_{s+t}) \in \mathbb{R}^{s+t} \ : \ x_1 + \cdots + x_{s+t} = 0\} \cong \mathbb{R}^{s+t-1}.$$

Por lo tanto por el lema 5.4 sólo basta que en H encontremos un subconjunto acotado B tal que

$$H = \bigcup_{e \in E} (e + B)\,. \tag{5.4}$$

Para tal efecto, recordemos que $\ell : (\mathbf{L}^{s,t})^* \to \mathbb{R}^{s+t}$ es un homomorfismo suprayectivo y como $H \subset \mathbb{R}^{s+t}$, entonces cualquier punto de H es la imagen de por lo menos un punto de $(\mathbf{L}^{s,t})^*$. Más aún, si $x \in (\mathbf{L}^{s,t})^*$, tenemos que $\ell(x) \in H$ si y sólo si $\mid N(x) \mid = 1$. Por lo tanto si tomamos

$$S = \{x \in (\mathbf{L}^{s,t})^* \ : \mid N(x) \mid = 1\},$$

entonces

$$\ell(S) = H \tag{5.5}$$

Notemos ahora que si $X_0 \subseteq S$ es acotado, entonces $\ell(X_0)$ también lo es. En efecto, ya que el conjunto S es cerrado, y así $\overline{X_0} \subseteq S$ es compacto, $\ell(X_0) \subseteq \ell(\overline{X_0})$ es acotado ya que $\ell(\overline{X_0})$ es compacto porque ℓ es continua.

Ahora, si $x \in S$, $X_0 \subseteq S$, y si $x_0 \in X_0$,

$$\mid N(xx_0) \mid = \mid N(x)N(x_0) \mid = \mid N(x) \mid\mid N(x_0) \mid = 1\,,$$

esto es que $xX_0 \subseteq S$ si $X_0 \subseteq S$. En particular si $u \in \mathcal{O}_{\mathbf{K}}^*$, entonces $\sigma(u) \in (\mathbf{L}^{s,t})^*$ y

$$\begin{aligned} \mid N(\sigma(u)) \mid &= \mid \sigma_1(u) \cdots \sigma_s(u) \mid \sigma_{s+1}(u) \mid^2 \cdots \mid \sigma_{s+t}(u) \mid^2 \mid \\ &= \mid N_K(u) \mid = \mid \pm 1 \mid = 1\,. \end{aligned}$$

Esto es que $\sigma(u) \in S$. Por lo tanto $\sigma(u)X_0 \subseteq S$ si $X_0 \subseteq S$.

Observemos ahora que si lográsemos encontrar $X_0 \subseteq S$ acotado tal que

$$S = \bigcup_{u \in \mathcal{O}_{\mathbf{K}}^*} (\sigma(u)X_0)\,, \tag{5.6}$$

entonces por las ecuaciones 5.5 y 5.6 tendríamos que

$$
\begin{aligned}
H = \ell(S) &= \ell\Big(\bigcup_{u\in\mathcal{O}_K^*}(\sigma(u)X_0)\Big)\\
&= \bigcup_{u\in\mathcal{O}_K^*}\ell(\sigma(u)X_0)\\
&= \bigcup_{u\in\mathcal{O}_K^*}[\ell(\sigma(u))+\ell(X_0)]\\
&= \bigcup_{u\in\mathcal{O}_K^*}[\mathcal{L}(u)+\ell(X_0)]\\
&= \bigcup_{e\in E}(e+\ell(X_0))\,.
\end{aligned}
$$

Haciendo $\ell(X_0) = B$ se tendría 5.4 y el teorema quedaría probado.

Encontremos entonces el adecuado X_0. Para esto recordemos que $\sigma(\mathcal{O}_K)$ es un retículo en $\mathbf{L}^{s,t}$. Si consideramos la transformación lineal $\lambda_y : \mathbf{L}^{s,t} \to \mathbf{L}^{s,t}$ dada en el lema 5.5, y si $y \in S \subset \mathbf{L}^{s,t}$, entonces $\det\lambda_y = N(y) = \pm 1$, es decir que la matriz asociada a λ_y es unimodular.

Ahora, como $\sigma(\mathcal{O}_K) = M$ es un retículo de dimensión $n = s+2t$ en $\mathbf{L}^{s,t}$ y λ_y es lineal, fácilmente se verifica que $\lambda_y(M) = yM$ es un retículo en $\mathbf{L}^{s,t}$. Más aún, como $\det\lambda_y = \pm 1$, por el lema 4.6 se tiene que el volumen V de cualquier dominio fundamental de yM es igual al volumen de un dominio fundamental de M, pues si Π es un dominio fundamental de M

$$v(\lambda_y(\Pi)) = v(\Pi)|J| = v(\Pi) \quad , \quad J \text{ es el jacobiano}$$

Elijamos números reales $c_1, \ldots, c_{s+t}$ mayores que cero tales que

$$Q = c_1 \cdots c_{s+t} > (4/\pi)^t V\,.$$

Si X es el conjunto de $x = (x_1, \ldots, x_{s+t}) \in \mathbf{L}^{s,t}$ para los cuales

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

entonces por el lema 4.19, existe $0 \neq x \in yM \cap X$, esto es una $x \in X$ tal que

$$x = y\sigma(\alpha) \quad , \quad 0 \neq \alpha \in \mathcal{O}_K \tag{5.7}$$

y

$$|\,N(x)\,| = |\,x_1\,| \cdots |\,x_s\,|\,|\,x_{s+1}\,|^2 \cdots |\,x_{s+t}\,|^2 < c_1 \cdots c_{s+t} = Q\,.$$

Por otro lado, también se tiene que

$$N(x) = N(y)N(\sigma(\alpha)) = \pm N_K(\alpha)$$

de donde se sigue que

$$|\,N_K(\alpha)\,| < Q\,. \tag{5.8}$$

Por otro lado, como el teorema 2.42 (c) nos dice que sólo un número finito de ideales tiene norma dada, entonces sólo un número finito de ideales tienen norma $< Q$. De este número finito de ideales, sea R el conjunto de ideales principales de norma $< Q$. Claramente $R \neq \emptyset$ ya que según la ecuación 5.8 se tiene que $N(\langle\alpha\rangle) = \mid N_K(\alpha) \mid < Q$ al menos para la α de 5.7, esto es que $\langle\alpha\rangle \in R$.

Recordando ahora que si $\gamma, \delta \in \mathcal{O}_K$ son asociados, entonces $\langle\gamma\rangle = \langle\delta\rangle$, se sigue que en $\mathcal{O}_K$ existe un número finito de números no asociados por parejas $\alpha_1, \ldots, \alpha_N$ tales que

$$R = \{\langle\alpha_1\rangle, \ldots, \langle\alpha_N\rangle\}.$$

Como $\langle\alpha\rangle \in R$, entonces α es asociado de exactamente uno de los α_i; esto es que $\alpha u = \alpha_i$, con $u \in \mathcal{O}_K^*$. De donde se tiene que $\sigma(\alpha)\sigma(u) = \sigma(\alpha_i)$. Ahora recordando que $x = y\sigma(\alpha)$ y que σ es un homomorfismo entre anillos se tiene que

$$y = x\sigma(\alpha_i^{-1})\sigma(u)\,. \tag{5.9}$$

Ahora definamos

$$X_0 = S \cap \left(\bigcup_{i=1}^{N} \sigma(\alpha_i^{-1})X\right). \tag{5.10}$$

Como X es acotado, lo son los conjuntos $\sigma(\alpha_i^{-1})X$, y como N es finito X_0 es acotado. Claramente X_0 no depende para nada de la elección de $y \in S$.

Afirmación: X_0 es el conjunto adecuado. En efecto, ya que si tomamos normas en 5.9 y teniendo en cuenta que $y, \sigma(u) \in S$ se tiene que $x\sigma(\alpha_i^{-1}) \in S$, y claramente también $x\sigma(\alpha_i^{-1}) \in \bigcup_{i=1}^{N} \sigma(\alpha_i^{-1})X$, y de aquí que $x\sigma(\alpha_i^{-1}) \in X_0$. Entonces 5.9 nos muestra que

$$y \in \sigma(u)X_0 \subseteq \bigcup_{u \in \mathcal{O}_K^*} \sigma(u)X_0\,,$$

y como y es arbitraria entonces

$$S \subseteq \bigcup_{u \in \mathcal{O}_K^*} \sigma(u)X_0\,.$$

La otra contención es obvia ya que $\sigma(u)X_0 \subseteq S\ \forall u \in \mathcal{O}_K^*$.

□

Teorema 5.7 *(*Teorema de las unidades de Dirichlet*).* *El grupo de las unidades de $\mathcal{O}_K$ es isomorfo a*

$$W \times \mathbf{Z} \times \underbrace{\cdots}_{s+t-1 \text{ veces}} \times \mathbf{Z}$$

donde W es el conjunto descrito en el lema 5.2

Demostración :

Prueba 1 : Por el teorema 5.6 se tiene que

$$\mathcal{O}_K^*/W \cong E \cong \mathbf{Z} \times \underbrace{\cdots}_{s+t-1 \text{ veces}} \times \mathbf{Z}\,. \tag{5.11}$$

También, por la observación hecha enseguida del lema 5.3 se tiene que $\mathcal{O}_K^*$ es un grupo abeliano finitamente generado, y por lo tanto $\mathcal{O}_K^*$ es isomorfo a un producto directo de grupos cíclicos (ver [1]).

Como W es un grupo cíclico finito constituido por todos los elementos de $\mathcal{O}_K^*$ de orden finito, entonces W es el subgrupo de $\mathcal{O}_K^*$ formado por la parte de torsión de $\mathcal{O}_K^*$. Así

$$\mathcal{O}_K^* \cong W \times L \quad \text{(ver [1], lema 9.1 pag. 90)} \tag{5.12}$$

donde L es libre de torsión. Por 5.11

$$\mathcal{O}_K^*/W \cong L \cong \mathbf{Z} \times \underbrace{\cdots}_{s+t-1 \text{ veces}} \times \mathbf{Z}\,.$$

Finalmente por 5.12 el resultado se sigue.

□

Prueba 2 : Por el teorema 5.6, E es un retículo de dimensión $s+t-1$ en $\mathbf{R}^{s+t}$. Sea $\{\mathcal{L}(u_1), \ldots, \mathcal{L}(u_{s+t-1})\}$ una $\mathbf{Z}$-base de E $(u_1, \ldots, u_{s+t-1} \in \mathcal{O}_K^*)$. Entonces para cualquier unidad $u \in \mathcal{O}_K^*$ existen enteros racionales a_i univocamente determinados tales que

$$\mathcal{L}(u) = \sum_{i+1}^{s+t-1} a_i \mathcal{L}(u_i) = \mathcal{L}\left(\prod_{i=1}^{s+t-1} u_i^{a_i}\right).$$

Por lo tanto se tiene que $u = w \prod_{i=1}^{s+t-1} u_i^{a_i}$, $w \in \ker \mathcal{L} = W$.

□

Para ilustrar el teorema de las unidades de Dirichlet, tenemos los siguientes:

Ejemplos :

1.- Sea $\mathbf{K} = \mathbb{Q}(\sqrt{d})$ un campo cuadrático.

(a) Si $d > 0$, los dos homomorfismos $\sigma_1, \sigma_2 : \mathbf{K} \to \mathbb{C}$ son reales y así $s = 2, t = 0$.

Por otro lado como las únicas raíces de la unidad en $\mathbf{K}$ son ± 1, y éstas son unidades del anillo de enteros $\mathcal{O}_\mathbf{K}$, entonces $W = \{\pm 1\}$ (W definido como en el lema 5.2). Por lo tanto

$$\mathcal{O}_\mathbf{K}{}^* \cong W \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z} .$$

Lo cual reafirma lo demostrado en el teorema 2.5 .

(b) Si $d < 0$, los dos homomorfismos $\sigma_1, \sigma_2 : \mathbf{K} \to \mathbb{C}$ son complejos ($\overline{\sigma_1} = \sigma_2$) y así $s = 0, t = 1$. Por otro lado, si $\alpha \in W$,

$$\mathcal{L}(\alpha) = \log |\, \sigma_1(\alpha) \,|^2 = 0 \quad \Rightarrow \quad |\, \sigma_1(\alpha) \,|^2 = 1 \quad \Rightarrow \quad N_K(\alpha) = 1 ,$$

pero por lo visto en la demostración de la proposición 2.3 se tiene que $W = \{\pm 1, \pm i\}$ si $d = -1$, $W = \{\pm 1, \pm\omega, \pm\omega^2\}, \omega = e^{2\pi i/3}$, si $d = -3$, y $W = \{\pm 1\}$ en cualquier otro caso.

Resumiendo tenemos que $\mathcal{O}_\mathbf{K}{}^* = W$, W como antes descrito.

Observación : Con lo visto en el ejemplo 1 fácilmente se tiene que

$$s + t - 1 = 0 \;\Leftrightarrow \begin{cases} s = 1, \;\; t = 0 \;\Leftrightarrow\; \mathbf{K} = \mathbb{Q} \qquad \text{ó} \\ s = 0, \;\; t = 1 \;\Leftrightarrow\; \mathbf{K} = \mathbb{Q}(\sqrt{d}) \;\; d < 0. \end{cases}$$

En estos casos $\mathcal{O}_\mathbf{K}{}^* = W$, es un grupo finito. En cualquier otro caso $\mathcal{O}_\mathbf{K}{}^*$ es un grupo infinito.

2.- Sea $\mathbf{K} = \mathbb{Q}(\xi)$ un campo ciclotómico (ξ raíz p-ésima primitiva de la unidad, p primo racional impar), en este caso $s = 0, t = \dfrac{p-1}{2}$. Ahora, como las únicas raíces de la unidad en $\mathbf{K} = \mathbb{Q}(\xi)$ son $\pm\xi^s$, $s \in \mathbb{Z}$ [ver lema 3.2] y $\pm\xi^s$ es unidad de $\mathcal{O}_\mathbf{K} = \mathbb{Z}[\xi]$, concluimos que $W = \{\pm\xi^s : 0 \le s \le p-1\}$ el cual tiene orden $2p$, y así

$$\mathcal{O}_\mathbf{K}{}^* \cong W \times \mathbb{Z} \times \underbrace{\cdots}_{\frac{p-3}{2} \text{ veces}} \times \mathbb{Z} .$$

Apéndice

En este apéndice se recordarán algunas definiciones básicas, así como también se demostrarán algunos resultados elementales que se usaron en el transcurso de este trabajo.

A.1 Anillos

La teoría de anillos es de vital importancia en el desarrollo de este trabajo, sin embargo no intentaremos hacer un análisis detallado de esta estructura algebraica, simplemente haremos mención de importantes teoremas, proposiciones, etc, la mayoría de ellos conocidos, por lo cual sólo demostraremos algunos de tales resultados.

Antes de empezar el recordatorio cabe mencionar que en este trabajo siempre que hablemos de anillos se supondra que tales anillos son conmutativos con uno, a menos que se especifique lo contrario.

Proposición A.1 *Si* $\mathbf{R}$ *es un anillo,* $\mathcal{I}$ *un ideal de* $\mathbf{R}$ *tal que* $1 \in \mathcal{I}$, *entonces* $\mathcal{I} = \mathbf{R}$. *Más aún si* $x \in \mathcal{I}$ *y* x *es una unidad, entonces* $\mathcal{I} = \mathbf{R}$.

□

Teorema A.2 *Cualquier dominio entero finito es un campo.*

□

Proposición A.3 *Si* $\mathbf{R}$ *es un anillo,* $\mathbf{R}$ *es un campo si y sólo si los únicos ideales de* $\mathbf{R}$ *son los triviales.*

□

Recordemos ahora que si φ es un homomorfismo entre los anillos $\mathbf{R}_1$ y $\mathbf{R}_2$. La imagen de 1 bajo φ no necesariamente es igual a 1. Sin embargo si φ es suprayectivo o si R_2 es un dominio entero ($\varphi \neq 0$), entonces si se puede garantizar lo anterior.

Resultados importantes sobre ideales maximales e ideales primos se dan enseguida.

Teorema A.4 *Si* $\mathbf{R}$ *es un anillo,* $\mathcal{I}$ *ideal de* $\mathbf{R}$, *entonces :*

a) $\mathcal{I}$ *es un ideal máximal de* $\mathbf{R}$ *si y sólo si* $\mathbf{R}/\mathcal{I}$ *es un campo.*
b) $\mathcal{I}$ *es un ideal primo de* $\mathbf{R}$ *si y sólo si* $\mathbf{R}/\mathcal{I}$ *es un dominio entero.*

□

Notemos que todo ideal máximal $\mathcal{M}$ de un anillo $\mathbf{R}$ es un ideal primo. En efecto, pues al ser $\mathcal{M}$ máximal por el teorema A.4 a), $\mathbf{R}/\mathcal{M}$ es un campo, y como todo campo es un dominio entero, entonces $\mathbf{R}/\mathcal{M}$ lo es. Finalmente por teorema A.4 b), $\mathcal{M}$ es un ideal primo.

Algo sobre operaciones con ideales de un anillo se dá en las siguientes dos proposiciones con las cuales se cierra la sección.

Proposición A.5 *Si $\mathcal{A}, \mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n$ son ideales de un anillo $\mathbf{R}$, entonces*

$$(\mathcal{A}+\mathcal{B}_1)(\mathcal{A}+\mathcal{B}_2)\cdots(\mathcal{A}+\mathcal{B}_n) \subseteq \mathcal{A}+\mathcal{B}_1\mathcal{B}_2\cdots\mathcal{B}_n \quad ;\forall\, n \in \mathbb{N}.$$

□

Proposición A.6 *Si $\mathbf{R}$ es un anillo y si $a, b \in \mathbf{R}$, entonces*

a) $\langle ab\rangle = \langle a\rangle\langle b\rangle$. *Esto es que el producto de dos ideales principales es principal (Usando inducción este resultado se puede generalizar a cualquier número de factores ideales principales).*
b) $\langle a, b\rangle = \langle a\rangle + \langle b\rangle$.

□

A.2 Divisibilidad en anillos

Las definiciones básicas de divisibilidad en anillos son bastantemente conocidas, por lo cual no las daremos, simplemente nos enfocaremos a definir lo que son elementos irreducibles y elementos primos en un anillo arbitrario $\mathbf{R}$. En el capítulo 2 se ve la diferencia que hay entre estos.

Definición A.7 *Si $a \in \mathbf{R}$ y a no es una unidad, diremos que a es irreducible si éste no tiene factores propios. Equivalentemente, a es irreducible si siempre que $a = bc$, entonces b ó c es una unidad.*

Definición A.8 *Si $\mathbf{R}$ es un anillo y $p \in \mathbf{R}, p \neq 0$ no unidad, diremos que p es primo si siempre que $p|ab, a, b \in \mathbf{R}$, entonces $p|a$ ó $p|b$.*

Es bien sabido que en $\mathbf{Z}$ se dá la factorización única en primos. También en $\mathbf{Z}$ los elementos irreducibles coinciden con los elementos primos. En el capítulo 2 se demuestra que si $\mathbf{R}$ es un anillo en donde los elementos irreducibles coinciden con los primos, entonces en $\mathbf{R}$ se dá la factorización única en irreducibles o primos.

Proposición A.9 *Si $\mathbf{R}$ es un anillo y $0 \neq p \in \mathbf{R}$ no unidad, entonces p es primo si y sólo si $\langle p\rangle$ es un ideal primo.*

□

A.3 Polinomios y su factorización

La notación que utilizaremos para los anillos de polinomios es la estándar. Esto es que $\mathbf{R}[\mathbf{x}]$ nos representa el anillo de polinomios en una indeterminada con coeficientes en el anillo $\mathbf{R}$ y $\mathbf{R}[\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n}]$ nos representa el anillo de polinomios en n indeterminadas con coeficientes en $\mathbf{R}$.

Recordemos que en $\mathbf{Z}$ decidir si un número $m \in \mathbf{Z}$ es o no primo (o irreducible) no es fácil. Es de esperarse que cuando trabajemos en el anillo de polinomios $\mathbf{K}[\mathbf{x}]$ ($\mathbf{K}$ un campo) sea también bastante complicado decidir si un polinomio $f(x) \in \mathbf{K}[\mathbf{x}]$ es o no irreducible.

Tres teoremas muy importantes por su poder de alcance son los siguientes.

Teorema A.10 *(Lema de Gauss). Sea $p(x) \in \mathbf{Z}[\mathbf{x}]$, y supongamos que $p(x) = g(x)h(x)$, donde $g(x), h(x) \in \mathbf{Q}[\mathbf{x}]$. Entonces existe $\lambda \in \mathbf{Q}, \lambda \neq 0$, tal que $\lambda g(x), \lambda^{-1}h(x) \in \mathbf{Z}[\mathbf{x}]$.*

□

Observación: *El Lema de Gauss nos afirma que si $p(x) \in \mathbf{Z}[\mathbf{x}]$ es reducible en $\mathbf{Q}[\mathbf{x}]$, entonces $p(x)$ también es reducible en $\mathbf{Z}[\mathbf{x}]$. Equivalentemente el Lema de Gauss nos afirma que si $p(x) \in \mathbf{Z}[\mathbf{x}]$ es irreducible en $\mathbf{Z}[\mathbf{x}]$, entonces $p(x)$ también es irreducible en $\mathbf{Q}[\mathbf{x}]$. Más aún, como $\mathbf{Z}[\mathbf{x}] \subseteq \mathbf{Q}[\mathbf{x}]$ y como claramente si $p(x) \in \mathbf{Z}[\mathbf{x}]$ es irreducible en $\mathbf{Q}[\mathbf{x}]$, también lo es en $\mathbf{Z}[\mathbf{x}]$, entonces Gauss nos dice que si $p(x) \in \mathbf{Z}[\mathbf{x}]$, $p(x)$ es irreducible en $\mathbf{Z}[\mathbf{x}]$ si y sólo si lo es en $\mathbf{Z}[\mathbf{x}]$.*

Decidir cuándo un polinomio $f(x) \in \mathbf{Z}[\mathbf{x}]$ es irreducible no es fácil. El siguiente criterio es muy importante y se puede usar en algunos casos.

Teorema A.11 *(Criterio de irreducibilidad de Eisenstein). Sea $f(x) \in \mathbf{Z}[\mathbf{x}]$ un polinomio, $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Supóngase que existe un primo $p \in \mathbf{Z}$ tal que*

a) $p \not| a_n$,
b) $p | a_i \quad ; \quad 0 \leq i \leq n-1$,
c) $p^2 \not| a_0$.

Entonces $f(x)$ es irreducible en $\mathbf{Z}[\mathbf{x}]$.(Por el Lema de Gauss $f(x)$ es irreducible en $\mathbf{Q}[\mathbf{x}]$).

□

Otro criterio importante es el siguiente

Teorema A.12 *Sea* $f(x) = a_0 + a_1 x \ldots + a_n x^n \in \mathbf{Z}[\mathbf{x}]$ *y sea* $q \in \mathbf{Z}$ *un entero tal que* $q \nmid a_n$. *Entonces si* $\bar{f}(x) = \bar{a_0} + \bar{a_1} x + \cdots + \bar{a_n} x^n \in \mathbf{Z}_q[\mathbf{x}]$ *es irreducible en* $\mathbf{Z}_q[\mathbf{x}]$, *también lo es* $f(x)$ *en* $\mathbf{Z}[\mathbf{x}]$. *(Las barras significan reducción módulo q).*

□

Ejemplo: *Si* $p \in \mathbf{Z}$ *es un primo impar. Entonces los siguientes polinomios son irreducibles en* $\mathbf{Z}[\mathbf{x}]$

$$\begin{array}{lll} \text{a)} & f(x) & = 1 + x + x^2 + \cdots + x^{p-1} \in \mathbf{Z}[\mathbf{x}] \\ \text{b)} & f(x) & = 1 + x^p + x^{2p} + \cdots + x^{(p-1)p} \in \mathbf{Z}[\mathbf{x}] \end{array}$$

Para probar esto, notemos que en general, dado $f(x) \in \mathbf{Z}[\mathbf{x}]$, se tiene que $f(x+1) \in \mathbf{Z}[\mathbf{x}]$ y además: $f(x)$ es irreducible en $\mathbf{Z}[\mathbf{x}]$ si y sólo si $f(x+1)$ es irreducible en $\mathbf{Z}[\mathbf{x}]$. Probemos pues entonces que $f(x+1)$ es irreducible.

a) Como

$$f(x) = \frac{x^p - 1}{x - 1},$$

entonces

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}.$$

Desarrollando esto último según el teorema del binomio de Newton se tiene que

$$f(x+1) = x^{p-1} + (\sum_{j=1}^{p-2} a_j x^{p-j-1}) + p,$$

en donde

$$a_j = \frac{p!}{(p-j)!j!}.$$

Finalmente $f(x+1)$ es irreducible según Eisenstein. En efecto, pues el propio primo p satisface las hipótesis del teorema A.11 . La prueba del inciso b) es similar a la de a).

A.4 Raíces ó ceros de polinomios

La factorización de un polinomio está bastantemente ligado con el tema de las raíces o ceros del mismo.

Un teorema importante que nos permite detectar raíces repetidas de un polinomio con coeficientes en un campo de característica cero es el siguiente.

Teorema A.12 *Sea* $f(x) = a_0 + a_1 x \ldots + a_n x^n \in \mathbf{Z}[\mathbf{x}]$ *y sea* $q \in \mathbf{Z}$ *un entero tal que* $q \nmid a_n$. *Entonces si* $\bar{f}(x) = \bar{a_0} + \bar{a_1} x + \cdots + \bar{a_n} x^n \in \mathbf{Z}_q[\mathbf{x}]$ *es irreducible en* $\mathbf{Z}_q[\mathbf{x}]$, *también lo es* $f(x)$ *en* $\mathbf{Z}[\mathbf{x}]$. *(Las barras significan reducción módulo q).*

□

Ejemplo: *Si* $p \in \mathbf{Z}$ *es un primo impar. Entonces los siguientes polinomios son irreducibles en* $\mathbf{Z}[\mathbf{x}]$

$$\begin{array}{lll} \text{a)} & f(x) & = 1 + x + x^2 + \cdots + x^{p-1} \in \mathbf{Z}[\mathbf{x}] \\ \text{b)} & f(x) & = 1 + x^p + x^{2p} + \cdots + x^{(p-1)p} \in \mathbf{Z}[\mathbf{x}] \end{array}$$

Para probar esto, notemos que en general, dado $f(x) \in \mathbf{Z}[\mathbf{x}]$, se tiene que $f(x+1) \in \mathbf{Z}[\mathbf{x}]$ y además: $f(x)$ es irreducible en $\mathbf{Z}[\mathbf{x}]$ si y sólo si $f(x+1)$ es irreducible en $\mathbf{Z}[\mathbf{x}]$. Probemos pues entonces que $f(x+1)$ es Irreducible.

a) Como

$$f(x) = \frac{x^p - 1}{x - 1},$$

entonces

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}.$$

Desarrollando esto último según el teorema del binomio de Newton se tiene que

$$f(x+1) = x^{p-1} + (\sum_{j=1}^{p-2} a_j x^{p-j-1}) + p,$$

en donde

$$a_j = \frac{p!}{(p-j)!j!}.$$

Finalmente $f(x+1)$ es irreducible según Eisenstein. En efecto, pues el propio primo p satisface las hipótesis del teorema A.11 . La prueba del inciso b) es similar a la de a).

A.4 Raíces ó ceros de polinomios

La factorización de un polinomio está bastantemente ligado con el tema de las raíces o ceros del mismo.

Un teorema importante que nos permite detectar raíces repetidas de un polinomio con coeficientes en un campo de característica cero es el siguiente.

Teorema A.13 *Sea* $0 \neq f(x) \in \mathbf{K}[\mathbf{x}]$, $\mathbf{K}$ *un campo de característica cero. Entonces* $f(x)$ *es divisible por el cuadrado de un polinomio de grado* ≥ 1 *si y sólo si* f *y* Df *(*Df *representa la derivada formal del polinomio* f*) tienen un factor común de grado* > 1.

Demostración : $\Rightarrow$) Supongamos que $f = g^2h$, donde $\partial(g) \geq 1$. Derivando se tiene que

$$Df = g^2Dh + h(2g)Dg = g(gDh + 2hDg)$$

Por lo tanto f y Df tienen a g como un factor común.

$\Leftarrow$) Supongamos que f no es divisible por el cuadrado de ningún polinomio de grado ≥ 1. Como en $\mathbf{K}[\mathbf{x}]$ se dá la factorización en irreducibles, entonces para cualquier factor irreducible g de f se tendría que $f = gh$, donde g y h son primos relativos (ya que si g y h tuvieran algún factor no constante en común, entonces f sería divisible por el cuadrado de tal factor). Ahora como f y Df tienen un factor común de grado ≥ 1, tal factor g lo podemos tomar irreducible. Entonces tenemos que

$$f = gh \quad \text{y} \quad Df = gl$$

donde $g, h, l \in \mathbf{K}[\mathbf{x}]$, g es irreducible y además g y h son primos relativos. Derivando tenemos que

$$Df = gDh + hDg$$

y como también $Df = gl$, entonces $gl = gDh + hDg$, de donde se concluye que $g|hDg$. Pero como g y h son primos relativos, entonces $g|Dg$. Ahora, por definición Dg es de grado menor que g. Entonces lo anterior sólo puede ocurrir si $Dg = 0$. Finalmente como $\mathbf{K}$ es un campo de caracterísrica cero, fácilmente se checa que $Dg = 0$ implica que g es una constante, lo cual es absurdo ya que por hipótesis $\partial(g) \geq 1$.

□

Un resultado muy conocido que se desprende del teorema anterior y cuya demostración no daremos es el siguiente.

Corolario A.14 *Un polinomio irreducible sobre un subcampo* $\mathbf{K}$ *de* $\mathbf{C}$*, no tiene raices repetidas en* $\mathbf{C}$.

□

A.5 Extensiones de campos

Recordemos que si $\mathbf{K}$ y $\mathbf{L}$ son campos todo homomorfismo no nulo

$$\varphi : \mathbf{K} \to \mathbf{L}$$

es inyectivo, ya que $\ker\varphi$ es un ideal de $\mathbf{K}$ y al ser $\mathbf{K}$ un campo, por la proposición A.3 , los únicos ideales de $\mathbf{K}$ son $\{0\}$ y $\mathbf{K}$. Pero como φ es no nulo, entonces $\ker\varphi = \{0\}$.

Con lo anterior tenemos que: $\varphi : \mathbf{K} \to \varphi(\mathbf{K})$ es un isomorfismo de campos y $\varphi(\mathbf{K}) \subseteq \mathbf{L}$. Esto es que en $\mathbf{L}$ existe una copia de $\mathbf{K}$.

En las anteriores circunstancias diremos que $\mathbf{L}$ es una *extensión* de $\mathbf{K}$.

De ahora en adelante, siempre que tengamos dos campos $\mathbf{K}, \mathbf{L}$, en donde $\mathbf{L}$ extiende a $\mathbf{K}$, simplemente escribiremos $\mathbf{L} : \mathbf{K}$.

Fácilmente se puede checar que si $\mathbf{L} : \mathbf{K}$ es una extensión de campos, entonces $\mathbf{L}$ tiene estructura de *espacio vectorial* sobre $\mathbf{K}$, donde la suma de vectores es la suma en $\mathbf{L}$ y la multiplicación de escalares $\lambda \in \mathbf{K}$ por vectores $v \in \mathbf{L}$ es justamente $\lambda v \in \mathbf{L}$.

La dimensión del espacio vectorial $\mathbf{L}$ sobre $\mathbf{K}$ es llamado el *grado* de la extensión o el *grado* de $\mathbf{L}$ sobre $\mathbf{K}$, y lo denotaremos como $[\mathbf{L} : \mathbf{K}]$. En el capítulo 1 se estudian bastantes ejemplos de extensiones de grado finito. Por otro lado, también existen extensiones de grado infinito, ya que por ejemplo fácilmente se puede probar que si $\mathbb{R}$ es el campo de los números reales entonces $[\mathbb{R} : \mathbb{Q}]$ es infinito.

Una importante propiedad multiplicativa de los grados de las extensiones se dá en el siguiente:

Teorema A.15 *Si* $\mathbf{H}, \mathbf{K}, \mathbf{L}$ *son campos, y* $\mathbf{H} \subseteq \mathbf{K} \subseteq \mathbf{L}$, *entonces*

$$[\mathbf{L} : \mathbf{H}] = [\mathbf{L} : \mathbf{K}][\mathbf{K} : \mathbf{H}].$$

□

A continuación daremos una forma de construir extensiones de campos.

Construcción : Si $\mathbf{K}$ es un campo y si $\Im = \{\mathbf{F}_\alpha\}$ es una familia de subcampos de $\mathbf{K}$, entonces $\mathbf{F} = \bigcap \mathbf{F}_\alpha$ es un subcampo de $\mathbf{K}$ y tenemos que $\mathbf{F}_\alpha : \mathbf{F}$, $\mathbf{K} : \mathbf{F}_\alpha$ y $\mathbf{K} : \mathbf{F}$ son extensiones de campos $\forall\, \alpha$.

Consideremos ahora la extensión $\mathbf{L} : \mathbf{K}$, y sea $\mathbf{Y} \subseteq \mathbf{L}$ cualquier subconjunto. Sea $\Im$ la familia de subcampos de $\mathbf{L}$ que contienen a $\mathbf{K}$ y a $\mathbf{Y}$. Notemos que $\Im \neq \emptyset$ pues $\mathbf{L} \in \Im$. Definamos $\mathbf{K(Y)} = \bigcap_{\mathbf{F} \in \Im} \mathbf{F}$,entonces

a) $\mathbf{K(Y)} \in \mathbf{L}$ es un subcampo ,
b) $\mathbf{K}, \mathbf{Y} \subseteq \mathbf{K(Y)}$,
c) $\mathbf{K(Y)}$ es el subcampo más chico de $\mathbf{F}$ que contiene a $\mathbf{K}$ y $\mathbf{Y}$.

Decimos que $\mathbf{K(Y)}$ es el subcampo de $\mathbf{F}$ obtenido al *adjuntar* $\mathbf{Y}$ a $\mathbf{K}$.

Si $\mathbf{Y} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, al campo $\mathbf{K(Y)} = \mathbf{K}(\{\alpha_1, \ldots, \alpha_n\})$ lo denotaremos como $\mathbf{K}(\alpha_1, \ldots, \alpha_n)$. En particular si $\mathbf{Y} = \{\alpha\}$, $\mathbf{K(Y)} = \mathbf{K}(\alpha)$, y se dira que la extensión $\mathbf{K}(\alpha)$: $\mathbf{K}$ es simple.

Definición A.16 *Si $\mathbf{L} : \mathbf{K}$ es una extensión de campos, $\alpha \in \mathbf{L}$ se dice que es algebraico sobre $\mathbf{K}$ si α es raíz de algún polinomio no nulo $p(x) \in \mathbf{K}[\mathbf{x}]$. Si α no es raíz de ningún polinomio en $\mathbf{K}[\mathbf{x}]$ diremos que α es trascendente sobre $\mathbf{K}$. También si $\mathbf{L} : \mathbf{K}$ es una extensión de campos y si todo $\alpha \in \mathbf{L}$ es algebraico sobre $\mathbf{K}$ diremos que la extensión $\mathbf{L} : \mathbf{K}$ es algebraica.*

En lo que resta de este trabajo estaremos sólo interesados en elementos algebraicos.

Si $\alpha \in \mathbf{L}$ es algebraico sobre $\mathbf{K}$, por el principio del buen orden en $\mathbb{N}$, existe un polinomio mónico $p(x)$ de grado mínimo, tal que $p(\alpha) = 0$. Este polinomio de grado mínimo llamado *el polinomio mínimo de α* es único como fácilmente se puede demostrar.

El siguiente Lema, así como también los restantes Teoremas de esta sección , son muy conocidos y sus demostraciones pueden verse en muchos libros como por ejemplo en [2].

Lema A.17 *Si $\mathbf{L} : \mathbf{K}$ es una extensión y $\alpha \in \mathbf{L}$ es algebraico sobre $\mathbf{K}$, entonces :*

a) *El polinomio mínimo $m(x)$ de α sobre $\mathbf{K}$ es irreducible en $\mathbf{K}[\mathbf{x}]$.*
b) *$m(x)$ divide a cualquier otro polinomio $p(x) \in \mathbf{K}[\mathbf{x}]$ tal que $p(\alpha) = 0$.*

□

Teorema A.18 *Si $\mathbf{L} : \mathbf{K}$ es una extensión de campos y si $\alpha \in \mathbf{L}$, entonces α es algebraico sobre $\mathbf{K}$ si y sólo si $\mathbf{K}(\alpha)$ es una extensión finita de $\mathbf{K}$. En este caso $[\mathbf{K}(\alpha) : \mathbf{K}] = \partial(p)$, donde p es el polinomio mínimo de α sobre $\mathbf{K}$, y $\mathbf{K}(\alpha) = \mathbf{K}[\alpha]$.*

□

Sólo una importante observación acerca del teorema A.18: Si $p(x) \in \mathbf{K}[\mathbf{x}]$ es el polinomio mínimo de α sobre $\mathbf{K}$, y si $\partial(p) = n$, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $\mathbf{K}(\alpha)$ sobre $\mathbf{K}$.

Con la observación de antemano hecha, se desprenden los dos siguientes Corolarios.

Corolario A.19 *Si* $\mathbf{L} : \mathbf{K}$ *es una extensión y si* $\alpha \in \mathbf{L}$ *es algebraico sobre* $\mathbf{K}$, *entonces todos los elementos de* $\mathbf{K}(\alpha)$ *son algebraicos sobre* $\mathbf{K}$. *Esto es que* $\mathbf{K}(\alpha)$: $\mathbf{K}$ *es una extensión algebraica.*

□

Corolario A.20 *Si* $\mathbf{L} : \mathbf{K}$ *es finita, entonces es algebraica.*

□

El recíproco del corolario A.20 no necesariamente es cierto, por ejemplo $\mathbf{A} : \mathbb{Q}$ ($\mathbf{A}$ el campo de todos los números algebraicos sobre $\mathbb{Q}$) es algebraica pero no finita como se puede ver en el capítulo 1. Sin embargo el recíproco es válido en las circunstancias dadas en el:

Teorema A.21 *Una extensión* $\mathbf{L} : \mathbf{K}$ *es finita si y sólo si es algebraica y* $\mathbf{L} = \mathbf{K}(\alpha_1, \ldots, \alpha_n)$ *(***finitamente generada***),* $\alpha_1, \ldots, \alpha_n \in \mathbf{L}$.

□

A.6 Polinomios simétricos

Definición A.22 *Si* $\mathbf{R}$ *es un anillo y* $f \in \mathbf{R}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$ *es un polinomio en* n *indeterminadas, se dice que* f *es simétrico si* f *es invariante bajo cualquier permutación de las indeterminadas.*

Ejemplo : Si $\mathbf{R}$ es un anillo.

a) En $\mathbf{R}[\mathbf{x_1}, \mathbf{x_2}]$; $f(x_1, x_2) = x_1 + x_2$ es simétrico, sin embargo $g(x_1, x_2) = x_1 x_2^2$ no lo es.

b) En $\mathbf{R}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$,

$$
\begin{aligned}
s_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n \\
s_2(x_1, \ldots, x_n) &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \\
&\vdots \qquad\qquad\qquad \vdots \\
s_r(x_1, \ldots, x_n) &= \text{suma de todos los posibles distintos} \\
&\quad \text{productos de } r \text{ distintos } x_i's \\
&\vdots \qquad\qquad\qquad \vdots \\
s_n(x_1, \ldots, x_n) &= x_1x_2 \cdots x_n
\end{aligned}
$$

son simétricos, y se les llaman los polinomios simétricos elementales.

Enseguida veremos algunos resultados sobre polinomios simétricos que serán de mucha importancia en el transcurso de este trabajo.

Sea $\mathbf{K}$ un campo y $f(x) \in \mathbf{K}[\mathbf{x}]$ un polinomio de grado n, y sea $\mathbf{L} : \mathbf{K}$ una extensión de campos, en donde

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad , \quad a_n \neq 0 \, . \tag{A.1}$$

f se puede descomponer en factores lineales sobre $\mathbf{L}$ como

$$f(x) = a_n(x - \alpha_1) \ldots (x - \alpha_n) \quad ; \quad \alpha_1, \ldots \alpha_n \in \mathbf{L} \, .$$

Desarrollando estos productos tenemos que:

$$f(x) = a_n(x_n - s_1 x^{n-1} + \cdots + (-1)^n s_n) \, , \tag{A.2}$$

donde $s_1, \ldots, s_n$ son los polinomios simétricos elementales en n indeterminadas con coeficientes en $\mathbf{K}$ evaluados en $\alpha_1, \ldots \alpha_n$. Esto es que $s_r = s_r(\alpha_1, \ldots, \alpha_n)$; $(1 \leq r \leq n)$.

Observación: Notemos que de las expresiones A.1 y A.2 se tiene que

$$\begin{aligned} a_{n-1} &= -a_n s_1(\alpha_1, \ldots, \alpha_n) \\ &\vdots \qquad\qquad \vdots \\ a_0 &= (-1)^n a_n s_n(\alpha_1, \ldots, \alpha_n) \, , \end{aligned}$$

y como $0 \neq a_n \in \mathbf{K}$, entonces $s_r(\alpha_1, \ldots, \alpha_n) \in \mathbf{K}$, $(1 \leq r \leq n)$.

Claramente un polinomio simétrico en $s_1, \ldots, s_n$ puede ser reescrito como un polinomio simétrico en $x_1, \ldots, x_n$. El recíproco también es cierto como se enuncia en el siguiente teorema cuya demostracion se puede ver en [8], pag. 25

Teorema A.23 *Si $\mathbf{R}$ es un anillo. Entonces cualquier polinomio simétrico en $\mathbf{R}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$ es expresable como un polinomio en los polinomios simétricos elementales $s_1, \ldots, s_n$ con coeficientes en $\mathbf{R}$.*

□

Un corolario al teorema anterior que por su poder de alcance tiene el derecho a ser llamado teorema es:

Teorema A.24 *Sea $\mathbf{L} : \mathbf{K}$ una extensión de campos y $f \in \mathbf{K}[\mathbf{x}], \partial(f) = n$, y supongamos que $\alpha_1, \ldots, \alpha_n$ son todas las raíces de f y que éstas están en $\mathbf{L}$. Si $h(x_1, \ldots, x_n) \in \mathbf{K}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$ es simétrico, entonces $h(\alpha_1, \ldots, \alpha_n) \in \mathbf{K}$.*

Demostración : Por el teorema A.23 , $h(x_1,\ldots,x_n)$ se puede expresar como un polinomio con coeficientes en $\mathbf{K}$ en los polinomios simétricos elementales $s_1,\ldots,s_n$. Esto es que

$$h(x_1,\ldots,x_n) = f(s_1,\ldots,s_n)\,; \quad f \in \mathbf{K}[\mathbf{x_1},\ldots,\mathbf{x_n}]\,,$$

entonces $h(\alpha_1,\ldots,\alpha_n) = f(s_1(\alpha_1,\ldots,\alpha_n),\ldots,s_n(\alpha_1\ldots,\alpha_n))$. Pero por la observación hecha antes del teorema A.23 , $s_r(\alpha_1\ldots,\alpha_n) \in \mathbf{K}$, $(1 \leq r \leq n)$ y por lo tanto $h(\alpha_1,\ldots,\alpha_n) \in \mathbf{K}$.

□

A.7 Grupos abelianos libres

Existe gran relación entre los grupos abelianos y los *módulos*. De hecho, fácilmente se puede checar que un grupo $\mathbf{M}$ es un grupo abeliano si y sólo si $\mathbf{M}$ es un $\mathbf{Z}$-módulo.

En lo que resta de esta sección, por comodidad trabajaremos con grupos abelianos aditivos. Sin embargo, todo lo que se haga será extensible a grupos abelianos multiplicativos.

Las definiciones de grupo abeliano *finitamente generado, dependencia e independencia lineal y bases* sobre $\mathbf{Z}$ serán omitidas y sólo recordaremos lo que es un grupo abellano *libre*

Definición A.25 *Un grupo abeliano con una $\mathbf{Z}$-base de n elementos es llamado un grupo abeliano libre de rango n.*

Mediante un cálculo muy sencillo se puede probar que si $\{x_1,\ldots,x_n\}$ y $\{y_1,\ldots,y_n\}$ son dos bases distintas de un grupo abeliano libre de rango n, en donde:

$$y_i = \sum_{j=1}^{n} a_{ij}x_j \quad , \quad x_i = \sum_{j=1}^{n} b_{ij}y_j \quad ; \quad a_{ij}, b_{ij} \in \mathbf{Z} \quad (1 \leq i,j \leq n)\,,$$

entonces las matrices $A = (a_{ij})$ y $B = (b_{ij})$ son *unimodulares*, es decir que su determinante es ± 1.

Lema A.26 *Sea $\mathbf{G}$ un grupo abeliano libre de rango n con base $\{x_1,\ldots,x_n\}$. Supóngase que $A = (a_{ij})$ es una matriz de $n \times n$ con entradas enteras. Entonces los elementos $y_i = \sum_{j=1}^{n} a_{ij}x_j$ forman una base de $\mathbf{G}$ si y sólo si A es unimodular.*

Demostración : $\Rightarrow$) Esto es inmediato por los parrafos previos al lema.

$\Leftarrow$) Si A es unimodular entonces $\det A \neq 0$, y se sigue que los y_i son linealmente independientes. Por otro lado como $\det A \neq 0$, A^{-1} existe y es igual a:

$$A^{-1} = \frac{1}{\det A}\tilde{A} = \pm\tilde{A}$$

donde $\tilde{A}$ es la matriz adjunta, la cual tiene entradas enteras. Finalmente haciendo $B = A^{-1} = (b_{ij})$, se obtiene

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

Demostrándose asi que los y_i generan a G.

□

Un resultado que será de gran utilidad y cuyos detalles de su demostración se pueden ver en [1], pag. 185, es el siguiente:

Teorema A.27 *Sea* **G** *un grupo abeliano libre, distinto de cero, de rango* n, *y sea* **H** *un subgrupo distinto de cero de* **G**. *Entonces* **H** *es abeliano libre, de rango* $s \leq n$. *Más aún existe una base* $\{x_1, \ldots, x_n\}$ *para* **G** *y enteros positivos* $d_1, \ldots, d_s$, *donde* d_i *divide a* d_{i+1} *para* $i = 1, \ldots, s-1$, *tales que* $\{d_1 x_1, \ldots, d_s x_s\}$ *es una base de* **H**.

□

Un resultado que será de vital importancia en el desarrollo de este trabajo es el siguiente

Teorema A.28 *Sea* **G** *un grupo abeliano libre de rango* n *y* **H** *un subgrupo de* **G**. *Entonces* **G/H** *es finito si y sólo si los rangos de* **G** *y* **H** *son iguales. Si este es el caso, y si* **G** *y* **H** *tienen* **Z**-*bases* $\{x_1, \ldots, x_n\}$ *y* $\{y_1, \ldots, y_n\}$ *respectivamente, con* $y_i = \sum_{j=1}^{n} a_{ij} x_j$, *entonces*

$$|\ \mathbf{G/H}\ | = |\ det(a_{ij})\ | \ .$$

Demostración : Si **H** tiene rango s, por el teorema A.27 podemos elegir **Z**-bases $\{u_1, \ldots, u_n\}$ de **G** y $\{v_1, \ldots, v_s\}$ de **H** con $v_i = d_i u_i$, $d_i \in \mathbf{Z}^+$ $(1 \leq i \leq s)$. Claramente **G/H** es finitamente generado. En efecto, pues $u_1 + \mathbf{H}, \ldots, u_n + \mathbf{H}$ generan a **G/H**.

Definamos ahora

$$\varphi : \mathbf{Z}^n \to \mathbf{G/H}\ ,$$

como

$$\varphi(a_1,\ldots,a_n) = a_1(u_1+\mathbf{H}) + \cdots + a_n(u_n+\mathbf{H})\,.$$

Fácilmente se puede checar que φ es un homomorfismo suprayectivo y además

$$ker\varphi = \{(d_1b_1,\ldots,d_sb_s,0,\ldots,0) \;:\; b_i \in \mathbb{Z}\;;\; i=1,\ldots.s\}$$

Entonces

$$\mathbb{Z}^n/ker\varphi \cong \mathbf{G}/\mathbf{H}\,. \tag{A.3}$$

Por otro lado, claramente:

$$ker\varphi \cong d_1\mathbb{Z}\times\cdots\times d_s\mathbb{Z}\times\{0\}\times \underbrace{\cdots}_{n-s \text{ veces}} \times\{0\}\,.$$

Por lo tanto volviendo a la expresión dada en A.3 se tiene que

$$\mathbf{G}/\mathbf{H} \cong \mathbf{Z}_{d_1}\times\cdots\times\mathbf{Z}_{d_s}\times\mathbf{Z}\times \underbrace{\cdots}_{n-s \text{ veces}} \times\mathbf{Z}\,.$$

Entonces $|\,\mathbf{G}/\mathbf{H}\,|$ es finito si y sólo si $n-s=0$, esto es que $n=s$; con lo cual queda probada la primera parte del teorema. Notemos también que en este caso

$$|\,\mathbf{G}/\mathbf{H}\,| = d_1\cdots d_n\,.$$

Por otro lado como las x_i y u_i son bases de $\mathbf{G}$ y las y_i y v_i son bases de $\mathbf{H}$, entonces se tiene que

$$\begin{array}{lll} u_i = \sum_{j=1}^n b_{ij}x_j & \text{matricialmente} & U = BX \\ v_i = \sum_{j=1}^n c_{ij}u_j & \text{matricialmente} & V = CU \\ y_i = \sum_{j=1}^n d_{ij}v_j & \text{matricialmente} & Y = DV\,, \end{array}$$

y de aquí deducimos que

$$Y = DCBX\,, \tag{A.4}$$

en donde las matrices $B=(b_{ij})$ y $D=(d_{ij})$ son unimodulares. Ahora como $v_i = d_iu_i$ para $(1\le i\le s=n)$, entonces

$$C=(c_{ij}) = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix}.$$

como

$$\varphi(a_1,\ldots,a_n) = a_1(u_1+\mathbf{H}) + \cdots + a_n(u_n+\mathbf{H})\,.$$

Fácilmente se puede checar que φ es un homomorfismo suprayectivo y además

$$ker\varphi = \{(d_1b_1,\ldots,d_sb_s,0,\ldots,0)\ :\ b_i \in \mathbb{Z}\ ;\ i=1,\ldots,s\}$$

Entonces

$$\mathbb{Z}^n/ker\varphi \cong \mathbf{G}/\mathbf{H}\,. \tag{A.3}$$

Por otro lado, claramente:

$$ker\varphi \cong d_1\mathbf{Z}\times\cdots\times d_s\mathbb{Z}\times\{0\}\times \underbrace{\cdots}_{n-s\ \text{veces}} \times\{0\}\,.$$

Por lo tanto volviendo a la expresión dada en A.3 se tiene que

$$\mathbf{G}/\mathbf{H} \cong \mathbf{Z}_{d_1}\times\cdots\times\mathbf{Z}_{d_s}\times\mathbf{Z}\times \underbrace{\cdots}_{n-s\ \text{veces}} \times\mathbf{Z}\,.$$

Entonces $|\ \mathbf{G}/\mathbf{H}\ |$ es finito si y sólo si $n-s=0$, esto es que $n=s$; con lo cual queda probada la primera parte del teorema. Notemos también que en este caso

$$|\ \mathbf{G}/\mathbf{H}\ | = d_1\cdots d_n\,.$$

Por otro lado como las x_i y u_i son bases de $\mathbf{G}$ y las y_i y v_i son bases de $\mathbf{H}$, entonces se tiene que

$$\begin{array}{lll} u_i = \sum_{j=1}^n b_{ij}x_j & \text{matricialmente} & U = BX \\ v_i = \sum_{j=1}^n c_{ij}u_j & \text{matricialmente} & V = CU \\ y_i = \sum_{j=1}^n d_{ij}v_j & \text{matricialmente} & Y = DV\,, \end{array}$$

y de aquí deducimos que

$$Y = DCBX\,, \tag{A.4}$$

en donde las matrices $B=(b_{ij})$ y $D=(d_{ij})$ son unimodulares. Ahora como $v_i = d_iv_i$ para $(1\le i\le s=n)$, entonces

$$C = (c_{ij}) = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix}.$$

Finalmente si $A = (a_{ij})$, como $Y = AX$ se tiene, por la igualdad A.4 y por el hecho de que $\{x_1, \ldots, x_n\}$ es base de G, que $A = DCB$ y de aquí que $\det A = (\det D)(\det C)(detB)$ y por lo tanto

$$| \det A | = | \pm 1 | \, | \det C \, | \, | \pm 1 | = | d_1 \cdots d_n | = | \mathbf{G/H} |$$

□

Teorema A.29 *Si G es un grupo conmutativo finito, entonces existe un $x \in G$ cuyo orden es el mínimo común múltiplo de los ordenes de los elementos de G.*

Demostración : Como G es un grupo conmutativo finito, entonces

$$G \cong \mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_s},$$

en donde $d_1 | d_2 | \ldots | d_s$ (ver [1], lema 9.3 pag. 91). Si y es el uno del anillo $\mathbf{Z}_{d_s}$ y ponemos $x = (0, \ldots, 0, y)$, el orden de x es claramente d_s. Ahora si $z = (z_1, \ldots, z_n) \in G$, se tiene que $d_s z = 0$, ya que d_i divide a d_s para toda i. Por lo tanto d_s es un múltiplo del orden de z y x es el elemento buscado.

□

Teorema A.30 *Si $\mathbf{K}$ es un subcampo de $\mathbb{C}$, entonces cualquier subgrupo finito G del grupo multiplicativo $\mathbf{K}^*$, consiste de raíces de la unidad y es cíclico.*

Demostración : Por el teorema A.29 , existe $z \in G$ cuyo orden n es tal que $y^n = 1$ para cualquier $y \in G$. Como un polinomio de grado n sobre un campo tiene a lo más n raíces en el campo, el número de elementos en G es a lo más n. Ahora como z tiene orden n, G contiene los n elementos $z, z^2, \ldots, z^n = 1$, los cuales son todos distintos. Por lo tanto G está compuesto de estos elementos y es cíclico.

□

Bibliografía

[1] J. B. Fraleigh. *Algebra abstracta.* SITESA , 1988.

[2] I. N. Herstein. *Algebra moderna.* Trillas , 1986.

[3] S. Lang. *Algebraic numbers.* Addison- Wesley Publ. Co. , 1964.

[4] D. A. Marcus. *Number fields.* Verlag , 1977.

[5] T. Ono. *An introduction to algebraic number theory.* Plenum Publ. Co. , 1990.

[6] H. Pollard. *The theory of algebraic numbers.* The mathematical association de America , 1961.

[7] P. Samuel. *Algebraic theory of numbers.* Hermann , 1970

[8] Ian Stewart. *Galois theory.* Chapman and Hall , 1973.

[9] I. N. Stewart and D. O. Tall. *Algebraic number theory.* Chapman and Hall , 1979.

[10] J. V. Uspenski. *Teoría de ecuaciones.* Editorial Limusa , 1990.