SOBRE LA FACTORIZACIÓN DE IDEALES EN DOMINIOS DE DEDEKIND

ASTRID CAROLINA ARCHILA PRADA

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD CIENCIAS

ESCUELA DE MATEMÁTICAS

BUCARAMANGA

2021

SOBRE LA FACTORIZACIÓN DE IDEALES EN DOMINIOS DE DEDEKIND

ASTRID CAROLINA ARCHILA PRADA

Trabajo de Grado para optar al título de
Matemática

Director
Hector Edonis Pinedo Tapia
Doctor en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2021

AGRADECIMIENTOS

Agradezco a mi papá por su amor, apoyo incondicional, sus consejos y esfuerzo, a mi hermano por su cariño y apoyo; a toda mi familia por sus buenos deseos y sus oraciones. Al Dr Hector Pinedo, director de esta tesis y profesor en mi proceso académico, por su apoyo puesto que gracias a sus consejos, conocimientos y correcciones logré culminar este trabajo.

También quiero agradecer a Diego Fernando Gamboa por su compañía, apoyo y por toda su ayuda, por estar en esos momentos tan cruciales y sobretodo por su paciencia.

CONTENIDO

RESUMEN

TÍTULO: SOBRE LA FACTORIZACÓN DE IDEALES EN DOMINIOS DE DEDEKIND [*]

AUTOR: ASTRID CAROLINA ARCHILA PRADA [**]

PALABRAS CLAVE: NÚMEROS Y ENTEROS ALGEBRAICOS, EXTENSIÓN DE CUERPOS, CUERPO NUMERICO, CONJUGADA, DISCRIMINANTE, ANILLO DE ENTEROS, DOMINIO DE DEDEKIND, NORMA DE UN IDEAL.

DESCRIPCIÓN:

Este trabajo se divide en dos capítulos, en el primero se dan definiciones, proposiciones y teoremas generales sobre estructuras algebraicas que resultan útiles para desarrollar las bases de números algebraicos en una manera relativamente elemental. También se enuncian caracterizaciones para los anillos noetherianos.

En el segundo capítulo, las dos primeras secciones establecen las propiedades de las extensiones de cuerpos de los números racionales que se obtienen de adjuntar números algebraicos. En particular, se demuestra que cada una de estas extensiones son de la forma $\mathbb{Q}(\theta)$ con θ un número algebraico (Teorema elemento primitivo 2.1.11). En la tercera sección se introduce el anillo de enteros de un cuerpo numérico $\mathbb{K}$, denotado por $\mathcal{D} = \mathbb{K} \cap \mathbb{B}$ siendo $\mathbb{B}$ el conjunto de números algebraicos; se prueba que $\mathcal{D}$ es noetheriano, integralmente cerrado y que todo ideal primo de $\mathcal{D}$ es maximal (Teorema 2.3.4). A partir de estas propiedades se define la estructura de dominio de Dedekind y se demuestra en este caso general que los ideales fraccionarios forman un grupo bajo la multiplicación (item 1. Teorema 2.3.7). De esto se deduce que todo ideal de $\mathcal{D}$ se escribe como producto finito de ideales primos y este producto es único salvo por el orden de los factores (item 2. Teorema 2.3.7). En la sección final se define la norma de un ideal y se demuestra que dado un entero positivo este es la norma de un número finito de ideales de $\mathcal{D}$ (Teorema 2.4.10), lo cual es posible por la factorización prima única en dominios de Dedekind.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Hector Edonis Pinedo Tapia, Doctor en Matemáticas.

ABSTRACT

TITLE: ON FACTORING IDEALS IN DEDEKIND DOMAINS [*]

AUTHOR: ASTRID CAROLINA ARCHILA PRADA [**]

KEYWORDS: ALGEBRAIC NUMBERS AND INTEGERS, FIELD EXTENSIONS, NUMERICAL FIELD, CONJUGATE, DISCRIMINANT, RINGS OF INTEGERS, DEDEKIND DOMAINS, NORM OF AN IDEAL.

DESCRIPTION:

This project is divided in two chapters. In the first one we give definitions, propositions and general theorems on algebraic structures which are useful for developing the fundations of the theory of algebraic numbers in a relatively elementary manner. Characterizations for noetherian rings are also stated.

In the second chapter, the first two sections establish properties of field extensions of rational numbers that are obtained from adjoining algebraic numbers. Particularly, it is shown that each of these extensions are of the form $\mathbb{Q}(\theta)$ with θ an algebraic number (primitive element Theorem 2.1.11). The third section introduces the ring of integers of a number field $\mathbb{K}$, denoted by $\mathcal{D} = \mathbb{K} \cap \mathbb{B}$ where $\mathbb{B}$ is the set of algebraic integers; it is proved that $\mathcal{D}$ is noetherian, integrally closed domain and that every prime ideal of $\mathcal{D}$ is maximal (Theorem 2.3.4). From these properties the Dedekind domain structure is defined and it is shown in this general case that fractional ideals form a group under multiplication (see item 1. Theorem 2.3.7). From this follows that every ideal of $\mathcal{D}$ is written as a finite product of prime ideals and this product is unique except for the order of the factors (see item 2. Theorem 2.3.7). In the final section, the definition of the norm of an ideal is given and it is shown that any fixed positive integer is the norm of a finite number of ideals of $\mathcal{D}$ (Theorem 2.4.10), which is possible because the factorization in primes is unique in Dedekind domains.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Hector Edonis Pinedo Tapia, Doctor en Matemáticas.

INTRODUCCIÓN

Análogo al teorema fundamental de la aritmética se cumple que la factorización única en irreducibles es verdadera en algunos anillos que contienen a los anillos de enteros pero en otros no, en este trabajo de grado se hará el estudio de anillos en el cual dicha factorización sea posible en términos de ideales. Para este estudio nos concentramos en dos ideas muy importantes, dichas ideas corresponden principalmente a los siguientes autores:

- **Kummer** tuvo la idea de que si no se puede hacer la factorización única de un número en un anillo de enteros, entonces quizá se podría extender el anillo a uno más grande para que así la factorización sea tanto posible como única. Por ejemplo:
  $6 = 2 \cdot 3 = \sqrt{-6}\sqrt{-6}$ en $\mathbb{Z}[\sqrt{-6}]$, con $\sqrt{-6}$ irreducible pero $\sqrt{-6}$ no divide a 2 o 3 en este anillo, puesto que $\frac{2}{\sqrt{-6}} = \sqrt{\frac{-2}{3}}$ y $\frac{3}{\sqrt{-6}} = \sqrt{\frac{-3}{2}}$ no pertenecen a $\mathbb{Z}[\sqrt{-6}]$.
  Él llamó a estos nuevos elementos introducidos como **"números ideales"**.

- **Dedekind** analizó las mismas ideas de Kummer pero en diferente dirección, introduciendo la noción de un **"ideal"** en la teoría de anillos. Dedekind mostró que aunque la factorización única puede fallar para los números, se puede desarrollar una teoría de la factorización única para los ideales. En esta teoría una de las definiciones más esenciales es la de **"ideales primos"**.

Para la realización de estas ideas se introducen los números algebraicos como solución de polinomios con coeficientes enteros, en el cual son importantes los enteros algebraicos. El contexto natural en el que se desarrollará será en un anillo de enteros algebraicos que está contenido en un cuerpo de números algebraicos asociado.

Luego se generaliza el concepto de **"ideal fraccionario"**, esto se realiza con el fin de tener una gran ventaja, donde el conjunto de los ideales fraccionarios no nulos forman un grupo bajo la multiplicación, para así introducir la factorización de ideales primos de una manera más fácil. Dadas propiedades es posible definir la norma de un ideal como la generalización de la norma de un elemento y probar que esta nueva norma tiene la propiedad multiplicativa, es decir que $N(IJ) = N(I)N(J)$ con I, J ideales, se usa esta y otras propiedades que se enunciarán en las secciones correspondientes para mostrar que cada ideal que cumpla dichas condiciones tiene un número finito de divisores.

1. PRELIMINARES

El objetivo de esta sección es entrar en contexto sobre las temáticas en la cual se fundamenta este trabajo de grado; se presentarán conceptos, definiciones, lemas y teoremas de diferentes aspectos como son los números algebraicos, conjugadas y discriminantes, factorización prima de ideales y norma de un ideal, los cuales son necesarios para entender este trabajo.

Se dará uso implícito de algunas definiciones que no serán enunciadas en este trabajo puesto que son conceptos básicos; como los son: **grupo, grupo abeliano, anillo, dominio, dominio de integridad, cuerpo, ideal, ideal maximal, ideal primo, anillo cociente, anillos de fracciones**, entre otros; todos estos conceptos pueden ser encontrados en las referencias [1] y [2].

1.1. GRUPOS ABELIANOS LIBRES Y CONDICIONES DE CADENA

Definición 1.1.1. Sea G un grupo abeliano. Un conjunto linealmente independiente que genere a G es llamada una base (o $\mathbb{Z}-base$), en este caso cada elemento $g \in G$ tiene representación única de la forma:

$$g = m_1 g_1 + m_2 g_2 + \cdots m_n g_n,$$

para algunos $g_1, \ldots, g_n \in G$ y $m_1, \ldots, m_n \in \mathbb{Z}$. En este caso se dice que G es un **grupo abeliano libre** con base $g_1, \ldots, g_n$. El rango de G es el número de elementos

---

[1] LEZAMA, Oswaldo. *Cuadernos de Álgebra N° 2, Anillos*. `http://gfnun.unal.edu.co/fileadmin/content/seminarios/sac2/cuadernos/anillos.pdf`. 2014.

[2] STEWART Ian & TALL, David. *Algebraic Number Theory and Fermat's Last Theorem: Third Edition (3rd ed.).* Massachusetts: A K Peters/CRC Press., 2002.

de la base.

Para ver que el rango está bien definido primero se demostrará un lema.

Lema 1.1.2. Sea $\mathbb{Z}$ el anillo conmutativo y $\mathbb{Z}^m \cong \mathbb{Z}^n$ como $\mathbb{Z}$-módulos entonces $m = n$.

Demostración. Si $\mathbb{Z}^m \cong \mathbb{Z}^n$ entonces $2\mathbb{Z}^m \cong 2\mathbb{Z}^n$, así se obtiene un isomorfismo inducido $\mathbb{Z}^m/2\mathbb{Z}^m \cong \mathbb{Z}^n/2\mathbb{Z}^n$. Luego $(\mathbb{Z}/2\mathbb{Z})^m \cong (\mathbb{Z}/2\mathbb{Z})^n$. Este último es un isomorfismo de espacios vectoriales, dado que $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ es un cuerpo. Por la definición de dimensión de espacios vectoriales se tiene que $m = n$.

□

Puesto que $\mathbb{Z}^n$ es denotado como el producto de n copias de el grupo aditivo de los enteros, esto muestra que un grupo con una base de n elementos es isomorfo a $\mathbb{Z}^n$. Así sea G con dos bases, una base con n elementos y la otra de m elementos. Entonces $G \cong \mathbb{Z}^n$ y $G \cong \mathbb{Z}^m$ y por transitividad $\mathbb{Z}^n \cong \mathbb{Z}^m$. Se concluye por el Lema 1.1.2 que $m = n$, es decir el rango está bien definido.

El siguiente resultado garantiza que los subgrupos de grupos abelianos libres también son libres. En efecto.

Teorema 1.1.3. Todo subgrupo H de un grupo abeliano libre G de rango n tiene rango $s \leq n$, además existe una base $u_1, \ldots, u_n$ para G y enteros positivos $\alpha_1, \ldots, \alpha_s$ tal que $\alpha_1 u_1, \ldots, \alpha_s u_s$ es una base para H.

Demostración. Por inducción sobre el rango n de G.
Para $n = 1$ se tiene que la base de G tiene solo un elemento, por lo tanto G es cíclico infinito así como H es subgrupo de G, entonces H es un grupo cíclico infinito. Ahora suponga que para cualquier grupo de rango $n - 1$, todo subgrupo H es abeliano libre de rango $s \leq n - 1$ y además existen una base $u_1, \ldots, u_{n-1}$ de G y enteros

positivos $\alpha_1, \ldots, \alpha_s$, tal que $\alpha_1 u_1, \ldots, \alpha_s u_s$ es una base para H. Si el rango de G es n y $H = \{0\}$ el teorema se tiene trivialmente, entonces sea $H \neq \{0\}$.
Sea $L = \{l_i > 0 : \exists h \in H, h = l_1 w_1 + \cdots + l_n w_n\}$, donde $l_i \in \mathbb{Z}^+$ y $L \subseteq \mathbb{N}$ con $L \neq \emptyset$ puesto que si $L = \emptyset$ entonces no existe $l_i \in \mathbb{Z}^+$ tal que $h \in H \setminus \{0\}$ tal que $h = l_1 w_1 + \cdots + l_n w_n$ entonces todos los $l_i \leq 0$. Dado que $l_i \neq 0$ se tiene que $l_i < 0$ para algún $i = 1, \ldots, n$ y como $-h \in H \setminus \{0\}$ entonces $-h = -l_1 w_1 - \cdots - l_n w_n$ esto implica que $-l_i \in L$, por lo tanto $L \neq \emptyset$, por consiguiente L tiene mínimo. Ahora, para toda base $w_1, \ldots, w_n \in G$ se define

$$\lambda(w_1, \ldots, w_n) = min\{l_i > 0 : \exists h \in H, h = l_1 w_1 + \cdots + l_n w_n\}.$$

Sea $w_1, \ldots, w_n$ una base de G tal que $\lambda(w_1, \ldots, w_n) = \alpha_1$ sea minimal y que exista $v_1 \in H$ tal que

$$v_1 = \alpha_1 w_1 + \beta_2 w_2 + \cdots + \beta_n w_n. \quad (\beta_i \in \mathbb{Z},\ 2 \leq i \leq n)$$

Tomando $\beta_i \in \mathbb{Z}$, y aplicando el algoritmo de la división se tiene que

$$\beta_i = \alpha_1 q_i + r_i \quad (2 \leq i \leq n) \tag{1}$$

donde $0 \leq r_i < \alpha_1$ y $q_i \in \mathbb{Z}$. Se define

$$u_1 = w_1 + q_2 w_2 + \cdots + q_n w_n,$$

se puede ver que $w_1 = u_1 - q_2 w_2 - \cdots - q_n w_n$, es decir w_1 es una combinación lineal de $u_1, w_2, \ldots, w_n$ por lo tanto $u_1, w_2, \ldots, w_n$ es una base de G. Con respecto a la

nueva base se tiene que:

$$\begin{aligned} v_1 &= \alpha_1 w_1 + \beta_2 w_2 + \cdots + \beta_n w_n \\ &= \alpha_1(u_1 - q_2 w_2 - \cdots - q_n w_n) + \beta_2 w_2 + \cdots + \beta_n w_n \\ &= \alpha_1 u_1 - \alpha_1 q_2 w_2 - \cdots - \alpha_1 q_n w_n + \beta_2 w_2 + \cdots + \beta_n w_n \\ &= \alpha_1 w_1 + (\beta_2 - \alpha_1 q_2) w_2 + \cdots + (\beta_n - \alpha_1 q_n) w_n \\ &= \alpha_1 u_1 + r_2 w_2 + \cdots + r_n w_n. \end{aligned}$$

Por la minimalidad de $\alpha_1 = \lambda(w_1, \ldots, w_n)$ y la ecuación (1) se tiene que

$$r_2 = r_3 = \cdots = r_n = 0,$$

por lo tanto $v_1 = \alpha_1 u_1$. Ahora sea G' el grupo abeliano libre de rango $n-1$, con generadores $w_2, \ldots, w_n$ y

$$H' = \{m_1 u_1 + m_2 w_2 + \cdots + m_n w_n \in H \,|\, m_1 = 0\}$$

un subgrupo abeliano libre de rango $s \leq n-1$, así por hipótesis de inducción se tiene que existen bases $u_2, \ldots, u_n$ de G' y $v_2, \ldots, v_s$ de H' tal que $v_i = \alpha_i u_i$ para enteros positivos α_i.

Sea V_1 el subgrupo generado por v_1. Note que $H = H' + V_1$. Es claro que $H' \cap V_1 = \{0\}$ y dado que $H', V_1 \leq H$ entonces $H' + V_1 \leq H$ así $H' + V_1 \subseteq H$, se verificará ahora que $H \subseteq H' + V_1$. Dado que $u_1, w_2, \ldots w_n$ es una base de G y H un subgrupo de G. Puesto que $h \in H$, existen $\gamma_1, \ldots, \gamma_n$ tales que

$$h = \gamma_1 u_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n,$$

con $\gamma_1 = \alpha_1 q + r_1$ $(0 \leq r_1 < \alpha_1)$ y por consiguiente se tiene que

$$\begin{aligned} h &= (\alpha_1 q + r_1)u_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n \\ &= \alpha_1 q u_1 + r_1 u_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n \\ &= q(\alpha_1 u_1) + r_1 u_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n \\ &= q v_1 + r_1 u_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n \end{aligned}$$

así $h - q v_1 = r_1 u_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n$. Luego por la minimalidad de α_1 se tiene que $r_1 = 0$, por lo tanto $h - q v_1 \in H'$; esto concluye que $h \in H' + V_1$. De esto se deduce que H es un subgrupo abeliano libre de G con rango $s \leq n$ donde $v_1 = \alpha_1 u_1, \ldots, v_s = \alpha_s u_s$ es una base de H.

□

A continuación, se presentará un teorema que será útil para realizar las demostraciones de Teorema 2.3.4 y Teorema 2.4.2. No se hará la demostración del teorema siguiente debido a que se desvía un poco al tema central del trabajo de grado.

Teorema 1.1.4. 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.

Demostración. Ver [2] Teorema 1.17.

□

Definición 1.1.5. Sean I, J ideales de R, si $I|J$ entonces existe un $L \in R$ tal que $LI = J$.

Definición 1.1.6. Sea $R[t_1, t_2, \ldots, t_n]$ el anillo de polinomios en indeterminadas $t_1, t_2, \ldots, t_n$ con coeficientes en R. Sea S_n el grupo simétrico de permutaciones sobre $\{1, 2, \ldots, n\}$.

Para cualquier permutación $\pi \in S_n$ y cualquier polinomio $f \in R[t_1, t_2, \ldots, t_n]$ se define el **polinomio simétrico** f^* como

$$f^*(t_1, \ldots, t_n) = f(t_{\pi(1)}, \ldots, t_{\pi(n)}).$$

Definición 1.1.7. Un anillo R es **noetheriano** si cada ideal I a la izquierda de R es finitamente generado, es decir, existen elementos $a_1, \ldots, a_n$ de I tal que $I = Ra_1 + Ra_2 + \cdots + Ra_n$.

El siguiente resultado presenta una caracterización de anillos noetherianos.

Proposición 1.1.8. Para un anillo R, e ideales a la izquierda de R, se tiene las siguientes propiedades:

1. R es noetheriano.
2. Toda cadena ascendente de ideales a la izquierda de R

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

   es estacionaria, es decir, existe un entero m tal que $I_m = I_{m+1} = \cdots$.

3. R satisface la condición maximal, es decir, cada familia no vacía de ideales a la izquierda de R tiene un elemento maximal.

Demostración. $1) \Rightarrow 2)$ Considere una cadena

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

Sea $I = \bigcup_{n=1}^{\infty} I_n$. Entonces I es un ideal, luego por $\mathbf{1}$. es finitamente generado, es decir, $I = \langle x_1, \ldots, x_m \rangle$ donde cada x_i pertenece a algún $I_{n(i)}$. Si $N = \max_i n(i)$, entonces se tiene que $I = I_N$, es decir, $I_n = I_N$ para todo $n \geq N$ probando $\mathbf{2}$.

$2) \Rightarrow 3)$ Tome una familia no vacía de ideales S. Se supone por contradicción que S no tiene un elemento maximal, es decir, sea $I_0 \in S$, donde I_0 no es maximal así es posible elegir $I_1 \in S$ con $I_0 \subsetneq I_1$ inductivamente, habiendo encontrado I_n, ya que este no es maximal, se puede escoger $I_{n+1} \in S$ con $I_n \subsetneq I_{n+1}$. Ahora se tiene que una cadena ascendente la cual no se estaciona, lo cual contradice la hipótesis.

$3) \Rightarrow 1)$ Sea I cualquier ideal, y sea S el conjunto de todos los ideales finitamente generados que están contenidos en I. Se tiene que $\{0\} \in S$, entonces S es diferente de vacío y así S tiene un elemento maximal J. Si $J \neq I$, se escoge $x \in I \setminus J$; por lo tanto $\langle J, x \rangle$ es finitamente generado y estrictamente mayor que J, lo cual es una contradicción, por consiguiente $J = I$ e I es finitamente generado.

□

Se finaliza esta sección con unos ejemplos que ayudarán a ilustrar las definiciones.

Ejemplo 1.1.9.

- El anillo $\mathbb{Z}$ es un DIP y por lo tanto es noetheriano. En general todo dominio de ideales principales son noetherianos.
- Cualquier cuerpo y en particular $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son noetherianos.
- Los anillos de polinomios sobre un anillo noetheriano son noetherianos.

  Ver en [3], el teorema de la base de Hilbert.

---

[3] JACOBSON, Nathan. *Basic Algebra: Second Edition (2th ed)*. Vol. 2. W.H. Freeman y Company, 1989.

1.2. MÓDULOS E IDEALES FRACCIONARIOS

En esta sección se introducen las definiciones básicas de módulos y submódulos de [4], útiles en la definición de ideal fraccionario de [5], que se utilizará en las próximas secciones.

Definición 1.2.1. Sea $(M, +)$ un grupo abeliano y $(A, +, \cdot, 1)$ un anillo. Se dice que M tiene una estructura de **módulo** a la derecha sobre el anillo A, si se ha definido un producto entre elementos de M y de A

$$M \times A \longrightarrow M$$
$$(m, a) \longmapsto m \cdot a$$

para el cual se cumplen las siguientes condiciones:

1. $(m_1 + m_2) \cdot a = m_1 \cdot a + m_2 \cdot a$,
2. $m \cdot (a_1 + a_2) = m \cdot a_1 + m \cdot a_2$,
3. $m \cdot (a_1 \cdot a_2) = (m \cdot a_1) \cdot a_2$,
4. $m \cdot 1 = m$.

con $m, m_1, m_2 \in M$ y $a, a_1, a_2 \in A$.
De manera similar se definen los A-módulos a izquierda y en general los A-módulo bilateral.

---

[4] LEZAMA, Oswaldo. *Cuadernos de Álgebra N° 6, Anillos y Módulos*. `http://gfnun.unal.edu.co/fileadmin/content/seminarios/sac2/cuadernos/anillosymodulos.pdf`. 2014.

[5] SUÁREZ, Mariano. *Dominios de Dedekind*. `http://mate.dm.uba.ar/~nbotbol/algebraII20092/apuntes/dedekind.pdf`. 2007.

Definición 1.2.2. Sea M un A-módulo y N un subconjunto no vacío de M. Se dice que N es un A**-submódulo** de M, si N es un subgrupo del grupo $(M, +)$, y además

$$n \cdot a \in N, \ para\ cada\ n \in N\ y\ cada\ a \in A$$

se escribe $N \leq M$.

Definición 1.2.3. Sean A un dominio y $\mathbb{F}$ su cuerpo de fracciones. Entonces un A-submódulo $I \subset \mathbb{F}$ es llamado un **ideal fraccionario** de A si existe algún $c \in A$ distinto de cero tal que $cI \subset A$.

Ejemplo 1.2.4. Los ideales fraccionarios de $\mathbb{Z}$ son de la forma $r\mathbb{Z}$ donde $r \in \mathbb{Q}$.
En particular si $A = \mathbb{Z}$ e

$$I = \left\{ \frac{n}{25} : n \in \mathbb{Z} \right\}.$$

I es un subconjunto no vacío de $\mathbb{Q}$ y $25I = \mathbb{Z}$. Por lo tanto, I es un ideal fraccionario de $\mathbb{Z}$.

Ejemplo 1.2.5. Sea $A = \mathbb{Z}$ y sea

$$I = \left\{ \frac{n}{5^m} : n \in \mathbb{Z}, m \in \mathbb{N} \right\}.$$

I es un subconjunto no vacío de $\mathbb{Q}$. Sin embargo, no existe $k \in \mathbb{Z}$ tal que $kI \subseteq \mathbb{Z}$. En efecto, sea $k \in \mathbb{Z}$ entonces existe $r \in \mathbb{N}$ máximo tal que $5^r | k$ y dada la definición del ideal I se tiene que $\frac{n}{5^{r+1}} \in I$, esto implica que $kI \nsubseteq \mathbb{Z}$. Por lo tanto I no es un ideal fraccionario.

2. NÚMEROS ALGEBRAICOS E IDEALES

En esta sección se presentará los números algebraicos los cuales son soluciones de ecuaciones polinómicas con coeficientes enteros. Entre estos números, los principales actores son las soluciones de ecuaciones polinomiales, cuyo coeficiente principal es 1. Estas raíces se llamarán enteros algebraicos.

Comenzando con cuerpos de números algebraicos los cuales tendrán estructura de subcuerpo del cuerpo de números complejos que obedecen a una condición de finitud: son de dimensión finita como espacios vectoriales sobre los racionales, es decir extensiones finitas de cuerpo así se deducirá que dichos cuerpos son de la forma $\mathbb{Q}(\theta)$ para algún número algebraico θ.

Se introduce la conjugada de un número algebraico y el discriminate de la base para $\mathbb{Q}(\theta)$ sobre $\mathbb{Q}$, utilizando la conjugada de θ se mostrará que el discriminante es siempre un número racional diferente de cero, y que el anillo de enteros algebraicos sobre un cuerpo numérico tiene una base integral (base entera) cuyo discriminante es un número entero; este entero es independiente de la elección de la base integral y es llamado el discriminante del cuerpo numérico.

Finalmente, se presenta la norma y la traza de un número algebraico, que resultan ser enteros ordinarios cuando el número algebraico es un entero algebraico.

2.1. NÚMEROS ALGEBRAICOS Y CUERPOS NUMÉRICOS

Definición 2.1.1. Un número complejo α es llamado **algebraico** si es algebraico sobre $\mathbb{Q}$, es decir, existe $p(x) \in \mathbb{Q}[x]$ con $p(x) \neq 0$ tal que $p(\alpha) = 0$. Si $p(x) \in \mathbb{Z}[x]$ con $p(x)$ un polinomio minimal entonces se dice que α es entero algebraico.

Ejemplo 2.1.2. 1. El número $z = \dfrac{1 + i\sqrt{3}}{2}$, es algebraico y un entero algebraico, porque su polinomio minimal es $x^2 - x + 1$.

2. El número $z = \dfrac{1+i\sqrt{5}}{2}$, es algebraico pero no es un entero algebraico, porque su polinomio minimal es $x^2 - x + \frac{3}{2}$.

Lema 2.1.3. Un entero algebraico es un número racional si y solo si este es un entero racional. Equivalentemente $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$, donde $\mathbb{B}$ es el conjunto de enteros algebraicos.

Demostración. Se tiene que $\mathbb{Z} \subseteq \mathbb{B} \cap \mathbb{Q}$. Sea $\alpha \in \mathbb{B} \cap \mathbb{Q}$, así $\alpha \in \mathbb{B}$ por lo tanto α es un entero algebraico y $\alpha \in \mathbb{Q}$ donde $p(t) = t - \alpha$ es el polinomio minimal sobre $\mathbb{Q}$. Luego por la Definición 2.1.1, $p(t) = t - \alpha$ es el polinomio minimal sobre $\mathbb{Q}$ con coeficientes en $\mathbb{Z}$, por consiguiente $-\alpha \in \mathbb{Z}$ lo que se concluye que $\alpha \in \mathbb{Z}$.

□

Definición 2.1.4. Si $\mathbb{K}/\mathbb{Q}$ es una extensión de cuerpos, entonces $\mathbb{K}$ tiene una estructura natural como un espacio vectorial sobre $\mathbb{Q}$. La dimensión de este espacio vectorial es llamado **el grado de la extensión** o el grado de $\mathbb{K}$ sobre $\mathbb{Q}$ y se escribe como $[\mathbb{K} : \mathbb{Q}]$.

Teorema 2.1.5. Sea F/K una extensión de cuerpos y L un cuerpo intermedio. Entonces F/K es finita si y solo si las extensiones F/L y L/K son ambas finitas. Y, en este caso, se verifica que:

$$[F : K] = [F : L][L : K].$$

Ver en [6]

Demostración. $\Rightarrow$) Suponga que F/K es finita. Como L es un subespacio vectorial de F sobre K claramente L/K es finita. Por otro lado si $\{\alpha_1, \ldots, \alpha_n\}$ es un conjunto generador de F como espacio vectorial sobre K, también lo será como espacio

---

[6] GÓMEZ SAURA, David. "Cuerpos finitos". España: Universidad de Murcia, 2014-2015.

vectorial sobre L luego F/L es finita.

$\Leftarrow$) Suponga que F/L y L/K son finitas y sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_m\}$ bases de F como espacio vectorial sobre L y de L como espacio sobre K respectivamente; se probará que $\{\alpha_j\beta_i : 1 \leq j \leq n, 1 \leq i \leq m\}$ es una base de F como espacio vectorial sobre L se tiene que

$$\theta = \sum_{1\leq j\leq n} b_j\alpha_j \textit{ donde } b_j \in L \ \forall j = 1, \ldots, n$$

y, por ser $\{\beta_1, \ldots, \beta_m\}$ una base de L como espacio vectorial sobre K, para cada b_j se tendrá que

$$b_j = \sum_{1\leq i\leq m} a_{ij}\beta_i \textit{ donde } a_{ij} \in K \ \forall i = 1, \ldots, m.$$

Sustituyendo estas expresiones en la anterior, se obtiene

$$\theta = \sum_{1\leq j\leq n} b_j\alpha_j = \sum_{1\leq j\leq n} \left(\sum_{1\leq i\leq m} a_{ij}\beta_i \right) \alpha_j = \sum_{\substack{1\leq j\leq n \\ 1\leq i\leq m}} a_{ij}(\beta_i\alpha_j).$$

Se ha visto que $\{\alpha_j\beta_i : 1 \leq j \leq n, \ 1 \leq i \leq m\}$ es un conjunto generador; se verá ahora que es linealmente independiente. Sean $a_{ij} \in K$ tales que

$$\sum_{\substack{1\leq j\leq n \\ 1\leq i\leq m}} a_{ij}(\beta_i\alpha_j) = 0.$$

Entonces por la independencia lineal de los α_j, se tiene que, para cada j

$$\sum_{1\leq i\leq m} a_{ij}\beta_j = 0$$

y de nuevo por la independencia lineal de los $\beta_i, a_{ij} = 0$ para todo $i = 1, \ldots, m$ y todo

$j = 1, \ldots, n$.

□

Definición 2.1.6. Sea $A \subset \mathbb{C}$ y K un subcuerpo de $\mathbb{C}$

1. $K[\alpha]$ es el anillo de polinomios sobre el cuerpo K en α, con

$$K[\alpha] = \{a_n\alpha^n + \cdots + a_0 \,:\, a_n, \ldots, a_1, a_0 \in K\}.$$

2. Se denota por $K(A)$ a la intersección de todos los cuerpos intermedios $K \subseteq L \subseteq \mathbb{C}$ tal que $A \subset L$. Esto resulta ser también un cuerpo intermedio de $\mathbb{C}/K$. Claramente, $K(A)$ es el cuerpo intermedio más pequeño que contiene a todo A. Se dice que $K(A)$ se obtiene de K adjuntando los elementos de A al cuerpo base K. Se puede describir $K(A)$ como:

$$K(A) = \left\{ \frac{f(\alpha)}{g(\alpha)} \,:\, \alpha \in A\, f, g \in K[x],\, g(\alpha) \neq 0 \right\},$$

   pues el lado derecho es un cuerpo que está contenido en $K(A)$.[7]

Proposición 2.1.7. Un polinomio irreducible sobre un subcuerpo K de $\mathbb{C}$ no tiene ceros múltiples en $\mathbb{C}$.

Demostración. Ver en [2], Corolario 1.6.

□

Teorema 2.1.8. Si L/K es una extensión de cuerpos y $\alpha \in L$, entonces α es algebraico sobre K si y solo si $K(\alpha)$ es una extensión finita de K. En este caso, $[K(\alpha) : K] = \partial p$ donde p es el polinomio minimal de α sobre K, y $K(\alpha) = K[\alpha]$.

---

[7] SPINDLER, Karlheinz. *Abstract Algebra with Aplications*. Vol. 2. New York: Marcel Dekker, INC, 1994.

Demostración. Suponga que $[K(\alpha) : K] = n < \infty$, las potencias $1, \alpha, \alpha^2, \ldots, \alpha^n \in K(\alpha)$ son linealmente dependientes sobre K, así existen

$$a_0(1) + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0, \quad (a_i \in K\, i = 1, \ldots, n)$$

por lo tanto α es algebraico sobre K.

Recíprocamente, suponga que α es algebraico con polinomio minimal p de grado m. Se verá que $K(\alpha)$ es el espacio vectorial sobre K generado por $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$. Se puede ver que $\alpha^m = -p(\alpha) + \alpha^m$ puesto que $p(\alpha) = 0$ por ser α algebraico, luego $\alpha^m = -p(\alpha) + \alpha^m = q(\alpha)$ donde $\partial q < m$ (∂q es el grado del polinomio q), es decir α^m se puede expresar como un polinomio de grado menor que m, entonces cualquier potencia mayor que m se puede escribir como un polinomio de grado menor que m. Si $0 \neq v \in K[\alpha]$ entonces por lo que se acaba de mostrar, se puede escribir $v = h(\alpha)$ donde $h \in K[t]$ y $\partial h < m$. Como p es el polinomio minimal entonces p es irreducible, por lo tanto p y h son primos relativos, así existen $f, g \in K[t]$ tal que

$$f(t)p(t) + g(t)h(t) = 1.$$

Entonces

$$\begin{aligned} 1 &= f(\alpha)p(\alpha) + g(\alpha)h(\alpha), \\ 1 &= f(\alpha)(0) + g(\alpha)h(\alpha), \\ 1 &= g(\alpha)h(\alpha), \end{aligned}$$

de manera que $\frac{1}{v} = \frac{1}{h(\alpha)} = g(\alpha) \in K[\alpha]$, y luego $g(\alpha)$ se puede ver como un polinomio de grado $< m$. Por lo tanto, es posible describir al cuerpo $K(\alpha)$ como

$$K(\alpha) = \{f(\alpha) : f(x) \in K[x], \partial f < \partial p\}.$$

Luego $K(\alpha)$ es un espacio vectorial sobre K generado por $1, \alpha, \ldots, \alpha^{m-1}$. Así $[K(\alpha) : K] = dim_K K(\alpha) = m$.

□

Teorema 2.1.9. El conjunto de números algebraicos es un subcuerpo de el cuerpo de los complejos $\mathbb{C}$.

Demostración. Por el Teorema 2.1.8 se tiene que α es algebraico si y solo si $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es finito. Suponga que α, β son algebraicos, entonces por el Teorema 2.1.5 se tiene que

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Como α es algebraico, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es finito, ahora dado que β es algebraico sobre $\mathbb{Q}$, es decir, existe un polinomio $p(t)$ con coeficientes en $\mathbb{Q}$ tal que $p(\beta) = 0$. Dado que los coeficientes de $p(t)$ también están en $\mathbb{Q}(\alpha)$ ($\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$) entonces β es algebraico sobre $\mathbb{Q}(\alpha)$, así que $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ es finito; por lo tanto $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ es finito, de modo que $\alpha + \beta, \alpha\beta$ y para $\beta \neq 0$, α/β pertenecen a $\mathbb{Q}(\alpha, \beta)$, por ser $\mathbb{Q}(\alpha, \beta)$ un cuerpo y $\mathbb{Q}(\alpha, \beta)$ está contenido en el conjunto de números algebraicos $\mathbb{A}$ entonces $\alpha + \beta, \alpha\beta$ y α/β están en $\mathbb{A}$ lo que implica que $\mathbb{A}$ es cuerpo, en consecuencia $\mathbb{A}$ es un subcuerpo de los $\mathbb{C}$.

□

Antes de continuar con el estudio de números algebraicos se recordarán algunas nociones sobre extensiones de cuerpos.

Definición 2.1.10. Sea $\mathbb{K}/\mathbb{Q}$. Si $\alpha_1, \ldots \alpha_n \in \mathbb{K}$, por el item 2. de la Definición 2.1.6 se escribe a $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ como el subcuerpo de $\mathbb{K}$ más pequeño que contiene a $\mathbb{Q}$ y los elementos $\alpha_1, \ldots, \alpha_n$.

Se define un cuerpo numérico $\mathbb{K}$, como un subcuerpo de $\mathbb{C}$ tal que $[\mathbb{K} : \mathbb{Q}]$ es finito. Esto implica que todo elemento de $\mathbb{K}$ es algebraico sobre $\mathbb{Q}$.

Si $\mathbb{K}$ es un cuerpo numérico entonces $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ para un número finito de números algebraicos $\alpha_1, \ldots, \alpha_n$ (por ejemplo, una base para $\mathbb{K}$ como espacio vectorial sobre $\mathbb{Q}$).

El siguiente resultado muestra que es posible reducir la cantidad de elementos $\alpha_1, \ldots \alpha_n$ a uno solo, este se le conoce como el **Teorema del elemento primitivo**.

Teorema 2.1.11. Si $\mathbb{K}$ es un cuerpo numérico entonces $\mathbb{K} = \mathbb{Q}(\theta)$ para algún número algebraico θ.

Demostración. Se verá que si $\mathbb{K} = \mathbb{Q}(\alpha, \beta)$ entonces $\mathbb{K} = \mathbb{Q}(\theta)$ para algún $\theta \in \mathbb{K}$. Sea $\theta = \alpha + f\beta$ donde $f \in \mathbb{Q}$. Note que $\theta \in \mathbb{K}$ puesto que $f \in \mathbb{Q}$ y $\alpha, \beta \in \mathbb{K}$. Sea $h(x)$ el polinomio minimal de β sobre $\mathbb{Q}$ y $g(x)$ el polinomio minimal de α sobre $\mathbb{Q}$, entonces $g(x), h(x)$ están en $\mathbb{Q}[x]$ y son irreducibles sobre $\mathbb{Q}$, luego

$$g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) = \prod_{i=1}^{m} (x - \alpha_i),$$

$$h(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_n) = \prod_{j=1}^{n} (x - \beta_j),$$

donde $m = \partial g$, $n = \partial h$, por el Corolario 2.1.7, los $\alpha_1, \ldots, \alpha_m$, $\beta_1, \ldots, \beta_n$ son todos elementos distintos que están en $\mathbb{C}$. Se escogerá la numeración de tal forma que $\alpha = \alpha_1$ y $\beta = \beta_1$, luego para cada $1 \leq i \leq m$ y $2 \leq j \leq n$ existe a lo más un elemento $f \in \mathbb{Q}$ tal que

$$\alpha_i + f\beta_j = \alpha + f\beta.$$

Puesto que $\mathbb{Q}$ es infinito, se puede suponer que a partir de aquí se elige f de modo que

$$\alpha + f\beta = \theta \neq \alpha_i + f\beta_j, \tag{2}$$

para todo $1 \leq i \leq m$ y $2 \leq j \leq n$.

Note que $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$ y es suficiente demostrar que $\beta \in \mathbb{Q}(\theta)$, puesto que $\alpha = \theta - f\beta$. Ahora

$$g(\theta - f\beta) = g(\alpha) = 0,$$

y se define el polinomio

$$r(x) = g(\theta - fx) \in \mathbb{Q}(\theta)[x]$$

entonces β es un cero de $h(x)$ y $r(x)$ como polinomios sobre $\mathbb{Q}(\theta)$. Se afirma que $h(x)$ y $r(x)$ tienen a β como el único cero en común. Para esto suponga que $h(\zeta) = r(\zeta) = 0$ entonces $\zeta \in \{\beta_1, \ldots, \beta_n\}$ y $\theta - f\zeta \in \{\alpha_1, \ldots, \alpha_m\}$; así $\zeta = \beta_j$, y además

$$\begin{aligned} \theta - f\zeta &= \alpha_i \\ \theta - f\beta_j &= \alpha_i \\ \alpha_i + f\beta_j &= \theta, \end{aligned}$$

la cual contradice la ecuación (7), por lo tanto $\zeta = \beta$.
Sea $p(x)$ el polinomio minimal de β sobre $\mathbb{Q}(\theta)$, entonces $p(x)|h(x)$ y $p(x)|r(x)$, así como h y r tienen un solo cero en común en $\mathbb{C}$ se tiene que el $\partial p = 1$, entonces

$$p(x) = x + \mu,$$

para $\mu \in \mathbb{Q}(\theta)$. Ahora $0 = p(\beta) = \beta + \mu$ de forma que $\beta = -\mu$ con $-\mu \in \mathbb{Q}(\theta)$, así $\beta \in \mathbb{Q}(\theta)$. Por consiguiente $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$.
Para terminar la demostración se puede encontrar un subconjunto finito $\{\gamma_1, \ldots, \gamma_k\}$ de $\mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\gamma_1, \ldots, \gamma_k)$, entonces por lo hecho anteriormente

$$\begin{aligned} \mathbb{K} &= \mathbb{Q}(\gamma_1, \ldots, \gamma_k), \\ &= \mathbb{Q}(\gamma_1, \gamma_2)(\gamma_3, \ldots, \gamma_k), \\ &= \mathbb{Q}(\theta_1, \gamma_3, \ldots, \gamma_k), \end{aligned}$$

continuando la inducción se encontrará un conjunto generado para $\mathbb{K}/\mathbb{Q}$ con solo un elemento, es decir si $\mathbb{K} = \mathbb{Q}(\gamma_1, \ldots, \gamma_k)$ entonces $\mathbb{K} = \mathbb{Q}(\theta)$ para algún número algebraico θ.

□

Ejemplo 2.1.12. Sea $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, con

$$p(x) = x^2 - 2 \text{ polinomio minimal de } \alpha = \sqrt{2},$$

$$q(x) = x^3 - 5 \text{ polinomio minimal de } \beta = \sqrt[3]{5}.$$

se verá que $\mathbb{K} = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$

Primero se van a encontrar sus respectivas raíces en $\mathbb{C}$:

- $$p(x) = 0 \Rightarrow x^2 - 2 = 0 \Rightarrow (x - \sqrt{2})(x + \sqrt{2}) = 0,$$

  $$\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}.$$

- $$q(x) = 0 \Rightarrow x^3 - 5 = 0 \Rightarrow (x - \sqrt[3]{5})(x^2 + \sqrt[3]{5}x + \sqrt[3]{5^2}) = 0,$$

  $$\beta_1 = \sqrt[3]{5},$$

$$\begin{aligned}
\beta_2 &= \frac{-\sqrt[3]{5} + \sqrt{\sqrt[3]{5}^2 - 4(1)(\sqrt[3]{5})^2}}{2}, \\
&= \frac{-\sqrt[3]{5} + \sqrt{-3(\sqrt[3]{5})^2}}{2}, \\
&= \frac{-\sqrt[3]{5} + \sqrt[3]{5}\sqrt{-3}}{2}, \\
&= \sqrt[3]{5}\left(\frac{1}{2}(-1+\sqrt{-3})\right) \\
&= \sqrt[3]{5}\omega,
\end{aligned}$$

donde $\omega = \frac{1}{2}(-1+\sqrt{-3})$,

$$\begin{aligned}
\beta_3 &= \frac{-\sqrt[3]{5} - \sqrt{\sqrt[3]{5}^2 - 4(1)(\sqrt[3]{5})^2}}{2}, \\
&= \frac{-\sqrt[3]{5} - \sqrt{-3(\sqrt[3]{5})^2}}{2}, \\
&= \frac{-\sqrt[3]{5} - \sqrt[3]{5}\sqrt{-3}}{2}, \\
&= \sqrt[3]{5}\left(\frac{1}{2}(-1-\sqrt{-3})\right), \\
&= \sqrt[3]{5}\left(\frac{1}{4}(-2-2\sqrt{-3})\right), \\
&= \sqrt[3]{5}\left(\frac{1}{4}(1-2\sqrt{-3}-3)\right), \\
&= \sqrt[3]{5}\left(\frac{1}{2}(-1+\sqrt{-3})\right)^2, \\
&= \sqrt[3]{5}\omega^2,
\end{aligned}$$

Luego para que $c \in \mathbb{R}, c \neq 0$ se satisface

$$\alpha_i + c\beta_k \neq \alpha + c\beta, \tag{3}$$

para $i = 1, 2$ y $k = 2, 3$. Entonces

$$\begin{aligned}
\alpha_1 + c\beta_2 &= \sqrt{2} + c(\omega\sqrt[3]{5}),\\
\alpha_1 + c\beta_3 &= \sqrt{2} + c(\omega^2\sqrt[3]{5}),\\
\alpha_2 + c\beta_2 &= -\sqrt{2} + c(\omega\sqrt[3]{5}),\\
\alpha_2 + c\beta_3 &= -\sqrt{2} + c(\omega^2\sqrt[3]{5}),
\end{aligned}$$

note que para cualquier $c \in \mathbb{R}$ estos números no son reales ya que ω, ω^2 no son números reales, por lo tanto el número $c = 1$ satisface (3), es decir $\alpha + (1)\beta = \sqrt{2} + \sqrt[3]{5}$. Así se tiene que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$.

La expresión de $\mathbb{K}$ como $\mathbb{Q}(\theta)$ no es única ya que se puede escribir como $\mathbb{Q}(\theta) = \mathbb{Q}(-\theta) = \mathbb{Q}(\theta + 1) = \ldots$

Definición 2.1.13. Suponga E un cuerpo y R un subanillo de E, se dice que un elemento $u \in E$ es **integral sobre** R o R**-integral** si existe un polinomio mónico $f(x) \in R[x]$ tal que $f(u) = 0$.[3]

Lema 2.1.14. Sea un anillo $R \subseteq \mathbb{C}$. Un número complejo θ es integral sobre R si y solo si $R[\theta]$ es finitamente generado como R-módulo.

Demostración. $\Rightarrow$) Si θ es integral sobre R, entonces para algún n se tiene

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_0 = 0, \tag{4}$$

donde $a_i \in R$. Luego cada potencia de θ está en el R-módulo $R[\theta]$, generado por $1, \theta, \ldots, \theta^{n-1}$, puesto que por la ecuación (4)

$$\theta^n = -a_{n-1}\theta^{n-1} - \cdots - a_0 \in R[\theta],$$

y multiplicando por θ la ecuación (4) se tiene que

$$\begin{aligned}\theta\theta^n + a_{n-1}\theta\theta^{n-1} + \cdots + a_0\theta = 0,\\ \theta^{n+1} + a_{n-1}\theta^n + \cdots + a_0\theta = 0,\\ \theta^{n+1} = -a_{n-1}\theta^n - \cdots - a_0\theta \in R[\theta],\end{aligned}$$

así sucesivamente. Sea $m \geq n$, haciendo inducción sobre m se tiene que $\theta^i \in R[\theta]$ para todo $i \leq m$, se verá que $\theta^{m+1} \in R[\theta]$, en efecto,

$$\begin{aligned}\theta^{m+1} &= \theta^{m+1-n+n} = \theta^{m+1-n}\theta^n,\\ &= \theta^{m+1-n}(-a_{n-1}\theta^{n-1} - \cdots - a_0),\\ &= -a_{n-1}\theta^{m+1-n}\theta^{n-1} - \cdots - a_0\theta^{m+1-n},\\ &= -a_{n-1}\theta^m - \cdots - a_0\theta^{m+1-n} \in R[\theta],\end{aligned}$$

esto prueba que $R[\theta]$ es finitamente generado.

$\Leftarrow$) Suponga que $R[\theta]$ es finitamente generado, con generadores $v_1, \ldots, v_n$. Es claro que θv_i es un polinomio, por lo tanto existen $b_{ij} \in R$ tales que

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

esto conduce un sistema de ecuaciones homogéneas para los v_i de la forma

$$\begin{aligned}(b_{11} - \theta)v_1 + b_{12}v_2 + \cdots + b_{1n}v_n = 0,\\ b_{21}v_1 + (b_{22} - \theta)v_2 + \cdots + b_{2n}v_n = 0,\\ \vdots\\ b_{n1}v_1 + b_{n2}v_2 + \cdots + (b_{nn} - \theta)v_n = 0,\end{aligned}$$

puesto que existe una solución $v_1, \ldots, v_n \in \mathbb{C}$ diferente a la solución nula, esto implica que el determinante

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

es cero. Note que dicho determinante es el polinomio característico de la transformación $p \mapsto \theta p$ para todo $p \in R[\theta]$, así θ satisface una ecuación polinómica mónica con coeficientes en R, lo cual implica que θ es integral.

□

Lema 2.1.15. Sean $R \subseteq R_1 \subseteq R_2$ anillos tales que R_2 es finitamente generado como R_1-módulo y R_1 es finitamente generado como R-módulo, entonces R_2 es finitamente generado como R-módulo.

Demostración. Sea $v \in R_2$ y $v_1, \ldots, v_n$ generadores de R_2 como R_1-módulo, entonces

$$v = a_1 v_1 + \cdots + a_n v_n,$$

para $a_i \in R_1$ con $(i = 1, \ldots, n)$. Dado que R_1 es finitamente generado, existen $u_1, \ldots, u_m$ generadores de R_1 como R-módulo, ahora como los $a_i \in R_1$ entonces

$$a_i = b_{i1} u_1 + \cdots + b_{im} u_m,$$

para $b_{ij} \in R$ con $i = 1, \ldots, n$ y $j = 1, \ldots, m$. Sustituyendo los a_i en v, se obtiene que

$$v = \sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} b_{ij} u_j \right) v_i, \tag{5}$$

renombrando b_{ij} como c_k donde $1 \leq k = (i-1)m + j \leq nm$ y reetiquetando $u_j v_i \in R_1 R_2 = R_2$ como w_k, entonces reemplazando en la ecuación (5) se tiene que

$$v = \sum_{k=1}^{nm} c_k w_k,$$

donde $w_k \in R_2$ y $c_k \in R$, por lo tanto w_k son generadores para R_2 como R-módulo y R_2 es finitamente generado.

□

2.2. CONJUGADAS Y DISCRIMINANTES

Los distintos ceros en $\mathbb{C}$ de un polinomio minimal de θ sobre $\mathbb{Q}$ se denominan sus $\mathbb{K}-$**conjugadas**, donde $\mathbb{K}$ es el cuerpo numérico y así es posible definir el discriminante de alguna base de $\mathbb{K} = \mathbb{Q}(\theta)$.

Teorema 2.2.1. Sea $\mathbb{K} = \mathbb{Q}(\theta)$ un cuerpo de grado n sobre $\mathbb{Q}$. Entonces existen exactamente n monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$ para $i = 1, 2, \ldots, n$. Los elementos $\sigma_i(\theta) = \theta_i$ son los diferentes ceros en $\mathbb{C}$ del polinomio minimal de θ sobre $\mathbb{Q}$.

Demostración. Sean $\theta_1, \ldots, \theta_n$ los ceros distintos del polinomio minimal p de θ, entonces cada θ_i también tiene un polinomio minimal q, el cual q es irreducible y divide a p ver Definición 1.1.5; así $p = q$. Si $\alpha \in \mathbb{Q}(\theta)$ entonces $\alpha = r(\theta)$ para un único $r \in \mathbb{Q}[t]$ con $\partial r < n$, esto se debe $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ es una base de $\mathbb{K} = \mathbb{Q}(\theta)$; por

lo tanto se tiene que

$$\begin{aligned}
\sigma_i(\alpha) &= \sigma_i(r(\theta)),\\
&= \sigma_i(a_0 + a_1\theta + \cdots + a_n\theta^n),\\
&= \sigma_i(a_0) + \sigma_i(a_1\theta) + \cdots + \sigma_i(a_n\theta^n),\\
&= \sigma_i(a_0) + \sigma_i(a_1)\sigma_i(\theta) + \cdots + \sigma_i(a_n)\sigma_i(\theta^n),\\
&= a_0 + a_1\sigma_i(\theta) + \cdots + a_n\sigma_i(\theta^n),\\
&= a_0 + a_1\theta_i + \cdots + a_n\theta_i^n,\\
&= r(\theta_i).
\end{aligned}$$

Luego existe un único isomorfismo de cuerpos $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ tal que $\sigma_i(r(\theta)) = r(\theta_i)$.

Recíprocamente, si $\sigma : \mathbb{K} \to \mathbb{C}$ es un monomorfismo entonces σ es la identidad en $\mathbb{Q}$. Así se tiene que

$$0 = \sigma(p(\theta)) = p(\sigma(\theta))$$

Lo anterior se da puesto que σ es la identidad en $\mathbb{Q}$, así el 0 lo envía al $0 = p(\theta)$ y σ es un monomorfismo; por lo tanto se concluye que $\sigma(\theta)$ es uno de los θ_i, luego σ es uno de los σ_i.

□

Nota 2.2.2.

- Los elementos $\sigma_i(\alpha)$, para $i = 1, \ldots, n$, son llamadas **$\mathbb{K}$-conjugadas** de α, donde α es un elemento cualquiera de $\mathbb{K}$. Aunque los θ_i son distintos, por ser raíces del polinomio minimal que no tiene raíces múltiples (y son las $\mathbb{K}$-conjugadas de θ) no siempre se da el caso en el cual las $\mathbb{K}$-conjugadas de α son distintas.
- Note que las $\mathbb{K}$-conjugadas de α no necesitan ser elementos de $\mathbb{K}$. Incluso los

θ_i no necesitan ser elementos de $\mathbb{K}$.

Sea $\mathbb{K} = \mathbb{Q}(\theta)$ de grado n y $\{\alpha_1, \ldots, \alpha_n\}$ una base de $\mathbb{K}$ (como espacio vectorial sobre $\mathbb{Q}$). Se define **el discriminante** de esta base como

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

Considerando otra base $\{\beta_1, \ldots, \beta_n\}$ se tiene que

$$\beta_k = \sum_{j=1}^{n} c_{jk}\alpha_j \quad (c_{jk} \in \mathbb{Q}),$$

para $k = 1, \ldots, n$ y $\det(c_{jk}) \neq 0$.

Por el producto de determinantes, el hecho de que los σ_i son monomorfismos, y que

$$[\sigma_i(\beta_k)] = \begin{bmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \cdots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{bmatrix}$$

$$= \begin{bmatrix} \sigma_1(c_{11}\alpha_1 + \cdots + c_{n1}\alpha_n) & \cdots & \sigma_1(c_{1n}\alpha_1 + \cdots + c_{nn}\alpha_n) \\ \vdots & \cdots & \vdots \\ \sigma_n(c_{11}\alpha_1 + \cdots + c_{n1}\alpha_n) & \cdots & \sigma_n(c_{1n}\alpha_1 + \cdots + c_{nn}\alpha_n) \end{bmatrix}$$

$$= \begin{bmatrix} \sigma_1(c_{11})\sigma_1(\alpha_1) + \cdots + \sigma_1(c_{n1})\sigma_1(\alpha_n) & \cdots & \sigma_1(c_{1n})\sigma_1(\alpha_1) + \cdots + \sigma_1(c_{nn})\sigma_1(\alpha_n) \\ \vdots & \cdots & \vdots \\ \sigma_n(c_{11})\sigma_n(\alpha_1) + \cdots + \sigma_n(c_{n1})\sigma_n(\alpha_n) & \cdots & \sigma_n(c_{1n})\sigma_n(\alpha_1) + \cdots +_n (c_{nn})\sigma_n(\alpha_n) \end{bmatrix}$$

$$= \begin{bmatrix} c_{11}\sigma_1(\alpha_1) + \cdots + c_{n1}\sigma_1(\alpha_n) & \cdots & c_{1n}\sigma_1(\alpha_1) + \cdots + c_{nn}\sigma_1(\alpha_n) \\ \vdots & \cdots & \vdots \\ c_{11}\sigma_n(\alpha_1) + \cdots + c_{n1}\sigma_n(\alpha_n) & \cdots & c_{1n}\sigma_n(\alpha_1) + \cdots + c_{nnn}(\alpha_n) \end{bmatrix}$$

$$= \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \cdots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \cdots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix},$$

se muestra que

$$\begin{aligned} \Delta[\beta_1, \ldots, \beta_n] &= \{\det[\sigma_i(\beta_k)]\}^2 \\ &= \left\{ \det \left[\sigma_i \left(\sum_{j=1}^{n} c_{jk}\alpha_j \right) \right] \right\}^2, \\ &= \left\{ \det \left[\sum_{j=1}^{n} \sigma_i \left(c_{jk}\alpha_j \right) \right] \right\}^2, \\ &= \left\{ \det \left[\sum_{j=1}^{n} \sigma_i(c_{jk})\sigma_i(\alpha_j) \right] \right\}^2, \\ &= \left\{ \det \left[\sum_{j=1}^{n} c_{jk}\sigma_i(\alpha_j) \right] \right\}^2, \\ &= \{\det(c_{jk})\}^2 \Delta[\alpha_1, \ldots, \alpha_n]. \end{aligned}$$

La siguiente definición y un resultado auxiliar permitirá calcular discriminantes de ciertas bases de $\mathbb{K}$ sobre $\mathbb{Q}$.

Definición 2.2.3. Una matriz de **Vandermonde** es una matriz cuadrada de la forma

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} & x_2^{n-1} \\ \cdots & \cdots & \vdots & \cdots & \cdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} & x_n^{n-1} \end{bmatrix},$$

donde los x_i son elementos de un cierto cuerpo $\mathbb{F}$.

Teorema 2.2.4. Si $\mathbb{A}$ es una matriz de Vandermonde, entonces

$$\det[\mathbb{A}] = \prod_{1 \leq i < j \leq n} (x_j - x_i),$$

donde el determinante es alternante y el producto de dos alternantes es simétrico.

Demostración. Por inducción sobre el orden, n, de la matriz. Si $n = 1$, no hay nada que mostrar. Sea $n = 2$, luego $\mathbb{A} = \begin{bmatrix} 1 & x_1 \\ 1 & x_2 \end{bmatrix}$ entonces, $\det[\mathbb{A}] = x_2 - x_1$. Ahora, sea $n > 1$ y suponga que el teorema es cierto para cualquier matriz de Vandermonde de tamaño $n - 1$. Sea $\mathbb{A}$ una matriz de Vandermonde de orden n. Usando las operaciones por fila se obtiene

$$\begin{aligned} \det[\mathbb{A}] &= \det \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-2} & x_1^{n-1} \\ 0 & x_2 - x_1 & x_2^2 - x_1^2 & \cdots & x_2^{n-2} - x_1^{n-1} & x_2^{n-1} - x_1^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & x_n - x_1 & x_n^2 - x_1^2 & \cdots & x_n^{n-2} - x_1^{n-2} & x_n^{n-2} - x_1^{n-1} \end{bmatrix} \\ &= \det \begin{bmatrix} x_2 - x_1 & x_2^2 - x_1^2 & \cdots & x_2^{n-2} - x_1^{n-2} & x_2^{n-1} - x_1^{n-1} \\ x_3 - x_1 & x_3^2 - x_1^2 & \cdots & x_3^{n-2} - x_1^{n-2} & x_3^{n-1} - x_1^{n-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ x_n - x_1 & x_n^2 - x_1^2 & \cdots & x_n^{n-2} - x_1^{n-2} & x_n^{n-2} - x_1^{n-1} \end{bmatrix} \end{aligned}$$

$$= \det\left(\begin{bmatrix} x_2 - x_1 & 0 & \cdots & 0 \\ 0 & x_3 - x_1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & x_n - x_1 \end{bmatrix} \begin{bmatrix} 1 & x_2 + x_1 & \cdots & \sum_{i=0}^{n-2} x_2^{n-2-i} x_1^i \\ 1 & x_3 + x_1 & \cdots & \sum_{i=0}^{n-2} x_3^{n-2-i} x_1^i \\ \vdots & \vdots & \cdots & \vdots \\ 1 & x_n + x_1 & \cdots & \sum_{i=0}^{n-2} x_n^{n-2-i} x_1^i \end{bmatrix}\right)$$

$$= \prod_{j=2}^{n}(x_j - x_1) \det \begin{bmatrix} 1 & x_2 + x_1 & \cdots & \sum_{i=0}^{n-2} x_2^{n-2-i} x_1^i \\ 1 & x_3 + x_1 & \cdots & \sum_{i=0}^{n-2} x_3^{n-2-i} x_1^i \\ \vdots & \vdots & \cdots & \vdots \\ 1 & x_n + x_1 & \cdots & \sum_{i=0}^{n-2} x_n^{n-2-i} x_1^i \end{bmatrix}$$

$$= \prod_{j=2}^{n}(x_j - x_1) \det \left(\begin{bmatrix} 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} \end{bmatrix} \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-2} \\ 0 & 1 & x_1 & \cdots & x_1^{n-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}\right)$$

$$= \prod_{j=2}^{n}(x_j - x_1) \det \begin{bmatrix} 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2}, \end{bmatrix}$$

y por la hipótesis inductiva se obtiene

$$\begin{aligned} \det[\mathbb{A}] &= \prod_{j=2}^{n}(x_j - x_1) \prod_{2 \le i < j \le n} (x_j - x_i) \\ &= \prod_{1 \le i < j \le n} (x_j - x_i). \end{aligned}$$

□

El objetivo es probrar que el discriminante de cualquier base es positiva, para esto se enunciará el siguiente Corolario, que se puede ver en [2], Corolario 1.14.

Corolario 2.2.5. Suponga que $\mathbb{K}$ es una extensión del cuerpo $\mathbb{Q}$, $p \in \mathbb{Q}[t]$, $\partial p = n$ y los ceros de p son $\theta_1, \ldots, \theta_n \in \mathbb{K}$. Si $h(t_1, \ldots, t_n) \in \mathbb{Q}[t_1, \ldots, t_n]$ es simétrico entonces $h(\theta_1, \ldots, \theta_n) \in \mathbb{Q}$.

El discriminante de cualquier base para $\mathbb{K} = \mathbb{Q}(\theta)$ es racional y diferente de cero.

Teorema 2.2.6. Si todas las $\mathbb{K}$-conjugadas de θ son números reales entonces el discriminante de cualquier base es positiva.

Demostración. Sea $\{1, \theta, \ldots, \theta^{n-1}\}$ una base. Si las conjugadas de θ son $\theta_1, \ldots, \theta_n$ entonces por la definición de discriminante se tiene que

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

Note que θ_i^j tiene la forma de la matriz de Vandermonde, por lo tanto utilizando la Definición 2.2.3 y el Teorema 2.2.4 se puede ver que

$$\Delta = \Delta[1, \theta, \ldots, \theta^{n-1}] = \left[\prod(\theta_i - \theta_j)\right]^2.$$

y Δ es simétrico, entonces por el Corolario 2.2.5 se tiene que Δ es racional. Dado que θ_i son distintos entonces $\Delta \neq 0$. Ahora, sea $\{\beta_1, \ldots, \beta_n\}$ una base, entonces

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

para ciertos números racionales c_{ik} y $\det[c_{ik}] \neq 0$, por consiguiente

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

y es racional. Claramente si todos los θ_i son reales entonces Δ es un número real positivo, luego también lo es $\Delta[\beta_1, \ldots, \beta_n]$.

□

Lema 2.2.7. Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $\mathbb{K}$ que consta de enteros, entonces el discriminante $\Delta[\alpha_1, \ldots, \alpha_n]$ es un entero diferente de cero.

Demostración. Por el Teorema 2.2.6 se tiene que $\Delta = \Delta[\alpha_1, \ldots, \alpha_n] \neq 0$ es racional, además Δ es un entero puesto que los α_i para todo $i = 1, \ldots, n$ lo son. Así por el Lema 2.1.3, Δ es un entero racional, diferente de cero.

□

2.3. FACTORIZACIÓN PRIMA DE IDEALES

En esta sección se notará por $\mathcal{D} = \mathbb{K} \cap \mathbb{B}$ al anillo de enteros de un cuerpo numérico $\mathbb{K}$ de grado n, donde $\mathbb{B}$ es el conjunto de los enteros algebraicos. Note que $\mathbb{K}$ y $\mathbb{B}$ son subanillos de $\mathbb{C}$ por lo que también lo es $\mathcal{D}$. Además $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{K}$ y $\mathbb{Z} \subseteq \mathbb{B}$; así que $\mathbb{Z} \subseteq \mathcal{D}$.

Definición 2.3.1. Una $\mathbb{Z}$-base para $(\mathcal{D}, +)$ es llamada una **base integral** para $\mathbb{K}$(o para $\mathcal{D}$).

Dicha base existe y esto se demostrará en el Teorema 2.3.3, pero no todas las bases son bases integrales. Por ejemplo, considere $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Claramente el elemento $\frac{1}{2} + \frac{1}{2}\sqrt{5}$ satisace la ecuación

$$t^2 - t - 1 = 0.$$

Por lo tanto, es un entero en $\mathbb{Q}(\sqrt{5})$, pero este no es un elemento de $\mathbb{Z}[\sqrt{5}]$.

Definición 2.3.2. Sea $\mathbb{K} = \mathbb{Q}(\theta)$ un cuerpo numérico de grado n y $\sigma_1, \ldots, \sigma_n$ los monomorfismos de $\mathbb{K} \to \mathbb{C}$, dados por el Teorema 2.2.1. Para algún $\alpha \in \mathbb{K}$ se define la **Norma** como:

$$N(\alpha) = N_{\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \prod_{i=1}^{n} \alpha_i.$$

Teorema 2.3.3. Cada cuerpo numérico $\mathbb{K}$ posee una base integral, y el grupo aditivo de $\mathcal{D}$ es abeliano libre de rango n igual al grado de $\mathbb{K}$.

Demostración. Se tiene que $\mathbb{K} = \mathbb{Q}(\theta)$ para un entero algebraico θ, es decir existen bases para $\mathbb{K}$ que consisten de enteros algebraicos: Por ejemplo $\{1, \theta, \ldots, \theta^{n-1}\}$. Se ha visto que las $\mathbb{Q}$-bases no necesitan ser bases integrales para $\mathbb{K}$. Sin embargo, por el Lema 2.2.7 el discriminante de una $\mathbb{Q}$-base que consta de enteros algebraicos es un entero. Sea $\{\omega_1, \ldots, \omega_n\}$ una base de enteros algebraicos donde $|\Delta\{\omega_1, \ldots, \omega_n\}|$ es la magnitud del discriminante más pequeña. Con estas condiciones $\{\omega_1, \ldots, \omega_n\}$ es una base integral. Suponga que no lo es, entonces existe un entero algebraico ω de $\mathbb{K}$ tal que

$$\omega = a_1\omega_1 + \cdots + a_n\omega_n,$$

para $a_i \in \mathbb{Q}$, no todos nulos en $\mathbb{Z}$ con $i = 1, \ldots, n$. Sea $a_1 \notin \mathbb{Z}$, entonces $a_1 = a + r$, donde $a \in \mathbb{Z}$ y $0 < r < 1$.
Defina

$$\begin{aligned}
\psi_1 &= \omega - a\omega_1, \\
&= a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n - a\omega_1, \\
&= (a_1 - a)\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n,
\end{aligned}$$

$$\psi_i = \omega_i \ \ (i = 2, \ldots, n).$$

De este sistema de ecuaciones se puede notar que

$$\begin{bmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \\ \vdots \\ \psi_n \end{bmatrix} = \begin{bmatrix} a_1 - a & a_2 & a_3 & \dots & a_n \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \\ \vdots \\ \omega_n \end{bmatrix}$$

Así $\{\psi_1, \dots, \psi_n\}$ es una base que consta de enteros algebraicos. Luego el discriminante para el cambio de base de los ω's a los ψ's es

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

entonces

$$\Delta[\psi_1, \dots, \psi_n] = r^2 \Delta[\omega_1, \dots, \omega_n]. \tag{6}$$

Puesto que $0 < r < 1$, la ecuación (6) contradice la minimalidad de $|\Delta\{\omega_1 \dots, \omega_n\}|$ se deduce que $\{\omega_1, \dots, \omega_n\}$ es una base integral, entonces $(\mathcal{D}, +)$ es un grupo abeliano libre de rango n.

□

El siguiente teorema es uno de los principales resultados que se estudia en este trabajo de grado y brindará información importante sobre la estructura del anillo $\mathcal{D}$.

Teorema 2.3.4. El anillo de enteros $\mathcal{D}$ de un cuerpo numérico $\mathbb{K}$ tiene las siguientes propiedades:

a) Es un dominio, con cuerpo de fracciones $\mathbb{K}$.

b) Es un anillo noetheriano.

c) Si $\alpha \in \mathbb{K}$ satisface una ecuación de un polinomio mónico con coeficientes en $\mathcal{D}$ entonces $\alpha \in \mathcal{D}$ ($\mathcal{D}$ es integralmente cerrado).

d) Todo ideal primo de $\mathcal{D}$ no nulo es maximal.

Demostración.

a) $\mathcal{D}$ es un dominio. En efecto:

Se tiene que $\mathcal{D} = \mathbb{K} \cap \mathbb{B}$ donde $\mathbb{K}$ es el cuerpo numérico y $\mathbb{B}$ es el conjunto de los enteros algebraicos, así $\mathcal{D} \subseteq \mathbb{K}$ y $\mathbb{K}$ es un cuerpo; entonces $\mathcal{D}$ no tiene divisores de cero, lo que implica que $\mathcal{D}$ es un Dominio.

Se verá que $\mathbb{K} = \mathbb{F}$, donde $\mathbb{F}$ es el cuerpo de fracciones de $\mathcal{D}$. En efecto, $\mathbb{F}$ es el cuerpo de fracciones, se sabe que $\mathbb{F}$ es el cuerpo más pequeño que contiene a $\mathcal{D}$, así como $\mathcal{D} \subseteq \mathbb{K}$ con $\mathbb{K}$ un cuerpo entonces se deduce que $\mathbb{F} \subseteq \mathbb{K}$.

Sea $b \in \mathbb{K}$, se tiene que b es un número algebraico; por lo tanto

$$a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 = 0, \tag{7}$$

con $a_0, \ldots, a_n \in \mathbb{Q}$, es decir $a_0 = \frac{p_0}{q_0}, \ldots, a_n = \frac{p_n}{q_n}$ con $p_i, q_i \in \mathbb{Z}$ y $q_i \neq 0$ para todo $i = 0, \ldots, n$, así multiplicando por el $mcm(q_0, \ldots, q_n)$ a la ecuación (7) se obtiene

$$c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 = 0, \tag{8}$$

con $c_0, \ldots, c_n \in \mathbb{Z}$, luego se multiplica por c_n^{n-1} a la ecuación (8) y se tiene

$$c_n c_n^{n-1} b^n + c_{n-1} c_n^{n-1} b^{n-1} + \cdots + c_1 c_n^{n-1} b + c_0 c_n^{n-1} = 0,$$

es decir

$$c_n^n b^n + c_{n-1}c_n^{n-1}b^{n-1} + \cdots + c_1 c_n^{n-2} c_n b + c_0 c_n^{n-1} = 0.$$

De donde se obtiene que

$$(c_n b)^n + c_{n-1}(c_n b)^{n-1} + \cdots + c_1 c_n^{n-2}(c_n b) + c_0 c_n^{n-1} = 0,$$

con $c_{n-i}c^{i-1} \in \mathbb{Z}$ para todo $i = 0, \ldots, n$.

Así se conluye que $p(c_n b) = 0$ con $p(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_1 c_n^{n-2} t + c_0 c_n^{n-1}$ un polinomio mónico minimal, por consiguiente se deduce $c_n b \in \mathcal{D}$.

Puesto que $c_n \in \mathbb{Z}$ y $\mathbb{Z} \subseteq \mathcal{D} \subseteq \mathbb{F}$ se tiene que $c_n b, c_n \in \mathbb{F}$, por lo tanto $b = \dfrac{c_n b}{c_n} \in \mathbb{F}$; y en consecuencia $\mathbb{K} \subseteq \mathbb{F}$ por lo tanto $\mathbb{K} = \mathbb{F}$, es decir, $\mathbb{K}$ es el cuerpo de fracciones de $\mathcal{D}$.

b) Note que por el Teorema 2.3.3, $(\mathcal{D}, +)$ es un grupo abeliano libre de rango n. Luego por el Teorema 1.1.3, si I es un ideal de $\mathcal{D}$ entonces $(I, +)$ es abeliano libre de rango $s \leq n$. Así, si $\{x_1, \ldots, x_s\}$ es una $\mathbb{Z}$-base para $(I, +)$, entonces $\langle x_1, \ldots, x_s \rangle = I$, por lo tanto I es un ideal finitamente generado. Lo que implica que $\mathcal{D}$ es noetheriano, por la Proposición 1.1.8.

c) Por hipótesis α satisface una ecuación de un polinomio mónico con coeficientes en $\mathcal{D}$, como $\mathcal{D} = \mathbb{B} \cap \mathbb{K}$, entonces

$$\alpha^n + \psi_{n-1}\alpha^{n-1} + \cdots + \psi_0 = 0, \tag{9}$$

donde $\psi_0, \ldots, \psi_{n-1} \in \mathbb{B}$, es decir $\psi_0, \ldots, \psi_{n-1}$ son enteros algebraicos; en otras palabras $\psi_0, \ldots, \psi_{n-1}$ son integrales sobre $\mathbb{Z}$. Luego como ψ_0, ψ_1 integral sobre $\mathbb{Z}$, por el Lema 2.1.14, $\mathbb{Z}[\psi_0]$ es finitamente generado como $\mathbb{Z}$-módulo y $\mathbb{Z}[\psi_0, \psi_1]$ es finitamente generado como $\mathbb{Z}[\psi_0]$-módulo. Así por el Lema 2.1.15,

$\mathbb{Z}[\psi_0, \psi_1]$ es finitamente generado como $\mathbb{Z}$-módulo. De la misma manera utilizando el Lema 2.1.14, $\mathbb{Z}[\psi_0, \psi_1, \psi_2]$ es finitamente generado como $\mathbb{Z}[\psi_0, \psi_1]$-módulo y por el Lema 2.1.15 $\mathbb{Z}[\psi_0, \psi_1, \psi_2]$ es finitamente generado como $\mathbb{Z}$-módulo. Repitiendo el argumento $n-1$ veces, se obtiene que $\mathbb{Z}[\psi_0, \ldots, \psi_{n-1}]$ es finitamente generado como $\mathbb{Z}$-módulo.

Sea $R_1 = \mathbb{Z}[\psi_0, \ldots, \psi_{n-1}]$, por la ecuación (9) α es integral sobre R_1, luego por el Lema 2.1.14, $R_1[\alpha] = \mathbb{Z}[\psi_0, \ldots, \psi_{n-1}, \alpha]$ es finitamente generado como R_1-módulo, así aplicando de nuevo el Lema 2.1.15, $R_1[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo, es decir $R_1[\alpha]$ es un grupo abeliano libre finitamente generado.

Ahora como $\mathbb{Z}[\alpha]$ es subgrupo de $R_1[\alpha]$ entonces por el Teorema 1.1.3, $\mathbb{Z}[\alpha]$ es abeliano libre finitamente generado, en otras palabras $\mathbb{Z}[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo y por el Lema 2.1.14 α es integral sobre $\mathbb{Z}$ lo que deduce que α es un entero algebraico.

Por último como $\alpha \in \mathbb{K}$ y α es un entero algebraico, es decir $\alpha \in \mathbb{B}$. Entonces $\alpha \in \mathbb{B} \cap \mathbb{K} = \mathcal{D}$.

d) Sea $\mathfrak{p}$ un ideal primo de $\mathcal{D}$ y $0 \neq \alpha \in \mathfrak{p}$ entonces

$$N = N(\alpha) = \alpha_1 \cdots \alpha_n,$$

donde los α_i son las conjugadas de α para todo $i = 1, \ldots, n$; escogiendo $\alpha_1 = \alpha$ se tiene que $N \in \mathfrak{p}$, así la norma es un múltiplo de α lo que implica que $\langle N \rangle \subseteq \mathfrak{p}$ ($N\mathcal{D} = \langle N \rangle$).

Como $\mathfrak{p} \in \mathcal{D}$ entonces $\mathfrak{p}/N\mathcal{D}$ es un anillo cociente de $\mathcal{D}/N\mathcal{D}$ así por el tercer teorema de isomorfismo se tiene que $(\mathcal{D}/N\mathcal{D})/(\mathfrak{p}/N\mathcal{D}) \cong \mathcal{D}/\mathfrak{p}$ entonces $\mathcal{D}/\mathfrak{p}$ es un anillo cociente de $\mathcal{D}/N\mathcal{D}$.

Como $\mathcal{D}$ es subgrupo de $\mathbb{K}$, por el Teorema 1.1.3, $\mathcal{D}$ es un grupo abeliano libre de rango finito n. Sea $v_1, \ldots, v_n$ una base de $\mathcal{D}$, como $N\mathcal{D}$ es un subgrupo de $\mathcal{D}$, de nuevo por el Teorema 1.1.3 se tiene que $N\mathcal{D}$ es un subgrupo abeliano libre de rango finito. $Nv_1, \ldots, Nv_n$ es una base de $N\mathcal{D}$. En efecto,

Sea $\alpha \in N\mathcal{D}$, entonces $\alpha = N\beta$ donde $\beta \in \mathcal{D}$, por lo tanto

$$\beta = a_1 v_1 + \cdots + a_n v_n,$$

luego

$$\begin{aligned} \alpha = N\beta &= N(a_1 v_1 + \cdots + a_n v_n), \\ &= Na_1 v_1 + \cdots + Na_n v_n, \\ &= a_1(Nv_1) + \cdots + a_n(Nv_n). \end{aligned}$$

Ahora se probará que es linelamente independiente. Suponga que

$$a_1(Nv_1) + \cdots + a_n(Nv_n) = 0,$$

como $N \neq 0$, entonces

$$a_1 v_1 + \cdots + a_n v_n = 0,$$

por hipótesis se tiene que $v_1, \ldots, v_n$ es una base de $\mathcal{D}$ entonces

$$a_1 = a_2 = \cdots = a_n = 0.$$

Por lo anterior $Nv_1, \ldots, Nv_n$ es una base de $N\mathcal{D}$, así por el Teorema 1.1.4, $\mathcal{D}/N\mathcal{D}$ es finito. Por consiguiente como $\mathcal{D}/\mathfrak{p}$ es grupo cociente de $\mathcal{D}/N\mathcal{D}$ y $\mathcal{D}/N\mathcal{D}$ es finito entonces $\mathcal{D}/\mathfrak{p}$ es un dominio finito (con 1 y conmutativo), por lo tanto $\mathcal{D}/\mathfrak{p}$ es un cuerpo, lo que concluye que $\mathfrak{p}$ es un ideal maximal.

□

Note que el item d) del Teorema 2.3.4 no se cumple para todos los anillos conmutativos, por ejemplo

Ejemplo 2.3.5. Sea $R = \mathbb{R}[x, y]$ el anillo de polinomios con coeficientes reales.
Se sabe que $\mathbb{R}[y]$ es un dominio, pero no es un cuerpo, puesto que no todos sus elementos son unidad y se tiene que $R/\langle x\rangle \cong \mathbb{R}[y]$, con $\langle x\rangle$ ideal de R. Así, por ser $R/\langle x\rangle$ un dominio entonces $\langle x\rangle$ es un ideal primo y como $R/\langle x\rangle$ no es un cuerpo entonces $\langle x\rangle$ no es un ideal maximal.

Los anillos que satisfacen todos los items del Teorema 2.3.4 son llamados **anillos de Dedekind**, por tanto el anillo de enteros $\mathcal{D}$ es un anillo de Dedekind.

Ejemplo 2.3.6. Todo Dominio de ideales principales (DIP) es un dominio de Dedekind.
En efecto, sea R un DIP con cuerpo de fracciones $\mathbb{K} = \mathbb{Q}(R)$ entonces todo ideal de R es finitamente generado, por lo tanto R es noetheriano. Luego como R es DIP se tiene que R es dominio de factorización única (DFU) y todo DFU es integralmente cerrado (ver en [8]), así R es integralmente cerrado. Por último todo ideal primo no nulo de un DIP es maximal. Por consiguiente se concluye que todo DIP es un dominio de Dedekind.

Teorema 2.3.7.
1. Los ideales fraccionarios de $\mathcal{D}$ diferentes de cero forman un grupo abeliano bajo la multiplicación ($I \cdot J = \{i \cdot j : i \in I, j \in J$; donde I, J son ideales fraccionarios de $\mathcal{D}\}$).

2. Todo ideal de $\mathcal{D}$ diferente de cero puede ser escrito como el producto de ideales primos y este se escribe de manera única excepto por el orden de los

[8] GÓMEZ RÍOS, Jorge. "El Anillo de los Enteros Algebraicos y Dominios de Dedekind". Bucaramanga: Universidad Industrial de Santander, 2015.

factores.

.

Ver demostración completa en [8], Teorema 3.9 y Teorema 3.15. Antes de hacer un bosquejo de la demostración se verán las siguientes observaciones útiles:

a) Sea $I \neq 0$ un ideal de $\mathcal{D}$. Entonces existen ideales primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ tal que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I$.

Por contradicción considere

$C = \{J$ ideal de $\mathcal{D}$: no existen ideales primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ tal que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq J\}$.

Como $C \neq \emptyset$ y $\mathcal{D}$ es noetheriano, entonces existe L un ideal maximal de C, como todo ideal maximal es primo entonces L es primo, así existen ideales M, N de $\mathcal{D}$ con $MN \subseteq L$ y $M \nsubseteq L, N \nsubseteq L$. Sea

$$L_1 = L + M \quad L_2 = L + N,$$

entonces $L_1 L_2 \subseteq L$, pero $L_1 \nsubseteq L$, $L_2 \nsubseteq L$.

Luego por la maximalidad de L existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$ tal que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq L_1$$
$$\mathfrak{p}_{s+1} \cdots \mathfrak{p}_r \subseteq L_2$$

por lo tanto

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq L_1 L_2 \subseteq L$$

contradiciendo a la elección de L.

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

Para cada ideal I de $\mathcal{D}$, se define

$$I^{-1} = \{x \in \mathbb{K} : xI \subseteq \mathcal{D}\}. \tag{10}$$

Es claro que I^{-1} es un $\mathcal{D}$-submódulo. Si $I \neq 0$ entonces para cualquier $c \in I$ con $c \neq 0$ se tiene que $cI^{-1} \subseteq \mathcal{D}$, así por la Definición 1.2.3, I^{-1} es un ideal fraccionario. Claramente $\mathcal{D} \subseteq I^{-1}$, entonces $I = I\mathcal{D} \subseteq II^{-1}$. Por (10)

$$II^{-1} = I^{-1}I \subseteq \mathcal{D}.$$

Esto significa que el ideal fraccionario II^{-1} es en realidad un ideal de $\mathcal{D}$.

Otro dato útil para los ideales I, J es que $J \subseteq I$ implica que

$$\mathcal{D} \subseteq I^{-1} \subseteq J^{-1}. \tag{11}$$

c) Si I es un ideal propio, entonces $I^{-1} \not\supseteq \mathcal{D}$.

Como $I \subseteq \mathfrak{p}$ para algún ideal maximal $\mathfrak{p}$, luego por (11), $\mathfrak{p}^{-1} \subseteq I^{-1}$. Es suficiente probar que $\mathfrak{p}^{-1} \neq \mathcal{D}$ para $\mathfrak{p}$ maximal. Para esto se debe encontrar un número que no está en $\mathcal{D}$ y esté en $\mathfrak{p}^{-1}$.

Para algún $a \in \mathfrak{p}$, $a \neq 0$. Usando el item a) con r el mínimo tal que

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

para $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ primos, por tanto $\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1} \nsubseteq \langle a \rangle$. Puesto que $\langle a \rangle \subseteq \mathfrak{p}$ y $\mathfrak{p}$ es primo, algún $\mathfrak{p}_i \subseteq \mathfrak{p}$ así sin pérdida de generalidad $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Por lo tanto $\mathfrak{p}_1 = \mathfrak{p}$ por el item d) del Teorema 2.3.4 los ideales primos en $\mathcal{D}$ son maximales y

además

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq \langle a \rangle,$$

por la minimalidad de r. Así se puede encontrar un $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus \langle a \rangle$, pero $b\mathfrak{p} \subseteq \langle a \rangle$ entonces $ba^{-1}\mathfrak{p} \subseteq \mathcal{D}$ y por (10) $ba^{-1} \in \mathfrak{p}^{-1}$, pero $b \notin a\mathcal{D}$ entonces $ba^{-1} \notin \mathcal{D}$ lo que concluye que $\mathfrak{p}^{-1} \neq \mathcal{D}$.

d) Si $I \neq 0$ es un ideal y $IS \subseteq I$ para cualquier conjunto $S \subseteq \mathbb{K}$, entonces $S \subseteq \mathcal{D}$.

La demostración es muy parecida al Lema 2.1.14 donde demuestra que θ es integral.

Ahora se procederá con la demostración del Teorema 2.3.7:
Demostración.

1. Se realizará en tres pasos.

   - Si $\mathfrak{p}$ es un ideal maximal, entonces $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{D}$.

     Por $b)$, $\mathfrak{p}\mathfrak{p}^{-1}$ es un ideal donde $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{D}$. Luego como $\mathfrak{p}$ es maximal

     $$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p} \text{ o } \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{D},$$

     si $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ entonces por $d)$ $\mathfrak{p}^{-1} \subseteq \mathcal{D}$ lo que contradice $c)$. Así $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{D}$.

   - Para cada ideal $I \neq 0$, $II^{-1} = \mathcal{D}$.

     Suponga que no, elija $I \neq 0$ maximal sujeto a $II^{-1} = \mathcal{D}$, entonces existe $\mathfrak{p}$ maximal tal que $I \subseteq \mathfrak{p}$; por $b)$ $\mathcal{D} \subseteq \mathfrak{p}^{-1} \subseteq I^{-1}$, así

     $$I \subseteq I\mathfrak{p}^{-1} \subseteq II^{-1} \subseteq \mathcal{D}. \tag{12}$$

     En particular, $I\mathfrak{p}^{-1} \subseteq \mathcal{D}$ entonces $I\mathfrak{p}^{-1}$ es un ideal. Ahora si $I = I\mathfrak{p}^{-1}$ por $d)$ $\mathfrak{p}^{-1} \subseteq \mathcal{D}$ lo cual contradice $c)$, así $I \subsetneq I\mathfrak{p}^{-1}$ y por la condición de

maximalidad de I implica que

$$I\mathfrak{p}^{-1}(I\mathfrak{p}^{-1})^{-1} = \mathcal{D}.$$

Luego por (10)

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

así

$$\mathcal{D} = I\mathfrak{p}^{-1}(I\mathfrak{p}^{-1})^{-1} \subseteq II^{-1} \subseteq \mathcal{D}$$

por lo tanto $II^{-1} = \mathcal{D}$.

- Cada ideal fraccionario I tiene un inverso I^{-1} tal que $II^{-1} = \mathcal{D}$.

  Se sabe que el conjunto de ideales fraccionarios de $\mathcal{D}$ es un semigrupo conmutativo, por lo que dado un ideal fraccionario I, solo se necesita encontrar otro ideal fraccionario $I^{'}$ tal que $II' = \mathcal{D}$, entonces I' será el inverso requerido. Pero existen J un ideal y $c \in \mathcal{D}$, $c \neq 0$ tal que $I = c^{-1}J$. Sea $I' = cJ^{-1}$, entonces $II' = \mathcal{D}$.

2. Se demostrará primero la factorización prima y luego la unicidad.

   - Cada ideal $I \neq 0$ es un producto de ideales primos.

     Por contradicción, suponga que existen ideales que no son producto de ideales primos. Sea $\{I_i\}$ la colección de tales ideales. Puesto que $\mathcal{D}$ es noetheriano existe I elemento maximal de la colección. Entonces I no es primo, pero se tendría que $I \subseteq \mathfrak{p}$ para algún ideal maximal y por (12)

     $$I \subsetneq I\mathfrak{p}^{-1} \subseteq \mathcal{D}.$$

     Como I es maximal

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

para ideales primos $\mathfrak{p}_2 \dots \mathfrak{p}_r$, así

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

- Factorización prima es única.

  Si se tienen ideales primos $\mathfrak{p}_1 \dots \mathfrak{p}_r, \mathfrak{q}_1 \dots \mathfrak{q}_s$ con

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

  entonces $\mathfrak{p}_1$ divide a algún $\mathfrak{q}_i$, luego por la maximalidad, $\mathfrak{p}_1 = \mathfrak{q}_i$. Multiplicando por $\mathfrak{p}_1^{-1}$ y usando inducción se obtiene la unicidad de la factorización hasta el orden de los factores.

□

Teorema 2.3.8. Para ideales I, J de $\mathcal{D}$, $I|J \; si \; y \; solo \; si \; I \supseteq J$.

Demostración. $\Rightarrow$) Por hipótesis $I|J$ entonces existe un ideal L de $\mathcal{D}$ tal que $LI = J$, se tiene que $LI \subseteq I$ por lo tanto $J = LI \subseteq I$.
$\Leftarrow$) Por hipótesis $I \supseteq J$ entonces $\mathcal{D} = I^{-1}I \supseteq I^{-1}J = L$, así existe un ideal L de $\mathcal{D}$ tal que $J = LI$, por lo tanto $I|J$.

□

2.4. NORMA DE UN IDEAL

Note que por el Teorema 2.3.3 el grupo $(\mathcal{D}, +)$ es un grupo abeliano libre de rango n. Luego se tiene que por el Teorema 1.1.3 si I es un ideal de $\mathcal{D}$ entonces $(I, +)$ es un grupo abeliano de rango $k \leq n$, por lo tanto el anillo cociente $\mathcal{D}/I$ es finito, gracias al teorema de Langrage.

Definición 2.4.1. Sea I un ideal de $\mathcal{D}$ entonces la **Norma** de I se define como

$$N(I) = |\mathcal{D}/I|.$$

Claramente $N(I)$ es un entero positivo.

Se mostrará una relación entre normas y discriminantes, en efecto se tiene el siguiente Teorema.

Teorema 2.4.2. 1. Todo ideal I de $\mathcal{D}$ con $I \neq 0$ tiene una $\mathbb{Z}$-base $\{\alpha_1, \ldots, \alpha_n\}$ donde n es el grado de $\mathbb{K}$.

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

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

Demostración.

1. Por el Teorema 2.3.3 se tiene que $(\mathcal{D}, +)$ es abeliano libre de rango n igual al grado de $\mathbb{K}$. Puesto que por la Definición 2.4.1, $N(I) = |\mathcal{D}/I|$ es un entero positivo y asi $\mathcal{D}/I$ es finito entonces por el Teorema 1.1.4 $(I, +)$ es abeliano libre de rango n, por lo tanto I tiene una $\mathbb{Z}$-base de la forma $\{\alpha_1, \ldots, \alpha_n\}$.

2. Sea $\{\omega_1, \ldots, \omega_n\}$ una $\mathbb{Z}$-base para $\mathcal{D}$ y suponga que $\alpha_i = \sum_{j=1}^{n} c_{ij}\omega_j$. Entonces por el Teorema 1.1.4 y la Definición 2.4.1

   $$N(I) = |\mathcal{D}/I| = |det[c_{ij}]|. \tag{13}$$

   Luego por la definición de discriminante

   $$\Delta[\alpha_1, \ldots, \alpha_n] = (det[c_{ij}])^2 \Delta[\omega_1, \ldots, \omega_n], \tag{14}$$

ahora reemplazando $N(I)$ de la ecuación (13) en la ecuación (14) se obtiene

$$\Delta[\alpha_1, \ldots, \alpha_n] = (N(I))^2 \Delta, \tag{15}$$

así despejando $N(I)$ de la ecuación (15) se tiene que

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

□

Corolario 2.4.3. Si $I = \langle a \rangle$ es un ideal principal de cualquier anillo R entonces $N(I) = |N(a)|$.

Demostración. Sea $\{\omega_1, \ldots, \omega_n\}$ una $\mathbb{Z}$-base de $\mathbb{K}$ y $\{a\omega_1, \ldots, a\omega_n\}$ una $\mathbb{Z}$-base de I, ahora por la definición de discriminante se tiene que

$$\Delta = \Delta[\omega_1, \ldots, \omega_n] = \{det[\sigma_i(\omega_j)]\}^2,$$

$$\Delta[a\omega_1, \ldots, a\omega_n] = \{det[\sigma_i(a\omega_j)]\}^2.$$

Note que la matriz

$$[\sigma_i(a\omega_j)] = \begin{bmatrix} \sigma_1(a\omega_1) & \sigma_1(a\omega_2) & \cdots & \sigma_1(a\omega_n) \\ \sigma_2(a\omega_1) & \sigma_2(a\omega_2) & \cdots & \sigma_2(a\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(a\omega_1) & \sigma_n(a\omega_2) & \cdots & \sigma_n(a\omega_n) \end{bmatrix},$$

$$= \begin{bmatrix} \sigma_1(a)\sigma_1(\omega_1) & \sigma_1(a)\sigma_1(\omega_2) & \cdots & \sigma_1(a)\sigma_1(\omega_n) \\ \sigma_2(a)\sigma_2(\omega_1) & \sigma_2(a)\sigma_2(\omega_2) & \cdots & \sigma_2(a)\sigma_2(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(a)\sigma_n(\omega_1) & \sigma_n(a)\sigma_n(\omega_2) & \cdots & \sigma_n(a)\sigma_n(\omega_n) \end{bmatrix},$$

$$= \begin{bmatrix} \sigma_1(a) & 0 & \cdots & 0 \\ 0 & \sigma_2(a) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \sigma_n(a) \end{bmatrix} \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{bmatrix},$$

$$= \sigma_i(a)\ \sigma_i(\omega_j),$$

por lo tanto,

$$det[\sigma_i(a\omega_j)] = det[\sigma_i(a)]\ det[\sigma_i(\omega_j)].$$

y

$$\begin{aligned} det[\sigma_i(a)] &= \begin{vmatrix} \sigma_1(a) & 0 & \cdots & 0 \\ 0 & \sigma_2(a) & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \sigma_n(a) \end{vmatrix} \\ &= \sigma_1(a)\sigma_2(a)\cdots\sigma_n(a), \\ &= \prod_{i=1}^{n} \sigma_i(a), \end{aligned}$$

así

$$\begin{aligned} \frac{\Delta[a\omega_1, \ldots, a\omega_n]}{\Delta} &= \frac{\{det[\sigma_i(a\omega_j)]\}^2}{\{det[\sigma_i(\omega_j)]\}^2}, \\ &= \frac{\{det[\sigma_i(a)\sigma_i(\omega_j)]\}^2}{\{det[\sigma_i(\omega_j)]\}^2}, \\ &= \frac{\{det[\sigma_i(a)]\}^2\{det[\sigma_i(\omega_j)]\}^2}{\{det[\sigma_i(\omega_j)]\}^2}, \\ &= \{det[\sigma_i(a)]\}^2, \end{aligned}$$

entonces

$$\left|\frac{\Delta[a\omega_1,\ldots,a\omega_n]}{\Delta}\right|^{1/2} = |\{det[\sigma_i(a)]\}| = \left|\prod \sigma_i(a)\right|,$$

por lo tanto se obtiene que

$$N(I) = \left|\frac{\Delta[a\omega_1,\ldots,a\omega_n]}{\Delta}\right|^{1/2} = \left|\prod \sigma_i(a)\right| = |N(a)|.$$

□

Ejemplo 2.4.4. Sea $\mathbb{K} = \mathbb{Q}(i)$ y $\mathcal{D} = \mathbb{Z}[i]$, una $\mathbb{Z}-$base de $\mathbb{K}$ (o $\mathcal{D}$) es $\{1, i\}$.
Sea $I = \langle 1+i\rangle$ un ideal de $\mathcal{D}$, donde $\{1+i, 1-i\}$ es una $\mathbb{Z}$-base de I, entonces se verá que $N(I) = \left|\frac{\Delta[\alpha_1,\alpha_2]}{\Delta}\right|^{1/2}$.

Primero se calculará la norma de el ideal con la Definición 2.3.2 y el Corolario 2.4.3

$$N(I) = N(\langle 1+i\rangle) = N(1+i) = \sigma_1(1+i)\sigma_2(1+i) = (1+i)(1-i) = 2.$$

Ahora se calculará los discriminantes de las respectivas bases

$$\begin{aligned}
\Delta[1+i.1-i] &= \left(det\begin{bmatrix}\sigma_1(1+i) & \sigma_1(1-i)\\ \sigma_2(1+i) & \sigma_2(1-i)\end{bmatrix}\right)^2,\\
&= \left(\begin{vmatrix}1+i & 1-i\\ 1-i & 1+i\end{vmatrix}\right)^2,\\
&= ((1+i)^2-(1-i)^2)^2,\\
&= (4i)^2,\\
&= -16.
\end{aligned}$$

$$\begin{aligned}\Delta = \Delta[1,i] &= \left(det \begin{bmatrix} \sigma_1(1) & \sigma_1(i) \\ \sigma_2(1) & \sigma_2(i) \end{bmatrix} \right)^2, \\ &= \left(\begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix} \right)^2, \\ &= (-i-i)^2, \\ &= (-2i)^2, \\ &= -4.\end{aligned}$$

Por lo tanto, por el Teorema 2.4.2 se tiene que

$$N(I) = \left| \frac{-16}{-4} \right|^{1/2} = |-4|^{1/2} = (4)^{1/2} = \sqrt{4} = 2.$$

Entonces se concluye que $N(I) = \left| \frac{\Delta[\alpha_1,\alpha_2]}{\Delta} \right|^{1/2} = 2$.

Ejemplo 2.4.5. Si $\mathcal{D}$ es el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ para un entero racional libre de cuadrados d, es decir, no existe un número primo p tal que p^2 divide a d, entonces

$$N\left(\left\langle a + b\sqrt{d} \right\rangle\right) = |N(a + b\sqrt{d})| = |a^2 + b^2 d|,$$

en particular, en $\mathcal{D} = \mathbb{Z}[\sqrt{-17}]$, entonces

$$N(\langle 18 \rangle) = |N(18)| = 18^2.$$

El teorema que se enunciará a continuación explica una de la características más importantes de la norma de un ideal, puesto que es la generalización de la norma de un elemento que satisface la propiedad multiplicativa.

Teorema 2.4.6. Si I y J son ideales de $\mathcal{D}$ diferentes de cero, entonces

$$N(IJ) = N(I)N(J).$$

Demostración. Por la factorización única e inducción en el número de factores es suficiente probar que

$$N(I\mathfrak{p}) = N(I)N(\mathfrak{p})$$

donde $\mathfrak{p}$ es primo. En efecto, teniendo esta igualdad entonces se concluye que $N(IJ) = N(I)N(J)$, para cualesquiera I, J ideales de $\mathcal{D}$, puesto que por el teorema de factorización única para ideales (item 2. del Teorema 2.3.7) se tiene que $J = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ son ideales primos.
Aplicando el tercer teorema de isomorfismo para anillos se tiene que

$$\mathcal{D}/I \cong (\mathcal{D}/I\mathfrak{p})/(I/I\mathfrak{p}) \tag{16}$$

aplicando a la ecuación (16) el Teorema de Lagrange y la fórmula de transitividad del índice; donde $I\mathfrak{p}, I$ son subgrupos(subanillos) de $\mathcal{D}$, se obtiene

$$|\mathcal{D}/I| = \frac{|\mathcal{D}/I\mathfrak{p}|}{|I/I\mathfrak{p}|}$$

$$|\mathcal{D}/I||I/I\mathfrak{p}| = |\mathcal{D}/I\mathfrak{p}|. \tag{17}$$

Ahora se demostrará que $|I/I\mathfrak{p}| = |\mathcal{D}/\mathfrak{p}|$. Por el item 2 del Teorema 2.3.7, es decir por la factorización única implica que $I \neq I\mathfrak{p}$, entonces se mostrará que $I \supsetneq I\mathfrak{p}$; es decir, se mostrará que no hay un ideal L estrictamente entre I e $I\mathfrak{p}$.
Para esto suponga que

$$I \supseteq L \supseteq I\mathfrak{p}, \tag{18}$$

como ideales fraccionarios y, por definición del inverso aplicado a la ecuación (18) se obtiene que

$$I^{-1}I \supseteq I^{-1}L \supseteq I^{-1}I\mathfrak{p},$$

y

$$\mathcal{D} \supseteq I^{-1}L \supseteq \mathfrak{p}.$$

Dado que $I^{-1}L \subseteq \mathcal{D}$, donde $I^{-1}L$ es un ideal, luego como $\mathfrak{p}$ es un ideal primo de $\mathcal{D}$ por el item d) del Teorema 2.3.4, $\mathfrak{p}$ es un ideal maximal entonces

$$I^{-1}L = \mathcal{D} \ \ o \ \ I^{-1}L = \mathfrak{p},$$

por lo tanto, $L = I$ o $L = I\mathfrak{p}$. Ahora como $I \supsetneq I\mathfrak{p}$ cualquier $a \in I \setminus I\mathfrak{p}$, es decir entre los ideales $I\mathfrak{p}$ e I no existen más ideales, por lo tanto

$$I\mathfrak{p} + \langle a \rangle = I. \tag{19}$$

Fije un a y defina $\rho : \mathcal{D} \to I/I\mathfrak{p}$ dada por $\rho(x) = I\mathfrak{p} + ax$, entonces ρ es un homomorfismo sobreyectivo $\mathcal{D}$-módulo, donde el kernel es un ideal que satisface

$$\mathfrak{p} \subseteq ker(\rho).$$

Ahora como $ker(\rho) \neq \mathcal{D}$, puesto que si $ker(\rho) = \mathcal{D}$, utilizando el primer teorema de Isomorfismo se tendría que $I/I\mathfrak{p} \cong \mathcal{D}/ker(\rho) = \mathcal{D}/\mathcal{D} = 0$, entonces $I/I\mathfrak{p} \cong 0$, es decir $I = I\mathfrak{p}$ lo cual es una contradicción y como $\mathfrak{p}$ es maximal entonces

$$ker(\rho) = \mathcal{D} \ \ o \ \ ker(\rho) = \mathfrak{p},$$

esto implica que $ker(\rho) = \mathfrak{p}$. Así $I/I\mathfrak{p} \cong \mathcal{D}/ker(\rho) = \mathcal{D}/\mathfrak{p}$ (como $\mathcal{D}$-módulo) por

consiguiente

$$|I/I\mathfrak{p}| = |\mathcal{D}/\mathfrak{p}|, \tag{20}$$

por último, reemplazando (20) en la ecuación (17) se obtiene que

$$|\mathcal{D}/I||\mathcal{D}/\mathfrak{p}| = |\mathcal{D}/I\mathfrak{p}|,$$

y por definición de norma

$$N(I)N(\mathfrak{p}) = |\mathcal{D}/I||\mathcal{D}/\mathfrak{p}| = |\mathcal{D}/I\mathfrak{p}| = N(I\mathfrak{p}).$$

□

Ejemplo 2.4.7. Si $\mathcal{D} = \mathbb{Z}[\sqrt{-17}]$ y $\mathfrak{p}_1 = \left\langle 2, 1+\sqrt{-17}\right\rangle$, $\mathfrak{p}_2 = \left\langle 3, 1+\sqrt{-17}\right\rangle$, $\mathfrak{p}_3 = \left\langle 3, 1-\sqrt{-17}\right\rangle$ entonces $N(\mathfrak{p}_1^2\,\mathfrak{p}_2^2\,\mathfrak{p}_3^2) = 2^2 \cdot 3^2 \cdot 3^2 = 18^2$.

Se puede notar que los generadores de $\mathfrak{p}_1$ son ambos factores de 18. Esto se debe a que $18 = 2 \cdot 3 \cdot 3 = (1+\sqrt{-17})(1-\sqrt{-17})$, por lo tanto $18 \in \mathfrak{p}_1$ es decir, $\langle 18\rangle \subseteq \mathfrak{p}_1$ lo que significa que $\mathfrak{p}_1$ es un factor de $\langle 18\rangle$, así por el Teorema 2.3.8 se tiene que $\mathfrak{p}_1|\langle 18\rangle$.
En efecto, se tiene que

$$1-\sqrt{-17} = 2-(1+\sqrt{-17}) \in \mathfrak{p}_1,$$

entonces

$$18 = (1+\sqrt{-17})(1-\sqrt{-17}) \in \mathfrak{p}_1^2,$$

lo que significa que $\langle 18\rangle \subseteq \mathfrak{p}_1^2$ así $\mathfrak{p}_1^2|\,\langle 18\rangle$ y $\mathfrak{p}_1^2$ es un factor de $\langle 18\rangle$.

Como $\mathfrak{p}_1 = \left\langle 2, 1+\sqrt{-17} \right\rangle$, los elementos de $\mathfrak{p}_1$ son de la forma:

$$\begin{aligned} & 2(a+b\sqrt{-17}) + (1+\sqrt{-17})(c+d\sqrt{-17}) \\ & = 2a + 2b\sqrt{-17} + c + d\sqrt{-17} + c\sqrt{-17} - 17d, \\ & = (2a + c - 17d) + (2b + c + d)\sqrt{-17} \\ & = r + s\sqrt{-17}, \end{aligned}$$

donde $r - s = 2a - 2b - 18d$, el cual siempre es par; claramente r puede ser tomada como cualquier entero y entonces s puede ser cualquier entero de la misma paridad (par o impar).

Esto implica que $\mathfrak{p}_1$ no es todo el anillo $\mathbb{Z}[\sqrt{-17}]$. Por otra parte, $\mathfrak{p}_1$ es maximal; sea $m + n\sqrt{-17} \notin \mathfrak{p}_1$ entonces m es par y n impar o viceversa, por lo tanto

$$\left\langle \mathfrak{p}_1, m + n\sqrt{-17} \right\rangle = \mathbb{Z}[\sqrt{-17}].$$

Similarmente, considerando $\mathfrak{p}_2 = \left\langle 3, 1+\sqrt{-17} \right\rangle$ los elementos de $\mathfrak{p}_2$ son de la forma

$$\begin{aligned} & 3(a+b\sqrt{-17}) + (1+\sqrt{-17})(c+d\sqrt{-17}) \\ & = 3a + 3b\sqrt{-17} + c + d\sqrt{-17} + c\sqrt{-17} - 17d, \\ & = (3a + c - 17d) + (3b + c + d)\sqrt{-17}, \\ & = r + s\sqrt{-17}, \end{aligned}$$

donde $r - s = 3(a + b - 6d)$. Así r, s puede ser cualquier entero el cual cumpla la condición de que

$$r \equiv s \, (mod \ 3),$$

una vez más se encuentra que $\mathfrak{p}_2$ es maximal y $18 = 2 \cdot 3 \cdot 3 \in \mathfrak{p}_2^2$, entonces $\mathfrak{p}_2^2 | \, \langle 18 \rangle$; es decir $\mathfrak{p}_2^2$ es un factor de $\langle 18 \rangle$.

Finalmente considerando $\mathfrak{p}_3 = \langle 3, 1 - \sqrt{-17} \rangle$ los elementos de $\mathfrak{p}_3$ son de la forma:

$$\begin{aligned} &3(a + b\sqrt{-17}) + (1 - \sqrt{-17})(c + d\sqrt{-17}), \\ &= 3a + 3b\sqrt{-17} + c + d\sqrt{-17} - c\sqrt{-17} + 17d, \\ &= (3a + c + 17d) + (3b + d + c)\sqrt{-17}, \end{aligned}$$

$$= r + s\sqrt{-17}. \tag{21}$$

Se obtiene el ideal primo tal que $\mathfrak{p}_3^2$ es un factor de $\langle 18 \rangle$ y el cálculo de la ecuación (21) muestra que $r + s\sqrt{-17} \in \mathfrak{p}_3$ si y solo si, $r + s \equiv 0 (mod\ 3)$.

Usando el item 1. del Teorema 2.3.8 se encuentra que

$$\mathfrak{p}_1^2 \mathfrak{p}_2^2 \mathfrak{p}_3^2 \supseteq \langle 18 \rangle .$$

El paso final para mostrar que $\mathfrak{p}_1^2 \mathfrak{p}_2^2 \mathfrak{p}_3^2 = \langle 18 \rangle$, se realiza mejor usando un argumento de conteo puesto que cada elemento en $\mathbb{Z}[\sqrt{-17}]$ es cualquiera en $\mathfrak{p}_1$ o de la forma $1 + x$ con $x \in \mathfrak{p}_1$, por consiguiente el número de elementos en el anillo cociente $\mathbb{Z}[\sqrt{-17}]/\mathfrak{p}1$ es

$$|\mathbb{Z}[\sqrt{-17}]/\mathfrak{p}_1| = 2,$$

luego por la Definición 2.4.1 se tiene que

$$N(\mathfrak{p}_1) = |\mathbb{Z}[\sqrt{-17}]/\mathfrak{p}_1| = 2.$$

Similarmente,

$$N(\mathfrak{p}_r) = |\mathbb{Z}[\sqrt{-17}]/\mathfrak{p}_r| = 3 \quad donde\ r = 2, 3.$$

Luego por lo dicho anteriormente y por el Teorema 2.4.6, se deduce que

$$N(\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2) = N(\mathfrak{p}_1^2)N(\mathfrak{p}_2^2)N(\mathfrak{p}_3^2) = 2^2 \cdot 3^2 \cdot 3^2 = 18^2.$$

Recuerde que en la teoría algebraica de números, a los números primos se les conoce como **números racionales primos** para distinguirlos de los números gaussianos primos. La primalidad depende del anillo donde se estudia.

Se termina este trabajo de grado enunciando algunas propiedades de la norma y de ideales en dominios de Dedekind.

Teorema 2.4.8. Sea I un ideal de un dominio de Dedekind $\mathcal{D}$, $I \neq 0$

1. Si $N(I)$ es primo, entonces I también lo es.
2. $N(I)$ es un elemento de I, o equivalentemente $I|N(I)$.
3. Si I es primo éste divide exactamente un primo racional $\mathfrak{p}$, y

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

donde $m \leq n$.

Demostración.

1. Sea

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r, \tag{22}$$

donde $\mathfrak{p}_i$ son ideales primos con $i = 1, \ldots, r$, luego aplicando la norma en la ecuación (22) y utilizando el Teorema 2.4.6 se tiene que

$$N(I) = N(\mathfrak{p}_1 \cdots \mathfrak{p}_r),$$

$$N(I) = N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_r), \tag{23}$$

por la ecuación (23) se tiene que $N(\mathfrak{p}_i)|N(I)$ con $i = 1, \ldots, r$ y $N(I)$ divide a algún $N(\mathfrak{p}_i)$ así, sin pérdida de generalidad se tiene que $N(I)|N(\mathfrak{p}_1)$.

Luego como $N(\mathfrak{p}_i)|N(I)$ con $i = 1, \ldots, r$ entonces $N(\mathfrak{p}_1)|N(I)$ y por lo dicho anteriormente $N(I)|N(\mathfrak{p}_1)$; por lo tanto

$$N(I) = N(\mathfrak{p}_1),$$

esto implica que

$$N(\mathfrak{p}_2) = \cdots = N(\mathfrak{p}_r) = 1,$$

es decir

$$\mathfrak{p}_2 = \cdots = \mathfrak{p}_r = \mathcal{D}. \tag{24}$$

Por consiguiente reemplazando (24) en la ecuación (22)

$$I = \mathfrak{p}_1 \mathcal{D} \cdots \mathcal{D} = \mathfrak{p}_1,$$

así $I = \mathfrak{p}_1$ entonces I es un ideal primo.

2. Como $N(I) = |\mathcal{D}/I|$ con $(\mathcal{D}/I, +)$ grupo, entonces por el teorema de Lagrange, dado $x + I \in \mathcal{D}/I$ se tiene que

$$N(I)(x + I) = I,$$

$$N(I)x + N(I)I = I,$$

$$N(I)x + I = I,$$

$$N(I)x \in I,$$

para todo $x \in \mathcal{D}$. Tomando $x = 1$ entonces $N(I) \in I$.

3. Por hipótesis I es un ideal primo, así $I \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$. Además por el item anterior $N(I)$ es un elemento de I y $N(I)$ es un entero positivo, entonces $N(I) \in I \cap \mathbb{Z}/\{0\}$, con lo que $I \cap \mathbb{Z} = \mathfrak{p}\mathbb{Z}$ para algún primo $\mathfrak{p}$, donde $\mathfrak{p}$ es el único primo racional de I.

   Como $\mathfrak{p} \in I$ entonces $\langle \mathfrak{p} \rangle = \mathcal{D}\mathfrak{p} \subseteq I$ así por la Proposición 2.3.8 se tiene que $I|\mathcal{D}\mathfrak{p}$ y del Teorema 2.4.6 se deduce que

$$N(I)|N(\mathcal{D}\mathfrak{p}) = N(\langle \mathfrak{p} \rangle),$$

   luego por el Corolario 2.4.3 $N(\langle \mathfrak{p} \rangle) = |N(\mathfrak{p})|$ así

$$N(I)||N(\mathfrak{p})|; \tag{25}$$

   por la definición de norma,

$$N(\mathfrak{p}) = \prod \sigma_i(\mathfrak{p}) = \mathfrak{p}^n \tag{26}$$

   ahora reemplazando la ecuación (26) en la ecuación (25) se tiene que

$$N(I)|\mathfrak{p}^n,$$

   por lo tanto $N(I) = \mathfrak{p}^m$ donde $m \leq n$.

□

Ejemplo 2.4.9. Si $\mathcal{D} = \mathbb{Z}[\sqrt{-17}]$, $\mathfrak{p}_1 = \left\langle 2, 1 + \sqrt{-17} \right\rangle$, por el Ejemplo 2.4.7 se tiene que $N(\mathfrak{p}_1) = 2$, luego por el item 1. del Teorema 2.4.8 es posible deducir que $\mathfrak{p}_1$ es primo.

Note que $N(\mathfrak{p}_1) = 2 \in \mathfrak{p}_1$, como se afirma en el item 2. del Teorema 2.4.8.

Se finaliza este trabajo con el siguiente resultado que habla de las propiedades más importantes que tienen los ideales del anillo de Dedekind $\mathcal{D}$ y sus normas.

Teorema 2.4.10. 1. Todo ideal de $\mathcal{D}$ diferente de cero tiene un número finito de divisores.

2. Un entero racional diferente de cero pertenece solo a un número finito de ideales de $\mathcal{D}$.

3. Dado un entero positivo N, existe a lo más un número finito de ideales que tienen norma N.

Demostración.

1. Note que por el item 2) del Teorema 2.3.7, cada ideal de $\mathcal{D}$ diferente de cero puede ser escrito de forma única como producto de ideales primos, por lo tanto cada ideal de $\mathcal{D}$ diferente de cero tiene un número finito de divisores.

2. Sea $a \neq 0$ un entero racional, entonces $\langle a \rangle = I$ para algún I ideal de $\mathcal{D}$, luego por el item anterior I tiene un número finito de divisores, es decir, $\langle a \rangle$ está contenido en un número finito de ideales de $\mathcal{D}$, por lo tanto a pertenece a un número finito de ideales de $\mathcal{D}$.

3. Sea $N(I) = n$, para cualquier ideal I de $\mathcal{D}$, por el item 2. del Teorema 2.4.8 n pertenece a I. Como n es un entero racional positivo, entonces por el item anterior n pertenece a un número finito de ideales de $\mathcal{D}$.

   Así, si existiera un número infinito de ideales con norma n entonces n pertenecería a cada uno de esos ideales, lo cual contradice que n pertenece a un número finito de ideales.

□

Ejemplo 2.4.11. Considerando el cálculo anterior

$$\langle 18\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2,$$

en $\mathbb{Z}[\sqrt{-17}]$ donde $\mathfrak{p}_1 = \left\langle 2, 1+\sqrt{-17}\right\rangle$, $\mathfrak{p}_2 = \left\langle 3, 1+\sqrt{-17}\right\rangle$ y $\mathfrak{p}_3 = \left\langle 3, 1-\sqrt{-17}\right\rangle$. Se encuentra que los únicos divisores primos de $\langle 18\rangle$ son $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$.

Si 18 pertenece a algún ideal I, entonces $\langle 18\rangle \subseteq I$ de donde $I \,|\, \langle 18\rangle$, entonces $I|\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$ y $I = \mathfrak{p}_1^q\mathfrak{p}_2^r\mathfrak{p}_3^s$ donde q, r, s son $0, 1$ o 2. Así 18 pertenece a un número finito de ideales.

¿Cuántos ideales I tiene norma 18?. Esto solo puede suceder cuando $I|18$ por el item 2) del Teorema 2.4.8

$$I = \mathfrak{p}_1^q\mathfrak{p}_2^r\mathfrak{p}_3^s,$$

lo cual implica

$$N(I) = 2^q 3^r 3^s.$$

Esta norma es 18 solamente cuando $q = 1$ y $r + s = 2$ lo que significa que I pueden ser $\mathfrak{p}_1\mathfrak{p}_2^2$, $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ o $\mathfrak{p}_1\mathfrak{p}_3^2$.

BIBLIOGRAFÍA

GALLIAN, Joseph. *Contemporary abstract algebra: Eigth edition (8th ed)*. Boston: Brooks/Cole Cengage Learning, 2013.

GÓMEZ RÍOS, Jorge. "El Anillo de los Enteros Algebraicos y Dominios de Dedekind". Bucaramanga: Universidad Industrial de Santander, 2015 (vid. págs. 45, 46).

GÓMEZ SAURA, David. "Cuerpos finitos". España: Universidad de Murcia, 2014-2015 (vid. pág. 19).

JACOBSON, Nathan. *Basic Algebra: Second Edition (2th ed)*. Vol. 2. W.H. Freeman y Company, 1989 (vid. págs. 15, 28).

LEZAMA, Oswaldo. *Cuadernos de Álgebra N° 2, Anillos*. http://gfnun.unal.edu.co/fileadmin/content/seminarios/sac2/cuadernos/anillos.pdf. 2014 (vid. pág. 9).

— *Cuadernos de Álgebra N° 6, Anillos y Módulos*. http://gfnun.unal.edu.co/fileadmin/content/seminarios/sac2/cuadernos/anillosymodulos.pdf. 2014 (vid. pág. 16).

ROMAN, Steven. *Field Theory: Second Edition (2ed)*. New York: Springer-Verlag, 2006.

ROTMAN, Joseph A. *An Introduction to theory of group*. New York: Springer-Verlag, 1995.

SPINDLER, Karlheinz. *Abstract Algebra with Aplications*. Vol. 2. New York: Marcel Dekker, INC, 1994 (vid. pág. 21).

STEWART Ian & TALL, David. *Algebraic Number Theory and Fermat's Last Theorem: Third Edition (3rd ed.).* Massachusetts: A K Peters/CRC Press., 2002 (vid. págs. 9, 13, 21, 37).

SUÁREZ, Mariano. *Dominios de Dedekind*. `http://mate.dm.uba.ar/~nbotbol/algebraII20092/apuntes/dedekind.pdf`. 2007 (vid. pág. 16).