EL ANILLO DE LOS ENTEROS ALGEBRAICOS Y DOMINIOS DE DEDEKIND

JORGE ELIÉCER GÓMEZ RÍOS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2015

EL ANILLO DE LOS ENTEROS ALGEBRAICOS Y DOMINIOS DE DEDEKIND

Autor

JORGE ELIÉCER GÓMEZ RÍOS

Trabajo de grado para optar al título de

Matemático

Director

HÉCTOR EDONIS PINEDO TAPIA

Doctor en Ciencias

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA

2015

Universidad Industrial de Santander

NOTA DE PROYECTO DE GRADO

NOMBRE DEL ESTUDIANTE: JORGE ELIÉCER GÓMEZ RÍOS	**21110159**
TITULO DEL PROYECTO : "El anillo de los enteros algebraicos y dominios de Dedekind "	
FACULTAD : ***Ciencias***	CARRERA: ***Matemáticas***
NOTA DEFINITIVA: **Cuatro, ocho (4.8)**	CREDITOS: *10*

DIRECTOR DEL PROYECTO: HÉCTOR EDONIS PINEDO

FIRMA: Hector Pinedo T.

CALIFICADORES

F _____ **ALBERTO HIGUERA MARÍN**	F _____ **ARNOLDO TEHERÁN HERRERA**	FECHA A *15* M *6* D *12*

ENTREGA DE TRABAJOS DE GRADO, TRABAJOS DE INVESTIGACIÓN O TESIS Y AUTORIZACIÓN DE SU USO A FAVOR DE LA UIS

Yo, **JORGE ELIÉCER GÓMEZ RÍOS**, mayor de edad, vecino de Bucaramanga, identificado con la Cédula de Ciudadanía **No 1.096.513.442** de Curití, actuando en nombre propio, en mi calidad de autor del trabajo de grado, del trabajo de investigación, o de la tesis denominada(o): **EL ANILLO DE LOS ENTEROS ALGEBRAICOS Y DOMINIOS DE DEDEKIND**, hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (CD o DVD) y autorizo a **LA UNIVERSIDAD INDUSTRIAL DE SANTANDER**, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

PARÁGRAFO: La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato virtual, electrónico, digital, óptico, uso en red, Internet, extranet, intranet, etc., y en general para cualquier formato conocido o por conocer.

EL AUTOR / ESTUDIANTE, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad sobre la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL AUTOR / ESTUDIANTE, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos la Universidad actúa como un tercero de buena fe. Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Bucaramanga, a los 19 días del mes de Junio de Dos Mil quince (2015).

EL AUTOR / ESTUDIANTE:

Jorge Eliécer Gómez Ríos.
CC 1.096.513.442

Agradecimientos

En el camino para alcanzar este logro varias personas han contribuido de una u otra manera, construyéndome profesional y personalmente. Quiero manifestar mi gratitud a algunos de ellos ya que me sería imposible mencionarlos a todos.

Expreso mis agradecimientos a los profesores que aportaron su granito de arena en mi formación académica durante toda mi carrera, especialmente a mi director de tesis Héctor Pinedo por su disposición, interés y valiosas sugerencias y correcciones; a mis familiares y amigos quienes han influido más indirectamente brindándome consejos y colaboración en otros aspectos.

Finalmente, quiero agradecer y dedicar este trabajo especialmente a mis padres, por el apoyo brindado durante todos estos años, sin ellos hubiese sido imposible llegar hasta aquí.

Índice general

Resumen

TÍTULO: EL ANILLO DE LOS ENTEROS ALGEBRAICOS Y DOMINIOS DE DEDEKIND[1]

AUTOR: Jorge Eliécer Gómez Ríos[2]

PALABRAS CLAVE: Enteros algebraicos; Dominios de Dedekind; Factorización única.

RESUMEN

La teoría de los números algebraicos se desarrolló en gran parte gracias al Último Teorema de Fermat. Varios matemáticos importantes del siglo XIX, entusiasmados por encontrar la prueba de este teorema (que para entonces era una conjetura), contribuyeron para que la teoría algebraica de números se consolidara como una rama importante de las matemáticas.

Este trabajo consiste en estudiar algunos conceptos y resultados de la teoría de los enteros algebraicos. En el primer capítulo se retoman algunos conceptos y resultados clásicos sobre anillos y cuerpos, necesarios para el buen entendimiento de lo expuesto en los siguientes dos capítulos.

En el segundo capítulo se prueba que los enteros de un cuerpo $\mathbb{L}$ sobre un anillo R, es decir, aquellos elementos en $\mathbb{L}$ que son raíz de un polinomio mónico en $R[X]$ forman un anillo en el que no necesariamente vale la factorización única. Sin embargo, se muestran algunos ejemplos de cuerpos numéricos, en los que su anillo de enteros es un dominio de factorización única, por ejemplo el anillo de los enteros de Gauss $\mathbb{Z}[i]$ y se usa este hecho para solucionar algunas ecuaciones diofánticas.

En el tercer capítulo, se definen y caracterizan los dominios de Dedekind en términos de la factorización única de ideales y en estos términos, se prueba que el anillo de los enteros de un cuerpo es un dominio en el que todo ideal propio se expresa de manera única como producto de ideales primos.

[1] Tesis.

[2] Facultad de Ciencias, Escuela de Matemáticas.
DIRECTOR: Dr. Héctor Edonis Pinedo Tapia.

Abstract

TITLE: THE RING OF ALGEBRAIC INTEGERS AND DEDEKIND DOMAINS [3]

AUTHOR: Jorge Eliécer Gómez Ríos[4]

KEYWORDS: Algebraic integers; Dedekind domains; unique factorization.

ABSTRACT

One of the principal reasons for the development of algebraic number theory was the Fermat's Last Theorem. During the nineteenth century, several important mathematicians tried to find proof this theorem (which by then was a conjecture), and contributed for the Algebraic Number Theory to be consolidated as an important branch of mathematics.

In this dissertation is going to be studied some concepts and results of the theory of algebraic integers.In the first chapter some classic concepts and results on rings and fields necessary for the proper understanding on the discussion following in the next two chapters are taken up.

In the second chapter is going to be proved that the integers of a field $\mathbb{L}$ over a ring R, that is, those elements in $\mathbb{L}$ that are roots of a monic polynomial in $R[X]$, form a ring which it is not necessary a unique factorization domain. However, some examples are going to be presented of numerical fields, in which the ring of integers is a unique factorization domain, for example the ring of Gaussian integers $\mathbb{Z}[i]$ and this fact is used to find solutions of some Diophantine equations.

In the third chapter the Dedekind domains are going to be defined and characterized in terms of the unique factorization of ideals and in these terms, it is proved that the ring of integers of a field is a domain in which every proper ideal is expressed in a unique way as a product of prime ideals.

[3]Thesis.

[4]Faculty of Science, School of Mathematics.
DIRECTED BY: Dr. Héctor Edonis Pinedo Tapia.

Introducción

Un problema interesante en Matemáticas ha sido el de simplificar o reducir los objetos de estudio a términos que son más sencillos estructuralmente, para facilitar su estudio. Un ejemplo de esto es el concepto de factorización y el resultado relacionado a este problema aparece en Teoría de Números, el cual es conocido como el Teorema Fundamental de la Aritmética (TFA), este afirma que todo número entero no nulo y no unidad se puede expresar de forma única como producto de factores primos.

Una generalización del TFA para dominios enteros, permite establecer el concepto de Dominio de Factorización Única (DFU), es decir dominios en los que todo elemento no nulo y no unidad se puede descomponer de manera única como producto de elementos irreducibles salvo el orden y asociados. En este trabajo estudiaremos versiones de esta propiedad en anillos conmutativos arbitrarios, en particular, veremos que existen anillos que la cumplen, pero en ellos todo ideal propio se descompone de forma única (salvo el orden) como producto de ideales primos, dominios con esta propiedad son llamados *Dominios de Dedekind*.

Un ejemplo importante de Dominio de Dedekind, es el *anillo de los enteros algebraicos.* El cual consiste de todos los elementos que son raíz de algún polinomio mónico sobre un anillo conmutativo dado. Mostraremos que en general, este anillo no es DFU, pero existen resultados que establecen condiciones necesarias y suficientes para que lo sea.

Objetivos

Objetivo General

Dados $\mathbb{L}$ un cuerpo, B un subanillo de $\mathbb{L}$ y R un subanillo de B. Definimos el conjunto

$$I_B(R) = \{\alpha \in B : \text{existe } f(X) \in R[X] \text{ mónico tal que } f(\alpha) = 0\};$$

llamado *clausura entera de R en B*. El objetivo de este trabajo es mostrar que este conjunto es un dominio entero en el que todo ideal propio se descompone de forma única (salvo el orden) en producto de ideales primos.

Objetivos Específicos

- Probar que $I_B(R)$ es un subanillo de B que contiene a R.
- Probar que el anillo $I_B(R)$ es un dominio de Dedekind.
- Utilizar propiedades estructurales de $I_B(R)$ para resolver algunas ecuaciones diofánticas.
- Estudiar algunos casos particulares e interesantes, como $R = \mathbb{Z}[i]$, enteros de Gauss, o cuando B es un cuerpo cuadrático.

Capítulo 1

Preliminares

En este capítulo se establecen algunos conceptos y resultados conocidos del álgebra, que son fundamentales en el desarrollo y comprensión de los capítulos posteriores. Varios de estos conceptos y resultados preliminares, así como algunos ejemplos aparecen en [5], [6] y [7].

1.1. Definiciones básicas

Definición 1.1. *Un* **anillo** *es un conjunto R dotado de dos operaciones binarias (usualmente escritas como adición "$+$" y multiplicación "$*$") tales que $(R,+)$ es un grupo abeliano, $(R,*)$ es un semigrupo y además:*

$$a*(b+c) = a*b + a*c \quad y \quad (a+b)*c = a*c + b*c,$$

para todos $a, b, c \in R$.
Sea R un anillo.

- *Un subconjunto $S \subseteq R$ es dicho* **subanillo** *de R, si S es un anillo bajo las operaciones adición y multiplicación en R.*
- *Si $(R,*)$ es conmutativo, decimos que R es un* **anillo conmutativo** *y cuando $(R,*)$ es un monoide, R es llamado* **anillo con identidad.**

- *R es un* **dominio integral**, *si es un anillo conmutativo con identidad* $1_R \neq 0_R$ *y no tiene divisores de cero, esto es, si satisface:*

  - *Si* $a, b \in R$ *son tales que* $a * b = 0$, *entonces* $a = 0$ *o* $b = 0$, *o equivalentemente, si* $a \neq 0$ *y* $b \neq 0$, *entonces* $a * b \neq 0_R$.

- *Un* **cuerpo** *es un anillo conmutativo, tal que el conjunto* $U(R)$ *formado por las unidades de R, esto es, por los* $a \neq 0_R$ *para los cuales la ecuación* $a * x = 1_R$ *tiene solución en R, es exactamente* $R \setminus \{0\}$.

Nota: En adelante, para simplificar la notación, escribiremos *ab* para notar la operación binaria multiplicación $a * b$ en cualquier anillo R, además las letras $\mathbb{F}$, $\mathbb{K}$, y $\mathbb{L}$, denotarán cuerpos.

Ejemplo 1.1. *El conjunto de los números enteros* $\mathbb{Z}$ *es un dominio entero con las operaciones suma y producto usuales. Sabemos que* $\mathbb{Z}$ *no es un cuerpo, ya que* $U(\mathbb{Z}) = \{\pm 1\}$.

Respecto a la aritmética en el dominio de los enteros se tienen los siguientes dos resultados.

Teorema 1.1. Algoritmo de la división:
Si $a, b \in \mathbb{Z}$, *con* $b \neq 0$, *entonces existen* $q, r \in \mathbb{Z}$ *únicos tales que*

$$a = bq + r \quad y \quad 0 \leq r \leq |b|.$$

Demostración. Ver [5], Capítulo 1. □

Teorema 1.2. Teorema Fundamental de la Aritmética
Todo entero $n \neq 0; \pm 1$ *se puede factorizar como producto de primos y esta factorización es única salvo por el orden de los factores.*

Demostración. Ver [5], Capítulo 1. □

Definición 1.2. *Sea R un anillo, un* **polinomio con coeficientes en** *R es una expresión de la forma:*

$$f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n,$$

donde los $a_i \in R$. El conjunto de todos los polinomios con coeficientes en R lo denotamos por $R[X]$. Cuando $a_n = 1_R$, el polinomio $f(X)$ es llamado **mónico**.

Tenemos que con la suma y el producto usual de polinomios, el conjunto $R[X]$ es un anillo, llamado el ***anillo de los polinomios con coeficientes en*** R. Sabemos que la estructura de $\mathbb{F}[X]$ es muy similar a la del anillo de los enteros $\mathbb{Z}$, en ambos tiene sentido hablar del algoritmo de la división, máximo común divisor, primalidad, y factorización única o teorema fundamental de la aritmética. En la mayoría de los casos las pruebas de estos teoremas y demás resultados clásicos alrededor de los anteriores conceptos son similares a las que conocemos de teoría de números para los enteros.

1.2. Ideales y Aritmética en dominios enteros

Definición 1.3. *Un subanillo $\mathfrak{I}$ de un anillo R es llamado* **ideal**, *si tiene la siguiente propiedad:*

Siempre que $r \in R$ y $a \in \mathfrak{I}$, entonces $ra \in \mathfrak{I}$ y $ar \in \mathfrak{I}$.

Los ***ideales triviales*** de R, son $\{0\}$ y él mismo. Se llamará ***ideal propio*** a todo ideal no trivial. Claramente un subconjunto no vacío $\mathfrak{I}$ de un anillo R es un ideal, si y solo si, satisface las siguientes propiedades:

i) si $a, b \in \mathfrak{I}$, entonces $a - b \in \mathfrak{I}$;

ii) si $r \in R$ y $a \in \mathfrak{I}$ entonces $ar, ra \in \mathfrak{I}$.

Sean R un anillo conmutativo con identidad, $c \in R$ e $\mathfrak{I}$ el conjunto de todos los múltiplos de c en R, esto es, $\mathfrak{I} = \{rc : r \in R\}$, entonces $\mathfrak{I}$ es un ideal en R, llamado ***ideal principal generado por*** c y denotado por $\langle c \rangle$. Un dominio en el que todo ideal es de esta forma es llamado ***dominio de ideales principales*** (DIP). Más general, si T es un subconjunto de R, entonces el conjunto

$$\langle T \rangle := \left\{ \sum_{i=1}^{k} r_i t_i : k \in \mathbb{N},\ r_i \in R,\ t_i \in T \right\}$$

es un ideal de R, llamado el ***ideal generado por*** T.

Ejemplo 1.2. *Sean R un anillo con identidad e $\mathfrak{I}$ un ideal en R, si $\mathfrak{I}$ contiene una unidad de R, se tiene que $\mathfrak{I} = R$. En efecto, sea $u \in U(R)$ tal que $u \in \mathfrak{I}$ entonces, existe $v \in R$ tal que $uv = 1 \in \mathfrak{I}$. Luego, para cada $r \in R$, $r = r \cdot 1 \in \mathfrak{I}$ y por lo tanto $\mathfrak{I} = R$.*

Ejemplo 1.3. *Un anillo conmutativo con identidad R es un cuerpo, si y solo si, sus únicos ideales son los triviales. De hecho, si R es un cuerpo e $\mathfrak{I} \neq \langle 0 \rangle$ es un ideal de R, entonces existe $0 \neq a \in \mathfrak{I}$, luego $a \in U(R)$ y por el Ejemplo 1.2 $\mathfrak{I} = R$. Recíprocamente, sea $0 \neq x \in R$, entonces $\langle x \rangle \neq \langle 0 \rangle$, por lo tanto $\langle x \rangle = R$. Como $1 \in R$, existe $x^{-1} \in R$ tal que $1 = xx^{-1}$ y en consecuencia R es cuerpo.*

Definición 1.4. *Sea $\mathfrak{I}$ un ideal de un anillo R. Decimos que dos elementos $a, b \in R$ son congruentes módulo $\mathfrak{I}$, y escribimos $a \equiv b \pmod{\mathfrak{I}}$ si $a - b \in I$.*

Tenemos que la relación de congruencia módulo $\mathfrak{I}$ es una relación de equivalencia en R lo que nos permite asociar a cada elemento $a \in R$ una clase de equivalencia que llamaremos ***clase de congruencia módulo*** $\mathfrak{I}$ dada por:

$$\begin{aligned}
[a] &= \{b \in R : b \equiv a \pmod{\mathfrak{I}}\} \\
&= \{b \in R : b - a = i, \text{con } i \in \mathfrak{I}\} \\
&= \{b \in R : b = a + i, \text{con } i \in \mathfrak{I}\} \\
&= \{a + i : i \in \mathfrak{I}\} := a + \mathfrak{I}.
\end{aligned}$$

Teorema 1.3. *Sea $\mathfrak{I}$ un ideal en un anillo R, entonces el conjunto de todas las clases de congruencia módulo $\mathfrak{I}$, denotado por:*

$$R/\mathfrak{I} := \{a + \mathfrak{I} : a \in R\},$$

es un anillo con las operaciones adición y multiplicación definidas como sigue:

Dados $a + \mathfrak{I}$ *y* $b + \mathfrak{I}$ *en* $R/\mathfrak{I}$*, entonces*

$$(a + \mathfrak{I}) + (b + \mathfrak{I}) := (a + b) + \mathfrak{I} \quad y \quad (a + \mathfrak{I})(b + \mathfrak{I}) := ab + \mathfrak{I}.$$

Demostración. Ver [5], Capítulo 6. □

Definición 1.5. *Sea R un anillo conmutativo con identidad.*

- *Un ideal* $\mathfrak{p}$ *de R es llamado* **ideal primo** *si* $\mathfrak{p} \neq R$ *y si* $ab \in \mathfrak{p}$*, entonces* $a \in \mathfrak{p}$ *o* $b \in \mathfrak{p}$.
- *Un ideal* $\mathfrak{m}$ *de R es llamado* **ideal maximal** *si* $\mathfrak{m} \neq R$ *y si* $\mathfrak{J}$ *es un ideal tal que* $\mathfrak{m} \subseteq \mathfrak{J} \subseteq R$*, entonces* $\mathfrak{m} = \mathfrak{J}$ *o* $\mathfrak{J} = R$.

Para anillos conmutativos con identidad se tiene la siguiente caracterización de los ideales primos y maximales.

Teorema 1.4. *Sea R un anillo conmutativo con identidad. Entonces:*

1. $\mathfrak{p}$ *es un ideal primo de R si, y solo si, el anillo cociente* $R/\mathfrak{p}$ *es un dominio integral.*
2. $\mathfrak{m}$ *es un ideal maximal de R si, y solo si, el anillo cociente* $R/\mathfrak{m}$ *es un cuerpo.*

Demostración. Ver [5], Sección 6.3. □

Como consecuencia del Teorema 1.4, todo ideal maximal en R es primo. También se tiene el siguiente resultado.

Teorema 1.5. *Si R es un dominio de ideales principales, entonces todo ideal primo no nulo de R es maximal.*

Ejemplo 1.4. *En* $\mathbb{Z}[X]$*, el ideal* $\langle X \rangle$ *es primo, pues* $\mathbb{Z}[X]/\langle X \rangle \cong \mathbb{Z}$*; pero se tiene que*

$$\langle X \rangle \subsetneq \langle X \rangle + \langle 2 \rangle \subsetneq \mathbb{Z}[X],$$

ya que $\langle X \rangle \not\ni X + 2 \in \langle X \rangle + \langle 2 \rangle$ *y* $\langle X \rangle + \langle 2 \rangle \not\ni X + 3 \in \mathbb{Z}[X]$*; luego* $\langle X \rangle$ *no es maximal y por lo tanto* $\mathbb{Z}[X]$ *no es dominio de ideales principales.*

Definición 1.6. *Sean R_1 y R_2 anillos. Un* **homomorfismo** *es una función $\sigma : R_1 \to R_2$ que preserva las operaciones y la unidad, es decir, para todos $r, s \in R_1$ se verifica que:*

$$\sigma(1_{R_1}) = 1_{R_2},$$
$$\sigma(r + s) = \sigma(r) + \sigma(s),$$
$$\sigma(rs) = \sigma(r)\sigma(s).$$

Si σ es inyectiva entonces σ se llama **monomorfismo**, *si es sobreyectiva se llama* **epimorfismo** *y si es biyectiva se llama* **isomorfismo**.

Para anillos cociente se tiene:

- Si $\Im$ un ideal en un anillo R, entonces la función $\pi : R \to R/\Im$ dada por $\pi(r) = r + \Im$, para todo $r \in R$; es un epimorfismo con kernel $\Im$. Ver [5], Teorema 6.10.

  La función π es llamada la ***proyección canónica*** de R sobre $R/\Im$.

- ***Primer Teorema del Isomorfismo:***
  Sea $\phi : A \to B$ un epimorfismo entre anillos con kernel K, entonces la función $\lambda : A/K \to B$ dada por $\lambda(a + K) = \phi(a)$, es un isomorfismo. Ver [5], Teorema 6.11.

Definición 1.7. *Sea R un anillo conmutativo.*

- *Dados $a, b, p \in R$ no nulos, a es un* **asociado** *de b si $a = bu$, para algún $u \in U(R)$. El elemento p es llamado* **irreducible** *si $p \notin U(R)$ y además los únicos divisores de p son sus asociados y las unidades de R.*

- *Un dominio integral R es un* **dominio de factorización única DFU** *(o* **dominio factorial***) si cada elemento en $R \setminus (U(R) \cup \{0_R\})$ es producto de elementos irreducibles y esta factorización es única salvo asociados; esto es, si*

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

con cada p_i y q_j irreducible, entonces $r = s$ y existe $\sigma \in S_r$ tal que p_i es un asociado de $q_{\sigma(i)}$ para cada $i \in \{1, 2, \cdots, r\}$.

Recordemos ahora un par de resultados que relacionan dominios integrales con DFU.

Teorema 1.6. *Un dominio integral R es un DFU si y solo si:*

1. *R satisface la condición de cadena ascendente en ideales principales; y*
2. *Si p es irreducible y $p|bc$, entonces $p|b$ o $p|c$.*

Demostración. Ver [5], página 238. □

Teorema 1.7. *Todo dominio de ideales principales es un dominio de factorización única.*

Demostración. Ver [5], página 240. □

Ejemplo 1.5. *Los anillos $\mathbb{Z}$ y $\mathbb{K}[X]$ son DFU. El recíproco del teorema anterior no es cierto ya que $\mathbb{Z}[X]$ es un DFU, pero no es un DIP.*

Todo dominio entero puede ser naturalmente incluido en un cuerpo, como veremos en la siguiente construcción.

Cuerpo de cocientes de un dominio entero

Para cualquier dominio entero R, podemos construir un cuerpo que contiene a R y consta de "cocientes" de los elementos de R, dicho cuerpo es llamado ***cuerpo de cocientes (o de fracciones)*** de R.

Formalmente, sea R un dominio entero y sea S el conjunto de pares definido como sigue:

$$S := \{(a, b) \mid a,\ b \in R \ \ y \ \ b \neq 0_R\}$$

Definamos la relación $\sim$ en S por:

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc \text{ en } R.$$

Se tiene que $\sim$ es una relación de equivalencia (ver [5, pág 255]) y por tanto particiona a S en clases de equivalencia disyuntas. Denotemos por $Q(R)$ el conjunto de todas las clases de equivalencia bajo $\sim$ y por $\frac{a}{b}$ a la clase de equivalencia de (a, b). Definamos entonces la adición y la multiplicación de estas clases como sigue:

- $\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$,
- $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$,

para todos $a, c \in R$ y $b, d \in R$ no nulos.

Tenemos que estas dos operaciones están bien definidas y que dan a $Q(R)$ estructura de cuerpo. Ver [5, pág 256-257].

Ejemplo 1.6.

- $Q(\mathbb{Z}) = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ y } b \neq 0 \right\} = \mathbb{Q}$.
- *El cuerpo de cocientes de* $\mathbb{K}[X]$ *se denota por* $\mathbb{K}(X)$ *y consiste en todos los cocientes* $\frac{f(X)}{g(X)}$, *donde* $f(X),\ g(X) \in \mathbb{K}[X]$ *y* $g(X) \neq 0_{\mathbb{K}}$. *El cuerpo* $\mathbb{K}(X)$ *se llama el* **cuerpo de funciones racionales** *sobre* $\mathbb{K}$.

1.3. Extensiones de Cuerpos

Definición 1.8. *Si* $\mathbb{K}$ *y* $\mathbb{L}$ *son cuerpos tales que* $\mathbb{K} \subseteq \mathbb{L}$, *diremos que* $\mathbb{L}$ *es una* **extensión** *de* $\mathbb{K}$ *y escribiremos* $\mathbb{L}/\mathbb{K}$ *para denotar este hecho.*

Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos y $S \subseteq \mathbb{L}$, el conjunto $\mathbb{K}(S)$ denota la intersección de todos los subcuerpos de $\mathbb{L}$ que contienen a $\mathbb{K}$ y a S; esta familia de subcuerpos es no vacía ya que $\mathbb{L}$ es por si mismo un cuerpo que tiene tal propiedad.

Como la intersección de cualquier familia de subcuerpos de $\mathbb{L}$ es también un cuerpo, $\mathbb{K}(S)$ es un cuerpo. Observe que $\mathbb{K}(S)$ está contenido en cada subcuerpo de $\mathbb{L}$ que contiene a $\mathbb{K}$ y a S, por lo tanto $\mathbb{K}(S)$ es el subcuerpo más pequeño de $\mathbb{L}$ que contiene a $\mathbb{K}$ y a S. Cuando $S = \{x_1, \cdots, x_n\}$, el cuerpo $\mathbb{K}(S)$ es denotado por $\mathbb{K}(x_1, \cdots, x_n)$.

Ejemplo 1.7. *Tenemos las extensiones simples* $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(i)/\mathbb{Q}$.

Definición 1.9. *Sea* $\mathbb{L}/\mathbb{K}$ *una extensión de cuerpos,*

- *Un elemento* $u \in \mathbb{L}$ *es llamado* **algebraico** *sobre* $\mathbb{K}$ *si* u *es raíz de algún polinomio no nulo en* $\mathbb{K}[X]$.
- *Se dice que* $\mathbb{L}$ *es una* **extensión algebraica** *de* $\mathbb{K}$ *si cada elemento de* $\mathbb{L}$ *es algebraico sobre* $\mathbb{K}$.

Ejemplo 1.8. $\mathbb{Q}(i)/\mathbb{Q}$ *es una extensión algebraica, pero* $\mathbb{Q}(\pi)/\mathbb{Q}$ *no es algebraica.*

Teorema 1.8. *Sean* $\mathbb{L}/\mathbb{K}$ *una extensión de cuerpos y* $\mathbb{F}$ *el conjunto de todos los elementos de* $\mathbb{L}$ *que son algebraicos sobre* $\mathbb{K}$. *Entonces* $\mathbb{F} \subseteq \mathbb{L}$ *y* $\mathbb{F}/\mathbb{K}$ *es algebraica.*

Demostración. Ver [5], página 286. □

Definición 1.10. *Sean* $\mathbb{L}$ *y* $\mathbb{L}'$ *extensiones de un cuerpo* $\mathbb{K}$. *Un homomorfismo no nulo* $\sigma : \mathbb{L} \to \mathbb{L}'$ *que mantiene fijo a* $\mathbb{K}$, *esto es,* $\sigma(x) = x$ *para todo* $x \in K$, *es llamado un* $\mathbb{K}$**–homomorfismo** *de* $\mathbb{L}$ *en* $\mathbb{L}'$. *El conjunto de todos los* $\mathbb{K}$*–homomorfismo de* $\mathbb{L}$ *en* $\mathbb{L}'$ *es denotado por* $Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{L}')$.

Definición 1.11. *Sea* $\mathbb{K}$ *un cuerpo y* $f(X) \in \mathbb{K}[X]$, *entonces una extensión* $\mathbb{L}$ *de* $\mathbb{K}$ *se llama* **cuerpo de ruptura** *(o cuerpo de raíces) de* $f(X)$ *sobre* $\mathbb{K}$ *si se cumple que:*

i) $f(X)$ *se factoriza completamente en* $\mathbb{L}$, *es decir:*

$$f(X) = c(X - u_1)(X - u_2)\cdots(X - u_n), \quad con \quad c, u_i \in \mathbb{L},\ i \in \{1, \cdots, n\}.$$

ii) $\mathbb{L}$ *es minimal respecto a la propiedad i), es decir* $\mathbb{L} = \mathbb{K}(u_1, u_2, \cdots, u_n)$.

Ejemplo 1.9. *Sea* $f(X) = X^2 + 1 \in \mathbb{R}[X]$, *entonces* $\mathbb{C}$ *es un cuerpo de ruptura de* $f(X)$, *pues* $X^2 + 1 = (X + i)(X - i)$ *en* $\mathbb{C}[X]$ *y* $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$. *Similarmente* $\mathbb{Q}\left(\sqrt{2}\right)$ *es un cuerpo de ruptura del polinomio* $X^2 - 2$ *en* $\mathbb{Q}[X]$, *pues* $X^2 - 2 = \left(X + \sqrt{2}\right)\left(X - \sqrt{2}\right)$ *y* $\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}\left(\sqrt{2}, -\sqrt{2}\right)$.

Algunas nociones útiles sobre cuerpos son las siguientes.

Definición 1.12. *Sea $\mathbb{L}|\mathbb{K}$ una extensión de cuerpos.*

- *Un polinomio $f(X) \in \mathbb{K}[X]$ de grado n se dice* **separable** *si tiene n raíces distintas en algún cuerpo de ruptura. Equivalentemente, $f(X)$ es separable si no tiene raíces repetidas en algún cuerpo de ruptura.*

- *Un elemento α que es algebraico sobre $\mathbb{K}$ es llamado* **separable** *sobre $\mathbb{K}$ si su polinomio minimal sobre $\mathbb{K}$ es separable y $\mathbb{L}|\mathbb{K}$ es llamada* **extensión separable** *sobre $\mathbb{K}$ si es algebraica y cada elemento $\alpha \in \mathbb{L}$ es separable sobre $\mathbb{K}[X]$.*

- *$\mathbb{L}|\mathbb{K}$ es* **normal** *si es algebraica y para todo $\alpha \in \mathbb{L}$, el polinomio minimal se factoriza completamente en $\mathbb{L}$.*

- *Se dice que $\mathbb{K}$ es* **algebraicamente cerrado** *si todo polinomio no constante en $\mathbb{K}[X]$ se factoriza completamente en $\mathbb{K}$.*

- *Si $\mathbb{L}$ es algebraicamente cerrado y es minimal con esta propiedad, entonces $\mathbb{L}$ es llamado una* **clausura algebraica** *de $\mathbb{K}$ y se denota por $\overline{\mathbb{K}}$.*

Observación 1.1. Toda clausura algebraica $\overline{\mathbb{K}}$ de un cuerpo $\mathbb{K}$ es normal.

Teorema 1.9. *Sea $\overline{\mathbb{K}}|\mathbb{K}$ una extensión de cuerpos, entonces $\overline{\mathbb{K}}$ es una clausura algebraica de $\mathbb{K}$ si y solo si $\overline{\mathbb{K}}|\mathbb{K}$ es algebraica y para toda extensión algebraica $\mathbb{L}|\mathbb{K}$ de $\mathbb{K}$ existe un $\mathbb{K}-$homomorfismo $\sigma : \mathbb{L} \to \overline{\mathbb{K}}$. (Esto significa que $\overline{\mathbb{K}}$ es la más grande extensión algebraica de $\mathbb{K}$.)*

Demostración. Ver [7], página 253. □

Teorema 1.10. *Sean $\mathbb{L}|\mathbb{K}$ una extensión algebraica de cuerpos y $\mathbb{E}$ una extensión normal de $\mathbb{K}$ tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{E}$. El grado de separabilidad de $\mathbb{L}|\mathbb{K}$ coincide con el número de $\mathbb{K}-$homormorfismos de $\mathbb{L}$ en $\mathbb{E}$.*

$$[\mathbb{L} : \mathbb{K}]_s = |Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{E})|.$$

Demostración. Ver [7], página 278. □

Sean $\mathbb{L}|\mathbb{K}$ una extensión separable de cuerpos con grado $[\mathbb{L} : \mathbb{K}] = n$ y $\overline{\mathbb{K}}$ una clausura algebraica de $\mathbb{K}$. Por el teorema 1.9 se verifica que $\mathbb{K} \subseteq \mathbb{L} \subseteq \overline{\mathbb{K}}$ y como $\overline{\mathbb{K}}$ es normal, el teorema anterior implica que existen n distintos $\mathbb{K}$–homomorfismos de $\mathbb{L}$ en $\overline{\mathbb{K}}$.
Finalmente tenemos:

Teorema 1.11. Lema de Dedekind: *Sean $\mathbb{L}|\mathbb{K}$ una extensión separable de cuerpos de grado n y $\sigma_1, \cdots, \sigma_n$ los $\mathbb{K}$–homomorfismos diferentes de $\mathbb{L}$ en $\overline{\mathbb{K}}$. Entonces $\sigma_1, \cdots, \sigma_n$ son linealmente independientes.*

1.4. Módulos

Definición 1.13. *Sea R un anillo conmutativo, un R-***módulo** *es un grupo abeliano M junto con una función $R \times M \longrightarrow M$, denotada por $(r, m) \mapsto rm$, que satisface:*

i) $r(m + n) = rm + rn$;

ii) $(r + s)m = rm + sm$;

iii) $(rs)m = r(sm)$;

iv) $1_R m = m$;

para todos $m, n \in M$ y todo $r, s \in R$.

Ejemplo 1.10. *Sea M un grupo abeliano. Los múltiplos enteros de elementos de M se definen inductivamente por:*

i) $1m = m$,

ii) $km = (k - 1)m + m$; *si* $k \geq 2$,

iii) $0m = 0_M$,

iv) $-km = k(-m)$,

donde $m \in M$ y $k \in \mathbb{Z}^+$; de lo que se sigue que todo grupo abeliano es un $\mathbb{Z}$-módulo.

Definición 1.14. *Sea M un R-módulo y N un subgrupo abeliano de M. Se dice que N es un R-***submódulo** *de M (o simplemente un* **submódulo** *de M), lo cual notaremos por $N \leq M$, si $rn \in N$, para cada $n \in N$ y cada $r \in R$.*

Ejemplo 1.11. *Sea R un anillo, $\Im \subseteq R$ un ideal, entonces $\Im$ es subanillo y por tanto subgrupo de R y además $ra \in \Im$, para cada $a \in \Im$ y cada $r \in R$. Esto es, los ideales de un anillo son submódulos.*

Presentamos ahora algunos conceptos sobre módulos que serán de nuestro interés en el desarrollo del trabajo:

Definición 1.15. *Sean R un anillo y M un R-módulo.*

- *Sean $m_1, m_2, \cdots, m_n$ elementos en M, diremos que $m \in M$ es* **combinación lineal** *de $m_1, m_2, \cdots, m_n$ si puede escribirse en la forma $m = a_1m_1 + a_2m_2 + \cdots + a_nm_n$, para algunos $a_i \in R$, $i = 1, 2, \cdots, n$.*
- *Si todo elemento m de M es C.L. de los elementos $m_1, m_2, \cdots, m_n \in M$ diremos que el conjunto $\{m_1, m_2, \cdots, m_n\}$* **genera** *a M sobre R. En este caso decimos que M es* **finitamente generado**.

Definición 1.16. *Un $\mathbb{K}$-módulo V sobre un cuerpo $\mathbb{K}$ es llamado* **espacio vectorial**. *El cuerpo $\mathbb{K}$ es llamado* **cuerpo de escalares** *de V. Una transformación lineal definida de un espacio vectorial V en su cuerpo de escalares $\mathbb{K}$ es llamada* **funcional lineal** *o simplemente* **funcional** *en V. El conjunto de todos los funcionales lineales en V es llamado el* **espacio dual** *de V y se denota por V^*.*

Note que si V es dimensión finita, entonces V y su dual V^* tienen la misma dimensión.

Capítulo 2

El anillo de los enteros algebraicos

Una ecuación Diofántica es una expresión de la forma

$$f(X_1, X_2, \cdots, X_n) = 0,$$

donde $f(X_1, X_2, \cdots, X_n) \in \mathbb{Z}[X_1, X_2, \cdots, X_n]$. Varios problemas de la Teoría de números consisten en dar solución a este tipo de ecuaciones. Un ejemplo de lo anterior es *El Último Teorema de Fermat*, uno de los teoremas más famosos en la historia de la matemática. Éste establece que la ecuación

$$X^n + Y^n = Z^n$$

no tiene soluciones enteras no triviales cuando $n > 2$. El teorema fue conjeturado por Pierre de Fermat en 1637, pero fue demostrado hasta 1995 por Andrew Wiles. Su fama se debe a que en los intentos por demostrarlo se estimuló el desarrollo de varias ramas de la matemática, entre ellas la *teoría algebraica de números* en el siglo XIX.

Esta rama tan importante de la teoría de números estudia las estructuras algebraicas relacionadas con *enteros algebraicos*. En este capítulo daremos las definiciones básicas y probaremos algunos resultados de la teoría de los enteros algebraicos. Al final, usaremos estos resultados como herramienta para solucionar algunos problemas que involucran ecuaciones Diofánticas.

Nota: En adelante nos referimos a anillos como *anillos conmutativos con unidad.*

Definición 2.1. *Un elemento $\alpha \in \mathbb{C}$ se dice que es un* **número algebraico** *si es raíz de algún polinomio mónico con coeficientes en $\mathbb{Q}[X]$, esto es, si existe $f(X) \in \mathbb{Q}[X]$, mónico, tal que $f(\alpha) = 0$.*

Definición 2.2. *Un* **cuerpo numérico** *es un subcuerpo $\mathbb{L}$ de los números complejos $\mathbb{C}$ tal que $\mathbb{L}$ es una extensión finita de los racionales $\mathbb{Q}$. Llamaremos a los elementos de $\mathbb{L}$* **números algebraicos.**

La siguiente definición generaliza las dos definiciones anteriores.

Definición 2.3. *Sea $\mathbb{L}$ un cuerpo y R, B anillos tales que $R \subseteq B \subseteq \mathbb{L}$. Diremos que $\alpha \in B$ es un* **entero** *sobre R si existe $f(X) \in R[X]$ mónico tal que $f(\alpha) = 0$.*

El conjunto formado por los elementos de B que son enteros sobre R es llamado la ***clausura entera de*** R ***en*** B y lo denotamos por $I_B(R)$. Cuando $B = \mathbb{L}$ y $R = \mathbb{Z}$, escribiremos simplemente $I_{\mathbb{L}}$, en particular los elementos de $I_{\mathbb{C}}$ son llamados ***enteros algebraicos***.

Ejemplo 2.1. *Para cada elemento $d \in \mathbb{Z}$, $\sqrt{d}$ es un entero algebraico, así como lo es cualquier raíz enésima de la unidad. Los polinomios mónicos que los anulan son $X^2 - d$ y $X^n - 1$, respectivamente.*

Nuestro primer objetivo es probar que los elementos enteros sobre un dominio entero forman un anillo, y para ello usaremos la siguiente caracterización de la integridad:

Teorema 2.1. *Sean $R \subseteq B \subseteq \mathbb{L}$ con $\mathbb{L}$ un cuerpo, R y B anillos y $\alpha \in B$. Las siguientes afirmaciones son equivalentes:*

1. *α es entero sobre R.*
2. *$R[\alpha] := \{f(\alpha) : f(X) \in R[X]\}$ es un R-módulo finitamente generado.*
3. *Existe un $R-$módulo finitamente generado M tal que $M \subseteq B$ y $\alpha M \subseteq M$.*

Demostración.
$(1 \Rightarrow 2)$ Como α es entero sobre R, existe $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ en $R[X]$ tal

que $f(\alpha) = 0$. Consideremos el $R-$módulo

$$M := R + R\alpha + \cdots + R\alpha^{n-1}.$$

Veamos que $M = R[\alpha]$. En efecto, $M \subseteq R[\alpha]$, pues si $x \in M$, entonces $x = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, donde $b_i \in R$ para todo $0 \leq i \leq n-1$. Luego $x = g(\alpha)$, con $g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} \in R[X]$. Para ver la otra contenencia basta mostrar que para todo $k \in \mathbb{N}$ se tiene que $1, \alpha, \cdots, \alpha^{n+k} \in M$. Si $k = 0$, como $f(\alpha) = 0$, entonces $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, esto es:

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

Luego $\alpha^n \in M$ y por lo tanto $1, \alpha, \cdots, \alpha^n \in M$. Ahora supongamos que $1, \alpha, \ldots, \alpha^{n+k-1} \in M$, como

$$\alpha^{n+k} = -a_{n-1}\alpha^{n+k-1} - \cdots - a_1\alpha^{k+1} - a_0\alpha^k,$$

tenemos que $\alpha^{n+k} \in M$, ya que M es $R-$módulo. Concluimos que $1, \alpha, \ldots, \alpha^{n+k} \in M$ para todo $k \in \mathbb{N}$ y así $M \supseteq R[\alpha]$, pues para todo $p(X) \in R[X]$, $p(\alpha) \in M$, luego $R[\alpha] = M$ y es generado por el conjunto $\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$.

$(2 \Rightarrow 3)$ Definamos $M := R[\alpha]$, entonces M es un $R-$módulo finitamente generado; $M \subseteq B$, pues $\alpha \in B$ y $R \subseteq B$ y $\alpha M \subseteq M$ ya que si $y \in \alpha M$, entonces $y = \alpha q(\alpha) \in R[\alpha]$, con $q(X) \in R[X]$.

$(3 \Rightarrow 2)$ Sea $\{m_1, m_2, \ldots, m_n\}$ un conjunto generador de M. Como $\alpha M \subseteq M$ tenemos que $\alpha m_j \in M$ para todo $j \in \{1, 2, \ldots, n\}$, así considerando los m_j como indeterminadas, tenemos el sistema de ecuaciones

$$\begin{cases} \alpha m_1 &= a_{11}m_1 + a_{12}m_2 + \cdots + a_{1n}m_n \\ \alpha m_2 &= a_{21}m_1 + a_{22}m_2 + \cdots + a_{2n}m_n \\ \vdots & \qquad\qquad \vdots \\ \alpha m_n &= a_{n1}m_1 + a_{n2}m_2 + \cdots + a_{nn}m_n \end{cases}$$

que es equivalente a

$$\begin{cases} 0 &= (a_{11}-\alpha)\,m_1 + a_{12}m_2 + \cdots + a_{1n}m_n \\ 0 &= a_{21}m_1 + (a_{22}-\alpha)\,m_2 + \cdots + a_{2n}m_n \\ \vdots & \qquad\qquad \vdots \\ 0 &= a_{n1}m_1 + a_{n2}m_2 + \cdots + (a_{nn}-\alpha)\,m_n \end{cases}$$

donde $a_{ij} \in R$ para todo $1 \leq i, j \leq n$. Reescribiendo el sistema como $S\mathbf{x} = 0$, donde

$$S := \begin{pmatrix} a_{11}-\alpha & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\alpha & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\alpha \end{pmatrix},$$

observamos que $\mathbf{x} = (m_1, m_2, \ldots, m_n)^t \neq \mathbf{0}$ es una solución. Luego $\det(S) = 0$, pues si así no fuera, el sistema tendría solución única, sin embargo $\mathbf{x}' = \mathbf{0}$ también soluciona el sistema lo que sería una contradicción. Ahora si $P_{S'}(X)$ es el polinomio característico de $S' := S + I\alpha$, tenemos que $P_{S'}(\alpha) = \det(S' - I\alpha) = \det(S) = 0$ y por lo tanto α es un entero sobre R. □

Corolario 2.2. *Si $\alpha_1, \alpha_2, \cdots, \alpha_m$ son enteros sobre R, entonces $R[\alpha_1, \alpha_2, \cdots, \alpha_m]$ es un $R-$módulo finitamente generado.*

Demostración. Realizaremos inducción sobre m, el número de elementos que son enteros sobre R.

Si $m = 1$ por el ítem 2 del Teorema 2.1 tenemos que $R[\alpha_1]$ es un $R-$módulo finitamente generado. Sea $1 < k \leq m$ y supongamos que el resultado es verdadero para $k-1$, es decir, que $R_{k-1} := R[\alpha_1, \alpha_2, \cdots, \alpha_{k-1}]$ es un $R-$módulo finitamente generado. Como α_k es un entero sobre R, existe $f(X) \in R[X]$ mónico tal que $f(\alpha_k) = 0$, pero $R \subseteq R[\alpha_1, \alpha_2, \cdots, \alpha_{k-1}]$, luego α_k también es entero sobre R_{k-1}, entonces $R_k = R_{k-1}[\alpha_k]$ es un $R_{k-1}-$módulo finitamente generado. Sean $\beta_1, \beta_2, \cdots, \beta_n$ un sistema de generadores de R_{k-1} sobre R y $\delta_1, \delta_2, \cdots, \delta_t$ un sistema de generadores R_k sobre R_{k-1}, afirmamos que $\left\{\delta_i\beta_j : 1 \leq i \leq t, 1 \leq j \leq n\right\}$ es un sistema de generadores de $R_k = R[\alpha_1, \alpha_2, \cdots, \alpha_k]$ sobre R. En efecto,

Si $x \in R_k$, entonces $x = \sum_{i=1}^{t} \delta_i r_i$ con $r_i \in R_{k-1}$. Por otra parte $r_i = \sum_{j=1}^{n_i} \beta_j c_{ji}$, con $c_{ij} \in R$ para $1 \leq i \leq t$, $1 \leq j \leq n_i$. Así,

$$x = \sum_{i=1}^{t} \delta_i \sum_{j=1}^{n_i} \beta_j c_{ji} = \sum_{\substack{1 \leq i \leq t \\ 1 \leq j \leq n_i}} \delta_i \beta_j c_{ji}.$$

Por el principio de inducción matemática, tenemos que R_m es un R-módulo finitamente generado, para todo $m \in \mathbb{Z}^+$. □

Corolario 2.3. *$I_B(R)$ es un subanillo de B que contiene a R.*

Demostración. Veamos que $I_B(R)$ es un subanillo de B, en efecto $I_B(R)$ es no vacío, ya que R es no vacío y si $a \in R$, entonces $f(X) = X - a \in R[X]$ es un polinomio mónico tal que $f(a) = 0$, esto es $a \in I_B(R)$, en particular $R \subseteq I_B(R)$. Probemos que $I_B(R)$ es cerrado bajo la suma y el producto. Sean $\alpha, \beta \in I_B(R)$, entonces $R[\alpha, \beta]$ es un $R-$módulo finitamente generado por el corolario anterior y tenemos que $\alpha - \beta,\ \alpha\beta \in R[\alpha, \beta]$. Luego,

$$(\alpha - \beta)R[\alpha, \beta] \subseteq R[\alpha, \beta] \text{ y}$$
$$(\alpha\beta)R[\alpha, \beta] \subseteq R[\alpha, \beta]$$

Así, por 3 del Teorema 2.1 tenemos que $\alpha - \beta$ y $\alpha\beta$ son enteros sobre R, es decir $\alpha - \beta,\ \alpha\beta \in I_B(R)$. □

Definición 2.4. *Sean $\mathbb{L}$ un cuerpo y R, B anillos con $R \subseteq B \subseteq \mathbb{L}$.*

- *Si $I_B(R) = R$, diremos que R es* **integralmente cerrado en** *B.*
- *Si R es integralmente cerrado en su cuerpo de fracciones decimos que R es* **integralmente cerrado**.
- *Si $I_B(R) = B$, diremos que B es* **entero sobre** *R.*

Ejemplo 2.2. *Toda extensión algebraica de un cuerpo $\mathbb{K}$ es entera sobre $\mathbb{K}$. En efecto, si $\mathbb{E}$ es una extensión algebraica de $\mathbb{K}$ y $b \in \mathbb{E}$, entonces existe $g(X) = a_n X^n + a_{n-1} X^{n-1} \cdots + a_1 X + a_0 \in$*

$\mathbb{K}[X]$, *de grado n tal que* $g(b) = 0$, *además como* $\mathbb{K}$ *es cuerpo,* $f(X) = a_n^{-1}g(X)$ *es mónico en* $\mathbb{K}[X]$ *y* $f(b) = 0$, *luego* $b \in I_{\mathbb{E}}(\mathbb{K})$ *y* $\mathbb{E} \subseteq I_{\mathbb{E}}(\mathbb{K})$. *Por lo tanto* $I_{\mathbb{E}}(\mathbb{K}) = \mathbb{E}$.

Los DFU son ejemplos de dominios integralmente cerrados como veremos a continuación.

Teorema 2.4. *Todo dominio de factorización única es integralmente cerrado.*

Demostración. Sea R un dominio de factorización única y $\mathbb{K} = Q(R)$ su cuerpo de fracciones. Es claro que $R \subseteq I_{\mathbb{K}}(R)$. Ahora si $\alpha \in I_{\mathbb{K}}(R)$, podemos escribir $\alpha = \dfrac{a}{b}$, con $a, b \in R$, $b \neq 0$ y $\text{mcd}(a, b) = 1$. Además, sabemos que existe $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in R[X]$ tal que $f(\alpha) = 0$ y por lo tanto

$$\frac{a^n}{b^n} = -\left(c_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + c_1\frac{a}{b} + c_0\right).$$

De modo que,

$$\begin{aligned} a^n &= -b^n\left(c_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + c_1\frac{a}{b} + c_0\right) \\ &= -b(c_{n-1}a^{n-1} + \cdots + c_1b^{n-2} + c_0b^{n-1}). \end{aligned}$$

Veamos que $b \in U(R)$. Si $b \notin U(R)$, como R es DFU, existe $p \in R$ irreducible tal que $p \mid b$, por la igualdad anterior $p \mid a^n$ y por tanto $p \mid a$ lo que contradice que a y b son primos relativos, entonces $b \in U(R)$. Luego $\alpha \in R$ y $R \supseteq I_{\mathbb{K}}(R)$, con lo que se concluye que $R = I_{\mathbb{K}}(R)$, esto es, R es integralmente cerrado. □

Ejemplo 2.3. $I_{\mathbb{Q}} = \mathbb{Z}$, *ya que* $\mathbb{Z}$ *es DFU y* $\mathbb{Q}$ *es su cuerpo de fracciones.*

2.1. Traza y Norma

En esta sección definimos los conceptos de traza y norma de un elemento, que resultarán útiles para determinar los enteros algebraicos de algunos cuerpos numéricos.

Sea $\mathbb{L}|\mathbb{K}$ una extensión de cuerpos con $[\mathbb{L} : \mathbb{K}] = n$, es decir que $\mathbb{L}$ como espacio vectorial sobre $\mathbb{K}$ tiene dimensión finita n. Para cada $\alpha \in \mathbb{L}$ definimos el operador lineal

$$\begin{aligned} \mu_\alpha : \mathbb{L} &\longrightarrow \mathbb{L} \\ y &\longmapsto \mu_\alpha(y) = \alpha y. \end{aligned}$$

Definición 2.5. *La* **norma** *y* **traza** *de α con respecto a $\mathbb{L}|\mathbb{K}$, que denotamos por $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ y $T_{\mathbb{L}|\mathbb{K}}(\alpha)$ respectivamente se definen como*

$$N_{\mathbb{L}|\mathbb{K}}(\alpha) := \det(\mu_\alpha);$$
$$T_{\mathbb{L}|\mathbb{K}}(\alpha) := Traza(\mu_\alpha).$$

Más precisamente, si $\mathcal{B} = \{\beta_1, \beta_2, \cdots, \beta_n\}$ una base de $\mathbb{L}$ sobre $\mathbb{K}$ y para cada $i \in \{1, \cdots, n\}$

$$\alpha\beta_i = \sum_{j=1}^{n} a_{ij}\beta_j,$$

con $a_{ij} \in \mathbb{K}$, entonces

$$N_{\mathbb{L}|\mathbb{K}}(\alpha) = \det(\mu_\alpha) = \det(A_\alpha);$$
$$T_{\mathbb{L}|\mathbb{K}}(\alpha) = Traza(\mu_\alpha) = Traza(A_\alpha) = \sum_{i=1}^{n} a_{ii};$$

donde $A_\alpha = \left[a_{ij}\right]_{\mathcal{B}}$, la matriz de la transformación μ_α en la base $\mathcal{B}$.

Notemos que $N_{\mathbb{L}|\mathbb{K}}$ y $T_{\mathbb{L}|\mathbb{K}}$ son funciones de $\mathbb{L}$ en $\mathbb{K}$ y además si $\mathcal{B}'$ es otra base de $\mathbb{L}$ sobre $\mathbb{K}$ y A'_α es la matriz de la transformación μ_α en la base $\mathcal{B}'$ entonces A'_α y A_α son matrices similares, por lo tanto tienen igual determinante e igual traza, luego $N_{\mathbb{L}|\mathbb{K}}$ y $T_{\mathbb{L}|\mathbb{K}}$ están bien definidas en el sentido de que no dependen de la base escogida.

Ejemplo 2.4. *Sean $\mathbb{K} = \mathbb{R}$ y $\mathbb{L} = \mathbb{C}$, entonces $[\mathbb{C} : \mathbb{R}] = 2$, y $\{1, i\}$ una base de $\mathbb{C}$ sobre $\mathbb{R}$. Si $\alpha = a + bi \in \mathbb{C}$, entonces*

$$\alpha \cdot 1 = a \cdot 1 + b \cdot i \quad y \quad \alpha \cdot i = -b \cdot 1 + a \cdot i.$$

Luego

$$A_\alpha = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Por lo tanto la traza y la norma de α en relación a $\mathbb{C}|\mathbb{R}$ son:

$$T_{\mathbb{C}|\mathbb{R}}(\alpha) = Traza\,(A_\alpha) = 2a \;\; y \;\; \mathbb{N}_{\mathbb{C}|\mathbb{R}}(\alpha) = \det(A_\alpha) = a^2 + b^2.$$

Definición 2.6. *El polinomio $P_\alpha(X) := \det(XI_n - A_\alpha)$ es llamado* **polinomio característico** *de α en $\mathbb{K}$, donde I_n es la matriz identidad en $M_n(\mathbb{K})$ y A_α la representación matricial de μ_α en alguna base.*

Se tiene que $P_\alpha(X)$ no depende de la base de $\mathbb{L}$ sobre $\mathbb{K}$ escogida para A_α y en este sentido está bien definido.

Proposición 2.5. ***Propiedades***
Sean $\mathbb{L}|\mathbb{K}$ una extensión de cuerpos, con $[\mathbb{L} : \mathbb{K}] = n$; $\alpha, \beta \in \mathbb{L}$; $P_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, el polinomio característico de α sobre $\mathbb{K}$ y $a, b \in \mathbb{K}$, entonces:

1. $T_{\mathbb{L}|\mathbb{K}}(\alpha) = -a_{n-1} \;\; y \;\; N_{\mathbb{L}|\mathbb{K}}(\alpha) = (-1)^n a_0$.
2. $P_\alpha(X) = m_\alpha(X)^k$ *donde* $k = [\mathbb{L} : \mathbb{K}(\alpha)]$ *y* $m_\alpha(X)$ *es el polinomio minimal de* α.
3. $T_{\mathbb{L}|\mathbb{K}}(a\alpha + b\beta) = aT_{\mathbb{L}|\mathbb{K}}(\alpha) + bT_{\mathbb{L}|\mathbb{K}}(\beta) \quad y \quad T_{\mathbb{L}|\mathbb{K}}(a) = na$.
4. $N_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\beta) \quad y \quad N_{\mathbb{L}|\mathbb{K}}(a) = a^n$.
5. *Si $\mathbb{L}$ es una extensión finita y separable de $\mathbb{K}$ y $\sigma_1, \sigma_2, \cdots, \sigma_n$ son los $\mathbb{K}$–homomorfismos de $\mathbb{L}$ en $\overline{\mathbb{K}}$, entonces:*

$$P_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha)),$$
$$N_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha),$$
$$T_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha).$$

Demostración. Ver [10], páginas 87 y 93. □

Teorema 2.6. *Sean R un dominio integralmente cerrado, $\mathbb{L}$ una extensión finita y separable de $\mathbb{K} = Q(R)$ y $\alpha \in I_{\mathbb{L}}(R)$, con $\alpha \neq 0$ entonces:*

1. $m_\alpha(X), P_\alpha(X) \in R[X]$, *y, por lo tanto,* $N_{\mathbb{L}|\mathbb{K}}(\alpha), T_{\mathbb{L}|\mathbb{K}}(\alpha) \in R$.

2. $\alpha | N_{\mathbb{L}|\mathbb{K}}(\alpha)$ *en* $I_{\mathbb{L}}(R)$.

3. $\alpha \in U(I_{\mathbb{L}}(R))$, *si y solo si,* $N_{\mathbb{L}|\mathbb{K}}(\alpha) \in U(R)$.

4. *Si* $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ *es irreducible en R, entonces* α *es irreducible en* $I_{\mathbb{L}}(R)$.

Demostración.

1. Como α es entero sobre R, existe $h(X) \in R[X]$ mónico tal que $h(\alpha) = 0$ y como $m_\alpha(X)$ es el polinomio minimal de α sobre $\mathbb{K}$, existe $g(X) \in \mathbb{K}[X]$ tal que,

$$m_\alpha(X)g(X) = h(X).$$

   Así $g(X)$ es mónico, ya que $m_\alpha(X)$ y $h(X)$ lo son. Escribiendo

$$g(X) = \prod_{i=1}^{m}(X - \beta_i) \quad \text{y} \quad m_\alpha(X) = \prod_{i=1}^{n}(X - \alpha_i),$$

   en $\overline{\mathbb{K}}[X]$, como $m_\alpha(X)g(X) \in R[X]$ tenemos que $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m \in I_{\overline{\mathbb{K}}}(R)$, por lo tanto los coeficientes de $g(X)$ y $m_\alpha(X)$ están en

$$I_{\overline{\mathbb{K}}}(R) \cap \mathbb{K} = I_{\mathbb{K}}(R) = R,$$

   donde la última igualdad se sigue de la hipótesis R es integralmente cerrado.
   Así, $m_\alpha(X) \in R[X]$ y como $P_\alpha(X) = m_\alpha(X)^k$, tenemos que $P_\alpha(X) \in R[X]$.

2. Sean $\sigma_1, \sigma_2, \cdots, \sigma_n$ son los $\mathbb{K}-$homomorfismos de $\mathbb{L}$ en $\overline{\mathbb{K}}$ y digamos que σ_1 es la identidad. Entonces:

$$N_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha) = \alpha\prod_{i=2}^{n}\sigma_i(\alpha).$$

Observe que $\prod_{i=2}^{n} \sigma_i(\alpha) \in I_{\mathbb{L}}(R)$, pues como $\alpha \in I_{\mathbb{L}}(R)$, existe $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[x]$ tal que $f(\alpha) = 0$. Luego, para cada $i \in \{1, 2, \cdots, n\}$

$$\begin{aligned} f(\sigma_i(\alpha)) &= \sigma_i^n(\alpha) + a_{n-1}\sigma_i^{n-1}(\alpha) + \cdots + a_1\sigma_i(\alpha) + a_0 \\ &= \sigma_i(\alpha^n) + a_{n-1}\sigma_i(\alpha^{n-1}) + \cdots + a_1\sigma_i(\alpha) + a_0 \\ &= \sigma_i(\alpha^n) + \sigma_i(a_{n-1}\alpha^{n-1}) + \cdots + \sigma_i(a_1\alpha) + \sigma_i(a_0) \\ &= \sigma_i(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\ &= \sigma_i(f(\alpha)) = 0. \end{aligned}$$

Por lo tanto $\sigma_i(\alpha) \in I_{\mathbb{L}}(R)$ para cada $i \in \{1, 2, \cdots, n\}$.

3. ($\Rightarrow$) Si $\alpha \in U(I_{\mathbb{L}}(R))$, existe $\beta \in I_{\mathbb{L}}(R)$ no nulo tal que $\alpha\beta = 1$, entonces $N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\beta) = 1$, luego $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ es invertible en R, esto es, $N_{\mathbb{L}|\mathbb{K}}(\alpha) \in U(R)$.

   ($\Leftarrow$) Por el ítem anterior, existe $\lambda \in I_{\mathbb{L}}(R)$ tal que $\lambda\alpha = N_{\mathbb{L}|\mathbb{K}}(\alpha)$. Así, si δ es el inverso de $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ en R, entonces $\lambda\delta$ es el inverso de α en $I_{\mathbb{L}}(R)$.

4. Si $\alpha = \beta\theta$ con $\beta, \theta \in I_{\mathbb{L}}(R)$, tenemos que

$$N_{\mathbb{L}|\mathbb{K}}(\alpha) = N_{\mathbb{L}|\mathbb{K}}(\beta)N_{\mathbb{L}|\mathbb{K}}(\theta).$$

   Como $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ es irreducible, entonces $N_{\mathbb{L}|\mathbb{K}}(\beta) \in U(R)$ o $N_{\mathbb{L}|\mathbb{K}}(\theta) \in U(R)$ y por el ítem anterior $\beta \in U(I_{\mathbb{L}}(R))$ o $\theta \in U(I_{\mathbb{L}}(R))$. Luego α es irreducible en $I_{\mathbb{L}}(R)$.

□

2.2. Enteros algebraicos de cuerpos cuadráticos

Definición 2.7. *Un* **cuerpo cuadrático** *es un subcuerpo* $\mathbb{L}$ *de* $\mathbb{C}$ *tal que* $[\mathbb{L} : \mathbb{Q}] = 2$.

Definición 2.8. *Un número entero* d *es* **libre de cuadrados** *si no existe un número primo* p *tal que* $p^2 \mid d$*, es decir si los factores primos de* d *son todos distintos.*

Caractericemos ahora los cuerpos cuadráticos en términos de los enteros libres de cuadrados.

Proposición 2.7. *Sea* $\mathcal{D} = \{d \in \mathbb{Z} : d \notin \{0, 1\}$ *y* d *es libre de cuadrados*$\}$. *La aplicación definida por* $d \longmapsto \mathbb{Q}\left(\sqrt{d}\right)$ *es una biyección de* $\mathcal{D}$ *sobre el conjunto de los cuerpos cuadráticos.*

Demostración. Dado $d \in \mathcal{D}$, entonces $\sqrt{d}$ es irracional. De hecho, si $\sqrt{d} = \frac{a}{b}$, con $a, b \in \mathbb{Z}$, $b \neq 0$ y $\text{mcd}(a, b) = 1$, entonces

$$b^2 d = a^2 \tag{2.1}$$

es decir, $d \mid a^2$. Como d es libre de cuadrados, tenemos que $d = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, con p_i primo para $1 \leq i \leq k$. Así, $p_i \mid a^2$ y por tanto $p_i \mid a$ para todo $1 \leq i \leq k$. Luego $d \mid a$ y $a = dk$ para algún $k \in \mathbb{Z}$. Reemplazando a en (2.1) tenemos que $b^2 = dk^2$ y $d \mid b^2$. Finalmente, usando el mismo argumento anterior podemos concluir que $d \mid b$ y como $\text{mcd}(a, b) = 1$, $d = 1$, lo que es una contradicción.

Concluimos que, $\mathbb{Q}\left(\sqrt{d}\right) \neq \mathbb{Q}$ y por lo tanto $\mathbb{Q}\left(\sqrt{d}\right)$ es un cuerpo cuadrático con base $\left\{1, \sqrt{d}\right\}$ sobre $\mathbb{Q}$.

Por otra parte, si $d \neq d'$, entonces $\mathbb{Q}\left(\sqrt{d}\right) \neq \mathbb{Q}\left(\sqrt{d'}\right)$. En efecto, escribiendo $\sqrt{d} = r + s\sqrt{d'}$, con $r, s \in \mathbb{Q}$, tenemos

$$d = r^2 + 2rs\sqrt{d'} + s^2 d'$$

y como $\sqrt{d'}$ es irracional, concluimos que $r = 0$ ó $s = 0$. Si $r = 0$, entonces $d = s^2 d'$ lo que contradice que d o d' es libre de cuadrados y si $s = 0$, entonces $\sqrt{d} = r$, lo que contradice la irracionalidad de $\sqrt{d}$ y la aplicación es inyectiva.

Para la sobreyectividad, considere $\mathbb{L}$ un cuerpo cuadrático y $\alpha \in \mathbb{L} \setminus \mathbb{Q}$, entonces $\mathbb{L} = \mathbb{Q}(\alpha)$. Como $[\mathbb{L} : \mathbb{Q}] = 2$ tenemos que 1, α y α^2 son linealmente dependientes, por lo tanto existen $a,\ b,\ c \in \mathbb{Q}$ tales que $a \neq 0$ y $a\alpha^2 + b\alpha + c = 0$. Multiplicando por $4a$ y completando cuadrados llegamos a

$$(2a\alpha + b)^2 = b^2 - 4ac. \tag{2.2}$$

Sean $\beta = 2a\alpha + b$ y $q = b^2 - 4ac$ de modo que $\mathbb{Q}\left(\sqrt{q}\right) = \mathbb{Q}(\beta) = \mathbb{L}$, gracias a (2.2). Ahora, como $b^2 - 4ac \in \mathbb{Q}$, existen $m, n \in \mathbb{Z}$, $n \neq 0$ tales que $b^2 - 4ac = \frac{m}{n}$ y $\text{mcd}(m, n) = 1$, de donde obtenemos que

$$\sqrt{b^2 - 4ac} = \sqrt{\frac{m}{n}} = \frac{\sqrt{mn}}{n}.$$

Finalmente, $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$, donde $d = mn$. Podemos asumir que d es libre de cuadrados, de lo contrario $d = e^2 f$ con $e, f \in \mathbb{Z}$ y f libre de cuadrados y en este caso $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(\sqrt{f}\right)$. □

Observación 2.1. Si $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$ es un cuerpo cuadrático, entonces los dos $\mathbb{Q}-$homomorfismos de $\mathbb{L}$ en $\mathbb{C}$, son precisamente $\sigma_1(x) = x$ y $\sigma_2(x) = \overline{x}$, donde $\overline{x}$ denota el conjugado de x, es decir, ; es decir, para $x = a+b\sqrt{d} \in \mathbb{L}$, $\sigma_2(x) = a-b\sqrt{d}$. Así, si $\alpha \in \mathbb{L}$, entonces $\alpha = m+n\sqrt{d}$, con $m, n \in \mathbb{Q}$ y $d \in \mathcal{D}$, por lo tanto:

$$N_{\mathbb{L}|\mathbb{Q}}(\alpha) = \prod_{i=1}^{2} \sigma_i(\alpha) = \left(m + n\sqrt{d}\right)\left(m - n\sqrt{d}\right) = m^2 - n^2 d.$$

En los siguientes dos teoremas caracterizamos los enteros algebraicos de un cuerpo cuadrático.

Teorema 2.8. *Sea $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$ un cuerpo cuadrático. Entonces el anillo $I_{\mathbb{L}}$ de los enteros algebraicos de $\mathbb{L}$ está dado por:*

$$I_{\mathbb{L}} = \left\{\frac{m}{2} + \frac{n}{2}\sqrt{d} \mid m, n \in \mathbb{Z},\ \ m^2 \equiv n^2 d \pmod 4\right\}.$$

Demostración.

($\subseteq$) Si $\alpha \in I_{\mathbb{L}} \subseteq \mathbb{L}$, entonces $\alpha = a + b\sqrt{d}$, con $a, b \in \mathbb{Q}$. Por el ítem 1 del Teorema 2.6, $P_\alpha(X) \in Z[X]$ y como $P_\alpha(X) = X^2 + 2aX + (a^2 - b^2)$, podemos concluir que $2a, (a^2 - b^2) \in \mathbb{Z}$ y por lo tanto $\triangle = (2a)^2 - 4(a^2 - b^2) = (2s)^2 d \in \mathbb{Z}$.

Sean $k_p \in \mathbb{Z}$ y $e_p \in \{0, 1\}$ los exponentes de un primo p en las factorizaciones de $2b$ y d respectivamente. Como $(2b)^2 d \in \mathbb{Z}$, tenemos que $2k_p + e_p \geq 0$. De ese modo, $k_p \geq -\frac{e_p}{2} \geq -\frac{1}{2}$, lo que implica que $k_p \geq 0$. Por lo tanto, $2b \in \mathbb{Z}$, luego $2a = m$ y $2b = n$ con $m, n \in \mathbb{Z}$.
Así, $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$ y $m^2 - n^2 d = 4\left(a^2 - b^2 d\right) = 4N_{\mathbb{L}|\mathbb{Q}}(\alpha)$, luego $m^2 \equiv n^2 d \pmod 4$.

($\supseteq$) Sean $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$, con $m, n \in \mathbb{Z}$ y $m^2 \equiv n^2 d \pmod 4$ y $\left\{1,\ \sqrt{d}\right\}$ una base de $\mathbb{L}|\mathbb{Q}$. Como,

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \quad \text{y} \quad \alpha\sqrt{d} = \frac{nd}{2} + \frac{m}{2}\sqrt{d},$$

tenemos que,

$$P_\alpha(X) = \det\begin{pmatrix} X - \frac{m}{2} & -\frac{n}{2} \\ -\frac{nd}{2} & X - \frac{m}{2} \end{pmatrix} = \left(X - \frac{m}{2}\right)^2 - \frac{n^2 d}{4} = X^2 - mX + \frac{(m^2 - n^2)d}{4} \in \mathbb{Z}[X]$$

y $P_\alpha(\alpha) = 0$, luego $\alpha \in I_{\mathbb{L}}$. □

Mostraremos ahora que $I_{\mathbb{L}}$ es un $\mathbb{Z}-$módulo libre, más específicamente, mostraremos el siguiente resultado:

Teorema 2.9. *Si* $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$*, donde d es un entero libre de cuadrados y*

$$\delta = \begin{cases} \sqrt{d}, & si\ d \equiv 2, 3 \pmod 4, \\ \dfrac{1 + \sqrt{d}}{2}, & si\ d \equiv 1 \pmod 4. \end{cases}$$

Entonces, $\{1, \delta\}$ *es una base del* $\mathbb{Z}-$*módulo* $I_{\mathbb{L}}$.

Demostración. El conjunto $\{1, \delta\}$ es linealmente independiente sobre $\mathbb{Z}$, pues es linealmente independiente sobre $\mathbb{Q}$ y sabemos que

$$I_{\mathbb{L}} = \left\{\frac{m}{2} + \frac{n}{2}\sqrt{d} \mid m, n \in \mathbb{Z},\ \ m^2 \equiv n^2 d \pmod 4\right\}.$$

Si $\delta = \sqrt{d}$, tenemos que $\delta \in I_{\mathbb{L}}$, y, si $\delta = \dfrac{1 + \sqrt{d}}{2}$, concluimos $\delta = \dfrac{1}{2} + \dfrac{1}{2}\sqrt{d}$ y $d \equiv 1 \pmod 4$ lo que implica que $\delta \in I_{\mathbb{L}}$, así $\mathbb{Z} + \mathbb{Z}\delta \subseteq I_{\mathbb{L}}$.
Ahora, sea $\alpha \in I_{\mathbb{L}}$, entonces $\alpha = \dfrac{m}{2} + \dfrac{n}{2}\sqrt{d}$, con $m, n \in \mathbb{Z}$ y $m^2 \equiv n^2 d \pmod 4$.
Consideremos dos casos:
Caso 1: Si $d \equiv 1 \pmod 4$, en este caso $m^2 \equiv n^2 \pmod 4$, luego existe $k \in \mathbb{Z}$ tal que $m^2 - n^2 = 4k$. Así, $(m - n)^2 = 4k - 2mn + 2n^2$, por lo tanto $m - n$ es par, de ese modo $m = 2k' + n$, con $k' \in \mathbb{Z}$, luego

$$\alpha = \frac{2k' + n}{2} + \frac{n}{2}\sqrt{d} = k' + n\frac{1 + \sqrt{d}}{2} = k' + n\delta \in \mathbb{Z} + \mathbb{Z}\delta.$$

Caso 2: Si $d \equiv 2,3 \pmod 4$, tenemos que $\delta = \sqrt{d}$, entonces es suficiente probar que m y n son pares. Si n es impar, o equivalentemente $n \equiv 1 \pmod 2$, tenemos, $n^2 \equiv 1 \pmod 4$, por lo tanto $m^2 \equiv n^2 d \equiv d \pmod 4$; pero si m es par, entonces $m^2 \equiv 0 \pmod 4$, así $d \equiv 0 \pmod 4$, contradicción; y si m es impar, $m^2 \equiv 1 \pmod 4$, así $d \equiv 1 \pmod 4$, y, de nuevo tenemos una contradicción. Luego n tiene que ser par.

Finalmente, como $m^2 \equiv n^2 d \equiv 0 \pmod 4$, tenemos que m también es par, así, $I_{\mathbb{L}} \subseteq \mathbb{Z}+\mathbb{Z}\delta$. □

Ejemplo 2.5. *Sea* $\mathbb{L} = \mathbb{Q}\left(\sqrt{-5}\right)$. *El domino* $I_{\mathbb{L}}$ *no es DFU. De hecho como* $-5 \equiv 3 \pmod 4$, *entonces* $I_{\mathbb{L}} = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. *Observe que:*

$$\left(1 + 2\sqrt{-5}\right)\left(1 - 2\sqrt{-5}\right) = 3 \cdot 7.$$

Basta mostrar que los factores $1 \pm 2\sqrt{-5}$, *3 y 7 son irreducibles en* $I_{\mathbb{L}}$. *Como ellos tienen norma 21, 21, 9 y 49 respectivamente, tenemos que si* $1 + 2\sqrt{-5}$ *fuese reducible, existen* $\alpha, \beta \in I_{\mathbb{L}} \setminus U(I_{\mathbb{L}})$ *tales que* $1 + 2\sqrt{-5} = \alpha\beta$, *entonces tendríamos que* $21 = N_{\mathbb{L}|\mathbb{Q}}(\alpha)N_{\mathbb{L}|\mathbb{Q}}(\beta)$, *luego* $N_{\mathbb{L}|\mathbb{Q}}(\alpha) \in \{3, -3, 7, -7\}$. *Pero esto es imposible, pues* $N_{\mathbb{L}|\mathbb{Q}}\left(a + b\sqrt{-5}\right) = a^2 + b^2 5 \notin \{3, -3, 7, -7\}$ *para cualesquiera* $a, b \in \mathbb{Z}$. *La irreducibilidad de* $1 - 2\sqrt{-5}$, *3 y 7 se prueba análogamente.*

Observación 2.2. La recíproca del ítem 4 del Teorema 2.6 no es cierta. De hecho, probamos en el Ejemplo 2.5 $1 + 2\sqrt{-5}$ es irreducible en $I_{\mathbb{L}}$, con $\mathbb{L} = \mathbb{Q}\left(\sqrt{-5}\right)$, pero $N_{\mathbb{L}|\mathbb{Q}}\left(1 + 2\sqrt{-5}\right) = 21$ no es irreducible en $\mathbb{Z}$.

2.3. Factorización única en los enteros algebraicos

Como vimos en el Ejemplo 2.5, aunque $\mathbb{Z}$ es un DFU, esto no implica que el anillo de enteros algebraicos de un cuerpo numérico tenga factorización única. A pesar de esto, podemos encontrar ejemplos de cuerpos numéricos $\mathbb{L}$, tales que $I_{\mathbb{L}}$ sea DFU, pero antes necesitamos recordar la noción de dominio Euclidiano.

Definición 2.9. *Un dominio integral* R *es un* **dominio Euclidiano**, *si existe una función* $\delta : R \setminus \{0\} \longrightarrow \mathbb{N}$ *con las siguientes propiedades:*

i) *Si* $a, b \in R \setminus \{0\}$, *entonces* $\delta(a) \leq \delta(ab)$.

ii) *Si* $a, b \in R$ *y* $b \neq 0$, *entonces existen* $q, r \in R$ *tales que* $a = qb + r$ *y* $r = 0$ *ó* $\delta(r) < \delta(b)$.

Ejemplo 2.6. $\mathbb{Z}$ *es un dominio Euclidiano con la función* δ *dada por* $\delta(a) := |a|$, *donde* $|a|$ *denota el valor absoluto de* a. *La propiedad i*) *se cumple, ya que* $|ab| = |a||b| \geq |b|$, *para todo* $a, b \in \mathbb{Z}$, $a \neq 0$ *y la propiedad ii*) *se sigue del Algoritmo de la División en los enteros.*

Ejemplo 2.7. *El anillo de polinomios* $\mathbb{K}[X]$, *sobre un cuerpo* $\mathbb{K}$ *es un dominio Euclidiano con la función* δ *dada por* $\delta(f(X)) := grad\ (f(X))$. *La propiedad i*) *se cumple porque:*

$$\begin{aligned} \delta(f(X)g(X)) = grad\ (f(X)g(X)) &= grad\ f(X) + grad\ g(X) \\ &\geq grad\ f(X) = \delta(f(X)), \end{aligned}$$

para todo $f(X),\ g(X) \in \mathbb{K}[X]$ *y la propiedad ii*) *es precisamente el Algoritmo de la División en* $\mathbb{K}[X]$.

En virtud de nuestro objetivo, probamos que:

Proposición 2.10. *Todo dominio Euclidiano es un DIP y por lo tanto un DFU.*

Demostración. Sea R un dominio Euclidiano con función δ. Dado un ideal no nulo $\mathfrak{a}$ de R, existe $c \in \mathfrak{a}$ no nulo, por lo tanto el conjunto $\{\delta(a) : a \in \mathfrak{a} \setminus \{0\}\} \subseteq \mathbb{N}$ es no vacío y por el Principio del Buen Orden, contiene un elemento minimal $\delta(b)$. Veamos que $\mathfrak{a} = \langle b \rangle$. De hecho, como $b \in \mathfrak{a}$ y $\mathfrak{a}$ es ideal, tenemos $\langle b \rangle \subseteq \mathfrak{a}$.
Por otra parte, si $a \in \mathfrak{a}$, por la propiedad *ii*) de la definición de dominio Euclidiano, existen $q,\ r \in R$ tales que $a = bq + r$, donde $r = 0$ ó $\delta(r) < \delta(b)$, pero $r = a - bq$ y $a,\ b \in \mathfrak{a}$, luego $r \in \mathfrak{a}$. Si $r \neq 0$, $\delta(r) < \delta(b)$ lo que contradice la minimalidad de $\delta(b)$. Así, $r = 0$ y $a = bq \in \langle b \rangle$, entonces $\mathfrak{a} \subseteq \langle b \rangle$. Por lo tanto $\mathfrak{a} = \langle b \rangle$ y R es un DIP. □

Para sacar provecho a este resultado, debemos encontrar cuerpos para los cuales el anillo de enteros sea Euclidiano. Estudiaremos esta propiedad en el anillo $I_{\mathbb{L}}$ de los enteros algebraicos de un cuerpo cuadrático $\mathbb{L} = \mathbb{Q}\left(\sqrt{d}\right)$.

Un candidato natural a ser la función δ es la norma absoluta, restricta a $I_{\mathbb{L}} \setminus \{0\}$, esto es, la función definida por:

$$\begin{aligned} \delta : I_{\mathbb{L}} \setminus \{0\} &\longrightarrow \mathbb{N} \\ \alpha &\longmapsto \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)\right|. \end{aligned} \tag{2.3}$$

Claramente esta función cumple la propiedad *i*) de la definición de dominio Euclidiano, pues para todo $\alpha, \beta \in I_{\mathbb{L}} \setminus \{0\}$,

$$\left|N_{\mathbb{L}|\mathbb{Q}}(\alpha\beta)\right| = \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)N_{\mathbb{L}|\mathbb{Q}}(\beta)\right| = \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)\right|\left|N_{\mathbb{L}|\mathbb{Q}}(\beta)\right| \geq \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)\right|,$$

donde la última desigualdad se cumple ya que $|N_{\mathbb{L}|\mathbb{Q}}(\beta)| \geq 1$.
Notemos que si $\alpha = m + n\sqrt{d}$ con $m, n \in \mathbb{Z}$ y $d \in \mathcal{D}$, entonces

$$\begin{aligned} \left|N_{\mathbb{L}|\mathbb{Q}}(\alpha)\right| = 0 &\iff N_{\mathbb{L}|\mathbb{Q}}(\alpha) = 0 \\ &\iff m^2 - n^2 d = 0 \\ &\iff m = n = 0 \\ &\iff \alpha = 0. \end{aligned}$$

La propiedad *ii*) solo se cumple en ciertos casos, como veremos a continuación.

Ejemplo 2.8. *El* **anillo de los enteros Gaussianos** $\mathbb{Z}[i]$ *es precisamente el anillo* $I_{\mathbb{L}}$ *de los enteros algebraicos del* **cuerpo de los números de Gauss** $\mathbb{L} = \mathbb{Q}(i)$*, donde* $i = \sqrt{-1}$*, es un dominio Euclidiano en relación a la norma* $N_{\mathbb{Q}(i)|\mathbb{Q}}(\alpha)$.

Demostración. Dados $\alpha,\ \beta \in \mathbb{Z}[i], \beta \neq 0$, entonces $\dfrac{\alpha}{\beta} \in \mathbb{C}$ y puede ser escrito en la forma $c + di$, con $c,\ d \in \mathbb{Q}$. Sea $k := [c] \in \mathbb{Z}$, la parte entera de c, entonces $k \leq c < k + 1$, es decir,

$$c \in [k, k+1) = \left[k, k + \frac{1}{2}\right] \cup \left[k + \frac{1}{2}, k + 1\right).$$

Luego, $c \in \left[k, k + \frac{1}{2}\right]$ o $c \in \left[k + \frac{1}{2}, k + 1\right)$. Si $c \in \left[k, k + \frac{1}{2}\right]$, $|k - c| \leq \frac{1}{2}$ y si $c \in \left[k + \frac{1}{2}, k + 1\right)$, $|t - c| < \frac{1}{2}$, con $t = k + 1 \in \mathbb{Z}$. En cualquier caso, para c y similarmente para d, existen $m,\ n \in \mathbb{Z}$

tales que $|m-c| \leq \frac{1}{2}$ y $|n-d| \leq \frac{1}{2}$. Además, como $\dfrac{\alpha}{\beta} = c + di$,

$$\begin{aligned}
\alpha &= \beta\,[c+di] \\
&= \beta\,[(c-m+m)+(d-n+n)i] \\
&= \beta\,[(m+ni)+((c-m)+(d-n)i)] \\
&= \beta\,[m+ni]+\beta\,[(c-m)+(d-n)i] \\
&= b\theta+\rho,
\end{aligned}$$

donde $\theta = m+ni \in \mathbb{Z}[i]$ y $\rho = \beta\,[(c-m)+(d-n)i] = \alpha - \beta\theta \in \mathbb{Z}[i]$ y

$$\begin{aligned}
N_{\mathbb{Q}(i)|\mathbb{Q}}(\rho) &= N_{\mathbb{Q}(i)|\mathbb{Q}}(\beta)N_{\mathbb{Q}(i)|\mathbb{Q}}\left((c-m)+(d-n)i\right) = N_{\mathbb{Q}(i)|\mathbb{Q}}(\beta)\left[(c-m)^2+(d-n)^2\right] \\
&\leq N_{\mathbb{Q}(i)|\mathbb{Q}}(\beta)\left[\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2\right] = \frac{1}{2}N_{\mathbb{Q}(i)|\mathbb{Q}}(\beta) < N_{\mathbb{Q}(i)|\mathbb{Q}}(\beta).
\end{aligned}$$

□

La Proposición 2.10 y el ejemplo anterior prueban que el dominio $\mathbb{Z}[i]$ de los enteros Gaussianos es un dominio de factorización única.

Análogamente podemos probar que $I_{\mathbb{Q}(\sqrt{d})}$ es Euclidiano, en relación a la norma, para $d \in \{-2,\ -3,\ -7,\ -11\}$ y estos, además de -1, son los únicos $d \in \mathcal{D}$ negativos con esta propiedad. En efecto, tenemos el siguiente resultado.

Teorema 2.11. *Sea $d \in \mathcal{D}$, $d < 0$. Entonces,*

- *el anillo de enteros algebraicos de $\mathbb{Q}\left(\sqrt{d}\right)$ es Euclidiano, si y solo si,*

$$d \in \{-1,\ -2,\ -3,\ -7,\ -11\}.$$

- *Para $d \in \mathcal{D}$, $d < -11$, el anillo de enteros algebraicos de $\mathbb{Q}\left(\sqrt{d}\right)$ no es Euclidiano.*

Demostración. Ver [8], página 92. □

Para los valores positivos de $d \in \mathcal{D}$, el proceso ha sido largo y ha involucrado a varios matemáticos. Dickson probó que $I_{\mathbb{Q}(\sqrt{d})}$ es Euclidiano en relación a la norma absoluta, esto

es, a la función definida en (2.3), para $d \in \{2,\ 3,\ 5,\ 13\}$. Perron añadió 6, 7, 11, 17, 21, 29 a esta lista y Oppenheimer, Remak y Rédei añadieron 19, 33, 37, 41, 55 y 73. Heilbronn probó en 1934 que la lista debía ser finita y finalmente, Chatland y Davenport en 1950 (y Inkeri en 1949, independientemente) terminaron el problema probando el siguiente teorema.

Teorema 2.12. *El anillo de enteros algebraicos de* $\mathbb{Q}\left(\sqrt{d}\right)$*, para* $d \in \mathcal{D}$ *positivo, es Euclidiano en relación a la norma absoluta, si y solo si,*

$$d \in \{2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73\}.$$

Demostración. Ver [2]. □

Sin embargo, no podemos afirmar que para los $d \in \mathcal{D}$ positivos que no están en esta lista $I_{\mathbb{Q}(\sqrt{d})}$ no sea un dominio Euclidiano con alguna función δ diferente a la norma absoluta. Por ejemplo, se puede verificar que para $d = 69$, $I_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ es un dominio Euclidiano con respecto a la función

$$\delta(a+b\omega) = \begin{cases} \left|a^2+ab-17b^2\right|, & \text{si } (a,b) \neq (10,3); \\ 26, & \text{si } (a,b) = (10,3); \end{cases}$$

donde $\omega = \frac{1+\sqrt{69}}{2}$. Ver [3].
Más aún, el número 26 puede ser reemplazado por cualquier entero mayor que 26, por lo que $\mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ es un dominio Euclidiano con respecto a infinitas funciones distintas.

Sabemos que para $I_{\mathbb{L}}$ ser un domino de factorización única es suficiente, más no necesario ser un dominio Euclidiano. De hecho, $\{-19,\ -43,\ -67,\ -163\}$ es el conjunto de los $d \in \mathcal{D}$ negativos tales que $I_{\mathbb{Q}(\sqrt{d})}$ es DFU, pero no Euclidiano ([1], Teorema 5.1). Existen también muchos $d \in \mathcal{D}$ positivos con esta propiedad, pero aún es un problema abierto determinar la existencia de infinitos números positivos $d \in \mathcal{D}$ tales que $I_{\mathbb{Q}(\sqrt{d})}$ es DFU (*Conjetura de Gauss*).

2.4. Aplicaciones de la factorización única

En esta sección aprovecharemos la factorización única del anillo de los enteros algebraicos de algunos cuerpos cuadráticos para resolver problemas de Teoría de Números. Algunos de ellos son casos particulares del Último Teorema de Fermat.
El siguiente lema nos será útil en la demostración de los teoremas posteriores.

Lema 2.13. *Sea R un DFU tal que cada elemento de $U(R)$ es un cubo. Si $a, b \in R$ son tales que $mcd(a, b) = 1$ y $ab = c^3$, para algún $c \in R$; entonces a y b son cubos.*

Demostración. Suponga que $c = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, donde p_i es irreducible para cada $i \in \{1, \cdots, n\}$, entonces

$$c^3 = p_1^{3\alpha_1} \cdots p_n^{3\alpha_n} = ab.$$

Como a y b son primos relativos, si p_i aparece en la factorización de a, entonces p_i no debe aparecer en la factorización de b. Sin pérdida de generalidad, podemos suponer que los irreducibles que dividen a a son $p_1, \cdots, p_k$ con $1 \leq k \leq n$. Si $k = n$, entonces $a = c^3$ y $b = 1$, luego el resultado es verdadero ya que las unidades son cubos. Si $k < n$,

$$a = p_1^{3\alpha_1} \cdots p_k^{3\alpha_k} = \left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right)^3 \quad \text{y} \quad b = p_{k+1}^{3\alpha_{k+1}} \cdots p_n^{3\alpha_n} = \left(p_{k+1}^{\alpha_{k+1}} \cdots p_n^{\alpha_n}\right)^3.$$

Por lo tanto, a y b son cubos.

□

Usando el hecho de que $\mathbb{Z}[i]$ es DFU se prueba el siguiente teorema:

Teorema 2.14. *La únicas soluciones enteras de la ecuación*

$$X^2 + 4 = Z^3 \tag{2.4}$$

$$\textit{son} \quad (X, Z) = (\pm 11, 5) \quad \textit{o} \quad (X, Z) = (\pm 2, 2).$$

Demostración. Supongamos primero que X es impar, y consideremos la siguiente factorización de la ecuación 2.4 en $\mathbb{Z}[i]$:

$$(2 + iX)(2 - iX) = Z^3.$$

Veamos que los dos factores de la izquierda son primos relativos. En efecto, si X y Z satisfacen la ecuación, un divisor común $\alpha := (a + ib)$ de $2 + iX$ y $2 - iX$ también divide a su suma, 4 y a su diferencia $2X$. Observe que $N_{\mathbb{L}|\mathbb{Q}}(\alpha) = a^2 + b^2$, $N_{\mathbb{L}|\mathbb{Q}}(4) = 16$ y $N_{\mathbb{L}|\mathbb{Q}}(2X) = 4X^2$ y por la multiplicidad de la norma tenemos que $a^2 + b^2 \mid 16$ y $a^2 + b^2 \mid 4X^2$, luego $a^2 + b^2 \mid 4$. Así, $(a, b) = (\pm 1, 0)$ o $(a, b) = (0, \pm 1)$ o $(a, b) = (\pm 1, \pm 1)$. En los casos $(a, b) = (\pm 1, 0)$ y $(a, b) = (0, \pm 1)$ obtenemos que α es una unidad; en los demás casos obtenemos que $N_{\mathbb{L}|\mathbb{Q}}(\alpha) = 2$ y por lo tanto α no dividiría a $2 + iX$ cuya norma es $4 + X^2$, impar.
En consecuencia, por el Lema 2.13, existen $c, d \in \mathbb{Z}$ tales que:

$$2 + iX = (c + id)^3 \text{ y conjugando,}$$
$$2 - iX = (c - id)^3 .$$

Sumando estas dos ecuaciones y dividiendo entre 2, tenemos que $2 = c\left(c^2 - 3d^2\right)$, luego $c \mid 2$, esto es $c = \pm 1$ o $c = \pm 2$. Claramente las únicas soluciones para c y d son $(c, d) = (-1, \pm 1)$ o $(c, d) = (2, \pm 1)$. Entonces:

$$Z^3 = ((c + id)(c - id))^3 = \left(c^2 + d^2\right)^3 .$$

Por lo tanto, $Z = c^2 + d^2 = 2,\ 5$ y $X = \pm 2,\ \pm 11$ respectivamente.
Nos falta ver el caso en que X es par. Supongamos que $X = 2x$, entonces Z también debe ser par, $Z = 2z$. Así la ecuación 2.4 nos queda

$$x^2 + 1 = 2z^3. \tag{2.5}$$

Lo que implica que x es impar. Factorizando 2.5 en $\mathbb{Z}[i]$ tenemos:

$$(1 + ix)(1 - ix) = 2z^3. \tag{2.6}$$

El máximo común divisor m de $1 - ix$ y $1 + ix$ divide también a su diferencia $2i = (1 + i)^2$. Como $1 + i$ es irreducible y $(1 + i)^2 \nmid 1 + ix$ (se sigue de que x es impar) entonces $m = 1 + i$.

Dividiendo cada miembro de la ecuación 2.6 entre $(1+i)^2$ obtenemos:

$$\left(\frac{1+ix}{1+i}\right)\left(\frac{1-ix}{1+i}\right) = -(iz)^3.$$

Donde los dos factores de la izquierda son primos relativos. De ese modo, cada uno de ellos debe ser un cubo, por el Lema 2.13. En particular $1+ix = (1+i)(r+is)^3$. Operando como antes, obtenemos que $1 = (r+s)\left(r^2 - 4rs + s^2\right)$, por lo tanto $(r,s) = (\pm 1, 0)$ o $(r,s) = (0, \pm 1)$. Lo que implica que $X = \pm 2$ y entonces $Z = 2$. □

Por el Algoritmo de la División, sabemos que los enteros primos impares se pueden clasificar en dos grupos; los de la forma $4n+1$ y los de la forma $4n+3$. Vamos a probar que todo primo del primer grupo puede escribirse como suma de dos cuadrados; este resultado fue propuesto por Fermat a Marin Mersenne en una carta fechada el 25 de diciembre de 1640, razón por la cual se le conoce también como Teorema de navidad de Fermat [1]. La prueba que mostramos a continuación se basa en la aritmética de los enteros gaussianos y fue dada por Dedekind.

Lema 2.15. *Sean p y c un enteros, con p primo y $mcd(p,c) = 1$. Si existen $x, y \in \mathbb{Z}$ tales que $cp = x^2 + y^2$, entonces*

$$p = a^2 + b^2,$$

para algunos $a, b \in \mathbb{Z}$.

Demostración. Supongamos que p es irreducible en $\mathbb{Z}[i]$, como

$$cp = x^2 + y^2 = (x+yi)(x-yi),$$

entonces $p \mid (x+yi)$ o $p \mid (x-yi)$; pero si $p \mid (x+yi)$, existe $u+vi \in \mathbb{Z}[i]$ tal que

$$x + yi = p(u+vi),$$

[1] Wikipedia, *Teorema de Fermat sobre la suma de dos cuadrados*. Disponible en: https://es.wikipedia.org/wiki/Teorema_de_Fermat_sobre_la_suma_de_dos_cuadrados

de ahí que $x = pu$ y $y = pv$, por lo tanto p también divide a $(x - yi)$; de ese modo

$$p^2 \mid (x + yi)(x - yi) = cp,$$

luego $p \mid c$, contradicción y lo mismo ocurre si $p \mid (x - yi)$.

Como p no es irreducible en $\mathbb{Z}[i]$, existen $a + bi,\ e + di \in \mathbb{Z}[i] \setminus U(\mathbb{Z}[i])$ tales que $p = (a + bi)(e + di)$ y conjugando se tiene que $p = (a - bi)(e - di)$, por lo tanto

$$\begin{aligned} p^2 &= (a + bi)(e + di)(a - bi)(e - di) \\ &= \left(a^2 + b^2\right)\left(e^2 + d^2\right). \end{aligned}$$

Entonces, $\left(a^2 + b^2\right) \mid p^2$ y como p es primo $\left(a^2 + b^2\right) \in \left\{1, p, p^2\right\}$, pero $\left(a^2 + b^2\right) \neq 1$ pues $(a + bi) \notin U(\mathbb{Z}[i])$ y si $\left(a^2 + b^2\right) = p^2$, entonces $\left(e^2 + d^2\right) = 1$, lo que contradice que $(e + di) \notin U(\mathbb{Z}[i])$, en consecuencia $a^2 + b^2 = p$. □

Lema 2.16. *Si p es un entero primo de la forma $4n + 1$, entonces la congruencia*

$$X^2 \equiv -1 \pmod{p}$$

tiene solución.

Demostración. Sea $X = 1 \cdot 2 \cdot 3 \cdots \dfrac{p-1}{2}$. Como $p - 1 = 4n$, en la factorización anterior de X hay un número par de términos, en consecuencia $X = (-1) \cdot (-2) \cdot (-3) \cdots \left(-\dfrac{p-1}{2}\right)$. Además $p - k \equiv -k \pmod{p}$ para todo $k \in \mathbb{Z}$, por lo tanto

$$\begin{aligned} X^2 &= \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right) \cdot (-1) \cdot (-2) \cdot (-3) \cdots \left(-\frac{p-1}{2}\right) \\ &\equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p-1}{2} \cdots (p-1) \\ &\equiv (p-1)! \equiv -1 \pmod{p}; \end{aligned}$$

donde la última congruencia se sigue del Teorema de Wilson. □

Teorema 2.17. ***(Fermat)*** *Si p es un entero primo de la forma $4n+1$, entonces*

$$p = a^2 + b^2,$$

para algunos $a, b \in \mathbb{Z}$.

Demostración. Por el Lema 2.16 existe x tal que $x^2 \equiv -1 \pmod{p}$. x puede ser escogido tal que $0 \leq x \leq p-1$, pues si $x \geq p$ tomamos el residuo que deja x al dividirse entre p. También podemos suponer que $x \leq \frac{p}{2}$, ya que si $x > \frac{p}{2}$, entonces $y = p - x$ satisface $y^2 \equiv -1 \pmod{p}$ y $y \leq \frac{p}{2}$. De ese modo, podemos asumir que existe $x \in \mathbb{Z}$ tal que $x \leq \frac{p}{2}$ y $x^2 + 1$ es múltiplo de p, digamos cp; luego

$$cp = x^2 + 1 \leq \frac{p^2}{4} + 1 < p^2,$$

por lo tanto $c < p$ y $p \nmid c$. Así, por el Lema 2.15 tenemos que $p = a^2 + b^2$ para algunos enteros a y b. □

Con la factorización única del anillo de enteros algebraicos de $\mathbb{Q}\left(\sqrt{-7}\right)$, Nagell probó el siguiente resultado conjeturado por Ramanujan.

Teorema 2.18. ***Teorema de Ramanujan-Nagell:***
La únicas soluciones de la ecuación $X^2 + 7 = 2^n$ en los enteros X y n son:

$\pm X$	1	3	5	11	181
n	3	4	5	7	15

.

Demostración. Ver [8], página 96. □

Con relación al Último Teorema de Fermat, se cree que el primer matemático que consiguió avanzar en su demostración fue el propio Pierre de Fermat, quien demostró el caso $n = 4$ usando la técnica del descenso infinito, una variante del principio de inducción. La importancia de este caso particular, radica en que partiendo de éste, se deduce que el teorema es cierto para todo n múltiplo de 4 y como un entero positivo $n > 2$ que no es múltiplo de 4 no es una potencia de 2. Entonces existe $p \neq 2$, primo tal que $n = pm$. Por tanto, para demostrar

que $X^n + Y^n = Z^n$ es imposible, si $XYZ \neq 0$ será suficiente demostrar que $X^p + Y^p = Z^p$ es imposible, si $XYZ \neq 0$. Luego, si p es un primo impar el Último Teorema de Fermat equivale a la no existencia de soluciones enteras no triviales de la ecuación

$$X^p + Y^p = Z^p.$$

En la prueba para $p = 3$, Euler consideró la factorización

$$X^3 + Y^3 = (X + Y)\left(X^2 - XY + Y^2\right),$$

mientras Direchlet y Legendre en sus pruebas para $p = 5$ consideraron

$$X^5 + Y^5 = (X + Y)\left(X^4 - X^3Y + X^2Y^2 - XY^3 + Y^4\right).$$

En ambos casos la estructura de las demostraciones es similar a la del Teorema 2.14. Sin embargo, es evidente que la complejidad del segundo factor aumenta a medida que p aumenta lo que hace que los casos de orden superior se vuelvan intratables.
En este contexto Lamé, dio un pasó adelante considerando el anillo de los enteros ciclotómicos

$$\mathbb{Z}[\omega] := \left\{a_{p-1}\omega^{p-1} + \cdots + a_1\omega + a_0 : a_i \in \mathbb{Z}, \text{ para } 0 \leq i \leq p-1\right\},$$

donde ω es una raíz $p-$ésima primitiva de la unidad. En efecto, sustituyendo X por X/Y y multiplicando por $-Y^p$ en

$$X^p + 1 = (X - 1)(X - \omega)\cdots(X - \omega^{p-1}),$$

obtenemos la siguiente factorización en $\mathbb{Z}[\omega]$:

$$X^p + Y^p = (X + Y)(X + \omega Y)\cdots(X + \omega^{p-1}Y).$$

Lamé conjeturó que si $\mathbb{Z}[\omega]$ tuviera factorización única sería posible generalizar los argu-

mentos de los casos que hemos comentado para obtener una prueba completa del teorema de Fermat, con la ventaja de trabajar con factores lineales.

Esta conjetura llamó la atención de muchos matemáticos de principios del siglo XIX, entre ellos Kummer, quien descubrió que los anillos de enteros ciclotómicos no siempre tienen factorización única, pero que la conjetura de Lamé era correcta. En el estudio de los enteros ciclotómicos, buscando contraejemplos de la factorización única; Kummer desarrolló una teoría que le permitía establecer un tipo de factorización única en estos anillos, para ello debió introducir la noción de divisores *'ideales'*.

Fue Dedekind quien a finales del siglo XIX formalizó la teoría de Kummer identificando sus divisores ideales con los ideales en el sentido usual de la teoría de anillos y probando que los resultados de Kummer son válidos en una clase muy general de anillos que estudiaremos en el siguiente capítulo.

Capítulo 3

Dominios de Dedekind

En el capítulo anterior vimos que en general, el anillo de los enteros de un cuerpo numérico no es un DFU. Sin embargo se tiene el resultado, un poco más débil, de que en éste anillo todo ideal propio se factoriza en forma única como producto de ideales primos. Para probar lo anterior, comenzamos introduciendo los conceptos de anillo noetheriano y dominio de Dedekind y estudiaremos algunas de sus caracterizaciones.

Definición 3.1. *Un anillo conmutativo R se dice* **noetheriano** *si satisface la condición de cadena ascendente (CCA) para ideales, esto es, si dada una cadena $\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \ldots \subseteq \mathfrak{i}_m \subseteq \ldots$ de ideales de R, entonces existe $n \in \mathbb{N}$ tal que $\mathfrak{i}_n = \mathfrak{i}_t$, para todo $t \geq n$.*

El nombre de anillo noetheriano se debe fundamentalmente al artículo *'Idealtheorie...'* [1] de Emmy Noether, allí aparecen por primera vez los conceptos modernos de anillo, ideal y módulo sobre un anillo, pero sin duda, el concepto que más se destaca en este artículo es el de la condición de cadena ascendente para ideales. Esta condición había sido previamente estudiada por Dedekind en 1894 y Lasker en 1905, pero la principal contribución de Noether fue definirla en un contexto abstracto y mostrar su importancia y naturalidad.

Ejemplo 3.1. *El anillo de los números enteros $\mathbb{Z}$ es noetheriano. De hecho, sea $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots \subseteq \langle a_m \rangle \subseteq \cdots$ es una cadena ascendente de ideales en $\mathbb{Z}$. Podemos asumir que $a_i > 0$ para todo $i \geq 1$, pues si $a_1 < 0$ tenemos que $\langle a_1 \rangle = \langle -a_1 \rangle$ y $-a_1 > 0$. Ahora, si $i \leq j$ tenemos que*

[1] E. Noether, *Idealtheorie in Ringbereichen, Math. Annalen 83* (1921), 24-66.

$a_i \in \langle a_j \rangle$. Así, $a_i = k_j a_j$, con $k_j \in \mathbb{Z}$, luego $a_j | a_i$ y $a_i \geq a_j$ para todo $i \leq j$. Si $a_i \neq a_j$ para todo $i \neq j$; $i, j \in \mathbb{N}$, entonces a_1 tendría infinitos divisores distintos, lo que es imposible. Por lo tanto, el conjunto $\{a_i\}_{i \geq 1}$ es finito y por el Principio del Buen Orden tiene mínimo, digamos a_n. De este modo, si $t \geq n$ tenemos que $a_n \leq a_t$ y como a_n es mínimo, $a_n = a_t$ y por lo tanto $\langle a_t \rangle = \langle a_n \rangle$, esto es, $\mathbb{Z}$ satisface CCA para ideales.

En 1890 Hilbert había probado [2] que todo ideal en el anillo de polinomios sobre el cuerpo de los números complejos $\mathbb{C}[X_1, \cdots, X_n]$ es finitamente generado. Noether demuestra que este resultado también es cierto para anillos noetherianos, es decir: Un anillo conmutativo R satisface la CCA para ideales si, y solamente si, todo ideal de R es finitamente generado. Otra forma familiar, equivalente a la CCA, es la condición de maximalidad por la que toda familia no vacía de ideales del anillo tiene un elemento maximal. El siguiente teorema nos muestra una caracterización de anillos noetherianos.

Teorema 3.1. *Sea R un anillo. Son equivalentes:*

1. *R es noetheriano.*

2. *R verifica la condición de maximalidad:*
   Sea $\mathcal{F}$ una familia no vacía de ideales de R, entonces $\mathcal{F}$ tiene un elemento maximal.

3. *Todo ideal de R es un R-módulo finitamente generado.*

Demostración.
$(1 \Rightarrow 2)$ Suponga que $\mathcal{F}$ es una familia no vacía de ideales de R que no contiene elemento maximal, entonces para cualquier $\mathfrak{i}_1 \in \mathcal{F}$, existe $\mathfrak{i}_2 \in \mathcal{F}$ tal que $\mathfrak{i}_1 \subsetneq \mathfrak{i}_2$. De esta manera podemos construir una cadena $\mathfrak{i}_1 \subsetneq \mathfrak{i}_2 \subsetneq \ldots \subsetneq \mathfrak{i}_m \subsetneq \ldots$ de ideales de R tal que $\mathfrak{i}_n \neq \mathfrak{i}_t$ para todo $n,\ t \in \mathbb{N}$, lo que contradice que R es noetheriano.

$(2 \Rightarrow 3)$ Sea $\mathfrak{i}$ un ideal de R, sabemos que $\mathfrak{i}$ es un $R-$módulo. Veamos que es finitamente generado. Sea $\mathcal{F} := \{\mathfrak{j} \subseteq \mathfrak{i} : \mathfrak{j} = \langle a_1, \cdots, a_m \rangle$ y $\mathfrak{j}$ es un ideal de $R\}$. $\mathcal{F}$ es no vacía (pues

[2] D. Hilbert, *Über die Theorie des algebraischen Formen, Math. Ann. 36* (1890), 471-534.

$\mathbf{0} \in \mathcal{F}$ y por hipótesis $\mathcal{F}$ tiene un elemento maximal $\mathfrak{m} = \langle a_1, \cdots, a_n \rangle$. Entonces, para todo $a \in \mathfrak{i}$ se tiene que $\langle a_1, \cdots, a_n, a \rangle \supseteq \langle a_1, \cdots, a_n \rangle = \mathfrak{m}$ y como este es maximal, se sigue que $\langle a_1, \cdots, a_n, a \rangle = \mathfrak{m}$, entonces $a \in \mathfrak{m}$ y por lo tanto $\mathfrak{i} = \mathfrak{m}$.

$(3 \Rightarrow 1)$ Sea $\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \ldots \subseteq \mathfrak{i}_m \subseteq \ldots$ una cadena ascendente de ideales de R. Denotemos por $\mathfrak{i} := \bigcup_{j \geq 1} \mathfrak{i}_j$ la unión de estos ideales, entonces $\mathfrak{i}$ es un ideal de R. Por hipótesis $\mathfrak{i}$ es finitamente generado, digamos $\mathfrak{i} = \langle a_1, \cdots, a_k \rangle$, donde notamos que para n suficientemente grande se tiene que $a_i \in \mathfrak{i}_n$, para todo $1 \leq i \leq k$ y por lo tanto $\mathfrak{i} \subseteq \mathfrak{i}_n$, es decir $\mathfrak{i}_n = \mathfrak{i}_t$, para todo $t \geq n$. $\square$

Ejemplo 3.2. *Sea $\mathbb{F}$ un cuerpo, entonces los únicos ideales de $\mathbb{F}$ son $\mathbf{0}$ y $\mathbb{F}$, que claramente son $\mathbb{F}-$módulos finitamente generados por 0 y 1 respectivamente, luego $\mathbb{F}$ es noetheriano. También, sabemos que los ideales de $\mathbb{L} := \mathbb{F}_1 \times \mathbb{F}_2 \times \cdots \times \mathbb{F}_n$ son de la forma $\mathfrak{j}_1 \times \mathfrak{j}_2 \times \cdots \times \mathfrak{j}_n$, donde $\mathfrak{j}_i$ es un ideal de $\mathbb{F}_i$ para cada $1 \leq i \leq n$. Por lo tanto, si los $\mathbb{F}_i$ son cuerpos, $\mathbb{L}$ tiene exactamente 2^n ideales y todos ellos son finitamente generados. De este modo, $\mathbb{L}$ es noetheriano.*

También se tiene que si R es un anillo noetheriano, $R[X]$ también es noetheriano, de donde, entonces el anillo de polinomios $R[X_1, \cdots, X_n]$ es noetheriano. Este resultado se conoce como el *Teorema de la base de Hilbert*.

Definición 3.2. *Un dominio R es de Dedekind si:*

i) *Es noetheriano.*

ii) *Es integralmente cerrado.*

iii) *Todo ideal primo no nulo es maximal.*

Ejemplo 3.3. *Si R es un DIP, entonces todo ideal de R es un $R-$módulo finitamente generado y por lo tanto R es noetheriano. También sabemos que todo DIP es DFU y R es integralmente cerrado por el Teorema 2.4. Además, en un DIP todo ideal primo no nulo es maximal. Entonces R es un dominio de Dedekind.*

El siguiente ejemplo nos muestra que la clase de dominios de Dedekind está contenida propiamente en la clase de anillos noetherianos.

Ejemplo 3.4. *Sea $\mathbb{F}$ un cuerpo. Los ideales principales $\langle X_1\rangle$ y $\langle X_2\rangle$ en el dominio polinomial $\mathbb{F}[X_1, X_2]$ son primos, pues X_1 y X_2 son irreducibles en $\mathbb{F}[X_1, X_2]$, pero no maximales ya que para $1 \leq i \leq 2$, tenemos*

$$\langle X_i\rangle \subsetneq \langle X_1, X_2\rangle \subsetneq \mathbb{F}[X_1, X_2].$$

En consecuencia $\mathbb{F}[X_1, X_2]$ es un anillo noetheriano que no es de Dedekind.

A continuación, probaremos un teorema que es clave para el desarrollo de los objetivos propuestos en este trabajo.

Teorema 3.2. *Sean R un dominio de Dedekind, $\mathbb{K} = Q(R)$, $\mathbb{L}$ una extensión finita y separable de $\mathbb{K}$ y $A = I_{\mathbb{L}}(R)$. Entonces A es un dominio de Dedekind.*

Para su demostración, necesitamos algunos resultados que probaremos en seguida.

Lema 3.3. *Sea R un dominio y $\mathbb{L}$ una extensión de $Q(R)$, entonces $Q(I_{\mathbb{L}}(R)) = I_{\mathbb{L}}(Q(R))$. En particular $Q(I_{\mathbb{L}}(R)) = \mathbb{L}$, si y solamente si, $\mathbb{L}$ es algebraica sobre $Q(R)$.*

Demostración. Para probar $Q(I_{\mathbb{L}}(R)) \subseteq I_{\mathbb{L}}(Q(R))$, mostraremos que $I_{\mathbb{L}}(Q(R))$ es un subcuerpo de $\mathbb{L}$ que contiene a $I_{\mathbb{L}}(R)$. Note primero que la contenencia $I_{\mathbb{L}}(Q(R)) \supseteq I_{\mathbb{L}}(R)$ es inmediata. Por lo tanto sólo mostraremos que $I_{\mathbb{L}}(Q(R))$ es cuerpo.
De hecho, si $\alpha, \beta \in I_{\mathbb{L}}(Q(R))$, entonces $\alpha - \beta \in I_{\mathbb{L}}(Q(R))$ y $\alpha\beta \in I_{\mathbb{L}}(Q(R))$.
Supongamos que $\beta \neq 0$, entonces existe $f(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} + X^n \in Q(R)[X]$ tal que $f(\beta) = 0$. Como $\beta \neq 0$, entonces existe $i = \min\left\{j \in \{1, \cdots, n-1\} : c_j \neq 0\right\}$ y así, $c_i\beta^i + c_{i+1}\beta^{i+1} + \cdots + \beta^n = 0$. Por lo tanto:

$$\beta^n\left(\frac{1}{\beta^{n-i}} + \frac{c_{i+1}}{c_i}\frac{1}{\beta^{n-(i+1)}} + \cdots + \frac{1}{c_i}\right) = 0.$$

Luego,

$$\left(\frac{1}{\beta}\right)^{n-i} + \frac{c_{i+1}}{c_i}\left(\frac{1}{\beta}\right)^{n-(i+1)} + \cdots + \frac{1}{c_i} = 0,$$

así, $\beta^{-1} \in I_{\mathbb{L}}(Q(R))$, de ese modo $I_{\mathbb{L}}(Q(R))$ es cuerpo.

Probemos que $Q(I_{\mathbb{L}}(R)) \supseteq I_{\mathbb{L}}(Q(R))$. Sea $\gamma \in I_{\mathbb{L}}(Q(R))$. Entonces existen $a_1, \cdots, a_n \in R$ y $b_1, \cdots, b_n \in R \setminus \{0\}$ tales que:

$$\gamma^n + \frac{a_1}{b_1}\gamma^{n-1} + \cdots + \frac{a_{n-1}}{b_{n-1}}\gamma + \frac{a_n}{b_n} = 0.$$

Sea $b = \prod_{i=1}^{n} b_i$, tenemos que $b \in R$ y $b\gamma^n + \theta_1\gamma^{n-1} + \cdots + \theta_{n-1}\gamma + \theta_n = 0$, donde $\theta_i := ba_ib_i^{-1} \in R$ para $1 \leq i \leq n$.

Multiplicando por b^{n-1}, se tiene que:

$$(b\gamma)^n + \theta_1(b\gamma)^{n-1} + \theta_2 b(b\gamma)^{n-2} + \cdots + \theta_n b^{n-1} = 0.$$

Así, si $h(X) = X^n + \theta_1 X^{n-1} + \theta_2 bX^{n-2} + \cdots + \theta_n b^{n-1} \in R[X]$, entonces $h(b\gamma) = 0$, luego $b\gamma = a \in I_{\mathbb{L}}(R)$ y como $b \in R \setminus \{0\}$, se tiene que $\gamma = \frac{a}{b} \in I_{\mathbb{L}}(Q(R))$. □

Lema 3.4. *Sean B y S subanillos de un cuerpo, con $B \subseteq S$, entonces $I_S(B) = I_S(I_S(B))$.*

Demostración. Sabemos que $B \subseteq I_S(B) \subseteq S$ y así, $I_S(B) \subseteq I_S(I_S(B)) \subseteq S$.

Sea $\alpha \in I_S(I_S(B))$, entonces existe $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in I_S(B)[X]$, tal que $f(\alpha) = 0$. De ese modo, α es entero sobre $S' = S[a_0, \cdots, a_{m-1}]$ y por lo tanto $S'[\alpha]$ es un $S'-$módulo finitamente generado. Sabemos que $a_i \in S'$ es entero sobre B, luego $S'[\alpha]$ es un $B-$módulo finitamente generado tal que $\alpha S'[\alpha] \subseteq S'[\alpha]$, de donde α es entero sobre B. □

- Sean R, A, $\mathbb{K}$, $\mathbb{L}$ como en el Teorema 3.2, entonces A es integralmente cerrado.

  De hecho, como $\mathbb{L}$ es extensión finita de $\mathbb{K}$, $\mathbb{L}$ es algebraica y por el Lema 3.3 $Q(A) = Q(I_{\mathbb{L}}(R)) = \mathbb{L}$, entonces

  $$I_{Q(A)}(A) = I_{\mathbb{L}}(A) = I_{\mathbb{L}}(I_{\mathbb{L}}(R)) = I_{\mathbb{L}}(R) = A,$$

  donde la penúltima igualdad es consecuencia del Lema 3.4

Lema 3.5. *Sean B y S dominios tales que $B \subseteq S$ y S es entero sobre B. Entonces:*

1. *Si* $\mathfrak{u}$ *es un ideal no nulo de* S, $\mathfrak{u} \cap B$, *es un ideal no nulo de* B.

2. $U(S) \cap B = U(B)$.

3. S *es un cuerpo, si y solo si,* B *es un cuerpo.*

4. *Un ideal primo* $\mathfrak{p}$ *de* S *es maximal en* S, *si y solo si,* $\mathfrak{p} \cap B$, *es maximal en* B.

Demostración.

1. Sea $\alpha \in \mathfrak{u}$ no nulo, tenemos que $\alpha \in S = I_S(B)$, pues S es entero sobre B, así, existe $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in B[X]$ de grado mínimo, tal que $f(\alpha) = 0$. Entonces,

$$a_0 = -\alpha\left(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1\right).$$

   Si $a_0 = 0$ entonces $\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1 = 0$ y así, $g(X) = X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_1 \in B[X]$ sería tal que $g(\alpha) = 0$, lo que contradice que $f(X)$ es el polinomio de grado mínimo con esta propiedad. Así a_0 es no nulo y observe que $a_0 \in \mathfrak{u} \cap B$. Luego $\mathfrak{u} \cap B$ es un ideal no nulo de B.

2. Es claro que $U(B) \subseteq U(S) \cap B$. Sea $\alpha \in U(S) \cap B$. Entonces $\alpha^{-1} \in S = I_S(B)$ y existen $c_1, c_2, \cdots, c_m \in B$ tales que $\alpha^{-m} + c_1\alpha^{-m+1} + \cdots + c_m = 0$. Multiplicando por α^{m-1} se tiene que $\alpha^{-1} + c_1 + c_2\alpha + \cdots + c_m\alpha^{m-1} = 0$ y por lo tanto

$$\alpha^{-1} = -\left(c_1 + c_2\alpha + \cdots + c_m\alpha^{m-1}\right) \in B.$$

3. Si S es cuerpo, entonces $U(B) = U(S) \cap B = (S \setminus \{0\}) \cap B = B \setminus \{0\}$ y así, B es cuerpo.

   Recíprocamente, supongamos que S no es cuerpo, entonces existe $\mathfrak{u}$ ideal no nulo de S tal que $\mathfrak{u} \neq S$, luego $1 \notin \mathfrak{u}$. Por el ítem 1, $\mathfrak{u} \cap B$ es un ideal no nulo de B y como $\mathfrak{u} \cap B \neq B$, B no es cuerpo.

4. Sea $\mathfrak{p}$ un ideal primo de S. Consideremos $\pi : S \to S/\mathfrak{p}$ la proyección canónica, vamos a probar que $\pi(S) = S/\mathfrak{p}$ es entero sobre $\pi(B)$, esto es, $I_{\pi(S)}(\pi(B)) = \pi(S)$. De hecho, si $\overline{\gamma} \in \pi(S)$, entonces $\overline{\gamma} = \pi(\gamma)$ para algún $\gamma \in S = I_S(B)$, entonces existe

$h(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in B[X]$ tal que $h(\gamma) = 0$. Consideremos ahora $\overline{h}(X) = X^n + \pi(a_{n-1})X^{n-1} + \cdots + \pi(a_0) \in \pi(B)[X]$, entonces $\overline{h}(\overline{\gamma}) = \overline{0}$, y $\overline{\gamma}$ es entero sobre $\pi(B)$.

Como Ker $\pi = \mathfrak{p}$ entonces la restricción de π a B tiene como kernel $\mathfrak{p} \cap B$, así por el Primer Teorema del Isomorfismo tenemos que $B/(B \cap \mathfrak{p}) \cong \pi(B)$.

Ahora, $\mathfrak{p}$ es maximal en S, si y solo si, $S/\mathfrak{p}$ es un cuerpo, lo que por la parte 3 ocurre, si y solo si, $B/(B \cap \mathfrak{p})$ es un cuerpo, lo que equivale a decir que $B \cap \mathfrak{p}$ es maximal en B.

□

- Sean R, A, $\mathbb{K}$, $\mathbb{L}$ como en el Teorema 3.2, vamos a probar que todo ideal primo no nulo de A es maximal.

  De hecho, si $\mathfrak{p}$ es un ideal primo no nulo de A, entonces, por el ítem 1 del lema anterior, $\mathfrak{p} \cap R$ es un ideal primo no nulo de R. Como R es dominio de Dedekind, $\mathfrak{p} \cap R$ es un ideal maximal de R. Luego por el ítem 4, el ideal $\mathfrak{p}$ de A es maximal.

Lema 3.6. *Sea R un dominio entero y θ un elemento algebraico sobre su cuerpo de fracciones. Entonces existe $b \in R$ no nulo tal que $b\theta$ es entero sobre R.*

Demostración. Por hipótesis, θ es raíz de un polinomio con coeficientes en $Q(R)$ y podemos suponer que este polinomio es mónico pues $Q(R)$ es un cuerpo. Así, existen $a_1, \cdots, a_n \in R$ y $b_1, \cdots, b_n \in R \setminus \{0\}$ tales que:

$$\theta^n + \frac{a_1}{b_1}\theta^{n-1} + \cdots + \frac{a_{n-1}}{b_{n-1}}\theta + \frac{a_n}{b_n} = 0.$$

Sea $b = \prod_{i=1}^{n} b_i \in R \setminus \{0\}$. Multiplicando por b^n la igualdad anterior, queda

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

donde $c_i = b^i a_i b_i^{-1} \in R$ para $i \in \{1, \cdots, n\}$. Luego $b\theta$ es entero sobre R. □

Observación 3.1. Sea $\mathbb{L}$ una extensión separable de $\mathbb{K} = Q(R)$ de grado n. Si $\{w_1, \cdots, w_n\}$ es una base de $\mathbb{L}|\mathbb{K}$, por el Lema 3.6 podemos suponer que cada w_i entero sobre R, ya que cada uno de ellos es algebraico sobre $\mathbb{K}$.

Para demostrar el Teorema 3.2 solo falta probar el siguiente lema:

Lema 3.7. *A es noetheriano.*

Demostración. Basta probar que A está contenido en un $R-$módulo finitamente generado, pues tal módulo será noetheriano y en consecuencia todo ideal de A es un submódulo de un módulo noetheriano, por lo tanto será finitamente generado.
Sean $\mathcal{B} = \{w_1, \cdots, w_n\}$ una base de $\mathbb{L}|\mathbb{K}$, tal que cada $w_i \in A$ y $T := T_{\mathbb{L}|\mathbb{K}}$ la traza inducida por esta extensión. La matriz $\left[T(w_i w_j)\right]$ tiene determinante no nulo, pues en caso contrario las columnas serían linealmente dependientes, es decir, existirían elementos $a_1, \cdots, a_n \in \mathbb{K}$ no todos nulos tales que:

$$0 = \sum_{j=1}^{n} a_j T(w_i w_j) = T\left(w_i \sum_{j=1}^{n} a_j w_j\right), \quad \text{para cada } 1 \leq i \leq n.$$

Si $\beta = \sum_{j=1}^{n} a_j w_j$, entonces $T(w_i\beta) = 0$ para cada $1 \leq i \leq n$.

Sea $\alpha \in \mathbb{L}$ entonces $\alpha\beta^{-1} = \sum_{j=1}^{n} d_j w_j$ para algunos $d_j \in \mathbb{K}$, luego

$$T(\alpha) = T\left(\sum_{j=1}^{n} d_j w_j \beta\right) = \sum_{j=1}^{n} d_j T(w_j\beta) = 0,$$

Por lo tanto $T = 0$ y como $\mathbb{L}$ es separable $T = \sum_{i=1}^{n} \sigma_i = 0$, donde los σ_i son los $\mathbb{K}-$homomorfismos de $\mathbb{L}$ en $\overline{\mathbb{K}}$. Pero esto es imposible ya que por el Lema de Dedekind, el conjunto $\{\sigma_i : 1 \leq i \leq n\}$ es linealmente independiente cuando $\mathbb{L}$ es separable sobre $\mathbb{K}$. En consecuencia la aplicación:

$$\begin{aligned} \phi : \mathbb{L} &\longrightarrow \mathbb{L}^* \\ x &\longmapsto \phi_x : \mathbb{L} \longrightarrow \mathbb{K} \\ &\qquad\quad y \longmapsto T(xy) \end{aligned}$$

es un isomorfismo de $\mathbb{L}$ en su espacio dual. En efecto, es claro que ϕ es un homomorfismo ya que T lo es. Así, basta probar que ϕ es un monomorfismo es decir, que $[\phi(w_i)]$, la matriz asociada a ϕ es invertible. Pero notemos que la matriz $[\phi(w_i)]_{\mathcal{B}}$ es precisamente $\left[T(w_i w_j)\right]$ y concluimos que ϕ es un isomorfismo.

Sea ahora $\mathcal{B}^* = \left\{w_1^*, \cdots, w_n^*\right\}$ la base dual de $\mathcal{B}$, entonces $\left\{w_1', \cdots, w_n'\right\}$ es una base de $\mathbb{L}|\mathbb{K}$, donde $\phi(w_i') = w_i^*$, como

$$w_i^*(w_j) = \begin{cases} 1, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

Tenemos:

$$T(w_i' w_j) = \phi(w_i')(w_j) = w_i^*(w_j) = \begin{cases} 1, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

Sabemos que para cada w_i' existe $c_i \in R \setminus \{0\}$ tal que $c_i w_i'$ es entero sobre R. Considerando $c = \prod_{j=1}^{n} c_j \in R \setminus \{0\}$ concluimos que cw_i' es entero sobre R. Sea $z \in A$, entonces $zcw_i' \in A$. Luego $T(zcw_i') = cT(zw_i') \in R$. Ahora, como $z \in \mathbb{L}$, podemos escribir $z = \sum_{j=1}^{n} y_j w_j$, con $y_j \in \mathbb{K}$, así

$$T(zw_i') = T\left(\sum_{j=1}^{n} y_j w_j w_i'\right) = \sum_{j=1}^{n} y_j T(w_j w_i') = y_i.$$

Consecuentemente $cy_i \in R$ por lo tanto:

$$z = \sum_{j=1}^{n} (y_j c)(c^{-1} w_j) \in R(c^{-1} w_1) + \cdots + R(c^{-1} w_n).$$

Luego A está contenido en un $R-$módulo finitamente generado. □

3.1. Factorización de Ideales

En el anillo $\mathbb{Z}$ todo ideal es principal y por el Teorema Fundamental de la Aritmética todo ideal propio lo podemos expresar de manera única como producto de ideales primos. Sin embargo, en general, aún en el caso noetheriano, no cabe esperar dicha descomposición de ideales. Veremos que ser de Dedekind es condición suficiente (y necesaria) para que en un anillo sea válida esta descomposición. Para esto, necesitaremos previamente generalizar la noción de ideal.

Un conjunto de la forma $\frac{a}{b}\mathbb{Z}$, con $a, b \in \mathbb{Z}$; $b \notin \{0, \pm 1\}$ y $\text{mcd}(a, b) = 1$ no es un ideal de $\mathbb{Z}$, pues $\frac{a}{b} \notin \mathbb{Z}$, aunque se comporta de manera similar. El conjunto resulta cerrado bajo la suma y producto por un entero, además, basta multiplicar cada uno de sus elementos por b para que se convierta en un ideal de $\mathbb{Z}$. Conjuntos con esta característica nos serán útiles en este capítulo.

Nota: En adelante $\mathbb{K} = Q(R)$ denotará el cuerpo de fracciones del dominio entero R.

Definición 3.3. *Sea $\mathfrak{m} \subseteq \mathbb{K}$ un $R-$módulo. Diremos que $\mathfrak{m}$ es un* **ideal fraccionario** *de R, si existe $a \in R$ no nulo tal que $a\mathfrak{m} \subseteq R$.*

En este caso es fácil ver que $a\mathfrak{m}$ es un ideal de R y claramente los ideales de R son ideales fraccionarios.

Ejemplo 3.5. *Todo $R-$submódulo I no nulo de $\mathbb{K}$ finitamente generado es un ideal fraccionario de R. De hecho, si I está generado por $b_1, \cdots, b_n \in \mathbb{K}$, entonces $I = Rb_1 + \cdots + Rb_n$ y para cada $1 \leq i \leq n$, $b_i = \frac{c_1}{a_i}$, con $a_i, c_i \in R$ y $a_i \neq 0$. Sea $a = \prod_{i=1}^{n} a_i$, luego $a \neq 0$ y $aI = Ra_2 \cdots a_n c_1 + \cdots + Ra_1 \cdots a_{n-1} c_n \subset R$.*

Ejemplo 3.6. *Sea R un DIP, entonces para $q \in \mathbb{K}$, $\mathfrak{m} = qR$, es un ideal fraccionario de R, pues si $q = \frac{m}{n}$ con $m,\ n \in R$ y $n \neq 0$, entonces $n\mathfrak{m} = mR \subseteq R$. Ahora, si $\mathfrak{m}$ es un ideal fraccionario de R, existe $a \in R$ no nulo tal que $a\mathfrak{m}$ es un ideal en R y como todo ideal en R es principal, entonces $a\mathfrak{m} = bR$ para algún $b \in R$. Así $\mathfrak{m} = sR$, donde $s = \frac{a}{b}$.*

Proposición 3.8. ***Propiedades***

Sean $\mathfrak{m}, \mathfrak{n}$ *ideales fraccionarios de R, entonces:*

1. $\mathfrak{mn} := \left\{ \sum_{i=1}^{k} m_i n_i : k \in \mathbb{N},\ m_i \in \mathfrak{m},\ y\ n_i \in \mathfrak{n} \right\}$ *es un ideal fraccionario de R.*
2. $\mathfrak{m}R = \mathfrak{m}$.

Demostración.

1. Como $\mathfrak{m}$ y $\mathfrak{n}$ son ideales fraccionarios de R, existen $r, q \in R$ tales que $r\mathfrak{m} \subseteq R$ y $q\mathfrak{n} \subseteq R$. Veamos que $(rq)\mathfrak{mn} \subseteq R$, en efecto, si $x \in (rq)\mathfrak{mn}$, $x = (rq)\sum_{i=1}^{k} m_i n_i$, para algún $k \in \mathbb{N}$ y $m_i \in \mathfrak{m},\ n_i \in \mathfrak{n}$ con $1 \leq i \leq k$, entonces

$$x = \sum_{i=1}^{k} (rq) m_i n_i = \sum_{i=1}^{k} (rm_i)(qn_i),$$

   donde $rm_i,\ qn_i \in R$ para cada $1 \leq i \leq k$. Luego $x \in R$.

2. Observe que $\mathfrak{m}R \supseteq \mathfrak{m}$, ya que $m = m \cdot 1$ para cada $m \in \mathfrak{m}$. Además si $x \in \mathfrak{m}R$, $x = \sum_{i=1}^{k} m_i r_i$ para algún $k \in \mathbb{N}$ y $m_i \in \mathfrak{m},\ r_i \in R$ con $1 \leq i \leq k$, pero $\mathfrak{m}$ es ideal fraccionario de R, entonces $\mathfrak{m}$ es un $R-$módulo y así $m_i r_i \in \mathfrak{m}$ para cada $1 \leq i \leq k$. Por lo tanto $x \in \mathfrak{m}$ y $\mathfrak{m}R \subseteq \mathfrak{m}$.

□

Definición 3.4. *Sea R un anillo. Un ideal fraccionario* $\mathfrak{n}$ *de R es* **invertible** *si existe* $\mathfrak{m}$*, ideal fraccionario de R tal que* $\mathfrak{nm} = \mathfrak{mn} = R$*. En tal caso,* $\mathfrak{m}$ *se llama el inverso de* $\mathfrak{n}$ *y se lo denota por* $\mathfrak{n}^{-1}$.

Los ideales fraccionarios tienen un papel importante en la caracterización de los dominios de Dedekind. El siguiente resultado desarrolla algunas de sus propiedades.

Teorema 3.9. *Sea R un dominio de Dedekind. Entonces los ideales fraccionarios de R forman un grupo con la multiplicación definida en 1 de la Proposición 3.8.*

Para demostrar el teorema anterior, probaremos primero algunos lemas.

Nota: En lo sucesivo R denotará un dominio de Dedekind a menos que se indique otra cosa y cuando hablemos de ideales primos se entenderá que nos referimos a ideales primos no nulos.

Lema 3.10. *Sea* $\mathfrak{i}$ *un ideal no nulo de* R*. Existen ideales primos* $\mathfrak{p}_1,\ \mathfrak{p}_2, \cdots, \mathfrak{p}_r$*, tales que* $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{i}$.

Demostración. Supongamos que la familia $\mathcal{F}$ de los ideales de R que no cumplen esta propiedad es no vacía. Como R es noetheriano, $\mathcal{F}$ tiene un elemento maximal $\mathfrak{j}$, y es claro que $\mathfrak{j}$ no es primo; por lo tanto, existen $a_1,\ a_2 \in R$, tales que $a_1a_2 \in \mathfrak{j}$, $a_1 \notin \mathfrak{j}$ y $a_2 \notin \mathfrak{j}$. Consideremos $\mathfrak{j}_1 = \langle \mathfrak{j}, a_1 \rangle$ (el ideal generado por $\mathfrak{j}$ y a_1) y $\mathfrak{j}_2 = \langle \mathfrak{j}, a_2 \rangle$, tenemos que $\mathfrak{j} \subsetneq \mathfrak{j}_1$ y $\mathfrak{j} \subsetneq \mathfrak{j}_2$. Como $\mathfrak{j}$ es maximal, $\mathfrak{j}_1 \notin \mathcal{F}$ y $\mathfrak{j}_2 \notin \mathcal{F}$. Así, existen ideales primos $\mathfrak{B}_1,\ \mathfrak{B}_2, \cdots, \mathfrak{B}_r$, y $\mathfrak{Q}_1,\ \mathfrak{Q}_2, \cdots, \mathfrak{Q}_s$, tales que $\mathfrak{B}_1 \cdot \mathfrak{B}_2 \cdot \ldots \cdot \mathfrak{B}_r \subseteq \mathfrak{j}_1$ y $\mathfrak{Q}_1 \cdot \mathfrak{Q}_2 \cdot \ldots \cdot \mathfrak{Q}_s \subseteq \mathfrak{j}_2$. Observe que si $x \in \mathfrak{j}_1\mathfrak{j}_2$, $x = \sum_{i=1}^{k} b_ic_i$, con $k \in \mathbb{N}$, $b_i \in \mathfrak{j}_1$ y $c_i \in \mathfrak{j}_2$, luego $b_i = j_i + a_1r_i$ y $c_i = j_i' + a_2r_i'$, con $j_i, j_i' \in \mathfrak{j}$ y $r_i, r_i' \in R$, así $b_ic_i = j_ij_i' + j_ia_2r_i' + a_1r_ij_i' + a_1a_2r_ir_i' \in \mathfrak{j}$, para $i \in \{1, \cdots, k\}$, por lo tanto $x \in \mathfrak{j}$. De este modo, $\mathfrak{j}_1\mathfrak{j}_2 \subseteq \mathfrak{j}$, entonces $\mathfrak{B}_1 \cdot \ldots \cdot \mathfrak{B}_r \cdot \mathfrak{Q}_1 \cdot \ldots \cdot \mathfrak{Q}_s \subseteq \mathfrak{j}$ lo que es una contradicción. Por lo tanto $\mathcal{F}$ es vacía. □

Lema 3.11. *Sea* $\mathfrak{p}$ *un ideal maximal de* R*, entonces existe un ideal fraccionario* $\mathfrak{n}$ *de* R*, tal que* $\mathfrak{p}\mathfrak{n} = R$.

Demostración. Sea $\mathbb{K} = Q(R)$ y $\mathfrak{n} := \{x \in \mathbb{K} : x\mathfrak{p} \subseteq R\}$. Entonces $\mathfrak{n}$ es un $R-$submódulo de $\mathbb{K}$ y, para $p \in \mathfrak{p}$, $p\mathfrak{n} \subseteq R$. Luego $\mathfrak{n}$ es un ideal fraccionario de R. Veamos que $\mathfrak{p}\mathfrak{n} = R$.
En efecto, sabemos que

$$\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{n} \subseteq R$$

y como $\mathfrak{p}$ es maximal, tenemos que $\mathfrak{p} = \mathfrak{p}\mathfrak{n}$ ó $\mathfrak{p}\mathfrak{n} = R$.
Supongamos que $\mathfrak{p} = \mathfrak{p}\mathfrak{n}$, entonces para cada $\alpha \in \mathfrak{n}$, $\alpha\mathfrak{p} \subseteq \mathfrak{p}$ y como R es noetheriano $\mathfrak{p}$ es un $R-$módulo finitamente generado, luego por el Teorema 2.1, α es un entero sobre R, y por lo tanto $\mathfrak{n} \subseteq I_{\mathbb{K}}(R) = R$, pero observe que $R \subseteq \mathfrak{n}$, entonces $R = \mathfrak{n}$. Veamos que $R \neq \mathfrak{n}$.

De hecho, considerando $a \in \mathfrak{p}$ no nulo, por el Lema 3.10 existe $r \in \mathbb{N}$ mínimo e ideales primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$, tales que $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \langle a \rangle \subseteq \mathfrak{p}$.

Si $r = 1$, entonces $\mathfrak{p}_1 \subseteq \langle a \rangle$, más como $\mathfrak{p}_1$ es maximal en R, tenemos que $\langle a \rangle = R$ ó $\mathfrak{p}_1 = \langle a \rangle$. Si $\langle a \rangle = R$, como $\langle a \rangle \subseteq \mathfrak{p} \subseteq R$, entonces $\mathfrak{p} = R$, lo que contradice que $\mathfrak{p}$ es maximal; si $\mathfrak{p}_1 = \langle a \rangle$, en particular se tiene que $a \in \mathfrak{p}_1$, luego $\mathfrak{p} \subseteq \mathfrak{p}_1$, así $\mathfrak{p} = \mathfrak{p}_1 = \langle a \rangle$ y $\mathfrak{m} = a^{-1}R$ es tal que $\mathfrak{m}\mathfrak{p} = R$. Observe que $a^{-1} = a^{-1} \cdot 1 \in \mathfrak{m}$, luego $a^{-1}\mathfrak{p} \subseteq \mathfrak{m}\mathfrak{p} = R$, entonces $a^{-1} \in \mathfrak{n} = R$ y $aa^{-1} = 1 \in \mathfrak{p}$, en consecuencia $\mathfrak{p} = R$, contradicción.

Supongamos que $r \geq 2$. Como $\mathfrak{p}$ es maximal (primo), alguno de los $\mathfrak{p}_i$, digamos $\mathfrak{p}_1$, está contenido en $\mathfrak{p}$, luego $\mathfrak{p}_1 = \mathfrak{p}$. Además como r es mínimo, se tiene que $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \nsubseteq \langle a \rangle$, así existe $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$ y $b \notin \langle a \rangle$. Por lo tanto, $b\mathfrak{p} \subseteq \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \langle a \rangle = aR$. Así, $ba^{-1}\mathfrak{p} \subseteq R$ y $ba^{-1} \in \mathfrak{n}$, más $b \notin \langle a \rangle$ y de ese modo $ba^{-1} \notin R$, de lo que se concluye que $\mathfrak{n} \neq R$. En consecuencia $\mathfrak{p} \neq \mathfrak{p}\mathfrak{n}$ y por lo tanto $\mathfrak{p}\mathfrak{n} = R$. □

Lema 3.12. *Todo ideal no nulo de R es el inverso de un ideal fraccionario de R.*

Demostración. Supongamos que la familia $\mathcal{F}$ de ideales de R que no cumplen la condición es no vacía, entonces $\mathcal{F}$ tiene un elemento maximal $\mathfrak{u}$. Por el Lema 3.11 $\mathfrak{u}$ no es maximal en R. Así, existe $\mathfrak{p}$, ideal maximal de R tal que $\mathfrak{u} \subsetneq \mathfrak{p}$, entonces

$$\mathfrak{m}_1 := \{x \in \mathbb{K} : x\mathfrak{p} \subseteq R\} \subseteq \mathfrak{m}_2 := \{x \in \mathbb{K} : x\mathfrak{u} \subseteq R\},$$

y $\mathfrak{u} \subseteq \mathfrak{u}\mathfrak{m}_1 \subseteq \mathfrak{u}\mathfrak{m}_2 \subseteq R$. Por lo tanto $\mathfrak{u}\mathfrak{m}_1$ es un ideal de R. Veamos que $\mathfrak{u} \subsetneq \mathfrak{u}\mathfrak{m}_1$.

De hecho, si $\mathfrak{u} = \mathfrak{u}\mathfrak{m}_1$, entonces cada $\alpha \in \mathfrak{m}_1$ es algebraico sobre R y así $\mathfrak{m}_1 \subseteq I_{\mathbb{K}}(R) = R$ y como $R \subseteq \mathfrak{m}_1$, entonces $\mathfrak{m}_1 = R$, pero como $\mathfrak{p}$ es maximal, en la prueba del Lema 3.11 mostramos que $\mathfrak{m}_1 \neq R$, luego $\mathfrak{u} \subsetneq \mathfrak{u}\mathfrak{m}_1$, así $\mathfrak{u}\mathfrak{m}_1 \notin \mathcal{F}$, por lo tanto existe $\mathfrak{j}$, ideal fraccionario de R tal que $(\mathfrak{u}\mathfrak{m}_1)\mathfrak{j} = R$. Luego $\mathfrak{m}_1\mathfrak{j}$ es el inverso de $\mathfrak{u}$, por lo tanto $\mathfrak{u} \notin \mathcal{F}$, contradicción. □

Lema 3.13. *Sea* $\mathfrak{i}$ *un ideal no nulo de R y* $\mathfrak{n}$ *un ideal fraccionario de R tal que* $\mathfrak{i}\mathfrak{n} = R$, *entonces* $\mathfrak{n} = \{x \in \mathbb{K} : x\mathfrak{i} \subseteq R\}$.

Demostración. Si $x \in \mathfrak{n}$, $x \in \mathbb{K}$ y $x\mathfrak{i} \subseteq \mathfrak{n}\mathfrak{i} = R$, luego $\mathfrak{n} \subseteq \{x \in \mathbb{K} : x\mathfrak{i} \subseteq R\}$. Por otra parte, si $x \in \mathbb{K}$ y $x\mathfrak{i} \subseteq R$, entonces $xR = x\mathfrak{n}\mathfrak{i} \subseteq R\mathfrak{n} = \mathfrak{n}$, donde la última igualdad se verifica por la

propiedad 2 de la Proposición 3.8. Así, $xR \subseteq \mathfrak{n}$ y $x = x \cdot 1 \in \mathfrak{n}$, luego $\mathfrak{n} \supseteq \{x \in \mathbb{K} : x\mathfrak{i} \subseteq R\}$. Por lo tanto $\mathfrak{n} = \{x \in \mathbb{K} : x\mathfrak{i} \subseteq R\}$. □

Lema 3.14. *Sea $\mathfrak{m}$ un ideal fraccionario no nulo de R, entonces existe $\mathfrak{n}$ ideal fraccionario de R tal que $\mathfrak{mn} = R$.*

Demostración. Como $\mathfrak{m}$ es un ideal fraccionario de R, existe $x \in R$ tal que $x\mathfrak{m} \subseteq R$. Además como $x\mathfrak{m}$ es un ideal de R, entonces por el Lema 3.12, existe $\mathfrak{j}$ ideal fraccionario de R tal que $x\mathfrak{m}\mathfrak{j} = R$. Observe que $\mathfrak{n} = x\mathfrak{j}$ es un ideal fraccionario de R tal que $\mathfrak{mn} = R$ lo que prueba el lema. □

Ya tenemos las herramientas suficientes para mostrar el Teorema 3.9.

Demostración. (Del Teorema 3.9)
La clausura de la operación se verifica por la propiedad 1 de la Proposición 3.8 y por el Lema 3.14 obtenemos que todo ideal fraccionario de R es invertible. Por lo tanto el conjunto formado por los ideales fraccionarios de R es un grupo multiplicativo con elemento neutro R (Propiedad 2 de la Proposición 3.8). □

Teorema 3.15. *Si R es un dominio de Dedekind, entonces todo ideal propio de R puede ser escrito de manera única como producto de ideales primos.*

Demostración. Sea $\mathcal{F}$ la familia de ideales de R que no pueden ser escritos como producto de primos y supongamos que $\mathcal{F}$ es no vacía, entonces $\mathcal{F}$ tiene un elemento maximal $\mathfrak{i}$, luego $\mathfrak{i}$ no es primo y por lo tanto no es maximal en R; así, existe $\mathfrak{p}$ ideal maximal de R tal que $\mathfrak{i} \subsetneq \mathfrak{p}$ y de ese modo $\mathfrak{i}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$; luego $\mathfrak{i}\mathfrak{p}^{-1}$ es un ideal de R.
Si $\mathfrak{i}\mathfrak{p}^{-1} = \mathfrak{i}$, para todo $\alpha \in \mathfrak{p}^{-1}$, $\alpha\mathfrak{i} \subseteq \mathfrak{i}$ y como $\mathfrak{i}$ es un $R-$módulo finitamente generado, tenemos que $\alpha \in I_{\mathbb{K}}(R) = R$; de ese modo $\mathfrak{p}^{-1} \subseteq R$; pero como $\mathfrak{p}$ es maximal ya mostramos que esto no ocurre, entonces $\mathfrak{i} \neq \mathfrak{i}\mathfrak{p}^{-1}$, y para $x \in \mathfrak{i}$, $x = x \cdot 1 \in \mathfrak{i}R \subseteq \mathfrak{i}\mathfrak{p}^{-1}$, por lo tanto $\mathfrak{i} \subsetneq \mathfrak{i}\mathfrak{p}^{-1}$, y como $\mathfrak{i}$ es maximal en $\mathcal{F}$, $\mathfrak{i}\mathfrak{p}^{-1} \notin \mathcal{F}$, así, existen ideales primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ tales que $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{i}\mathfrak{p}^{-1}$, entonces $\mathfrak{p} \cdot \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{i}$, lo que es una contradicción, luego $\mathcal{F}$ es vacía.
Probemos la unicidad de esta factorización. Sean $\mathfrak{p}_1, \cdots, \mathfrak{p}_n, \mathfrak{q}_1, \cdots, \mathfrak{q}_s$, ideales primos de R tales que $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s$. Entonces $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subseteq \mathfrak{p}_1$. Como $\mathfrak{p}_1$ es primo,

existe i, supongamos $i = 1$, tal que $\mathfrak{q}_i = \mathfrak{q}_1 \subseteq \mathfrak{p}_1$, pero $\mathfrak{q}_1$ es maximal así que $\mathfrak{q}_1 = \mathfrak{p}_1$. Tenemos que $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s$. Continuando con este procedimiento, si $r < s$, tendríamos que $R = \mathfrak{q}_{r+1} \cdot \ldots \cdot \mathfrak{q}_s$, y de ese modo para cada $i \in \{r+1, \cdots, s\}$ $R \subseteq \mathfrak{q}_i$, y así $R = \mathfrak{q}_i$ lo que contradice la maximalidad de $\mathfrak{q}_i$. Análogamente se prueba que $s \nless r$. En conclusión $r = s$ y existe $\sigma \in S_r$ tal que $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$. □

Se puede probar que el recíproco de este teorema también es verdadero. Por lo tanto, un dominio integral R es de Dedekind si, y solamente si, se verifica que todo ideal propio en R se puede expresar de manera única como producto de ideales primos. Ver [9, Teorema 5.20].

Observación 3.2. Del Teorema anterior, se sigue que, si $\mathfrak{n}$ es un ideal fraccionario de R, entonces existen ideales primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ tales que $\mathfrak{n} = \mathfrak{p}_1^{m_1} \cdot \ldots \cdot \mathfrak{p}_n^{m_n}$, con $m_1, \cdots, m_n \in \mathbb{Z}$. Ver [4, pág 74].

Definición 3.5. *Sea R un dominio de Dedekind, $\mathfrak{a}$ y $\mathfrak{b}$ ideales no nulos de R. Decimos que $\mathfrak{a}$ divide a $\mathfrak{b}$ si existe $\mathfrak{j}$ ideal de R tal que $\mathfrak{a}\mathfrak{j} = \mathfrak{b}$, en tal caso escribimos $\mathfrak{a}|\mathfrak{b}$.*

El siguiente resultado muestra que en el contexto de los ideales "contener" es equivalente a "dividir".

Proposición 3.16. *Sea R un dominio de Dedekind, $\mathfrak{a}$ y $\mathfrak{b}$ ideales no nulos de R. Entonces $\mathfrak{a}|\mathfrak{b}$, si y solo si $\mathfrak{a} \supseteq \mathfrak{b}$.*

Demostración. Si $\mathfrak{a}|\mathfrak{b}$, existe $\mathfrak{j}$ ideal de R tal que $\mathfrak{a}\mathfrak{j} = \mathfrak{b}$ y $\mathfrak{a} \supseteq \mathfrak{b}$. Recíprocamente, si $\mathfrak{a} \supseteq \mathfrak{b}$, entonces $R = \mathfrak{a}^{-1}\mathfrak{a} \supseteq \mathfrak{a}^{-1}\mathfrak{b}$ y por lo tanto $\mathfrak{j} = \mathfrak{a}^{-1}\mathfrak{b}$ es un ideal de R, con $\mathfrak{j}\mathfrak{a} = \mathfrak{b}$, esto es, $\mathfrak{a}|\mathfrak{b}$. □

Ejemplo 3.7. *Factorización del ideal principal $\langle 6\rangle$ en $\mathbb{Z}\left[\sqrt{-5}\right]$.*
Tenemos que $6 = 2\cdot 3$ en $\mathbb{Z}\left[\sqrt{-5}\right]$ y es claro que $\langle 6\rangle = \langle 2\rangle\langle 3\rangle$. Pero $\langle 2\rangle$ no es un ideal primo, de hecho el producto $6 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) \in \langle 2\rangle$ pero $\left(1 + \sqrt{-5}\right) \notin \langle 2\rangle$ y $\left(1 - \sqrt{-5}\right) \notin \langle 2\rangle$. Sea $\mathfrak{p}_1 = \left\langle 2, 1 + \sqrt{-5}\right\rangle$ el ideal en $\mathbb{Z}\left[\sqrt{-5}\right]$ generado por 2 y $1 + \sqrt{-5}$. Entonces cada elemento $x \in \mathfrak{p}_1$ es de la forma

$$\begin{aligned} x &= 2\left(a + b\sqrt{-5}\right) + \left(1 + \sqrt{-5}\right)\left(c + d\sqrt{-5}\right) \\ &= (2a + c - 5d) + (2b + c + d)\sqrt{-5} \\ &= r + s\sqrt{-5} \end{aligned}$$

Donde $a, b, c, d \in \mathbb{Z}$ *y* $r - s = 2a - 2b - 6d = 2t$, *con* $t \in \mathbb{Z}$, *esto es,* $r \equiv s \pmod 2$. *Por otra parte si* $x = a + b\sqrt{-5}$ *es tal que* $a \equiv b \pmod 2$, *entonces para* $a \equiv b \equiv 0 \pmod 2$ *se tiene que* $a = 2m$ *y* $b = 2n$, *con* $m, n \in \mathbb{Z}$, *así* $x = 2\left(m + n\sqrt{-5}\right) + 0\left(1 + \sqrt{-5}\right) \in \mathfrak{p}_1$ *y para* $a \equiv b \equiv 1 \pmod 2$ *se verifica que* $a = 2(m' - 1)$ *y* $b = 2(n' - 1)$, *con* $m', n' \in \mathbb{Z}$, *así* $x = 2\left(m' + n'\sqrt{-5}\right) - \left(1 + \sqrt{-5}\right) \in \mathfrak{p}_1$.

Lo anterior muestra que $x = r + s\sqrt{-5} \in \mathfrak{p}_1$ *si, y solo si, r y s son ambos pares o ambos impares. Luego* $\mathbb{Z}\left[\sqrt{-5}\right]/\mathfrak{p}_1 = \{0 + \mathfrak{p}_1, 1 + \mathfrak{p}_1\}$, *ya que si* $r + s\sqrt{-5}$ *es tal que r es impar y s es par, entonces* $\left(r + s\sqrt{-5}\right) - 1 = (r - 1) + s\sqrt{-5} \in \mathfrak{p}_1$ *pues* $r - 1$ *y s son pares. Así,* $\left(r + s\sqrt{-5}\right) + \mathfrak{p}_1 = 1 + \mathfrak{p}_1$. *Similarmente, si r es par y s es impar* $(r - 1) + s\sqrt{-5} \in \mathfrak{p}_1$ *pues* $r - 1$ *y s son impares, así* $\mathbb{Z}\left[\sqrt{-5}\right]/\mathfrak{p}_1$ *es isomorfo a* $\mathbb{Z}_2$, *en consecuencia* $\mathfrak{p}_1$ *es un ideal primo en* $\mathbb{Z}\left[\sqrt{-5}\right]$.

Con argumentos similares se prueba que los ideales $\mathfrak{p}_2$ *y* $\mathfrak{p}_3$ *son ideales primos, donde*

$$\begin{aligned} \mathfrak{p}_2 &= \left\langle 3, 1 + \sqrt{-5} \right\rangle, \\ \mathfrak{p}_3 &= \left\langle 3, 1 - \sqrt{-5} \right\rangle. \end{aligned}$$

Veamos que $\mathfrak{p}_1^2 = \mathfrak{p}_1\mathfrak{p}_1$ *es precisamente* $\langle 2 \rangle$. *En efecto, tenemos que:*

$$1 - \sqrt{-5} = 2 - \left(1 + \sqrt{-5}\right) \in \mathfrak{p}_1,$$

entonces

$$6 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) \in \mathfrak{p}_1^2.$$

Como $2 \in \mathfrak{p}_1$, $4 \in \mathfrak{p}_1^2$, *luego* $2 = 6 - 4 \in \mathfrak{p}_1^2$. *En consecuencia* $\langle 2 \rangle \subseteq \mathfrak{p}_1^2$.

Por otra parte, $\mathfrak{p}_1^2 = \left\langle 2, 1+\sqrt{-5}\right\rangle^2$, *entonces* $\mathfrak{p}_1^2 = \left\langle 4, 2\left(1+\sqrt{-5}\right), \left(1+\sqrt{-5}\right)^2\right\rangle$. *De hecho, como* $4,\ 2\left(1+\sqrt{-5}\right),\ \left(1+\sqrt{-5}\right)^2 \in \mathfrak{p}_1^2$ *tenemos que*

$$\mathfrak{p}_1^2 \supseteq \left\langle 4, 2\left(1+\sqrt{-5}\right), \left(1+\sqrt{-5}\right)^2\right\rangle,$$

además, si $x \in \mathfrak{p}_1^2$ *y* $x = \sum_{i=1}^{k} p_i q_i$, *con* $k \in \mathbb{N}$ *y* $p_i, q_i \in \mathfrak{p}_1$ *y*

$$\begin{aligned} q_i p_i &= \left[2\alpha + \left(1+\sqrt{-5}\right)\beta\right]\left[2\alpha' + \left(1+\sqrt{-5}\right)\beta'\right] \\ &= 4\alpha\alpha' + 2\left(1+\sqrt{-5}\right)(\alpha\beta' + \alpha'\beta) + \left(1+\sqrt{-5}\right)^2\beta\beta', \end{aligned}$$

donde $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}\left[\sqrt{-5}\right]$, *así para cada* $i \in \{1, \cdots, k\}$, $q_i p_i \in \left\langle 4, 2\left(1+\sqrt{-5}\right), \left(1+\sqrt{-5}\right)^2\right\rangle$, *de ese modo* $x \in \left\langle 4, 2\left(1+\sqrt{-5}\right), \left(1+\sqrt{-5}\right)^2\right\rangle$, *por lo tanto*

$$\mathfrak{p}_1^2 \subseteq \left\langle 4, 2\left(1+\sqrt{-5}\right), \left(1+\sqrt{-5}\right)^2\right\rangle.$$

Ahora, como $\left(1+\sqrt{-5}\right)^2 = -4 + 2\sqrt{-5}$, *podemos afirmar que* $\mathfrak{p}_1^2 \subseteq \langle 2\rangle$, *ya que cada generador de* $\mathfrak{p}_1^2$ *es múltiplo de 2. Luego*

$$\mathfrak{p}_1^2 = \langle 2\rangle.$$

También tenemos que $\mathfrak{p}_2\mathfrak{p}_3 = \langle 3\rangle$. *De hecho,*
Como $\mathfrak{p}_2\mathfrak{p}_3 = \langle 9, 3\left(1+\sqrt{5}\right), 3\left(1-\sqrt{5}\right), 6\rangle$, *entonces* $\mathfrak{p}_2\mathfrak{p}_3 \subseteq \langle 3\rangle$, *ya que cada generador de* $\mathfrak{p}_2\mathfrak{p}_3$ *es múltiplo de 3. Para la otra inclusión observe que* $9, 6 \in \mathfrak{p}_2\mathfrak{p}_3$, *luego* $9 - 6 = 3 \in \mathfrak{p}_2\mathfrak{p}_3$, *por lo tanto* $\langle 3\rangle \subseteq \mathfrak{p}_2\mathfrak{p}_3$.
En conclusión, el ideal $\langle 6\rangle$ *es producto de cuatro ideales primos:*

$$\langle 6\rangle = \langle 2\rangle\langle 3\rangle = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3.$$

En el Ejemplo 3.3 probamos que los dominos de ideales principales son dominios de Dedekind, sin embargo existen dominios de Dedekind que no son dominios de ideales principales,

es el caso de $\mathbb{Z}\left[\sqrt{-5}\right]$ que por el Teorema 3.2 es de Dedekind pero vimos en el capítulo anterior que no tiene factorización única.

Para finalizar, mostraremos que una condición suficiente para que un dominio de Dedekind tenga factorización única es que tenga un número finito de ideales primos, pues sucede que dichos anillos son siempre dominios de ideales principales. Para probarlo necesitamos una versión del Teorema Chino del Resto para ideales.

Dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ de un anillo R se llaman ***comaximales*** o ***"primos relativos"*** si $\mathfrak{a}+\mathfrak{b} = R$. Por ejemplo, dos ideales $\mathfrak{p}$ y $\mathfrak{q}$ tales que $\mathfrak{q} \nsubseteq \mathfrak{p}$, con $\mathfrak{p}$ maximal en un anillo R son comaximales. De hecho, $\mathfrak{p} \subseteq \mathfrak{p} + \mathfrak{q} \subseteq R$, pero $\mathfrak{p}$ es maximal, entonces $\mathfrak{p} = \mathfrak{p} + \mathfrak{q}$ ó $\mathfrak{p} + \mathfrak{q} = R$. Si $\mathfrak{p} = \mathfrak{p} + \mathfrak{q}$, entonces $\mathfrak{q} \subseteq \mathfrak{p} + \mathfrak{q} = \mathfrak{p}$, contradicción, luego $\mathfrak{p} + \mathfrak{q} = R$.

Teorema 3.17. ***Teorema Chino del Resto:***

Sea R un dominio, $\mathfrak{u}_1, \mathfrak{u}_2, \cdots, \mathfrak{u}_n$ ideales de R tales que $\mathfrak{u}_i + \mathfrak{u}_j = R$, para todo $i \neq j$ (comaximales dos a dos). Dados $x_1, x_2 \cdots, x_n \in R$, existe $x \in R$ tal que $x \equiv x_i \pmod{\mathfrak{u}_i}$ para $i = 1, 2, \cdots, n$.

Demostración. Para $n = 2$, como $\mathfrak{u}_1 + \mathfrak{u}_2 = R$, existen $a_1 \in \mathfrak{u}_1$ y $a_2 \in \mathfrak{u}_2$ tales que $a_1 + a_2 = 1$, por lo tanto $a_1 \equiv 1 \pmod{\mathfrak{u}_2}$ y $a_2 \equiv 1 \pmod{\mathfrak{u}_1}$. Sea $x = x_2a_1 + x_1a_2$, entonces $x - x_1a_2 = x_2a_1 \in \mathfrak{u}_1$, luego $x \equiv x_1a_2 \equiv x_1 \pmod{\mathfrak{u}_1}$ y similarmente $x \equiv x_2 \pmod{\mathfrak{u}_2}$.

En el caso general, para $i \geq 2$ existen $a_i \in \mathfrak{u}_i$, $b_i \in \mathfrak{u}_i$ tales que $a_i + b_i = 1$, entonces

$$1 = \prod_{i=2}^{n} (a_i + b_i) \in \mathfrak{u}_1 + \prod_{i=2}^{n} \mathfrak{u}_i = R.$$

Por el caso $n = 2$, existe $y_1 \in R$ tal que $y_1 \equiv 1 \pmod{\mathfrak{u}_1}$ y $y_1 \equiv 0 \pmod{\mathfrak{u}_2 \cdots \mathfrak{u}_n}$, en particular $y_1 \in \prod_{i=2}^{n} \mathfrak{u}_i \subseteq \mathfrak{u}_i$, luego $y_1 \equiv 0 \pmod{\mathfrak{u}_i}$ para $i \geq 2$. Análogamente, podemos encontrar elementos $y_i \in R$ que cumplan:

$$y_i \equiv 1 \pmod{\mathfrak{u}_i}, \quad y_i \equiv 0 \pmod{\mathfrak{u}_j} \text{ para } i \neq j.$$

Tomando $x = x_1y_1 + \cdots + x_ny_n$ tenemos que para cada $i \in \{1, \cdots, n\}$

$$x - x_iy_i = \sum_{\substack{j=1 \\ j\neq i}}^{n} x_jy_j \in \mathfrak{u}_i.$$

En consecuencia, $x \equiv x_i \pmod{\mathfrak{u}_i}$ para $i = 1, 2, \cdots, n$. □

Teorema 3.18. *Si R es un dominio de Dedekind con un número finito de ideales primos entonces R es un dominio de ideales principales y por lo tanto tiene factorización única.*

Demostración. Sean $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ los ideales primos de R. Como $\mathfrak{p}_1$ es maximal, $\mathfrak{p}_1^2 \subsetneq \mathfrak{p}_1$, y así, existe $r_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$. Además de eso, $\mathfrak{p}_1^2 \not\subseteq \mathfrak{p}_i$ y cada $\mathfrak{p}_i$ es maximal para $i \in \{2, \cdots, n\}$, por lo tanto los ideales $\mathfrak{p}_1^2, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ son comaximales dos a dos, así por el Teorema Chino del Resto existe $r \in R$ tal que

$$r \equiv r_1 \pmod{\mathfrak{p}_1^2} \text{ y } r \equiv 1 \pmod{\mathfrak{p}_i},$$

con $i \in \{2, \cdots, n\}$. Por lo tanto $r \in \mathfrak{p}_1, r \notin \mathfrak{p}_1^2$ y $r \notin \mathfrak{p}_i$, para cualquier $i \in \{2, \cdots, n\}$, luego

$$\langle r \rangle \subseteq \mathfrak{p}_1, \quad \langle r \rangle \not\subseteq \mathfrak{p}_1^2 \quad \text{y} \quad \langle r \rangle \not\subseteq \mathfrak{p}_i,$$

donde $i \in \{2, \cdots, n\}$.
Como R es de Dedekind, $\langle r \rangle = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2} \cdots \mathfrak{p}_n^{k_n}$, $k_i \in \mathbb{N} \cup \{0\}$, entonces $k_i = 0$ para $i \in \{2, \cdots, n\}$ de ese modo $\langle r \rangle = \mathfrak{p}_1^{k_1}$, por lo tanto $k_1 = 1$ y $\mathfrak{p}_1$ es principal. De manera análoga se prueba que los otros $\mathfrak{p}_i$ son principales y como todo ideal de R es producto de potencias de los $\mathfrak{p}_i$, entonces todo ideal de R es principal. □

La siguiente es una demostración algebraica de que hay infinitos números primos dada por Washington [3] usando algunos resultados que hemos estudiado.

[3] L.C. Washington, *The infinitude of primes via commutative algebras.* Manuscrito sin publicar 1980.

Ejemplo 3.8. *Sabemos que* $\mathbb{Z}\left[\sqrt{-5}\right]$ *es de Dedekind, pero no DFU, por lo tanto debe tener infinitos ideales primos.*

Sea $p \in \mathbb{Z}$ *primo, entonces existe* $k \in \mathbb{N}$ *tal que* $\langle p \rangle = \prod_{i=1}^{k} \mathfrak{q}_i^{n_i}$, *con* $\mathfrak{q}_i$ *ideal primo de* $\mathbb{Z}\left[\sqrt{-5}\right]$ *para cada* $i \in \{1, \cdots, k\}$. *Supongamos que el número de primos es finito, entonces el conjunto*

$$X = \left\{\mathfrak{q} : \mathfrak{q} \text{ es ideal primo de } \mathbb{Z}\left[\sqrt{-5}\right] \text{ y } \mathfrak{q} \mid \langle p \rangle \text{ para algún primo } p \in \mathbb{Z}\right\}$$

es finito. Como $\mathbb{Z}\left[\sqrt{-5}\right]$ *tiene infinitos ideales primos podemos escoger a* $\mathfrak{q}_1$, *un ideal primo de* $\mathbb{Z}\left[\sqrt{-5}\right]$ *tal que* $\mathfrak{q}_1 \notin X$. *Pero* $\mathbb{Z}\left[\sqrt{-5}\right]$ *es entero sobre* $\mathbb{Z}$ *entonces,* $\mathfrak{q}_1 \cap \mathbb{Z}$ *es un ideal primo (maximal) de* $\mathbb{Z}$ *por el Lema 3.5 y como los ideales primos de* $\mathbb{Z}$ *son generados por un primo, tenemos que* $\mathfrak{q}_1 \cap \mathbb{Z} = \langle p_1 \rangle$ *con* p_1 *primo. Luego* $\mathfrak{q}_1 \mid \langle p_1 \rangle$ *pues* $\langle p_1 \rangle \subseteq \mathfrak{q}_1$, *así* $\mathfrak{q}_1 \in X$, *contradicción, por lo tanto existen infinitos números primos.*

Conclusiones

Teniendo en cuenta los aspectos desarrollados en este trabajo, se ha podido probar que los enteros de un cuerpo $\mathbb{L}$ sobre un anillo R, es decir aquellos elementos en $\mathbb{L}$ que son raíz de un polinomio mónico en $R[X]$; forman un anillo en el que no necesariamente vale la factorización única. Sin embargo, más allá de este hecho, en este trabajo, hemos mostrado que existen cuerpos numéricos, en los cuales su anillo de enteros es un dominio de factorización única, por ejemplo el anillo de los enteros de Gauss $\mathbb{Z}[i]$; lo cual constituye una herramienta importante en la solución de ecuaciones diofánticas y casos particulares del Último Teorema de Fermat.

Para suplir en parte la falencia de factorización única de elementos en los anillos de enteros, definimos los dominios de Dedekind como aquellos que cumplen ciertas condiciones de finitud y establecimos una caracterización importante en términos de factorización única de ideales. Específicamente, probamos que en dichos dominios todo ideal propio se puede factorizar como producto de ideales primos y este producto es único salvo el orden de los factores. En este contexto vimos que el anillo de los enteros de un cuerpo es un dominio de Dedekind, aunque no necesariamente es dominio de ideales principales ni de factorización única.

Bibliografía

[1] A. Baker. *Trascendental number theory*. Cambridge University press. 1975.

[2] E. S. Barnes, H.P.F. Swinnerton-Dyer. *The inhomogeneus minima of binary quadratic forms (I)*. Acta Mathematica 87 (1952), 259-323.

[3] D. A. Clark. *A quadratic field which is Euclidean but not norm-Euclidean*. Manuscripta Mathematica 83 (1994) 327-330.

[4] O. Endler. *Teoria dos números algebráicos*. Segunda edição, Projecto euclides, Rio de Janeiro, IMPA, 2006.

[5] T. Hungerford. *Abstract Algebra An Introduction*. Third Edition. Cleveland State University.

[6] P. Martin. *Introdução á Teoria dos Grupos e á Teoria de Galois*. Publicações IME-USP.

[7] K. Spindler. *Abstract Algebra with Applications*. Volume 2: Rings and Fields, Chapman and Hall/CRC Pure and Applied Mathematics, 1993.

[8] I. Stewart and W. Tall. *Algebraic Number Theory and Fermat's Last Theorem*. Third Edition, AK-Peters, Naticks-Massachusets, 2002.

[9] F. Zaldívar. *Introducción al álgebra conmutativa*. 2011. Disponible en: http://www.math.unam.mx/javier/felipe/conmutativa.pdf

[10] O. Zariski, P. Samuel, I. S. Cohen. *Commutative Algebra I: 1 and 2*. Graduate text in methematics, Springer, 1975