**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE CIENCIAS**

# ANILLOS DE DEDEKIND

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE:**

**MATEMÁTICA**

**P R E S E N T A :**

**CATALINA APOLINAR GARCÍA**


**DIRECTOR DE TESIS:**
**DRA. MARÍA DEL CARMEN HERÉNDIRA GÓMEZ LAVEAGA**
**2015**

Ciudad Universitaria, D. F.

**Hoja de datos del jurado**

1. Datos del alumno
Apolinar
García
Catalina
50 82 57 33
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
307020099

2. Datos del asesor
Dra.
María del Carmen Heréndira
Gómez
Laveaga

3. Datos del sinodal 1
Dra.
Bertha María
Tomé
Arreola

4. Datos del sinodal 2
Mat.
Julio César
Guevara
Bravo

5. Datos del sinodal 3
Mat.
Ernesto
Mayorga
Saucedo

6. Datos del sinodal 4
M. en C.
Rolando
Gómez
Macedo

7. Datos del trabajo escrito
Anillos de Dedekind
73 p
2015

# Agradecimientos

A mi mamá, Catalina, quien siempre me ha dado todo su amor, apoyo y comprensión. Porque sin ella nada de esto sería posible. A mi padre, de quien siempre recibí amor y confianza.

A mi hermano Guillermo. Gracias por estar a mi lado, por cuidarme y por tu cariño. A Lupita, por alegrar la vida de esta familia y a Alma por su paciencia y comprensión.

A mi tutora y maestra Carmen Gómez Laveaga, por su paciencia y por todas sus enseñanzas en este maravilloso mundo de las matemáticas.

A mis amigos más queridos Nancy, Jessica, Berenice, Ricky, Tere, Adriana, Luis, Dulce, Ángela, Fernando, Yemi, Carmen y Edgar, gracias por su amistad y por alegrar mi vida.

# Índice general

# Introducción

El objetivo de esta tesis es ofrecer una introducción al estudio de los anillos de Dedekind, demostrar algunas propiedades que los caracterizan y que sirven como base para un estudio más profundo de los mismos.

El desarrollo de los anillos de Dedekind comenzó con el estudio de los campos de números algebraicos, es decir, con extensiones de campos finitas sobre el campo de los números racionales $\mathbb{Q}$ y con el subanillo de los enteros algebraicos de dicha extensión, que son los elementos de la extensión que satisfacen un polinomio mónico con coeficientes en $\mathbb{Z}$. Muchos matemáticos dieron por hecho que estos anillos eran de factorización única y basaron muchos de sus resultados en esta suposición, debido a que los números enteros y el anillo de polinomios con coeficientes en un campo si son anillos de factorización única. Un de los ejemplos más conocidos de esto último es el caso del matemático Gabriel Lamé quien en 1847 anunció a la Academia de Ciencias de París que había demostrado el último teorema de Fermat. Sin embargo, su demostración estaba basada en la factorización única de los campos ciclotómicos y Kummer había demostrado que ésto no se cumplía. Otro ejemplo nos lo da el dominio

$$\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\},$$

que no es un dominio de factorización única ya que

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

y se puede demostrar que $2, 3, 1 \pm \sqrt{-5}$ son elementos primos del dominio.

Fue así como Kummer y Richard Dedekind (1831-1916) introdujeron el concepto de ideal de un anillo y Dedekind introdujo las nociones de ideal primo y demostró que en los anillos de enteros algebraicos todo ideal es producto de un número finito de ideales primos y que esta descomposición es única. Esta propiedad es de gran importancia pues es lo más parecido a ser un dominio de ideales principales y compensa en cierto modo el hecho de que los anillos de enteros algebraicos no siempre sean de factorización única.

En algunos textos definen a un anillo de Dedekind como un dominio entero noetheriano, enteramente cerrado, es decir, que todo elemento que es raíz de un polinomio con coeficientes en el dominio pertenece éste mismo, y en el que todo ideal primo es maximal. No es difícil ver que el anillo de los números enteros es un anillo de Dedekind pues es un

dominio de ideales principales y más adelante demostraremos que los anillos de enteros algebraicos también son anillos de Dedekind . Sin embargo en esta tesis daremos otra definición, y posteriormente demostraremos que son equivalentes, que nos permitirá enunciar y demostrar algunos resultados no sólo para campos de característica cero, como lo son los campos de números algebraicos.

Entre las propiedades más importantes de los anillos de Dedekind que se demostrarán en esta tesis son que todo ideal puede descomponerse como producto de ideales primos de manera única. Este hecho y el constante trabajo que se realiza entre los anillos de enteros algebraicos y su correspondiente campo de cocientes nos permite generalizar el concepto de ideal al de ideal fraccionario. Los ideales fraccionarios tienen la propiedad de formar un grupo multiplicativo y permiten determinar qué tan cerca está un anillo de Dedekind de ser un dominio de ideales principales y en consecuecnia de factorización única, lamentablemente esto último no lo veremos en esta tesis.

Uno de los teoremas que se demostrarán en esta tesis es que dado un anillo de Dedekind, su cerradura entera en una extensión de su campo de cocientes es también un anillo de Dedekind. A partir de aquí podemos generalizar el concepto de la norma de un elemento en un campo numérico al de norma de un ideal y además podemos demostrar que es multiplicativa.

La importancia de los anillos de Dedekind se debe a que en la práctica es difícil encontrar anillos de factorización y todavía más difícil es que esta factorización sea única, sin embargo los anillos de Dedekind al ser noetherianos resultan ser de factorización y aunque no todos son de factorización única existen resultados que caracterizan a los que sí lo son, estos resultados no se demostrarán pero tenemos, por ejemplo, que en extensiones cuadráticas de los racionales $\mathbb{Q}[\sqrt{d}]$ donde de $d$ es libre de cuadrados y negativa, se tiene factorización única solamente en los casos $d = -1, -2, -3, -7, -11$ (véase la referencia [4], capítulo 4, sección 7).

En el caso de teoría algebraica de números, los anillos de Dedekind permiten obtener todas las soluciones a ciertas ecuaciones diofantinas y estudiar la ley de reciprocidad cuadrática.

# Capítulo 1

# Preliminares

Para el desarrollo de esta tesis suponemos conocidos algunos conceptos y resultados básicos de teoría de anillos, extensiones de campos y teoría de módulos. A continuación, enunciaremos los conceptos y resultados que serán utilizados con mayor frecuencia y que vale la pena ser mencionados.

Cabe aclarar que en este trabajo cuando hablemos de un anillo $R$ nos estaremos refiriendo, a menos que se especifique lo contrario, a un anillo conmutativo con unidad.

## 1.1. Ideales primos e ideales maximales

Empezaremos enunciando el teorema de correspondencia para anillos conmutativos.

**Teorema 1.1.1.** *Sea $I$ un ideal propio de un anillo conmutativo $R$. Entonces el homomorfismo natural $\pi : R \to R/I$ dado por $\pi(r) = r + R/I$ induce una correspondencia biyectiva entre los ideales de $R$ que contienen a $I$ y los ideales de $R/I$, dada por*

$$\pi'(a) = a + I$$

*con $a \in J$. Además todo ideal del anillo cociente $R/I$ es de la forma $J/I$ para un único ideal $J$ de $R$ que contiene a $I$.*

**Definición 1.1.2.** *Decimos que un ideal $I$ de un anillo $R$ es un ideal primo si $I \neq R$ y $ab \in I$ implica $a \in I$ o $b \in I$.*

**Observación 1.1.3.** *Un anillo $R$ es un dominio entero si y sólo si el ideal $\langle 0 \rangle$ es un ideal primo. En efecto, $R$ es dominio entero si y sólo si $ab = 0$ implica que $a = 0$ o $b = 0$, es decir, $ab \in \langle 0 \rangle$ implica $a \in \langle 0 \rangle$ o $b \in \langle 0 \rangle$.*

**Definición 1.1.4.** *Decimos que un ideal $I$ de un anillo $R$ es ideal maximal si $I \neq R$ y si $J$ es un ideal de $R$ tal que $I \subseteq J \subseteq R$, entonces $I = J$ o $J = R$.*

**Observación 1.1.5.** *El ideal $J/I$ del anillo $R/I$ es un ideal primo si y sólo si $J$ es ideal primo de $R$ tal que $I \subseteq J \subseteq R$.*

*Demostración.* Sean $a+I, b+I \in R/I$ tales que $(a+I)(b+I) \in J/I$. Esto es $ab+I \in J/I$, lo que implica que $ab \in J$ que es un ideal primo. Luego $a \in J$ o $b \in J$. Por lo tanto $a+I \in J/I$ o $b+I \in J/I$. Inversamente, sean $a, b \in R$ tales que $ab \in J$. Entonces $(a+I)(b+I) = ab+I \in J/I$. Luego $a+I \in J/I$ o $b+I \in J/I$ ya que $J/I$ es un ideal primo. Por lo tanto $a \in J$ o $b \in J$. □

**Observación 1.1.6.** *El ideal $J/I$ del anillo $R/I$ es un ideal maximal si y sólo si $J$ es un ideal maximal de $R$ que contiene a $I$.*

*Demostración.* Sea $A$ ideal de $R$ tal que $I \subseteq J \subseteq A \subseteq R$. Entonces $J/I \subseteq A/I \subseteq R/I$. Como $J/I$ es ideal maximal, entonces $J/I = A/I$ o $A/I = R/I$. Luego $J = A$ o $A = R$. Inversamente sea $A/I$ ideal de $R/I$ tal que $J/I \subseteq A/I \subseteq R/I$. Esto implica que $I \subseteq J \subseteq A \subseteq R$. Luego $J = A$ o $A = R$ ya que $J$ es ideal maximal. □

**Proposición 1.1.7.** *Un ideal $I$ de un anillo $R$ es ideal primo si y sólo si $R/I$ es un dominio entero.*

*Demostración.* $\Longrightarrow$) Sean $a+I, b+I \in R/I$ tales que $I = (a+I)(b+I) = ab+I$. Esto implica que $ab \in I$ y como $I$ es un ideal primo, entonces $a \in I$ o $b \in I$, luego $I = a+I$ o $I = b+I$.

Por lo tanto $R/I$ es un dominio entero.

$\Longleftarrow$) Sean $a, b \in R$ tales que $ab \in I$. Luego $I = ab+I = (a+I)(b+I)$, y por ser $R/I$ un dominio entero, entonces $I = a+I$ o $I = b+I$, lo que significa $a \in I$ o $b \in I$.

Por lo tanto $I$ es un ideal primo. □

**Proposición 1.1.8.** *Un anillo $R$ es un campo si y sólo si sus únicos ideales son $\langle 0 \rangle$ y él mismo.*

*Demostración.* $\Longrightarrow$) Sea $I \neq \langle 0 \rangle$ un ideal de $R$. Entonces existe $a \in I$ tal que $a \neq 0$, como $R$ es campo existe $a^{-1} \in R$ y por ser $I$ un ideal $aa^{-1} = 1 \in I$. En consecuencia $I = R$.

$\Longleftarrow$) Sea $R$ un anillo cuyos únicos ideales son el ideal $\langle 0 \rangle$ y él mismo. Sea $a \in R$ tal que $a \neq 0$, esto implica que el ideal $\langle a \rangle = \{ra | r \in R\} = R$, por lo que existe $r \in R$ tal que $ra = 1$.

Por lo tanto $R$ es campo. □

**Proposición 1.1.9.** *Un ideal $I$ de un anillo $R$ es maximal si y sólo si $R/I$ es campo.*

*Demostración.* $\Longrightarrow$) Supongamos que $I$ es ideal maximal de $R$. Para demostrar que $R/I$ es campo demostraremos que los únicos ideales que posee son el ideal $\langle \overline{0} \rangle$ y él mismo. Por el teorema de la correspondencia sea $J/R$ un ideal de $R/I$, $J$ es un ideal de $R$ tal

que $I \subseteq J \subseteq R$, pero como $I$ es maximal, entonces $I = J$ o $J = R$. Luego $J/I = \langle \overline{0} \rangle$ o $J/I = R/I$.

$\Longleftarrow$) Sea $J$ ideal de $R$ tal que $I \subseteq J \subseteq R$, entonces $J/I$ es un ideal de $R/I$ que como es campo, por la proposición 1.1.8, $J/I = \langle \overline{0} \rangle$ o $J/I = R/I$. Esto implica que $J = I$ o $J = R$. Por lo tanto $I$ es un ideal maximal. □

**Teorema 1.1.10.** *Todo anillo $R$ no trivial tiene al menos un ideal maximal.*

*Demostración.* Para la demostración de este teorema utilizaremos el lema de Zörn. Sea

$$\mathfrak{J} = \{I | I \text{ ideal propio de } R\}$$

$(\mathfrak{J}, \subseteq)$ es un conjunto parcialmente ordenado. Notemos que $\mathfrak{J} \neq \emptyset$ pues el ideal cero pertenece a $\mathfrak{J}$. Sea $C = \{A_\alpha\}_{\alpha \in \Lambda}$ una cadena de ideales en $\mathfrak{J}$ y $\mathfrak{A} = \bigcup A_\alpha$. Es claro que $\mathfrak{A}$ es cota superior de $C = \{A_\alpha\}$. A continuación mostraremos que $\mathfrak{A}$ es un ideal propio de $R$. Si $a, b \in \mathfrak{A}$, entonces existen $A_\alpha$ y $A_\beta$ ideales de $R$ en $C$ tales que $a \in A_\alpha$ y $b \in A_\beta$; sin pérdida de generalidad podemos suponer que $A_\alpha \subseteq A_\beta$, por lo que $a \in A_\beta$, luego $a + b \in A_\beta \subseteq \mathfrak{A}$ pues $A_\beta$ es ideal de $R$ . Ahora sea $r \in R$ y $a \in \mathfrak{A}$. Entonces existe $A_\alpha$ ideal de $R$ en $C$ tal que $a \in A_\alpha$ y por lo tanto $ra \in A_\alpha \subseteq \mathfrak{A}$. Finalmente $0 \in \mathfrak{A}$ pues $0 \in A_\alpha$ para toda $\alpha$. Si se tuviese que $\mathfrak{A} = R$, se tendría que $1 \in A_\alpha$ para alguna $\alpha$ y en consecuencia $A_\alpha = R$, lo cual no es posible pues $A_\alpha$ es ideal propio para toda $\alpha$. Por lo tanto, $\mathfrak{A} \in \mathfrak{J}$.

Luego $\mathfrak{J}$ tiene un elemento maximal. □

**Corolario 1.1.11.** *Todo ideal $I$ de un anillo $R$ está contenido en un ideal maximal.*

*Demostración.* Por el teorema anterior $R/I$ tiene al menos un ideal maximal $J/I$. Notemos que $J$ es un ideal maximal de $R$ que contiene a $I$, pues si $Q$ es un ideal de $R$ tal que $I \subseteq J \subseteq Q \subseteq R$, entonces $J/I \subseteq Q/I \subseteq R/I$ y como $J/I$ es ideal maximal, entonces $J/I = Q/I$ o $Q/I = R/I$, lo que implica $J = Q$ o $Q = R$ por el teorema de la correspndencia. □

## 1.2. Dominios de Factorización Única y Dominios Noetherianos

Sea D un dominio entero. Denotaremos por $U(D)$ al conjunto de los elementos con inverso multiplicativo en D, es decir,

$$U(D) = \left\{u \in D \mid \text{existe } u^{-1} \in D \text{ tal que } uu^{-1} = 1\right\}$$

**Definición 1.2.1.** *Sean $a, b \in D$. Decimos que $a$ divide a $b$, y lo denotaremos por $a \mid b$, si existe $c \in D$ tal que $ac = b$.*

**Definición 1.2.2.** *Decimos que $p \in D$ es irreducible si $p \neq 0$, $p \notin U(D)$ y si $p = ab$, entonces $a \in U(D)$ o $b \in U(D)$.*

**Definición 1.2.3.** *Decimos que $p \in D$ es primo si $p \neq 0$, $p \notin U(D)$ y si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

**Definición 1.2.4.** *Decimos que $a, b \in D$ son asociados si existe $u \in U(D)$ tal que $b = ua$.*

Sea $R$ un anillo y $a \in R$. Denotaremos por $\langle a \rangle$ al ideal generado por $a$, es decir, $\langle a \rangle = \{ra \mid r \in R\}$. Un ideal es principal si $I = \langle a \rangle$.

**Proposición 1.2.5.** *Sea $D$ un dominio entero y sean $a, b \in D$. Entonces*

1. *$a \mid b$ y $b \mid a$ si y sólo si $a$ y $b$ son asociados.*
2. *$a \mid b$ si y sólo si $\langle b \rangle \subseteq \langle a \rangle$.*
3. *$\langle a \rangle = \langle b \rangle$ si sólo si $a$ y $b$ son asociados.*
4. *$a \in U(D)$ si y sólo si $\langle a \rangle = D$.*
5. *El ideal principal $I =< a >$ es primo si y sólo si $a$ es primo.*
6. *$a \in D$ es un elemento irreducible si y sólo si el ideal $\langle a \rangle$ es maximal en el conjunto de ideales principales propios de $D$.*

*Demostración.* 1. $\Longrightarrow$) $a \mid b$ y $b \mid a$ implica que $a = sb$ y $b = ra$ con $s, r \in D$. Luego $a = sra$ y como $D$ es un dominio entero, entonces $(1 - sr)a = 0$, si $a = 0$, entonces $b = 0$ y el resultado es trivial, de lo contrario $sr = 1$, es decir, $s, r \in U(D)$. Por lo tanto $a$ y $b$ son asociados.

$\Longleftarrow$) Supongamos que $a$ y $b$ son asociados. En consecuencia existe $u \in U(D)$ tal que $a = ub$ y por tanto $au^{-1} = b$. Luego $a \mid b$ y $b \mid a$.

2. $\Longrightarrow$) Si $a \mid b$, entonces $as = b$ para alguna $s \in D$, por lo que $\langle b \rangle \subseteq \langle a \rangle$.

   $\Longleftarrow$) Ahora, si $\langle b \rangle \subseteq \langle a \rangle$, entonces $b = sa$ y de ahí que $a \mid b$.

3. Por el inciso (2), $\langle a \rangle = \langle b \rangle$ si y sólo si $a \mid b$ y $b \mid a$ y esto último ocurre si y sólo si $a$ y $b$ son asociados, por el inciso (1).

4. $\Longrightarrow$) Como $a \in U(D)$ entonces existe $u \in D$ tal que $au = 1$. Sea $r \in D$. Entonces $r = aur = a(ur) \in \langle a \rangle$.

   $\Longleftarrow$) Como $\langle a \rangle = D$ existe $u \in D$ tal que $ua = 1$.

5. $\Longrightarrow$) Sean $c, b \in D$ tales que $a \mid cb$. Entonces $cb \in < a >= I$ y como $I$ es un ideal primo entonces $c \in I$ o $b \in I$. Luego $a \mid c$ o $a \mid b$ y por lo tanto $a$ es primo.

   $\Longleftarrow$) Sean $c, b \in D$ tales que $cb \in I$. En consecuencia $a \mid cb$ y por ser $a$ primo, entonces $a \mid c$ o $a \mid b$. Luego $c \in I$ o $b \in I$ y por lo tanto $I$ es in ideal primo.

6. $\Longrightarrow$) Supongamos $a$ irreducible y $b \in D$ tal que $\langle a\rangle \subsetneq \langle b\rangle$. Entonces $a = sb$ para alguna $s \in D$ y esto implica que $s \in U(D)$ o $b \in U(D)$. Pero si $s \in U(D)$, entonces se tendría que $\langle a\rangle = \langle b\rangle$ que no es el caso. Luego $b \in U(D)$ y por lo tanto $\langle b\rangle = D$.

   $\Longleftarrow$) Supongamos $\langle a\rangle$ maximal en el conjunto de ideales principales propios de $D$ y supongamos que $a = bc$, donde $b, c \notin U(D)$. Entonces $\langle a\rangle \subsetneq \langle b\rangle \subsetneq D$, pues $b, c$ no son unidades lo que contradice la maximalidad de $\langle a\rangle$.

□

**Proposición 1.2.6.** *Sea $D$ un dominio entero y $p \in D$. Si $p$ es primo, entonces $p$ es irreducible.*

*Demostración.* Sean $a, b \in D$ tales que $p = ab$, en consecuencia $\langle p\rangle \subseteq \langle a\rangle$ y $\langle p\rangle \subseteq \langle b\rangle$. Por otro lado $ab \in \langle p\rangle$ que es un ideal primo pues $p$ es primo, por lo tanto $a \in \langle p\rangle$ o $b \in \langle p\rangle$ y por lo tanto $\langle a\rangle \subseteq \langle p\rangle$ o $\langle b\rangle \subseteq \langle p\rangle$. Luego $a$ es asociado de $p$ o $b$ es asociado de $p$ (pproposición 1.2.5 inciso 3), es decir, $a \in U(D)$ o $b \in U(D)$. Por lo tanto $p$ es irreducible. □

En general, un elemento irreducible no es primo, véase el ejemplo 6.2.6.

**Definición 1.2.7.** *Sea $D$ un dominio entero. Decimos que $D$ es un **dominio de factorización** si para toda $r \in D$, $r \notin U(D)$ y $r \neq 0$, existen $p_1, p_2, \ldots, p_n$ elementos irreducibles de $D$ tales que $r = p_1 p_2 \ldots p_n$.*

**Definición 1.2.8.** *Sea $D$ un dominio entero. Decimos que $D$ es un **dominio de factorización única (DFU)** si*

1. *$D$ es de factorización*
2. *La expresión de cada $r \in D$, $r \notin U(D)$ y $r \neq 0$ como producto de irreducibles es única. Es decir, si $r = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$ donde $p_i$ y $q_j$ son irreducibles para toda $i$ y para toda $j$, entonces $n = m$ y cada $p_i$ es asociado de $q_j$, para alguna $j$.*

Los ejemplos que hasta el momento conocemos de DFU son:

**Ejemplo 1.2.9.** *El anillo de enteros $\mathbb{Z}$.*

**Ejemplo 1.2.10.** *El anillo de polinomios $K[x]$ con coeficientes en un campo $K$.*

**Definición 1.2.11.** *Sea $I$ ideal de un anillo conmutativo $R$. Decimos que $I$ es **finitamente generado** si existen $a_1, a_2, \ldots, a_n \in I$ tales que para toda $a \in I$, se tiene que*

$$a = \sum_{i=1}^{n} r_i a_i$$

*donde $r_i \in R$ para toda $i = 1, \ldots, n$.*

**Definición 1.2.12.** *Decimos que un anillo conmutativo $R$ es* ***noetheriano*** *si todo ideal de $R$ es finitamente generado.*

**Definición 1.2.13.** *Decimos que un dominio $D$ es de* ***ideales principales (DIP)*** *si todo ideal $I$ de $D$ es principal.*

Como ejemplo de ideales noetherianos tenemos a los DIP.

El siguiente teorema es de gran importancia, pues nos permite describir a los anillos noetherianos de diferentes maneras.

**Teorema 1.2.14.** *Sea $R$ un anillo conmutativo. Entonces son equivalentes:*

1. *$R$ es noetheriano*
2. *Toda cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ se detiene. Es decir, existe $n \in \mathbb{N}$ tal que $I_n = I_{n+k}$, para toda $k \in \mathbb{N}$.*
3. *Todo conjunto no vacío de ideales de $R$, tiene un elemento maximal.*

*Demostración.* 1) $\Longrightarrow$ 2) Supongamos que $R$ es noetheriano y sea $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ una cadena ascendente de ideales de $R$. Sea $I = \bigcup I_j$. En la demostración del teorema 1.1.10, mostramos que $I$ es un ideal de $R$ por lo que existen $a_{j_1}, a_{j_2}, \ldots, a_{j_n} \in I$ tales que $I = \langle a_{j_1}, a_{j_2}, \ldots, a_{j_n} \rangle$, ya que $R$ noetheriano. Luego, existen $I_{j_1}, I_{j_2}, \ldots, I_{j_n}$ ideales tales que $a_{j_i} \in I_{j_i}$, para toda $i \in \{1, 2, \ldots, n\}$. Podemos suponer, sin pérdida de generalidad, que $I_{j_r} \subseteq I_{j_s}$, si $r \leq s$. Esto implica que $I_{j_i} \subseteq I_{j_n}$ para toda $i \in \{1, 2, \ldots, n\}$, por lo que $a_{j_i} \in I_{j_n}$ para toda $i$. Por consiguiente

$$I = \langle a_{j_1}, a_{j_2}, \ldots, a_{j_n} \rangle \subseteq I_{j_n} \subseteq I.$$

Luego $I_{j_n} = I$ y para toda $k \in \mathbb{N}$ se tiene que $I_{j_n} \subseteq I_{j_{n+k}} \subseteq I = I_{j_n}$.

2) $\Longrightarrow$ 3) Sea $\mathfrak{J} \neq \emptyset$ un conjunto de ideales de $R$ y supongamos que no tiene elementos maximales. Si $I_0 \in \mathfrak{J}$, como $\mathfrak{J}$ no tiene elementos maximales, entonces existe $I_1 \in \mathfrak{J}$ tal que $I_0 \subsetneq I_1$, luego existe $I_2 \in \mathfrak{J}$ tal que $I_1 \subsetneq I_2$ y así construímos recursivamente una cadena ascendente de ideales $I_0 \subsetneq I_2 \subsetneq \cdots I_n \subsetneq \cdots$ que no se detiene, lo cual contradice nuestra hipótesis.

3) $\Longrightarrow$ 1) Supongamos que $R$ no es noetheriano, entonces existe $I$ ideal de $R$ tal que no es finitamente generado. Esto implica que si $\{a_1, a_2, \ldots, a_n\} \subseteq I$, entonces $\langle a_1, a_2, \ldots, a_n \rangle \subsetneq I$. Sea

$$\mathfrak{J} = \{\langle a_1, a_2, \ldots, a_n \rangle \mid \{a_1, \ldots, a_n\} \subseteq I, n \in \mathbb{N} - \{0\}\}$$

$\mathfrak{J}$ es un conjunto de ideales de $R$ distinto del vacío y por lo tanto posee un elemento maximal $J = \langle b_1, b_2, \ldots, b_n \rangle$. Como $J \in \mathfrak{J}$, entonces existe $a \in I - J$ y esto implica que

$$J \subsetneq \langle b_1, b_2, \ldots, b_n, a \rangle \in \mathfrak{J}$$

lo cual contradice que $J$ es maximal. Por lo tanto todo ideal de $R$ es finitamenete generado. □

**Teorema 1.2.15.** *Si $D$ es un dominio entero noetheriano, entonces $D$ es un dominio de factorización.*

*Demostración.* Sea $a \in D - \{0\}$. Si $a$ es irreducible, entonces ya está expresada como un producto finito de irreducibles. Supongamos que $a$ no es irreducible y que no se puede expresar como producto de un número finito de irreducibles, entonces existen $b_1, a_1 \in D - U(D)$ tales que $a = b_1 a_1$, pero como $a$ no es producto de un número finito de irreducibles, entonces al menos uno de estos dos elementos, digamos $a_1$, no es producto de un número finito de irreducibles, por lo tanto existen $b_2, a_2 \in D - U(D)$ tales que $a_1 = b_2 a_2$, pero como $a_1$ no es producto de un número finito de irreducibles, entonces al menos uno de estos dos elementos , digamos $a_2$, no es producto de un número finito de irreducibles. Lo cual implica que $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle$.

Procediendo recursivamente obtenemos una cadena estricta ascendente de ideales que no se detiene

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots \langle a_n \rangle \subsetneq \cdots$$

lo cual contradice que $D$ es un anillo noetheriano. Por lo tanto todo elemento de $D - \{0\}$ es producto de un número finito de irreducibles. □

**Teorema 1.2.16.** *Sea $D$ un dominio de factorizacón. Entonces $D$ es $DFU$ si y sólo si todo elemento irreducible es primo.*

*Demostración.* $\Longrightarrow$) Sea $p \in D$ un elemento irreducible y supongamos que $p \mid ab$. Esto implica que $pr = ab$ para alguna $r \in D$. Como $D$ es dominio de factorización, entonces

$$pr_1 r_2 \cdots r_k = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m$$

donde $r_l, a_i, b_j$ son irreducibles. Por ser $D$ un DFU, $p$ es asociado de alguna $a_i$ o de alguna $b_j$, por lo tanto $p \mid a$ o $p \mid b$. Luego $p$ es primo.

$\Longleftarrow$) Sea $a \in D$ y supongamos que $a = p_1 \cdots p_n = q_1 \cdots q_m$ donde $p_i, q_j$ son elementos irreducibles. Primero mostraremos que cada $p_i$ es asociado de alguna $q_j$. En efecto, como $p_i \mid q_1 \cdots q_m$ y $p_i$ es primo, entonces $p_i \mid q_j$, para alguna $j$, al ser $q_j$ irreducible se tiene que $p_i = u q_j$ con $u \in U(D)$.

Demostraremos que $n = m$ por inducción sobre $k = \text{máx}\{n, m\}$. Para $k = 1$ la afirmación es obvia. Para $k = 2$ supongamos que $n < m$, entonces tendríamos $p_1 = q_1 q_2$. Supongamos que $p_1$ y $q_1$ son asociados, luego $p_1 = u p_1 q_2$. Cancelando $p_1$ en ambos lados tendríamos $1 = u q_2$, lo cual implica que $q_2 \in U(D)$, que no es posible pues es irreducible. Por lo tanto $m = n$.

Supongamos que es válido para $n - 1$. Sea $a = p_1 \cdots p_n = q_1 \cdots q_m$, bajo un reordenamiento de los índices podemos suponer que $p_1$ y $q_1$ son asociados, por lo que $p_1 \cdots p_n = u p_1 \cdots q_m$. Cancelando $p_1$ en ambos lados, se tiene que $p_2 \cdots p_n = u q_2 \cdots q_m$ y por hipótesis de inducción $n - 1 = m - 1$ y por lo tanto $n = m$. □

**Teorema 1.2.17.** *Si $D$ es dominio de ideales principlaes ($DIP$), entonces $D$ es $DFU$.*

*Demostración.* Como $D$ es DIP, entonces es noetheriano y por el teorema 1.2.15 es dominio de factorización. Utilizaremos el teorema 1.2.16 para mostrar que es DFU. Sea $p \in D$ un elemento irreducible, supongamos que $p \mid ab$ y que $p \nmid a$, esto implica que $a \notin \langle p \rangle$. Como $p$ es irreducible, entonces $\langle p \rangle$ es ideal maximal en el conjunto de ideales principales (por la proposición 1.2.5 6), por lo que es un ideal maximal de $D$. En consecuencia $\langle p \rangle \subsetneq \langle p, a \rangle$, lo cual implica que $\langle p, a \rangle = D$, por lo tanto existen $r, s \in D$ tales que $1 = pr + as$ y multiplicando por $b$ se tiene que $b = bpr + abs$. Por lo tanto $p \mid b$, pues $p \mid br$ y $p \mid ab$. Luego $p$ es primo y $D$ es DFU. □

## 1.3. Extensiones de campos

En lo que resta del capítulo $k$ denotará un campo.

**Definición 1.3.1.** *Decimos que un campo $K$ es una extensión sobre un campo $k$, si $k$ es un subcampo de $K$. Denotaremos por $K/k$ a una extensión de $K$ sobre $k$.*

Sea $K/k$ una extensión de campos y sea $S \subseteq K$. Denotaremos por $k(S)$ al mínimo subcampo de $K$ que contiene tanto a $k$ como a $S$. Si $S = \{a_1, \ldots, a_n\}$ utilizaremos la siguiente notación $k(S) = k(a_1, \ldots, a_n)$.

**Observación 1.3.2.** *Ya que la intersección de subcampos de $K$ es un subcampo de $K$, no es difícil ver que $k(S)$ es la intersección de todos los subcampos de $K$ que contienen tanto a $S$ como a $k$. Además $K$ es un $k$-espacio vectorial y denotaremos por $[K : k]$ a la dimensión de $K$ sobre $k$.*

**Definición 1.3.3.** *Decimos que una extensión de campos $K/k$ es finita si $[K : k]$ es finita.*

Sea $K/k$ una extensión de campos y sea $a \in K$. Consideremos el subanillo de $K$

$$k[a] = \{f(a) \mid f(x) \in k[x]\}.$$

Como $k(a)$ es el mínimo subcampo que contiene tanto a $k$ como $a$, entonces $k(a)$ es el campo de cocientes de $k[a]$, es decir,

$$k(a) = \left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in k[x], g(a) \neq 0 \right\}$$

**Definición 1.3.4.** *Sea $K/k$ una extensión de campos. Decimos que $a \in K$ es **algebraico** sobre $k$, si existe un polinomio $f(x) \in k[x]$ distinto de cero tal que $f(a) = 0$. Decimos que $K/k$ es una **extensión algebraica** si todo elemento de $K$ es algebraico sobre $k$.*

**Teorema 1.3.5.** *Si $K/k$ es una extensión finita, entonces es algebraica.*

*Demostración.* Por definición de extensión finita, se tiene que $[K : k] = n$, $n \in \mathbb{N}$. Esto implica que para toda $a \in K$, el conjunto $\{1, a, \ldots, a^n\}$ es linealmente dependiente, es decir, existen $c_0, \ldots, c_n \in k$ tales que $c_0 + c_1 a + \cdots + c_n a^n = 0$, donde al menos uno de los $c_i \neq 0$. Por lo tanto, a es raíz del polinomio $f(x) = c_0 + \cdots + c_n x^n$. □

**Teorema 1.3.6.** *Sean $K/k$ una extensión de campos y $a \in K$ algebraico sobre $k$. Entonces existe un único polinomio mónico e irreducible $p(x) \in k[x]$ tal que $p(a) = 0$. Además si $g(x) \in k[x]$ es tal que $g(a) = 0$, entonces $p(x) \mid g(x)$. Más aún, $k(a) = k[a]$ y para cada $f(a) \in k[a]$, existe un único $t(x) \in k[x]$ tal que $t(x) = 0$ o $grt(x) < grp(x)$ y $f(a) = t(a)$.*

*Demostración.* Definamos el homomorfismo $\phi : k[x] \longrightarrow k[a]$, dado por $\phi(f(x)) = f(a)$. Como $a$ es algebraico, entonces $ker\phi \neq \langle 0 \rangle$ y como $k[x]$ es DIP, entonces $ker\phi = \langle p(x) \rangle$. No es difícil ver que $\phi$ es suprayectiva pues si $f(a) \in k[a]$ entonces $\phi(f(x)) = f(a)$, luego por el primer teorema de isomorfismos $k[x]/\langle p(x) \rangle \cong k[a]$, lo que implica que $k[x]/\langle p(x) \rangle$ es un dominio entero. En consecuencia $\langle p(x) \rangle$ es un ideal primo, por lo que $p(x)$ es primo y en consecuencia $p(x)$ es irreducible en $k[x]$; además podemos considerar $p(x)$ mónico. Si $g(x) \in k[x]$ es tal que $g(a) = 0$, entonces $g(x) \in ker\phi$ y por lo tanto $p(x) \mid g(x)$.

Ahora, $p(x)$ irreducible en $k[x]$ implica que $\langle p(x) \rangle$ es ideal maximal, por lo que $k[x]/\langle p(x) \rangle$ es campo. Luego $k[a]$ es campo y por lo tanto $k(a) = k[a]$.

Sea $f(a) \in k[a]$, con $f(x) \in k[x]$. Por el algoritmo de la división para polinomios existen $q(x), t(x) \in k[x]$ tales que $f(x) = p(x)q(x) + t(x)$ donde $t(x)$ es único y $t(x) = 0$ o $grt(x) < grp(x)$, por lo que $f(a) = t(a)$. Luego

$$k(a) = \{t(a) \mid \ grt(x) < grp(x) \text{ o } t(x) = 0\}.$$

□

Denotaremos por $Irr(k, a)$ al polinomio mónico irreducible con coeficientes en $k$ del teorema anterior y que tiene a $a$ como raíz.

**Corolario 1.3.7.** *Sea $K/k$ una extensión y sea $a \in K$ algebraico sobre $k$. Entonces $k(a)$ es una extensión finita y por lo tanto algebraica, además $[k(a) : k] = grIrr(k, a)$.*

*Demostración.* Sea $Irr(k, a) = p(x)$ de grado n. El conjunto $\left\{1, a, \ldots, a^{n-1}\right\}$ es una base para $k(a)$. En efecto, es generador ya que por el teorema anterior

$$k(a) = \{t(a) \mid \ grt(x) < grp(x) \text{ o } t(x) = 0\}$$

y es un connjunto linealmente independiente pues $p(x)$ es el polinomio de grado mínimo que tiene a $a$ como raíz. □

## 1.4. Campos de descomposición y extensiones normales

**Definición 1.4.1.** *Sean $K$ y $L$ extensiones de $k$. Decimos que $K$ y $L$ son $k-isomorfos$ si existe un isomorfismo $\sigma : K \to L$ tal que $\sigma(a) = a$ para toda $a \in k$.*

**Teorema 1.4.2.** *Sea $K/k$ una extensión y sean $a, b \in K$ tales que $Irr(k, a) = Irr(k, b)$. Entonces $k(a)$ y $k(b)$ son $k-isomorfos$. Es más, existe un $k-isomorfismo$ $\sigma : k(a) \longrightarrow k(b)$ tal que $\sigma(a) = b$.*

*Demostración.* Definamos la función $\sigma : k(a) \longrightarrow k(b)$ de la siguiente forma: sea $t(a) \in k(a)$, donde, $t(x) \in k[x]$ y $t(x) = 0$ o $grt(x) < grIrr(k, a) = p(x)$, definimos

$$\sigma(t(a)) = t(b).$$

Primero mostraremos que está bien definida: Sean $t(a), s(a) \in k(a)$ tales que $t(a) = s(a)$ donde $t(x) = 0$ o $grt(x) < grp(x)$ y $s(x) = 0$ o $grs(x) < grp(x)$. Entonces $t(a) - s(a) = 0$ y esto implica que $p(x) \mid t(x) - s(x)$ y además $gr\,(t(x) - s(x)) < grp(x)$ , por lo tanto $t(b) - s(b) = 0$ y $t(b) = s(b)$. Ahora mostraremos que $\sigma$ es un isomorfismo. Si $t(a), s(a) \in k(a)$, entonces $gr\,(t(x) + s(x)) < grp(x)$ y por lo tanto

$$\begin{aligned}\sigma(t(a) + s(a)) &= t(b) + s(b)\\ &= \sigma(t(a)) + \sigma(s(a)).\end{aligned}$$

Sean $q(x), h(x) \in k[x]$, tales que $t(x)s(x) = q(x)p(x) + h(x)$ con $grh(x) < grp(x)$. Esto implica que $t(a)s(a) = q(a)p(a) + h(a)$ y como $p(a) = 0$, entonces $t(a)s(a) = h(a) \in k(a)$. Así,

$$\begin{aligned}\sigma(t(a)s(a)) &= \sigma(h(a))\\ &= h(b)\\ &= t(b)s(b)\\ &= \sigma(t(a))\sigma(s(a)).\end{aligned}$$

Claramente $\sigma$ es suprayectiva y es inyectiva ya que si $t(b), s(b) \in k(b)$ son tales que $t(b) = s(b)$, entonces $t(b) - s(b) = 0$, esto implica que $p(x) \mid t(x) - s(x)$, por lo tanto $t(a) - s(a) = 0$ y $t(a) = s(a)$. Finalmente, $\sigma(c) = c$ para todo $c \in k$ y si consideramos el polinomio $q(x) = x \in k[x]$, entonces $\sigma(a) = \sigma(q(a)) = q(b) = b$. □

**Teorema 1.4.3.** *Sea $p(x) \in k[x]$ no constante e irreducible. Entonces existe una extensión $K$ de $k$ que contiene una raíz de $p(x)$. Si $K$ y $L$ son extensiones de $k$ que contienen raíces $a$ y $b$ de $p(x)$ respectivamente, entonces existe un $k-isomorfismo$ $\sigma : k(a) \longrightarrow k(b)$ tal que $\sigma(a) = b$.*

*Demostración.* Sea $K = k[x]/\langle p(x)\rangle$, el cual es campo pues $p(x)$ es irreducible. Demostraremos que $K$ es dicha extensión, primero mostraremos que el homomorfismo $i : k \hookrightarrow K$ dado por $i(a) = a+\langle p(x)\rangle$ es inyectivo y por lo tanto podemos ver a $k$ como un subcampo de $K$, identificando cada elemento $a$ de $k$ con $a+\langle p(x)\rangle$ de $K$ . Sean $a+\langle p(x)\rangle, b+\langle p(x)\rangle \in K$ tales que $a + \langle p(x)\rangle = b + \langle p(x)\rangle$, esto pasa si y sólo si $a - b \in \langle p(x)\rangle$, lo que implica que $p(x) \mid a - b$, lo cual es posible si y sólo si $a = b$ ya que $p(x)$ no es constante. Por lo tanto $K$ es una extensión de $k$. Ahora sea $\overline{x} = x + \langle p(x)\rangle \in K$ y $p(x) = a_n x^n + \cdots + a_0$. Entonces,

$$\begin{aligned} p(\overline{x}) &= a_n\overline{x}^n + \cdots a_1\overline{x} + a_0 \\ &= \overline{a_n} \cdot \overline{x}^n + \cdots \overline{a_1} \cdot \overline{x} + \overline{a_0} \\ &= \overline{p(x)} \\ &= \overline{0}. \end{aligned}$$

Por lo tanto $K$ tiene una raíz de $p(x)$. La demostración de la otra parte del teorema es por el teorema 1.4.2. □

**Definición 1.4.4.** *Decimos que $f(x) \in k[x]$ se descompone en $K[x]$, donde $K$ es una extensión de campos sobre $k$, si*

$$f(x) = c(x - a_1)\cdots(x - a_n)$$

*donde $c, a_1, a_2, \ldots, a_n \in K$.*

**Definición 1.4.5.** *Sea $f(x) \in k[x]$. Decimos que una extensión $K/k$ es un campo de descomposición de $f(x)$ sobre $k$, si $f(x)$ se descompone en $K[x]$ y $K = k(a_1, a_2, \ldots, a_n)$.*

Demostraremos la existencia de un campo de descomposición para cualquier polinomio. Pera eso utilizaremos los siguientes lemas:

**Lema 1.4.6.** *Si $k$ y $k'$ son campos isomorfos, entonces $k[x]$ y $k'[x]$ son isomorfos.*

*Demostración.* Sea $\sigma$ el isomorfismo entre $k$ y $k'$. Definamos $\overline{\sigma} : k[x] \longrightarrow k'[x]$ dado por $\overline{\sigma}(a_n x^n + \cdots + a_0) = \sigma(a_n)x^n + \cdots + \sigma(a_0)$. Sean $a_n x^n + \cdots + a_0, b_m x^m + \cdots + b_0 \in k[x]$ con $m \geq n$, entonces

$$\begin{aligned} \overline{\sigma}((a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_0)) &= \overline{\sigma}(b_m x^m + \cdots + (a_n + b_n)x^n + \cdots + (a_0 + b_0)) \\ &= \sigma(b_m)x^m + \cdots + \sigma(a_n + b_n)x^n + \cdots + \sigma(a_0 + b_0) \\ &= \sigma(b_m)x^m + \cdots + \sigma(a_n)x^n + \sigma(b_n)x^n + \cdots + \sigma(a_0) + \sigma(b_0) \\ &= \overline{\sigma}(a_n x^n + \cdots + a_0) + \overline{\sigma}(b_m x^m + \cdots + b_0) \end{aligned}$$

$$\begin{aligned}
\overline{\sigma}((a_nx^n+\cdots+a_0)\cdot(b_mx^m+\cdots+b_0)) &= \overline{\sigma}\left(\sum_{k=0}^{n+m}\left(\sum_{i+j=k}a_ib_j\right)x^k\right)\\
&= \sum_{k=0}^{n+m}\sigma\left(\left(\sum_{i+j=k}a_ib_j\right)\right)x^k\\
&= \sum_{k=0}^{n+m}\left(\sum_{i+j=k}\sigma\left(a_ib_j\right)\right)x^k\\
&= \sum_{k=0}^{n+m}\left(\sum_{i+j=k}\sigma(a_i)\sigma(b_j)\right)x^k\\
&= (\sigma(a_n)x^n+\cdots+\sigma(a_0))\cdot(\sigma(b_m)x^m+\cdots+\sigma(b_0))\\
&= \overline{\sigma}(a_nx^n+\cdots+a_0)\cdot\overline{\sigma}(b_mx^m+\cdots+b_0).
\end{aligned}$$

De ahí que $\overline{\sigma}$ sea un homomorfismo. Es inyectivo, ya que si $\overline{\sigma}(a_nx^n+\cdots+a_0)=0$, entonces $\sigma(a_n)x^n+\cdots+\sigma(a_0)=0$, lo que implica que $\sigma(a_i)=0$ para toda $i$, y como $\sigma$ es isomorfismo, entonces $a_i=0$. Claramente en un homomorfismo suprayectivo ya que $\sigma$ es suprayectiva. □

**Lema 1.4.7.** *Sea $\sigma : k \longrightarrow k'$ un isomorfismo de campos. Si $p(x)\in k[x]$ es un polinomio irreducible, entonces $\overline{\sigma}(p(x))\in k'[x]$ es un polinomio irreducible. Si $a\in K$ raíz de $p(x)$ y $b\in L$ es una raíz de $\overline{\sigma}(p(x))$, entonces existe un isomorfismo $\phi : k(a)\longrightarrow k'(b)$, tal que $\phi\mid_k=\sigma$ y $\phi(a)=b$.*

*Demostración.* Por el lema anterior $k[x]\cong k'[x]$. Para fines prácticos denotaremos por $(\sigma p)(x)$, donde $p(x)\in k[x]$, al homomorfismo $\overline{\sigma}(p(x))$ del lema 1.4.6. Definamos el homomorfismo $\phi : k(a)\longrightarrow k'(b)$ de la siguiente forma: para $q(a)\in k(a)$, donde $q(x)\in k[x]$ y $q(x)=0$ o $grq(x)<grIrr(k,a)=p(x)$, sea

$$\phi(q(a))=(\sigma q)(b).$$

Sean $(\sigma f)(x),(\sigma g)(x)\in k'[x]$ tales que $(\sigma p)(x)=(\sigma f)(x)(\sigma g)(x)$, lo que implica que $p(x)=f(x)g(x)$, luego $f(x)$ es constante o $g(x)$ es constante, ya que $p(x)$ es irreducible y como $\sigma(c)\in k'$ para todo $c\in k$, entonces $(\sigma f)(x)$ es constante o $(\sigma g)(x)$ es constante. Por lo tanto $(\sigma p)(x)$ es irreducible en $k'[x]$. Ahora mostraremos que $\phi$ es un isomorfismo. Sean $t(a),s(a)\in k(a)$, entonces $gr\left(t(x)+s(x)\right)<grp(x)$ y por lo tanto

$$\begin{aligned}
\phi(t(a)+s(a)) &= \phi((t+s)(a))\\
&= (\sigma(t+s))(b)\\
&= (\sigma(t)+\sigma(s))(b)\\
&= (\sigma t)(b)+(\sigma s)(b)\\
&= \phi(t(a))+\phi(s(a)).
\end{aligned}$$

Sean $q(x), h(x) \in k[x]$, tales que $t(x)s(x) = q(x)p(x) + h(x)$ con $grh(x) < grp(x)$, esto implica que $t(a)s(a) = q(a)p(a) + h(a)$ y como $p(a) = 0$, entonces $t(a)s(a) = h(a) \in k(a)$. Así,

$$\begin{aligned}\phi(t(a)s(a)) &= \phi(h(a)) \\ &= (\sigma h)(b) \\ &= (\sigma t)(b)(\sigma s)(b) \\ &= \phi(t(a))\phi(s(a)).\end{aligned}$$

Es un homomorfismo suprayectivo ya que $\sigma$ es un isomorfismo. Es inyectivo pues si $(\phi t)(b), (\phi s)(b) \in k'(b)$ son tales que $(\phi t)(b) = (\phi s)(b)$, entonces $(\phi t - \phi s)(b) = (\phi(t - s))(b) = 0$, esto implica que $(\sigma p)(x) \mid (\phi(t - s))(x)$, por lo tanto $p(x) \mid (t - s)(x)$, lo que implica que $(t - s)(a) = 0$ y $t(a) = s(a)$. Finalmente, para todo $c \in k$, se tiene que $\phi(c) = (\sigma c)(b) = \sigma(c)(b) = \sigma(c)$ y si consideramos el polinomio $q(x) = x \in k[x]$, entonces

$$\phi(a) = \phi(q(a)) = (\sigma q)(b) = b.$$

□

**Teorema 1.4.8.** *Todo polinomio no constante $f(x) \in k[x]$ tiene un campo de descomposición sobre $k$ y cualesquiera dos campos de descomposición de $f(x)$ sobre $k$ son $k - isomorfos$.*

*Demostración.* Para demostrar que existe un campo de descomposición de un polinomio $f(x) \in k[x]$, basta con demostrar que existe una extensión $K$ de $k$ que contiene todas las raíces de $f(x)$, el campo de descomposición que buscamos es el subcampo de $K$ que se obtiene al agregar todas las raíces de $f(x)$ a $k$.

Sea $n = grf(x)$, haremos la demostración por inducción sobre $n$. Si $n = 1$, es claro que $K = k$. Supongamos que para todo polinomio de grado mayor que 1 y menor que $n$ con coeficientes en algún campo $L$, existe una extensión $F$ de $L$, tal que $f(x)$ se descompone en $F[x]$. Consideremos el caso en el que $f(x)$ es reducible en $k[x]$, es decir, $f(x) = g(x)h(x)$ con $g(x), h(x) \in k[x]$ y $grg(x) < n$ y $grh(x) < n$. Por nuestra hipótesis de inducción, se sigue que existe una extensión $L$ de $k$ tal que $g(x)$ se descompone en $L[x]$. Luego $h(x) \in k[x] \subseteq L[x]$ y por nuestra hipótesis de inducción existe una extensión $K$ de $L$ tal que $h(x)$ se descompone en $K[x]$. Por lo tanto, $f(x)$ y $g(x)$ se descomponen en $K[x]$. Ahora supongamos que $f(x)$ es irreducible en $k[x]$, entonces por el Teorema 1.4.3 existe una extensión $L$ de $k$ que contiene una raíz $a$ de $f(x)$. Luego $f(x) = (x - a)g(x) \in L[x]$ y $grg(x) = n - 1$. Por la hipótesis de inducción existe una extensión $K$ de $L$ tal que $g(x)$ se descompone en $K$. Por lo tanto $f(x)$ se descompone en $K$.

Sean $K$ y $L$ dos campos de descomposición de $f(x) \in k[x]$ y $p(x) \in k[x]$ un polinomio no constante e irreducible que divide a $f(x)$. Sean $a_1 \in K$ y $b_1 \in L$ raíces del polinomio

$p(x)$. Entonces, por el Teorema 1.4.3, existe un $k - isomorfismo\ \sigma : k(a_1) \longrightarrow k(b_1)$ tal que $\sigma(a_1) = (b_1)$. Supongamos que

$$f(x) = (x - a_1) \cdots (x - a_r)g(x) \in k(a_1)[x]$$

donde $g(x)$ no tiene raíces en $k(a_1)$. Por el Lema 1.4.6, $k(a_1)[x] \cong k(b_1)[x]$ y $(\sigma f)(x) = (x - \sigma(a_1)) \cdots (x - \sigma(a_r))(\sigma g)(x) \in k(b_1)[x]$. Sean $b_i = \sigma(a_i)$. Supongamos que $c \in k(b_1)$ es raíz de $(\sigma f)$. Como $\sigma$ es isomorfismo, entonces existe $d \in k(a_1)$ tal que $\sigma(d) = c$, lo que implica

$$0 = (\sigma f)(c) = (\sigma f)(\sigma(d)) = \sigma(f(d)).$$

Luego $f(d) = 0$, por lo que $d = a_i$ para alguna $i$. Por lo tanto $(\sigma g)(x)$ no tiene raíces en $k(b_1)[x]$.

Si $g(x)$ es un polinomio constante, entonces $K = k(a_1)$ y $L = k(b_1)$ y habremos terminado. De lo contrario, existe $q(x) \in k(a_1)[x]$ irreducible tal que $q(x) \mid g(x)$. Por el lema 1.4.7, $(\sigma q)(x) \in k(b_1)[x]$ es un factor irreducible de $(\sigma g)(x)$. Sean $a_{r+1} \in K$ y $b_{r+1} \in L$ raíces de $q(x)$ y de $(\sigma q)(x)$ respectivamente, por el lema 1.4.7, existe un isomorfismo $\phi : k(a_1, a_{r+1}) \longrightarrow k(b_1, b_{r+1})$, tal que $\phi(c) = \sigma(c)$ para toda $c \in k(a_1)$. Procediendo recursivamente, obtendremos un isomorfismo $\rho : k(a_1, \ldots, a_n) \longrightarrow k(b_1, \ldots, b_n)$ tal que $\rho(a_i) = b_i$ y $\rho \mid_k = 1_k$. □

**Definición 1.4.9.** *Decimos que una extensión $K$ de $k$ es una extensión normal si es algebraica sobre $k$ y si todo polinomio irreducible en $k[x]$ que posee una raíz en $K$ se descompone en $K[x]$.*

**Teorema 1.4.10.** *Sea $K$ el campo de descomposición sobre $k$ del polinomio $f(x) \in k[x]$. Entonces $K$ es una extensión normal de $k$.*

*Demostración.* Sea $f(x) \in k[x]$ y sean $a_1, \ldots, a_n \in K$ las raíces de $f(x)$ y $K = k(a_1, \ldots, a_n)$. Sea $p(x) \in k[x]$ irreducible y sea $b \in K$ una de sus raíces. Sea $L$ un campo de descomposición de $p(x)$ sobre $K$ y $b' \in L$ otra de sus raíces. Por el teorema 1.4.2, existe un $k - isomorfismo$ $\sigma$ de $k(b)$ en $k(b')$ tal que $\sigma(b) = (b')$. Es fácil ver que $K$ es un campo de descomposición de $f(x)$ sobre $k(b)$ y que $K(b')$ es campo de descomposición de $f(x)$ sobre $k(b')$ y haciendo ciertas adaptaciones del teorema 1.4.8, tenemos que existe un isomorfismo $\tau : K \longrightarrow K(b')$ tal que $\tau|_{k(b)} = \sigma$. En particular $\tau(b) = \sigma(b) = b'$ y $f(\tau(a_i)) = \tau(f(a_i)) = \tau(0) = 0$ para toda $i$, por lo que las $\tau(a_i)$ son una permutación de las raíces $a_1, \ldots, a_n$ de $f(x)$ que pertenecen a $K$. Luego, como $b \in k(a_1, \ldots, a_n)$ entonces $b = g(a_1, \ldots, a_n)$ donde $g(x) \in k[x]$, esto implica que

$$\begin{aligned} b' &= \tau(b) \\ &= \tau(g(a_1, \ldots, a_n)) \\ &= g(\tau(a_1), \ldots, \tau(a_n)) \in K. \end{aligned}$$

Por lo tanto $p(x)$ se descompone en $K$. □

**Teorema 1.4.11.** *Sea $K$ una extensión normal finita de $k$. Entonces $K$ es campo de descomposición de algún polinomio en $k[x]$.*

*Demostración.* Como $K/k$ es una extensión de campos finita, entonces $K = k(a_1, \ldots, a_n)$ con $a_1, \ldots, a_n \in K$. Sean $f_i(x) = Irr(k, a_i)$. Sea

$$f(x) = f_1(x) \cdots f_n(x).$$

Como $K/k$ es una extensión normal entonces cada $f_i(x)$ se descompone en $K$, por lo tanto $f(x)$ de descompone en $K$ y además $K = k(a_1, \ldots, a_n) = k(a_1, \ldots, a_n, b_1, \ldots, b_m)$ donde $b_1, \ldots, b_m$ son el resto de las raíces de $f(x)$. Por lo tanto $K$ es campo de descomposición de $f(x)$. □

**Teorema 1.4.12.** *Sea $K$ una extensión finita de $k$. Entonces existe una extensión normal finita $F$ de $k$ que contiene a $K$ y que además es mínima en el sentido de que si $L$ es otra extensión normal finita de $k$ que contiene a $K$, entonces $F$ y $L$ son $K - isomorfos$.*

*Demostración.* Como $K/k$ es una extensión de campos finita, entonces $K = k(a_1, \ldots, a_n)$ con $a_1, \ldots, a_n \in K$. Sea

$$f(x) = f_1(x) \cdots f_n(x)$$

donde $f_i(x) = Irr(k, a_i)$ para $i = 1, \ldots, n$. Se sigue que $f(x) \in K[x]$. Sea $F$ un campo de descomposición de $f(x)$ sobre $K$, en consecuencia por el teorema 1.4.10 $F/k$ es una extensión normal que contiene a $K$ y es finita pues $F$ se obtiene al agregar las raíces de $f(x)$. Sea $L/k$ otra extensión normal finita que contiene a $K$, esto implica que $f_i(x)$ se descompone en $L[x]$ pues $a_i \in L$ para cada $i \in \{i, \ldots, n\}$, por lo tanto $F$ y $L$ son campos de descomposición de $f(x)$ y por el teorema 1.4.8 son $K - isomorfos$. □

## 1.5. Campos finitos

Definimos el campo primo de un campo $k$ como la intersección de todos sus subcampos, es decir, el subcampo más pequeño que contiene $k$. Empezaremos denotándolo por $\Delta$.

Definamos la función $\phi : \mathbb{Z} \longrightarrow k$ dado por $\phi(n) = n \cdot 1 = 1 + \cdots + 1$. Es fácil ver que $\phi$ es un homomorfismo de anillos cuya imagen está contenida en $\Delta$, ya que $1 \in \Delta$.

A continuación, enunciaremos un teorema que nos permite caracterizar el campo primo de un campo.

**Teorema 1.5.1.** *El campo primo de un campo $k$ es isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}_p$, para algún $p$ primo.*

*Demostración.* Para la demostración de este teorema consideraremos los siguientes casos:

1. $ker\phi = \langle 0 \rangle$: esto implica que $\Delta$ contiene un subanillo $R$ isomorfo a $\mathbb{Z}$. Luego $\Delta$ contiene un campo isomorfo al campo de cocientes del anillo $R$ que es isomorfo $\mathbb{Q}$. Por definición de campo primo, se tiene que $\Delta \cong \mathbb{Q}$.

2. $ker\phi \neq \langle 0 \rangle$: como $\mathbb{Z}$ es DIP, entonces $ker\phi = \langle p \rangle$. Luego $\mathbb{Z}/\langle p \rangle$ es isomorfo a un subanillo $R$ de $\Delta$ y por tanto es un dominio entero. Entonces $\langle p \rangle$ es un ideal primo lo que implica que $p$ es primo. Por otro lado, $\mathbb{Z}/\langle p \rangle$ también es campo, ya que $\mathbb{Z}$ es DFU. Luego $R$ es campo y por definición de campo primo se tiene $\Delta \cong \mathbb{Z}/\langle p \rangle = \mathbb{Z}_p$.

□

**Definición 1.5.2.** *Decimos que un campo $k$ es de característica $p$, $p$ primo, si $\Delta \cong \mathbb{Z}_p$. Si $\Delta \cong \mathbb{Q}$, entonces diremos que es de característica 0. Denotaremos la característica de un campo por $car(k)$.*

**Observación 1.5.3.** *Si $car(k) = 0$, entonces para toda $a \in k$ y para toda $n \in \mathbb{N}$ tales que $na = 0$ se tiene que $n = 0$ o $a = 0$.*

*Si $car(k) = p$ y $na = 0$, entonces $p \mid n$ o $a = 0$.*

Sea $K$ un campo finito. Si $\text{car}(K) = 0$, entonces $K$ contendría un subcampo isomorfo a $\mathbb{Q}$ que es infinito, contradiciendo que $K$ es finito. Por lo tanto todo campo finito es de característica $p$.

Sea $K$ un campo finito de característica $p$. De aquí en adelante denotaremos por $GF(p)$ al campo primo de $K$. Como $K$ y $GF(p)$ son finitos, entonces $K/GF(p)$ es una extensión finita.

**Teorema 1.5.4.** *Si $K$ es un campo finito de característica $p$ y $[K : GF(p)] = n$, entonces $K$ tiene $p^n$ elementos. Cualesquiera dos campos con $p^n$ elementos son isomorfos.*

*Demostración.* Sea $a_1, \ldots, a_n$ una base de $K$ sobre $GF(p)$. Por lo que

$$K = \{c_1a_1 + \cdots + c_na_n \mid c_i \in GF(p)\}.$$

Como $|GF(p)| = p$, cada $c_i$ tiene $p$ posibilidades y por lo tanto $K$ tiene $p^n$ elementos.

Sean $\{b_1, \ldots, b_{p^n}\}$ todos los elementos de $K$. Si consideramos el grupo multiplicativo de orden $h = p^n - 1$, de todos los elementos de $K$ distintos de cero, entonces tenemos que $b_i^h = 1$, lo que implica $b_i^{p^n} = (b_i^{p^n-1})(b_i) = b_i$. Por lo tanto, el polinomio $f(x) = x^{p^n} - x \in GF(p)[x]$ tiene $p^n$ raíces en $K$. Esto implica que $K$ es campo de descomposición de $f(x)$ y además es el mínimo campo que contiene todas su raíces. Por lo tanto, por el Teorema 1.4.8, cualquier campo de descomposición de $f(x)$ es isomorfo a $K$ y cualquier campo con $p^n$ elementos es campo de descomposición del polinomio $f(x)$. □

**Teorema 1.5.5.** *El grupo multiplicativo de un campo finito es cíclico.*

*Demostración.* Sea $K$ un campo finito con $p^n$ elementos. Sea

$$K_p = \{c \in K \mid c \neq 0\}.$$

El grupo multiplicativo $K_p$ es de orden $h = p^n - 1 = q_1^{r_1} \cdots q_m^{r_m}$, con cada $q_i$ primo y $q_i \neq q_j$ si $i \neq j$. Sea $h_i = h/q_i$ para cada $i = 1, \ldots, m$. Como $h_i < h$ existe $b_i \in K$ que no es raíz

del polinomio $f(x) = x^{h_i} - 1$, es decir, $b_i^{h_i} \neq 1$. Sean $a_i = b_i^{h/q_i^{r_i}}$ y $a = a_1 \cdots a_m$. Luego $a_i^{q_i^{r_i}} = b_i^h = 1$, por ser $K_p$ un grupo de orden $h$. Esto implica que el orden de $a_i$ divide a $q_i^{r_i}$. Supongamos que el orden de $a_i$ es $q_i^{r_i-1}$, entonces

$$1 = a_i^{q_i^{r_i-1}} = \left(b_i^{h/q_i^{r_i}}\right)^{q_i^{r_i-1}} = b_i^{h/q_i}$$

lo que contradice la elección de $b_i$.

Afirmamos que el orden de $a$ es $h$. Denotemos por $O(a)$ al orden de $a$ y supongamos que $O(a) \neq h$. Como $a^h = 1$, entonces $O(a) \mid h$. Luego existe un factor primo $q_1$ de $h$, tal que $q_1^{r_1} \mid h$ pero $q_1^{r_1} \nmid O(a)$. Entonces $a^{h/q_1} = 1$. Esto implica que $a^{h/q_1} = a_1^{h/q_1} \cdots a_m^{h/q_1}$. Como $q_i^{r_i} \mid h/q_1$ para $i = 2, \ldots, m$, entonces $a_i^{h/q_1} = 1$. Luego $a_1^{h/q_1} = 1$, por lo que $q_1^{r_1}$ que es el orden de $a_1$, divide a $h/q_1$ lo cual es falso. Por lo tanto $O(a) = h$ y por lo tanto $K_p$ es un grupo cíclico. □

## 1.6. Extensiones separables y puramente inseparables

**Definición 1.6.1.** *Sea $K$ un extensión de $k$ y sea $a \in K$ algebraico sobre $k$. Decimos que $a$ es **separable** sobre $k$ si es raíz simple de $Irr(k, a)$. Decimos que $K/k$ es una **extensión separable** si es algebraica y todo elemento en $K$ es separable sobre $k$.*

**Proposición 1.6.2.** *Sea $K/k$ una extensión separable y $k \subseteq L \subseteq K$. Entonces $K/L$ es una extensión separable.*

*Demostración.* Sea $a \in K$ y $p(x) = Irr(L, a)$. Si $q(x) = Irr(k, a)$, entonces $p(x) \mid q(x)$. Como $K/k$ es separable entonces $a$ es raíz de multiplicidad 1 de $q(x)$. Luego $a$ es raíz de multiplicidad 1 de $p(x)$. Por lo tanto $K/L$ es separable. □

**Definición 1.6.3.** *Sea $K$ una extensión de $k$ y $a \in K$ algebraico sobre $k$. Decimos que $a$ es **puramente inseparable** sobre $k$ si $p(x) = Irr(k, a) = (x - a)^m$ para alguna $m > 0$.*

**Definición 1.6.4.** *Una extensión $K/k$ de campos es puramente inseparable sobre $k$ si es finita y cada uno de sus elementos es puramente inseparable sobre $k$.*

**Teorema 1.6.5.** *Sea $a \in K$ puramente inseparable sobre $k$ un campo de característica $p > 0$. Entonces existe un entero $e \geq 0$ tal que $gr(Irr(k, a)) = p^e$ y además $a^{p^e} \in k$ pero $a^{p^f} \notin k$ para $0 \leq f < e$.*

*Demostración.* Sea $mp^e$ el grado del polinomio $p(x) = Irr(k, a)$, con $(m, p) = 1$. Luego

$$p(x) = (x - a)^{mp^e} = \left((x - a)^{p^e}\right)^m = \left(x^{p^e} - a^{p^e}\right)^m$$

por ser $a$ puramente inseparable y $k$ de característica $p$. Esto implica que uno de los coeficientes de $p(x)$ es $ma^{p^e}$ y como $p(x) \in k[x]$, entonces $ma^{p^e} \in k$. Luego $a^{p^e} \in k$, ya que $(m, p) = 1$, y $x^{p^e} - a^{p^e} \in k[x]$. Esto implica que $m = 1$, de lo contrario $x^{p^e} - a^{p^e} \in k[x]$ divide a $p(x)$ que es irreducible en $k[x]$. Si $a^{p^f} \in k$ para $0 \leq f < e$, entonces $x^{p^f} - a^{p^f} \in k[x]$ dividiría a $p(x)$ que es irreducible en $k[x]$. □

**Corolario 1.6.6.** *Si $K/k$ es una extensión de campos finita, puramente inseparable y $k$ de característica $p > 0$, entonces $[k : k] = p^e$ para algún entero positivo $e$.*

*Demostración.* Sean $a_1, \ldots, a_n \in K$ tales que $K = k(a_1, \ldots, a_n)$. Entonces podemos obtener $K$ con la siguiente torre de campos $k_1 = k(a_1)$, $k_2 = k_1(a_2)$, ..., $K = k_n = k_{n-1}(a_n)$. Demostraremos que $a_i$ es puramente inseparable sobre $k_{i-1}$ para $i = 2, \ldots, n$. Sea $p(x) = Irr(k, a_i)$ y $q_i(x) = Irr(k_{i-1}, a_i)$. Entonces $q_i(x) \mid p(x)$. Esto implica que $q_i(x) = (x - a)^{r_i}$ pues $a$ es puramente inseparable. Luego $a_i$ es puramente inseparable sobre $k_{i-1}$. Por el teorema 1.6.5 $[k_i : k_{i-1}] = p^{r_i}$. Por lo tanto

$$[K : k] = \prod_{i=1}^{n} [k_i : k_{i-1}] = p^r.$$

□

El siguiente par de teoremas no se demuestran. La demostración puede verse en [1].

**Teorema 1.6.7.** *Si $a_1, \ldots, a_n \in K$ son separables sobre $k$, entonces $k(a_1, \ldots, a_n)$ es una extensión separable sobre $k$.*

**Teorema 1.6.8.** *Sea $K$ una extensión algebraica sobre un campo $k$. Entonces $K$ se puede obtener por medio de una extensión separable seguida de una extensión puramente inseparable.*

## 1.7. Teorema del elemento primitivo

Sea $K/k$ una extensión normal y finita, denotaremos por $G(K/k)$ al conjunto de todos los $k - automorfismos$ de $K$, esto es

$$G(K/k) = \{\sigma : K \longrightarrow K \mid \sigma \text{ es isomorfismo y } \sigma|_k = Id_k\}$$

$G(K/k)$ con la composición entre $k - automorfismos$ es un grupo donde $1_k$ es el neutro multiplicativo.

**Observación 1.7.1.** *$G(K/k)$ es un grupo finito.*

*Demostración.* Como $K$ es una extensión normal y finita, entonces es campo de descomposición de algún polinomio $f(x) \in k[x]$ (teorema 1.4.11) y $K = k(a_1, a_2, \ldots, a_n)$ donde $a_1, a_2, \ldots, a_n$ son todas las raíces de $f(x)$ en $K$. Luego para todo $\sigma \in G(K/k)$ se tiene $0 = \sigma(f(a_i)) = f(\sigma(a_i))$ para toda $i$, por lo que $\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)$ es una permutación de las raíces $a_1, a_2, \ldots, a_n$. Por otro lado, los $k - automorfismos$ están determinados por la acción de las $a_1, a_2, \ldots, a_n$ pues éstas froman una base de $K$. Por lo tanto $G(K/k)$ tiene a lo más $n!$ $k - automorfismos$. □

**Lema 1.7.2.** *Si $K/k$ es una extensión finita y separable, entonces existe un número finito de subcampos entre $K$ y $k$.*

*Demostración.* Por el teorema 1.4.12 existe una extensión finita y normal $F$ de $k$ tal que $k \subseteq K \subseteq F$. Sea $K = k(a_1, \ldots, a_n)$. En la demostración del teorema 1.4.12 vimos que $F$ es el campo de descomposición del polinomio $f(x) = \prod_{i=1}^{n} f_i(x)$, donde $f_i(x) = Irr(k, a_i)$, para $i = 1, \ldots, n$. Como $K/k$ es separable, entonces cada raíz de $f(x)$ es separable y por el teorema **??**, la extensión $F/k$ es separable. Consideremos el grupo $G(F/k)$ que por la observación 1.7.1 es un grupo finito. Sea $L$ un campo tal que $k \subseteq L \subseteq F$. $G(F/L)$ es un subgrupo de $G(F/k)$, ya que si $\sigma \in G(F/L)$ es un $F - automorfismo$ que deja fijo a $L$, entonces también deja fjo a $k$. Mostraremos que existe una correspondencia inyectiva entre los subcampos intermedios de $F$ y $k$ y los subgrupos de $G(F/k)$.

Sea $M \neq L$ un subcampo intermedio de $F$ y $k$. Demostraremos que $G(F/M) \neq G(F/L)$. Sin pérdida de generalidad, podemos suponer que existe $a \in M - L$. Como $F/k$ es separable, entonces $F/L$ también es separable. Por lo que $Irr(L, a)$ tiene al menos una raíz $a' \in F$ distinta de $a$. Entonces existe $\sigma \in G(F/L)$ tal que $\sigma(a) = a'$. Por lo tanto $\sigma \notin G(F/M)$ y $G(F/L) \neq G(F/M)$. Como $G(F/k)$ es finito, sólo tiene un número finito de subgrupos, por lo que existe sólo un número finito de campos entre $F$ y $k$. Si $L$ es un campo intermedio de $K$ y $k$, entonces también es un campo intermedio de $F$ y $k$. Por lo tanto existe sólo un número finito de campos entre $K$ y $k$. □

**Teorema 1.7.3.** *Toda extensión finita y separable $K$ de $k$ es simple, es decir, existe $a \in K$ tal que $K = k(a)$.*

*Demostración.* Si $k$ es finito, entonces $K$ también es finito y por el teorema 1.5.5, su subgrupo multiplicativo es cíclico. Sea $a$ el generador del grupo multiplicativo. Entonces $K = k(a)$.

Supongamos que $k$ es infinito. Sean $a, b \in K$. Consideremos el campo $k(a + cb)$ con $c \in k$. Claramente $k(a + cb) \subseteq k(a, b)$. Mostraremos que se da la otra contención. Como $k$ es un campo infnito y por el lema 1.7.2, entre $K$ y $k$ sólo existe un número finito de campos intermedios, entonces existe $d \in k$ y $d \neq c$ tal que $k(a + cb) = k(a + db)$. Luego $a + db \in k(a + cb)$. Esto implica que $(a + cb) - (a + db) = (c - d)b \in k(a + cb)$ y así $b \in k(a + cb)$ y por lo tanto $a = (a + cb) - cb \in k(a + cb)$. Por lo tanto $k(a, b) \subseteq k(a + cb)$ y así se obtiene la igualdad.

Esta demostración se hizo para cuando la extensión es de la forma $k(a_1, a_2)$, pero si tenemos una extensión de la forma $k(a_1, \ldots, a_n)$ aplicamos el mismo procedimiento de manera inductiva a los campos $k = k_0$ y $k_i = k_{i-1}(a_i)$ con $i \in \{1, \ldots, n\}$. □

# Capítulo 2

# Localización

**Definición 2.0.4.** *Sea $R$ un dominio entero. Sea $S \subsetneq R$, $S \neq \emptyset$ y que no contiene al 0. Diremos que $S$ es un subconjunto multiplicativo de $R$, si para toda $x, y \in S$ se tiene que $xy \in S$.*

A continuación demostraremos que existe un anillo $R_S$, que contiene a $R$ y a los inversos multiplicativos de los elementos de $S$. Se puede construir este anillo definiendo una relación de equivalencia de la siguiente forma $(r, s)$ $(r', s')$ si y sólo si $rs' = r's$. Y cada elemento de $R_S$ es una clase de equivalencia inducida por la relación. Sin embargo, en esta tesis demostraremos la existencia de este anillo como sigue:

**Proposición 2.0.5.** *Sea $R$ un dominio entero y $S$ un subconjunto multiplicativo de $R$. Entonces existe un anillo al cual denotaremos por $R_S$, que contiene un subanillo isomorfo a $R$ y a los inversos multiplicativos de todos los elementos de $S$, además $R_S$ está generado por $R$ y por $s^{-1}, s \in S$.*

*Demostración.* Sea $K$ el campo de cocientes de $R$. Definimos

$$R_S = \left\{ \frac{r}{s} : r \in R, s \in S \right\}$$

demostraremos que $R_S$ es un subanillo de $K$.

En efecto, para cualesquiera $\frac{r}{s}, \frac{r'}{s'} \in R_S$ se tiene que

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \in R_S$$
$$\frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'} \in R_S$$

$\frac{0}{s} \in R_S$ que es el cero de $K$ y $\frac{s}{s} \in R_S$ que es el neutro multiplicativo de $K$. Para ver que $R$ es isomorfo a un subanillo de $R_S$ identificamos a cada $r \in R$ con el elemento $\frac{rs}{s} \in R_S$, con $s \in S$. Nótese que esta inclusión es inyectiva pues si $\frac{rs}{s} = \frac{r's}{s}$, entonces $rs^2 = r's^2$ y

en consecuencia $r = r'$. Ésto implica que $R \subseteq R_S$. Por otro lado, para toda $t \in S$ tenemos que $t\frac{1}{t} = \frac{1}{1}$ la identidad de $R_S$, es decir, $t$ es invertible en $R_S$. □

A continuación haremos algunas observaciones sobre el anillo $R_S$:

**Observación 2.0.6.** *Sea $T$ un anillo y $\phi : R \to T$ un homomorfismo de anillos tal que todo elemento de $\phi(S)$ es invertible en $T$. Entonces existe un único homomorfismo de anillos $\Phi : R_S \to T$ tal que $\Phi|_R = \phi$.*

*En efecto, definamos $\Phi\left(\frac{r}{s}\right) = \frac{\Phi(r)}{\Phi(s)}$. Mostremos que $\Phi$ es homomorfismo*

$$\begin{aligned}
\Phi\left(\frac{r}{s} + \frac{r'}{s'}\right) &= \Phi\left(\frac{rs' + sr'}{ss'}\right) \\
&= \frac{\phi(r)\phi(s') + \phi(s)\phi(r')}{\phi(s)\phi(s')} \\
&= \frac{\phi(r)}{\phi(s)} + \frac{\phi(r')}{\phi(s')} \\
&= \Phi\left(\frac{r}{s}\right) + \Phi\left(\frac{r'}{s'}\right) \\
\Phi\left(\frac{r}{s}\frac{r'}{s'}\right) &= \Phi\left(\frac{rr'}{ss'}\right) \\
&= \frac{\phi(rr')}{\phi(ss')} \\
&= \frac{\phi(r)}{\phi(s)}\frac{\phi(r')}{\phi(s')} \\
&= \Phi\left(\frac{r}{s}\right)\Phi\left(\frac{r'}{s'}\right) \\
\Phi(1) &= 1.
\end{aligned}$$

*Para toda $r \in R$ se tiene que*

$$\Phi(r) = \Phi\left(\frac{rs}{s}\right) = \frac{\phi(rs)}{\phi(s)} = \frac{\phi(r)\phi(s)}{\phi(s)} = \phi(r).$$

*Esto nos dice que $R_S$ es el anillo más chico que contine a $R$ y a los inversos multiplicativos de $S$.*

**Observación 2.0.7.** *Sea $\widehat{S} = S \cup \{1\}$. Entonces $R_S \cong R_{\widehat{S}}$*

*Demostración.* Definamos $\phi : R \to R_{\widehat{S}}$ por $\phi(r) = \frac{r}{1}$, claramente $\phi$ es un homomorfismo inyectivo y además cada elemento de $\phi(S)$ es invertible. Definamos el homomorfismo $\Phi$ como en la observación anterior. Demostraremos que $\Phi$ es un isomorfismo. En efecto, sean

$\frac{r}{s}, \frac{r'}{s'} \in R_S$ tales que $\Phi\left(\frac{r}{s}\right) = \Phi\left(\frac{r'}{s'}\right)$, esto implica que $\frac{\phi(r)}{\phi(s)} = \frac{\phi(r')}{\phi(s')}$, luego $\phi(r)\phi(s') = \phi(r')\phi(s)$ y así $\phi(rs') = \phi(r's)$, por lo que $rs' = r's$, por lo tanto $\frac{r}{s} = \frac{r'}{s'}$. Ahora sea $\frac{r'}{\widehat{s}} \in R_{\widehat{S}}$. Si $\widehat{s} \in S$, entonces $\Phi\left(\frac{r'}{\widehat{s}}\right) = \frac{r'}{\widehat{s}}$ y si $\widehat{s} = 1$, entonces $\Phi(r') = \phi(r') = r'$ y por lo tanto $\Phi$ es suprayectivo. □

*Esto muestra que podemos suponer que* $1 \in S$*, así que de aquí en adelante consideraremos que* $1 \in S$*.*

**Definición 2.0.8.** *Sea* $R$ *un dominio entero y* $S$ *un subconjunto multiplicativo de* $R$*. Definimos la localización de* $R$ *en* $S$ *como el anillo* $R_S$ *de la Proposición 2.0.5.*

Ahora demostraremos un resultado que nos permite establecer la relación que existe entre los ideales del anillo $R$ y los ideales de su localizado $R_S$; en especial cuando los ideales son primos.

**Proposición 2.0.9.** *Sea* $R$ *un dominio entero y* $S$ *un subconjunto multiplicativo de* $R$*.*

1. *Si* $\mathfrak{q}$ *es un ideal de* $R_S$*, entonces* $\mathfrak{q} \cap R$ *es un ideal de* $R$ *y* $(\mathfrak{q} \cap R)R_S = \mathfrak{q}$*, lo que significa que la correspondencia* $\mathfrak{q} \xrightarrow{\phi} \mathfrak{q} \cap R$ *entre los ideales de* $R_S$ *y los ideales de* $R$ *es inyectiva y además preserva la inclusión.*

2. *La correspondencia restringida a los ideales primos de* $R_S$ *es biyectiva sobre los ideales primos* $\mathfrak{p}$ *de* $R$ *tales que* $\mathfrak{p} \cap S = \emptyset$*. En este caso la aplicación inversa es* $\mathfrak{p} \mapsto \mathfrak{p}R_S$*.*

*Demostración.* 1. Sea $\mathfrak{q}$ ideal de $R_S$. Para demostrar que $\phi$ es inyectiva, demostraremos que la aplicación $\mathfrak{q} \mapsto \mathfrak{q} \cap R \mapsto (\mathfrak{q} \cap R)R_S$ es la identidad, lo que nos lleva a mostrar que $(\mathfrak{q} \cap R)R_S = \mathfrak{q}$. En efecto, como $(\mathfrak{q} \cap R) \subseteq \mathfrak{q}$, entonces $(\mathfrak{q} \cap R)R_S \subseteq \mathfrak{q}R_S = \mathfrak{q}$. Ahora sea $\frac{q}{s} \in \mathfrak{q}$ con $q \in R$ y $s \in S$. Luego $q = \frac{q}{s}s \in \mathfrak{q} \cap R$, por lo que $q\frac{1}{s} \in (\mathfrak{q} \cap R)R_S$. Por lo tanto $\phi$ es inyectiva y claramente preserva la inclusión.

2. Notemos que si $\mathfrak{q}$ es un ideal primo de $R_S$, entonces $\mathfrak{q} \cap R$ es un ideal primo de $R$ tal que $(\mathfrak{q} \cap R) \cap S = \emptyset$, pues para $a, b \in R$ tales que $ab \in \mathfrak{q} \cap R$ se tiene que $a \in \mathfrak{q} \cap R$ o $b \in \mathfrak{q} \cap R$, por ser $\mathfrak{q}$ un ideal primo de $R_S$. Por otro lado, si $x \in (\mathfrak{q} \cap R) \cap S$, entonces $1 = x\frac{1}{x} \in \mathfrak{q}$, por lo que $\mathfrak{q} = R_S$, pero esto no es posible pues $\mathfrak{q}$ es un ideal primo. Por lo tanto $(\mathfrak{q} \cap R) \cap S = \emptyset$

   Ahora sea $\mathfrak{p}$ ideal primo de $R$ tal que $\mathfrak{p} \cap S = \emptyset$ y sea $\mathfrak{q} = \mathfrak{p}R_S$. Mostremos que $\mathfrak{q}$ es ideal primo de $R_S$: sean $\frac{r}{s}, \frac{r'}{s'} \in R_S$ tales que $\frac{r}{s}\frac{r'}{s'} \in \mathfrak{q}$, entonces $\frac{rr'}{ss'} = \frac{p}{\widehat{s}}$ con $p \in \mathfrak{p}$ y $\widehat{s} \in S$, luego $(rr')\widehat{s} = p(ss') \in \mathfrak{p}$, por lo que $rr' \in \mathfrak{p}$ pues $\widehat{s} \notin \mathfrak{p}$, esto implica que $r \in \mathfrak{p}$ o $r' \in \mathfrak{p}$, por lo tanto $\frac{r}{s} \in \mathfrak{p}R_S$ o $\frac{r'}{s'} \in \mathfrak{p}R_S$.

   Mostremos que $\mathfrak{q} \cap R = \mathfrak{p}$: primero como $\mathfrak{p} \subset \mathfrak{p}R_S = \mathfrak{q}$, entonces $\mathfrak{p} = \mathfrak{p} \cap R \subset \mathfrak{q} \cap R$. Ahora sea $u = \frac{x}{s} \in \mathfrak{q} \cap R$ con $x \in \mathfrak{p}$ y $s \in S$, luego $us = x \in \mathfrak{p}$, esto implica que $u \in \mathfrak{p}$ pues $s \notin \mathfrak{p}$.

   □

**Proposición 2.0.10.** *Sea $R$ un dominio entero, $S$ un subconjunto multiplicativo de $R$ y $\mathfrak{p}$ un ideal maximal de $R$ tal que $\mathfrak{p} \cap S = \emptyset$. Entonces $R/\mathfrak{p} \cong R_S/\mathfrak{p}R_S$.*

*Demostración.* Definamos

$$\phi : R/\mathfrak{p} \to R_S/\mathfrak{p}R_S$$

por

$$\phi\left(r + \mathfrak{p}\right) = r + \mathfrak{p}R_S.$$

Es claro que $\phi$ es un homorfismo de anillos. Mostremos que es inyectivo. Sea $r+\mathfrak{p} \in R/\mathfrak{p}$ tal que $\phi\left(r + \mathfrak{p}\right) = \overline{0}$, entonces $r \in \mathfrak{p}R_S$, por lo que $r = \frac{x}{s}$ con $x \in \mathfrak{p}$ y $s \notin \mathfrak{p}$, luego $rs = x \in \mathfrak{p}$ y como $\mathfrak{p}$ es primo y $s \notin \mathfrak{p}$, entonces $r \in \mathfrak{p}$, es decir, $r + \mathfrak{p} = 0 + \mathfrak{p}$.

Ahora veamos que $\phi$ es suprayectivo. Sea $\frac{r}{s} \in R_S$. Como $\mathfrak{p}$ es un ideal maximal, entonces $\mathfrak{p} + \langle s\rangle = R$, por lo que existe $q \in R$, $q \neq 0$ y $p \in \mathfrak{p}$ tal que $p + qs = 1$, lo que implica que $q = \frac{1-p}{s}$. Luego

$$\begin{aligned}
\phi(rq + \mathfrak{p}) &= rq + \mathfrak{p}R_S \\
&= r\frac{1-p}{s} + \mathfrak{p}R_S \\
&= \frac{r}{s} - \frac{rp}{s} + \mathfrak{p}R_S \\
&= \frac{r}{s} + \mathfrak{p}R_S.
\end{aligned}$$

Por lo tanto $\phi$ es un isomorfismo. □

**Proposición 2.0.11.** *Si $S$ es un subconjunto multiplicativo en un dominio entero noetheriano $R$, entonces $R_S$ también es un dominio noetheriano.*

*Demostración.* Sea $\mathfrak{q}$ un ideal de $R_S$. Entonces, por la Proposición 2.0.9, $\mathfrak{q} \cap R = \mathfrak{p}$ es un ideal de $R$ que es un dominio noetheriano, por lo tanto $\mathfrak{p}$ es finitamente generado. Sean $a_1, a_2, \ldots, a_n \in R$ tales que $\mathfrak{p} = \langle a_1, a_2, \ldots, a_n\rangle$, entonces $\mathfrak{q} = \mathfrak{p}R_S = \langle a_1, a_2, \ldots, a_n\rangle R_S$ y $\langle a_1, a_2, \ldots, a_n\rangle R_S$ es un ideal de $R_S$ finitamente genereado. Por lo tanto $R_S$ es un dominio entero noetheriano. □

## 2.1. Localización de ideales primos

A continuación exhibiremos el ejemplo más importante de localización y analizaremos algunas de sus propiedades. Sea $\mathfrak{p}$ un ideal primo de un anillo $R$ y sea $S = R-\mathfrak{p}$. Observemos que ser un ideal primo es equivalente a que $R - \mathfrak{p}$ sea un subconjunto multiplicativamente cerrado, pues si $\mathfrak{p}$ es un ideal primo de $R$ y $a, b \in R - \mathfrak{p} = S$ pero $ab \notin S$, entonces $ab \in \mathfrak{p}$, por lo que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$ lo cual es una contradicción. Inversamente, si $S$ es un subconjunto multiplicativamente cerrado y $ab \in \mathfrak{p}$ pero $a \notin \mathfrak{p}$ y $b \notin \mathfrak{p}$, entonces $a, b \in S$ por lo que $ab \in S$, lo cual es una contradicción.

**Definición 2.1.1.** *Definimos la localización de $R$ en $\mathfrak{p}$, a la cual denotaremos por $R_\mathfrak{p}$, como el anillo $R_{R-\mathfrak{p}}$. Es decir,*

$$R_\mathfrak{p} = \left\{ \frac{a}{b} \mid a, b \in R, b \notin \mathfrak{p} \right\}.$$

**Proposición 2.1.2.** *Si $\mathfrak{p}$ es ideal primo de un dominio entero $R$, entonces la localización $R_\mathfrak{p}$ posee un único ideal maximal, que es $\mathfrak{p}R_\mathfrak{p}$.*

*Demostración.* Supongamos que $\mathfrak{q}$ es un ideal maximal de $R_\mathfrak{p}$ distinto de $\mathfrak{p}R_\mathfrak{p}$. Entonces $\mathfrak{q}$ es un ideal primo de $R_\mathfrak{p}$. Por la proposición 2.0.9, $\mathfrak{q}' = \mathfrak{q} \cap R$ es un ideal primo de $R$ distinto de $\mathfrak{p}$, por lo que existe $x \in \mathfrak{q}' - \mathfrak{p} \subseteq R - \mathfrak{p}$, lo cual implica que $x$ es invertible en $R_\mathfrak{p}$ y $x \in \mathfrak{q}$. Luego $\mathfrak{q} = R_\mathfrak{p}$ que no puede ser. Por lo tanto el único ideal maximal de $R_\mathfrak{p}$ es $\mathfrak{p}R_\mathfrak{p}$. □

## 2.2. Anillos locales

**Definición 2.2.1.** *Decimos que un anillo conmutativo $R$ es un anillo local si posee un único ideal maximal.*

**Ejemplo 2.2.2.** *Sea $R$ un dominio entero y $\mathfrak{p}$ un ideal primo de $R$. Por la Proposición 2.1.2 $R_\mathfrak{p}$ es un anillo local.*

**Lema 2.2.3.** *Sea $R$ un anillo local y $\mathfrak{p}$ su único ideal maximal. Entonces todo elemento de $R - \mathfrak{p}$ es invertible. En particular si $m \in \mathfrak{p}$, entonces $1 + m$ es invertible.*

*Demostración.* Sea $x \in R - \mathfrak{p}$. Luego $\langle x \rangle \nsubseteq \mathfrak{p}$ que es el único ideal maximal propio y como todo ideal propio debe estar contenido en algún ideal maximal , entonces $\langle x \rangle = R$. Por lo tanto existe $y \in R$ tal que $xy = 1$.

Ahora si $m \in \mathfrak{p}$ entonces $1 + m \notin \mathfrak{p}$, pues de lo contrario $1 \in \mathfrak{p}$ lo cual no es posible. Por lo tanto $1 + m$ es invertible. □

**Proposición 2.2.4.** *Sea $R$ un anillo local, $\mathfrak{p}$ su único ideal maximal y $M$ un $R$ módulo finitamente generado tal que $\mathfrak{p}M = M$. Entonces $M = 0$.*

*Demostración.* Sea $\{m_1, m_2, \ldots, m_n\}$ un conjunto generador de $M$. Como $\mathfrak{p}M = M$, entonces para cada $i \in \{1, 2, \ldots, n\}$ se tiene que

$$m_i = \sum_{j=1}^{n} a_{ij} m_j$$

con $a_{ij} \in \mathfrak{p}$. Esto nos lleva a el sistema de ecuaciones lineales

$$\begin{aligned} a_{11}x_1 - 1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 - 1 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{n1} + a_{n2}x_2 + \cdots + a_{nn}x_n - 1 &= 0 \end{aligned}$$

cuya matriz asociada es

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

y donde $\overline{m} = (m_1, m_2, \ldots, m_n)$ es un vector solución no trivial, es decir, $A\overline{m}^t = 0$. Mostraremos que, al igual que en el caso en que $R$ es campo, el determinante de $A$ es distinto de cero.

Sea $B$ la matriz adjunta de $A$, entonces

$$BA = det(A)I_n$$

donde $I_n$ es la matriz identidad de orden n. Entonces

$$\begin{aligned} (0, 0, \ldots, 0) = BA\overline{m}^t &= det(A)I_n\overline{m}^t \\ &= d\overline{m}^t \\ &= (dm_1, \ldots, dm_n) \end{aligned}$$

donde $d = det(A)$. Como $\{m_1, \ldots, m_n\}$ es un conjunto generador, entonces $dM = 0$. Por otro lado, al desarrollar el determinante de $A$ obtenemos productos y sumas de elementos de la forma $a_{ij}$ con elementos de la forma $1 - a_{kk}$ y $a_{ij}$ y como $\mathfrak{p}$ es un ideal de $R$, entonces $d = 1 + u$ con $u \in \mathfrak{p}$. Por lo tanto, por el lema 2.2.3, $d$ es invertible en $R$ y en consecuencia $d \neq 0$.

Así $dM = 0$ y $d \neq 0$ implica que $M = 0$. □

**Corolario 2.2.5** (LEMA DE NAKAYAMA)**.** *Sea $R$ un anillo local, $\mathfrak{p}$ su único ideal maximal y $M$ un $R$ módulo finitamente generado. Sea $L$ un submódulo de $M$ tal que $L + \mathfrak{p}M = M$. Entonces $L = M$.*

*Demostración.* Sea $m + L \in M/L$. Como $L + \mathfrak{p}M = M$, entonces $m = l + pm_0$ con $l \in L$ y $pm_0 \in \mathfrak{p}M$. Por lo que

$$m + L = l + pm_0 + L = pm_0 + L$$

y así $M/L \subseteq \mathfrak{p}\,(M/L)$ y claramente $\mathfrak{p}\,(M/L) \subseteq M/L$. Luego $\mathfrak{p}\,(M/L) = M/L$ y como $M$ es finitamente generado, entonces $M/L$ también lo es. Por la proposición 2.2.4 $M/L = 0$ y por lo tanto $M = L$ □

# Capítulo 3

# Dependencia Entera

**Definición 3.0.6.** *Sean $R \subseteq R'$ anillos. Decimos que $b \in R'$ es entero sobre $R$ si existe un polinomio mónico $f(x) \in R[x]$ tal que $f(b) = 0$.*

Por ejemplo, $i = \sqrt{-1}$ es entero sobre $\mathbb{Z}$, pues es raíz del polinomio $x^2 + 1$.
Sea $b \in R'$ entero sobre $R$. Denotaremos por $R[b]$ al conjunto

$$\left\{ a_0 b^0 + \cdots + a_n b^k \mid a_0, \ldots, a_n \in R, k \in \mathbb{N} \right\}.$$

Es fácil ver que $R[b]$ es un subanillo de $R'$.

**Proposición 3.0.7.** *Sea $R$ un subanillo de $R'$ y sea $b \in R'$. Entonces son equivalentes:*

1. *$b$ es entero sobre $R$.*

2. *$R[b]$ es un $R$ módulo finitamente generado.*

3. *$R[b]$ está contenido en un subanillo $B$ de $R'$ que además es un $R$ módulo finitamente generado.*

4. *Existe un $R[b]$ módulo $M$ que como $R$ módulo es finitamente generado y tal que si $y \in R[b]$ y $yM = 0$, entonces $y = 0$.*

*Demostración.* 1) $\Longrightarrow$ 2) Sea $f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_o$, con $\alpha_i \in R$ tal que $f(b) = 0$.

Esto implica que $b^n = \sum_{i=0}^{n-1} a_i b^i$, con $a_i = -\alpha_i$ luego

$$\begin{aligned} b^{n+1} &= bb^n \\ &= b\sum_{i=0}^{n-1} a_i b^i \\ &= a_{n-1}b^n + \sum_{i=0}^{n-2} a_i b^{i+1} \\ &= a_{n-1}\sum_{i=0}^{n-1} a_i b^i + \sum_{i=0}^{n-2} a_i b^{i+1} \\ &= \sum_{i=0}^{n-1} c_i b^i \end{aligned}$$

y de la misma manera se obtiene que $b^k = \sum_{i=0}^{n-1} \alpha_i b^i$ para toda $k \geq n$ y con $\alpha_i \in R$. Por lo tanto $R[b]$ es un $R$ módulo finitamente generado con $1, b, \ldots, b^{n-1}$ como generadores.

2) $\Longrightarrow$ 3) Como $R \subseteq R[b] \subseteq R'$, basta tomar $B = R[b]$ que es un $R$ módulo finitamente generado.

3) $\Longrightarrow$ 4) Como $R[b] \subseteq B$ y $B$ es un $R$ módulo finitamente generado, entonces $B$ es un $R[b]$ módulo, por lo que haremos $B = M$. Sea $y \in R[b]$ tal que $yM = 0$, como $1 \in M$, entonces $y = y1 = 0$.

4) $\Longrightarrow$ 1) Sea $M$ generado por $\{m_1, m_2, \ldots, m_n\}$ como $R$ módulo. Entonces para cada $i = 1, \ldots, n$ se tiene que

$$bm_i = \sum_{j=1}^{n} r_{ij} m_j$$

con $r_{ij} \in R$ y $0 \leq i \leq n$ . Esta expresión puede verse como un sistema de ecuaciones lineales homogéneo cuya matriz asociada está dada por $A = bI_n - [r_{ij}]$, donde $I_n$ es la matriz identidad de $n \times n$ y $\overline{m} = (m_1, \ldots, m_n)$ es un vector solución, es decir, $A\overline{m}^t = \overline{0}$. Ahora sea $B$ la matriz adjunta de $A$ y sea $d = det(A)$, entonces $BA = dI_n$ lo que implica que

$$\overline{0} = BA\overline{m}^t = dI_n\overline{m}^t = d\overline{m}.$$

Por lo que $dM = 0$ que por hipótesis implica $d = 0$. Ahora $f(x) = det(xI_n - [r_{ij}])$ es un polinomio mónico con coeficientes en $R$ tal que $f(b) = det(A) = d = 0$. Por lo tanto $b$ es entero sobre $R$. □

**Proposición 3.0.8.** *Sean $b_1, \ldots, b_n \in R'$ enteros sobre $R$. Entonces el subanillo $R[b_1, \ldots, b_n]$ de $R'$ es un $R$ módulo finitamente generado.*

*Demostración.* Haremos la demostración por inducción sobre $n$. Para $n = 1$ es el caso del inciso 2. de la proposición 3.0.7. Supongamos que se cumple para $n - 1 \geq 0$, es decir, supongamos que $R[b_1, \ldots, b_{n-1}] = R''$ es un $R$ módulo finitamente generado y sean $a_1, \ldots, a_t$ sus generadores. Como $b_n$ es entero sobre $R$ también es entero sobre $R''$ , por el inciso 2 de la proposición 3.0.7, $R''[b_n]$ es un $R''$ módulo finitamente generado con $1, b_n, \ldots, b_n^k$ para alguna $k$ como generadores. Mostremos que los elementos de la forma $a_i b_n^j$ forman un conjunto generador. Si $x \in R''[b_n]$, entonces $x = \sum_{j=1}^{k} y_j b_n^j$ con $y_j \in R''$ y por otro lado, si $y_j \in R''$, entonces $y_j = \sum_{i=1}^{t} r_i a_i$ con $r_i \in R$, esto implica que

$$\begin{aligned} x &= \sum_{j=1}^{k} y_j b_n^j \\ &= \sum_{j=1}^{k} \left( \sum_{i=1}^{t} r_i a_i \right) b_n^j \\ &= \sum_{j=1}^{k} \sum_{i=1}^{t} r_i a_i b_n^j \end{aligned}$$

por lo que $a_i b_n^j$ es un conjunto generador y $R''[b_n] = R[b_1, \ldots, b_n]$ es un $R$ módulo finitamente generado. □

**Teorema 3.0.9.** *El conjunto de elementos de $R'$ que son enteros sobre $R$ es un subanillo de $R'$ que contiene a $R$.*

*Demostración.* Sean $x, y \in R'$ enteros sobre $R$. Por la proposición anterior $R[x, y]$ es un $R$ módulo finitamente generado. Además $x \pm y \in R[x, y]$ y $xy \in R[x, y]$, por lo que $R[x \pm y] \subseteq R[x, y]$ y $R[xy] \subseteq R[x, y]$. Luego por el inciso tres de la proposición 3.0.7 $x \pm y$ y $xy$ son enteros sobre $R$ y el conjunto de elementos enteros sobre $R$ es un subanillo de $R'$ que claramente contiene a $R$, pues todo elemento de $R$ es entero sobre $R$. □

Ahora estudiaremos el caso en el que $R$ es un dominio entero y $R' = K$ su campo de cocientes. Empecemos con la siguiente definición:

**Definición 3.0.10.** *Sea $R$ un dominio entero y $K$ su campo de cocientes. Llamaremos cerradura entera de $R$ en $K$ al conjunto de elementos en $K$ enteros sobre $R$. Si $R$ es igual a su cerradura entera, diremos que $R$ es enteramente cerrado.*

A continuación veremos algunos resultados y ejemplos de dominios enteramente cerrados. Empezaremos con la siguiente proposición y su corolario que nos permiten obtener dominios enteramente cerrados a partir de la cerradura entera de un dominio en su campo de cocientes.

**Proposición 3.0.11.** *Sean $R \subseteq R' \subseteq R''$ anillos tales que $R''$ es entero sobre $R'$ y $R'$ entero sobre $R$. Entonces $R''$ es entero sobre $R$.*

*Demostración.* Sea $b \in R''$. Como $R''$ es entero sobre $R'$, existe un polinomio mónico

$$f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0$$

con $r_i \in R'$, tal que $f(b) = 0$. Ya que $R'$ es entero sobre $R$, el anillo $B = R[r_0, \ldots, r_{n-1}]$ es un $R$ módulo finitamente generado (proposición 3.0.8). Luego $B[b]$ es un $R$ módulo finitamente generado pues si $y \in B[b]$ entonces $y = g(b)$ con $g(x) \in R[r_0, \ldots, r_{n-1}][x]$ y como $B$ es un $R$ módulo finitamente generado, entonces $B[b]$ es un $R$ módulo finitamenete generado. Finalmente $R[b] \subseteq B[b]$ y por el tercer inciso de la proposicion 3.0.7, $b$ es entero sobre $R$. □

**Corolario 3.0.12.** *La cerradura entera $R'$ de un dominio entero $R$ es enteramente cerrada.*

*Demostración.* Sea $R''$ la cerradura entera de $R'$. Entonces por la proposición 3.0.11 $R''$ es entero sobre $R$, esto implica que $R'' \subseteq R'$ y por lo tanto $R'' = R'$. Luego la cerradura entera de un dominio es enteramente cerrada. □

**Ejemplo 3.0.13.** *Todo DFU es enteramente cerrado.*

*Demostración.* Sea $R$ un DFU y $\frac{x}{y}$ un elemento de su campo de cocientes, entero sobre $R$. Como $R$ es un DFU, podemos suponer que los únicos factores en común de $x$ y $y$ son unidades. Como $\frac{x}{y}$ es entero, tenemos la siguiente expresión

$$\left(\frac{x}{y}\right)^n = \sum_{i=0}^{n-1} r_i \left(\frac{x}{y}\right)^i$$

donde $r_i \in R$ con $i = 1, \ldots, n-1$. Multiplicando ambos lados de la expresión por $y^n$ se obtiene

$$x^n = y \sum_{i=0}^{n-1} r_i x^i y^{n-1-i}$$

lo que implica que $y$ divide a $x^n$ y como la descomposición en primos es única entonces se tendría que cualquier primo que divide a $y$ también divide a $x^n$ y en consecuencia a $x$. Pero supusimos que los únicos factores en común de $x$ y $y$ eran unidades, entonces $y \in U(R)$ y por lo tanto $\frac{x}{y} = xy^{-1} \in R$. Por lo tanto todo DFU es enteramente cerrado. □

**Ejemplo 3.0.14.** *Todo DIP es enteramente cerrado. Esto se debe a que todo DIP es DFU.*

**Ejemplo 3.0.15.** *Sea $R$ enteramente cerrado y sea $S \subseteq R$ un subconjunto multiplicativo. Entonces el localizado $R_S$ es enteramente cerrado.*

*Demostración.* Sea $u$ un elemento del campo de cocientes de $R_S$ entero sobre $R_S$. Entonces existe un polinomio mónico

$$f(x) = x^n + \frac{\rho_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{\rho_0}{s_0}$$

tal que $f(u) = 0$, con $r_i, s_i \in R$. Multiplicando cada término, tanto en el numerador como en el denominador, de la expresión por $\overline{s}_i = s_0 \cdots s_{i-1}s_{i+1} \cdots s_{n-1}$, se obtiene un polinomio de la forma

$$x^n + \frac{r_{n-1}}{s}x^{n-1} + \cdots + \frac{r_0}{s}$$

donde $s = s_0 \cdots s_{n-1}$ y $r_i \in R$, que sigue teniendo a $u$ como raíz. Por lo que

$$u^n + \frac{r_{n-1}}{s}u^{n-1} + \cdots + \frac{r_0}{s} = 0$$

multiplicando este polinomio por $s^n$ obtenemos

$$(su)^n + r_{n-1}(su)^{n-1} + r_{n-2}s(su)^{n-2} + \cdots + r_0 s^{n-1} = 0.$$

Esto implica que $su$ es raíz de un polinomio mónico con coeficientes en $R$, que es enteramente cerrado, por lo que $su \in R$. Luego $u = \frac{su}{s} \in R_S$ y por lo tanto $R_S$ es enteramente cerrado. □

**Ejemplo 3.0.16.** *El anillo $\mathbb{Z}[\sqrt{5}]$, que es un dominio entero cuyo campo de cocientes es $\mathbb{Q}\left[\sqrt{5}\right]$ no es enteramente cerrado, ya que $\frac{1}{2}\left(1+\sqrt{5}\right) \in \mathbb{Q}\left[\sqrt{5}\right] - \mathbb{Z}[\sqrt{5}]$ es raíz del polinomio $f(x) = x^2 - x - 1 = \left(x - \frac{1}{2}(1+\sqrt{5})\right)\left(x - \frac{1}{2}(1-\sqrt{5})\right)$.*

**Proposición 3.0.17.** *Sea $K$ el campo de cocientes de una familia de dominios enteramente cerrados $\{R_i\}$. Entonces $\bigcap R_i$ es un dominio enteramente cerrado.*

*Demostración.* Sea $b \in K$ entero sobre $R = \bigcap R_i$. Entonces $b$ es raíz de un polinomio

$$f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0$$

con $r_j \in R$. Luego cada $r_j \in R_i$, para toda $i$ y para toda $j \in \{0, \ldots, n-1\}$, por lo que $b$ es entero sobre cada $R_i$, que al ser enteramente cerrados se tiene que $b \in R_i$ para toda $i$, lo que implica $b \in \bigcap R_i$. Por lo tanto $\bigcap R_i$ es enteramente cerrado. □

**Proposición 3.0.18.** *Sea $R$ un dominio entero, $K$ su campo de cocientes y $L$ una extensión de campos sobre $K$. Sea $b \in L$ algebraico sobre $K$ y sea $f(x) = Irr(K, b)$. Si $b$ es entero sobre $R$, entonces los coeficientes de $f(x)$ son enteros sobre $R$. Si $R$ es enteramente cerrado, entonces $b$ es entero sobre $R$ si y sólo si $f(x) \in R[x]$.*

*Demostración.* Sea $L'$ un campo de decomposición de $f(x)$ que contiene a $L$ y sean $b = b_1, \ldots, b_n$ las raíces de $f(x)$. Supongamos que $b$ es entero sobre $R$. Entonces existe un polinomio mónico $g(x) \in R[x]$ tal que $g(b) = 0$. Como $f(x) = Irr(K, b)$, entonces $f(x)$ divide a $g(x)$ y por lo tanto todas las raíces $b_1, \ldots, b_n$ de $f(x)$ son raíces de $g(x)$, lo que implica que cada $b_i$ es entero sobre $R$. Por lo tanto los coeficientes de $f(x)$ que son sumas y productos de las $b_i$ son enteros sobre $R$.

Si $R$ es enteramente cerrado entonces $b_1, \ldots, b_n \in R$ y por lo tanto $f(x) \in R[x]$. □

Este resultado nos dice que para determinar si un elemento es entero se puede recurrir al polinomio mínimo irreducible. Una aplicación de este último resultado nos lo da la siguiente proposición.

**Proposición 3.0.19.** *Sea $d$ un número entero libre de cuadrados. Entonces la cerradura entera de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{d}]$ es:*

1. $\mathbb{Z} + \mathbb{Z}[\sqrt{d}]$ *si* $d \equiv 2, 3$ *mod 4*
2. $\frac{1}{2}\left(\mathbb{Z} + \mathbb{Z}[\sqrt{d}]\right)$ *si* $d \equiv 1$ *mod 4*

*Demostración.* Podemos suponer que un elemento en $\mathbb{Q}[\sqrt{d}]$ es de la forma $\frac{a+b\sqrt{d}}{c}$ con $a, b, c \in \mathbb{Z}$ y tales que $(a, b, c) = 1$. Si $\frac{a+b\sqrt{d}}{c}$ es entero sobre $\mathbb{Z}$, entonces los coeficientes de su polinomio irreducible $f(x)$ sobre $\mathbb{Q}$ son enteros sobre $\mathbb{Z}$, por la proposición 3.0.18, pero $\mathbb{Z}$ es enteramente cerrado pues es un DFU, por lo tanto los coeficientes de $f(x)$ deben ser números enteros. Luego

$$f(x) = \left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right) = x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 d}{c^2}$$

y por lo mencionado anteriormente se tiene que $\frac{2a}{c}, \frac{a^2-b^2d}{c^2} \in \mathbb{Z}$.

Si $(a, c) \neq 1$, entonces existe $e \in \mathbb{Z}$ tal que $e \mid a$, $e \mid c$ y $e \neq 1$. Lo cual implica que $e^2 \mid c^2$ y en consecuencia $e^2 \mid a^2 - b^2 d$. Además $e^2 \mid a^2$ y por lo tanto $e^2 \mid b^2 d$. Como $d$ es libre de cuadrados, entonces $e \mid b$, lo que contradice que $(a, b, c) = 1$, por lo tanto $(a, c) = 1$. Como $c \mid 2a$ y $(a, c) = 1$, entonces $c = 1$ o $c = 2$.

Si $c = 1$, entonces los coeficientes de $f(x)$ pertenecen a los números enteros para cualquier elección de $d$. Analicemos el caso en el que $c = 2$ y $a$ y $b$ son impares, pues supusimos que $(a, b.c) = 1$. El cuadrado de un número impar es de la forma $(2k + 1)^2 = 4k^2 + 4k + 1$, esto implica que $a^2 \equiv 1 \equiv b^2 \bmod 4$. Luego $0 \equiv a^2 - b^2 d \equiv 1 - d \bmod 4$ y por lo tanto $d \equiv 1 \bmod 4$.

Supongamos $d \equiv 1 \bmod 4$. Si $a$ y $b$ son impares, entonces $a^2 - b^2 d \equiv 0 \bmod 4$ y $\frac{a^2-b^2d}{c^2} \in \mathbb{Z}$ tanto para el caso $c = 1$ como para el caso $c = 2$ que son los únicos posibles. El caso $a$ impar y $b$ par, implica $a^2 - b^2 d \equiv 1 \bmod 4$, por lo que $\frac{a^2-b^2d}{c^2} \in \mathbb{Z}$ sólo para el caso

$c = 1$. Ya habíamos observado que el caso $a$ par y $c = 2$ no es posible, esto implica que si $a$ es par, entonces $c = 1$ y por lo tanto $\frac{a^2-b^2d}{c^2} \in \mathbb{Z}$.

Supongamos que $d \equiv 2 \mod 4$, $\frac{a^2-b^2d}{c^2} \in \mathbb{Z}$ y $c = 2$. Si $a$ y $b$ son impares, entonces $0 \equiv a^2 - b^2d \equiv -1 \mod 4$, que es una contradicción. Si $a$ es impar y $b$ par, entonces $0 \equiv a^2 - b^2d \equiv 1$, que es una contradicción. Supongamos que $d \equiv 3 \mod 4$, $\frac{a^2-b^2d}{c^2} \in \mathbb{Z}$ y $c = 2$. Si $a$ y $b$ son impares, entonces $0 \equiv a^2 - b^2d \equiv 2 \mod 4$, que es una contradicción. Si $a$ es impar y $b$ par, entonces $0 \equiv a^2 - b^2d \equiv 1$, que es una contradicción. Por lo tanto, si $d = 2, 3$, entonces $c = 1$.

□

# Capítulo 4

# Anillos de Dedekind

En este capítulo empezaremos el estudio de los anillos de Dedekind que es el tema principal de esta tesis. Pero primero hablaremos de anillos de valuación discreta.

**Definición 4.0.20.** *Sea $R$ un anillo. Decimos que $R$ es un* ***Dominio de Valuación Discreta (DVD)*** *si es un dominio de ideales principales que contiene un sólo ideal maximal.*

A continuación demostraremos algunas propiedades de los DVD y los ejemplos nos los darán los anillos de Dedekind más adelante.

**Proposición 4.0.21.** *Sea $R$ un DVD que no es campo y sea $p \in R$ tal que $\mathfrak{p} = \langle p \rangle$ es el único ideal maximal de $R$. Entonces se cumplen los siguientes enunciados:*

1. *$R$ es un dominio noetheriano.*
2. *Todo elemento $x \in R$, $x \neq 0$ es de la forma $x = up^k$ con $u \in U(R)$, para alguna $k \in \mathbb{Z}$ no negativa.*
3. *Todo ideal $I$ no trivial es de la forma $I = \langle p^k \rangle$, para alguna $k \in \mathbb{Z}$ no negativa.*
4. *$R$ es enteramente cerrado.*
5. *$\mathfrak{p}$ es el único ideal primo no trivial.*

*Demostración.* 1. Por definición $R$ es DIP y todo DIP es noetheriano.

2. Sea $x \neq 0$, $x \in R$. Todo DIP es DFU por el teorema 1.2.17, por lo que existen $a_1, \ldots, a_k \in R$ elementos irreducibles tales que $x = \prod_{i=1}^{k} a_i^{r_i}$. Luego $a_i \mid x$, lo que implica que $\langle x \rangle \subseteq \langle a_i \rangle$ para toda $i = 1, \ldots, k$. Cada $\langle a_i \rangle$ está contenida en algún ideal maximal, en este caso el único ideal maximal es $\mathfrak{p}$, lo que implica que $\langle a_i \rangle \subseteq \langle p \rangle$, para toda $i = 1, \ldots, k$. Luego $p \mid a_i$, por lo tanto existe $u_i \in U(R)$ tal que $u_i p = a_i$, pues $a_i$ es irreducible para toda $i = 1, \ldots, k$. Por lo tanto $x = \prod_{i=1}^{k} u_i p = up^k$.

3. Sea $I$ ideal de $R$ que es DIP. Entonces $I = \langle x \rangle$ para alguna $x \in R$. Por el inciso anterior, $x = up^k$ con $u \in U(R)$, por lo tanto $I = \langle x \rangle = \langle up^k \rangle = \langle p^k \rangle$.

4. En el ejemplo 3.0.14 vimos que todo DIP es enteramente cerrado.

5. Sea $I = \langle p^k \rangle$ un ideal primo. Si $k > 1$, entonces $p \cdot p^{k-1} \in I$. Lo que implica $p \in I$ o $p^{k-1} \in I$, que es una contradicción. Por lo tanto $k = 1$ y entonces $I = \mathfrak{p}$.

□

**Definición 4.0.22.** *Decimos que un anillo $R$ es de **Dedekind**, si es un dominio entero noetheriano tal que para todo ideal primo $\mathfrak{p}$ no trivial la localización $R_\mathfrak{p}$ es un DVD.*

**Proposición 4.0.23.** *Sea $R$ un anillo de Dedekind. Entonces se cumplen los siguientes enunciados:*

1. *Todo ideal primo no trivial de $R$ es un ideal maximal.*

2. *Si $S$ es un subconjunto multiplicativo de $R$, entonces la localización $R_S$ es un anillo de Dedekind.*

*Demostración.* 1. Sea $\mathfrak{p}_1$ ideal primo no trivial de $R$. Entonces existe $\mathfrak{p}_2$ ideal maximal tal que $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$. Luego, $\mathfrak{p}_1 R_{\mathfrak{p}_2} \subseteq \mathfrak{p}_2 R_{\mathfrak{p}_2}$ es una cadena de ideales primos de $R_{\mathfrak{p}_2}$ que es DVD. Por la proposición 2.1.2, el único ideal maximal es $\mathfrak{p}_2 R_{\mathfrak{p}_2}$. Luego, por el inciso 5 de la proposición 4.0.21, el único ideal primo es $\mathfrak{p}_2 R_{\mathfrak{p}_2}$. Por lo tanto y debido a la correspondencia biyectiva que existe entre los ideales primos de $R_{\mathfrak{p}_2}$ y los ideales primos de $R$ cuya intersección con $R - \mathfrak{p}_2$ es vacía (proposición 2.0.9), $\mathfrak{p}_1 = \mathfrak{p}_2$.

2. En la proposición 2.0.11 demostramos que si $R$ es noetheriano, entonces $R_S$ también es un anillo noetheriano. Los ideales primos de $R_S$ son de la forma $\mathfrak{p}R_S$, donde $\mathfrak{p}$ es un ideal primo de $R$ tal que $\mathfrak{p} \cap S = \emptyset$. Para mostrar que $(R_S)_{\mathfrak{p}R_S}$ es un DVD, mostraremos que

$$R_\mathfrak{p} = (R_S)_{\mathfrak{p}R_S}\,.$$

Si $\frac{x}{y} \in (R_S)_{\mathfrak{p}R_S}$, entonces $x, y \in R_S$ y $y \notin \mathfrak{p}R_S$. Luego $x = \frac{x'}{s}$ y $y = \frac{y'}{s'}$ con $x', y' \in R$ y $s, s' \in S$ y además $\frac{y'}{s'} \notin \mathfrak{p}R_S$, lo que implica $y' \notin \mathfrak{p}$. Se sigue que

$$\frac{x}{y} = \frac{\frac{x'}{s}}{\frac{y'}{s'}} = \frac{x's'}{y's}$$

donde $x's, y's \in R$ y $y's \notin \mathfrak{p}$, de lo contrario $s \in \mathfrak{p}$ que no es posible pues $S \cap \mathfrak{p} = \emptyset$ o $y' \in \mathfrak{p}$ que no sucede. Por lo tanto $(R_S)_{\mathfrak{p}R_S} \subseteq R_\mathfrak{p}$.

Sea $\frac{x}{y} \in R_\mathfrak{p}$, donde $x, y \in R$ y $y \notin \mathfrak{p}$. Luego por la inclusión de $R$ en $R_S$ se tiene que $x, y \in R_S$ y $y \notin \mathfrak{p}R_S$ y esto implica que $\frac{x}{y} \in (R_S)_{\mathfrak{p}R_S}$.

□

## 4.1. Factorización en ideales primos

Los ejemplos de anillos de Dedekind los estudiaremos más adelante. En este capítulo estudiaremos algunas propiedades que nos serán de gran utilidad a lo largo de esta tesis, entre ellas que todo ideal de un anillo de Dedekind se puede factorizar como producto de ideales primos. Éste será el objetivo de esta sección.

**Definición 4.1.1.** *Sean $P$ y $Q$ ideales de un anillo $R$. Decimos que $P$ y $Q$ son co-maximales si $P + Q = R$.*

**Teorema 4.1.2** (Teorema Chino del Residuo para Anillos)**.** *Sean $Q_1, \ldots, Q_n$ ideales co-maximales dos a dos de un anillo $B$, es decir, $Q_i + Q_j = B$ para toda $i \neq j$. Sea $I = \bigcap_{i=1}^{n} Q_i$. Entonces el homomorfismo diagonal*

$$b \xrightarrow{\Delta} (b + Q_1, \ldots, b + Q_n)$$

*induce el siguiente isomorfismo de anillos*

$$B/I \cong B/Q_1 \oplus \cdots \oplus B/Q_n.$$

*Demostración.* Haremos la demostración por inducción sobre n. El caso $n = 1$ es trivial, por lo que haremos la demostración para $n = 2$. Sea $\Delta : B \to B/Q_1 \oplus B/Q_2$ dada por $\Delta(b) = (b + Q_1, b + Q_2)$. Luego $b \in ker(\Delta)$ si y sólo si $b \in I = Q_1 \cap Q_2$. Como $Q_1$ y $Q_2$ son co-maximales, existen $q_1 \in Q_1$ y $q_2 \in Q_2$ tales que $1 = q_1 + q_2$. Entonces para toda $b \in B$, $b = bq_1 + bq_2$ y

$$\Delta(bq_1) = (bq_1 + Q_1, bq_1 + Q_2) = (0 + Q_1, b(1 - q_2) + Q_2) = (0 + Q_1, b + Q_2).$$

Así que $\Delta(\langle q_1 \rangle) \cong B/Q_2$. Análogamente $\Delta(\langle q_2 \rangle) \cong B/Q_1$. Luego

$$\Delta(B) = \Delta(B(q_1 + q_2)) = \Delta(Bq_1 + Bq_2) = \Delta(\langle q_1 \rangle) + \Delta(\langle q_2 \rangle) \cong B/Q_1 \oplus B/Q_2.$$

Supongamos ahora que se cumple para $n - 1 \geq 2$ y demostremos que es válido para n. Sean $Q'_i = Q_i$ para toda $i < n - 1$ y sea $Q'_{n-1} = Q_n \cap Q_{n-1}$. Mostraremos que la hipótesis de inducción puede aplicarse a los ideales $Q'_j$. Se tiene que $\bigcap_{i=1}^{n} Q_i = \bigcap_{i=1}^{n-1} Q'_i$. Para toda $i \neq j$, $i, j < n - 1$ se cumple $Q'_i + Q'_j = Q_i + Q_j = B$. Mostremos que para toda $i < n - 1$, $Q'_i + Q'_{n-1} = B$. Tenemos que

$$\begin{aligned} B = B \cdot B &= (Q_n + Q_i)(Q_{n-1} + Q_i) \\ &\subseteq Q_n Q_{n-1} + Q_n Q_i + Q_i Q_{n-1} + Q_i \\ &\subseteq Q_n Q_{n-1} + Q_i \\ &\subseteq Q_n \cap Q_{n-1} + Q_i \\ &= Q'_{n-1} + Q'_i \subseteq B. \end{aligned}$$

Luego para toda $i < n-1$, $Q'_i + Q'_{n-1} = B$ . Por nuestra hipótesis de inducción

$$B/\bigcap_{i=1}^{n-1} Q'_i \cong B/Q'_1 \oplus \cdots \oplus B/Q'_{n-1}.$$

Por el caso $n = 2$, el homomorfismo

$$b \longrightarrow (b + Q_{n-1}, b + Q_n)$$

induce el isomorfismo $B/Q'_{n-1} \cong B/Q_{n-1} \oplus B/Q_n$. Por lo tanto

$$\begin{aligned} B/I &\cong B/Q'_1 \oplus \cdots \oplus B/Q'_{n-1} \\ &= B/Q_1 \oplus \cdots \oplus B/Q_{n-2} \oplus B/Q'_{n-1} \\ &\cong B/Q_1 \oplus \cdots \oplus B/Q_{n-2} \oplus B/Q_{n-1} \oplus B/Q_n. \end{aligned}$$

□

**Teorema 4.1.3** (Teorema Chino del Residuo para Módulos)**.** *Sean $Q_1, \ldots, Q_n$ ideales co-maximales dos a dos de un anillo $B$. Sean $I = \bigcap_{i=1}^{n} Q_i$ y $M$ un $B$ módulo izquierdo. Entonces el homomorfismo diagonal*

$$m \xrightarrow{\overline{\Delta}} (m + Q_1M, \ldots, m + Q_nM)$$

*induce el isomorfismo de $B$ módulos*

$$M/IM \cong M/Q_1M \oplus \cdots \oplus M/Q_nM.$$

*Demostración.* Supongamos que $IM = \langle 0 \rangle$. A continuación demostraremos que el mapeo diagonal es suprayectivo, haremos la demostración por inducción sobre $n$. El caso $n = 1$ es trivial, por lo que haremos la demostración para $n = 2$. Sea $\Delta : B \to B/Q_1 \oplus B/Q_2$ dada por $\Delta(b) = (b + Q_1, b + Q_2)$. Como $Q_1$ y $Q_2$ son co-maximales, existen $q_1 \in Q_1$ y $q_2 \in Q_2$ tales que $1 = q_1 + q_2$. Entonces para toda $b \in B$, $b = bq_1 + bq_2$ y

$$\Delta(bq_1) = (bq_1 + Q_1, bq_1 + Q_2) = (0 + Q_1, b(1 - q_2) + Q_2) = (0 + Q_1, b + Q_2).$$

Así que $\Delta(\langle q_1 \rangle) \cong B/Q_2$. Análogamente $\Delta(\langle q_2 \rangle) \cong B/Q_1$. Luego

$$\Delta(B) = \Delta(B(q_1 + q_2)) = \Delta(Bq_1 + Bq_2) = \Delta(\langle q_1 \rangle) + \Delta(\langle q_2 \rangle) \cong B/Q_1 \oplus B/Q_2.$$

Supongamos que se cumple para $n - 1 \geq 2$ y demostremos que es válido para n. Sean $Q'_i = Q_i$ para toda $i < n - 1$ y sea $Q'_{n-1} = Q_n \cap Q_{n-1}$, en el Teorema Chino del Residuo para Anillos demostramos que las $Q'_i$ son co-maximales. Luego por hipótesis de inducción

$$\Delta(B) \cong B/Q'_1 \oplus \cdots \oplus B/Q'_{n-1}.$$

Por el Teorema Chino del residuo para el caso $n = 2$ tenemos

$$\begin{aligned}\Delta(B) &\cong B/Q_1' \oplus \cdots \oplus B/Q_{n-1}' \\ &= B/Q_1 \oplus \cdots \oplus B/Q_{n-2} \oplus B/Q_{n-1}' \\ &\cong B/Q_1 \oplus \cdots \oplus B/Q_{n-2} \oplus B/Q_{n-1} \oplus B/Q_n.\end{aligned}$$

Sea $v_i$ el elemento que bajo el mapeo diagonal va a dar al elemento

$$(0 + Q_1, \ldots, 1 + Q_i, \ldots, 0 + Q_n),$$

esto es, $v_i \in Q_j$ para toda $j \neq i$ y $1 - v_i \in Q_i$.

Consideremos el homomorfismo $\phi : M \longrightarrow v_i M$, dado por $\phi(m) = v_i m$. Afirmamos que el $\ker\phi = Q_i M$. Sea $m \in M$ tal que $v_i m = 0$. Luego $m = m - v_i m = (1 - v_i)m \in Q_i M$ pues $1 - v_i \in Q_i$. Ahora $\phi(Q_i M) = v_i Q_i M$, $v_i Q_i \subseteq Q_j$, ya que $v_i \in Q_j$ para toda $j \neq i$. Además $v_i Q_i \subseteq Q_i$ por ser un ideal. Luego $v_i Q_i \subseteq I$ y $v_i Q_i M \subseteq IM \subseteq \langle 0 \rangle$. Ésto implica que $\ker\phi = Q_i M$ y por el primer teorema de isomorfismos $M/Q_i M \cong v_i M$.

Ésto significa que basta demostrar que $M = v_1 M \oplus \cdots \oplus v_n M$. Primero mostremos que $M = v_1 M + \cdots + v_n M$. Sea $i \in \{1, \ldots, n\}$. Luego para toda $j = 1, \ldots, n$, $j \neq i$ se tiene que $v_i \in Q_j$ y $1 - v_i \in Q_i$. Esto implica que

$$v_1 + \cdots + v_{i-1} + (v_i - 1) + v_{i+1} \cdots + v_n \in Q_i$$

para toda $i = 1, \ldots, n$. Luego $v_1 + \cdots + v_n - 1 \in I$, esto implica que $(v_1 + \cdots + v_n - 1)m \in IM = \langle 0 \rangle$. Por lo tanto, $v_1 m + \cdots + v_n m - 1m = 0$ y $m = v_1 m + \cdots + v_n m$. Ahora sea $\sum_{i=1}^{n} v_i m_i = 0$. Entonces para toda $j = 1, \ldots, n$, se tiene que

$$v_j \sum_{i=1}^{n} v_i m_i = v_j v_j m_j = 0$$

pues para toda $i \neq j$, $v_j v_i m_i \in IM = \langle 0 \rangle$. Luego

$$v_j m_j = v_j m_j - v_j v_j m_j = (1 - v_j) v_j m_j \in v_j Q_j M \subseteq IM = \langle 0 \rangle.$$

Por lo tanto $v_j m_j = 0$. Luego $M = v_1 M \oplus \cdots \oplus v_n M$.

Si $IM \neq \langle 0 \rangle$, entonces tomamos el $B$-módulo $N = M/IM$ y observemos que se cumple $IN = \langle 0 \rangle$. Aplicando el caso anterior tenemos que

$$N \cong N/Q_1 N \oplus \cdots \oplus N/Q_n N.$$

Luego para toda $i = 1, \ldots, n$, se tiene que $N/Q_i N = (M/IM)/Q_i (M/IM) \cong M/Q_i M$ por el segundo teorema de isomorfismos para módulos. Por lo tanto

$$M/IM \cong M/Q_1 M \oplus \cdots \oplus M/Q_n M.$$

□

**Proposición 4.1.4.** *Sean $Q_1, \ldots, Q_n$ ideales co-maximales dos a dos de un anillo $B$. Entonces $\bigcap_{i=1}^{n} Q_i = \prod_{i=1}^{n} Q_i$.*

*Demostración.* Siempre se cumple que $\prod_{i=1}^{n} Q_i \subseteq \bigcap_{i=1}^{n} Q_i$, por lo que basta demostrar $\bigcap_{i=1}^{n} Q_i \subseteq \prod_{i=1}^{n} Q_i$. Haremos la demostración por inducción sobre $n$. Como $Q_1$ y $Q_2$ son ideales co-maximales, existen $q_i \in Q_i$, $i = 1, 2$, tales que $1 = q_1 + q_2$. Luego para toda $q \in Q_1 \cap Q_2$ se cumple que $q = qq_1 + qq_2 \in Q_1 \cdot Q_2$. Por lo tanto $Q_1 \cap Q_2 \subseteq Q_1 \cdot Q_2$. Supongamos que se cumple para $n - 1 \geq 2$ y demostremos que es válido para $n$. Sean $Q'_j = Q_j$ si $j < n - 1$ y $Q'_{n-1} = Q_n \cap Q_{n-1}$. En la demostración del Teorema Chino del Residuo para anillos demostramos que las $Q'_j$ son co-maximales, por lo que podemos aplicar la hipótesis de inducción. Así

$$\begin{aligned}
\bigcap_{i=1}^{n} Q_i &= \bigcap_{i=1}^{n-1} Q'_i \\
&= \left(\prod_{i=1}^{n-2} Q_i\right) Q'_{n-1} = \left(\prod_{i=1}^{n-2} Q_i\right)(Q_{n-1} \cap Q_n) \\
&= \left(\prod_{i=1}^{n-2} Q_i\right) Q_{n-1} \cdot Q_n = \prod_{i=1}^{n} Q_i.
\end{aligned}$$

□

**Lema 4.1.5.** *Sea $R$ un anillo conmutativo noetheriano. Entonces todo ideal de $R$ contiene un producto de ideales primos.*

*Demostración.* Haremos la demostración por contradicción. Supongamos que el conjunto de ideales de $R$ que no contienen productos de ideales primos es no vacío y llamemos $\mathfrak{J}$ a dicho conjunto. Como $R$ es un anillo noetheriano, entonces $\mathfrak{J}$ tiene un maximal $J$. En particular $J$ no es un ideal primo, lo que significa que existen $a, b \in J$ tales que $ab \in J$, pero $a \notin J$ y $b \notin J$. Luego $J \subset J + \langle a \rangle$ y $J \subset J + \langle b \rangle$. Como $J$ es maximal en $\mathfrak{J}$, entonces los ideales $J + \langle a \rangle$ y $J + \langle b \rangle$ contienen un producto de ideales primos. Luego $(J + \langle a \rangle)(J + \langle b \rangle) \subseteq J + \langle ab \rangle \subseteq J$. Lo que implica que $J$ contiene un producto de ideales primos, ya que $(J + \langle a \rangle)(J + \langle b \rangle)$ contiene un producto de ideales primos, lo cual no es posible pues $J \in \mathfrak{J}$. □

**Corolario 4.1.6.** *Sea $R$ un anillo conmutativo noetheriano. Entonces existen ideales primos $P_1, \ldots, P_n$ de $R$ y enteros positivos $a_1, \ldots, a_n$ tales que $P_1^{a_1} \cdots P_n^{a_n} = \langle 0 \rangle$.*

*Demostración.* Por el lema 4.1.5 todo ideal de $R$ contiene un producto de ideales primos, en particular el ideal $\langle 0 \rangle$ contiene un producto de ideales primos. Por lo tanto existen ideales primos $P_1, \ldots, P_n$ de $R$ y enteros positivos $a_1, \ldots, a_n$, tales que $P_1^{a_1} \cdots P_n^{a_n} = \langle 0 \rangle$. □

**Lema 4.1.7.** *Sea $R$ un anillo conmutativo y sean $P_1$ y $P_2$ ideales maximales distintos de $R$. Entonces $P_1^m + P_2^n = R$ para todo $n, m \in \mathbb{Z}^+$.*

*Demostración.* Demostraremos que $P_1^m + P_2^n = R$, para toda $n, m \in \mathbb{Z}^+$, por inducción sobre $n$. Para $n = 1$: por ser $P_1$ y $P_2$ ideales maximales, entonces $P_1 + P_2 = R$. Luego

$$R = R^m = (P_1 + P_2)^m \subseteq P_1^m + P_2$$

para toda $m \in \mathbb{Z}^+$. Lo que implica que $R = P_1^m + P_2$ para toda $m \in \mathbb{Z}^+$. Supongamos que para toda $n - 1 > 0$, se cumple que $P_1^m + P_2^{n-1} = R$ para toda $m \in \mathbb{Z}^+$. Luego

$$P_2^{n-1} = P_2^{n-1}R = P_2^{n-1}\left(P_1^m + P_2\right) \subseteq P_1^m + P_2^n.$$

Lo que implica que

$$R = P_1^m + P_2^{n-1} \subseteq P_1^m + (P_1^m + P_2^n) \subseteq P_1^m + P_2^n \subseteq R$$

para toda $m \in \mathbb{Z}^+$. □

**Lema 4.1.8.** *Sea $R$ un anillo conmutativo noetheriano en el que todo ideal primo es maximal y sean $P_1, \ldots, P_n$ ideales primos tales que $\prod_{i=1}^n P_i^{a_i} = \langle 0 \rangle$. Entonces existe un isomorfismo de anillos*

$$R \cong \bigoplus_{i=1}^{n} R/P_i^{a_i}.$$

*Demostración.* El ideal $P_i$ es un ideal maximal ya que es un ideal primo, para toda $i = 1, \ldots, n$. Luego por el lema 4.1.7 $P_i^{a_i} + P_j^{a_j} = R$, para toda $i \neq j$ $i, j \in \{1, \ldots, n\}$. Esto implica que se cumplen las hipótesis del teorema chino del residuo y por lo tanto

$$R/\bigcap_{i=1}^{n} P_i^{a_i} \cong \bigoplus_{i=1}^{n} R/P_i^{a_i}.$$

Por otro lado, $\bigcap_{i=1}^n P_i^{a_i} = \prod_{i=1}^n P_i^{a_i} = \langle 0 \rangle$ por la proposición 4.1.4. Luego

$$R \cong R/\prod_{i=1}^{n} P_i^{a_i} \cong R/\bigcap_{i=1}^{n} P_i^{a_i} \cong \bigoplus_{i=1}^{n} R/P_i^{a_i}.$$

□

**Lema 4.1.9.** *Si un ideal primo $\mathfrak{P}$ de un anillo $R$ contiene un producto de ideales $\mathfrak{a}_1 \cdots \mathfrak{a}_n$, entonces $\mathfrak{P}$ contiene a uno de ellos.*

*Demostración.* Si $\mathfrak{a}_i \nsubseteq \mathfrak{P}$ para toda $i = 1, \ldots, n$, entonces existe $a_i \in \mathfrak{a}_i - \mathfrak{P}$. Luego $a_1 \cdots a_n \notin \mathfrak{P}$ ya que $\mathfrak{P}$ es primo. Pero $a_1 \cdots a_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{P}$ que nos lleva a una contradicción. □

**Corolario 4.1.10.** *Sea $R$ un anillo conmutativo noetheriano en el que todo ideal primo es maximal y sean $P_1, \ldots, P_n$ ideales primos tales que $\prod_{i=1}^{n} P_i^{a_i} = \langle 0 \rangle$. Entonces los ideales $P_1, \ldots, P_n$ son todos los ideales primos de $R$.*

*Demostración.* Sea $R_i = R/P_i^{a_i}$. Si $J/P_i^{a_i}$ es ideal primo de $R_i$, entonces $J$ es ideal primo de $R$ y contiene a $P_i^{a_i}$ (observación 1.1.5), por el lema 4.1.9 $P_i \subseteq J$ y por ser maximales $J = P_i$, así que $P_i/P_i^{a_i}$ es el único ideal primo de $R_i$. Ahora los ideales de $R_1 \oplus \cdots \oplus R_n$ son de la forma $J_1 \oplus \cdots \oplus J_n$, donde cada $J_i$ es ideal de $R_i$. Luego $J_1 \oplus \cdots \oplus J_n$ es ideal primo si y sólo si $R_1 \oplus \cdots \oplus R_n/J_1 \oplus \cdots \oplus J_n \cong R_1/J_1 \oplus \cdots \oplus R_n/J_n$ es un dominio entero, esto último sucede si y sólo si $J_i = P_i/P_i^{a_i}$ para alguna $i$ y $J_k = R_k$ para toda $k = 1, \ldots, n$ y $k \neq i$. Por el lema 4.1.8 $R \cong \bigoplus_{i=1}^{n} R/P_i^{a_i}$, lo cual implica que todo ideal primo $P$ de $R$ es isomorfo un ideal primo, a saber $P_i/P_i^{a_i}$ para alguna $i = 1, \ldots, n$. Luego $P = P_i$ para alguna $i$. □

**Lema 4.1.11.** *Sea $P$ ideal maximal de un anillo conmutativo $R$ y sea $n$ un entero positivo. Entonces la inclusión de $R$ en $R_P$ induce el isomorfismo*

$$R/P^n \cong R_P/P^n R_P.$$

*Demostración.* Definamos el homomorfismo $f : R/P^n \longrightarrow R_P/P^n R_P$ dado por $f(r + P^n) = r + P^n R_P$. Es un homomorfismo inyectivo ya que si $r + P^n R_P = r' + P^n R_P$, entonces $r - r' \in P^n R_P$. Luego $r - r' \in P^n$ y así $r + P^n = r' + P^n$. Ahora veamos que es un homomorfismo suprayectivo. Sea $\frac{r}{s} \in R_P$. Esto significa que $r \in R$ y $s \notin P$. Luego $\langle s \rangle + P = R$ ya que $P$ es ideal maximal. Demostraremos por inducción que $\langle s \rangle + P^n = R$ para cualquier entero positivo $n$. El caso $n = 1$ ya lo vimos. Supongamos que para $n-1 > 0$ se cumple $\langle s \rangle + P^{n-1} = R$. Luego

$$P^{n-1} = P^{n-1}R = P^{n-1}\left(\langle s \rangle + P\right) \subseteq \langle s \rangle + P^n.$$

Esto implica que

$$R = \left(\langle s \rangle + P^{n-1}\right) \subseteq \langle s \rangle + P^n.$$

Por lo tanto $\langle s \rangle + P^n = R$.

Esto implica que existen $c \in R$ y $q \in P^n$ tales que $cs + q = 1$. Luego $c = \frac{1-q}{s} \in R_P$. Entonces

$$f(rc + P^n) = rc + P^n R_P = r\frac{1-q}{s} + P^n R_P = \frac{r}{s} - \frac{rq}{s} + P^n R_P = \frac{r}{s} + P^n R_P$$

ya que $\frac{rq}{s} \in P^n R_P$. □

**Corolario 4.1.12.** *Sea $R$ un anillo de Dedekind y $\mathfrak{p}$ un ideal primo no trivial de $R$. Entonces todo ideal de $R/\mathfrak{p}^a$ es una potencia de $\mathfrak{p}/\mathfrak{p}^a$ para todo entero positivo $a$. Más aún $\mathfrak{p}/\mathfrak{p}^a$ es un ideal principal.*

*Demostración.* Por el lema 4.1.11 $R/\mathfrak{p}^a \cong R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}$. El ideal $\mathfrak{p}/\mathfrak{p}^a$ es un ideal principal ya que $R_\mathfrak{p}$ es dominio de ideales principales. El único ideal maximal de $R_\mathfrak{p}$ es $\mathfrak{p}R_\mathfrak{p}$. Luego, por la proposición 4.0.21 todo ideal de $R_\mathfrak{p}$ es una potencia de $\mathfrak{p}R_\mathfrak{p}$. Por lo tanto todo ideal de $R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}$ es una potencia de $\mathfrak{p}R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}$. Es claro que bajo el isomorfismo del lema 4.1.11 el ideal $\mathfrak{p}/\mathfrak{p}^a$ se aplica en el ideal $\mathfrak{p}R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}$. Por lo tanto todo ideal de $R/\mathfrak{p}^a$ es una potencia de $\mathfrak{p}/\mathfrak{p}^a$. □

**Teorema 4.1.13.** *Sea $R$ un anillo de Dedekind y $A$ un ideal no trivial de $R$. Entonces $A$ está contenido solamente en un número finito de ideales primos $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ y además $A = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n}$ para algunos enteros positivos $b_i$.*

*Demostración.* Sea $J/A$ un ideal primo de $R/A$. Entonces $J$ es ideal primo de $R$ que contiene a $A$, como $R$ es de Dedekind, entonces $J$ es ideal maximal (proposición 4.0.23). Por lo tanto $J/A$ es ideal maximal de $R/A$. Luego por el corolario 4.1.6, existe un número finito de ideales primos $\mathfrak{p}_1/A, \mathfrak{p}_2/A, \ldots, \mathfrak{p}_n/A$ de $R/A$ tales que

$$(\mathfrak{p}_1^{a_1}/A) \cdot (\mathfrak{p}_2^{a_2}/A) \cdots (\mathfrak{p}_n^{a_n}/A) = A/A$$

con $a_1, \ldots, a_n$ enteros positivos. Luego $\mathfrak{p}_1^{a_1} \cdot \mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_n^{a_n} \subseteq A$. Además por el corolario 4.1.10 $\mathfrak{p}_1/A, \mathfrak{p}_2/A, \ldots, \mathfrak{p}_n/A$ son los únicos ideales primos de $R/A$. Luego $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ son los únicos ideales primos de $R$ que contienen a $A$ y $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} = A$. □

**Teorema 4.1.14.** *Sea $R$ un anillo de Dedekind y $A$ un ideal no trivial de $R$. Entonces $A = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n}$ de manera única.*

*Demostración.* Los ideales $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ son únicos ya que son todos los ideales que contienen a $A$. Los enteros $b_i$ están determinados por $A$ como el mínimo entero positivo tal que $AR_{\mathfrak{p}_i} = \mathfrak{p}_i^{b_i} R_{\mathfrak{p}_i}$. □

Si $A$ es un ideal de $R$, decimos que $x \equiv y \pmod{A}$ si $x - y \in A$.

**Lema 4.1.15.** *Sean $R$ un anillo de Dedekind con un número finito de ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, $a_1, \ldots, a_n$ enteros positivos y $y_1, \ldots, y_n$ elementos de $R$. Entonces existe $x \in R$ tal que $x \equiv y_i \ mod\ \mathfrak{p}_i^{a_i}$ para toda $i$.*

*Demostración.* Por el teorema chino del residuo para anillos, el homomorfismo diagonal de $R$ sobre $\bigoplus R/\mathfrak{p}_i^{a_i}$ es suprayectivo. Luego existe $x \in R$ tal que

$$(x + \mathfrak{p}_1^{a_1}, \ldots, x + \mathfrak{p}_n^{a_n}) = (y_1 + \mathfrak{p}_1^{a_1}, \ldots, y_n + \mathfrak{p}_n^{a_n}).$$

Por lo tanto $x \equiv y_i \pmod{P_i^{a_i}}$. □

**Teorema 4.1.16.** *Sea $R$ un anillo de Dedekind con un número finito de ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Entonces $R$ es un dominio de ideales principales.*

*Demostración.* Sea $y \in \mathfrak{p}_1 - \mathfrak{p}_1^2$. Por el lema 4.1.15 existe $x_1 \in R$ tal que

$$\left(x_1 + \mathfrak{p}_1^2, x_1 + \mathfrak{p}_2, \ldots, x_1 + \mathfrak{p}_n\right) = \left(y + \mathfrak{p}_1^2, 1 + \mathfrak{p}_2, \ldots, 1 + \mathfrak{p}_n\right).$$

Luego $x_1 - y \in \mathfrak{p}_1^2$ y $x_1 - 1 \in \mathfrak{p}_i$ para $i = 2, \ldots, n$, lo que implica que $x_1 \in \mathfrak{p}_1 - \mathfrak{p}_1^2$ y $x_1 \notin \mathfrak{p}_i$ para $i = 2, \ldots, n$. Luego el único ideal primo que contiene al ideal $\langle x_1 \rangle$ es $\mathfrak{p}_1$. Más aún $\langle x_1 \rangle \nsubseteq \mathfrak{p}_1^2$. Como todo ideal es producto de potencias de ideales primos, entonces $\langle x_1 \rangle = \mathfrak{p}_1$. De la misma forma, podemos encontrar $x_i \in R$ tal que $\mathfrak{p}_i = \langle x_i \rangle$ para toda $i$. Por lo tanto todo ideal primo es principal y en cosecuencia todo ideal es principal, ya que todo ideal se factoriza como producto de ideales primos. □

## 4.2. Caracterización de anillos de Dedekind

Hasta ahora no hemos tenido ejemplos claros de anillos de Dedekind pues la definición que dimos es un poco complicada. Es por eso que en esta sección demostraremos algunas caracterizaciones de los anillos de Dedekind.

**Lema 4.2.1.** *Sea $R$ un dominio entero. Entonces*

$$R = \bigcap_{\mathfrak{p}\ maximal} R_{\mathfrak{p}}.$$

*Demostración.* Para todo ideal maximal $\mathfrak{p}$ se cumple que $R \subseteq R_{\mathfrak{p}}$, por lo que $R$ está contenido en la intersección. Demostremos la otra contención. Sea $x = \frac{a}{b} \in \bigcap R_{\mathfrak{p}}$, con $a, b \in R$ y sea

$$\mathfrak{A} = \{y \in R \mid ya \in \langle b \rangle\}.$$

$\mathfrak{A}$ es un ideal de $R$ ya que para todo $y, w \in \mathfrak{A}$, $(y - w)a \in \langle b \rangle$ y para todo $r \in R$, $rya \in \langle b \rangle$.

Para cada ideal maximal $\mathfrak{p}$ se cumple que $x = \frac{r}{s}$ donde $r \in R$ y $s \notin \mathfrak{p}$. Lo que implica que $sa = rb \in \langle b \rangle$. Esto significa que $s \in \mathfrak{A}$ y como $s \notin \mathfrak{p}$, entonces $\mathfrak{A} \nsubseteq \mathfrak{p}$. Por lo tanto $\mathfrak{A} = R$. Esto implica que para todo $y \in R$ $ya \in \langle b \rangle$, en particular $1a = a \in \langle b \rangle$. Luego $b$ divide a $a$ y por lo tanto $x \in R$. □

**Lema 4.2.2.** *Sea $R$ un dominio entero y sean $\mathfrak{A} \subseteq \mathfrak{B}$ ideales de $R$. Si $\mathfrak{A}R_{\mathfrak{p}} = \mathfrak{B}R_{\mathfrak{p}}$ para todo ideal maximal $\mathfrak{p}$, entonces $\mathfrak{A} = \mathfrak{B}$.*

*Demostración.* Sea $b \in \mathfrak{B}$. Para cada ideal maximal $\mathfrak{p}$ se tiene que $b \in \mathfrak{A}R_{\mathfrak{p}}$. Luego $b = \frac{a}{s}$ con $a \in \mathfrak{A}$ y $s \notin \mathfrak{p}$. Sea

$$\mathfrak{Q} = \{y \in R \mid by \in \mathfrak{A}\}.$$

De manera análoga a la demostración del lema 4.2.1 se puede mostrar que $\mathfrak{Q}$ es ideal de $R$. Luego $bs = a \in \mathfrak{A}$. Esto implica que $s \in \mathfrak{Q}$ y $s \notin \mathfrak{p}$. Por lo tanto $\mathfrak{Q} \nsubseteq \mathfrak{p}$ para todo ideal maximal $\mathfrak{p}$. Luego $\mathfrak{Q} = R$ ya que todo ideal debe estar contenido en un ideal maximal. Esto implica que $b = 1b \in \mathfrak{A}$. □

**Proposición 4.2.3.** *Sea $A$ un dominio noetheriano, enteramente cerrado y con un único ideal primo no trivial $\mathfrak{p}$. Entonces $A$ es un dominio de ideales principales.*

*Demostración.* Como $\mathfrak{p}$ es el único ideal primo de $A$, entonces es el único ideal maximal de $A$. Sea $a \in \mathfrak{p}$ distinto de cero y $M = A/\langle a\rangle$. Definimos para cada $m + \langle a\rangle \in M$ el ideal

$$An\left(m + \langle a\rangle\right) = \{r \in A \mid rm + \langle a\rangle = \langle a\rangle\} = \{r \in A \mid rm \in \langle a\rangle\}.$$

Sea

$$\mathfrak{J} = \{An\left(m + \langle a\rangle\right) \mid m \notin \langle a\rangle\}.$$

Como $A$ es un dominio entero noetheriano existe un ideal $\mathfrak{q}$ que es maximal en $\mathfrak{J}$. Sea $b \in A$ tal que $\mathfrak{q} = An\left(b + \langle a\rangle\right)$. Nótese que $\mathfrak{q} \neq \langle 0\rangle$ ya que $a \in \mathfrak{q}$ pues $ab + \langle a\rangle = \langle a\rangle$ .

El ideal $\mathfrak{q}$ es primo: supongamos que no es así, es decir, existen $x, y \in A$ tales que $xy \in \mathfrak{q}$ pero $x \notin \mathfrak{q}$ y $y \notin \mathfrak{q}$. Notemos que $yb \notin \langle a\rangle$ ya que $y \notin \mathfrak{q}$, lo que implica $An\left(yb + \langle a\rangle\right) \in \mathfrak{J}$. Sea $r \in \mathfrak{q}$, es decir, $rb \in \langle a\rangle$. Luego $r(yb) = y(rb) \in \langle a\rangle$, esto es, $r \in An\left(yb + \langle a\rangle\right)$ . En consecuencia $\mathfrak{q} \subseteq An\left(yb + \langle a\rangle\right)$. Por otro lado, $x(yb) = (xy)b \in \langle a\rangle$ ya que $xy \in \mathfrak{q}$, lo que significa que $x \in An\left(yb + \langle a\rangle\right)$. Por lo tanto $\mathfrak{q} \subsetneq An\left(yb + \langle a\rangle\right)$, que no es posible pues $\mathfrak{q}$ es maximal en $\mathfrak{J}$. Como el único ideal primo distinto de cero es $\mathfrak{p}$, entonces $\mathfrak{q} = \mathfrak{p}$.

$\mathfrak{p}$ es ideal principal: $\mathfrak{p}b \subseteq \langle a\rangle = Aa$ ya que $\mathfrak{q} = \mathfrak{p}$ y $\langle b\rangle \nsubseteq \langle a\rangle$ puesto que $\mathfrak{q} \in \mathfrak{J}$. Luego $\frac{b}{a} \notin A$, ya que si $a \mid b$, entonces $\langle b\rangle \subseteq \langle a\rangle$ que no es posible. Como $\mathfrak{p}b \subseteq Aa$, entonces $\mathfrak{p}\frac{b}{a} \subseteq A$. Si $\mathfrak{p}\frac{b}{a} \neq A$, entonces $\mathfrak{p}\frac{b}{a} \subseteq \mathfrak{p}$. Pero por el inciso 4. de la proposición 3.0.7, $\frac{b}{a}$ es entero sobre $A$ y por ser $A$ enteramente cerrado $\frac{b}{a} \in A$, que es una contradicción. Luego $\mathfrak{p}\frac{b}{a} = A$ y así $\mathfrak{p} = A\frac{a}{b}$, es decir, $\mathfrak{p}$ es un ideal principal.

Sea $p = \frac{a}{b}$ y sea $\mathfrak{A}$ un ideal no trivial de $A$. Luego $p\mathfrak{A} \subseteq \mathfrak{A}$, por lo que $\mathfrak{A} \subseteq \mathfrak{A}p^{-1}$. Para mostrar que $\mathfrak{A}$ es ideal principal consideremos la cadena

$$\mathfrak{A} \subsetneq \mathfrak{A}p^{-1} \subsetneq \mathfrak{A}p^{-2} \subsetneq \mathfrak{A}p^{-3} \subsetneq \cdots .$$

Nótese que las contenciones deben ser propias ya que si $\mathfrak{A}p^{-k} = \mathfrak{A}p^{-k-1}$, entonces al multiplicar $\mathfrak{A}p^{-k}$ por $p^{-1}$ obtendríamos otra vez $\mathfrak{A}p^{-k}$. Esto implicaría que $p^{-1} = \frac{b}{a}$ es entero sobre $A$ y en consecuencia $\frac{b}{a} \in A$ que no es posible. Sea $n \in \mathbb{N}$ tal que $\mathfrak{A}p^{-n} \subseteq A$ y $\mathfrak{A}p^{-n-1} \nsubseteq A$. Dicha $n$ existe ya que $A$ es un dominio noetheriano y la parte de la cadena contenida en $A$ debe ser finita. Si $\mathfrak{A}p^{-n} \subseteq \mathfrak{p} = Ap$, entonces $\mathfrak{A}p^{-n-1} \subseteq A$, que contradice la elección de $n$. Luego $\mathfrak{A}p^{-n} = A$. Por lo tanto $\mathfrak{A} = Ap^n = \langle p^n\rangle$.

□

**Teorema 4.2.4.** *Sea $R$ un dominio entero que no es campo. Entonces los siguientes enunciados son equivalentes:*

1. *$R$ es un anillo de Dedekind.*
2. *$R_{\mathfrak{p}}$ es DVD para cada ideal maximal $\mathfrak{p}$ de $R$ y para toda $a \in R$ distinta de cero existe sólo un número finito de ideales primos que contienen a $a$.*

*3. $R$ es noetheriano, enteramente cerrado y todo ideal primo no trivial es maximal.*

*Demostración.* 1) $\Longrightarrow$ 2) Como todo ideal maximal es ideal primo, entonces $R_{\mathfrak{p}}$ es DVD para cada ideal maximal $\mathfrak{p}$ de $R$. Sea $a \in R$ distinto de cero. Si $J/\langle a\rangle$ es ideal primo del anillo $R/\langle a\rangle$, entonces $J$ es ideal primo de $R$. Luego $J$ es ideal maximal, ya que en un anillo de Dedekind todo ideal primo es maximal (proposición 4.0.23) y por lo tanto el ideal $J/\langle a\rangle$ es un ideal maximal. Esto implica que se satisfacen las hipótesis del corolario 4.1.10 para el anillo $R/\langle a\rangle$ y el anillo $R/\langle a\rangle$ contiene sólo un número finito de ideales primos. Por lo tanto existe sólo un número finito de ideales primos que contienen a $a$.

2) $\Longrightarrow$ 3) Primero mostraremos que todo ideal primo no trivial es maximal. Sea $\mathfrak{q}$ ideal primo de $R$. Entonces existe un ideal maximal $\mathfrak{p}$ tal que $\mathfrak{q} \subseteq \mathfrak{p}$. Por hipótesis $R_{\mathfrak{p}}$ es DVD y por lo tanto contiene un único ideal maximal que es $\mathfrak{p}R_{\mathfrak{p}}$. Por otro lado $\mathfrak{q}R_{\mathfrak{p}}$ es ideal primo. Luego $\mathfrak{q}R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ por las propiedades de DVD, es decir, $\mathfrak{q}R_{\mathfrak{p}}$ es ideal maximal. Por la correspondencia biyectiva entre los ideales primos de $R_{\mathfrak{p}}$ y los ideales primos de $R$ cuya intersección con $R - \mathfrak{p}$ es vacía, se tiene que $\mathfrak{q} = \mathfrak{p}$. Por lo tanto todo ideal primo es maximal.

Ahora mostraremos que $R$ es enteramente cerrado. $R_{\mathfrak{p}}$ es DIP para todo ideal maximal $\mathfrak{p}$ de $R$. En el ejemplo 3.0.14 vimos que todo DIP es enteramente cerrado, por lo que $R_{\mathfrak{p}}$ es enteramente cerrado para todo ideal maximal $\mathfrak{p}$ de $R$. Luego $R = \bigcap R_{\mathfrak{p}}$ (lema 4.2.1) y la intersección de dominios enteramente cerrados es enteramente cerrada (proposición 3.0.17). Por lo tanto $R$ es enteramente cerrado.

$R$ es noetheriano, más aún todo ideal $\mathfrak{A}$ de $R$ está generado por dos elementos, es decir, $\mathfrak{A} = \langle a\rangle + \langle b\rangle$ con $a, b \in \mathfrak{A}$. Sea $a \in \mathfrak{A}$ y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos de $R$ que contienen a $a$. Ya vimos que todo ideal primo es maximal, por lo tanto $R_{\mathfrak{p}_i}$ es DIP para toda $i = 1, \ldots, n$. Esto implica que existe $c_i \in R_{\mathfrak{p}_i}$ tal que $\mathfrak{A}R_{\mathfrak{p}_i} = \langle c_i\rangle$. Notemos que podemos suponer que $c_i \in \mathfrak{A}$ ya que si $c_i = \frac{x}{s}$ con $x \in \mathfrak{A}$ y $s \notin \mathfrak{p}_i$, entonces

$$\begin{aligned}\langle c_i\rangle &= \left\{ y\frac{x}{s} \mid y \in R_{\mathfrak{p}_i} \right\} \\ &= \left\{ \left(\frac{y}{s}\right) x \mid \frac{y}{s} \in R_{\mathfrak{p}_i} \right\}.\end{aligned}$$

Sea $\mathfrak{C} = \langle a\rangle + \langle c_1\rangle + \cdots + \langle c_n\rangle$. Claramente $\mathfrak{C} \subseteq \mathfrak{A}$ ya que $a, c_1, \ldots, c_n \in \mathfrak{A}$. Mostraremos que para todo ideal maximal $\mathfrak{p}$, $\mathfrak{A}R_{\mathfrak{p}} = \mathfrak{C}R_{\mathfrak{p}}$ para poder utilizar el lema 4.2.2. Sea $\mathfrak{p}$ un ideal maximal de $R$. Si $\mathfrak{p}$ no contiene a $a$, entonces $\frac{1}{a} \in R_{\mathfrak{p}}$. Luego $a \cdot \frac{1}{a} = 1 \in \mathfrak{A}R_{\mathfrak{p}}$ y $a \cdot \frac{1}{a} = 1 \in \mathfrak{C}R_{\mathfrak{p}}$. Por lo tanto $\mathfrak{A}R_{\mathfrak{p}} = \mathfrak{C}R_{\mathfrak{p}} = R_{\mathfrak{p}}$. Si $\mathfrak{p}$ contiene a $a$, es decir, $\mathfrak{p} = \mathfrak{p}_i$ para alguna $i$, entonces $c_i \in \mathfrak{C}R_{\mathfrak{p}_i}$. Luego $\mathfrak{A}R_{\mathfrak{p}_i} = \langle c_i\rangle \subseteq \mathfrak{C}R_{\mathfrak{p}_i}$, lo que implica $\mathfrak{A}R_{\mathfrak{p}_i} = \mathfrak{C}R_{\mathfrak{p}_i}$. Por lo tanto, por el lema 4.2.2, $\mathfrak{A} = \mathfrak{C}$.

Por el teorema chino del residuo para módulos se tiene el siguiente isomorfismo:

$$\mathfrak{A}/\left(\mathfrak{p}_1 \cdots \mathfrak{p}_n\right)\mathfrak{A} \cong \mathfrak{A}/\mathfrak{p}_1\mathfrak{A} \oplus \cdots \oplus \mathfrak{A}/\mathfrak{p}_n\mathfrak{A}.$$

Sea $b \in \mathfrak{A}$ tal que bajo dicho isomorfismo se obtiene el elemento $(c_1 + \mathfrak{p}_1\mathfrak{A}, \ldots, c_n + \mathfrak{p}_n\mathfrak{A})$. Sea $\mathfrak{D} = \langle a\rangle + \langle b\rangle$. Afirmamos que $\mathfrak{A} = \mathfrak{D}$. Por la manera en que definimos $b$ se tiene que

$b - c_i \in \mathfrak{p}_i\mathfrak{A} \subseteq \mathfrak{A}$. Luego $\mathfrak{D} \subseteq \mathfrak{A}$ y mostraremos que $\mathfrak{A}R_\mathfrak{p} = \mathfrak{D}R_\mathfrak{p}$ para todo ideal maximal $\mathfrak{p}$. Sea $\mathfrak{p}$ ideal maximal de $R$. Si $a \notin \mathfrak{p}$, entonces $\mathfrak{A}R_\mathfrak{p} = \mathfrak{D}R_\mathfrak{p} = R_\mathfrak{p}$. Para los ideales $\mathfrak{p}_i$ que contienen a $a$, demostraremos que

$$\mathfrak{D}R_{\mathfrak{p}_i} + \mathfrak{p}_i\mathfrak{A}R_{\mathfrak{p}_i} = \mathfrak{A}R_{\mathfrak{p}_i}.$$

Como $\mathfrak{D} \subseteq \mathfrak{A}$, entonces $\mathfrak{D}R_{\mathfrak{p}_i} \subseteq \mathfrak{A}R_{\mathfrak{p}_i}$ y como $\mathfrak{p}_i\mathfrak{A} \subseteq \mathfrak{A}$, entonces $\mathfrak{p}_i\mathfrak{A}R_{\mathfrak{p}_i} \subseteq \mathfrak{A}R_{\mathfrak{p}_i}$. Luego $\mathfrak{D}R_{\mathfrak{p}_i} + \mathfrak{p}_i\mathfrak{A}R_{\mathfrak{p}_i} \subseteq \mathfrak{A}R_{\mathfrak{p}_i}$. Para la otra contención notemos que $c_i = b + (c_i - b) \in \mathfrak{D}R_{\mathfrak{p}_i} + \mathfrak{p}_i\mathfrak{A}R_{\mathfrak{p}_i}$. Luego $\mathfrak{A}R_{\mathfrak{p}_i} = \langle c_i \rangle \subseteq \mathfrak{D}R_{\mathfrak{p}_i} + \mathfrak{p}_i\mathfrak{A}R_{\mathfrak{p}_i}$. En consecuencia $\mathfrak{D}R_{\mathfrak{p}_i} + \mathfrak{p}_i\mathfrak{A}R_{\mathfrak{p}_i} = \mathfrak{A}R_{\mathfrak{p}_i}$ y por el lema de Nakayama $\mathfrak{A}R_{\mathfrak{p}_i} = \mathfrak{D}R_{\mathfrak{p}_i}$. Luego $\mathfrak{A} = \mathfrak{D}$ y $\mathfrak{A}$ está generado por a lo más dos elementos.

3) $\Longrightarrow$ 1) El único ideal maximal de $R_\mathfrak{p}$ es $\mathfrak{p}R_\mathfrak{p}$, para todo ideal primo $\mathfrak{p}$, por la proposición 2.1.2. Como $R$ es enteramente cerrado, entonces $R_\mathfrak{p}$ también es enteramente cerrado por el ejemplo 3.0.15. Esto implica que $R_\mathfrak{p}$ satisface las hipótesis de la proposición 4.2.3 y en consecuencia $R_\mathfrak{p}$ es DIP. Por lo tanto $R$ es un anillo de Dedekind.

□

## 4.3. Ideales fraccionarios

En esta sección $R$ denotará un anillo de Dedekind y $K$ su campo de cocientes.

**Definición 4.3.1.** *Un **ideal fraccionario** $M$ de $R$ es un $R$-submódulo finitamente generado de $K$, no trivial.*

Notemos que si $M$ es un ideal fraccionario, entonces existe $t \in R$ tal que $tM \subseteq R$. Sean $\frac{m_1}{t_1}, \ldots, \frac{m_n}{t_n}$ los generadores de $M$ y $t = t_1 \cdots t_n$. Entonces para toda $x \in M$ se tiene que $x = \sum_{i=1}^n r_i \frac{m_i}{t_i}$, con $r_i \in R$. Luego $tx = \sum_{i=1}^n \widehat{r}_i m_i$, donde $\widehat{r}_i \in R$. Esto implica que $tx \in R$ para toda $x \in M$. Por lo tanto $tM \subseteq R$.

**Definición 4.3.2.** *Si $M$ es un ideal fraccionario de $R$, entonces $M^{-1}$ es el conjunto*

$$M^{-1} = \{x \in K \mid xM \subseteq R\}.$$

**Ejemplo 4.3.3.** *Como $R$ es un anillo noetheriano, entonces todo ideal es finitamente generado. Por lo tanto todo ideal de $R$ es un ideal fraccionario.*

**Ejemplo 4.3.4.** *Sea $y \in K$ distinto de cero. Entonces $Ry$ es un ideal fraccionario de $R$. Además $(Ry)^{-1} = Ry^{-1}$.*

*En efecto, como $y^{-1} \in (Ry)^{-1}$ ya que $y^{-1}Ry = R$, entonces $Ry^{-1} \subseteq (Ry)^{-1}$. Si $x \in (Ry)^{-1}$, entonces $xRy = Rxy \subseteq R$. Luego $xy \in R$ y por lo tanto $x \in Ry^{-1}$. Por lo tanto $(Ry)^{-1} = Ry^{-1}$.*

En esta sección demostraremos que el conjunto de ideales fraccionarios de $R$ es un grupo. Definamos el producto entre dos ideales fraccionarios $M$ y $N$ de la siguiente manera:

$$MN = \left\{ \sum m_i n_i \mid m_i \in M, n_i \in N \right\}.$$

Para la demostración de la siguiente proposición necesitaremos un resultado para módulos finitamente generados cuya demostración puede consultarse en [3] página 56.

**Proposición 4.3.5.** *Sea $R$ un anillo noetheriano y $M$ un $R$-módulo finitamente generado. Entonces $M$ es un $R$-módulo noetheriano y por lo tanto todos sus submódulos son finitamente generados.*

**Proposición 4.3.6.** *1. Si $M$ es ideal fraccionario de $R$, entonces $M^{-1}$ es un ideal fraccionario.*

*2. Si $M$ y $N$ son ideales fraccionarios, entonces $MN$ es un ideal fraccionario.*

*Demostración.* 1. Sea $m \in M$ distinto de cero. Entonces $M^{-1}m \subseteq R$ y en consecuencia $M^{-1} \subseteq Rm^{-1}$. Luego $Rm^{-1}$ es un $R$-módulo finitamente generado y como $R$ es un anillo noetheriano, entonces por la proposición 4.3.5 $M^{-1}$ es un $R$-módulo finitamente generado.

2. Sean $\{x_k\}_{k\in K}$ y $\{y_j\}_{j\in J}$ conjuntos finitos generadores de $M$ y $N$ respectivamente. Sea $x = \sum m_i n_i \in MN$. Luego

$$\begin{aligned} x = \sum m_i n_i &= \sum \left( \sum r_k x_k \right) \left( \sum s_j y_j \right) \\ &= \sum \widehat{r}_i x_k y_j \end{aligned}$$

donde $r_k, s_j, \widehat{r}_i \in R$. Por lo tanto $\{x_k y_j\}$ es un conjunto generador finito.

□

**Definición 4.3.7.** *Un ideal fraccinario $M$ es invertible, si $MM^{-1} = R$.*

Sea $S$ un subconjunto multiplicativo de $R$. Denotaremos por $M_S$ al $R$-módulo $MR_S$ y por $(M^{-1})_S$ al $R$-módulo $(M_S)^{-1}$. Si $n$ es un entero positivo, entonces definimos $M^{-n} = (M^{-1})^n$.

**Proposición 4.3.8.** *Sean $M$, $N$ ideales fraccionarios de $R$ y $S$ un subconjunto multiplicativo de $R$.*

*1. $(MN)_S = (M_S)(N_S)$.*

*2. Si $R$ es DIP, entonces todo ideal fraccionario es principal.*

*3. $(MN)^{-1} = M^{-1}N^{-1}$.*

*Demostración.* 1. Por definición

$$(MN)_S = MNR_S = (MR_S)(NR_S) = (M_S)(N_S).$$

2. Sea $t \in R$ distinto de cero tal que $tM \subseteq R$. Luego $tM = Ry$ con $y \in R$, ya que $R$ es DIP. Por lo tanto $M = R\frac{y}{t}$.

3. Por definición $M^{-1}N^{-1}MN = \left(M^{-1}M\right)\left(N^{-1}N\right) \subseteq R$. Luego $M^{-1}N^{-1} \subseteq (MN)^{-1}$. Por otro lado $(MN)^{-1}MN \subseteq R$, lo que implica $(MN)^{-1}M \subseteq N^{-1}$ y así $(MN)^{-1} \subseteq M^{-1}N^{-1}$.

□

**Lema 4.3.9.** *Todo ideal de $R$ no trivial es invertible.*

*Demostración.* Sea $M$ un ideal de $R$. Entonces $MM^{-1} = B$ es un ideal de $R$. Demostraremos que para todo ideal maximal $P$ de $R$ se cumple que $BR_P = R_P$. Sea $P$ ideal maximal de $R$. Entonces

$$BR_P = B_P = \left(MM^{-1}\right)_P = M_P\left(M^{-1}\right)_P = M_P M_P^{-1} = R_P = RR_P$$

ya que $R_P$ es DIP y todo ideal fraccionario es invertible. Por el lema 4.2.2 $B = R$. □

**Teorema 4.3.10.** *Sea $M$ un ideal fraccionario de $R$. Entonces*

$$M = P_1^{a_1} \cdots P_n^{a_n}$$

*donde $P_1, \ldots, P_n$ son ideales primos de $R$ y $a_1, \ldots, a_n$ números enteros. Además esta expresión es única.*

*Demostración.* Sea $t \in R$ tal que $tM \subseteq R$. Por el teorema 4.1.14 los ideales $tM$ y $Rt$ son producto de ideales primos de $R$, estos es, $tM = \prod P_i^{a_i}$ y $Rt = \prod Q_j^{b_j}$. Luego

$$\prod P_i^{a_i} = tM = (Rt)M = \left(\prod Q_j^{b_j}\right)M.$$

Como todo ideal de $R$ es invertible, entonces

$$M = \prod P_i^{a_i} \prod Q_j^{-b_j}.$$

Supongamos que

$$M = \prod P_i^{a_i} \prod S_k^{-c_k} = \prod Q_j^{b_j} \prod T_h^{-d_h},$$

donde los ideales $P_i$ y los ideales $S_k$ son distintos, los ideales $Q_j$ y $T_h$ son distintos y $a_i, c_k, b_j$ y $d_h$ son enteros positivos. Como los ideales de $R$ son invertibles, entonces

$$\prod P_i^{a_i} \prod T_h^{d_h} = \prod Q_j^{b_j} \prod S_k^{c_k}.$$

Luego los ideales $P_i$ son iguales, bajo algún reordenamiento, a los idelaes $S_k$ y los ideales $Q_j$ son iguales, bajo algún reordenamiento, a los ideales $T_h$ por la unicidad de la descomposición en ideales primos en un anillo de Dedekind del teorema 4.1.14. □

**Corolario 4.3.11.** *Todo ideal fraccionario es invertible.*

*Demostración.* Sea $M$ un ideal fraccionario. Por el teorema 4.3.10

$$M = P_1^{a_1} \cdots P_n^{a_n}$$

donde $P_1, \ldots, P_n$ son ideales primos de $R$ y $a_1, \ldots, a_n$ son enteros. Luego

$$MM^{-1} = (P_1^{a_1} \cdots P_n^{a_n}) \left(P_1^{-a_1} \cdots P_n^{-a_n}\right) = \left(P_1^{a_1} P_1^{-a_1}\right) \cdots \left(P_n^{a_n} P_n^{-a_n}\right) = R.$$

□

Con esto no sólo hemos demostrado que el conjunto de ideales fraccionarios de un anillo de Dedekind es un grupo, sino también que es un grupo libre, cuyos generadores son los ideales maximales de $R$. Si denotamos por $I(R)$ a este grupo, $P(R)$ al subgrupo de ideales fraccionarios principales y $C(R) = I(R)/P(R)$ el grupo cociente. Podemos observar que si $R$ es DIP, entonces $C(R) = 1$. Por esta razón el grupo $C(R)$ es utilizado para medir qué tan cerca está $R$ de ser un anillo de ideales principales.

# Capítulo 5

# Normas y Trazas

Sea $L/K$ una extensión de campos finita. Para cada $x \in L$ definimos la función $r_x : L \to L$ por $r_x(y) = yx$. La función $r_x$ es una transformación lineal, ya que $L$ es un $K$-espacio vectorial. En efecto, sean $y, z \in L$ y $a \in K$. Entonces

$$\begin{aligned} r_x(y+z) &= (y+z)\,x \\ &= yx + zx \\ &= r_x(y) + r_x(z) \\ r_x(ay) &= (ay)\,x \\ &= a\,(yx) \\ &= a r_x(y). \end{aligned}$$

A continuación mostraremos algunas propiedades sobre esta función.

**Proposición 5.0.12.** *Sean $x, y \in L$ y $a \in K$. Entonces se cumplen los siguientes enunciados:*

1. $r_{x+y} = r_x + r_y$.
2. $r_{xy} = r_y r_x$.
3. $r_{ax} = a r_x$.

*Demostración.* Sea $z \in L$. Entonces:

1. $r_{x+y}(z) = z(x+y) = zx + zy = r_x(z) + r_y(z)$.
2. $r_{xy}(z) = z(xy) = (zx)y = r_y(zx) = r_y(r_x(z)) = r_y r_x(z)$.
3. $r_{ax}(z) = z(ax) = a(zx) = a r_x(z)$.

□

**Definición 5.0.13.** *Sea $\beta$ una base ordenada de $L$ sobre $K$ y sea $A$ la matriz asociada a la transformación $r_x$ con respecto a la base $\beta$. Entonces:*

1. *La traza de $L$ sobre $K$ es la función $T_{L/K}(x) = traza(r_x) = traza(A)$.*
2. *La norma de $L$ sobre $K$ es la función $N_{L/K}(x) = det(r_x) = det(A)$.*

Las funciones traza y norma están bien definidas ya que si $\gamma$ es otra base ordenada de $L$ sobre $K$ y $B$ es la matriz asociada con respecto a la base $\gamma$ , entonces existe una matriz invertible $Q$ tal que $A = QBQ^{-1}$. Luego

$$T_{L/K}(x) = traza(A) = traza\left(QBQ^{-1}\right) = traza(B)$$

y

$$N_{L/K}(x) = det(A) = det\left(QBQ^{-1}\right) = det(B)$$

por lo que son funciones que no dependen de la base que elijamos. Ahora mostraremos algunas propiedades.

**Proposición 5.0.14.** *Sea $L/K$ una extensión de campos finita. Sean $x, y \in L$ y $a \in K$. Entonces se cumplen los siguientes enunciados:*

1. $T_{L/K}(x + y) = T_{L/K}(x) + T_{L/K}(y)$.
2. $T_{L/K}(ax) = aT_{L/K}(x)$.
3. $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.
4. $N_{L/K}(ax) = a^n N_{L/K}(x)$, *donde $n$ es la dimensión de $L$ sobre $K$.*
5. *Sea $E$ un campo tal que $K \subseteq E \subseteq L$. Entonces* $T_{L/K}(x) = T_{E/K}\left(T_{L/E}(x)\right)$.

*Demostración.* Sean $A$ y $B$ las matrices asociadas a las transformaciones $r_x$ y $r_y$ respectivamente. Entonces, por la proposición 5.0.12 y por las propiedades del determinante y la traza de matrices, tenemos

1.
$$\begin{aligned} T_{L/K}(x+y) &= traza\left(r_{x+y}\right) = traza\left(r_x + r_y\right) \\ &= traza(A+B) = traza(A) + traza(B) \\ &= T_{L/K}(x) + T_{L/K}(y). \end{aligned}$$

2.
$$\begin{aligned} T_{L/K}(ax) &= traza\left(r_{ax}\right) = traza\left(ar_x\right) \\ &= traza(aA) = a \cdot traza(A) \\ &= aT_{L/K}(x). \end{aligned}$$

3.

$$\begin{aligned} N_{L/K}(xy) &= det\,(r_{xy}) = det\,(r_y r_x) \\ &= det(BA) = det(B)det(A) \\ &= N_{L/K}(x)N_{L/K}(y). \end{aligned}$$

4.

$$\begin{aligned} N_{L/K}(ax) &= det\,(r_{ax}) = det\,(ar_x) \\ &= det(aA) = a^n det(A) \\ &= a^n N_{L/K}(x). \end{aligned}$$

5. Para el último inciso sea $\{a_1, \ldots, a_n\}$ una base de $E$ sobre $K$ y sea $\{b_1, \ldots, b_m\}$ una base de $L$ sobre $E$. Entonces para toda $x \in L$ se tiene que

$$xb_i = \sum_j \beta_{ij} b_j$$

donde $\beta_{ij} \in E$ para toda $i, j = 1, \ldots, m$. Luego

$$T_{L/E}(x) = \sum_i \beta_{ii}.$$

Como $\beta_{ii} \in E$, entonces

$$\beta_{ii} a_p = \sum_q \alpha_{pq} a_q$$

donde $\alpha_{pq} \in K$. Luego

$$T_{E/K}(\beta_{ii}) = \sum_p \alpha_{pp}.$$

Lo que implica

$$\begin{aligned} T_{E/K}\left(T_{L/E}(x)\right) &= T_{E/K}\left(\sum_i \beta_{ii}\right) \\ &= \sum_i T_{E/K}\left(\beta_{ii}\right) \\ &= \sum_i \sum_p \alpha_{pp}. \end{aligned} \tag{5.1}$$

Por otro lado los elementos $\{a_q b_j\}$ son una base de $L$ sobre $K$. Luego

$$\begin{aligned} xa_p b_i = a_p\left(xb_i\right) &= a_p \sum_j \beta_{ij} b_j \\ &= \sum_j \left(a_p \beta_{ij}\right) b_j = \sum_j \left(\sum_q \alpha_{pq} a_q\right) b_j \\ &= \sum_j \sum_q \alpha_{pq} a_q b_j. \end{aligned}$$

Por lo tanto $T_{L/K}(x) = \sum_i \sum_p \alpha_{pp}$ que coincide con la ecuación 5.1.

□

Definimos el polinomio característico de un elemento $x \in L$ como el polinomio característico de la transformación $r_x$, es decir,

$$f(t) = det\left(tI - r_x\right).$$

Sabemos que es un polinomio mónico y que además $f(r_x) = 0$ por el teorema de Cayley-Hamilton. Más aún $f(x) = 0$ ya que para toda $z \in L$

$$0 = f(r_x)(z) = f(x)z.$$

**Lema 5.0.15.** *Sea $A = (a_{ij})$ la matriz asociada a la transformación $r_x$ con $x \in L$ y sea $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ el polinomio característico de $x$. Entonces*

1. $a_0 = (-1)^n N_{L/K}(x)$.
2. $a_{n-1} = -T_{L/K}(x)$.

*Demostración.* 1. Evaluando $t = 0$ en el polinomio característico tenemos

$$a_0 = f(0) = det\left(-r_x\right)) = (-1)^n N_{L/K}(x).$$

2. Haremos la demostración por inducción sobre $n$. Para $n = 1$ es claro que se cumple. Para $n = 2$ tenemos que

$$det\begin{pmatrix} t - a_{11} & a_{12} \\ a_{21} & t - a_{22} \end{pmatrix} = t^2 - \left(a_{11} + a_{22}\right)t + \left(a_{11}a_{22} - a_{21}a_{12}\right)$$

donde podemos ver que se cumple el lema. Supongamos que el lema es cierto para $n - 1 > 2$. Sea $A_n$ la matriz que se obtiene al eliminar la columna $n$ y la fila $n$ de la

matriz $A$. Luego al desarrollar sobre la columna $n$

$$\begin{aligned} det\,(tI_n - A) &= det \begin{pmatrix} t-a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & t-a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{2n} & \cdots & t-a_{nn} \end{pmatrix} \\ &= (t-a_{nn})\, det\,(tI_{n-1} - A_n) + g(t) \end{aligned}$$

donde $g(t)$ es un polinomio de grado menor o igual a $n-2$. Por hipótesis de inducción

$$\begin{aligned} f(t) &= (t-a_{nn})\, det\,(tI_{n-1} - A_n) + g(t) \\ &= (t-a_{nn})\left(t^{n-1} - traza\,(A_n)\, t^{n-2} + \cdots\right) + g(t) \\ &= t^n - (a_{nn} + traza\,(A_n))\, t^{n-1} + g'(t) \\ &= t^n - traza(A) t^{n-1} + g'(t) \end{aligned}$$

donde $g'(t)$ es un polinomio de grado menor a $n-1$. Por lo tanto $a_{n-1} = -traza(A)$. □

Sea $(,) : L \times L \to K$ dada por

$$(x, y) = T_{L/K}(xy).$$

La función $(,)$ es una forma bilineal simétrica ya que para todo $x, y, z \in L$ y $a, b \in K$ se cumple que

$$\begin{aligned} (ax + by, z) &= T_{L/K}\left((ax + by)z\right) \\ &= T_{L/K}\left(axz + byz\right) \\ &= aT_{L/K}(xz) + bT_{L/K}(yz) \\ &= a(x, z) + b(y, z) \\ (x, y) &= T_{L/K}(xy) = T_{L/K}(yx) = (y, x). \end{aligned}$$

**Definición 5.0.16.** *Decimos que una forma bilineal es no degenerada si $(x, y) = 0$ para toda $y \in L$, entonces $x = 0$.*

**Teorema 5.0.17.** *Sea $L/K$ una extensión de campos finita. La extensión $L/K$ de campos es separable si y sólo si la forma bilineal $(x, y) = T_{L/K}(xy)$ es no degenerada.*

*Demostración.* $\Longrightarrow$) Supongamos que $L/K$ es una extensión separable de grado $n$. Sea $x \in L$ tal que para todo $y \in L$ se cumple $(x, y) = 0$. Por el teorema del elemento primitivo existe $\theta \in L$ tal que $L = K(\theta)$. Además $1, \theta, \ldots, \theta^{n-1}$ es una base de $L$ sobre $K$ para alguna $n$. Así que para mostrar que es una forma bilineal no degenerada basta mostrar que

$\left(x, \theta^i\right) = 0$ para toda $i$. Sea $D = (d_{ij})$ la matriz cuyas entradas son $d_{ij} = \left(\theta^{i-1}, \theta^{j-1}\right)$. Como $x \in L$, entonces $x = \sum_{i=0}^{n-1} b_i \theta^i$ donde $b_i \in K$ para toda $i$. Luego para toda $j = 0, \ldots, n-1$

$$\begin{aligned} \left(x, \theta^j\right) &= \left(\sum_{i=0}^{n-1} b_i \theta^i, \theta^j\right) \\ &= \sum_{i=0}^{n-1} b_i \left(\theta^i, \theta^j\right) = 0. \end{aligned} \tag{5.2}$$

Esta expresión es equivalente a la ecuación

$$(b_0, b_1, \ldots, b_n)\, D = 0.$$

Por lo que basta demostrar que $D$ es una matriz no singular, de este modo $b_i = 0$ para toda $i = 0, \ldots, n-1$ y por lo tanto $x = 0$. Sea $f(t) = Irr(K, \theta)$ y $F$ un campo de descomposición de $f(t)$ sobre $K$, esto es

$$f(t) = \prod_{i=1}^{n} (t - \theta_i)$$

con $\theta_i \in F$. Como $L/K$ es una extensión separable, entonces $\theta_i \neq \theta_j$ para toda $i \neq j$.

El polinomio característico de $\theta$ sobre $K$ es de grado $n$ y además vimos que se anula en $\theta$. Como $f(t)$ es el polinomio mínimo de $\theta$ sobre $K$, entonces $f(t)$ divide al polinomio característico de $\theta$. Lo que implica que son iguales ya que ambos tienen el mismo grado y son mónicos. Al hacer el desarrollo de $f(t)$ obtenemos que el coeficiente de $t^{n-1}$ es $\theta_1 + \cdots + \theta_n$ y como consecuencia del lema 5.0.15 se tiene que

$$T_{L/K}(\theta) = \theta_1 + \cdots + \theta_n.$$

Sea $M_\theta$ la matriz asociada a la transformación lineal $r_\theta$. Entonces $\theta_1, \ldots, \theta_n$ son los valores propios de $r_\theta$ ya que son las raíces de su polinomio característico $f(t)$. Como $\theta_i \neq \theta_j$ para toda $i \neq j$, entoces $M_\theta$ es diagonalizable sobre $F$ y por lo tanto existe una matriz invertible $Q$ tal que

$$Q M_\theta Q^{-1} = diag\,(\theta_1, \ldots, \theta_n)$$

donde $diag\,(\theta_1, \ldots, \theta_n)$ denota a la matriz que tiene en la diagonal a los elementos $\theta_1, \ldots, \theta_n$ y cero en las demás entradas.

La matriz asociada a la transformación $r_{\theta^k}$ es $M_\theta^k$ ya que $r_{\theta^k} = r_\theta \cdots r_\theta$. Luego

$$Q M_\theta^k Q^{-1} = diag\left(\theta_1^k, \ldots, \theta_n^k\right)$$

de donde es fácil ver que la traza está dada por

$$T_{L/K}\left(\theta^k\right) = \theta_1^k + \cdots + \theta_n^k. \tag{5.3}$$

Sea

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_n \\ \theta_1^2 & \theta_2^2 & \cdots & \theta_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \cdots & \theta_n^{n-1} \end{pmatrix}$$

que se conoce como matriz de van der Monde. La entrada $ij$ de la matriz $VV^t$ es de la forma

$$\sum_{k=1}^{n} \theta_k^{i-1}\theta_k^{j-1} = \sum_{k=1}^{n} \theta_k^{i+j-2} = T_{L/K}\left(\theta^{i+j-2}\right) = T_{L/K}\left(\theta^{i-1}\theta^{j-1}\right) = d_{ij}$$

haciendo $k = i + j - 2$ en la ecuación 5.3. Luego $VV^t = D$ y en consecuencia

$$detD = det\left(VV^t\right) = (detV)^2$$

ya que $detV = detV^t$. Se sabe que el determinante de la matriz de van der Monde es

$$\prod_{1 \le i < j \le n} (\theta_j - \theta_i).$$

Como $L/K$ es separable, entonces $\theta_i \neq \theta_j$ si $i \neq j$ y en consecuencia

$$detV \neq 0.$$

Por lo tanto $detD \neq 0$ y la forma bilineal $(,)$ es no degenerada.

$\Longleftarrow$) Supongamos que $L/K$ no es separable. Entonces $K$ es de característica $p$, para algún primo y además existe un campo $F$ tal que $K \subseteq F \subseteq L$, donde $L/F$ es una extensión de campos puramente inseparable y $F/K$ es una extensión de campos separable. Luego $[L : F] = p^m$ para alguna $m \geq 1$ y además para toda $x \in L$ existe un entero positivo $e$ tal que $x^{p^e} \in F$. Nuestro objetivo será demostrar que si $x \in L - F$, entonces $(x, y) = 0$ para toda $y \in L$. Si $xy \notin F$, entonces existe un entero positivo $f$ tal que $Irr(F, xy) = t^{p^f} - a$, con $a \in F$. Sea $q(t)$ el polinomio característico de $xy$ sobre $F$. Luego $Irr(F, xy) \mid q(t)$ y $grq(t) = p^m$, en consecuencia

$$q(t) = \left(t^{p^f} - a\right)^{p^{m-f}}.$$

Esto implica que el coeficiente de $t^{p^m-1}$ es cero ya que $K$ es de característica $p$, por el lema 5.0.15 $T_{L/F}(xy) = 0$. Si $xy \in F$, entonces

$$T_{L/F}(xy) = xyT_{L/F}(1) = xyp^m = 0.$$

Luego, por el inciso (5) de la proposición 5.0.14

$$(x, y) = T_{L/K}(xy) = T_{F/K}\left(T_{L/F}(xy)\right) = T_{F/K}(0) = 0.$$

Por lo tanto (,) es no degenerada.

□

**Teorema 5.0.18** (Teorema de la Base Dual)**.** *Sea $L/K$ una extensión de campos finita y separable y sea $\{u_1, \ldots, u_n\}$ una base $L$ sobre $K$. Entonces existe una base $\{v_1, \ldots, v_n\}$ de $L$ sobre $K$ tal que*

$$T_{L/K}(u_i v_j) = \delta_{ij}$$

*donde $\delta_{ij} = 0$ si $i \neq j$ y $\delta_{ij} = 1$ si $i = j$.*

*Demostración.* Toda función $K$-lineal de $L$ sobre $K$ es de la forma $x \longrightarrow (x, y)$ para alguna $y \in L$. Para cada $i = 1, \ldots, n$, sea $v_i \in L$ el elemento que determina la función $K$-lineal de la siguiente forma $u_j \longrightarrow 0$ si $i \neq j$ y $u_i \longrightarrow 1$. $\{v_1, \ldots, v_n\}$ es un conjunto linealmente independiente ya que si $\sum_{i=1}^{n} a_i v_i = 0$, entonces

$$0 = \left( \sum_{i=1}^{n} a_i v_i, u_j \right) = \sum_{i=1}^{n} a_i (v_i, u_j) = a_j (v_j . u_j) = a_j.$$

Por lo tanto $\{v_1, \ldots, v_n\}$ es una base de $L$ sobre $K$. □

A la base $\{v_1, \ldots, v_n\}$ se le conoce como la base dual de $\{u_1, \ldots, u_n\}$ con respecto a la forma bilineal (,).

**Proposición 5.0.19.** *Sea $L/K$ una extensión de campos finita y separable de grado $n$. Sea $x \in L$, $p(t) = Irr(K, x)$ y sean $x_1, \ldots, x_n$ las raíces de $p(x)$ en algún campo de descomposición, cada una repetida $r = [L : K(x)]$ veces. Entonces $T_{L/K}(x) = x_1 + \cdots + x_n$ y $N_{L/K}(x) = x_1 \cdots x_n$, además el polinomio característico de $x$ respecto a $L$ es de la forma $f(t) = p(t)^r$.*

*Demostración.* Primero supongamos que $x$ es elemento primitivo de la extensión, es decir, $L = K(x)$. Entonces el polinomio característico de $x$ sobre $K$ es de grado $n$ con coeficientes en $K$ y además se anula en $x$. Como $p(t)$ es el polinomio mínimo de $x$ sobre $K$, entonces $p(t)$ divide al polinomio característico de $x$. Lo que implica que son iguales ya que ambos tienen el mismo grado y son mónicos. Al hacer el producto de los factores de $f(t)$, obtenemos que el coeficiente de $t^{n-1}$ es $-(x_1 + \cdots + x_n)$ y el término constante es $(-1)^n x_1 \cdots x_n$. El lema 5.0.15 nos dice que estos coeficientes son la $T_{L/K}(x)$ y la $N_{L/K}(x)$ respectivamente. Luego $T_{L/K}(x) = x_1 + \cdots + x_n$ y $N_{L/K}(x) = x_1 \cdots x_n$. Para demostrar el caso general sea $\{y_1, \ldots, y_q\}$ una base de $K(x)$ sobre $K$ y $\{z_1 \ldots, z_r\}$ una base de $L$ sobre $K(x)$. Entonces $\{y_i z_j\}$ es una base de $L$ sobre $K$ y además $n = qr$. Si $x y_i = \sum_{k=1}^{q} a_{ik} y_k$, entonces

$$\begin{aligned} x\,(y_i z_j) &= (x y_i)\, z_j \\ &= \left( \sum_{k=1}^{q} a_{ik} y_k \right) z_j \\ &= \sum_{k=1}^{q} a_{ik} y_k z_j. \end{aligned}$$

Sea $M$ la matriz asociada a la transformación $r_x$ en $K(x)$. Entonces ordenando la base $\{y_i z_j\}$ obtenemos que la matriz asociada a la transformación $r_x$ en $L$ es de la forma

$$\overline{M} = \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & M. \end{pmatrix}.$$

Luego el polinomio característico de $x$ es

$$f(t) = det\left(tI_n - \overline{M}\right) = det\left(tI_q - M\right)^r.$$

Utilizando que $x$ es elemento primitivo en $K(x)$, tenemos que $p(t) = det\left(M - tI_q\right)$. Desarrollando el polinomio característico y por el lema 5.0.15 tenemos el resultado.

□

**Proposición 5.0.20.** *Sea $R$ un dominio entero, $K$ su campo de cocientes, $L$ una extensión finita y separable sobre $K$. Si $x \in L$ es entero sobre $R$, entonces los coeficientes del polinomio característico $f(t)$ de $x$ son enteros sobre $R$. En particular $T_{L/K}(x)$ y $N_{L/K}(x)$ son enteros sobre $R$.*

*Demostración.* Sea $p(t) = \prod_{i=1}^{n}(t - x_i)$ el polinomio mínimo de $x$ sobre $K$. Por la proposición 5.0.19 se tiene $f(t) = p(t)^r$. Luego para cada $i = 1, \ldots, n$, existe un $K$-isomorfismo $\sigma_i : K(x) \longrightarrow K(x_i)$ tal que $\sigma_i(x) = x_i$. Sea $q(t) = t^k + \cdots + a_0$ un polinomio con coeficientes en $R$ tal que $q(x) = 0$. Aplicando $\sigma_i$ a $q(x)$ obtenemos

$$\begin{aligned} 0 &= \sigma_i\left(x^k + a_{k-1}x^{k-1} + \cdots + a_0\right) \\ &= \sigma_i(x)^k + a_{k-1}\sigma_i(x)^{k-1} + \cdots + a_o \\ &= x_i^k + a_{k-1}x_i^{k-1} + \cdots + a_o. \end{aligned}$$

esto significa que $x_i$ es entero sobre $R$. Cada coeficiente de $f(t)$ es entero sobre $R$ ya que es suma de productos de elementos enteros sobre $R$, en particular por el lema 5.0.15 $T_{L/K}(x)$ y $N_{L/K}(x)$ son enteros sobre $R$. □

**Corolario 5.0.21.** *Si $R$ es enteramente cerrado, entonces $T_{L/K}(x)$ y $N_{L/K}(x)$ pertenecen a $R$.*

# Capítulo 6

# Extensiones de Anillos de Dedekind

El objetivo de este capítulo es demostrar que la cerradura entera de un anillo de Dedekind en una extensión de su campo de cocientes es también un anillo de Dedekind. Este es uno de los teoremas más importantes de esta tesis, ya que gracias a él podemos dar ejemplos no triviales de anillos de Dedekind y además nos permite obtener nuevos anillos de Dedekind a partir de los que ya conocemos.

**Lema 6.0.22.** *Sean $R \subseteq R'$ dominios enteros, $R$ enteramente cerrado y $R'$ entero sobre $R$ en una extensión del campo de cocientes de $R$. Si $\mathfrak{P}$ es un ideal primo no trivial de $R'$, entonces $\mathfrak{P} \cap R$ es un ideal primo no trivial de $R$.*

*Demostración.* $\mathfrak{P} \cap R \neq \langle 0 \rangle$: sea $x \in \mathfrak{P}$ distinto de cero y sea $f(t) = t^n + \cdots + a_0$ el polinomio mónico con coeficientes en $R$ tal que $f(x) = 0$ y de grado mínimo. Entonces $a_0 \neq 0$ ya que de otro modo podríamos factorizar $f(t)$ como producto de polinomios con coeficientes en $R$

$$f(t) = t\left(t^{n-1} + a_{n-1}t^{n-2} + \cdots + a_1\right) = tq(t)$$

donde $q(x) = 0$ y $gr(p(t)) < gr(f(t))$, que no es posible ya que supusimos que $f(t)$ era de grado mínimo. Luego

$$-a_0 = x^n + \cdots + a_1 x \in \mathfrak{P}$$

lo que implica que $a_0 \in \mathfrak{P} \cap R$. $\mathfrak{P} \cap R$ es primo: sean $a, b \in R$ tales que $ab \in \mathfrak{P} \cap R$. Esto implica que $ab \in \mathfrak{P}$, que es primo y por lo tanto $a \in \mathfrak{P}$ o $b \in \mathfrak{P}$. Luego $a \in \mathfrak{P} \cap R$ o $b \in \mathfrak{P} \cap R$. □

**Corolario 6.0.23.** *Si $A$ es campo y $B$ es un dominio entero que contiene a $A$ y entero sobre $A$, entonces $B$ es un campo.*

*Demostración.* Si $B$ no es campo, entonces contiene un ideal maximal $\mathfrak{P}$ propio. Por el lema 6.0.22, $\mathfrak{P} \cap A \subseteq A$ es un ideal primo distinto de cero. Luego $\mathfrak{P} \cap A = A$ ya que $A$ es campo. Esto implica que $1 \in \mathfrak{P} \cap A \subseteq \mathfrak{P}$. Por lo tanto $\mathfrak{P} = B$ lo que contradice la elección de $\mathfrak{P}$. □

**Lema 6.0.24.** *Sea $R$ un anillo de Dedekind, $K$ su campo de cocientes, $E$ una extensión finita sobre $K$ y $R'$ la cerradura entera de $R$ en $E$. Si $\{a_1, \ldots, a_n\}$ es una base de $E$ sobre $K$, entonces existe $\{s_1, \ldots, s_n\} \subseteq R$ tal que $\{s_1 a_1, \ldots, s_n a_n\} \subseteq R'$ es una base de $E$ sobre $K$.*

*Demostración.* Sea

$$Irr(K, a_i) = t^k + \sum_{j=0}^{k-1} \frac{\rho_j}{\tau_j} t^j$$

con $\rho_j, \tau_j \in R$ para toda $j = 0, \ldots, k-1$. Si $\lambda_j = \tau_0 \cdots \tau_{j-1} \tau_{j+1} \cdots \tau_{k-1}$, entonces

$$\frac{\rho_j}{\tau_j} \frac{\lambda_j}{\lambda_j} = \frac{\rho_j \lambda_j}{\theta_i}$$

donde $\theta_i = \tau_0 \cdots \tau_{k-1}$. Luego

$$Irr(K, a_i) = t^k + \frac{\mu_{k-1}}{\theta_i} t^{k-1} + \cdots + \frac{\mu_0}{\theta_i}$$

donde $\mu_j \in R$ para $j = 0, \ldots, k-1$, $\theta_i \neq 0$ y $\theta_i \in R$ para cada $i = 1, \ldots, n$. Multiplicando por $\theta^k$ y evaluando en $a_i$ obtenemos

$$0 = \mu_0 \theta_i^{k-1} + \mu_1 \theta_i^{k-2} (\theta_i a_i) + \cdots + \mu_{k-1} (\theta_i a_i)^{k-1} + (\theta_i a_i)^k .$$

Esto implica que $(\theta_i a_i)$ es entero sobre $R$. El conjunto $\{\theta_1 a_1, \ldots, \theta_k a_k\}$ es linealmente independiente, ya que si

$$0 = \sum_{i=1}^{n} \beta_i (\theta_i a_i) = \sum_{i=1}^{n} (\beta_i \theta_i) a_i = 0,$$

entonces $\beta_i \theta_i = 0$ ya que $\{a_1, \ldots, a_n\}$ es un conjunto linealmente independiente. Esto implica que $\beta_i = 0$ ya que $\theta_i \neq 0$ para toda $i = 1, \ldots, n$. Por lo tanto siempre es posible encontrar una base de $E$ que esté contenida en $R'$. □

**Teorema 6.0.25.** *Sea $R$ un anillo de Dedekind, $K$ su campo de cocientes, $L$ una extensión finita y separable sobre $K$ y $R'$ la cerradura entera de $R$ en $L$. Entonces $R'$ es un anillo de Dedekind.*

*Demostración.* Para la demostración de este teorema utilizaremos el inciso (3) del teorema 4.2.4.

1. $R'$ es enteramente cerrado: si $A$ es la cerradura entera de $R'$ en $L$, entonces $A$ es entero sobre $R$ ya que $R'$ es entero sobre $A$ (proposición 3.0.11). Esto implica que $A \subseteq R'$ por definición de $R'$. Luego $A = R'$.

2. $R'$ es noetheriano: sea $\{a_1, \ldots, a_k\}$ una base de $L$ sobre $K$. Por el lema 6.0.24 podemos suponer $a_i \in R'$ para toda $i = 1, \ldots, k$. Sea $\{b_1, \ldots, b_k\}$ la base dual tal que $T_{L/K}(a_i b_j) = \delta_{ij}$. Mostraremos que $R' \subseteq \sum_i^k Rb_i$, es decir, $R'$ es un $R$-módulo finitamente generado. Sea $y \in R'$. Entonces $y = \sum_i \alpha_i b_i$ con $\alpha_i \in K$. Luego

$$\begin{aligned} T_{L/K}(a_j y) &= T_{L/K}\left(a_j \left(\sum_i \alpha_i b_i\right)\right) \\ &= \sum_i \alpha_i T_{L/K}(a_j b_i) \\ &= \alpha_j. \end{aligned}$$

   Por el corolario 5.0.21 $\alpha_j = T_{L/K}(a_j y) \in R$, ya que $a_j y \in R'$. Por lo tanto para toda $j = 1, \ldots, k$ se tiene que $\alpha_j \in R$. Luego $y \in \sum_i Rb_i$. Todo ideal de $R'$ es submódulo de un $R$-módulo finitamente generado y como $R$ es noetheriano, entonces todo ideal es finitamente generado (proposición 4.3.5).

3. Todo ideal primo $\mathfrak{P}$ de $R'$ es un ideal maximal: sea $\mathfrak{p} = \mathfrak{P} \cap R$, por el lema 6.0.22 es un ideal primo de $R$ distinto de cero. Luego $\mathfrak{p}$ es un ideal maximal ya que $R$ es un anillo de Dedekind. Esto implica que $R/\mathfrak{p}$ es un campo contenido en el dominio entero $R'/\mathfrak{P}$. Sea $\overline{x} = x + \mathfrak{P} \in R'/\mathfrak{P}$. Entonces $x$ satisface un polinomio $f(t)$ mónico con coeficientes en $R$. Si $f(t) = t^k + \cdots + a_o$, con $a_o, \ldots, a_{k-1} \in R$, entonces $\overline{x}$ satisface el polinomio $\overline{f(t)} = t^k + \overline{a_{k-1}} t^{k-1} + \ldots + \overline{a_0} \in (R/\mathfrak{p})[t]$. En efecto

$$\overline{f(\overline{x})} = \overline{x}^k + \overline{a_{k-1}}\overline{x}^{k-1} + \cdots + \overline{a_0} = \overline{f(x)} = \overline{0}$$

   por lo tanto $R'/\mathfrak{P}$ es entero sobre $R/\mathfrak{p}$. Luego por el corolario 6.0.23 $R'/\mathfrak{P}$ es campo y en consecuencia $\mathfrak{P}$ es ideal maximal.

□

Observemos que en el teroema 6.0.25 se demostró que si $L/K$ es separable, entonces $R'$ es un $R$ módulo finitamente generado, este hecho nos será útil más adelante.

Ahora demostraremos el caso general, es decir, para cualquier extensión finita $L/K$. En realidad es suficiente demostrar el teorema para extensiones finitas puramente inseparables ya que toda extensión algebraica se puede obtener por medio de una extensión separable seguida de una extensión puramente inseparable (teorema 1.6.8). Además si $E$ es un campo tal que $E/K$ es una extensión separable, $L/E$ es una extensión puramente inseparable, $R'$ la cerradura entera de $R$ en $E$ y $R''$ la cerradura entera de $R'$ en $L$, entonces $R''$ es la cerradura entera de $R$ en $L$, por lo tanto $R''$ es un anillo de Dedekind.

**Teorema 6.0.26.** *Sea $R$ un anillo de Dedekind, $E$ su campo de cocientes, $L$ una extensión finita y puramente inseparable sobre $E$ y $R'$ la cerradura entera de $R$ en $L$. Entonces $R'$ es un anillo de Dedekind.*

*Demostración.* Para mostrar que $R'$ es de Dedekind utilizaremos el segundo inciso del teorema 4.2.4.

1. Todo elemento $x \in R'$ pertenece sólo a un número finito de ideales primos: demostraremos que existe una función inyectiva $\phi$ entre los ideales primos de $R'$ y los ideales primos de $R$ dada por $\mathfrak{P} \mapsto \mathfrak{P} \cap R$, donde $\mathfrak{P}$ es un ideal primo de $R'$. Por el lema 6.0.22, $\mathfrak{p} = \mathfrak{P} \cap R$ es un ideal primo de $R$ distinto de cero.

   Obsérvese que $x \in R'$ si y sólo si existe $e$, un entero positivo, tal que $x^{p^e} \in R$. En efecto, como $L/E$ es una extensión puramente inseparable, entonces por el teorema 1.6.5 existe $e$ un entero positivo tal que $x^{p^e} \in E$, además $x^{p^e}$ es entero sobre $R$ ya que $x$ lo es, lo que implica que $x^{p^e} \in R$. Si $x^{p^e} \in R$, entonces $x$ es raíz del polinomio $f(t) = t^{p^e} - x^{p^e} \in R[t]$, por lo tanto $x$ es entero sobre $R$ y $x \in R'$.

   Sean $\mathfrak{P}$ y $\mathfrak{Q}$ ideales primos de $R'$ tales que $\mathfrak{P} \cap R = \mathfrak{Q} \cap R$. Si $x \in \mathfrak{P} \subseteq R'$, entonces existe $e$ un entero positivo tal que $x^{p^e} \in \mathfrak{P} \cap R = \mathfrak{Q} \cap R$, luego $x \in \mathfrak{Q}$ ya que es ideal primo. Por lo tanto $\mathfrak{P} \subseteq \mathfrak{Q}$, la otra contención se demuestra de la misma forma, por lo que $\mathfrak{P} = \mathfrak{Q}$. Luego $\phi$ es inyectiva.

   Sea $x \in R'$. Entonces $\phi$ restringida a los ideales primos que contienen a $x$ también es inyectiva y además está en correspondencia con los ideales primos de $R$ que contienen a $x^{p^e}$. Como $R$ es de Dedekind, sólo contiene un número finito de ideales primos que contienen a $x^{p^e}$ y por lo tanto sólo puede haber un número finito de ideales primos de $R'$ que contengan a $x$.

2. $R'_{\mathfrak{P}}$ es DVD para todo ideal maximal $\mathfrak{P}$ de $R'$: sea $S = R - \mathfrak{p}$, donde $\mathfrak{p} = \mathfrak{P} \cap R$. $S$ es un subconjunto multiplicativo de $R$ y en consecuencia de $R'$. Nuestro primer objetivo es mostrar que $R'_{\mathfrak{P}} = R'_S$. Claramente $R - \mathfrak{p} \subseteq R' - \mathfrak{p}$, lo que implica $R'_S \subseteq R'_{\mathfrak{P}}$. Sea $\frac{x}{y} \in R'_{\mathfrak{P}}$ con $x \in R'$ y $y \in R' - \mathfrak{P}$. Si $q \in \mathbb{N}$ es tal que $y^q \in E$, entonces $y^q \in R - \mathfrak{p} = S$ ya que de lo contrario $y \in \mathfrak{P}$ lo que contradice la elección de $y$. Luego $\frac{x}{y} = \frac{xy^{q-1}}{y^q} \in R'_S$. Veamos que $R'_{\mathfrak{P}}$ es la cerradura entera de $R_{\mathfrak{p}}$ en $L$. Sea $\frac{x}{y} \in L$ entero sobre $R_S$. Entonces

$$\frac{x^k}{y^k} + \frac{a_{k-1}}{s}\frac{x^{k-1}}{y^{k-1}} + \cdots + \frac{a_0}{s} = 0$$

   con $a_0, \ldots, a_{k-1} \in R$ y $s \in S$. Multiplicando por $s^k$ obtenemos

$$\frac{s^k x^k}{y^k} + a_{k-1}\frac{s^{k-1}x^{k-1}}{y^{k-1}} + \cdots + s^{k-1}a_0 = 0.$$

   Esto implica que $\frac{sx}{y}$ es entero sobre $R$. Luego $\frac{sx}{y} = r \in R'$ y en consecuencia $\frac{x}{y} = \frac{r}{s} \in R'_S$. Inversamente sea $\frac{x}{y} \in R'_S$, con $x \in R'$ y $y \in S$. Como $R'$ es entero sobre $R$,

entonces $x$ satisface un polinomio

$$x^k + a_{k-1}x^{k-1} + \cdots + a_0 = 0$$

con $a_0, \ldots, a_{k-1} \in R$. Dividiendo entre $y^k$ obtenemos

$$\frac{x^k}{y^k} + \frac{a_{k-1}}{y}\frac{x^{k-1}}{y^{k-1}} + \cdots + \frac{a_0}{y^k} = 0$$

donde $\frac{a_i}{y^{k-i}} \in R_S$. Por lo tanto $\frac{x}{y}$ es entero sobre $R_S$.

Ahora mostremos que $R'_{\mathfrak{P}}$ es un DVD. Sea $\mathfrak{q} = \langle \pi \rangle$ el único ideal maximal de $R_{\mathfrak{p}}$. Anteriormente mostramos que existe una correspondencia uno a uno entre los ideales primos de $R'$ y los ideales primos de $R$. De forma análoga podemos mostrar que existe una correspondencia uno a uno entre los ideales primos de $R'_{\mathfrak{P}}$ y los ideales primos de $R_{\mathfrak{p}}$. Esto implica que $R'_{\mathfrak{P}}$ posee un único ideal maximal $\mathfrak{Q}$ tal que $\mathfrak{Q} \cap R_{\mathfrak{p}} = \mathfrak{q}$. Nos queda por demostrar que $R'_{\mathfrak{P}}$ es DIP. Sea $y \in \mathfrak{Q}$. Entonces $y^q = u\pi^n \in R_{\mathfrak{p}}$ con $u \in U(R_{\mathfrak{p}})$ por la proposición 4.0.21. Elijamos $n$ mínimo tal que $u\pi^n \in \mathfrak{q}$. Sea $x \in R'_{\mathfrak{P}}$ distinto de cero. Entonces $x^q = u_1\pi^d$ con $u_1 \in U(R_{\mathfrak{p}})$ y $d$ un entero positivo. Luego $d = nt + r$, con $0 \leq r < n$. Esto implica que

$$\left(xy^{-t}\right)^q = x^q y^{-qt} = u_1\pi^d u^{-t}\pi^{-nt} = u_2\pi^{d-nt} = u_2\pi^r \in R_{\mathfrak{p}}.$$

Luego $\left(xy^{-t}\right) \in R'_{\mathfrak{P}}$. Por la elección de $n$ se tiene que $\left(xy^{-t}\right) \notin \mathfrak{Q}$ que es el único ideal maximal de $R'_{\mathfrak{P}}$. Luego $\left\langle xy^{-t} \right\rangle = R'_{\mathfrak{P}}$ y en consecuencia $xy^{-t}$ pertenece a las unidades de $R'_{\mathfrak{P}}$. Por lo tanto $x = u_3 y^t$ para toda $x \in R'_{\mathfrak{P}}$. Por lo tanto todo ideal es principal y $R'_{\mathfrak{P}}$ es DVD.

□

Usualmente se define un anillo de Dedekind como un dominio noetheriano, enteramente cerrado en el que todo ideal primo es maximal, en el capítulo cuatro demostramos que esta definición y la que se da en esta tesis son equivalentes. En la demostración del teorema 6.0.25 utilizamos este hecho, que es uno de los resultados más importantes y conocidos sobre los anillos de Dedekind. Sin embargo, en el teorema 6.0.26 no es posible demostrar que $R'$ es un anillo noetheriano como en el teorema 6.0.25, por lo que la tercera equivalencia resulta de gran importancia.

A partir de este teorema podemos dar ejemplos de anillos de Dedekind no triviales.

**Ejemplo 6.0.27.** *El anillo de los enteros $\mathbb{Z}$ es un DIP, por lo tanto es noetheriano, enteramente cerrado y todo ideal primo es maximal. Por lo tanto es una anillo de Dedekind.*

**Ejemplo 6.0.28.** *Sea $\mathbb{Q}\left(\sqrt{d}\right)$ una exensión sobre $\mathbb{Q}$, el campo de cocientes del anillo de los enteros, y $d$ libre de cuadrados. Por la proposición 3.0.19 el anillo $\mathbb{Z}+\mathbb{Z}\sqrt{d}$ es un anillo de Dedekind si $d \equiv 2, 3$ mod 4 y si $d \equiv 1$ mod 4, entonces $\frac{1}{2}\left(\mathbb{Z}+\mathbb{Z}\sqrt{d}\right)$ es un anillo de Dedekind.*

## 6.1. Extensiones de Ideales Primos

Sea $R$ un anillo de Dedekind, $K$ su campo de cocientes, $L$ una extensión finita sobre $K$ y $R'$ la cerradura entera de $R$ en $L$. Sea $\mathfrak{p}$ un ideal primo de $R$. Entonces $pR'$ es un ideal de $R'$ que es un anillo de Dedekind, por lo que existen $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ ideales primos de $R'$ y $e_1, \ldots, e_g$ enteros positivos tales que

$$\mathfrak{p}R' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

**Observación 6.1.1.** *Los ideales $\mathfrak{P}_i$ con $i = 1, \ldots, g$ son todos los ideales primos de $R'$ tales que $\mathfrak{P}_i \cap R = \mathfrak{p}$. En efecto por el lema 6.0.22 $\mathfrak{P}_i \cap R$ es un ideal primo de $R$ no trivial. Además $\mathfrak{p} \subseteq \mathfrak{p}R' \subseteq \mathfrak{P}_i$ para toda $i$. Luego $\mathfrak{p} = \mathfrak{p} \cap R \subseteq \mathfrak{P}_i \cap R$. Como $\mathfrak{p}$ es un ideal maximal, entonces $\mathfrak{P}_i \cap R = \mathfrak{p}$.*

**Definición 6.1.2.** *Con la notación descrita en los párrafos anteriores, definimos el índice de ramificación de $\mathfrak{P}_i$ sobre $R$ como la potencia de $\mathfrak{P}_i$ que aparece en la factorización de $\mathfrak{p}R'$ como producto de ideales primos. Denotaremos el índice de ramificación de $\mathfrak{P}_i$ sobre $R$ por $e(\mathfrak{P}_i/R)$.*

**Ejemplo 6.1.3.** *Sea $L = \mathbb{Q}(\sqrt{2})$ y $R'$ la cerradura entera de $\mathbb{Z}$ en $L$. El ideal primo $\langle 2 \rangle$ tiene la siguiente factorización en $R'$*

$$\langle 2 \rangle R' = \left(\sqrt{2}R'\right)^2.$$

*Por la proposición 3.0.19 $R' = \mathbb{Z} + \mathbb{Z}\sqrt{2}$. Luego el ideal $\sqrt{2}R'$ es un ideal primo ya que*

$$\sqrt{2}R' = \sqrt{2}\left(\mathbb{Z} + \mathbb{Z}\sqrt{2}\right) = 2\mathbb{Z} + \mathbb{Z}\sqrt{2}.$$

*Lo que implica*

$$R'/\sqrt{2}R' = \left(\mathbb{Z} + \mathbb{Z}\sqrt{2}\right) / \left(2\mathbb{Z} + \mathbb{Z}\sqrt{2}\right) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$$

*que es campo. Luego $\sqrt{2}R'$ es un ideal maximal y en consecuencia primo, con índice de ramificación sobre $\mathbb{Z}$ igual a 2.*

Si $L/K$ es una extensión de campos separable, entonces $R'$ es un $R$ - módulo finitamente generado. Luego $R'/\mathfrak{P}$ es un $R/\mathfrak{p}$-módulo finitamente generado que contiene un subanillo isomorfo a $R/\mathfrak{p}$, lo que implica que $R'/\mathfrak{P}$ es una extensión de campos finita sobre $R/\mathfrak{p}$. A la dimensión $[R'/\mathfrak{P} : R/\mathfrak{p}]$ le llamaremos el grado relativo de $\mathfrak{P}$ sobre $\mathfrak{p}$.

**Teorema 6.1.4.** *Sea $R$ un anillo de Dedekind, $K$ su campo de cocientes, $L$ una extensión finita y separable sobre $K$ y $R'$ la cerradura entera de $R$ en $L$. Sea $\mathfrak{p}$ un ideal primo de $R$ y sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ ideales primos de $R'$ y $e_1, \ldots, e_g$ enteros positivos tales que*

$$\mathfrak{p}R' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

*Entonces*

$$\sum_{i=1}^{g} e_i f_i = [L : K] = n$$

*donde*

$$f_i = \left[R'/\mathfrak{P}_i : R/\mathfrak{p}\right].$$

*Demostración.* Consideremos la siguiente sucesión de ideales para cada $i = 1, \ldots, g$

$$R' \supseteq \mathfrak{P}_i \supseteq \mathfrak{P}_i^2 \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i}. \tag{6.1}$$

Dos elementos consecutivos son de la forma $\mathfrak{P}$ y $\mathfrak{P}\mathfrak{P}_i$ donde $\mathfrak{P} = \mathfrak{P}_i^{n_i}$, $n_i \leqslant e_i$. Luego, el anillo $\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i$ es un $R'$ - módulo que se anula al multiplicar por elementos de $\mathfrak{P}_i$, por lo tanto es un $R'/\mathfrak{P}_i$ espacio vectorial. Los subespacios vectoriales de $\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i$ son de la forma $\mathfrak{Q}/\mathfrak{P}\mathfrak{P}_i$ donde $\mathfrak{Q}$ es un ideal de $R'$ tal que $\mathfrak{P}\mathfrak{P}_i \subset \mathfrak{Q} \subset \mathfrak{P}$, que no es posible pues no existen ideales propios entre $\mathfrak{P}$ y $\mathfrak{P}\mathfrak{P}_i$. Luego $\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i$ no tiene subespacios vectoriales propios y por lo tanto es de dimensión 1 sobre $R'/\mathfrak{P}_\mathfrak{i}$. Luego $\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i$ es un $R/\mathfrak{p}$ espacio vectorial de dimensión $f_i$ ya que $[\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i : R/\mathfrak{p}] = [\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i : R'/\mathfrak{P}_i][R'/\mathfrak{P}_i : R/\mathfrak{p}]$. De la sucesión 6.1 obtenemos $e_i$ cocientes de términos consecutivos de la forma $\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i$. Esto implica que la dimensión de $R'/\mathfrak{P}_i^{e_i}$ sobre $R/\mathfrak{p}$ es igual a la suma de las dimensiones de estos cocientes, es decir, $e_i f_i$. Luego por el teorema chino del residuo para anillos

$$R'/\mathfrak{p}R' = \bigoplus_{i=1}^{g} R'/\mathfrak{P}_i^{e_i},$$

lo que implica que $[R'/\mathfrak{p}R' : R/\mathfrak{p}] = \sum_{i=1}^{g} e_i f_i$.

Como $R'$ es un $R$-módulo finitamente generado, entonces $R'_S$ es un $R_S$-módulo finitamente generado, donde $S = R - \mathfrak{p}$. Sea $\{x_1, \ldots, x_n\}$ un conjunto mínimo generador de $R'_S$ sobre $R_S$. Por ser $R$ anillo de Dedekind $R_S$ es un DVD por lo que tiene un único ideal maximal $(R_S)p$, con $p \in R$. Nuestro objetivo es mostrar que $\{x_1, \ldots, x_n\}$ es una base de $L$ sobre $K$. Si $\{x_1, \ldots, x_n\}$ no es linealmente independiente, entonces existe una expresión de la forma

$$\sum_{i=1}^{n} \frac{a_i}{b_i} x_i = 0$$

donde $a_i, b_i \in R$ $b_i \neq 0$ y no todas las $a_i = 0$. Al multiplicar por $\frac{b_1 \cdots b_n}{s}$ con $s \in S$ obtenemos una expresión de la forma

$$\sum_{i=1}^{n} \lambda_i x_i = 0$$

donde $\lambda_i \in R_S$ para toda $i$. Como $R_S$ es DVD, entonces $\lambda_i = u_i p^{r_i}$, con $u \in U(R_S)$ (proposición 4.0.21). Debido a que no todas las $\lambda_i$ son cero, entonces podemos tomar $r_k$

como la máxima potencia de $p$ que divide a toda $\lambda_i$. Luego factorizando $p^{r_k}$ obtenemos

$$p^{r_k}\left(\sum_{i\neq k}\mu_i x_i + u_k x_k\right) = 0$$

donde $\mu_i \in R_S$. Lo que implica

$$x_k = -u_k^{-1}\sum_{i\neq k}\mu_i x_i$$

donde $\mu_i \in R_S$. Esto significa que $R'_S$ está generado por menos de $n$ elementos, lo que contradice la elección que habíamos hecho del conjunto $\{x_1,\ldots,x_n\}$.

Si $\sum_i Kx_i$ es distinto de $L$, entonces existe $y \in L - \sum_i Kx_i$ $y \neq 0$ tal que

$$Ky \cap \sum_i Kx_i = \langle 0\rangle .$$

$L/K$ es una extensión finita y por lo tanto algebraica, lo que implica que existe $f(t) \in K[t]$ mónico tal que $f(y) = 0$. Sea $f(t) = t^m + \sum_{i=0}^{m-1}\frac{\alpha_i}{\beta_i}t^i$ con $\alpha_i, \beta_i \in R$, $\beta_i \neq 0$ para toda $i = 1,\ldots,m-1$ y $\beta = \beta_0\cdots\beta_{m-1}$. Entonces

$$0 = \left(y^m + \sum_{i=0}^{m-1}\frac{\alpha_i}{\beta_i}y^i\right)\beta^m = (\beta y)^m + \sum_{i=0}^{m-1}\gamma_i(\beta y)^i$$

donde $\gamma_i \in R$ para toda $i = 1,\ldots,m-1$.

Luego

$$\beta y \in R' \subseteq R'_S = \sum_i R_S x_i \subseteq \sum_i Kx_i.$$

Lo que implica que $y = 0$ que contradice la elección de $y$. Por lo tanto $\{x_1,\ldots,x_n\}$ es una base de $L$ sobre $K$ y por lo tanto $n = [L:K]$.

Por la proposición 2.0.10 $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ y como $R'_\mathfrak{p} = \sum R_\mathfrak{p}x_i$, entonces

$$\sum_i (R/\mathfrak{p})\,\overline{x_i} \cong \sum_i (R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p})\,\overline{x_i} \cong R'_\mathfrak{p}/\mathfrak{p}R'_\mathfrak{p}.$$

La dimensión de $\sum_i (R/\mathfrak{p})\,\overline{x_i}$ es $n = [L:K]$ y ya mostramos que la dimensión de $R'_\mathfrak{p}/\mathfrak{p}R'_\mathfrak{p} = \sum_{i=1}^g e_i f_i$. □

## 6.2. Norma de un ideal

Sea $R$ un anillo de Dedekind, $K$ su campo de cocientes, $L$ una extensión finita sobre $K$ y $R'$ la cerradura entera de $R$ en $L$ . Si $x \in R'$, entonces por el lema 5.0.21 $N_{L/K}(x) \in R$. En este capítulo utilizaremos la notación $N(x)$ en vez de $N_{L/K}(x)$.

**Definición 6.2.1.** *Sea $A$ un ideal de $R'$. La norma del ideal $A$ es el ideal de $R$ generado por todos los elementos $N(a)$ con $a \in A$. Esto es $N(A) = \sum_{a\in A} R\,(N(a))$.*

A continuación demostraremos algunas propiedades.

**Teorema 6.2.2.** *Sea $R$ un anillo de Dedekind, $K$ su campo de cocientes, $L$ una extensión finita sobre $K$ y $R'$ la cerradura entera de $R$ en $L$. Si $A, B$ son ideales de $R'$ , entonces*

1. *$N(R'a) = R\,(N(a))$ con $a \in R'$.*
2. *Si $S$ es un subconjunto multiplicativo de $R$, entonces $N\,(A_S) = N(A)_S$.*
3. *$N(AB) = N(A)N(B)$.*

*Demostración.* 1. Primero notemos que $N(R') = R$. En efecto, $1 \in R'$, luego $N(1) = 1 \in N(R')$. Esto implica que $N(R') = R$. Luego

$$N(R'a) = \sum_{r\in R'} RN(ra) = \sum_{r\in R'} RN(r)N(a) = N(R')N(a) = RN(a).$$

2. Sea $n = [L : K]$ y sea $\frac{a}{s} \in A_S$ con $a \in A$ y $s \in S$. Entonces $N\left(\frac{a}{s}\right) = \frac{1}{s^n}N(a)$. Luego

$$N\,(A_S) = \sum_{a\in A} R\frac{1}{s^n}N(a) = \frac{1}{s^n}\sum_{a\in A} RN(a) \subseteq N(A)_S.$$

Para demostrar la otra contención sea $x \in N(A)_S$. Entonces $x = \frac{N(a)}{s}$ con $a \in A$ y $s \in S$. Luego

$$x = \frac{N(a)}{s} = s^{n-1}N\left(\frac{a}{s}\right) \in N(A_S).$$

3. Para este inciso utilizaremos el lema 4.2.2, es decir, demostraremos que para todo ideal maximal $\mathfrak{p}$ de $R$ se cumple $N(AB)_\mathfrak{p} = (N(A)N(B))_\mathfrak{p}$. $R_\mathfrak{p}$ es un DVD cuyo único ideal maximal es $\mathfrak{p}R_\mathfrak{p}$. Luego $R'_\mathfrak{p}$ es la cerradura entera de $R_\mathfrak{p}$ en $L$, esto implica que los únicos ideales primos de $R'_\mathfrak{p}$ son los ideales primos de la factorización de $\mathfrak{p}R'_\mathfrak{p}$ (observación 6.1.1). Luego, por el teorema 4.1.16, $R'_\mathfrak{p}$ es DIP. Esto implica que $R'_\mathfrak{p}A = A_\mathfrak{p} = R'_\mathfrak{p}a$ y $R'_\mathfrak{p}B = B_\mathfrak{p} = R'_\mathfrak{p}b$ donde $a, b \in R'_\mathfrak{p}$. Luego por los incisos (1) y (2 )de este teorema

$$\begin{aligned} N(AB)_\mathfrak{p} &= N\left((AB)_\mathfrak{p}\right) = N\left(A_\mathfrak{p}B_\mathfrak{p}\right) \\ &= N\left(R'_\mathfrak{p}aR'_\mathfrak{p}b\right) = N\left(R'_\mathfrak{p}ab\right) \\ &= R'_\mathfrak{p}N(a)N(b) = R'_\mathfrak{p}N(a)R'_\mathfrak{p}N(b) \\ &= N\left(R'_\mathfrak{p}a\right)N\left(R'_\mathfrak{p}b\right) = N\left(A_\mathfrak{p}\right)N\left(B_\mathfrak{p}\right) \\ &= N(A)_\mathfrak{p}N(B)_\mathfrak{p} = \left(N(A)N(B)\right)_\mathfrak{p}. \end{aligned}$$

□

No demostraremos el siguiente teorema pero puede consultarse en [2] página 44.

**Teorema 6.2.3.** *Sea $R$ un anillo de Dedekind, $K$ su campo de cocientes, $L$ una extensión finita sobre $K$ y $R'$ la cerradura entera de $R$ en $L$. Sean $A$ un ideal de $R'$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ ideales primos de $R'$ y $a_1, \ldots, a_g$ enteros positivos tales que*

$$A = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_g^{a_g}.$$

*Sea $\mathfrak{p}_i = \mathfrak{P}_i \cap R$ y sea $f_i$ el grado relativo de $\mathfrak{P}_i$ sobre $R \cap \mathfrak{P}_i$. Entonces*

$$N(A) = \prod_{i=1}^{g} \mathfrak{p}_i^{a_i f_i}.$$

Si $K = \mathbb{Q}$, $R = \mathbb{Z}$ y $A$ un ideal de $R$, entonces $N(A) = (m)$ con $m$ un entero. Si pedimos $m \geq 0$, entonces este entero está determinado de manera única. Llamaremos a $m$ la norma absoluta de $A$ y la denotaremos por $\|N(A)\|$. En otras palabras

$$N(A) = R\|N(A)\|$$

con $\|N(A)\| \geq 0$.

**Proposición 6.2.4.** *Sea $A$ un ideal distinto de cero de la cerradura entera $R'$ de $\mathbb{Z}$ en una extensión finita de $\mathbb{Q}$. Entonces $\|N(A)\|$ es el número de elementos del anillo $R'/A$.*

*Demostración.* Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ ideales primos de $R'$ y $a_1, \ldots, a_g$ enteros positivos tales que

$$A = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_g^{a_g}.$$

Por el Teorema Chino del Residuo

$$R'/A \cong \bigoplus_{i=1}^{g} R'/\mathfrak{P}_i^{a_i}.$$

De manera análoga a la demostración del teorema 6.1.4 cada anillo de la forma $\mathfrak{P}_i^{b_i}/\mathfrak{P}_i^{b_i+1}$ es un $R'/\mathfrak{P}_i$ espacio vectorial de dimensión uno, con $0 \leq b_i < a_i$. Además $R'/\mathfrak{P}_i^{a_i}$ es isomorfo a la suma directa de estos espacios. Luego $|R'/\mathfrak{P}_i^{a_i}| = |R'/\mathfrak{P}_i|^{a_i}$. Además $R'/\mathfrak{P}_i$ es una extensión de grado $f_i$ sobre $\mathbb{Z}/p_i\mathbb{Z}$ para algún primo $p_i$, que es un campo con $p_i$ elementos, esto implica que $R'/\mathfrak{P}_i \cong \mathbb{Z}_{p_i}^{f_i}$. Por lo tanto $|R'/\mathfrak{P}_i| = p_i^{f_i}$. Entonces $|R'/\mathfrak{P}_i^{a_i}| = |R'/\mathfrak{P}_i|^{a_i} = p_i^{a_i f_i}$ y en consecuencia

$$\left|R'/A\right| = \prod_{i=1}^{g} p_i^{a_i f_i}.$$

Por el teorema 6.2.3

$$N(A) = \prod_{i=1}^{g} \langle p_i \rangle^{a_i f_i} = \left\langle \prod_{i=1}^{g} p_i^{a_i f_i} \right\rangle,$$

es decir,

$$\|N(A)\| = \prod_{i=1}^{g} p_i^{a_i f_i} = \left|R'/A\right|.$$

□

**Proposición 6.2.5.** *Sea $K = \mathbb{Q}$, $L$ una extensión finita sobre $K$ y $R'$ la cerradura entera de $R = \mathbb{Z}$ en $L$. Entonces $x \in U(R')$ si y sólo si $N(x) = \pm 1$.*

*Demostración.* $\Longrightarrow$) Si $x \in U(R')$, entonces existe $u \in R'$ tal que $ux = 1$. Tomando normas tenemos que $N(u)N(x) = \pm 1$, lo que implica $N(x) = \pm 1$. $\Longleftarrow$) Sea $f(t) = t^k + \cdots + a_0$ el polinomio característico de $x$. Por el lema 5.0.15 $a_0 = \pm N(x) = \pm 1$. Luego $x\left(x^{k-1} + \cdots + a_1\right) = \pm 1$. Luego $u = x^{k-1} + \cdots + a_1$ es entero sobre $R$ ya que $x$ es entero sobre $R$. Por lo tanto $u$ es el inverso de $x$ en $R'$. □

**Ejemplo 6.2.6.** *Por la proposición 3.0.19 $R' = \mathbb{Z}[\sqrt{-5}]$ es la cerradura entera de $\mathbb{Z}$ en $\mathbb{Q}(\sqrt{-5})$ y por tanto es un anillo de Dedekind. En $R'$ se tiene que*

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

*Encontraremos la descomposición en ideales primos del ideal $\langle 6 \rangle$ en $R'$. Comsideremos el ideal $\mathfrak{p}_1 = \left\langle 2, 1 + \sqrt{-5} \right\rangle$. Claramente $6 \in \mathfrak{p}_1$, lo que implica que $\mathfrak{p}_1 \mid \langle 6 \rangle$. Además $1 - \sqrt{-5} = 2 - \left(1 + \sqrt{-5}\right)$, esto implica que $6 \in \mathfrak{p}_1^2$. Luego $\mathfrak{p}_1^2 \mid \langle 6 \rangle$. Los elementos de $\mathfrak{p}_1$ son de la forma*

$$y = 2\left(a + b\sqrt{-5}\right) + \left(1 + \sqrt{-5}\right)\left(c + d\sqrt{-5}\right)$$

*con $a, b, c, d \in \mathbb{Z}$. Luego*

$$y = (2a + c - 5d) + (2b + d + c)\sqrt{-5} = r + s\sqrt{-5}$$

*donde $r = 2a + c - 5d$, $s = 2b + d + c$ y $r - s = 2a - 6d - 2b$, esto es, $r \equiv s \bmod 2$. Esto implica que $r$ y $s$ son de la misma paridad, lo que nos servirá para demostrar que $\mathfrak{p}_1$ es un ideal maximal. Si $x = m + n\sqrt{-5} \notin \mathfrak{p}_1$, entonces $m$ es par y $n$ es impar o bien $m$ impar y $n$ par. Al tomar el cociente $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_1$ obtenemos que sus únicos elementos son las clases $\sqrt{-5} + \mathfrak{p}_1$ y $0 + \mathfrak{p}_1$. Por lo tanto $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_1$ es un campo y en consecuencia $\mathfrak{p}_1$ es un ideal maximal. Más aún $\|N(\mathfrak{p}_1)\| = 2$.*

*Ahora consideremos el ideal $\mathfrak{p}_2 = \left\langle 3, 1 - \sqrt{-5} \right\rangle$. Es claro que $\mathfrak{p}_2 \mid \langle 6 \rangle$. Los elementos de $\mathfrak{p}_2$ son de la forma*

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

*con* $a, b, c, d \in \mathbb{Z}$. *Luego* $y = (3a + c + 5d) + (3b + d - c)\sqrt{-5} = r' + s'\sqrt{-5}$ *donde* $r' + s' = 3a+3b+6d$. *Esto implica que* $r'+s' \equiv 0 \ mod\ 3$. *Al tomar el cociente* $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_2$ *obtenemos que sus únicos elementos son* $0+\mathfrak{p}_2, \sqrt{-5}+\mathfrak{p}_2$ *y* $2\sqrt{-5}+\mathfrak{p}_2$. *Por lo tanto* $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_2$ *es un campo con tres elementos y en consecuencia* $\mathfrak{p}_2$ *es un ideal maximal. Más aún* $\|N(\mathfrak{p}_2)\| = 3$.

*Ahora consideremos el ideal* $\mathfrak{p}_3 = \langle 3, 1 + \sqrt{-5}\rangle$. *Es claro que* $\mathfrak{p}_3 \mid \langle 6\rangle$. *Los elementos de* $\mathfrak{p}_3$ *son de la forma*

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

*con* $a, b, c, d \in \mathbb{Z}$. *Luego* $y = (3a + c - 5d)+(3b + d + c)\sqrt{-5} = r''+s''\sqrt{-5}$ *donde* $r''-s'' = 3a-3b-6d$. *Esto implica que* $r'-s' \equiv 0 \ mod\ 3$. *Al tomar el cociente* $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_3$ *obtenemos que sus únicos elementos son* $0+\mathfrak{p}_3, \sqrt{-5}+\mathfrak{p}_3$ *y* $2\sqrt{-5}+\mathfrak{p}_3$. *Por lo tanto* $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_3$ *es un campo con tres elementos y en consecuencia* $\mathfrak{p}_3$ *es un ideal maximal. Más aún* $\|N(\mathfrak{p}_3)\| = 3$.

*Por lo tanto* $\langle 6\rangle = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$.

*Notemos que* $\mathfrak{p}_1$ *no es un ideal principal. Si* $\mathfrak{p}_1 = \langle 2, 1 + \sqrt{-5}\rangle = \langle \alpha + \beta\sqrt{-5}\rangle$, *entonces*

$$N\left(\langle \alpha + \beta\sqrt{-5}\rangle\right) = \langle N\left(\alpha + \beta\sqrt{-5}\right)\rangle = \langle \alpha^2 + \beta^2\rangle .$$

*Luego* $\|N(\mathfrak{p}_1)\| = 2 = \alpha^2 + \beta^2$. *Esto implica que* $\alpha = \beta = \pm 1$. *Como* $2 \in \mathfrak{p}_1$, *entonces existe* $\gamma + \delta\sqrt{-5}$ *tal que*

$$\pm 2 = \left(\gamma + \delta\sqrt{-5}\right)\left(1 + \sqrt{-5}\right) = (\gamma - 5\delta) + (\delta + \gamma)\sqrt{-5}$$

*o bien*

$$\pm 2 = \left(\gamma + \delta\sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = (\gamma + 5\delta) + (\delta - \gamma)\sqrt{-5}.$$

*Luego* $\delta + \gamma = 0$, *lo que implica* $\delta = -\gamma$, *lo que implica* $\pm 2 = -6\delta$, *es decir,* $6 \mid 2$ *que no sucede. En el otro caso tendríamos* $\delta = \gamma$ *y de nuevo* $6\delta = 2$.

*Ahora mostraremos que* $R' = \mathbb{Z}[\sqrt{-5}]$ *no es un anillo de factorización única, para eso mostraremos que* $2, 3, 1 \pm \sqrt{-5}$ *son irreducibles en* $R'$, *nótese además que* 2 *no es primo ya que* $2 \mid \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$ *pero no divide a ninguno de estos elementos pues de lo contrario* $\mathfrak{p}_1$ *sería ideal principal, que no sucede como hemos visto. Las normas de estos elementos son* $4, 9, 6$ *respectivamente. Si* $2 = ab$ *con* $a, b \in R' - U(R')$, *entonces* $4 = N(a)N(b)$. *Como* $a$ *y* $b$ *no son unidades, entonces* $N(a) \neq \pm 1$ *y* $N(b) \neq \pm 1$, *proposición 6.2.5. La norma de un elemento* $x + y\sqrt{-5} \in R'$ *es de la forma* $x^2 + y^2 5$, *lo que nos lleva a* $N(b) = N(a) = 2 = x^2 + y^2 5$. *Si* $|y| > 1$, *entonces* $x^2 + y^2 5 > 2$. *Por lo tanto* $y = 0$ *y en consecuencia* $x^2 = 2$ *que no es posible en los enteros. Si* $3 = ab$ *con* $a, b \in R' - U(R')$, *entonces* $9 = N(a)N(b)$. *Como* $a$ *y* $b$ *no son unidades, entonces* $N(a) \neq 1$ *y* $N(b) \neq 1$. *Luego* $N(b) = N(a) = 3 = x^2 + y^2 5$. *Si* $|y| > 1$, *entonces* $x^2 + y^2 5 > 3$. *Por lo tanto* $y = 0$ *y en consecuencia* $x^2 = 3$ *que no es posible en los enteros. Si* 3 *fuera asociado de* $1 \pm \sqrt{-5}$, *entonces* $3 = u\left(1 \pm \sqrt{-5}\right)$ *con* $u \in U(R')$. *Al tomar normas* $N(3) = N(u)N(1 \pm \sqrt{-5})$, *luego* $9 = 6$ *que no sucede. Análogamente,* 2 *no es asociado de* $1 \pm \sqrt{-5}$ *ya que* $2 \neq 6$. *Por lo tanto la factorización no es única. Sin embargo, al ser* $R'$ *un anillo de Dedekind podemos*

*descomponer sus ideales como producto de ideales primos de manera única, lo cual es de gran utilidad ya que es lo más parecido a ser un anillo de factorización única y por esta razón comenzó el estudio de estos anillos.*

# Referencias


[1] Paul J. McCarthy; Algebraic Extensions of Fields; Dover Publications; EUA; 1976.

[2] Gerald J. Janusz ; Algebraic Number Fields; American Mathematical Society, Editorial Board; EUA; 2$^{\underline{a}}$ Edición; 1996.

[3] Pierre Samuel; Teoría Algebraica de números; Barcelona, España; Ediciones Omega; 1972.

[4] Ian Stewart, David Tall; Algebraic Number Theory and Fermat's Last Teorem; Taylor and Francis; EUA; 3$^{\underline{a}}$ Edición; 2001.