00324
8

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ANILLOS DE DEDEKIND EN TEORÍA DE NÚMEROS ALGEBRÁICA

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A

ALEXEI ELEUSIS DÍAZ VERA

DIRECTOR DE TESIS: MAT. LUIS RICARDO COLAVITA FERREYRA

2003

PAGINACION DISCONTINUA

DRA. MARÍA DE LOURDES ESTEVA PERALTA
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:

Anillos de Dedekind en Teoría de Números Algebráica

realizado por Alexei Eleusis Díaz Vera

con número de cuenta 09757171-5 , quién cubrió los créditos de la carrera de Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis
Propietario Mat. Luis Ricardo Colavita Ferreyra

Propietario M. en C. Clotilde García Villa

Propietario Dra. María del Carmen Gómez Laveaga

Suplente Dra. Bertha María Tomé Arreola

Suplente Dr. Juan Morales Rodríguez

Consejo Departamental de Matemáticas

M. en C. José Antonio Gómez Ortega

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMÁTICAS

2

A mis padres, Salamina y Darby.

Índice general

III

Introducción

Este trabajo es la materialización del seminario de tesis dirigido por Luis Colavita Ferreyra en el cual participamos Óscar Ponce Bañuelos y yo.

El objetivo del trabajo de tesis era demostrar que se tenía la madurez y capacidad necesaria para estudiar un tema por nuestra cuenta, en este caso una introducción a la teoría de los números algebráica. Para ello comenzamos estudiando taoría de números clásica, es decir, los *enteros algebráicos en extensiones numéricas finitas de los números racionales*, después estudiamos en característica cero *anillos de Dedekind en extensiones finitas de campos de cocientes de anillos de Dedekind* y por último estudiamos la generalización de todo esto, es decir, *anillos de Dedekind en abstracto, extensiones, separables, totalmente inseparables y levantamientos de ideales primos.*

Este trabajo está organizado de la siguiente manera: el el capítulo 1 se presentan las bases algebráicas necesarias para una buena compresión del material, no se incluyen demostraciones de todos los resultados pero tuve especial cuidado en incluir una demostración de los resultados que iban a ser utilizados en pruebas de la parte principal de la tesis. En el capítulo 2 se presentan los anillos de Dedekind en abstracto, sus propiedades y una descripción general. Por último, en el capítulo 3, revisamos algunos aspectos de las extensiones de los anillos de Dedekind.

Quiero agradecer a mis padres Salamina y Darby por todo su apoyo, pues sin él no habria logrado lo que tengo. También quiero agradecer y reconocer a Luis Colavita el ser un gran maestro, no sólo académicamente. Por último quiero agradecer también a Luis Colavita, Carmen Gómez, Clotilde García y nuevamente a mis padres por su paciencia, que para todo fin práctico fue infinita. A todos ellos mi gratitud y reconocimiento.

Capítulo 1

Preliminares algebráicos

1.1. Anillos

En este trabajo supondremos que el lector está familiarizado con la teoría de anillos elemental, los anillos que manejaremos en todos los casos serán conmutativos con 1. Además los morfismos de anillos deberán siempre asignar el 1 en el 1. A continuación presentaremos los conceptos y resultados que usaremos en estas notas y en la mayoría de los casos no daremos demostración de éstos. Sin embargo pueden ser consultados en la bibliografía recomendada.

Definición 1.1.1 *Sea A un anillo y sean $a, b \in A$ diremos que a* divide a *b $(a|b)$ si existe $c \in A$ tal que $b = ac$.*

Definición 1.1.2 *Sea A un anillo y sea $u \in A$ diremos que u es una* unidad *de A si $u|1$.*

Denotaremos por $U(A)$ al conjunto de las unidades del anillo A.

Proposición 1.1.3 *Sea A un anillo, el conjunto de las unidades de A forma un* grupo abeliano *respecto a la multiplicación en A.*

Definición 1.1.4 *Sea A anillo y $a, b \in A$ diremos que a es* asociado *de b si existe $u \in U(A)$ tal que $b = ua$.*

Proposición 1.1.5 *La relación* ser asociado *es de equivalencia.*

Definición 1.1.6 *Sea A un anillo, diremos que un elemento no nulo $m \in A - U(A)$ es irreducible si para todos $a, b \in A$ tales que $m = ab$ existe $u \in U(A)$tal que $a = um$ ó $b = um$.*

Definición 1.1.7 *Sea A un anillo, sea $p \in A - U(A)$ elemento no nulo, diremos que p es primo si para todos $a, b \in A$ tales que $p|ab$ se tiene que $p|a$ ó $p|b$.*

Definición 1.1.8 *Sea A anillo y sea $\mathfrak{P} \subsetneq A$ ideal, diremos que $\mathfrak{P}$ es primo si para toda pareja $a, b \in A$ cada vez que $a \cdot b \in \mathfrak{P}$ se cumple que $a \in \mathfrak{P}$ o $b \in \mathfrak{P}$.*

Definición 1.1.9 *Sea A anillo y $\mathfrak{I} \subset A$ ideal, diremos que $\mathfrak{I}$ es pincipal si existe $a \in A$ tal que para todo $b \in \mathfrak{I}$ existe $x \in A$ tal que $b = ax$, en tal caso denotaremos a $\mathfrak{I}$ por Aa o por (a).*

Proposición 1.1.10 *En todo dominio entero los elementos primos son también irreducibles.*

Demostración. Sea $p \in D$ primo y $p = ab$ factorización de p, como p es primo entonces $p|a \vee p|b$ supongamos sin pérdida de generalidad que $p|a$ entonces $a = px$, sustituyendo en la factorización de p tenemos $p = pxb$ de donde $xb = 1$ y por lo tanto $b \in U(D)$ lo cual prueba que p es irreducible.

■

Observación 1.1.11 *Notemos que el recíproco de la proposición anterior no es siempre cierto, es decir, en un dominio entero los elementos irreducibles no necesariamente son primos. Esta situación se verá mejor en el siguiente ejemplo.*

Ejemplo 1.1.12 *Consideremos el anillo $\mathfrak{D} = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$ con las operaciones ususales heredadas de $\mathbb{R}$. Observemos ahora que $4 = 2 \cdot 2 = -(1 + \sqrt{5})(1 - \sqrt{5})$ son dos factorizaciones distintas de 4 en irreducibles y que 2 no divide a $1 + \sqrt{5}$ ni a $1 - \sqrt{5}$ e inversamente ninguno de estos dos elementos divide a 2. Es decir ninguno es primo.*

Definición 1.1.13 *Sea A anillo y $a \in A$ elemento no nulo, diremos que a* se factoriza en irreducibles *si existen $m_1, \ldots, m_n \in A$ elementos irreducibles tales que $a = m_1 \cdots m_n$.*

El siguiente teorema es una generalización del teorema chino del residuo visto en álgebra superior.

Teorema 1.1.14 (Teorema chino del residuo) *Sea A anillo y $\mathfrak{O}_1, \ldots, \mathfrak{O}_n$ ideales de A tales que para $i \neq j$ $A = \mathfrak{O}_i + \mathfrak{O}_j$. Sea $\mathfrak{I} = \bigcap \mathfrak{O}_i$, entonces*

$$A/\mathfrak{I} = \bigoplus A/\mathfrak{O}_i.$$

Demostración. Sea $\varphi : A \to \bigoplus A/\mathfrak{O}_i$ dada por $\varphi(a) = (a+\mathfrak{O}_1, \ldots, a+\mathfrak{O}_n)$, claramente es un morfismo de anillos en el que $\mathfrak{I} \subset Nuc\ \varphi$ veremos que la igualdad se da. Sea $a \in Nuc\ \varphi$ entonces $a \in \mathfrak{O}_i$ para toda i entre 1 y n por lo tanto $a \in \mathfrak{I}$. Veremos ahora que φ es un epimorfismo, para probar eso basta probar que $(0 + \mathfrak{O}_1, \ldots, 0 + \mathfrak{O}_{i-1}, 1 + \mathfrak{O}_i, 0 + \mathfrak{O}_{i+1}, \ldots, 0 + \mathfrak{O}_n)$ está en la imagen de φ, es decir, que para toda i entre 1 y n existe $a_i \in A$ tal que:

- $a_i \in \mathfrak{O}_j$ para toda $j \neq i$.
- $a_i - 1 \in \mathfrak{O}_i$.

sabemos que para una i fija $1 = b_{ij} + c_{ij}$ con $b_{ij} \in \mathfrak{O}_i$ y $c_{ij} \in \mathfrak{O}_j$ entonces $c_{ij} = 1 - b_{ij}$ de donde

$$c_i = \prod_{j=1}^{n} c_{ij} = 1 + a_i$$

con $a_i \in \mathfrak{O}_i$ además

$$c_i \in \bigcap_{j \neq i} \mathfrak{O}_j$$

de donde se sigue el resultado deseado.

■

1.2. Dominios de ideales principales

Ahora revisaremos brevemente un tipo de anillos que extienden las propiedades de $\mathbb{Z}$ respecto a la formación de ideales.

Definición 1.2.1 *Un* dominio entero D *es* dominio de ideales principales *(abreviado DIP) si todo ideal en D es de la forma (a) con $a \in D$.*

Ejemplo 1.2.2 *Los ejemplos clásicos de DIP son $\mathbb{Z}$ y $K[x]$.*

Lema 1.2.3 *Sea D un DIP, entonces para todo $p \in D$ p es irreducible si y sólo si (p) es maximal.*

Demostración. $\Rightarrow$) Sea $p \in D$ irreducible y sea $q \in D\backslash\{0\}$ tal que $(p) \subset (q)$ esto quiere decir que $p = qx$ como p es irreducible se tiene necesariamente que $x \in U(D)$ por lo tanto $(p) = (q)$ lo cual quiere decir que (p) es maximal.

$\Leftarrow$) Como (p) es maximal se tiene que es también ideal primo y por lo tanto p es primo.

■

Proposición 1.2.4 *En un DIP todo elemento irreducible es también primo.*

Demostración. Es consecuencia directa de (1.2.3).

■

Lema 1.2.5 *Sea D DIP y sean $a, b \in D$ entonces las siguientes propiedades valen en D:*

1. *$a|b$ si y sólo si $(b) \subseteq (a)$.*
2. *$(a) = (b)$ si y sólo si a y b son asociados.*
3. *Existe el máximo común divisor de a y b denotado por $(a; b)$, un elemento $m \in D$ tal que las relaciones "$x|a$ y $x|b$" y "$x|m$" son equivalentes.*
4. *En D vale la* identidad de Bezout, *es decir, existen $x, y \in D$ tales que $(a; b) = ax + by$.*

Dominios de valuación discreta

Definición 1.2.6 *Un* anillo local *es un anillo con sólo un ideal maximal.*

Definición 1.2.7 *Un* dominio de valuación discreta *(abreviado DVD) es un DIP* local.

Propiedades de los DVD.
Sea D un DVD y $\pi \in D$ tal que $D\pi$ es el ideal maximal en D.

1. $\forall x \in D\backslash\{0\} \exists k \in \mathbb{N} \exists u \in U(D) \quad x = \pi^k u$

2. Todo ideal no nulo en D es de la forma $D\pi^k$.

3. D solo tiene un ideal primo no nulo, a saber $D\pi$.

Ejemplo 1.2.8 *Sea* $D = \{\frac{a}{b} \in \mathbb{Q} | b$ *es impar*$\}$ *entonces, con las operaciones usuales de* $\mathbb{Q}$, D *es un* dominio de valuación discreta *y su ideal primo es* $\mathfrak{P} = \{\frac{a}{b} \in D | a$ *es par*$\}$, *su elemento primo es* $\frac{2}{1}$. *Observemos que* $\mathbb{Z} \subseteq D \subseteq \mathbb{Q}$.

El procedimiento del ejemplo anterior es en realidad *localizar* los enteros en el complemento de $2\mathbb{Z}$, lo mismo podría hacerse para cualquier ideal primo y el hecho de que $\mathbb{Z}$ sea DIP garantiza que el anillo resultante será un DVD. Veremos más sobre estas técnicas en la sección 1.6.

1.3. Dominios euclideanos

Una herramienta importante con la que se prueba el *Teorema fundamental de la aritmética* para los *enteros* es el algoritmo de la división, lo mismo sucede con el anillo de polinomios $K[x]$, la unicidad de la factorización en irreducibles hace uso de esta misma propiedad. Esta puede ser generalizada en un tipo de dominios enteros a los que llamaremos *dominios euclideanos.*

Definición 1.3.1 *Sea* D *un dominio entero, una* función euclideana *para* D *es una función* $\phi : D\backslash\{0\} \longrightarrow \mathbb{N}$ *tal que:*

(i) Para toda pareja $a, b \in D\backslash\{0\}$ *si* $a|b$ *entonces* $\phi(a) \leq \phi(b)$.

(ii) Para toda pareja $a, b \in D\backslash\{0\}$ *existen* $q, r \in D$ *tales que* $a = bq + r$ *con* $r = 0$ *o* $\phi(r) \leq \phi(b)$.

Definición 1.3.2 *Un* dominio euclideano *es una pareja* (D, ϕ) *donde* D *es dominio entero y* ϕ *es una función euclideana.*

El hecho de que el *codominio* de toda *función euclideana* sean los números naturales será de gran utilidad, como veremos a continuación, pues podremos hacer uso de la estructura algebráica de éstos últimos para obtener resultados acerca de los *dominios euclideanos.*

Proposición 1.3.3 *Todo* dominio euclideano *es un dominio de ideales principales.*

Demostración. Sea D dominio euclideano y $\mathfrak{A} \subset D$ ideal no nulo. Sea $a \in \mathfrak{A}$ tal que $\phi(a)$ es mínimo en la imagen de $\mathfrak{A}$ bajo ϕ. Afirmamos que $\mathfrak{A} = (a)$ para probar esto tomemos un elemento $b \in \mathfrak{A}$ arbitrario y no nulo entonces $b = aq + r$ con $r = 0$ o $\phi(r) < \phi(a)$ pero como b y aq son elemetos de $\mathfrak{A}$ se tine necesariamente que r también lo es, y por la forma en que elegimos a a se tiene que $r = 0$ lo cual prueba que $\mathfrak{A} = (a)$.

■

Proposición 1.3.4 *Sea D un* dominio euclideano *y ϕ su* función euclideana, *entonces lo siguiente se cumple:*

a) Para todo $a \in D$ se tiene que $\phi(1) \leq \phi(a)$

b) Para todo $a \in D$ se cumple que $a \in U(D)$ si y sólo si $\phi(a) = \phi(1)$

Demostración.

a) Esto es consecuencia inmediata de que para toda $a \in D$ 1 divide a a.

b) $\Rightarrow$) Sea $u \in U(D)$ como $u|1$ se sigue la igualdad.

$\Leftarrow$) Sea $a \in D$ tal que $\phi(a) = \phi(1)$ entonces $1 = aq + r$ con $r = 0$ o $\phi(r) < \phi(a)$ nuevamente r debe ser cero porque $\phi(a)$ es mínima y por lo tanto $a \in U(D)$.

■

Enteros gaussianos

Veremos ahora un ejemplo de *Dominio euclideano* diferente de $\mathbb{Z}$ y $K[x]$.

Definición 1.3.5 *Un* entero gaussiano *es un número complejo de la forma $a+bi$ con $a, b \in \mathbb{Z}$. Para un entero gaussiano $\alpha = a+bi$ definiremos la* norma de α *denotada por $N(\alpha) = a^2 + b^2$.*

Denotaremos por $\mathbb{Z}[i]$ al conjunto de todos los enteros gaussianos.

Observación 1.3.6 *El conjunto de los enteros gaussianos forma un dominio entero con las operaciones heredadas de $\mathbb{C}$.*

Observación 1.3.7 *Sean $\alpha, \beta \in \mathbb{Z}[i]$ entonces:*

- $N(\alpha) \geq 0$.
- $N(\alpha) = 0$ *si y sólo si* $\alpha = 0$.
- $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proposición 1.3.8 *La norma de los enteros gaussianos es una* función euclideana. *Es decir, $(\mathbb{Z}, N)$ es un dominio euclideano.*

Demostración. Observemos que para todo entero gaussiano no nulo se cumple que su norma es mayor o igual que 1 por lo tanto para toda pareja de elementos no nulos $\alpha, \beta \in \mathbb{Z}[i]$ el hecho de que la norma sea multiplicativa garantiza que $N(\alpha) \leq N(\alpha\beta)$, lo cual prueba que se satisface el primer axioma de funciones euclideanas.

Falta ver que vale el algoritmo de la división. Sea $\alpha = a_1 + a_2 i$ y $\beta = b_1 + b_2 i \neq 0$. Debemos encontrar $\gamma, \delta \in \mathbb{Z}[i]$ tales que $\alpha = \beta\gamma + \delta$ con $N(\delta) < N(\beta)$ o $\delta = 0$. Expresemos a $\gamma = q_1 + q_2$ y trataremos de determinar que condiciones deben de cumplir q_1 y q_2, entonces tendríamos que:

$$\delta = (a_1 + a_2 i) - (b_i + b_2 i)(q_1 + q_2 i)$$

$$= (a_1 - b_1 q_1 + b_2 q_2) + (a_2 - b_1 q_2 - b_2 q_1)i.$$

Entonces la prueba se reduce a encontrar valores enteros para q_1 y q_2 tales que:

$$N(\delta = (a_1 - b_1 q_1 + b_2 q_2)^2 + (a_2 - b_1 q_2 - b_2 q_1)^2 < b_1^2 + b_2^2,$$

es decir,

$$\frac{(a_1 - b_1 q_1 + b_2 q_2)^2}{b_1^2 + b_2^2} + \frac{(a_2 - b_1 q_2 - b_2 q_1)^2}{b_1^2 + b_2^2} < 1.$$

Observemos ahora que

$$d^2 = \frac{(a_1 - b_1 q_1 + b_2 q_2)^2}{b_1^2 + b_2^2}$$

el cuadrado de la distancia euclideana de un punto de coordenadas (q_1, q_2) a una recta l cuya ecuación es $a_1 - b_1 x + b_2 y = 0$. Análogamente

$$d'^2 = \frac{(a_2 - b_1 q_2 - b_2 q_1)^2}{b_1^2 + b_2^2}$$

es el cuadrado de la distancia euclideana del punto con coordenadas (q_1, q_2) a la recta l' de ecuación $a_2 - b_2 x - b_y = 0$. Nótese además que l y l' son perpendiculares. Sea P el punto de intersección de l y l', por el teorema de Pitágoras sabemos que $d^2 + d'^2$ es el cuadrado de la distancia entre P y el punto de coordenadas (q_1, q_2), entonces nustro problema nuevamente se reduce, ahora debemos encontrar $q_1, q_2 \in \mathbb{Z}$ tal que su distancia euclideana a P sea menor que 1, pero esto siempre es posible,por lo tanto la norma de los enteros gaussianos es una función euclideana.

■

1.4. Anillos noetherianos.

El estudio de los anillos nochterianos es importante para nosotros pues los anillos que más nos interesan, que son los anillos de *Dedekind* son noetherianos.

Definición 1.4.1 (Anillo noetheriano) *Un anillo A es* noetheriano *si para toda cadena ascendente de ideales $\mathfrak{A}_1 \subseteq \cdots \subseteq \mathfrak{A}_n \subseteq \cdots$ existe $N \in \mathbb{N}$ tal que $\mathfrak{A}_N = \mathfrak{A}_{N+1} = \cdots$.*

Teorema 1.4.2 *Sea A anillo, son equivalentes para A:*

I) *A es noetheriano.*

II) *Todo ideal de A es finitamente generado.*

III) *Todo subconjunto no vacío de ideales de A tiene elementos maximales.*

Demostración.
I)⇒II) Probaremos esto por contradicción. Supongamos que existe un ideal $\mathfrak{I} \subset A$ que no es finitamente generado, entonces exite un conjunto

$$\{a_1, \ldots, a_n, \ldots\} \subset \mathfrak{I}$$

tal que para todo natural n se cumple que

$$a_n \notin < a_1, \ldots, a_{n-1} >$$

entonces la siguiente cadena de ideales

$$< a_1 > \subset < a_1, a_2 > \subset \cdots \subset < a_1, \ldots, a_n > \subset \cdots$$

no se estaciona. De donde podemos concluir que en un anillo noetheriano los ideales son finitamente generados.
II)⇒III) Sea $\emptyset \neq \mathscr{S}$ conjunto de ideales de A y sea $\mathscr{C}$ cadena no vacía en $\mathscr{S}$, sea

$$\mathfrak{C} = \bigcup_{\mathfrak{I} \in \mathscr{C}} \mathfrak{I}$$

entonces existen $a_1, \ldots, a_n \in \mathfrak{C}$ tales que $\mathfrak{C} = < a_1, \ldots, a_n >$ pero por construcción existe $\mathfrak{I} \in \mathscr{C}$ tal que $a_1, \ldots, a_n \in \mathfrak{I}$ por lo tanto $\mathscr{C}$ se estaciona en $\mathfrak{I}$ y es por lo tanto elemeto maximal de $\mathscr{S}$.
III)⇒I) Dado que toda cadena de ideales en A tiene al menos un elemento maximal y que el hecho de ser cadena la restringe a tener no más de un maximal, se tiene necesariamente que se estaciona y el anillo es por lo tanto noetheriano.

■

Corolario 1.4.3 *Todo DIP es* noetheriano.

Demostración. Esto es porque todo ideal es finitamente generado.

■

Corolario 1.4.4 *Todo dominio euclideano es* noetheriano.

■

Proposición 1.4.5 *En un dominio noetheriano D la factorización en irreducibles es posible, aunque no necesariamente es única.*

Demostración. Sea $(a) \subset D$ maximal con la propiedad de ser ideal principal propio y que el generador no puede ser factorizado en irreducibles, veremos que tal ideal no existe. Claramente a no puede ser irreducible pues en tal caso el mismo sería una factorización en irreducibles, por lo tanto, sea $a = bc$ factorización de a donde ni b ni c son unidades, claramente tampoco pueden ser irreducibles pues serían una factorización de a en irreducibles, por lo tanto $(a) \subsetneq (b)$ y $(a) \subsetneq (c)$ por la maximalidad de (a) se tiene que
$b = u_1 p_1 \cdots p_n$ y $c = u_2 q_1 \cdots q_m$ son factorizaciones en irreducibles y por lo tanto $a = (u_1 u_2) p_1 \cdots p_n q_1 \cdots q_m$ es una factorización en irreducibles de a por lo tanto dicho a no puede existir y por lo tanto el resultado es válido.

■

Ejemplo 1.4.6 *Consideremos el anillo* $\mathfrak{O} = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$ *con las operaciones ususales heredadas de* $\mathbb{R}$. *Observemos ahora que* $4 = 2 \cdot 2 = -(1 + \sqrt{5})(1 - \sqrt{5})$ *son dos factorizaciones distintas de* 4 *en irreducibles y que* 2 *no divide a* $1 + \sqrt{5}$ *ni a* $1 - \sqrt{5}$ *e inversamente ninguno de estos dos elementos divide a* 2. *Es decir ninguno es primo.*

Corolario 1.4.7 *La factorización en* irreducibles *es posible en todo DIP.*

Demostración. Esto es por que todo DIP es noetheriano.

■

Definición 1.4.8 *Sea* A *anillo y sea* $\mathfrak{I}_1, \ldots, \mathfrak{I}_n \subseteq A$ *familia de ideales de* A *definiremos el producto de ideales* $\mathfrak{I}_1 \cdots \mathfrak{I}_n = \{\sum a_{1i} \cdots a_{ni} | a_{ji} \in \mathfrak{I}_i\}$.

Lema 1.4.9 *Sea* A *anillo y sean* $\mathfrak{I}, \mathfrak{J}, \mathfrak{P} \subseteq A$ *ideales, entonces* $\mathfrak{P}$ *es ideal primo si y sólo si cada vez que* $\mathfrak{I} \cdot \mathfrak{J} \subseteq \mathfrak{P}$ *se debe tener que* $\mathfrak{I} \subseteq \mathfrak{P}$ *o* $\mathfrak{J} \subseteq \mathfrak{P}$.

Lema 1.4.10 *Sea* A *anillo noetheriano, todo ideal en* A *contiene un producto de ideales primos.*

Demostración. Probaremos esto por reducción al absurdo, sea $\mathfrak{I}$ ideal de A maximal respecto de la propiedad de que es ideal propio de A y no contiene un producto de ideales primos claramente $\mathfrak{I}$ no puede ser un ideal primo, entonces existen $a, b \in A$ tales que ninguna está en $\mathfrak{I}$ y $ab \in \mathfrak{I}$ entonces si hacemos $\mathfrak{J} = \mathfrak{I} + < a >$ y $\mathfrak{K} = \mathfrak{I} + < b >$ tenemos que $\mathfrak{I}$ está contenido propiamente en ambos y además, por la maximalidad de $\mathfrak{I}$, cada uno contiene un producto de ideales primos, pero $\mathfrak{J}\mathfrak{K} \subset \mathfrak{I}$ y por lo tanto también $\mathfrak{I}$ contiene un producto de ideales primos, lo cual contradice la maximalidad de $\mathfrak{I}$, de donde se sigue el resultado.

■

Corolario 1.4.11 *Sea* A *anillo noetheriano, entonces existen ideales primos distintos* $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n$ *y enteros no negativos* $a_1, a_2, \ldots, a_n$ *tales que* $(0) = \mathfrak{P}_1^{a_1} \mathfrak{P}_2^{a_2} \cdots \mathfrak{P}_n^{a_n}$

■

Observación 1.4.12 *En el caso de que D sea un* dominio entero noetheriano *entonces el ideal* (0) *es primo y el mismo es su factorización en ideales primos.*

Lema 1.4.13 *Sea A anillo* noetheriano que no es dominio entero *en el que cada ideal primo es maximal. Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ ideales primos distintos de A tales que:*

$$(0) = \mathfrak{P}_1^{a_1}\mathfrak{P}_2^{a_2}\cdots\mathfrak{P}_n^{a_n}$$

entonces:

$$A \cong \bigoplus A/\mathfrak{P}_i^{a_i}$$

Demostración. Esto se sigue inmediatamente de *Teorema Chino del Residuo.*

■

Corolario 1.4.14 *Sea A anillo* noetheriano que no es dominio entero *en el que todos los ideales primos son maximales. Los ideales al los que se refiere el lema anterior: $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ son todos los ideales primos de A.*

Demostración. Esto se debe a que los ideales en la imagen son de la forma $\bigoplus \mathfrak{I}_i/\mathfrak{P}_i^{a_i}$ con $\mathfrak{I}_i \subset \mathfrak{P}_i$ ideales de A pero los únicos ideales primos son aquellos en los que todos los sumandos son cero excepto uno que debe de ser $\mathfrak{P}_i$ precisamente. Estos ideales son la imagen de los ideales primos de A y por lo tanto son todos.

■

1.5. Dominios de factorización única

En esta sección estudiaremos un tipo muy importante de anillos llamados de *factorización única* que son anillos en los que pueden tratarse conceptos como *máximo común divisor, mínimo común múltiplo* y un poco más de la teoría de divisibilidad desarrollada en $\mathbb{Z}$ y $K[x]$. El resultado principal de esta sección (1.5.6) nos permitirá construir una infinidad de *dominios de factorización única* a partir de uno dado.

Definición 1.5.1 *Un* dominio entero D *es un* dominio de factorización única *(abreviado DFU) si se cumplen las siguientes dos condiciones:*

i) *Todo elemento no nulo en D que no sea una unidad se puede expresar como un producto finito de elementos irreducibles.*

ii) *Si $p_1 \cdots p_r$ y $q_1 \cdots q_s$ son dos factorizaciones del mismo elemento con p_i, q_j irreducibles , entonces $r = s$ y existe una renumeración de los q_j tal que p_i y q_i son asociados para toda i.*

Ejemplo 1.5.2 *Es por todos conocido que tanto $\mathbb{Z}$ como $K[x]$ son ejemplos de DFU, con K un campo arbitrario.*

Veremos ahora un criterio para determinar cuando la factorización en irreducibles es única, si es que esta es posible.

Teorema 1.5.3 *Sea D un dominio en el que la factorización en irreducibles es posible. Entonces la factorización es única si y solo si todo elemento* irreducible *en D es también* primo.

Demostración.
$\Rightarrow$) Supongamos que la factorización en irreducibles es única y sea $p \in D$ irreducible, mostraremos que p es primo, supongamos que $p|ab$ con $a, b \in D\backslash\{0\}$ entonces $pc = ab$ factorizamos a a, b, c en irreducibles:

$$a = p_1 \cdots p_n$$

$$b = q_1 \cdots q_m$$

$$c = r_1 \cdots r_l$$

donde p_i, q_i, r_i son irreducobles entonces

$$p(r_1 \cdots r_l) = (p_1 \cdots p_n)(q_1 \cdots q_m)$$

la factorización única implica que p es asociado de algún irreducible de los p_i o q_i, es decir, p divide a a o a b y por lo tanto p es primo.

$\Leftarrow$) Lo probaremos por inducción sobre la cantidad de factores en una factorización en irreducibles, supongamos que

$$p_1 \cdots p_n = q_1 \cdots q_m$$

la inducción la haremos sobre n.

- $n = 0$) Esto es evidente.
- $n = 1$) $p_1 = q_1 \cdots q_m$, supongamos sin pérdida de generalidad que q_1 es irreducible, entonces $m = 1$ pues en caso contrario se tendría que $q_2 \cdots q_m \in U(A)$ lo cual es una contradicción.
- Paso inductivo. Supongamos que el resultado es válido para n, es decir, si $p_1 \cdots p_n = q_1 \cdots q_m$ entonces $n = m$ y hay una renumeración de los q_i tal que p_i es asociado de q_i.

  Sea $p_1 \cdots p_{n+1} = q_1 \cdots q_m$ donde los p_i y los q_i son irreducibles entonces p_{n+1} es asociado de algún q_i por ser primo, supongamos sin pérdida de generalidad que p_{n+1} es asociado de q_m entonces $p_1 \cdots p_n = q_1 \cdots q_{m-1}$, por hipótesis de inducción tenemos que $n = m - 1$ y que hay una renumeración de los q_i tal que p_i es asociado de q_i, lo cual prueba la unicidad de la factorización.

■

Corolario 1.5.4 *Todo DIP es DFU.*

Demostración. Es consecuencia directa de (1.2.4) y (1.5.3).

■

Corolario 1.5.5 *Todo dominio euclideano es* dominio de factorización única.

■

A continuación el resultado más importante concerniente a los *dominios de factorización única.* No daremos la prueba de este resultado porque nos desviaría de nuestro objetivo. Sin embargo su importancia y utilidad son evidentes.

Teorema 1.5.6 *Sea D DFU, entonces $D[x]$ es DFU.*

Corolario 1.5.7 *Si K es un campo, entonces $K[x_1, x_2, \ldots, x_n]$ es DFU.*

■

1.6. Anillo de fracciones

En esta sección estudiaremos una generalización de la construcción de los racionales a partir de los enteros pero aplicada en anillos en general.

Definición 1.6.1 *Sea A anillo y $S \subset A$ un conjunto no vacío, diremos que S* es multiplicativo *si para toda pareja $s, t \in S$ se tiene que $st \in S$.*

Definición 1.6.2 *Sea A anillo y $S \subset A$ conjunto multiplicativo, definiremos la siguiente relación en $A \times S$. $(a, s) \sim (a', s')$ si y sólo si existe $t \in S$ tal que $t(as' - a's) = 0$.*

Proposición 1.6.3 *La relación definida en (1.6.2) es de equivalencia.*

Demostración.

- Reflexividad. Claramente $(a, s) \sim (a, s)$ pues para cualquier $t \in S$ $t(as - as) = 0$.
- Simetría. Sean $(a, s), (a', s') \in A \times S$ tales que $(a, s) \sim (a', s')$ entonces existe $t \in S$ tal que $t(as' - a's) = 0$ pero $t(as' - a's) = -t(a's - as')$ por lo tanto $(a', s') \sim (a, s)$.
- Transitividad. Sean $(a, s) \sim (a', s')$ y $(a', s') \sim (b, t)$ en $A \times S$ entonces existen $r, r' \in S$ tales que:

$$r(as' - a's) = 0 \tag{1.1}$$

$$r'(a't - bs') = 0 \tag{1.2}$$

quisiéramos probar que existe $u \in S$ tal que $u(at - bs) = 0$. Multiplicando (1.1) por t y (1.2) por s y restándolas tenemos:

$$rs'(at - bs) = 0$$

lo cual prueba lo que deseábamos pues S es multiplicativo y por esa razón $rs' \in S$.

De donde podemos concluir que la relación es de equivalencia.

■

Definición 1.6.4 (Anillo de fracciones) *Sea $S^{-1}A = A \times S/\sim$. Denotaremos a la clase de (a,s) por $\frac{a}{s}$. Daremos además estructura de anillos a $S^{-1}A$ de la siguiente manera:*

- $\frac{a}{s} + \frac{a'}{s'} = \frac{as'+a's}{ss'}$
- $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$

Proposición 1.6.5 *La estructura definida en 1.6.4 está bien definida, es decir, no depende de los representantes. Y $S^{-1}A$ con estas operaciones es un anillo.*

Demostración. Como la suma y producto definidos en (1.6.4) son conmutativos, basta probar el resultado para un operando.

Sean $\frac{a}{s} = \frac{a'}{s'}, \frac{b}{t} \in S^{-1}A$ sabemos que existe $r \in S$ tal que $r(as' - a's) = 0$.

- Suma. De lo anterior se sigue que

$$t^2 r(as' - a's) = 0$$

$$rt(t(as' - a's) + b(ss' - ss)) = 0$$

$$rt(ats' + bss' - a'ts - bs's) = 0$$

$$rt((at + bs)s' - (a't + bs')s) = 0$$

$$r((at + bs)s't - (a't + bs')st) = 0$$

  que por definición indica que $\frac{at+bs}{st} = \frac{a't+bs'}{s't}$ que es lo que queríamos probar.

- Producto. Sabemos que $btr(as' - a's) = 0$ de donde $r(abs't - a'bst) = 0$ que por definición indica que $\frac{ab}{st} = \frac{a'b}{s't}$.

El resto de la demostración sale con cálculos directos.

■

Observación 1.6.6 *Notemos el hecho de que si el 0 de un anillo es parte de un conjunto multiplicativo, al construir el anillo de fracciones el resultado será el anillo 0. Por esta razón convendremos, a menos que se indique, que ningún conjunto multiplicativo tendrá al 0 como elemento.*

Observación 1.6.7 *Si S es un conjunto multiplicativo en A y $S^* = S \cup \{1\}$ entonces $S^{-1}A \cong S^{*-1}A$. Supondremos a partir de este punto, sin pérdida de generalidad, que todo conjunto multiplicativo tendrá al 1 como elemento.*

Observación 1.6.8 *Si D es un dominio entero el conjunto $S = D - \{0\}$ es multiplicativo y en este caso $S^{-1}D$ es el campo de cocientes de D.*

Observación 1.6.9 *Cuando construimos un anillo de fracciones teniendo como base un dominio entero, el resultado será también un dominio entero, que es además subanillo del campo de cocientes del anillo original.*

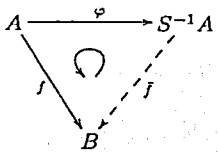
Sea A anillo y $S \subset A$ multiplicativo, sea $\varphi : A \to S^{-1}A$ dada por $\varphi(a) = \frac{a}{1}$. Llamaremos a φ la vinculación natural entre A y $S^{-1}A$ y se puede probar que:

- Para todo $s \in S$ el elmento $\varphi(s) \in U(S^{-1}A)$.
- Para todo $a \in A$. $\varphi(a) = 0$ si y sólo si existe $s \in S$ tal que $as = 0$.
- Para todo $x \in S^{-1}A$ existen $a \in A$ y $s \in S$ tales que $x = \frac{a}{s}$.

Veremos ahora una propiedad muy importante que tiene el *morfismo* φ. En cierto sentido esta propiedad indica que el anillo de fracciones es mínimo anillo, salvo inyectividad, con la propiedad de que todos los elementos de un conjunto multiplicativo se vuelven invertibles.

Teorema 1.6.10 (Propiedad universal del anillo de fracciones) *Sea A anillo y $S \subset A$ multiplicativo y sea φ La vinculación natural entre A y $S^{-1}A$. Entonces φ es un morfismo de anillos con las siguientes propiedades:*

1. *Para todo $s \in S$ se tiene que $\varphi(s) \in U(S^{-1}A)$.*
2. *Para todo anillo B y para todo morfismo $f : A \to B$ con la propiedad de que $f(S) \subset U(S^{-1}A)$ existe un único morfismo $\bar{f} : S^{-1}A \to B$ con la propiedad de que $\bar{f} \cdot \varphi = f$.*



Demostración. La primera parte es muy sencilla pues solo es necesario hacer la observación de que para $s \in S$ se tiene que $\varphi(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}$. Por lo tanto $s \in U(S^{-1}A)$.

Para la segunda parte tendremos que trabajar un poco más, sea $f : A \to B$ tal que para todo $s \in S$ $f(s) \in U(B)$ entonces definiremos $\bar{f} : S^{-1}A \to B$ como sigue: $\bar{f}\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$, primero mostraremos que esta función está bien definida, supongamos que $\frac{a}{s} = \frac{a'}{s'}$ entonces exite $t \in S$ tal que $t(as'-a's) = 0$ como $f(t) \in U(B)$ se tiene necesariamente que $f(as'-a's) = 0$ es decir $f(a)f(s') = f(a')f(s)$ de donde $f(a)f(s)^{-1} = f(a')f(s')^{-1}$ por lo tanto $\bar{f}$ está bien definida. Ahora bien para ver la unicidad de la función sea $g : S^{-1}A \to B$ con la propiedad de que $g \cdot \varphi = f$ entonces para $s \in S$ se cumple $f(s) = g \cdot \varphi(s) = g\left(\frac{s}{1}\right)$ de donde podemos deducir que $g\left(\frac{1}{s}\right) = f(s)^{-1}$ entonces para $\frac{a}{s}$ arbitraria en $S^{-1}A$ se tiene que:

$$g\left(\frac{a}{s}\right) = g\left(\frac{a}{1} \cdot \frac{1}{s}\right) = g\left(\varphi(a)\right) \cdot g\left(\frac{1}{s}\right) = f(a)f^{-1}(s) = \bar{f}\left(\frac{a}{s}\right)$$

lo cual prueba la unicidad de $\bar{f}$.

■

Proposición 1.6.11 *Sea A un anillo, S un conjunto multiplicativo y $\varphi : A \to S^{-1}A$ el morfismo natural, entonces:*

a) Cada ideal de $S^{-1}A$ es de la forma $S^{-1}\mathfrak{A}$.

b) Para todo $\mathfrak{A} \subset A$ $\quad S^{-1}\mathfrak{A} = (1) \Leftrightarrow \mathfrak{A} \cap S \neq \emptyset$

c) Los ideales primos de $S^{-1}A$ están en correspondencia biyectiva con los ideales primos de A que no cortan a S.

d) Si A es noteheriano, entonces $S^{-1}A$ es noetheriano.

Demostración.

a) Sea $\mathfrak{A} \subset S^{-1}A$ ideal y sea $\frac{a}{s} \in \mathfrak{A}$ entonces $\frac{a}{1} = \frac{a}{s} \cdot \frac{s}{1} \in \mathfrak{A}$ por lo que $\frac{a}{s} \in S^{-1}\varphi^{-1}(\mathfrak{A})$.

b) $\Rightarrow$) Sea $S^{-1}\mathfrak{A}$ ideal de $S^{-1}A$ y supongamos que $S^{-1}\mathfrak{A} = (1)$ eso quiere decir que existen $a \in \mathfrak{A}$ $s \in S$ tales que $\frac{a}{s} = \frac{1}{1}$ pero $\frac{a}{s} = \frac{1}{1}$ si y solo si existe $t \in S$ tal que $t(a - s) = 0$ pero $ta \in \mathfrak{A}$ por lo tanto $ts \in \mathfrak{A}$, como S es multiplicativo también se tiene que $ts \in S$ por lo tanto $\mathfrak{A} \cap S \neq \emptyset$.

$\Leftarrow$) Sea $S^{-1}\mathfrak{A}$ ideal de $S^{-1}A$ tal que $\mathfrak{A} \cap S \neq \emptyset$ y sea $s \in \mathfrak{A} \cap S$ entonces $\frac{1}{1} = \frac{s}{s} \in S^{-1}\mathfrak{A}$ por lo tanto $S^{-1}\mathfrak{A} = (1)$.

c) Sea $\mathfrak{Q} \subset S^{-1}A$ ideal primo por a) sabemos que $\mathfrak{Q}$ es de la forma $S^{-1}\mathfrak{P}$ y sabemos que la imagen inversa de un ideal primo es también ideal primo, por lo tanto $\mathfrak{P}$ es ideal primo en A y por b) sabemos que $\mathfrak{P} \cap S = \emptyset$. Ahora si comenzamos con un ideal primo $\mathfrak{P} \subset A$ y consideramos $S^{-1}\mathfrak{P}$ veremos que es un ideal primo en $S^{-1}A$ pues si $\frac{a}{s} \cdot \frac{a'}{s'} \in S^{-1}\mathfrak{P}$ se tiene que $a \cdot a' \in \mathfrak{P}$ por lo tanto $a \in \mathfrak{P}$ o $a' \in \mathfrak{P}$. es decir, $S^{-1}\mathfrak{P}$ es ideal primo. Hemos visto dos aplicaciones de ideales primos de A que no cortan a S en ideales de $S^{-1}A$ y viceversa, ahora veremos que son inversas una de la otra, sea $\mathfrak{Q} \subset S^{-1}A$ ideal primo y $\frac{a}{s} \in \mathfrak{Q}$ tenemos que $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s}$ y que $a \in \varphi^{-1}(\mathfrak{Q})$ por lo tanto $\frac{a}{s} \in S^{-1}\varphi^{-1}(\mathfrak{Q})$ entonces $\mathfrak{Q} = S^{-1}\varphi^{-1}(\mathfrak{Q})$. Inversamente sea $a \in \varphi(S^{-1}\mathfrak{P})$ con $\mathfrak{P}$ ideal primo en A ajeno con S entonces existen $a' \in \mathfrak{P}$ y $s \in S$ tales que $\frac{a}{1} = \frac{a'}{s}$ por lo tanto exste $t \in S$ tal que $t(as - a') = 0$ pero como $a' \in \mathfrak{P}$ entonces $as \in \mathfrak{P}$ y por lo tanto $a \in \mathfrak{P}$ pues $\mathfrak{P}$ y S son ajenos. Lo cual prueba que ambas aplicaciones son inversas una de la otra.

d) Para probar esto basta notar que para un ideal $S^{-1}\mathfrak{I} \subset S^{-1}A$ con $\mathfrak{I}$ ideal de A, el conjunto de generadores de $\mathfrak{I}$ es también conjunto de generadores para $S^{-1}\mathfrak{I}$.

■

Ejemplo 1.6.12 *Sea A anillo conmutativo y $\mathfrak{P}$ ideal primo de A, sea $S = A \backslash \mathfrak{P}$ entonces $S^{-1}A$ es un anillo local que tiene como único ideal primo a $\mathfrak{P}$ y todos lo elementos que no están en $\mathfrak{P}$ son invertibles. Este ejemplo se presentará tan frecuentemente que a $S^{-1}A$ lo denotaremos por $A_{\mathfrak{P}}$ y no puede prestarse a confusiones pues un ideal no puede ser un conjunto multiplicativo según habíamos convenido. A este proceso le llamaremos* localización.

Ejemplo 1.6.13 *Sea $S = \{2^n | n \in \mathbb{N}\}$ este conjunto es multiplicativo, entonces $S^{-1}\mathbb{Z} = \{\frac{a}{b} \in \mathbb{Q} | (a; 2) = 1, b = 2^n$ para alguna $n \in \mathbb{N}\}$.*

El siguiente par de resultados muestran lo útil que es el proceso de localización, es decir, como puede probarse que un anillo tiene una propiedad a partir de que todas las localizaciones la tienen.

Lema 1.6.14 *Sea D cualquier dominio entero, entonces:*

$$D = \bigcap_{\mathfrak{M} max} D_{\mathfrak{M}} = \bigcap_{\mathfrak{P} primo} D_{\mathfrak{P}}$$

con la primera intersección tomada sobre los ideales maximales y la segunda sobre los ideales primos.

Demostración. Por comodidad denotaremos por E al conjunto $\bigcap_{\mathfrak{M} max} D_{\mathfrak{M}}$, la contención de D en E claramente se da pues D está contenido en cada intersecando. Para probar la otra contención consideraremos $x = \frac{a}{s} \in E$ y el siguiente ideal:

$$\mathfrak{A} = \{y \in D | ya \in Ds\}.$$

Para cada ideal maximal $\mathfrak{M}$ existen $p, q \in D$ con $q \notin \mathfrak{M}$ tales que $x = \frac{p}{q}$, entonces $qa = ps$ por lo tanto $\mathfrak{A} \nsubseteq \mathfrak{M}$ de donde $\mathfrak{A} = A$ lo cual nos permite concluir que $a = rs$ para alguna $r \in A$, es decir, $x \in D$ lo cual prueba el resultado. Para ver que el resultado también vale para ideales primos basta observar que entre los ideales primos se encuentran los maximales y que el resultado es consecuencia del hecho de que el complemento de cada ideal primo es multiplicativo.

■

Lema 1.6.15 *Sea D dominio entero y $\mathfrak{A} \subset \mathfrak{B}$ ideales de D tales que para cada ideal maximal $\mathfrak{M} \subset D$ se cumple que $\mathfrak{A}D_{\mathfrak{M}} = \mathfrak{B}D_{\mathfrak{M}}$ entonces $\mathfrak{A} = \mathfrak{B}$. Análogamente si para todo ideal primo $\mathfrak{P} \subset D$ se cumple que $\mathfrak{A}D_{\mathfrak{P}} = \mathfrak{B}D_{\mathfrak{P}}$ entonces $\mathfrak{A} = \mathfrak{B}$.*

Demostración. Sea $b \in \mathfrak{B}$ y el ideal:

$$\mathfrak{C} = \{x \in D | xb \in \mathfrak{A}\}$$

ahora sea $\mathfrak{M}$ cualquier ideal maximal de D, por hipótesis $b \in \mathfrak{A}D_{\mathfrak{M}}$ entonces $b = \frac{a}{s}$ con $a \in \mathfrak{A}, s \notin \mathfrak{M}$ de donde $a = sb$ y por lo tanto $s \in \mathfrak{C}$ y por lo tanto $\mathfrak{C} = D$ lo cual conluye la prueba del resultado. Para ver que el resultado también vale para ideales primos basta observar que entre los ideales primos se encuentran los maximales y que el resultado es consecuencia del hecho de que el complemento de cada ideal primo es multiplicativo.

■

1.7. Dependencia entera

En esta sección estudiaremos el concepto de dependencia entera, y nos interesará particularmente el caso de los dominios enteros.

En esta sección A y A' denotarán anillos y supondremos que A es subanillo de A'.

Definición 1.7.1 *Un elemento $a \in A'$ es entero sobre A si existe $f(x) \in A[x]$ mónico tal que $f(a) = 0$ Diremos que $f(x)$ es la* ecuación de dependencia entera.

Proposición 1.7.2 *Las siguientes afirmaciones son equivalentes:*

(1) $a \in A'$ es entero sobre A.

(2) $A[a]$ es un A-módulo finitamente generado.

(3) $A[a]$ está contenido en un subanillo B de A' que es un A-módulo finitamente generado.

(4) Existe en A' un A-módulo M tal que M es finitamente generado y el único elemento $y \in A[a]$ para el que $yM = 0$ es $y = 0$.

Demostración.

(1) $\Rightarrow$ (2) Si el polinomio mónico que se anula en a tiene grado n entonces $A[a]$ está generado por $1, a, \ldots, a^n$.

(2) $\Rightarrow$ (3) Tómese $B = A[a]$.

(3) $\Rightarrow$ (4) Tómese $M = B$. Dado que $1 \in B$ se tendrá siempre que $y \in yB$ y por lo tanto se sigue el resultado deseado.

(4) $\Rightarrow$ (1) Sean $M_1, \ldots, m_n$ generadores de M dobre A. Sean r_{ij} elementos de A tales que:

$$bm_i = \sum_j r_{ij} m_j.$$

Esto puede reescribirse de la siguiente manera

$$0 = \sum (r_{ij} - b\delta_{ij}) m_j,$$

donde δ_{ij} es la delta de Kronecker. Si N es la matriz de coeficientes de estas ecuaciones entonces si $d = det(N)$ se cumple necesariamente que $dM = 0$. Por esta razón se tiene que $d = 0$. Considérese ahora el polinomio $f(x) = det(x \cdot I - [r_{ij}])$. Por la forma en que fue construido el polinomio se tiene que a es raíz de $f(x)$, por lo tanto a es entero sobre a.

■

Proposición 1.7.3 *Suponga que $a_1, \ldots, a_n$ son elementos de A' enteros sobre A, entonces $A[a_1, \ldots, a_n]$ es un A-módulo finitamente generado.*

Corolario 1.7.4 *El conjunto de todos los elementos de A' que son enteros sobre A forman un subanillo de A' que contiene a A.*

Definición 1.7.5 *Diremos que A' es entero sobre A si todos los elementos de A' son enteros sobe A.*

Definición 1.7.6 *Sea D dominio entero,* la cerradura entera *de D es el conjunto de todos los elementos en $Q(D)$ que son enteros sobre D. Diremos que D es enteramente cerrado si la cerradura entera de D es D mismo.*

Una forma de construir dominios enteramente cerrados es tomar un dominio arbitrario y luego su cerradura entera en el campo cociente, la siguiente proposición garantiza que el dominio resultante es enteramente cerrado.

Proposición 1.7.7 *Si $A \subset A' \subset A''$ son anillos con A' entero sobre A y A'' entero sobre A' entonces A'' es entero sobre A.*

Hay una clase particular de dominios enteramente cerrados y esta es la de los dominios de factorización única.

Teorema 1.7.8 *Todo DFU es enteramente cerrado.*

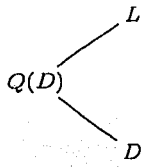
A continuación un resultado que nos facilitará determinar cuando un elemento es entero sobre un anillo.

Proposición 1.7.9 *Sea D dominio entero y K su campo de cocientes. Sea a un elemento algebráico sobre K. Sea $f(x) \in K[x]$ polinomio mónico que se anula en a, si a es entero sobre D entonces los coeficientes de $f(x)$ son enteros sobre D. Si D es enteramente cerrado entonces a es entero sobre D si y solo si $f(x) \in D[x]$.*

Proposición 1.7.10 *Sea K campo y $\{D_i\}$ una familia de dominios enteramente cerrados contenidos en K, entonces $\bigcap D_i$ es enteramente cerrado.*

1.8. Extensiones algebráicas

En este punto desviaremos nuestra atención de los anillos a los campos y extensiones finitas de éstos, es decir dado un campo consideraremos otro que lo contenga y que como espacio vectorial tenga dimensión finita. Los casos de mayor interés serán las extensiones (L) del campo de cocientes ($Q(D)$) de un dominio entero D, donde además no fijaremos en los elementos enteros sobre D.



Definición 1.8.1 *Un campo E es una* extensión de campo del campo F *si F es subcampo de E.*

Ejemplo 1.8.2 *Tanto $\mathbb{R}$ como $\mathbb{C}$ son extesiones de $\mathbb{Q}$.*

Ejemplo 1.8.3 *Una extensión de $\mathbb{R}$ es $\mathbb{C}$.*

Ejemplo 1.8.4 *Sea K un campo arbitrario, entonces $K(x)$, el campode funciones racionales, es una extensión de K.*

El siguiente teorema nos garantiza la existencia de un campo $\bar{K}$ donde podemos encontrar raices para cualquier polinomio no constante con coeficientes en cualquier campo, lo cual es muy útil. No daremos la demostración de este teorema en este trabajo pero puede ser consultado en cualquier texto de álgebra moderna.

Teorema 1.8.5 *Sea K un campo arbitrario, entonces existe una extensión de $K \leq \bar{K}$ tal que todo polinomio no constante con coeficientes en $\bar{K}$ tiene todas sus raices en $\bar{K}$. A $\bar{K}$ lo llamaremos* la cerradura algebráica de K.

Definición 1.8.6 *Sea K un campo, diremos que K es* algebráicamente cerrado *si la cerradura algebráica de K coincide con K.*

El siguiente resultado nos servirá como un criterio para determinar cuándo un campo es *algebráicamente cerrado*, pero más aun, cuando un campo sea algebráicamente cerrado tendremos una mejor descripción del anillo de polinomios con coeficientes en el campo.

Teorema 1.8.7 *Sea K un campo, entonces K es algebráicamente cerrado si y solo si todo polinomio no constante en $K[x]$ puede descomponerse en factores lineales.*

Demostración. $\Rightarrow$) Procederemos por inducción sobre el grado del polinomio, lo que queremos probar es que todo polinomio de grado $n > 0$ se puede descomponer en factores lineales.

- $n = 1$. En este caso para $f(x)$ de grado 1 él mismo es una descomposición en factores lineales.
- Paso inductivo. Supongamos que el resultado es válido para todo polinomio de grado n. Sea $f(x) \in K[x]$ de grado $n+1$, dado que K es algebráicamente cerrado $f(x)$ tiene al menos una raiz $\alpha \in K$. Sabemos que α es raiz de $f(x)$ si y solo si el polinomio $x - \alpha$ divide a $f(x)$ por lo tanto $f(x) = (x-\alpha)g(x)$ con $(x) \in K[x]$ de grado n, por hipótesis de inducción se tiene que $g(x)$ se descompone en factores lineales en $K[x]$ por lo tanto $g(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ si hacemos $\alpha_{n+1} = \alpha$ tenemos que

$$f(x) = \prod_{i=0}^{n+1}(x - \alpha_i)$$

que es lo que queríamos probar.

$\Leftarrow$) Esta parte es inmediata pues el término constante de cada factor lineal es raíz del polinomio y está en K. Así que todas las raíces de un polinomio estan en K.

■

A continuación revisaremos brevemente algunos conceptos importantes en las extensiones algebráicas.

Definición 1.8.8 *Sea $K \leq L$ una extensión de campos y $\alpha \in L$, diremos que α es* algebráico *sobre K si existe $0 \neq f(x) \in K[x]$ tal que $f(\alpha) = 0$. Si α no es algebráico diremos que es* trascendente.

Ejemplo 1.8.9 *El número $\sqrt{2} \in \mathbb{R}$ es algebráico sobre $\mathbb{Q}$ porque es raiz del poliomio $x^2 - 2$. De la misma manera el número $i \in \mathbb{C}$ es algebráico sobre $\mathbb{Q}$ porque es raiz del polinomio $x^2 + 1$. Por último el número $\pi \in \mathbb{R}$ es trascendental sobre $\mathbb{Q}$.*

Definición 1.8.10 *Sea $K \leq L$ una extensión de campos, diremos que L es* extensión algebráica *de K si todo elemento de L es algebráico sobre K.*

Corolario 1.8.11 *Un campo algebráicamente cerrado K no tiene extensiones algebráicas propias, es decir, la única extensión algebráica de K es K mismo.*

■

Teorema 1.8.12 *Sea $K \leq L$ una extensión de campos y $\alpha \in L$ algebráico sobre K, entonces existe un único $f(x) \in K[x]$ tal que $f(x)$ es irreducible, mónico y $f(\alpha) = 0$, además para todo polinomio $g(x) \in K[x]$ si $g(\alpha) = 0$ entonces $f(x)$ divide a $g(x)$.*

Demostración. Sabemos que existe al menos un polinomio $q(x) \in K[x]$ que se anula en α entonces el siguiente conjunto $\mathfrak{A} = \{p(x) \in K[x] | p(\alpha) = 0\}$ es un ideal maximal de $K[x]$ que como sabemos es un dominio euclideano y por lo tanto podemos expresar $\mathfrak{A} = (p(x))$ con $p(x)$ irreducible y mónico. La segunda parte es inmediata de esto.

■

Definición 1.8.13 *Sea $K \leq L$ una extensión de campos y sea $\alpha \in L$ algebráico sobre K, al polinomio mónico determinado de manera única por α mostrado en el teorema anterior lo llamaremos* el polinomio irreducible asociado a α sobre K *y lo denotaremos por $irr_K(\alpha)$. Definimos el* grado de $K(\alpha)$ sobre K *como el grado de $irr_K(\alpha)$.*

El siguiente resultado será de utilidad en secciones posteriores cuando estudiemos los grados e índices de las extensiones algebráicas. No daremos la prueba de este resultado pero la prueba puede hacerse fácilmente usando el lema de Zorn.

Teorema 1.8.14 *Sea $K \leq L$ extensión algebráica y $\bar{K}$ la cerradura algebráica de K, entonces existe al menos un monomorfismo de L en $\bar{K}$ que deja fijo a K.*

A partir de este punto hablaremos de elementos algebráicos sobre campos sin mencionar específicamente en que lugar se encuentra dicho elemento pues podemos suponer que se encuentra en la *cerradura algebráica*. Esto se debe como ya vimos, a que toda extensión algebráica la podemos ver como un subcampo de la cerradura algebráica.

Definición 1.8.15 *Sea $K \leq L$ una extensión de campos y $\alpha \in L$, definimos $K(\alpha)$ como el mínimo subcampo de L que contenga a K y α.*

Definición 1.8.16 *Una extensión de campo L de K es una* extensión simple *si existe $\alpha \in L$ tal que $L = K(\alpha)$.*

Observación 1.8.17 *Sea K un campo y α algebráico sobre K, sea $n = \partial(irr_K(\alpha))$ que es el grado del polinomio irreducible asociado a α sobre K, entonces $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base para $K(\alpha)$ como K espacio vectorial.*

Si $K \subseteq L$ y $\alpha \in L$ es trascendente sobre K podemos considerar el anillo $K[\alpha]$ que consiste de las series finitas de potencias de α con coeficientes en K, es decir un anillo isomorfo a $K[x]$. En este caso, $K(\alpha)$ es $Q(K[\alpha])$ y es un campo isomorfo a $K(x)$.

Corolario 1.8.18 *Sea K un campo y $K(\alpha)$ una extensión simple, con α algebráico sobre K, entonces todo elemento de $K(\alpha)$ es algebráico sobre K.*

Daremos ahora a estos conceptos un nombre pues aparecerán muy frecuentemente en el estudio de nuestra teoría.

Definición 1.8.19 *Si L es una extensión de K de dimensión finita, diremos que L es* una extensión finita de grado n *sobre K y denotaremos el grado de L sobre K por $[L : K]$ que como ya mencionamos es la dimensión de L sobre K.*

Veremos ahora un par de propiedades de las *extensiones finitas*. No veremos las demostraciones de éstos resultados pero pueden ser consultados en textos de álgebra moderna.

Teorema 1.8.20 *Sea K un campo arbitrario, entonces toda* extensión finita *de K es algebráica.*

Teorema 1.8.21 *Sean $K \leq L$ y $L \leq E$ extensiones finitas, entonces E es una extensión finita de K y $[E : K] = [E : L][L : K]$.*

Corolario 1.8.22 *Si $K_1, K_2, \ldots, K_t$ son campos y K_{i+1} es extensión finita de K_i para toda $i \in \{1, \ldots, t-1\}$ entonces K_t es extensión finita de K_1 y $[K_t : K_1] = [K_t : K_{t-1}][K_{t-1} : K_{t-2}] \cdots [K_2 : k_1]$.*

Corolario 1.8.23 *Sean $K \leq L$ y $L \leq E$ extensiones finitas, entonces E es una extensión algebráica de K.*

Corolario 1.8.24 *Si $\beta \in K(\alpha)$ con α algebráico sobre K, entonces $[K(\beta) : K]$ divide a $[F(\alpha) : K]$, es decir, $\partial irr_K(\beta)$ divide a $\partial irr_K(\alpha)$.*

Como podemos ver este par de teoremas tienen consecuecias inmediatas que nos ayudan a entender un poco más la naturaleza de las extensiones finitas, veremos ahora la relación que existe entre dos elementos algebráicos de un campo con el mismo polinomio irreducible asociado y sus extensiones simples.

Definición 1.8.25 *Sea L extensión algebráica de K. $\alpha, \beta \in L$ son* conjugados *bajo K si $irr_K(\alpha) = irr_K(\beta)$.*

Teorema 1.8.26 *Sea K campo y α, β algebráicos sobre K, con $[K(\alpha) : K] = n$, entonces α y β son conjugados respecto a K si y solo si el morfismo $\psi_\alpha^\beta : K(\alpha) \to K(\beta)$ dado por*

$$\psi_\alpha^\beta(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}$$

es un isomorfismo.

No veremos la prueba de este resultado pero es consecuencia de 1.8.17.

Corolario 1.8.27 *Sea K campo y α algebráico sobre K, entonces todo monomorfismo $\psi : K(\alpha) \to \bar{K}$ con la propiedad de que $\psi_{|K} = 1_K$ asocia a α un conjugado de α respecto a K.*

Dado un campo K y α un elemento algebráico sobre K, nos gustaría saber entre otras cosas cuántos conjugados tiene α respecto a K, cuántos monomorfismos hay de $K(\alpha)$ en $\bar{K}$ que dejan fijo a K, más aún, dado L extensión algebráica finita de K, nos gustaría saber cuándo $L = K(\alpha)$ para algún α algebráico sobre K. Los siguientes resultados están enfocados a determinar este tipo de cosas. El primero es una herramienta auxiliar para demostrar lo que nos interesa.

Teorema 1.8.28 *Sea $K \leq L$ extensión finita y $\sigma : K \longrightarrow K'$ un isomorfismo. Entonces el número de extensiones de σ a monomorfismos de L en $\bar{K}'$ solo depende de K y L.*

Ahora estamos en condiciones de introducir la definición ligada a este teorema.

Definición 1.8.29 *Sea $K \leq L$ extensión finita,* el índice de L sobre K *es el número de monomorfismos de L en $\bar{K}$ que dejan fijo a K. Lo denotaremos por $\{L : K\}$. A pesar de que el índice de una extensión puede definirse para extensiones algebráicas arbitrarias, nos restringiremos a extensiones finitas pues es donde nos interesa trabajar.*

Corolario 1.8.30 *Si L es extensión finita de K y E de L entonces:*

$$\{E : K\} = \{E : L\}\{L : K\}$$

Corolario 1.8.31 *Sea K campo y α algebráico sobre K, entonces:*

$$\{K(\alpha) : K\}$$

es el número de ceros distintos de $irr_K(\alpha)$.

Veremos ahora un resultado que relaciona el índice y el grado de una extensión.

Teorema 1.8.32 *Sea L extensión finita de K entonces $\{L : K\}$ divide a $[L : K]$.*

Ahora que conocemos esta relación estudiaremos un poco el caso en que el índice y el grado coinciden.

Definición 1.8.33 *Una extensión finita L de K se llama* separable *si $\{L : K\} = [L : K]$. Un elemento algebráico α es* separable sobre K *si $K(\alpha)$ es* separable sobre K. *Un polinomio $f(x) \in K[x]$ es* separable sobre K *si todas las raices de $f(x)$ son separables sobre K.*

A continuación veremos que la propiedad de ser separable es cerrada bajo extensiones finitas.

Teorema 1.8.34 *Si $K \leq L$ y $L \leq E$ son extensiones finitas entonces E es* separable sobre *K si y solo si E es* separable sobre *L y L es* separable sobre *K.*

También es de nuestro interés saber para qué campos sus extensiones finitas son siempre separables.

Lema 1.8.35 *Sea $\bar{K}$ la cerradura algebráica de K y*

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

cualquier polinomio mónico en $\bar{K}[x]$, si $(f(x))^m \in K[x]$ y $m \cdot 1 \neq 0$ en K entonces $f(x) \in K[x]$.

Definición 1.8.36 *Un campo es* perfecto *si cada extensión finita es separable.*

Teorema 1.8.37 *Todo campo de característica cero es perfecto.*

Teorema 1.8.38 *Todo campo finito es perfecto.*

Estos resultados nos dicen que si queremos encontrar extensiones que no sean separables, debemos buscarlas en campos infinitos de característica p con p un número primo.

Ahora uno de los teoremas más importantes para nuestro estudio, su importancia reside principalmente en que será muy útil en las secciones siguientes.

Teorema 1.8.39 (Teorema del elemento primitivo) *Sea L una extensión finita separable de K campo infinito. Entonces existe $\alpha \in L$ tal que $L = K(\alpha)$ (α es un elemento primitivo). Es decir, toda extensión finita separable es simple.*

Una vez que hemos caracterizado las extensiones separables, vamos a tratar de describir todas las extensiones finitas en general, pero para ello introduciremos un nuevo tipo de extensiones finitas llamadas *totalmente inseparables* y las vamos a estudiar un poco antes de continuar pues una vez que tengamos descritos estos dos tipos de extensiones finitas, todas las demás las podremos estudiar descomponiéndolas en dos extensiones, una separable y otra totalmente inseparable.

Definición 1.8.40 *Sea K campo y L una extensión finita de K, diremos que L es una* extensión totalmente inseparable de K *si* $\{L : K\} = 1$. *Un elemento α algebráico sobre K es* totalmente inseparable sobre K *si $K(\alpha)$ es* totalmente inseparable sobre K. *Un polinomio $f(x) \in K[x]$ es* totalmente inseparable sobre K *si todas las raices de $f(x)$ son* totalmente inseparables sobre K.

Así como ser separable es una propiedad cerrada bajo extensiones, el ser totalmente inseparable también lo es.

Teorema 1.8.41 *Sean $K \leq L$ y $L \leq E$ extensiones finitas de campos, entonces E es totalmente inseparable sobre K si y solo si E es totalmente inseparable sobre L y L es totalmente inseparable sobre K.*

Corolario 1.8.42 *Sea K campo y L extesión finita de K, entonces L es totalmente inseparable sobre K si y sólo si para toda $\alpha \in L \backslash K$ α es totalmente inseparable sobre K.*

Veremos a continuación como descomponer una extensión finita en dos extensiones que facilitarán su estudio y comprensión.

Lema 1.8.43 *Sea K campo de característica $p \neq 0$ y $\alpha \in \bar{K} \backslash K$, entonces α es totalmente inseparable sobre K si y solo si exite un natural n tal que $\alpha^{p^n} \in K$.*

Teorema 1.8.44 *Sea K campo de característica $p \neq 0$ y L extensión finita de K entonces el siguiente conjunto $E = \{\alpha \in L | \alpha$ es separable sobre $K\}$ forma un campo que es una extensión separable sobre K y además L es totalmente inseparable sobre E.*

Definición 1.8.45 *El campo construido en el teorema anterior se llama la* cerradura separable de L *sobre K.*

Con esto concluimos el estudio de extensiones algebráicas de campos.

1.9. Teoría de Galois

En esta sección revisaremos muy brevente algunos resultados de la teoría de Galois que nos serán de utilidad en seciones posteriores, sin embargo, cabe mencionar que la teoría de Galois por si sola es muy interesante y elegante, además su aplicación ha ayudado a resolver problemas clásicos de la teoría de ecuaciones como la irresolubilidad de un polinomio de grado cinco por medio de radicales, entre otras cosas.

La teoría de Galois lo que hace principalmente es relacionar la teoría de grupos con la de campos. Revisaremos algunos resultados que nos serán de utilidad en esta sección, algunos de ellos ya los estudiamos previamente.

1) Sean K campo, $\alpha, \beta \in \bar{K}$ con α y β conjugados respecto a K, entonces existe un isomorfismo $\psi_\alpha^\beta : K(\alpha) \to K(\beta)$ que asigna α en β.

2) Sea $K \leq L$ extensión finita, entonces cada monomorfismo de L en $\bar{K}$ que deje fijo a K debe asignar cada elemento de L un conjugado respecto a K.

3) Si $K \leq L$ es extensión, entonces el conjunto de todos los automorfismos de L que dejan fijo a K forman un grupo respecto a la composición, denotado por $G(L/K)$. Dado $S \subset G(L/K)$ el conjunto de los elementos de L que quedan fijos bajos S es un campo denotado por L_S, además $K \leq L_S$.

4) Un campo L, es de descomposición de K si $K \leq L$ y todo monomorfismo de L en $\bar{K}$ que deja fijo a K es un automorfismo de L. Si L es una extensión finita y campo de descomposición, entonces $|G(L/K)| = \{L : K\}$.

5) Si $K \leq L$ es extensión finita, entonces $\{L : K\} | [L : K]$. Si además L es separable sobre K entonces $\{L : K\} = [L : K]$, además L es separable sobre K si para toda $\alpha \in L$ $irr_K(\alpha)$ tiene todos sus ceros de multiplicidad 1.

Definición 1.9.1 *Una extensión finita L de K se llama* extensión finita normal *si es un campo de descomposición y extensión separable de K.*

El resultado siguiente es muy fuerte pues nos dice que una extensión finita normal se mantiene siendo normal para todos los campos intermedios.

Teorema 1.9.2 *Sea E extensión finita normal de K y L extensión finita de K tal que $K \leq L \leq E$. Entonces E es una extensión finita normal de L y $G(E/L)$ es un subgrupo de $G(E/K)$ que consiste de todos los automorfismos que dejan fijo a L. Más aun, dos automorfismos $\sigma, \tau \in G(E/K)$ inducen el mismo automorfismo en $G(E/L)$ si y solo si su clase derecha es la misma en $G(E/L)$.*

El teorema anterior nos muestra que hay una biyección entre los isomorfismos de E que dejan fijo a L y las clases derechas de $G(E/K)$ en $G(E/L)$. Nótese que no es posible decir que esas clases correspondan a automorfismos de L sobre K, dado que no necesariamente L es campo de descomposición de K. El resultado es que L es de descomposición si y solo si $G(E/L)$ es normal en $G(E/K)$, es decir, la extensión es normal si y solo si el subgrupo es normal. Además veremos que $\frac{G(E/K)}{G(E/L)} \cong G(L/K)$.

Definición 1.9.3 *Sea $K \leq L$ extensión finita, entonces $G(L/K)$ es el* grupo de Galois de L sobre K.

Teorema 1.9.4 (Teorema principal de la teoría de Galois) *Sea L un extensión normal finita de K con grupo de Galois $G(L/K)$. Para un campo E entre K y L, sea E_λ el subgrupo de $G(L/K)$ que deja fijo a E. Entonces λ es una correspondencia una a uno entre los campos intermedios de K y L y los subgrupos de $G(L/K)$ con las siguientes propiedades:*

1) $E_\lambda = G(L/E)$

2) $E = K_{G(L/K)} = K_{E_\lambda}$

3) Para $H \leq G(L/K)$, $K_{H\lambda} = H$.

4) $[L : E] = |E_\lambda|$; $[E : K] = \{G(L/K) : E_\lambda\}$.

5) E es una extensión normal de K si y solo si E_λ es un subgrupo normal de $G(L/K)$. Cuando E_λ es un subgrupo normal de $G(L/K)$ entonces $\frac{G(L/K)}{G(L/E)} \cong G(E/K)$.

6) El reticulado de subgrupos de $G(L/K)$ es isomorfo al reticulado invertido de campos entre K y L.

1.10. Módulos

En esta sección, que será muy corta, presentaremos algunos resultados que utilizaremos más adelante cuando estudiemos extensiones de *anillos de Dedekind.*

La siguiente proposición y su corolario son para módulos sobre anillos locales.

Proposición 1.10.1 *Sea A anillo local y $\mathfrak{M}$ su ideal maximal, sea M A-módulo finitamente generado tal que $\mathfrak{M}M = M$ entonces $M = 0$.*

Demostración. Sea

$$M = \sum_{i=1}^{n} Am_i \tag{1.3}$$

con $m_1, \ldots, m_n \in M$. Como $\mathfrak{M}M = M$ existen elementos $a_{ij} \in \mathfrak{M}$ tales que:

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

Sea $T = (a_{ij}) - I$, con I la matriz identidad. Entonces $T \cdot (m_1 \ \cdots \ m_n)^t$ es un replanteamiento de (1.3). Sea S la matriz adjunta de T entonces $ST \cdot (m_1 \ \ldots \ m_n)^t = (dm_1, \ldots, dm_n)^t$ con $D = det(T)$ además d es congruente con $(-1)^n$ módulo $\mathfrak{M}$ por lo tanto $d \in U(A)$ pero como $dM = 0$ se tiene necesariamente que $M = 0$.

■

Corolario 1.10.2 (Lema de Nakayama) *Sea A anillo local y $\mathfrak{M}$ su ideal maximal, sea M A- módulo finitamente generado y L un submódulo de M tal que $L + \mathfrak{M}M = M$, entonces $L = M$.*

Demostración. Consideremos $M/L = L/L + \mathfrak{M}M/L$, es decir, para todas las clases generadas por L hay un representante en $\mathfrak{M}M$, es decir, $\mathfrak{M}(M/L) = M/L$ por (1.10.1) $M/L = 0$ y por lo tanto $L = M$ lo cual concluye nuestra demostración.

■

Teorema 1.10.3 (Teorema chino del residuo para módulos) *Sea A anillo y $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n$ ideales de A tales que para $i \neq j$ $A = \mathfrak{Q}_i + \mathfrak{Q}_j$. Sea $\mathfrak{I} = \bigcap \mathfrak{Q}_i$ y M un A módulo entonces:*

$$M/\mathfrak{I}M \cong \bigoplus M/\mathfrak{Q}_i M$$

Aun podemos decir un poco más de lo que pasa en una situación como la del *Teorema Chino del Residuo.*

Proposición 1.10.4 *Sea A anillo y $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n$ ideales de A tales que para $i \neq j$ $A = \mathfrak{Q}_i + \mathfrak{Q}_j$. Sea $\mathfrak{I} = \bigcap \mathfrak{Q}_i$, entonces:*

$$\mathfrak{I} = \mathfrak{Q}_1 \cdots \mathfrak{Q}_n$$

Demostración. Demostraremos el resultado por inducción sobre n.

- $n = 2$

$$\mathfrak{O}_1\mathfrak{O}_2 = \{\sum_{i=1}^{k} a_i b_i | a_i \in \mathfrak{O}_1, b_i \in \mathfrak{O}_2\}$$

claramente $\mathfrak{O}_1\mathfrak{O}_2 \subset \mathfrak{O}_1 \cap \mathfrak{O}_2$ probaremos ahora la otra contención, sea $a \in \mathfrak{O}_1 \cap \mathfrak{O}_2$ como $1 = a' + b'$ con $a' \in \mathfrak{O}_1, b' \in \mathfrak{O}_2$ entonces $a = aa' + ab'$ y ambos sumandos son elementos de $\mathfrak{O}_1 \cap \mathfrak{O}_2$ por lo tanto $a \in \mathfrak{O}_1\mathfrak{O}_2$.

- Paso inductivo. *Hipótesis de inducción. Supongamos que el resultado es válido para n.*
  Nuevamente

$$\mathfrak{O}_1 \cdots \mathfrak{O}_n\mathfrak{O}_{n+1} \subset \bigcap_{i=1}^{n+1} \mathfrak{O}_i$$

si probamos que

$$\bigcap_{i=1}^{n} \mathfrak{O}_i + \mathfrak{O}_{n+1} = A$$

habremos terminado pues se reduce al caso $n = 2$. Sabemos que $1 = b_i + c_i$ con $b_i \in \mathfrak{O}_{n+1}$ y $c_i \in \mathfrak{O}_i$ entonces $c_i = 1 - b_i$ de donde

$$c = \prod_{i=1}^{n} c_i = 1 + a$$

con $a \in \mathfrak{O}_{n+1}$ además

$$c \in \bigcap_{i=1}^{n} \mathfrak{O}_i$$

de donde se sigue el resultado deseado.

■

1.11. Resultados adicionales

La razón por la cual esta sección existe es que los resultados aquí mencionados serán usados en demostraciones posteriores, razón por la cual no es necesario revisarlos sino hasta que se utilicen, pues es entonces que se entenderá su utilidad, aún cuando varios de ellos valen para anillos arbitrarios.

El siguiente resultado es válido para cualquier tipo de anillos conmutativos.

Lema 1.11.1 *Sea A anillo y $\mathfrak{P}_1 \neq \mathfrak{P}_2$ ideales maximales de A, entonces para toda pareja $a, b \in \mathbb{N}$ se tiene que $\mathfrak{P}_1{}^a + \mathfrak{P}_2{}^b = A$*

Demostración. Observemos que $\mathfrak{P}_1^a$ no puede estar contenido en $\mathfrak{P}_2$ a menos que $\mathfrak{P}_1 = \mathfrak{P}_2$ por lo tanto $\mathfrak{P}_1^a + \mathfrak{P}_2 = A$. Supongamos ahora que para cierto natural n se cumple que $\mathfrak{P}_1^a + \mathfrak{P}_2^n = A$ entonces

$$\mathfrak{P}_2^n = \mathfrak{P}_2^n A = \mathfrak{P}_2^n(\mathfrak{P}_1^a + \mathfrak{P}_2) \subseteq \mathfrak{P}_1^a + \mathfrak{P}_2^{n+1}.$$

Por lo tanto

$$A = \mathfrak{P}_1^a + \mathfrak{P}_2^n \subseteq \mathfrak{P}_1^a + (\mathfrak{P}_1^a + \mathfrak{P}_2^{n+1}) = \mathfrak{P}_1^a + \mathfrak{P}_2^{n+1}.$$

El resultado es válido por inducción.

■

Veamos ahora un resultado que nos indica condiciones suficientes para que un anillo sea DVD.

Proposición 1.11.2 *Sea D un dominio enteramente cerrado, noetheriano y local. Entonces D es un DVD.*

Demostración. Sea $0 \neq a \in \mathfrak{P}$ donde $\mathfrak{P}$ es el único ideal maximal de D, sea $D' = D/Da$ para cada $x \in D'$ sea

$$ann(x) = \{d \in D | dx = 0\}.$$

Por ser D noetheriano existe un elemento maximal en el conjunto $\{ann(x) | x \neq 0, x \in D'\}$. Sea $b \in D$ tal que $\mathfrak{Q} = ann(b+Da)$ es maximal. $\mathfrak{Q}$ es no nulo pues $a \neq 0$ y por lo tanto $a \in \mathfrak{Q}$. Veremos que $\mathfrak{Q}$ es primo para probar esto supongamos que es falso y que existen $x, y \in D$ tales que $xy \in \mathfrak{Q}$ y que

ninguno de los dos es elemento de $\mathfrak{Q}$ entonces $y(b+Da) \neq 0$ y $ann(yb+Da)$ contiene a x y a $\mathfrak{Q}$ lo cual es una contradicción a la elección de $\mathfrak{Q}$. Por lo tanto $\mathfrak{Q}$ es primo y por lo tanto es el único ideal primo no nulo de D, es decir, el ideal maximal de D son todos los elementos de D que multiplicados por b van a dar a Da. Probaremos ahora que $\mathfrak{Q}$ es principal, primero observemos que $\frac{b}{a} \notin D$ pues si así fuera tendríamos que $b+Da = 0+Da$ y por elección esto no es posible. Afirmamos además que $\mathfrak{Q} = D\frac{a}{b}$. Para ver que esto se cumple veamos que como consecuencia de que $\mathfrak{Q}b \subseteq Da$ tenemos que $\mathfrak{Q}\frac{b}{a}$ es un ideal de D, el caso en que $\mathfrak{Q}\frac{b}{a} \subseteq \mathfrak{Q}$ no es posible pues en caso de que se diera tendríamos por la parte 4 de 1.7.2 que $\frac{b}{a}$ es entero sobre D y por lo tanto estaría en D lo cual sería una contradicción, por lo tanto $\mathfrak{Q}\frac{b}{a} = D$ y $\mathfrak{Q} = D\frac{a}{b}$. Denotemos por comodidad a $\mathfrak{Q}$ por $D\pi$. Consideremos ahora $\mathfrak{A}$ ideal propio de D y consideremos la cadena

$$\mathfrak{A} \subseteq \mathfrak{A}\pi^{-1} \subseteq \mathfrak{A}\pi^{-2} \subseteq \cdots.$$

Si $\mathfrak{A}\pi^{-k} = \mathfrak{A}\pi^{-k-1}$ entonces tendríamos que π^{-1} es algebráico sobre D lo cual es falso. Como D es noetheriano la parte de la cadena que está contenida en D se estaciona. Supongamos que $\mathfrak{A}^{-k} \subseteq D$ y $\mathfrak{A}^{-k-1} \nsubseteq D$, observemos que si $\mathfrak{A}\pi^k \subseteq D\pi$ tendríamos que $\mathfrak{A}\pi^{-k-1} \subseteq D$ lo cual no es posible por lo tanto se debe tener que $\mathfrak{A}\pi^{-k} = D$ y por lo tanto $\mathfrak{A} = D\pi^k$ lo cual concluye la prueba del resultado.

■

Lema 1.11.3 *Sean $A \subset B$ dominios enteros con B entero sobre A y A enteramente cerrado. Si $\mathfrak{P} \subset B$ es ideal primo no nulo entonces $\mathfrak{P} \cap A$ es ideal primo no nulo de A.*

Demostración. Sea $0 \neq a \in \mathfrak{P}$ y sea $f(x) = \sum a_i x^i$ el polinomio mínimo de a sobre el campo de cocientes de A. Por 1.7.9 sabemos que los $a_i \in A$ y además $a_0 \neq 0$ pues $f(x)$ es irreducible y

$$a_0 = \sum_{i=1}^{n} -a_i a^i \in \mathfrak{P} \cap A,$$

lo cual prueba el lema.

■

Corolario 1.11.4 *Si $A \subset B$ son campo y dominio entero respectivamente con B entero sobre A entonces B es un campo.*

Demostración. Si B no fuera campo entonces existiría un ideal primo $\mathfrak{P}$ propio que cortado con A daría un ideal primo, pero como A es campo se tendría necesariamente que $\mathfrak{P} \cap A = A$, es decir $1 \in \mathfrak{P}$ lo cual es imposible.

■

Lema 1.11.5 *Sea D un DVD, K su campo de cocientes, L extensión finita totalmente inseparable de K y D' la cerradura entera de D en L. Entonces D' es DVD.*

Demostración. Sabemos que existe $q = p^r \in \mathbb{N}$ tal que para todo $x \in L$ se tiene que $x^q \in K$. Si $D = K$ entonces $D' = L$ y no hay nada que probar, supongamos por lo tanto que D no es un campo y sea $\mathfrak{p} = D\pi$ el ideal maximal de D. La aplicación de ideales de primos D' en ideales primos de D dada por $\mathfrak{P} \to \mathfrak{P} \cap D$ es inyectiva por lo tanto D' solo tiene un ideal primo no nulo, llamémosle $\mathfrak{P}$ a este ideal. Para todo $y \in \mathfrak{P}$ tenemos que $y^q = u\pi^n$ con $u \in U(D)$ y $n \in \mathbb{N}$. Sea $y \in \mathfrak{P}$ tal que la n es mínima. Sea $x \in D'\backslash\{0\}$ y sea $x^q = u_1\pi^d$ con $u_1 \in U(D)$ y $d \in \mathbb{N}$. Sea $d = nt + r$ con $0 \leq r < n$. Entonces:

$$(xy^{-t})^q = x^q(y^q)^{-t} = u_1\pi^d u^{-t}\pi^{-nt} = u_2\pi^r,$$

donde $u_2 \in U(D)$. Por lo tanto $(xy^{-t})^q \in D$ lo cual quiere decir que xy^{-t} es elemento de D'. Por la elección mínima de n se tiene que $xy^{-t} \notin \mathfrak{P}$ y por lo tanto es una unidad, es decir $x = vy^t$ donde $v \in U(D')$. Lo que hemos probado es que todo elemento no nulo de D' es una unidad de D' por una potencia de y. Como consecuencia inmediata se sigue que los únicos ideales no nulos de D' son los ideales principales generados por potencias de y, lo cual prueba que D' es un DVD.

■

Capítulo 2

Anillos de Dedekind

Ya en esta parte de nuestro estudio nos adentraremos a la parte que más nos interesa que son los anillos de *Dedekind*. Primero estudiaremos algunas propiedades elementales y algunos ejemplos.

Se cree que cuando Fermat demostró su último teorema trabajó sobre anillos de Dedekind y que además pensaba que éstos eran dominios de factorización única, que es en realidad una idea bastante brillante para su época, pues los anillos de Dedekind todavía no se estudiaban. Más adelante veremos que hay ejemplos de anillos de Dedekind que no son de factorización única, pero la unicidad de factorización, en los anillos de Dedekind, se pasó de los elementos a los ideales y se pueden obtener resultados bastante interesantes.

2.1. Propiedades elementales

Primero que nada debemos conocer a estos anillos que tanto nos interesan.

Definición 2.1.1 (Anillo de Dedekind) *Un anillo D se llama de* Dedekind *si cumple lo siguinte:*

a) Es dominio entero.

b) Es noetheriano.

c) Para todo ideal primo no nulo $\mathfrak{P} \subset D$ $D_{\mathfrak{P}}$ es DVD.

Ejemplo 2.1.2 *Todo DIP es de* Dedekind. *En particular $\mathbb{Z}$. Veremos más adelante que los DIP no son los únicos anillos de* Dedekind.

Lema 2.1.3 *Sea D anillo de* Dedekind *entonces D tiene las siguientes propiedades:*

1) Todo ideal primo no nulo es maximal.

2) Si $S \subset D$ es multiplicativo, entonces $S^{-1}D$ es de Dedekind.

Demostración.

1) Sean $\mathfrak{P} \subset \mathfrak{Q}$ ideales primos de D entonces $\mathfrak{P}$ es ideal primo en $D_{\mathfrak{Q}}$ lo cual es una contradicción a que $D_{\mathfrak{Q}}$ sea DVD, por tanto una situación como esta no puede presentarse en un anillo de Dedekind.

2) Los ideales primos de $S^{-1}D$ son de la forma $S^{-1}\mathfrak{P}$ con $\mathfrak{P}$ ideal primo en D ajeno a S, afirmamos que $D_{\mathfrak{P}} \cong (S^{-1}D)_{S^{-1}\mathfrak{P}}$ y el primero es un DVD, para verificar esto tomemos $f : D_{\mathfrak{P}} \to (S^{-1}D)_{S^{-1}\mathfrak{P}}$ definida de la siguiente manera $f(\frac{a}{s}) = \frac{\frac{a}{1}}{\frac{s}{1}}$. En primer lugar veremos que f está bien definida y después veremos que es isomorfismo. Supongamos que $\frac{a}{s} = \frac{a'}{s'}$ entonces $as' - a's = 0$ que es por definición que $\frac{\frac{a}{1}}{\frac{s}{1}} = \frac{\frac{a'}{1}}{\frac{s'}{1}}$ por lo tanto f está bien definida. Que f es un monomorfismo se sigue de que $D_{\mathfrak{P}}$ sea un dominio entero y de las propiedades del anillo de fracciones, para probar que es epimorfismo tomemos $\frac{\frac{a}{1}}{\frac{s'}{1}}$ en el dominio de f entonces $ss' \notin \mathfrak{P}$ dado que $\mathfrak{P}$ es ajeno con S y que $s' \notin \mathfrak{P}$. entonces $f(\frac{a}{ss'}) = \frac{\frac{a}{1}}{\frac{ss'}{1}} = \frac{\frac{a}{1}}{\frac{s'}{1}}$ por lo tanto f es también epimorfismo y por lo tanto isomorfismo.

■

Lema 2.1.4 *Sea $\mathfrak{P}$ ideal primo de D anillo de* Dedekind, *entonces:*

$$D/\mathfrak{P}^a \cong D_{\mathfrak{P}}/\mathfrak{P}^a D_{\mathfrak{P}}.$$

Demostración. Sea $f : D \to D_{\mathfrak{P}}/\mathfrak{P}^a D_{\mathfrak{P}}$ dada por $f(d) = \frac{d}{1} + \mathfrak{P}^a D_{\mathfrak{P}}$, claramente $nucf = \mathfrak{P}^a$ ahora para ver que f es epimorfismo sea $\frac{a}{s} + \mathfrak{P}^a D_{\mathfrak{P}}$ en el dominio de f, dado que $\mathfrak{P}$ es maximal se tiene que $Ds + \mathfrak{P} = D$ supongamos ahora que tenemos que $Ds + \mathfrak{P}^k = D$ para alguna $k \in \mathbb{N}$ entonces:

$$\mathfrak{P}^k = \mathfrak{P}^k D = \mathfrak{P}^k(Ds + \mathfrak{P}) \subseteq Ds + \mathfrak{P}^{k+1}$$

por lo tanto

$$D = Ds + \mathfrak{P}^k \subseteq Ds + (Ds + \mathfrak{P}^{k+1}) = Ds + \mathfrak{P}^{k+1}$$

por lo tanto $D = Ds + \mathfrak{P}^a$. Por lo tanto existe $c \in D$ y $q \in \mathfrak{P}^a$ tales que $cs + q = 1$. Entonces $f(rc) = \frac{rc}{1} + \mathfrak{P}^a D_{\mathfrak{P}} = r(\frac{1}{s} - \frac{q}{s}) + \mathfrak{P}^a D_{\mathfrak{P}} = \frac{r}{s} + \mathfrak{P}^a D_{\mathfrak{P}}$. Por lo tanto f es epimorfismo y también isomorfismo

■

La utilidad de este resultado se verá en el siguiente corolario.

Corolario 2.1.5 *Todo ideal de $D/\mathfrak{P}^a$ es una potencia de $\mathfrak{P}/\mathfrak{P}^a$ más aun $\mathfrak{P}/\mathfrak{P}^a$ es ideal principal.*

Demostración. Aplicando el lema 2.1.4 a $D_{\mathfrak{P}}$ se sigue el resultado, recordando además que $D_{\mathfrak{P}}$ es DVD y por la propiedad 3) de los dominios de valuación discreta se sigue el resultado.

■

2.2. Factorización de ideales en anillos de Dedekind

Observemos la siguiente situación, dado un ideal no primo $\mathfrak{A} \subset D$ con D de *Dedekind*, $D/\mathfrak{A}$ sigue siendo noetheriano pero no es dominio entero, entonces por 1.4.14 $D/\mathfrak{A}$ tiene un número finito de ideales primos, pero los ideales primos de $D/\mathfrak{A}$ están en correspondencia biyectiva con los ideales primos de D que contienen a $\mathfrak{A}$. Esto quiere decir que solo una cantidad finita de ideales primos de D contienen a $\mathfrak{A}$. Esto nos permitirá demostrar el siguiente resultado.

Teorema 2.2.1 *Sea D anillo de* Dedekind *y $\mathfrak{A}$ ideal no nulo de D, sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ los ideales primos que contienen a $\mathfrak{A}$ entonces existen números naturales $a_1, \ldots, a_n$ tales que:*

$$\mathfrak{A} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_n^{a_n}$$

todos determinados de manera única por $\mathfrak{A}$.

Demostración. Todo excepto la unicidad ha sido probado, la unicidad de $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ queda determinada al ser los ideales primos de D que contienen a $\mathfrak{A}$ los a_i están determinados por que cada uno es la mínima potencia en la que el ideal maximal de $D_{\mathfrak{P}_i}/\mathfrak{A}D_{\mathfrak{P}_i}$ es cero, es decir, $\mathfrak{A}/D_{\mathfrak{P}_i} = \mathfrak{P}_i^{a_i} D_{\mathfrak{P}_i}$.

■

2.3. Equivalencias de la definición

En esta parte veremos que los anillos de *Dedekind* pueden describirse de varias maneras equivalentes, esto además de interesante resulta muy útil pues si por alguna razón no podemos demostrar directamente que un anillo cumple con los axiomas de la definición, podemos probar que cumple con propiedades equivalentes.

Teorema 2.3.1 *Sea D dominio entero que no es campo, entonces son equivalentes para D:*

(1) D es anillo de Dedekind.

(2) Para cada ideal maximal $\mathfrak{P}$, $D_{\mathfrak{P}}$ es DVD y para cada elemento $0 \neq a \in D$ solo una cantidad finita de ideales primos de D contienen a a.

(3) D es noetheriano, enteramente cerrado y cada ideal primo no nulo de D es maximal.

Demostración. (1)⇒(2) Esta parte ya ha sido prácticamente demostrada solo falta probar que dado $a \in D$ solo hay una cantidad finita de ideales primos que contienen a a pero esto es consecuencia inmediata de que el ideal (a) solo está contenido en una cantidad finita de ideales primos.

(2)⇒(3) Sea $\mathfrak{P}$ ideal primo no nulo de D si $\mathfrak{P}$ no fuera maximal entonces se tendría que existe $\mathfrak{P} \subset \mathfrak{Q}$ con $\mathfrak{Q}$ ideal primo maximal de D entonces $\mathfrak{P}D_{\mathfrak{Q}}$ es ideal primo no maximal en $D_{\mathfrak{Q}}$ lo cual contradice que $D_{\mathfrak{Q}}$ sea DVD, por lo tanto cada ideal primo en D es maximal. Ahora bien cada $D_{\mathfrak{P}}$ es enteramente cerrado por lo tanto D es enteramente cerrado como consecuencia de 1.7.10 y de 1.6.14. El hecho de que D es noetheriano se sigue del siguiente resultado.

Proposición 2.3.2 *Sea D dominio entero que satisface la condición 2 de 2.3.1 y sea $\mathfrak{A} \subset A$ ideal no nulo. Para toda $a \in \mathfrak{A}\backslash\{0\}$ existe $b \in \mathfrak{A}$ tal que $Da + Db = \mathfrak{A}$. Es decir, cada ideal esta generado por dos elementos o es principal.*

Demostración. Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ los ideales primos de D que contienen a a. Cada localización $D_{\mathfrak{P}_i}$ es DIP por lo tanto existe $c_i \in D$ tal que

$$\mathfrak{A}D_{\mathfrak{P}_i} = c_i D_{\mathfrak{P}_i}.$$

Podemos escribir $c_i = \frac{x}{s}$ con $x \in \mathfrak{A}$ y $s \in D\backslash\mathfrak{P}_i$, observemos que $c_i D_{\mathfrak{P}_i} = xD_{\mathfrak{P}_i}$, así que sin pérdida de generalidad podemos suponer que $c_i \in \mathfrak{A}$, podemos en este momento probar que $\mathfrak{A}$ es finitamente generado, sea $\mathfrak{C} = Da + Dc_1 + \cdots + Dc_n$ claramente $\mathfrak{C} \subset \mathfrak{A}$, si $\mathfrak{P}$ es ideal primo tal que $a \notin \mathfrak{P}$ entonces $\frac{1}{a} \in D_{\mathfrak{P}}$ y por lo tanto $\mathfrak{C}D_{\mathfrak{P}} = \mathfrak{A}D_{\mathfrak{P}}$. Por 1.6.15 se tiene que $\mathfrak{C} = \mathfrak{A}$. Para encontrar b lo haremos escogiéndolo de tal forma que bajo el isomorfismo de 1.10.3 que garantiza que:

$$\mathfrak{A}/\mathfrak{P}_1 \cdots \mathfrak{P}_n\mathfrak{A} \cong \bigoplus_{i=1}^{n} \mathfrak{A}/\mathfrak{P}_i\mathfrak{A}$$

la imagen de b sea $(c_1 + \mathfrak{P}_1\mathfrak{A}, \ldots, c_n + \mathfrak{P}_n\mathfrak{A})$. Entonces $b - c_i \in \mathfrak{P}_i\mathfrak{A}$ y además $Da + Db \subseteq \mathfrak{A}$. Probaremos la igualdad usando la misma técnica. Sea $\mathfrak{D} = Da + Db$ para $\mathfrak{P}$ ideal primo de D se tiene que $\mathfrak{D}D_{\mathfrak{P}} = \mathfrak{A}D_{\mathfrak{P}} = D_{\mathfrak{P}}$, si $\mathfrak{P} = \mathfrak{P}_i$ entonces $c_i = b + (c_i - b) \in \mathfrak{D}D_{\mathfrak{P}} + \mathfrak{P}\mathfrak{A}D_{\mathfrak{P}}$. Por lo tanto esta suma contiene a $c_i D_{\mathfrak{P}} = \mathfrak{A}D_{\mathfrak{P}}$. Por otra parte $\mathfrak{D} \subseteq \mathfrak{A}$ por lo tanto la suma está contenida en $\mathfrak{A}D_{\mathfrak{P}}$, de aquí se sigue que:

$$\mathfrak{D}D_{\mathfrak{P}} + \mathfrak{P}\mathfrak{A}D_{\mathfrak{P}} = \mathfrak{A}D_{\mathfrak{P}}.$$

Las hipótesis de 1.10.2 se cumplen y por lo tanto $\mathfrak{D}D_{\mathfrak{P}} = \mathfrak{A}D_{\mathfrak{P}}$ y por 1.6.15 se tiene que $\mathfrak{A} = \mathfrak{D} = Da + Db$.

■

(3)⇒(1) Sea $\mathfrak{P}$ ideal maximal de D, entonces $D_{\mathfrak{P}}$ es un anillo noetheriano local con $\mathfrak{P}D_{\mathfrak{P}}$ su único ideal primo no nulo por 1.11.2 se sigue lo que deseamos.

■

2.4. Ideales fraccionarios y el grupo de clases

En esta sección D denotará un anillo de *Dedekind* y K su campo de cocientes.

Definición 2.4.1 *LLamaremos* ideal fraccionario *de D a todo D-submódulo no nulo de K finitamente generado.*

Definición 2.4.2 *Si $\mathfrak{M}$ es ideal fraccionario de D definiremos*

$$\mathfrak{M}^{-1} = \{x \in K | x\mathfrak{M} \subset D\}$$

.

Ejemplo 2.4.3 *Sea $0 \neq y \in K$ entonces Dy es ideal fraccionario de D y $(Dy)^{-1} = Dy^{-1}$.*

Ejemplo 2.4.4 *Todo ideal no nulo de D es ideal fraccionario.*

Observación 2.4.5 *Si $\mathfrak{M}$ es ideal fraccionario entonces $\mathfrak{M}^{-1}$ también lo es.*

Definición 2.4.6 *Sean $\mathfrak{M}, \mathfrak{N}$ ideales fraccionarios de D definiremos*

$$\mathfrak{M}\mathfrak{N} = \{x \in K | x = \sum m_i n_i, m_i \in \mathfrak{M}, n_i \in \mathfrak{N}\}$$

observemos que el producto de ideales fraccionarios es nuevamente ideal fraccionario.

Lema 2.4.7 *Si $\mathfrak{P} \subset D$ es ideal primo no nulo entonces $\mathfrak{P}\mathfrak{P}^{-1} = D$.*

Demostración. Sea $\mathfrak{P}$ ideal primo de D, entonces $\mathfrak{A} = \mathfrak{P}\mathfrak{P}^{-1}$ es ideal en D, para cualquier ideal maximal $\mathfrak{Q}$ en D sabemos que $D_{\mathfrak{Q}}$ es DIP así que $\mathfrak{P}D_{\mathfrak{Q}}$ es principal y por lo tanto $\mathfrak{A}D_{\mathfrak{Q}} = (\mathfrak{P}D_{\mathfrak{Q}})(\mathfrak{P}D_{\mathfrak{Q}})^{-1} = D_{\mathfrak{Q}}$, dado que esto es válido para todo $\mathfrak{Q}$ maximal entonces por 1.6.15 se tiene que $\mathfrak{A} = D$

■

Teorema 2.4.8 *Cualquier ideal fraccionario $\mathfrak{M}$ de D puede ser expresado de forma única, salvo orden, como producto de potencias enteras de ideales primos.*

Demostración. Sea $\mathfrak{M}$ ideal raccional con generadores $m_1, \ldots, m_n$ para toda i se tiene que $m_i \in K$ por lo tanto existe $s \in D$ tal que $m_i s \in D$ para toda i por lo tanto $\mathfrak{M}s \subseteq D$ y para cada ideal hay una factorización de la siguiente forma:

$$Ds = \prod \mathfrak{Q}_j^{b_j} \qquad \mathfrak{M}s = \prod \mathfrak{P}_i^{a_i}$$

donde tanto los $\mathfrak{P}_i$ y los $\mathfrak{Q}_i$ son ideales primos en D por lo tanto

$$\mathfrak{M}\mathfrak{Q}_1^{b_1} \cdot \mathfrak{Q}_t^{b_t} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_k^{a_k}$$

y por 2.4.7 se sigue que:

$$\mathfrak{M} = \prod \mathfrak{P}_i^{a_i} \cdot \prod \mathfrak{Q}_j^{-b_j}$$

con esto probamos que cada ideal fraccionario se puede expresar como producto de potencias de ideales primos con exponentes enteros, falta probar la unicidad, para ello consideremos

$$\mathfrak{M} = \prod \mathfrak{P}_i^{a_i} \cdot \prod \mathfrak{Q}_j^{-b_j} = \prod \mathfrak{X}_i^{c_i} \cdot \prod \mathfrak{Y}_j^{-d_j}$$

dos factorizaciónes en potencias de ideales primos de D entonces nuevamente por 2.4.7 se tiene que

$$\prod \mathfrak{P}_i^{a_i} \cdot \prod \mathfrak{Y}_j^{d_j} = \prod \mathfrak{X}_i^{c_i} \cdot \prod \mathfrak{Q}_i^{b_i}$$

que es una factorización de ideales primos en D que por ser única implica que la factorización de $\mathfrak{M}$ también es única.

■

Lo que este resultado nos dice es que el conjunto de *ideales fraccionarios de D* forma un grupo libre abeliano respecto de la multiplicación con base los ideales primos de D.

Ahora que tenemos este resultado sería interesante poder dar una descripción más precisa de como es este grupo, más aun, saber que tan lejos está un anillo de dedekind de ser de ideales principales.

Definición 2.4.9 *Denotaremos por por* $\mathbf{I}(D)$ *al grupo de ideales fraccionarios de D.*

Definición 2.4.10 *Denotaremos por* $\mathbf{P}(D)$ *al subgrupo de* $\mathbf{I}(D)$ *consistente de los ideales fraccionarios principales. Es decir los ideales fraccionarios de la forma* Dx *con* $x \in K$.

Por último consideraremos un grupo más que nos servirá para determinar que tan lejos estaba nuestro anillo de Dedekind de ser de ideales principales.

Definición 2.4.11 (Grupo de clases de ideales) *Denotaremos por* $\mathbf{C}(D)$ *a* $\mathbf{I}(D)/\mathbf{P}(D)$ *y lo llamaremos el grupo de clases de ideales de D.*

Este grupo es un invariante de los anillos de Dedekind. En ocasiones D se escoge de su campo de cocientes K de una manera especial, de esta forma $\mathrm{C}(D)$ es un invariante de K. Por ejemplo si tomamos K una extensión finita de $\mathbb{Q}$ y D la cerradura entera de $\mathbb{Z}$ en K entonces $\mathrm{C}(D)$ es invariante de K, es un resultado muy importante de la teoría algebráica de los números que en este caso $\mathrm{C}(D)$ es finito. Un resultado muy importante, aunque no lo probaremos, es que si tomamos $\mathcal{O}$ el anillo de los elementos enteros sobre $\mathbb{Z}$ de un campo número K, es decir, una extensión finita de $mathbbQ$, entonces $\mathrm{C}(D)$ es finito.

2.5. Norma y traza.

En esta sección consideraremos la siguiente situación, dada L extensión finita de K y dado $y \in L$ definiremos $m_y : L \to L$ dada por $m_y(x) = yx$. Esta es claramente una función K-lineal que es además biyectiva cuando $y \neq 0$. Toda matriz asociada a la transformación m_y tendrá como invariante la traza y el determinante. Por está razón podemos definir sin problemas lo siguiente.

Definición 2.5.1 *Sea $K \subset L$ extensión finita de campos y sea $y \in L$ definiremos la* traza de L/K de y *de la siguiente manera: $T_{L/K}(y) = tr(m_y)$. También definiremos la* norma de L sobre K de y *como sigue: $N_{L/K}(y) = det(m_y)$*

Proposición 2.5.2 *Sean $K \subset L$ extensión finita de campos, $x, y \in L$ y $a \in K$ entonces la norma y la traza tienen las siguientes propiedades:*

i) $T_{L/K}(x + y) = T_{L/K}(x) + T_{L/K}(y)$

ii) $T_{L/K}(ax) = aT_{L/K}(x)$

iii) $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$

iv) $N_{L/K}(ax) = a^n N_{L/K}(x)$ *donde n es la dimensión de L/K.*

v) *Si $K \subset E \subset L$ entonces para $x \in L$ $T_{L/K}(x) = T_{L/E}(T_{E/K}(x))$.*

Demostración.

i) Solo hay que observar que $m_{x+y} = m_x + m_y$.

II) Esto se debe a que $m_{ax} = am_x$.

III) Esto es inmediato del hecho que $m_{xy} = m_x \cdot m_y$.

IV) Para esta propiedad necesitaremos un poco más de trabajo. Sean

$$a_1, \ldots, a_k \in E$$

base sobre K y $b_1, \ldots, b_m \in L$ base sobre E, para $x, y \in L$ sea $xb_i = \sum \beta_{ij}(x)b_j$, $ya_i = \sum \alpha_{ij}(y)a_j$. Entonces

$$T_{E/K}(y) = \sum \alpha_{ii}(y), \qquad T_{L/E}(x) = \sum \beta ii(x).$$

De donde se sigue que

$$T_{E/K}(T_{L/E}(x)) = \sum \sum \alpha_{ii}(\beta_{jj}(x)).$$

Por otro lado sabemos que los productos a_ib_j forman una base de L sobre K y que

$$xa_sb_t = \sum_j a_s\beta_{tj}(x)b_j = \sum_j \sum_i \alpha_{si}(\beta_{tj}(x))a_ib_j$$

de donde podemos concluir que $T_{L/K}(x) = \sum\sum(\alpha_{ii}(\beta_{jj}(x))$ que era lo que se deseaba probar.

■

Veremos ahora un resultado que relaciona la norma y traza de un elemento con sus conjugados, que además nos facilitará su cálculo.

Teorema 2.5.3 *Sea $K \subset L$ extensión finita separable, entonces para cada $\theta \in L$:*

- $T_{L/K}(\theta) = \sigma_1(\theta) + \cdots + \sigma_n(\theta)$
- $N_{L/K}(\theta) = \sigma_1(\theta)\sigma_2(\theta)\cdots\sigma_n(\theta)$.

Donde los σ_i son los monomorfismos de L en $\bar{K}$ que dejan fijo a K.

Demostración. El resultado es inmediato para elemntos primitivos pues ni la norma ni la traza dependen de la elección de la base de la extensión. Ahora bien si θ no es un elemento primitivo entonces el polinomio característico de m_θ es una potencia de $irr_K(\theta)$ y se tiene que

$$T_{L/K}(\theta) = d(\theta_1 \cdots \theta_m)$$

$$N_{L/K}(\theta) = (\theta_1 \cdots \theta_m)^d.$$

Donde $[L : K(\theta)] = d$ y $[K(\theta) : K] = m$. Sea F extensión normal de K tal que $L \subset F$, sea G el grupo de Galois de G/K y $H \subset G$ el subgrupo de G que deja fijo a L. Sea H_1 el subgrupo de G que deja fijo a θ entonces $H \subset H_1$, $d = [H_1 : H]$ y $m = [G : H_1]$. Sean $\tau_1, \ldots, \tau_m$ representantes de G/H_1 y $\gamma_1, \ldots, \gamma_d$ represententes de H_1/H, entonces los productos $\tau_i\gamma_j$ son representantes de G/H y por lo tanto

$$\sum_{i=1}^{n} \sigma_i(\theta) = \sum_{i=1}^{m}\sum_{j=1}^{d} \tau_i\gamma_j = d\sum_{i=1}^{m} \tau_i(\theta) = d(\theta_1 + \cdots + \theta_m),$$

$$\prod_{i=1}^{n} \sigma_i(\theta) = \prod_{i=1}^{m}\prod_{j=1}^{d} \tau_i\gamma_j(\theta) = (\theta_1 \cdots \theta_m)^d.$$

Lo cual prueba el resultado.

■

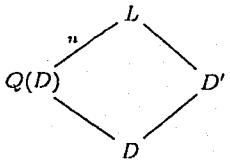
Ahora veremos un resultado que nos será de mucha utilidad en las siguientes secciónes, no incluimos la prueba pero es un resultado que puede ser revisado en un texto de álgebra lineal.

Teorema 2.5.4 *Sea $K \subset L$ extensión finita separable y sean $u_1, \ldots, u_n$ base de L sobre K. Entonces existen $v_1, \ldots, v_n \in L$ base sobre K tales que $T_{L/K}(u_iv_j) = \delta_{ij}$ donde δ_{ij} es la de Kronecker.*

Capítulo 3

Extensiones de anillos de Dedekind

En esta última sección estudiaremos la siguente situación:



donde D es anillo de Dedekind, $Q(D)$ es campo de cocientes de D, L es extensión finita de grado n y D' es la cerradura entera de D en L. Veremos que D' siempre será anillo de Dedekind y trataremos de ver como es la factorización de ideales primos en D' en función de cómo es en D. Pero antes de poder describir a D' deberemos estudiar L pues no necesariamente es una extensión separable y mucho menos simple, así que deberemos descomponerla como vimos en la sección 1.8 para poder dar más detalles de la situación.

3.1. Extensiones separables y totalmente inseparables.

Sin más preámbulo revisaremos los teoremas que describen esta situación.

Teorema 3.1.1 *Sea D anillo de Dedekind, $Q(D)$ su campo de cocientes,*

L extensión finita separable de $Q(D)$ y D' la cerradura entera de D en L. Entonces D' es anillo de Dedekind.

Demostración. Probaremos que D' satisface la condición 3 de 2.3.1. Primero que nada observemos que D' es enteramente cerrado por cómo fue elegido y por la transitividad de la dependencia entera. Sea $\mathfrak{P}$ ideal primo no nulo en D' probaremos que es maximal, sabemos por 1.11.3 que $\mathfrak{P} \cap D = \mathfrak{p}$ es ideal primo no nulo de D, de donde $D'/\mathfrak{P}$ es un dominio entero que contiene a $D/\mathfrak{P}$ que es un campo. Sea $\bar{t} = t + \mathfrak{P} \in D'/\mathfrak{P}$, entonces existe un polinomio mónico

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in D[x]$$

tal que $f(t) = 0$, sea $\bar{f}(\bar{x}) \in D'/\mathfrak{p}[\bar{x}]$ el polinomio resultante de reducir los coeficientes de $f(x)$, entonces $\bar{f}(\bar{t}) = 0$ por lo tanto $D'/\mathfrak{P}$ es entero sobre $D/\mathfrak{p}$ y por 1.11.4 $D'/\mathfrak{P}$ es un campo y por lo tanto $\mathfrak{P}$ es maximal. Probaremos ahora que D' es noetheriano, para hacer eso elijamos $a_1, \ldots, a_n$ base de E sobre $Q(D)$, sin pérdida de generalidad podemos suponer que para toda i se tiene que $a_i \in Q(D)'$. Por 2.5.4 podemos tomar $b_1, \ldots b_n \in E$ base sobre $Q(D)$ tal que

$$T_{E/Q(D)}(a_i b_j) = \delta_{ij}.$$

Sea ahora $y \in D'$ arbitrario. Existen elementos $c_j \in Q(D)$ tales que $y = \sum c_j b_j$. Podemos calcular los c_j de la siguiente manera

$$T_{E/Q(D)}(y a_j) = \sum_k c_k T_{E/Q(D)}(b_k a_j) = c_j.$$

Es decir $c_j \in D$ y por lo tanto

$$D' \subset \sum_j D b_j.$$

Esto quiere decir que D' está contenido en un D-módulo finitamente generado. Cualquier ideal de D' está también contenido en un D-módulo finitamente generado y es por lo tanto finitamente generado como D-módulo. Esto prueba que D' es noetheriano.

■

Teorema 3.1.2 *Sea D anillo de Dedekind, $Q(D)$ su campo de cocientes, L extensión finita totalmente inseparable de $Q(D)$ y D' la cerradura entera de D en L. Entonces D' es anillo de Dedekind.*

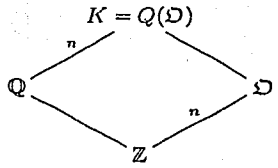
Demostración. Probaremos que D' cumple la propiedad 2 de 2.3.1. Dado que la extensión es totalmente inseparable se debe tener que $Q(D)$ es de característica $p \neq 0$, además existe $q = p^r$ para alguna $r \in \mathbb{N}$ tal que para todo $x \in L$ se cumple que $x^q \in Q(D)$. Si x es elemento de D' entonces $x^q \in Q(D) \cap D' = D$ e inversamente si x es elemento de L y $x^q \in D$ entonces $x \in D'$. Mostraremos que hay una correspondencia uno a uno entre los ideales primos de D y D'. Sea $\mathfrak{P}$ ideal primo no nulo de D' entonces $\mathfrak{p} = \mathfrak{P} \cap D$ es ideal primo no nulo de D y por lo tanto maximal. Para cada $x \in \mathfrak{P}$ se tiene que $x^q \in D \cap \mathfrak{P}$ e inversamente si $x \in D'$ es tal que $x^q \in \mathfrak{p}$ entonces $x \in \mathfrak{P}$ por ser algebráico sobre D y $\mathfrak{P}$ ideal primo, entonces la correspondencia $\mathfrak{P} \longrightarrow \mathfrak{p} = \mathfrak{P} \cap D$ es uno a uno. Tomemos ahora $a \in D' \backslash \{0\}$, dado que D es anillo de Dedekind solo hay una cantidad finita de ideales primos de D que contienen a a^q y por lo tanto solo hay una cantidad finita de ideales primos de D' que contienen a a. Esto completa la mitad de la prueba, nos falta probar que para todo $\mathfrak{P}$ ideal maximal de D' el anillo $D'_{\mathfrak{P}}$ es DVD. Primero estudiaremos el problema en el caso en que D es un DVD. Sea $\mathfrak{P}$ ideal maximal de D' y $\mathfrak{p} = \mathfrak{P} \cap D$. Entonces $S = D \backslash \mathfrak{p}$ es multiplicativo. Observemos que $S^{-1}D' = D'_{\mathfrak{P}}$, la inclusión de izquierda a derecha es inmediata para probar la otra tomemos $\frac{x}{y} \in D'_{\mathfrak{P}}$ con $x, y \in D'$ y $y \notin \mathfrak{P}$, entonces $y^q \in D \backslash \mathfrak{p} = S$ por lo tanto $\frac{x}{y} = \frac{xy^{q-1}}{y^q} \in S^{-1}D'$. Así que si observamos que $S^{-1}D'$ es la cerradura entera de $S^{-1}D$ en L el resto de la prueba es consecuencia de 1.11.5.

■

Corolario 3.1.3 *Sea D anillo de Dedekind, $Q(D)$ su campo de cocientes, L extensión de grado finito sobre $Q(D)$ y D' la cerradura entera de D en L. Entonces D' es anillo de Dedekind.*

■

Ahora si tenemos todo el derecho de decir que dada una extensión K de grado finito sobre $\mathbb{Q}$ el conjunto de enteros algebráicos de K sobre $\mathbb{Z}$ forma un anillo de Dedekind. Vale la pena mencionar que en este caso el anillo es un $\mathbb{Z}$-módulo libre con la suma y su rango es la dimensión de K sobre $\mathbb{Q}$. Hecho que en el caso general no es cierto.



Ejemplo 3.1.4 *Consideremos el anillo de enteros de* $\mathbb{Q}(\sqrt{5})$ *sobre* $\mathbb{Z}$ *llamemos* $\mathfrak{O}$ *a este anillo. Sabemos que* $p + q\sqrt{5}$ *es entero algebraico si y solo si* $2p, p^2 - 5q^2 \in \mathbb{Z}$. *Por lo tanto* $p = \frac{1}{2}P$ *con* $P \in \mathbb{Z}$. *si* P *es par entonces* $p^2 \in \mathbb{Z}$ *y no hay restricciones sobre* $5q^2$. *Si* P *es impar entonces* q *es necesariamente de la forma* $\frac{1}{2}Q$ *con* $Q \in \mathbb{Z}$, *es decir,* $\mathfrak{O} = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{5}]$. *Observemos ahora que* $4 = 2 \cdot 2 = -(1 + \sqrt{5})(1 - \sqrt{5})$ *son dos factorizaciones distintas de* 4 *y por lo tanto* $\mathfrak{O}$ *no es DFU y mucho menos DIP.*

Ahora regresaremos al caso general con $D \subset D'$ anillos de Dedekind con campos de cocientes K y L respectivamente. Veremos que relación hay entre los ideales primos de D y su factorización en D'.

Sea $\mathfrak{p}$ ideal primo no nulo de D. Entonces el ideal extendido que no necesariamente es primo $D'\mathfrak{p}$ de D' se factoriza de la siguiente forma:

$$D'\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \tag{3.1}$$

con $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ ideales primos distintos de D' y $e_1, \ldots, e_g \in \mathbb{N}$. Todos determinados de forma única por $\mathfrak{p}$. Y los factores primos de $D'\mathfrak{p}$ son aquellos $\mathfrak{P}$ tales que $D \cap \mathfrak{P}_i = \mathfrak{p}$.

Definición 3.1.5 *El número* e_i *se denomina como* el índice de ramificación de $\mathfrak{P}_i$ en D. *Algunas veces denotaremos por* $e(\mathfrak{P}/D)$ *o* $e(\mathfrak{P}/\mathfrak{p})$ *al índice de ramificación de* $\mathfrak{P}$ *sobre* D *cuando* $D \cap \mathfrak{P} = \mathfrak{p}$.

En ocasiones es útil comparar cocientes de D y D', obsérvese que $D'/\mathfrak{P}_i$ es una extensión de campo de $D/\mathfrak{p}$ el siguiente resultado nos da una cota para la dimensión del primero sobre el segundo como espacio vectorial.

Lema 3.1.6 *Supóngase que* $[L : K]$ *es finito. Sea* $\mathfrak{A}$ *ideal de* D' *tal que* $\mathfrak{A} \cap D = \mathfrak{p}$ *donde* $\mathfrak{p}$ *es ideal primo no nulo. Entonces:*

$$[D'/\mathfrak{A} : D/\mathfrak{p}] \leq [L : K]$$

donde $[D'/\mathfrak{A} : D/\mathfrak{p}]$ *es la dimensión de* $D'/\mathfrak{A}$*como* $D/\mathfrak{p}$ *espacio vectorial.*

Demostración. La prueba se puede hacer más fácilmente si suponemos que $\mathfrak{p}$ es principal, si hacemos $S = D\backslash\mathfrak{p}$ entonces $S^{-1}D$ es DVD además $\mathfrak{A}S^{-1}D' \cap S^{-1}D = \mathfrak{p}S^{-1}D$ y $S^{-1}D'/\mathfrak{A}S^{-1}D' \cong D'/\mathfrak{A}$, así que podemos probar el lema con $S^{-1}D$ y $S^{-1}D'$ en lugar de D y D'. Es decir, podemos suponer que $\mathfrak{p}$ es principal generado por π.

Sea $x_i \subset D'$ conjunto finito tal que las clases $x_i + \mathfrak{A}$ sean linealmente independientes sobre $D/\mathfrak{p}$. Supongamos que hay una combinación lineal $\sum a_i x_i = 0$ con $a_i \in K$, podemos suponer sin pérdida de generalidad que los a_i están en D. Supongamos que no todos los a_i son cero entonces sea $n \in \mathbb{N}$ tal que $\pi^n | a_i$ para toda i y π^{n+1} ya no, entonces después de cancelar esta potencia de π en los a_i tenemos que

$$\sum \bar{a}_i \bar{x}_i = \bar{0}$$

y alguno de los coeficientes es no nulo lo cual contradice la elección de x_i por lo tanto los x_i son linealmente independientes sobre K y se sigue la desigualdad deseada.

■

Definición 3.1.7 *La dimensión* $f_i = [D'/\mathfrak{P}_i : D/\mathfrak{p}]$ *es llamada el* grado relativo de $\mathfrak{P}_i$ sobre $\mathfrak{p}$. *Algunas veces denotaremos por* $f(\mathfrak{P}_i/D)$ *o* $f(\mathfrak{P}/\mathfrak{p})$ *al grado relativo.*

Ahora podemos ver que relación existe entre los índices de ramificación, los grados relativos y la dimensión del anillo cociente.

Teorema 3.1.8 $[D'/\mathfrak{p}D' : D/\mathfrak{p}] = \sum e_i f_i$. *Si* $[L : K]$ *es finito,* $S = D\backslash\mathfrak{p}$ *y* $S^{-1}D'$ *es finitamente generado como* $S^{-1}D$*-módulo entonces* $\sum e_i f_i = [L : K]$.

Demostración. Por la ecuación 3.1 y 1.1.14 sabemos que:

$$D'/\mathfrak{p}D' \cong \bigoplus D'/\mathfrak{P}_i^{e_i}.$$

Veremos que $D'/\mathfrak{P}_i^{e_i}$ tiene dimensión $e_i f_i$ sobre $D/\mathfrak{p}$ y de esta forma obtenemos la igualdad deseada. Los cocientes $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ son espacios vectoriales de dimensión 1 sobre $D'/\mathfrak{P}_i$ pues por 2.3.1 sabemos que podemos generar a $\mathfrak{P}_i^a$ con dos elementos y uno de ellos lo podemos elegir en $\mathfrak{P}_i^{a+1}\backslash\{0\}$ y por lo tanto el espacio tiene dimensión 1, de donde podemos concluir que tiene dimensión f_i sobre $D/\mathfrak{p}$.

■

Corolario 3.1.9 *Sea L extensión finita separable de K entonces:*

$$\sum e_i f_i = [L : K].$$

3.2. Extensiones normales.

Veremos ahora que si L es extensión normal de K se puede dar más información sobre la factorización de primos de D al levantarlos a D'.

Proposición 3.2.1 *Sea L extensión normal de K. Entonces la factorización en 3.1 de $\mathfrak{p}$ es de la siguiente forma:*

$$D'\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e \tag{3.2}$$

más aun todos los grados relativos son iguales, llamemos f a estos grados, entonces $efg = [L : K]$, además el grupo de Galois permuta a los $\mathfrak{P}_i$ transitivamente.

Demostración. Sea σ el automorfismo de L que manda a $\mathfrak{P}_1$ en $\mathfrak{P}_i$, entonces el hecho de que $\sigma(\mathfrak{p}D') = \mathfrak{p}D'$ y la factorización en ideales primos sea única tiene como consecuencia que $\sigma(\mathfrak{P}_1^{e_1}) = \mathfrak{P}_i^{e_i}$ y por lo tanto $e_1 = e_i$. También sucede que σ induce un isomorfismo de $D'/\mathfrak{P}_1$ en $D'/\mathfrak{P}_i$ por lo tanto $f_i = f_i$. Todo esto junto con 3.1.9 garantizan que $efg = [L : K]$.

■

Definición 3.2.2 *El ideal primo $\mathfrak{P}$ de D'* se ramifica respecto a *D si tiene índice de ramificación mayor a 1 o si el campo $D'/\mathfrak{P}$ no es separable sobre $D/D\cap\mathfrak{P}$. Diremos que el ideal $\mathfrak{p}$ primo en D se ramifica en D' si es dividido por algún ideal primo que se ramifica en D'.*

Ejemplo 3.2.3 En este ejemplo tomaremos la cerradura entera de $\mathbb{Z}$ en $\mathbb{Q}(i)$, donde $i^2 = -1$, sabemos que $irr_{\mathbb{Q}(i)}(i) = x^2 + 1$ y también que cualquier elemento $z \in \mathbb{Q}(i)$ puede expresarse como $z = x + yi$ de forma única con $x, y \in \mathbb{Q}$. Para que z sea entero sobre $\mathbb{Z}$ es necesario y suficiente que $T(z) = 2x \in \mathbb{Z}$ y $N(z) = x^2 + y^2 \in \mathbb{Z}$, de donde podemos concluir que x es de la forma $\frac{a}{2}$ y $y^2 = \frac{4b-a^2}{4}$ con $T(z) = a, N(z) = b \in \mathbb{Z}$ por lo que y es de la forma

$\frac{c}{2}$ con $c \in \mathbb{Z}$, es decir, $4b = a^2 + c^2$, esto es posible si y sólo si a y c son pares, es decir, $x, y \in \mathbb{Z}$. Por lo tanto la cerradura entera de $\mathbb{Z}$ en $\mathbb{Q}(i)$ es $\mathbb{Z}[i]$ el anillo de los *enteros gaussianos*.

Dado un número primo, p la relación $\sum e_i f_i = 2$ muestra que la factorización de (p) en $\mathbb{Z}[i]$ es de alguna de las siguentes tres formas: $p\mathbb{Z}[i] = \mathfrak{P}_1 \cdot \mathfrak{P}_2$ (con $\mathbb{Z}[i]/\mathfrak{P}_1 \cong \mathbb{Z}[i]/\mathfrak{P}_2 \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$) o $p\mathbb{Z}[i]\mathfrak{P}$ (con $\mathbb{Z}[i]/\mathfrak{P} : \mathbb{Z}_p] = 2$) o $p\mathbb{Z}[i] = \mathfrak{P}^2$ (con $\mathbb{Z}[i]/\mathfrak{P} \cong \mathbb{Z}_p$).

Del hecho de que $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ y de que $\mathfrak{P}_1 \cap \mathbb{Z} = p\mathbb{Z}$ (o $\mathfrak{P}_2 \cap \mathbb{Z} = p\mathbb{Z}$, o $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$) se sigue que $\mathbb{Z}[i]/\mathfrak{P}_1$ es generado sobre $\mathbb{Z}_p$ por el $\mathfrak{P}_1$ residuo de i, es decir, por una raiz de $x^2 + 1$ en alguna extensión de $\mathbb{Z}_p$. Debemos entonces determinar en qué extensiones x^2+1 tiene raices sobre $\mathbb{Z}_p$ o, equivalentemente cuándo -1 es un cuadrado módulo p. En el caso $p = 2$ se cumple. Ahora bien si p es un primo impar entonces el grupo multiplicativo de $\mathbb{Z}_p$ es cíclico de orden $p - 1$, si denotamos por k a un generador de este grupo tenemos que $-1 = x^{\frac{p-1}{2}}$, es decir, -1 es un cuadrado en $\mathbb{Z}_p$ si y sólo si $\frac{p-1}{2}$ es par, y esto sólo sucede si p es de la forma $4n+1$. Hemos probado entonces que los primos de la forma $4n + 3$ tienen la propiedad de que el ideal generado por ellos es un ideal primo en $\mathbb{Z}[i]$, tales primos son irreducibles en $\mathbb{Z}[i]$.

Usaremos ahora el hecho de que $\mathbb{Z}[i]$ es euclideano con la norma. De la multiplicatividad de la norma podemos ver que las unidades de $\mathbb{Z}[i]$ son precisamente aquellos elementos de norma 1 a saber $1, -1, i. -i$. Dado un número primo p de la forma $4n + 1$ consideremos la descomposición $p\mathbb{Z}[i] = \mathfrak{P}_1 \cdot \mathfrak{P}_2$ y denotemos por $a + bi$ a un generador de $\mathfrak{P}_1$. Observemos que dado que $f : \mathbb{Q}(i) \to \mathbb{Q}(i)$ dado por $f(x + yi) = x - yi$ es un automorfismo del campo, se debe tener que $(a - bi)\mathbb{Z}[i]$ es un ideal primo distinto de $\mathfrak{P}_1$ pues en caso contrario se tendría que $\frac{a+bi}{a-bi}$ es una unidad de $\mathbb{Z}[i]$, lo cual no es posible, es decir, todos los primos de la forma $4n + 1$ tienen la propiedad de que el ideal generado por ellos se descompone como un producto de dos ideales primos distintos en $\mathbb{Z}[i]$. Más aún $p\mathbb{Z}[i] = (a^2 + b^2)\mathbb{Z}[i]$ de donde podemos concluir además que p es la suma de dos cuadrados.

Hemos probado entonces que $2\mathbb{Z}[i] = \mathfrak{P}^2$ con $\mathfrak{P} = (1 + i)\mathbb{Z}[i]$ es el único ideal primo de $\mathbb{Z}$ que se ramifica en $\mathbb{Z}[i]$.

Aquí detendremos el estudio de los anillos de Dedekind, pero podemos mencionar que en todo anillo de Dedekind la cantidad de ideales primos que se ramifican en una extensión será siempre una cantidad finita.

Bibliografía

[1] John B. Fraleigh, *A First Course in Abstract Algebra, Second edition*: Addison-Wesley publishing company, 1976.

[2] M.F. Atiyah, I.G. Macdonald, *Introducción al Álgebra Conmutativa* : Editorial Reverté, 1989.

[3] Ian Stewart, David Tall, *Algebraic Number Theory*: Chapman and Hall, 1979.

[4] Pierre Samuel, *Teoría Algebráica de Números*, Paris: Ediciones Omega, 1972.

[5] Gerald J. Janusz, *Algebraic Number Fields, Second Edition*: Graduate Studies in Mathematics, American Mathematical Society, 1996.

[6] scar Zariski, Pierre Samuel, *Commutative Algebra, Volume I*: Springer-Verlag, 1958.