UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE MATEMÁTICAS

INTRODUCCIÓN A LA TEORÍA DE ANILLOS CONMUTATIVOS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE

LICENCIADO EN MATEMÁTICA

PRESENTADO POR

EFRAIN VILCA TOMAYLLA

LIMA – PERÚ

2003

A mi esposa Matilde y mi hija Valeria.

AGRADECIMIENTOS

Esta monografía "Introducción a la teoría de anillos conmutativos", es el resultado del curso de estructuras algebraicas que se dictó en la Universidad Nacional de Ingeniería para la obtención de la licenciatura en Matemáticas.

Espero que este material sirva como punto de partida a aquellos estudiantes interesados en el álgebra conmutativa. Desde aquí agradezco al Dr. Carlos Chavez por su asesoría y colaboración en el desarrollo de este trabajo.

INDICE

Glosario de Símbolos.

$\square$	Fin de definición.
$\blacksquare$	Fin de demostración.
$\in$	Pertenencia
$\mathbf{Z}$	Conjunto de los números enteros
$\mathbf{Z}^+$	Conjunto de los números enteros positivos
$\mathbf{Q}$	Conjunto de los números racionales
$\mathbf{R}$	Conjunto de los números reales
1_A	Elemento unidad del anillo *A*.
$\exists$	Existencia
f	Función (homomorfismo)
$Ker(f)$	Kernel del homomorfismo *f*
I	Conjunto ideal de un anillo
$\bigcup_\alpha I_\alpha$	Unión arbitraria de ideales
$\bigcap I$	Intersección de ideales
I^{-1}	Inversa de un ideal
P	Conjunto ideal primo de un anillo
A/I	Anillo cociente por el ideal *I*
$A \setminus P$	Conjunto de elementos que están en *A* y no en *P*
$\langle a \rangle$	Ideal generado por *a*
$A[x]$	Anillo de polinomio sobre un anillo *A*.
ϕ	Conjunto vacío
$=$	Relación
$a \sim \mathrm{b}$	*a* esta relacionado con *b*.
$a \mid b$	*A* divide a *b*.
$\sum$	Suma
$\prod$	Producto
$\subset$	Esta incluido en
$\subset$	Esta incluido propiamente en
	Esta incluido ó es igual a
$A \cong B$	*A* es isomorfo a *B*
$\mathbf{I}$	Matriz identidad

1. INTRODUCCIÓN

La historia del álgebra conmutativa empieza en el siglo IX con trabajos en la teoría de números y la geometría algebraica.

En la teoría de números se estudia escencialmente el anillo de los números enteros **Z**, como son los números primos, factorización, divisibilidad, congruencias, etc. Mientras que en la geometría algebraica se estudia el algebra que son los anillos de polinomios en varias variables y la geometría que es el conjunto de ceros de una familia de polinomios. Por ejemplo, el círculo unitario son los ceros del polinomio $x^2 + y^2 - 1$.

Los anillos conmutativos son conjuntos dotados con dos operaciones binarias "+" y "." cumpliendo las leyes asociativas, conmutativas y distributivas. Como ejemplos importantes tenemos el anillo de números enteros **Z** y el anillo de polinomios $F[x]$, donde F es un campo.

Así pues, el algebra conmutativa es escencialmente el estudio de los anillos conmutativos.

En la teoría de anillos conmutativos podemos establecer como consecuencia de las definiciones de anillos, un objeto fundamental, que son los ***ideales***, estos son, los subgrupos aditivos que son invariantes bajo la multiplicación por cualquier elemento arbitrario del anillo. Podemos distinguir también ciertas clases de ideales: ideales primos, ideales primarios, ideales maximales, etc.

Los ideales pueden ser sumados, multiplicados e intersectados, lo que nos da una nueva clase de estructura combinatoria del conjunto de ideales en un anillo; En particular los ***ideales primos*** juegan un rol importante en este conjunto de ideales.

El término "ideal" viene de la palabra "número ideal", esto debido a Kummer; Los ideales fueron reconocidos como una generalización del concepto de número. En el anillo de los enteros **Z**, cada ideal puede ser generado por un solo número, por el cual los conceptos de "ideal" y "número" son casi idénticos en **Z** (y en cualquier dominio de ideales principales). En un anillo en general, el concepto "ideal" permite generalizar muchas propiedades de los enteros, como ideales

primos en lugar de números primos. En ciertas clases de anillos importantes de la teoría de números, como son los dominios Dedekind, se tiene una nueva versión del teorema fundamental de la arimética: Cada ideal distinto de cero tiene una descomposición única como un producto de ideales primos.

Muchos resultados importantes de la teoría de anillos conmutativos dependen de la condición de finitud, como en el caso de los anillos Noetherianos donde toda sucesión ascendente de ideales se estaciona o termina. El Teorema Básico de Hilbert ($A[x]$ es Noetheriano si A lo es) establece la importancia de incluir en su demostración la condición de finitud.

Empezaremos por revisar algunos conceptos y resultados generales sobre anillos, homomorfismos, ideales, anillo cociente, anillo de polinomios, factorización, localización y módulos que serán base fundamental para tratar el tema: Introducción a la teoría de los anillos conmutativos.

1.1 ANILLOS.

Definición 1.1 *Un conjunto A no vacío es un* ***anillo****, si en A están definidas dos operaciones $+$ y $.$ tales que para todo $a,b,c \in A$ se verifican las siguientes propiedades*:

i. $(a+b)+c = a+(b+c)$ (*ley asociativa*)

ii. $a+b = b+a$ (*ley conmutativa*)

iii. *Existe un elemento* $0 \in A$, *tal que* $a+0 = a$

iv. *Para todo* $a \in A$, *existe un elemento que denotaremos* $-a$ *tal que* $a+(-a) = (-a)+a = 0$

v. $a.(b.c) = (a.b).c$

vi. $a.(b+c) = a.b + a.c$ y $(b+c).a = .b.c + c.a$ (*ley distributiva*).□

Los axiomas del **i**. al **iv**. expresan que A es un grupo abeliano bajo la operación $+$.

Un anillo A se dice ***anillo con unidad***, si existe un elemento $1 \in A$ tal que $1.a = a.1 = a$ para todo $a \in A$.
Un anillo A se dice ***anillo conmutativo***, si $a.b = b.a$ para todo $a,b \in A$.

Un anillo A se dice que es un ***dominio entero***, si es un anillo conmutativo con unidad y si dados $a, b \in A$ tal que $a.b = 0$, entonces $a = 0$ ó $b = 0$.
Un elemento a de un anillo A con unidad se dice ***inversible***, si existe un elemento al que denotaremos $a^{-1} \in A$ tal que $a.a^{-1} = a^{-1}.a = 1$.
Un anillo A se dice ***anillo de división***, si todo elemento distinto de cero de A es inversible.
Un elemento $a \neq 0$, de un anillo A, tal que $a.b = 0$ para algún $b \neq 0$ en A, se llama ***divisor de cero***.
Un subconjunto B de un anillo A, se dice ***subanillo*** de A si y solo si: B es cerrado bajo las operaciones de A (Es decir, para todo $a, b \in B$, $a + b$ y $a.b$ pertenecen a B) y B es un anillo bajo las operaciones inducidas de A.
Un anillo conmutativo A con unidad y donde cada elemento distinto de cero es inversible se llama ***campo***.

Observaciones.

- Cada campo es un dominio entero, el recíproco no siempre es cierto. Por ejemplo **Z** es un dominio entero pero no es un campo.
- Todo subanillo de un dominio entero es un dominio entero.

1.2. HOMOMORFISMOS.

En un anillo existe una estructura bajo las operaciones + y ., nuestro propósito es definir dentro de la clase de funciones entre anillos, aquellas que respeten esta estructura.

Definición 1.2.1 *Sean A y B dos anillos. Una función $f : A \to B$, se dice que es un **homomorfismo de anillos** si para todo $a, b \in A$ se verifica lo siguiente*:

i. $f(a + b) = f(a) + f(b)$

ii. $f(a.b) = f(a).f(b)$ □

En otras palabras, f respeta la suma y la multiplicación entre anillos.

Definición 1.2.2 *Un homomorfismo de anillos* $f : A \to B$ *se dice*:

a. ***homomorfismo de anillo con unidad*** *si* $f(1_A) = 1_B$.

b. ***epimorfismo*** *si es sobreyectivo.*

c. ***monomorfismo*** *si es inyectivo.*

d. ***isomorfismo*** *si es biyectivo.*

e. ***endomorfismo*** *si es homomorfismo en sí mismo.*

f. ***automorfismo*** *si es biyectivo en sí mismo.*□

Sea $f : A \to B$ un homomorfismo de anillos, entonces la ***imagen*** de f es el conjunto:

$$\mathrm{Im}(f) = \{b \in B / (\exists\, a \in A)\, f(a) = b\} = f(A),$$

Sea $f : A \to B$ un homomorfismo de anillos, entonces el ***Kernel*** (*ó núcleo*) de f es el conjunto:

$$Ker(f) = \{a \in A / f(a) = 0\}$$

Se demuestra que:

- Si $f : A \to B$ es un homomorfismo de anillos, entonces:

  $f(0) = 0$

  $f(-a) = -f(a)$, para todo $a \in A$.

  $\mathrm{Im}(f)$ es un subanillo de B.
- Si $f : A \to B$ es un homomorfismo de anillos, entonces f es un isomorfismo si y solo si $Ker(f) = \{0\}$ y $\mathrm{Im}(f) = B$.

1.3. IDEALES.

Definición 1.3.1. *Un subconjunto* I *de un anillo* A *se llama* ***ideal*** *bilátero de* A, *si se verifica lo siguiente*:

i. I *es un subgrupo de* A *en relación a la operación* $+$ *y*

ii. *Para todo* $a \in A$ *y todo* $x \in I$, $x.a \in I$ *y* $a.x \in I$. □

Si solo se pide la condición $a.x \in I$, para todo $x \in I$, $a \in A$, el ideal se llamará ***ideal***

a izquierda.

Si solo se pide la condición $x.a \in I$, para todo $x \in I$, $a \in A$, el ideal se llamará ***ideal a derecha***.

Estas distinciones se desvanecen si A es un anillo conmutativo. Así pues, de aquí en adelante el término "ideal" significará "ideal bilátero".

Sea A un anillo conmutativo y $a \in A$, entonces el conjunto $A.a = \{a.x / x \in A\}$ es un ideal generado por a, denotado por $\langle a \rangle$. Este es el menor ideal de A que contiene a a. y se le llama el ***ideal principal*** generado por a.

Un domino entero donde todos sus ideales son ideales principales se llama ***dominio de ideales principales*** (DIP).

Ejemplo 1.3.1.

a. El conjunto de los números pares **2Z**, es un ideal principal del anillo de enteros **Z**, denotado por $\langle 2 \rangle$.

b. El conjunto de todos los polinomios de $\mathbf{R}[x]$ que son divisibles por el polinomio $x^2 + 1$ es un ideal de $\mathbf{R}[x]$.

Sean $a_1, a_2, ..., a_n \in A$, el ideal generado por $a_1, a_2, ..., a_n$, denotado por $\langle a_1, a_2, ..., a_n \rangle$ es la intersección de todos los ideales de A que contienen a todos los a_i.

Se demuestra que:

- Si I y J son ideales de A, entonces $I.J = \left\{ \sum_{i=1}^{n} x_i.y_i / x_i \in I,\ y_i \in J, n \in \mathbf{Z}^+ \right\}$ es un ideal de A, además $I.J \subset I \cap J$.
- Si I y J son ideales de A, entonces $I + J = \left\{ x_i + .y_i / x_i \in I,\ y_i \in J \right\}$ es un ideal de A.
- Si $I = \bigcap_{\alpha} I_{\alpha}$ es una intersección arbitraria de ideales I_{α} de A, entonces I es un ideal de A.
- Si I y $J_1, J_2, ..., J_n$ son ideales de A, entonces $I.(J_1 + J_2 + ... + J_n) = I.J_1 + I.J_2 + ... + I.J_n$.
- Si $f : A \to B$, un homomorfismo de anillos, entonces el $Ker(f)$ siempre es un ideal bilátero.
- Sea $f : A \to B$, un homomorfismo de anillos, si J un ideal de B, entonces

$f^{-1}(J) = \{a \in A / f(a) \in J\}$ es un ideal de A.

Ejemplo 1.3.2.

a. En el anillo **Z**, si $I = \langle m \rangle$ y $J = \langle n \rangle$, entonces $I + J$ es el ideal generado por el máximo común divisor de m y n.

b. En el anillo **Z**, si $I = \langle m \rangle$ y $J = \langle n \rangle$, entonces $I \cap J$ es el ideal generado por el mínimo común múltiplo de m y n.

c. En el anillo **Z**, si $I = \langle m \rangle$ y $J = \langle n \rangle$, entonces $IJ = \langle mn \rangle$. De aquí podemos concluir que $IJ = I \cap J$ si y solo si m y n son coprimos.

Los ideales primos son fundamentales en la teoría de anillos conmutativos.

Definición 1.3.2. *Sea A un anillo e I un ideal de A, $I \neq A$, entonces*:

i. *I es un **ideal primo** en A, si para todo $a, b \in A$ tal que $a.b \in I$, implica que $a \in I$ ó $b \in I$.*

ii. *I es un **ideal maximal** en A, si para cada ideal M en A tal que $I \subset M$, implica que $M = I$ ó $M = A$.* □

Se demuestra que:

- Un ideal maximal es un ideal primo, el recíproco no siempre es cierto.
- En un dominio de ideales principales cada ideal primo distinto de cero es maximal.
- Un anillo conmutativo A es un campo si y solo si los únicos ideales son $\{0\}$ y el mismo A.
- Sea $f : A \to B$ un homomorfismo de anillos. Si J es un ideal primo en B, entonces $f^{-1}(J)$ es un ideal primo en A. Pero si J es un ideal maximal en B, entonces $f^{-1}(J)$ no necesariamente es maximal en A.

Ejemplo 1.3.3.

a. En el anillo **Z**, el ideal $\langle p \rangle$ es primo si $p = 0$ ó p es un número primo.

b. $4\mathbf{Z}$ no es un ideal primo pues, $2.2 = 4 \in 4\mathbf{Z}$, pero $2 \notin 4\mathbf{Z}$.

c. $\{\bar{0}\}$ no es un ideal primo en $\mathbf{Z}_6$, pues $\bar{2}.\bar{3} = \bar{0}$ pero $\bar{2}, \bar{3} \notin \{\bar{0}\}$.

d. El ideal **4Z** no es maximal en **Z**, pues $\mathbf{4Z} \subsetneq \mathbf{2Z} \subsetneq \mathbf{Z}$.

Observaciones.

- En el anillo de los enteros **Z**, los ideales maximales son los ideales primos distintos de cero, los cuales son generados por un número primo.

1.4. ANILLO COCIENTE.

Sea A un anillo e I un ideal de A, definimos en A una relación de equivalencia de la siguiente forma:
Dos elementos a, b de A están relacionados entre si $(a \sim b)$, si y solo si $a - b \in I$.
La clase de un elemento $a \in A$ es el subconjunto $a + I = \{a + x / x \in I\}$, denotada por $\bar{a}$.
Denotamos por A/I el conjunto de todas las clases de equivalencia.
Definiendo las operaciones $+$ y $.$ en A/I de la siguiente forma:
$\bar{a} + \bar{b} = \overline{a+b}$ y
$\bar{a}.\bar{b} = \overline{a.b}$
Se demuestra que A/I es un anillo con respecto a estas operaciones.

Definición 1.4 *Sea A un anillo e I un ideal de A. El anillo A/I construído en el párrafo anterior se llama* ***anillo cociente*** *de A por el ideal I.* □

Se demuestra que:

- Sea $f : A \to A/I$ definido por $f(a) = \bar{a}$ para todo $a \in A$, entonces f es un epimorfismo de anillos y $Ker(f) = I$; Esta función se llama ***homomorfismo canónico de paso al cociente***.
- Teorema Fundamental para Homomorfismo de Anillos: Sea $f : A \to B$ un homomorfismo de anillos, entonces $A/Ker(f) \cong \mathrm{Im}(f)$.
- Existe una correspondencia uno a uno entre los ideales de A/I y los ideales de A que contienen a I.

- Un ideal I es primo en A si y solo si el anillo cociente A/I es un dominio entero.
- Un ideal I es maximal en A si y solo si el anillo cociente A/I es un campo.

Ejemplo 1.4.

a. Si p es un número primo, entonces el ideal $\langle p \rangle$ es maximal en anillo de enteros **Z**. Luego el anillo cociente $\mathbf{Z}/\langle p \rangle = \mathbf{Z}_p$ es un campo.

b. Sea F un campo. Entonces $F[x]$ es un dominio de ideales principales, puesto que los ideales de $F[x]$ tienen la forma $I = \langle f(x) \rangle$, donde $f(x)$ es un polinomio mónico de menor grado. El ideal I es primo (y de aquí maximal) si y solo si $f(x)$ es irreducible. Entonces si $f(x)$ es irreducible, el anillo $F[x]/\langle f(x) \rangle$ es un campo.

c. En el anillo de polinomios $\mathbf{Z}[x]$, el ideal $\langle n, x \rangle$ generado por $n \in \mathbf{Z}$ y x es un ideal primo si y solo si n es un número primo. En efecto, definiendo la función $f : \mathbf{Z}[x] \to \mathbf{Z}_n$ por $f(a_0 + a_1x + ... + a_nx^n) = a_0$ para todos los polinomios $a_0 + a_1x + ... + a_nx^n \in \mathbf{Z}[x]$, se demuestra que f es un epimorfismo de anillos y que el $Ker(f) = \langle n, x \rangle$. Así pues, $\mathbf{Z}[x]/\langle n, x \rangle \cong \mathbf{Z}_n$, de manera que $\langle n, x \rangle$ es un ideal primo si y solo si $\mathbf{Z}_n$ es un dominio entero, lo cual ocurre si y solo si n es un número primo.

1.5. ANILLO DE POLINOMIOS.

Definición 1.5 *Sea A un anillo conmutativo con unidad. El anillo de polinomios sobre A en una variable x es el conjunto $A[x]$ de secuencias en A con un número finito de términos distintos de cero. Si $(a_0, a_1, a_2, ...)$ es un elemento en $A[x]$ con $a_n = 0$ para todo $n > N$, entonces usualmente escribimos este elemento como:*

$$\sum_{i=0}^{N} a_i x^i = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_Nx^N.$$

La adición y la multiplicación en $A[x]$ se definen como:

$$\sum_{i=0}^{N} a_i x^i + \sum_{i=0}^{N} b_i x^i = \sum_{i=0}^{N} (a_i + b_i) x^i$$

$$\sum_{i=0}^{N} a_i x^i \cdot \sum_{i=0}^{N} b_i x^i = \sum_{i=0}^{N} (\sum_{j=0}^{i} a_j b_{i-j}) x^i$$

$A[x]$ es un anillo bajo estas operaciones.□

Un anillo de polinomios en dos variables x, y se define como:

$$A[x,y] = A[x].A[y]$$

Un anillo de polinomios en un número finito de variables $x_1, x_2, ..., x_n$ se define como:

$$A[x_1, x_2, ..., x_n] = A[x_1, x_2, ..., x_{n-1}].A[x_n] = A[x_1]A[x_2]..A[x_n].$$

1.6. LOCALIZACIÓN.

La construcción de anillos de fracciones y el proceso asociado de localización son quizás las herramientas más importantes en el álgebra conmutativa. Por ejemplo el procedimiento para la construcción de los números racionales **Q** del anillo de los enteros **Z**, se puede extender fácilmente a cualquier dominio entero A y construir el campo de fracciones de A.

Definición 1.6.1 *Sea A un anillo y S un subconjunto de A. S es llamado* ***subconjunto multiplicativo*** *si $1 \in S$ y para todo par $s,t \in S$, se tiene que $s.t \in S$.* □

Ejemplo 1.6.1.

a. El conjunto $S = A - \{0\}$ es un subconjunto multiplicativo si A es un dominio entero

b. El conjunto $S = A \setminus P$ es un subconjunto multiplicativo si P es un ideal primo en A, y se denota como A_P.

c. El conjunto $S_c = \{1, c, c^2, c^3, ...\}$ es un subconjunto multiplicativo, para cada $c \in A$.

Definimos una relación $\equiv$ en $A \times S$

$(a,s) \sim (b,t)$ *si y solo si existe* $u \in S$ *tal que* $(a.t - b.s).u = 0$.

Se puede demostrar que $\equiv$ es una relación de equivalencia.

Denotamos por a/s las clases de equivalencias de (a,s) con respecto a $\equiv$

Sea $S^{-1}A$ el conjunto de todas las clases de equivalencia

Definiendo las operaciones $+$ y $.$ en $S^{-1}A$ de la siguiente forma:

$$a/s + b/t = (a.t + b.s)/s.t$$

$$(a/s).(b/t) = a.b/s.t.$$

donde el cero de $S^{-1}A$ es $0/1$ y la unidad es $1/1$.

Se demuestra que $S^{-1}A$ es un anillo con respecto a estas operaciones.

Definición 1.6.2. *Sea A un anillo conmutativo y sea S un subconjunto multiplicativo no vacío de A. El anillo $S^{-1}A$ construido en el parráfo anterior se llama* ***anillo de fracciones*** *de A con respecto a S*

Ejemplo 1.6.2.

a. Si A es un dominio entero y $S = A - \{0\}$, entonces el anillo $S^{-1}A$ es un ***campo de fracciones*** de A.

b Sea P un ideal primo de A y $S = A \setminus P$ es un subconjunto multiplicativo de A. Entonces el anillo $A_P = (A \setminus P)^{-1}A = \{r/s / r \in A, s \notin P\}$ se llama la ***localización*** de A en P.

Se demuestra que:

- Sea $f : A \to S^{-1}A$ definido por $f(a) = a/1$, para todo $a \in A$, entonces f es un homomorfismo de anillos y cada elemento de $S^{-1}A$ es de la forma $f(a)/f(s)$ para algún $a \in A$ y algún $s \in S$.

Observaciones.

- Cada dominio entero puede ser sumergido en un campo, el campo más pequeño en el que se puede sumergir es su campo de fracciones.
- Si A es un dominio entero y $S = A - \{0\}$, entonces la relación de equivalencia en $A \times S$ se reduce a $(a,s) \sim (b,t)$ *si y solo* $a.t = b.s$.

Ejemplo 1.6.3.

a. El campo de fracciones del anillo de los números enteros **Z** es el campo de los números racionales **Q**.

b. Si $A = \mathbf{Z}$ y S es el conjunto de los números pares, entonces $S^{-1}A$ puede ser

identificado con el siguiente subanillo de **Q** : $\left\{\frac{a}{b} / a,b \in \mathbf{Z},\ b \text{ par}\right\}$.

c. Si $A = \mathbf{Z}$ y $P = \langle p \rangle$, donde p es un número primo y $S = A \setminus P$; Entonces A_P es el conjunto de todos los números racionales m/n donde n y p son coprimos.

1.7. FACTORIZACIÓN.

Uno de los temas más importantes en la teoría de anillos conmutativos es el tema de la factorización en primos. En uno de los intentos de la prueba del ultimo teorema de Fermat (propuesto por Lamé en 1847) se usó el supuesto de que el anillo de enteros cyclotmic $\mathbf{Z}[\omega_n]$ era de factorizacion única, donde $\omega_n = \mathbf{e}^{2\pi i/n}, n \in \mathbf{Z}^+$. Desafortunadamente esto no es cierto en general para todo $n \in \mathbf{Z}^+$. Cauchy descubrió que falla cuando $n = 23$ (En el anillo $\mathbf{Z}[\mathbf{e}^{2\pi i/23}]$ se tiene que el número 2 es irreducible, pero no primo). Este resultado fue un retroceso para las matemáticas de ese tiempo.

Definición 1.7.1. *Sea A un dominio entero y $a,b \in A$, entonces a divide a b si existe $c \in A$ tal que $b = c.a$, y lo denotamos por $a \mid b$.* □

Definición 1.7.2. *Sea A un dominio entero y $p \in A$, tal que p no es inversible. Entonces se dice que p es **irreducible** si $p = a.b$ implica que a es inversible ó que b es inversible.*□

Definición 1.7.3. *Sea A un dominio entero. Entonces decimos que A es un **dominio de factorización única** (**DFU**) si $a \in A, a \neq 0$, a no inversible, entonces existen números primos únicos $p_1, p_2, ..., p_n \in A$ (salvo el orden), y exponentes únicos $e_1, e_2, ..., e_n \in \mathbf{Z}^+$ tal que $a = p_1^{e_1}.p_2^{e_2}.....p_n^{e_n}$..*□

Ejemplo 1.7.

a. El anillo de los enteros **Z** y el anillo de polinomios $F[x]$, donde F es un campo, son dominios de factorización única.

Se demuestra que:

- Si p es primo, entonces p es irreducible. El recíproco no siempre es cierto. Por ejemplo en el anillo $\mathbf{Z}[\sqrt{-5}]$, 3 es irreducible pero no primo, pues se tiene que $(4+\sqrt{-5})(4-\sqrt{-5}) \in \langle 3\rangle$, mientras que $(4+\sqrt{-5}) \notin \langle 3\rangle$ y $(4-\sqrt{-5}) \notin \langle 3\rangle$.
- Si A es un DIP, entonces A es un DFU.
- A es un DFU si y solo si $A[x]$ es un DFU.

1.8. MODULOS.

El concepto de módulo que definiremos a continuación es una generalización del concepto de espacio vectorial, donde los escalares son elementos de un anillo con unidad.

Definición 1.8 *Sea A un anillo con unidad. Un conjunto no vacío M es llamado A –módulo a izquierda, si M es un grupo abeliano en relación a la operación $+$ y existe una multiplicación escalar $\mu : A \times M \to M$ denotada por $\mu(a,m) = a.m$, para todo $a \in A$ y todo $m \in M$, tal que para todo $a_1, a_2 \in A$ y todo $m_1, m_2 \in M$,* se *verifica lo siguiente*:

i. $a(m_1 + m_2) = a.m_1 + a.m_2$

ii. $(a_1 + a_2).m = a_1.m + a_2.m$

iii. $a_1(a_2.m) = (a_1.a_2)m$

iv. $1(m) = m$. □

Sea M un A –módulo izquierda, un ***submodulo*** de M es cualquier subconjunto de M que es A –módulo bajo las operaciones inducidas de M.
Sea M un A –módulo izquierda y $m \in M$, el conjunto $A.m = \langle m\rangle = \{a.m / a \in A\}$ es un submódulo de M el más pequeño que contiene a m, también es llamado ***submodulo cíclico*** generado por m.
Sea M un A –módulo a izquierda, M se dice ***finitamente generado*** si existen $m_1, m_2, \ldots, m_n \in M$ tal que $M = \sum_{j=1}^{n} Am_j$. De este modo se dice que $\{m_1, m_2, \ldots, m_n\}$ es un conjunto de generadores de M.

Ejemplo 1.8.

a. Todo espacio vectorial sobre un campo F, es un F–módulo.

b. Todo ideal I de un anillo conmutativo A es un A–módulo. En particular A mismo es un A–módulo.

2. ANILLOS NOETHERIANOS

Los anillos Noetherianos son de lejos la clase más importante de anillos en el estudio de anillos conmutativos. A partir de esta sección el término "anillo" significará "anillo conmutativo con unidad".

Definición 2.1. *Un anillo A se llama anillo* ***Noetheriano*** *si para cada sucesión ascendente de ideales de A,*

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

existe un entero positivo n, tal que $I_n = I_{n+1} = I_{n+2} = \ldots$ □

Equivalentemente podemos definir que un anillo es Noeteriano, si toda sucesión ascendente de ideales se estaciona ó termina.

Definición 2.2. *Un anillo noetheriano se llama* ***dominio Noetheriano*** *si como anillo es un dominio entero.*□

Definición 2.3. *Un anillo A se llama anillo* ***Artiniano*** *si para cada sucesión descendente de ideales de A,*

$$I_1 \supset I_2 \supset I_3 \supset \ldots$$

existe un entero positivo n, tal que $I_n = I_{n+1} = I_{n+2} = \ldots$ □

Ejemplo 2.1.

a. El anillo de los números enteros **Z** es Noetheriano, pues cada sucesión ascendente de ideales se estaciona, pero no es Artiniano, porque si $a \in \mathbf{Z}$ y $a \neq 0$, entonces se tiene que $\langle a \rangle \supset \langle a^2 \rangle \supset \langle a^3 \rangle \ldots \supset \langle a^n \rangle \ldots$, lo cual es una sucesión estrictamente decreciente.

Teorema 2.1. *Las siguientes afirmaciones en un anillo A son equivalentes*:

a. *A es un anillo Noetheriano.*

b. *Cada conjunto S no vacío, de ideales de A tiene un elemento maximal: Es decir, existe un ideal $I \in S$ tal que, si $J \in S$ e $I \subset J$, entonces $I = J$.*

c. *Cada ideal de A es finitamente generado*: *Es decir, si I es un ideal de A, entonces existen elementos $b_1, b_2, ..., b_n$ en I, tal que* $I = \langle b_1, b_2, .., b_n \rangle = \left\{ \sum_{i=1}^{n} a_i b_i \,/\, a_i \in A, n \in \mathbf{Z}^+ \right\}$

Demostración.

a.⇒b. Sea S un conjunto no vacío de ideales en un anillo Noetheriano A, y supongamos que S no posee un elemento maximal. Sea $I_1 \in S$, como I_1 no es maximal en S, entonces existe un ideal $I_2 \in S$ tal que $I_1 \subsetneq I_2$. Repitiendo el mismo argumento, encontramos un ideal $I_3 \in S$ tal que $I_1 \subsetneq I_2 \subsetneq I_3$, y así sucesivamente. De este modo, tendríamos una sucesión ascendente de ideales $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq$ ....que no termina. Lo que contradice el hecho que A es Noetheriano. Por lo tanto existe por lo menos un ideal I_n en A el cual es maximal en S.

b.⇒c. Sea I un ideal de A, y sea $S = \left\{ J / J \subset I,\ J \text{ ideal en } A, J \text{ finitamente generado} \right\}$. Claramente S no es vacío puesto que $\{0\} \in S$, entonces S contiene un elemento maximal digamos J_0. Si $b \in I$, entonces $J_0 + \langle b \rangle$ es un ideal finitamente generado contenido en I y conteniendo a J_0 , esto implica que $J_0 + \langle b \rangle = J_0$, y $b \in J_0$, luego $I \subset J_0$. Así que $J_0 = I$. Concluimos entonces que I es finitamente generado.

c.⇒a. Sea $I_1 \subset I_2 \subset I_3 \subset ...$ una sucesión ascendente de ideales en A. Entonces $I = \bigcup I_k$ es un ideal de A. De aquí I es finitamente generado, digamos $I = \langle b_1, b_2, ... b_n \rangle$. Luego existe un entero m, tal que $b_i \in I_m$ para $i = 1, 2, ..n$ e $I \subset I_m$. De $I \subset I_m \subset I = \bigcup I_k$ concluimos que $I_m = I_{m+1} = I_{m+2} = ...$ Por lo tanto A es Noetheriano. ■

Corolario 2.1. *Si A es un dominio de ideales principales, entonces A es un anillo Noetheriano*.

Demostración.

Si A es un dominio de ideales principales entonces cada ideal de A es un ideal principal. Es decir cada ideal es generado por un elemento de A, aplicando el Teorema 2.1.c. se concluye que A es Noetheriano.■

Ejemplo 2.2.

a. En particular cualquier campo y **Z** son anillos Noetherianos pues son dominios de ideales principales.

b. Sea A un anillo, el anillo de polinomios $A[x_1, x_2, ...]$ de infinitas indeterminadas no es Noetheriano pues: $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset ...$ es una sucesión de ideales estrictamente creciente. Como $A[x_1, x_2, ...]$ es un dominio entero entonces éste está incluido en su campo de fracciones. Así pues, un subanillo de un anillo Noetheriano no necesariamente es Noetheriano.

Teorema 2.2. *Sea A un anillo, si A es Noetheriano, entonces cualquier imagen homomorfa de A es Noetheriano.*

Demostración.

Sea $f : A \to B$ un epimorfismo de un anillo Noetheriano A sobre un anillo B. Si J es un ideal de B, entonces $f^{-1}(J)$ es un ideal de A y es finitamente generado. Es decir existen elementos $a_1, a_2, ..., a_n \in A$ tal que $f^{-1}(J) = \langle a_1, a_2, ..., a_n \rangle$. Así pues, para cada elemento $b \in J$ existe $a \in f^{-1}(J)$ tal que $f(a) = b$, como $a = \sum_{i=1}^{n} \beta_i . a_i$, $\beta_i \in A$, entonces $b = f(a) = \sum_{i=1}^{n} f(\beta_i) . f(a_i)$. Luego $J = \langle f(a_1), f(a_2), ... f(a_n) \rangle$ es finitamente generado. De aquí concluimos que cada ideal de B es finitamente generado. Por lo tanto B es un anillo Noetheriano.■

Teorema 2.3. *Sea I un ideal de A tal que toda sucesión ascendente de ideales de A contenidos en I se estaciona. Entonces si A/I es Noetheriano, implica que A también es Noetheriano.*

Demostración.

Sea I un ideal de A con la propiedad de que cada sucesión ascendente de ideales de A contenidos en I se estaciona y supóngase que A/I es Noetheriano.
Sea $J_1 \subset J_2 \subset J_3 \subset ...$una sucesión ascendente de ideales de A. Entonces:

$$J_1 \cap I \subset J_2 \cap I \subset J_3 \cap I \subset ...$$

es una sucesión ascendente de ideales de A contenidos en I, y

$$(J_1 + I)/I \subset (J_2 + I)/I \subset (J_3 + I)/I \subset ...$$

es una sucesión ascendente de ideales de A/I.

Por nuestra hipotesis ambas sucesiones se estacionan; es decir existe un entero positivo n tal que:

$$J_n \cap I = J_{n+h} \cap I \text{ y}$$

$$(J_n + I)/I = (J_{n+h} + I)/I, \text{ para cada } h = 1, 2, 3, \ldots.$$

Supóngase que $b_h \in J_{n+h}$ para algún entero positivo h. Puesto que $(J_n + I)/I = (J_{n+h} + I)/I$, existen elementos $a_1, a_2 \in I$ y $b \in J_n$ tal que $(b_h + a_1) - (b - a_2) \in I$, de aquí $b_h - b \in I$. Como $J_n \subset J_{n+h}$ entonces $b \in J_{n+h}$. Luego $b_h - b \in J_{n+h} \cap I = J_n \cap I$.

De aquí $b_h \in J_n$, así $J_{n+h} \subset J_n$, y $J_n = J_{n+h}$ para cada $h = 1, 2, 3, \ldots$; Es decir la sucesión $J_1 \subset J_2 \subset J_3 \subset \ldots$ se estaciona. Por lo tanto, A es Noetheriano. ■

Teorema 2.4. *Si A es Noetheriano y S es un subconjunto multiplicativo en A tal que $S^{-1}A \neq 0$, entonces $S^{-1}A$ es Noetheriano.*

Demostración.

Sea A un anillo, y S un subconjunto multiplicativo de A. Entonces existe un homomorfismo $\alpha_s : A \to S^{-1}A$ definido por $\alpha_s(a) = a/1$, donde cada elemento de $S^{-1}A$ puede ser escritos en la forma $\alpha_s(a)/\alpha_s(s)$ para algún $a \in A$, $s \in S$ (ver Sección 1.6)

Sea J un ideal de AS^{-1}, entonces es claro que $I = \{a \in A / \alpha_s(a) \in J\}$ es un ideal en A y el ideal $\langle \alpha_s(I) \rangle$ generado por $\alpha_s(I)$ en $S^{-1}A$ está contenido en J. Si $\alpha' \in J$, entonces $\alpha' = \alpha_s(a)/\alpha_s(s)$ para algún $a \in A, s \in S$. Puesto que J es un ideal en AS^{-1}, $\alpha_s(a) \in J$, de aquí $a \in I$ y así $\alpha' \in \langle \alpha_s(I) \rangle$. Esto implica que $J = \langle \alpha_s(I) \rangle$.

Si A es Noetheriano, entonces I es finitamente generado, lo que implicaría que J también es finitamente generado. Por lo tanto, AS^{-1} es Noetheriano.■

***Corolario* 2.2**. *Si A es un anillo Noetheriano y P es un ideal primo de A, entonces A_P es Noetheriano.*

Demostración.

Sea $S = A \setminus P$ y aplicando el Teorema 2.4.■

Teorema 2.5. *Si A es Noetheriano e I un ideal de A, entonces A/I es*

Noetheriano.

Demostración.

Sea $f : A \to A/I$ definido por $f(a) = \bar{a}$ para todo $a \in A$. Entonces f es un epimorfismo de anillos. Como A es Noetheriano, por el teorema 2.2 se tiene que A/I es Noetheriano.■

El siguiente Teorema es una herramienta poderosa para probar en casos específicos la Noetherianidad de un anillo y una herramienta fundamental en el estudio de la geometría algebraica y el álgebra conmutativa.

Teorema 2.6. (**TEOREMA BÁSICO DE HILBERT**) *Si A es un anillo Noetheriano, entonces también lo es el anillo de polinomios $A[x]$.*

Demostración.

Sea J un ideal $A[x]$ demostraremos que J es finitamente generado sobre $A[x]$. Consideremos el siguiente ideal de A. Para cada entero $k \geqq 0$, sea $I_k = \left\{a \in A / p(x) \in J \subset A[x],\ p(x) = a.x^k + \sum_{i=0}^{k-1} a_i.x^i\right\} \cup \{0\}$, es decir, I_k es el ideal que contiene al 0 y los coeficientes principales de los polinomios de grado k de J. Entonces $I_0 \subset I_1 \subset I_2 \subset \ldots$ es una sucesión ascendente de ideales en A. Puesto que A es Noetheriano, existe un entero m tal que $I_m = I_{m+1} = \ldots$ y los ideales $I_0, I_1, I_2 \ldots$ son finitamente generados. Para cada $i = 0, 1, \ldots m$ sea $\{a_{i1}, a_{i2} \ldots, a_{im_i}\}$ un comjunto de generadores para I_i, y sea f_{ij} un polinomio en J de grado i con coeficientes a_{ij} para $j = 1, .. n_i$. Procederemos a demostrar que el conjunto de polinomios $\{f_{ij}\}$ $i = 0, 1, \ldots m; j = 1, .. n_i$ genera J. Puesto que $I_m = I_d$ para cualquier entero $d \geqq m$, los coeficientes de $x^{d-m}f_{m1}, x^{d-m}f_{m2}, \ldots, x^{d-m}f_{mn_m}$, generan I_d. De aquí, si f es un polinomio en J de grado $d \geqq m$, entonces existen elementos $b_1, b_2, \ldots b_{n_m}$ en A tal que $f - \sum_{j=1}^{n_m} b_j f_{mn_j}$ es un polinomio en J de grado menor que d. Si f es un polinomio en J de grado $d < m$, entonces existen elementos $c_1, c_2, \ldots c_{n_d}$ en A tal que $f - \sum_{j=1}^{n_d} c_j f_{dj}$ es un polinomio en J de grado menor que d. Un argumento inductivo muestra que, si $f \in J$ entonces f es combinación A-lineal de los f_{ij}. Luego J es finitamente generado, y esto completa la demostración. ■

Corolario 2.3. *Si A es un anillo Noetheriano, entonces también lo es cualquier anillo de polinomios con un número finito de indeterminadas* $A[x_1, x_2, ..., x_n]$.

Demostración.

Por inducción sobre n y aplicando el teorema de Hilbert 2.6, pues $A[x_1, x_2, ..., x_n] = (A[x_1, x_2, ..., x_{n-1}])[x_n]$.■

Corolario 2.4. *Sea B un anillo el cual es finitamente generado sobre un subanillo A de B. Si A es Noetheriano, entonces también lo es B.*

Demostración.

Como B es finitamente generado sobre A, entonces existen $b_1, b_2, ..., b_n \in B$ tal que cada elemento de B se escribe como combinación lineal de potencias de $b_1, b_2, ..., b_n$ con coeficientes en A, lo que es equivalente a decir que el homomorfismo de anillo $f_{b_1,b_2,...,b_n} : A[x_1, x_2, ..., x_n] \to B$ definido como $p \mapsto p(b_1, b_2, ..., b_n)$ es un epimorfismo. Como A es Noetheriano, entonces por el Corolario 2.3 $A[x_1, x_2, ..., x_n]$ es Noetheriano. Así pues, por el Teorema 2.2 el anillo B también es Noetheriano.■

Ejemplo 2.3.

a. Sea $\mathbf{Z}[i] = \{a + bi / a, b \in \mathbf{Z}\}$, el anillo de los enteros gaussianos. Si definimos una funcion $f : \mathbf{Z}[x] \to \mathbf{Z}[i]$ por $(x \mapsto i)$, se demuestra que f es un epimorfismo de anillos. Luego como $\mathbf{Z}$ es Noetheriano, entonces por el Teorema de Hilbert 2.6 el anillo $\mathbf{Z}[x]$ es Noetheriano y de aquí por el Teorema 2.2 el anillo $\mathbf{Z}[i]$ también es Noetheriano.

Lema 2.1. *En un anillo Noetheriano A cada ideal contiene un producto de ideales primos.*

Demostración.

Supóngase que no; Entonces sea S el conjunto de ideales de A los cuales no son primos y no contienen ningun producto de ideales primos, y que $S \neq \varnothing$. Puesto

que A es Noetheriano, S contiene un elemento maximal I. Puesto que $I \in S$, entonces I no es un ideal primo, es decir existen $a,b \in A$, $a,b \notin I$ tal que $a.b \in I$. Sean $I_1 = \langle a \rangle + I$ y $I_2 = \langle b \rangle + I$. ideales de A. Entonces $I \subsetneq I_1$ e $I \subsetneq I_2$ y $I_1 I_2 \subset I$. Puesto que I es un elemento maximal en S. I_1 y I_2 contienen un producto de ideales primos. Por tanto I contiene un producto de ideales primos. Lo cual es una contradición. Así pues, $S = \varnothing$ y el lema queda probado.■

Definición 2.4. *Sea A un anillo Noetheriano, un ideal $I \neq A$ se llama* ***irreducible*** *si $I = B \cap C$, entonces $I = B$ ó $I = C$.* □

Lema 2.2. *En un anillo Noetheriano A cada ideal es una intersección finita de ideales irreducibles.*

Demostración.

Supóngase que no; Entonces sea S el conjunto de ideales en A los cuales no son irreducibles y tampoco son una intersección finita de ideales irreducibles, y que $S \neq \varnothing$. Puesto que A es Noetheriano, S contiene un elemento maximal I. Puesto que I no es irreducible, entonces se tiene que $I = B \cap C$, donde $B \supset I$ y $C \supset I$. Como I es maximal entonces B y C son intersecciones finitas de ideales irreducibles, lo que implicaría que I es irreducible; lo cual es una contradicción. Así pues, $S = \varnothing$ y el lema queda probado.■

3. DESCOMPOSICIÓN PRIMARIA

La descomposición primaria de un ideal en ideales primarios es base fundamental de la teoría de ideales. Para la geometría algebraica provee los fundamentos algebraicos para descomponer una variedad algebraica en componentes irreducibles. Desde el punto de vista de la teoria de números permite generalizar la factorización de enteros como un producto de potencias de primos.

El anillo de números enteros **Z** y el anillo de polinomios $F[x]$, donde F es un campo, son dominios de factorización única (DFU); Pero esto no es cierto para cualquier anillo conmutativo en general. como por ejemplo el anillo $\mathbf{Z}[\sqrt{-5}]$, en el cual $6 = 2.3 = (1+\sqrt{-5}).(1-\sqrt{-5})$, donde se puede demostrar que $2, 3, 1+\sqrt{-5}$ y $1-\sqrt{-5}$ son irreducibles en el anillo $\mathbf{Z}[\sqrt{-5}]$.

En general no todo ideal en un anillo Noetheriano es igual a un producto de ideales primos. Por ejemplo, en el anillo de polinomios con 2 indeterminadas $F[x,y]$, consideremos el ideal $\langle x^2, y\rangle$ generado por los elementos x^2 e y. Como $F[x,y]/\langle y\rangle \cong F[x]$, el único ideal primo que contiene a $\langle x^2, y\rangle/\langle y\rangle$ es $\langle x, y\rangle/\langle y\rangle$, esto implica que en $F[x,y]$ el único ideal primo que contiene $\langle x^2, y\rangle$ es $\langle x, y\rangle$. Puesto que $\langle x, y\rangle^2 = \langle x^2, x.y, y^2\rangle$, el cual está contenido propiamente en $\langle x^2, y\rangle$ esto imposibilita que podamos expresar $\langle x^2, y\rangle$ como un producto de ideales primos. Así pues para poder obtener una apropiada generalización de la "factorización única" de ideales (no de elementos) para una amplia clase de anillos (los anillos Noetherianos) es necesario reemplazar el producto de ideales por intersección de ideales y reemplazar potencias de ideales primos por ideales primarios.

De este modo un ideal primo es la generalización de un número primo y la correspondiente generalización de la potencia de un primo es un ideal primario.

En esta sección probaremos que en un anillo Noetheriano, cada ideal es una intersección de un número finito de ideales "*primarios*".

Definición 3.1. *Un ideal I en un anillo A es un* ***ideal primario*** *si éste satisface la siguiente condición*: *Si $a.b \in I$, $a, b \in A$, $a \notin I$, entonces existe un entero positivo*

n, *tal que* $b^n \in I$. □

Definición 3.2. *El* ***radical*** $\sqrt{I}$ *de un ideal* I *en* A *es la intersección de todos los ideales primos en* A *los cuales contienen a* I.

Si $P = \sqrt{I}$, entonces I se dice que es P –primario.□

Ejemplo 3.1.

a. En el anillo de enteros **Z**, para cada primo $p \in \mathbf{Z}$ y cada entero positivo n, el ideal $\langle p^n \rangle$ es un ideal primario con radical $\sqrt{\langle p^n \rangle} = \langle p \rangle$. En efecto, sean $a, b \in \mathbf{Z}$ con $a.b \in \langle p^n \rangle$, entonces $p^n \mid ab$, así $p \mid a$ ó $p \mid b$. Si $a \notin \langle p^n \rangle$, entonces $p \nmid a$ implica que $p^n \mid b$, de aquí $b \in \langle p^n \rangle$. Así pues, $\langle p^n \rangle$ es un ideal primario.

Corolario 3.1. *Sean* I, Q *ideales de un anillo* A *con* $I \subseteq Q$. *Entonces* Q *es un ideal primario de* A *si y solo si* Q/I *es un ideal primario de* A/I.

Demostración.

⇒ Supongamos que Q es un ideal primario. Sean $\bar{a}, \bar{b} \in A/I$, tal que $\bar{a}.\bar{b} \in Q/I$ y $\bar{a} \notin Q/I$. Entonces $a, b \in A$, $a.b \in Q$ y $a \notin Q$. Por nuestra hipotesis Q es un ideal primario, entonces existe $n \in \mathbf{Z}^+$ tal que $b^n \in Q$, lo que implica que $\bar{b}^n \in Q/I$. Así pues, Q/I es un ideal primario.

⇐ Recíprocamente, supongamos que Q/I es un ideal primario de A/I. Sean $a, b \in A$, tal que $a.b \in Q$ y $a \notin Q$. Entonces $\bar{a}, \bar{b} \in A/I$, $\bar{a}.\bar{b} \in Q/I$ puesto que $I \subseteq Q$ y $\bar{a} \notin Q$. Por nuestra hipotesis Q/I es un ideal primario, entonces existe $n \in \mathbf{Z}^+$ tal que $\bar{b}^n \in Q/I$, lo que implica que $b^n \in Q$. Así pues, Q es un ideal primario..■

Definición 3.3 *Un elemento* a *de un anillo* A *es* ***nilpotente*** *si*, $a^n = 0$ *para algún entero positivo* n. □

Se puede demostrar que el conjunto de los elementos nilpotentes de A forman un ideal de A.

Definición 3.4 *Sean A un anillo, el* ***nilradical*** *de A se define como el ideal*

$$\aleph(A) = \{a \in A / a^n = 0, \text{para algún } n \in \mathbf{Z}^+\}. \ \square$$

Proposición 3.1. *Sea A un anillo, entonces*:

a *El nilradical de $A/\aleph(A)$ es 0.*

b *El nilradical de A es la intersección de todos los ideales primos de A.*

Demostración.

a. Sea $\bar{a} \in A/\aleph(A)$ representado por a. Entonces $\bar{a}^n$ es representado por a^n, de manera que $\bar{a}^n = 0$ implica que $a^n \in \aleph(A)$, y de aquí $(x^n)^k = 0$ para algún $k \in \mathbf{Z}^+$, entonces $a \in \aleph(A)$. Así pues $\bar{a} = 0$.

b. Sea S la intersección de todos los ideales primos de A. Si $a \in \aleph(A)$, entonces $a^n = 0$ para algún $n \in \mathbf{Z}^+$, así a^n pertence a cada ideal primo de A. Lo que implica que a pertence a cada ideal primo de A. Así pues, $a \in S$. Recíprocamente, supongamos que $a \notin \aleph(A)$, entonces $a^k \neq 0$ para todo $k \in \mathbf{Z}^+$. Sea Σ el conjunto de ideales con la siguiente propiedad: $a^k \notin I$ para todo $k \in \mathbf{Z}^+$. Entonces Σ no es vacío pues $0 \in \Sigma$. Aplicando el Lema de Zorn, con respecto a la inclusión, Σ tiene un elemento maximal P. Demostraremos que P es un ideal primo. Sean $x,y \notin P$. Entonces los ideales $P + \langle x \rangle$ y $P + \langle y \rangle$ contienen estrictamente a P y no pertencen a Σ; así $a^m \in P + \langle x \rangle$ y $a^n \in P + \langle y \rangle$ para algún $m,n \in \mathbf{Z}^+$, Esto implica que $a^{m+n} \in P + \langle xy \rangle$, y de aquí $P + \langle xy \rangle \notin \Sigma$ y así $xy \notin P$. Así pues, P es un ideal primo tal que $a \notin P$, de manera que a no está en la intersección de todos los ideal primos de A ■

Corolario 3.2. *Un ideal I de un anillo A, es primario si y solo si cada divisor de cero en A/I es nilpotente.*

Demostración.

⇒ Supongamos que I un ideal primario y sea $\bar{a} \in A/I$ un divisor de cero entonces $\bar{a}.\bar{b} = \bar{0}$ para algún $\bar{b} \neq \bar{0}$ de aquí $a,b \in A$ y $a.b \in I$ además $b \notin I$. Entonces como I es un ideal primario existe un entero $n \in \mathbf{Z}^+$ tal que $a^n \in I$, lo que implica que $\bar{a}^n = \bar{0}$. Por tanto $\bar{a}$ es nilpotente.

$\Leftarrow$ Supongamos que cada divisor de cero de A/I es nilpotente. Sean $a,b \in A$, $a.b \in I$ y $a \notin I$, entonces $\bar{a}.\bar{b} = \bar{0}$ para algún $\bar{b} \neq \bar{0}$, como $\bar{b}$ es divisor de cero de A/I entonces es nilpotente, por tanto existe un entero $n \in \mathbf{Z}^+$ tal que $\bar{b}^n = \bar{0}$, lo que implica que $b^n \in I$. Por tanto I es un ideal primario.■

Ejemplo 3.2.

a. Aplicando el corolario 3.1. Sea $A = F[x,y]$, donde F es un campo, e $I = \langle x, y^2 \rangle$. Entonces $A/I \cong F[y]/\langle y^2 \rangle$, en el cual los divisores de cero son todos los multiplos de y, y de aquí son nilpotentes. Así pues I es un ideal primario, cuyo radical es $P = \langle x,y \rangle$. Puesto que $P^2 \subsetneq I \subsetneq P$, concluimos que un ideal primario no necesariamente es un producto de ideales primos.

Teorema 3.1. *Sea I un ideal en un anillo A, entonces el radical de I es*:

$$\sqrt{I} = \{a \in A / a^n \in I, \text{ para algún } n \in \mathbf{Z}^+\}.$$

Demostración.

Supóngase $a \in A$ tal que $a^n \in I$ para algún entero positivo n. Si P es un ideal primo conteniendo a I, entonces $a^n \in P$, de aquí $a \in P$, Por tanto $a \in \sqrt{I}$.
De otro lado, razonemos por el absurdo, supóngase que $a \in A$ y para cualquier entero positivo n, $a^n \notin I$. El Teorema será probado si mostramos que existe un ideal primo P en A tal que $I \subset P$ y $a \notin P$. Sea $\vartheta = \{J / J \text{ ideal en } A,\ I \subset J,\ J \cap \{a, a^2, a^3, \ldots\} = \varnothing\}$, entonces ϑ es parcialmente ordenado por la inclusión de conjuntos y satisface la condición del Lema de Zorn. Así que ϑ tiene un elemento maximal P_0. Claramente $I \subset P_0$ y $a \notin P_0$. Demostraremos que P_0 es un ideal primo. Supóngase que b, c son elementos en A los cuales no pertencen a P_0. Como P_0 es maximal en ϑ, cada uno de los ideales $\langle b \rangle + P_0$ y $\langle c \rangle + P_0$ tienen una intersección no vacía con $\{a, a^2, a^3, \ldots\}$, luego $\langle bc \rangle + P_0 = [\langle b \rangle + P_0][\langle c \rangle + P_0]$ incluye a $\{a, a^2, a^3, \ldots\}$, por lo tanto $bc \notin P_0$ y así P_0 es el ideal primo deseado. (Note que no se usó la conmutividad de A en la demostración del teorema).■

Corolario 3.3. *El radical de un ideal primario es un ideal primo.*

Demostración.

Sea I un ideal primario, si $a.b \in \sqrt{I}$ tal que $a \notin \sqrt{I}$, donde $a,b \in A$, entonces existe un entero positivo n tal que $(a.b)^n = a^n b^n \in I$, y $a^n \notin I$, luego por ser I un ideal primario existe algún entero positivo m, $(b^n)^m = b^{nm} \in I$, entonces $b \in \sqrt{I}$. Así pues, $\sqrt{I}$ es un ideal primo.■

Proposición 3.2. *Sea A un anillo. Si I es un ideal de A tal que $\sqrt{I}$ es un ideal maximal de A, entonces I es un ideal primario de A.*

Demostración

La imagen de $\sqrt{I}$ en A/I es el nilradical de A/I, de aquí A/I tiene un único ideal primo, por la proposición 3.1. Así pues, cada elemento de A/I es una unidad ó nilpotente, y así cada divisor de cero en A/I es nilpotente. Así pues, por el Corolario 3.2. el ideal I es un ideal primario.■

Corolario 3.4. *Sean $I_1, I_2, ... I_n$ ideales primarios en un anillo. Si $\sqrt{I_1} = \sqrt{I_2} = ... = \sqrt{I_n} = P$, entonces $I = I_1 \cap I_2 \cap ... I_n$ es un ideal primario cuyo radical es P.*

Demostración

Si $a \in P$, entonces existen enteros positivos m_i tal que $a^{m_i} \in I_i$ para $i = 1, 2, ..., n$. Luego tomando $m = Max_i\{m_i\}$ se tiene que $a^m \in I$, entonces $a \in \sqrt{I}$. Así $P \subset \sqrt{I}$. Si $b \in \sqrt{I}$ entonces $b^m \in I$ para algún entero positivo m, luego $b^m \in I_i$, y $b \in P$, Así $\sqrt{I} \subset P$. Concluimos entonces que $P = \sqrt{I}$.
Si $a.b \in I$, $a \notin I$, existe algún entero positivo k tal que $a \notin I_k$, puesto que I_k es primario, $b^r \in I_k$ para algún entero positivo r. Luego $b \in P$ y como $P = \sqrt{I}$, $b^s \in I$ para algún entero positivo s, esto implica que $\sqrt{I}$ es un ideal primario.■

Definición 3.5 Sean I y J ideales de un anillo A, entonces: $[I : J] = \{a \in A \,/\, a.b \in I, \text{ para todo } b \in J\}$ es un ideal llamado el ***cociente residual*** de I por J. □

Note que $I \subset [I : J]$. En efecto, sea $a \in I$ entonces $a.b \in I$ para todo $b \in J$, luego $a \in [I : J]$.

Necesitamos el siguiente lema para probar que en un anillo Noetheriano cada ideal es una interseccion finita de ideales primarios.

Lema 3.1. *Sea A un anillo Noetheriano e I* un ideal de A *el cual no es primario. Entonces existen ideales B y C en A tal que $I \subsetneq B$, $I \subsetneq C$* e $I = B \cap C$.

Demostración.

Puesto que I no es un ideal primario existen elementos $b, c \in A$ tal que $b.c \in I$, $b \notin I$ y $c^k \notin I$ para cualquier entero positivo k. Sea $B = \langle b \rangle + I$, entonces B es un ideal en A el cual contiene a I propiamente.
Ahora si consideraremos los siguientes ideales $[I : \langle c \rangle], [I : \langle c^2 \rangle], [I : \langle c^3 \rangle], \ldots$ de A. Entonces la sucesión $[I : \langle c \rangle] \subset [I : \langle c^2 \rangle] \subset [I : \langle c^3 \rangle] \subset \ldots$ es ascendente. En efecto sea $a \in [I : \langle c^n \rangle]$ entonces $a.b \in I$ para todo $b \in \langle c^n \rangle$, de aquí $b \in \langle c^{n+1} \rangle$, luego $a \in [I : \langle c^{n+1} \rangle]$. Puesto que A es Noetheriano, existe un entero positivo n tal que: $[I : \langle c^n \rangle] = [I : \langle c^{n+1} \rangle] = [I : \langle c^{n+2} \rangle] = \ldots$ Sea $C = \langle c^n \rangle + I$, entonces C es un ideal en A el cual contiene a I propiamente. Demostremos que $I = B \cap C$. Es claro que $I \subset B \cap C$. Nos queda por probar que $B \cap C \subset I$. Sea $d \in B \cap C$, entonces existen $a_1, a_2 \in A$ y $e_1, e_2 \in I$ tal que $d = a_1.b + e_1 = a_2.c^n + e_2$. Claramente $d.c = a_1.b.c + e_1 c \in I$ y de $d.c = a_2.c^{n+1} + e_2 c$ se tiene que $a_2.c^{n+1} \in I$. Luego $a_2 \in [I : \langle c^{n+1} \rangle] = [I : \langle c^n \rangle]$, así $a_2.c^n \in I$ y $d = a_2.c^n + e_2 c \in I$. Concluimos entonces que $B \cap C = I$ ■

Teorema 3.2. *Cada ideal en un anillo Noetheriano A tiene una* ***descomposición primaria***: *Es decir, cada ideal en A es la intersección de un número finito de ideales primarios en A.*

Demostración.

Supóngase que no; Entonces sea S el conjunto de ideales en A que no son intersecciones finitas de ideales primarios.y $S \neq \varnothing$. Puesto que A es Noetheriano, entonces S contiene un elemento maximal I. Como $I \in S$, e I no es primario, entonces por el Lema 3.1 existen ideales B y C que contienen propiamente a I tal

que $I = B \cap C$. Puesto que I es maximal en S, entonces $B \notin S$ y $C \notin S$. Luego B y C son intersecciones finitas de ideales primarios, por tanto $I = B \cap C$. también lo sería, lo cual sería una contradicción. Así pues, $S = \varnothing$ y el teorema queda probado.■

En general, la descomposición de un ideal en una intersección de ideales primarios no es única. Por ejemplo hemos visto en el Corolario 3.4, que si I_1, I_2 son ideales primarios con $\sqrt{I_1} = \sqrt{I_2}$, entonces $I = I_1 \cap I_2$ es primario, así $I = I_3$ e $I = I_1 \cap I_2$ son dos descomposiciones primarias de I.

Definición 3.6 *Una descomposición primaria,* $I = \bigcap_{i=1}^{n} I_i$ *es* ***reducida*** *si* $\bigcap_{i \neq j} I_i \neq \bigcap_{i=1}^{n} I_i$ *para cada* $j = 1,2...,n$ *y* $\sqrt{I_r} \neq \sqrt{I_s}$ *para* $r \neq s$, $r,s = 1,2,...,n$. □

Definición 3.7 *Si* $I = \bigcap_{i=1}^{n} I_i$ *es un descomposicion primaria reducida de* I, *entonces* $\left\{\sqrt{I_i}\right\}_{i=1}^{n}$ *es el conjunto de* ***ideales primos asociados*** *a* I. □

Definición 3.8 *Sea* $\left\{\sqrt{I_i}\right\}_{i=1}^{n}$ *un conjunto de ideales primos asociados de un ideal* I. *Entonces* $\sqrt{I_r}$ $(1 \leqq r \leqq n)$ *es un* ***ideal primo aislado*** *de* I *si* $\sqrt{I_r} \not\supseteq \sqrt{I_i}$ *para* $i = 1,...,r-1,r+1,...n$. □

El término *aislado*, viene de la geometría algebraica.

Corolario 3.5 *Sea* A *un anillo e* I *un ideal de* A, *Si* $I \subset \bigcup_{i=1}^{m} P_i$ *donde los* P_i *son ideales primos en* A, *entonces* $I \subset P_k$ *para algún* k.

Demostración.

Supongamos que I no está incluido en ningún P_i (podemos asumir sin pérdida de generalidad que para $i \neq j$ $P_i \not\supseteq P_j$ de otro modo eliminamos P_j), entonces $I \cap \bigcap_{j=1, j \neq i}^{m} P_j$ no está incluido en P_i, $i = 1,2,...,m$. Para cada $i = 1,2,...,m$ sea a_i un elemento en A tal que $a_i \in I \cap \bigcap_{j=1, j \neq i}^{m} P_j$ y $a_i \notin P_i$, entonces $\sum_{i=1}^{m} a_i \notin P_i$ para $i = 1,2,...,m$, lo que implica que $\sum_{i=1}^{m} a_i \notin \bigcup_{i=1}^{m} P_i$. Lo cual sería una contradicción.■

Teorema 3.3. *Sea* A *un anillo Noetheriano e* I *un ideal de A. Sean* $I = \bigcap_{i=1}^{m} I_i$ *e*

$I = \bigcap_{j=1}^{n} I_j'$ *dos descomposiciones primarias reducidas de* I *. Entonces* $m = n$ *y* $\{\sqrt{I_i}\}_{i=1}^{m} = \{\sqrt{I_j'}\}_{j=1}^{n}$.

Demostración.

Sean $I = \bigcap_{i=1}^{m} I_i = \bigcap_{j=1}^{n} I_j'$ descomposiciones primarias reducidas de I y sea $P_i = \sqrt{I_i}$, $P_j' = \sqrt{I_j'}$ $(i = 1,2,...,m, j = 1,2,...,n)$. En el conjunto $\{P_i\}_{i=1}^{m} \cup \{P_j'\}_{j=1}^{n}$ existe un ideal el cual no está contenido propiamente en cualquiera de los otros ideales de este conjunto. Supongamos sin pérdida de generalidad que P_1 es tal ideal. Demostremos que $P_1 = P_j'$ para algún j. Supongamos lo contrario que $P_1 \neq P_j'$ para $j = 1,2,...,n$. Puesto que $P_1 \nsubseteq \bigcup_{i=2}^{m} P_i \cup \bigcup_{j=1}^{n} P_j'$, existe un elemento $a \in P_1$ tal que $a \notin \bigcup_{i=2}^{m} P_i \cup \bigcup_{j=1}^{n} P_j'$. Como $P_1 = \sqrt{I_1}$, entonces existe un entero positivo k tal que $a^k \in I_1$.

Afirmamos que $I : \langle a^k \rangle = I_2 \cap I_3 \cap ... \cap I_m$. En efecto, claramente $I_2 \cap I_3 \cap ... \cap I_m \subset [I : \langle a^k \rangle]$; y si $b \in A$, y $b \notin I_i$ para algún $i \geqq 2$, entonces (puesto que $a \notin P_i$) $a^k.b \notin I_i$, luego $b \notin [I : \langle a^k \rangle]$.

Con un argumento similar se demuestra que $[I : \langle a^k \rangle] = I'_1 \cap I'_2 \cap ... \cap I'_n$.

Luego $I_2 \cap I_3 \cap ... \cap I_m = I'_1 \cap I'_2 \cap ... \cap I'_n = I$. Esto contradice la suposición de que la descomposición primaria es reducida. Concluimos entonces que $P_1 \in \{P_j'\}_{j=1}^{n}$, digamos que $P_1 = P_1'$. Puesto que $P_1 = P_1'$ es maximal en el conjunto $\{P_i\}_{i=1}^{m} \cup \{P_j'\}_{j=1}^{n}$, existe algún $a \in P_1$ con $a \notin \bigcup_{i=2}^{m} P_i \cup \bigcup_{j=2}^{n} P_j'$ y así existe un entero $k \geqq 1$ tal que $a^k \in I_1$ y $a^k \in I_1'$.

Con un argumento similar se demuestra que:

$[I : \langle a^k \rangle] = I_2 \cap I_3 \cap ... \cap I_m = I'_2 \cap I'_3 \cap ... \cap I'_n$.

El teorema ahora se completa por inducción.■

El teorema 3.3 nos dice que los ideales primos asociados de un ideal I en un anillo Noetheriano están únicamente determinados. En general los ideales primarios en una descomposición primaria de I no son únicos. Además, si I es un ideal primario en una descomposición primaria de I tal que $\sqrt{I}$ es un ideal primo aislado de I, entonces I es únicamente determinado. entonces tenemos.

Teorema 3.4. *Sea I un ideal en un anillo Noetheriano A, y sea*

$I = \bigcap_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i'$ *una descomposición primaria reducida de* I *tal que* $\sqrt{I_1} = \sqrt{I_1'} = P_1$. Si P_1 *es un ideal primo aislado de* I, *entonces* $I_1 = I_1'$.

Demostración.

Puesto que P_1 es un ideal primo aislado de I, existe para cada $i = 2,3,...,n$ algún elemento $a_i \in \sqrt{I_i}$ con $a_i \notin P_1$. Sea $a = \prod_{i=2}^{n} a_i$. Entonces $a \in \sqrt{I_i}$ para cada $i = 2,3,...,n$ y $a \notin P_1$. Por el teorema 3.3 $\left\{\sqrt{I_i}\right\}_{i=1}^{n} = \left\{\sqrt{I_j'}\right\}_{j=1}^{n}$. Esto implica que existe un entero positivo k tal que $a^k \in I_i$ y $a^k \in I_j'$, $i,j = 2,3,...n$. Demostraremos que para cualquier k, $[I : \langle a^k \rangle] = I_1$ y $[I : \langle a^k \rangle] = I_1'$.

Si $b \in I_1$ ($b \in I_1'$), entonces $a^k.b \in I_1 \cap I_2 \cap ... \cap I_n$ ($a^k.b \in I_1' \cap I_2' \cap ... \cap I_n'$). De aquí $b \in [I : \langle a^k \rangle]$ y $I_1 \subset [I : \langle a^k \rangle]$ ($I_1' \subset [I : \langle a^k \rangle]$). Si $c \in [I : \langle a^k \rangle]$, entonces $a^k.c \in I$ y $a^k.c \in I_1$ ($a^k.c \in I_1'$). Esto implica que $c \in I_1$ ($c \in I_1'$), ya que si $c \notin I_1$ ($c \notin I_1'$), entonces $a \in P_1$; Pero por nuestra elección de a, tenemos que $a \notin P_1$. Concluimos entonces que $[I : \langle a^k \rangle] \subset I_1$ ($[I : \langle a^k \rangle] \subset I_1'$). Así pues, $[I : \langle a^k \rangle] = I_1 = I_1'$, y el teorema queda demostrado.■

4. ELEMENTOS ENTEROS

En las secciones previas nos hemos ocupado de anillos en los cuales cada ideal es finitamente generado. En esta sección estudiaremos aquellos elementos α de un anillo B para los cuales el subanillo $A[\alpha]$ de B generado por α y un subanillo fijo A de B es un A –módulo finitamente generado.

Definición 4.1. *Sea A un subanillo de un anillo conmutativo B.*

a. *Un elemento $\alpha \in B$ es* ***entero*** *sobre A si existe un polinomio mónico $f(x) \in A[x]$ tal que $f(\alpha) = 0$; Es decir, existe un conjunto $\{a_i\}_{i=1}^{n}$ de elementos de A tal que $\alpha^n + \sum_{i=1}^{n} a_i \alpha^{n-i} = 0$.*

b. *El anillo B se dice que es una* ***extensión integral*** *de A si cada elemento de B es entero sobre A.* □

La Definición 4.1.a. extiende la definición de los números enteros algebraicos.

Ejemplos 4.1.

a. Cada elemento de A es entero sobre A, pues para todo $a \in A$, a es raiz del polinomio $x - a$.

b. El elemento $-\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ del anillo $\mathbf{Q}[\sqrt{-3}]$, es entero sobre **Z**, pues es raíz del polinomio $x^3 - 1$.

c. Los elementos enteros del anillo de los números racionales **Q** sobre **Z** son solo los elementos de **Z**. En efecto, un número racional $r/s \in \mathbf{Q}$ donde r y s son primos relativos es entero sobre **Z**, si y solo si $(r/s)^n + a_{n-1}(r/s)^{n-1} + \ldots + a_0 = 0$ para algunos enteros a_i. Multiplicando por s^n deducimos que s divide a r^n, y de aquí $s = \pm 1$ y $r/s \in \mathbf{Z}$. Esto también significa que no se puede encontrar una extensión integral A de **Z** tal que $\mathbf{Z} \subset A \subset \mathbf{Q}$.

Teorema 4.1. *Sea A un subanillo de un anillo conmutativo B, y $\alpha \in B$. Las siguientes afirmaciones son equivalentes*:

a *α es entero sobre A.*

b *El subanillo $A[\alpha]$ de B generado por A y α es un A –módulo finitamente*

generado.

c *$A[\alpha]$ está contenido en un subanillo C de B, donde C es un A–módulo finitamente generado.*

d *B contiene un A–módulo finitamente generado M, tal que M contiene un elemento que no es divisor de cero en B y $\alpha M \subset M$.*

Demostración.

a.⇒**b.** Supongamos que α es entero sobre A. Entonces existen elementos $a_1, a_2, ..a_n$ en A tal que $\alpha^n = \sum_{i=1}^{n} a_i \alpha^{n-i}$. De aquí α^n está en un A–módulo generado por $1, \alpha, \alpha^2, ..., \alpha^{n-1}$. Por inducción se demuestra que $\alpha^{n+k} \in A + A\alpha + ... + A\alpha^{n-1}$ para cada entero positivo k. Puesto que cada elemento en $A[\alpha]$ se representa de la siguiente forma $\sum_{i=0}^{m} a_i \alpha^i$ ($a_i \in A$, $m \in \mathbf{Z}^+$). Concluimos que $A[\alpha]$ es un A–módulo, el cual es generado por $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ sobre A.

b.⇒**c.** Definiendo $C = A[\alpha]$.

c.⇒**d.** Supongamos que el punto **c.** se cumple. Definiendo $M = A[\alpha]$, se tiene que $1 \in M$ y 1 no es un divisor de cero, entonces M satisface las condiciones indicadas en el punto **d.** Puesto que M es un subanillo conteniendo a α, se tiene que $\alpha M \subset M$.

d.⇒**a.** Sea M un A–módulo finitamente generado contenido en B tal que M contiene un elemento el cual no es un divisor de cero y $\alpha M \subset M$. Sean $\{\beta_1, \beta_2, ..., \beta_n\}$ un conjunto de generadores de M como A–módulo, donde β_1 no es un divisor de cero. Puesto que $\alpha M \subset M$, existen elementos $a_{ij} \in A$ tal que $\alpha\beta_1 = \sum_{j=1}^{n} a_{ij}\beta_j$, $i = 1, 2, ..., n$. De aquí $\det(\alpha \mathrm{I} - (a_{ij}))\beta_k = 0$ ($k = 1, 2, ..., n$), donde I es la matriz identidad $n \times n$. Puesto que β_1 no es un divisor de cero, $\det(\alpha \mathrm{I} - (a_{ij})) = 0$. Luego α es una raiz del polinomio mónico $\det[\alpha I - (a_{ij})]$ con coeficientes en A. ■

Corolario 4.1. *Sea A un subanillo de un anillo conmutativo B. Si B es finitamente generado como A–módulo, entonces B es una extensión integral de A.*

Demostración.

Por el teorema anterior, cada elemento de B es entero sobre A por tanto B es un extensión integral de A.■

Ejemplos 4.2.

a. El anillo de los enteros gaussianos $\mathbf{Z}[i]$ es una extensión integral de **Z**, como también lo es $\mathbf{Z}[\sqrt{-5}]$, debido a que ambos son finitamente generados como módulos sobre **Z**.

b. Sea A un subanillo de un anillo B tal que B es finitamente generado como A –módulo. Así pues, si $B = \sum_{i=1}^{n} Aa_i$, entonces se puede demostrar que $B[x] = \sum_{i=1}^{n} A[x]a_i$, Es decir que el anillo de polinomios $B[x]$ es un extensión integral de $A[x]$.

Corolario 4.2. *Sea A un subanillo de un anillo B. Sean $\alpha_i \in B$ $(i = 1,2,...,n)$ enteros sobre A. Entonces $A[\alpha_1, \alpha_2, ...\alpha_n]$ (El subanillo generado por $A, \alpha_1, \alpha_2, ...\alpha_n$) es un A –módulo finitamente generado, y cada elemento de $A[\alpha_1, \alpha_2, ...\alpha_n]$ es entero sobre A.*

Demostración.

Por el teorema 4.1. el enunciado del corolario es válido para $n = 1$. Por inducción, supongamos que el enunciado es válido para $n < k$. Sean $\alpha_1, \alpha_2, ...\alpha_k$ elementos de B los cuales son enteros sobre A. Claramente, α_k es entero sobre $A[\alpha_1, \alpha_2, ...\alpha_{k-1}]$. De aquí $A[\alpha_1, \alpha_2, ..., \alpha_{k-1}][\alpha_k] = A[\alpha_1, \alpha_2, ..., \alpha_k]$ es un $A[\alpha_1, \alpha_2, ..., \alpha_{k-1}]$ –módulo finitamente generado. Por nuestra hipótesis de inducción, $A[\alpha_1, \alpha_2, ..., \alpha_{k-1}]$ es un A –módulo finitamente generado. Luego $A[\alpha_1, \alpha_2, ..., \alpha_k]$ es A –módulo finitamente generado. Si $\{\beta_i\}_{i=1}^{r}$ y $\{\alpha_j\}_{j=1}^{s}$ son conjuntos que generan $A[\alpha_1, \alpha_2, ..., \alpha_k]$ sobre $A[\alpha_1, \alpha_2, ..., \alpha_{k-1}]$ y $A[\alpha_1, \alpha_2, ..., \alpha_{k-1}]$ sobre A respectivamente, entonces $\{\beta_i \alpha_j\}_{i=1,2,...r, j=1,2...s}$ es un conjunto que genera a $A[\alpha_1, \alpha_2, ..., \alpha_k]$ sobre A. Del Teorema 4.1.**c**. concluimos que cada elemento de $A[\alpha_1, \alpha_2, ..., \alpha_k]$ es entero sobre A.■

Corolario 4.3 *Sea A un subanillo de un anillo B. Entonces*

$\bar{A} = \{\alpha \in B / \alpha$ *es entero sobre* $A\}$ *es subanillo de* B *conteniendo a* A.

Demostración

Es claro que $A \subset \bar{A}$, nos queda por probar que $\bar{A}$ es un subanillo de B. Sea $\alpha, \beta \in \bar{A}$, entonces existen $f(x), g(x) \in A[x]$ polinomios mónicos tal que $f(\alpha) = 0$ y $g(\beta) = 0$ de grado n y m respectivamente. Entonces como en la demostración del Teorema 4.1 el subanillo $A[\alpha, \beta]$ es generado como A –módulo por $\{\alpha^i \beta^j\}$, para $i = 0, 1, ..., n$ y $j = 0, 1, ..., m$. Puesto que $\alpha - \beta$ y $\alpha.\beta$ pertenecen a $A[\alpha, \beta]$, esto implica que ambos pertenecen a $\bar{A}$. Así pues, $\bar{A}$ es un subanillo de B.■

Definición 4.2. *Sea* A *un subanillo de un anillo conmutativo* B.

a. *Un subanillo* C *de* B *conteniendo a* A *es entero sobre* A *si cada elemento de* C *es entero sobre* A.

b. *El subanillo* $\bar{A}$ de B, *de todos los elementos enteros sobre* A, *es llamado* ***clausura integral*** *de* A *en* B.

c. *Si* $\bar{A} = A$, *entonces decimos que* A *es* ***integralmente cerrado*** *en* B. *Si* D *es un dominio entero el cual es integralmente cerrado en su campo de fracciones, entonces simplemente se dice que* D *es integralmente cerrado.* □

Ejemplos 4.3.

a. Del Ejemplo **4.1 c**. podemos concluir que **Z** es integralmente cerrado en **Q**.

b Cualquier Dominio de ideales principales es integralmente cerrado en su campo de fracciones.

c. Sea A un dominio gaussiano, entonces A es integralmente cerrado. Sea F el campo de fracciones de A. Supóngase que $a/b \in F$ es entero sobre A, donde $a, b \in A$. Sea $f \in A[x]$ un polinomio mónico de menor grado en el cual a/b es una raíz. Entonces en $F[x]$, $(x - a/b) \mid f$, Así pues, $f = x - a/b$ y $a/b \in A$.

Proposición 4.1 *Sea* A *un subanillo de un dominio entero* D, *y asumiendo que* D *es una extensión integral de* A. *Entonces* D *es un campo si y solo si* A *es un campo.*

Demostración.

⇒ Supongamos que A es un campo. Sea $u \in D$, $u \neq 0$, y sea $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ un polinomio mónico en $A[x]$ de menor grado en el conjunto de polinomios que tienen a u como una raíz. Entonces $u^n + a_{n-1}u^{n-1} + ... + a_1u + a_0 = 0$, y si $a_0 = 0$ entonces podríamos obtener un polinomio mónico aún de menor grado que n con u como raíz. Así pues, tenemos que $a_0 \neq 0$, y la ecuación $u(u^{n-1} + a_{n-1}u^{n-2} + ... + a_1) = -a_0$ muestra que u es inversible en D si y solo si a_0 es inversible en A. Puesto que A es supuesto como un campo, esto implica que D es un campo.

⇐ Recíprocamente, supongamos que D es un campo. Sea $a \in A$, $a \neq 0$. Entonces existe $a^{-1} \in D$, Puesto que D es entero sobre A existe un polinomio mónico $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ en $A[x]$, tal que $f(a^{-1}) = 0$. Así $(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + ... + a_1(a^{-1}) + a_0 = 0$, multiplicando por a^n obtenemos $1 + a_{n-1}a + ... + a_1a^{n-1} + a_0a^n = 0$. Esto muestra que $a^{-1} = -a_{n-1} - ... - a_0a^{n-1}$ pertenece a A. Así pues, A es un campo.■

Observaciones.

- De la proposición 4.1, podemos observar que **Q** no es una extensión integral de cualquiera de sus subanillos.

Corolario 4.4 *Sea A un subanillo de un anillo B y sea B un subanillo de un anillo C. Si B es entero sobre A y C es entero sobre B, entonces C es entero sobre A.*

Demostración.

Sea $\gamma \in C$, entonces existen elementos $\beta_1, \beta_2, ...\beta_n \in B$ tal que $\gamma^n + \sum_{i=1}^{n} \beta_i\gamma^{n-i} = 0$. Puesto $\beta_1, \beta_2, ...\beta_n$ son enteros sobre A, entonces por el corolario 4.2 $A[\beta_1, \beta_2, .., \beta_n]$ es un A–módulo finitamente generado. Pero $A[\beta_1, \beta_2, .., \beta_n, \gamma]$ es un $A[\beta_1, \beta_2, .., \beta_n]$–módulo finitamente generado, de aquí un A–módulo finitamente generado. Esto implica por el Teorema 4.1.c. que γ es entero sobre A. Concluimos entonces que C es entero sobre A.■

5. DOMINIOS DEDEKIND

La factorización única en primos puede fallar como observamos en el anillo $\mathbf{Z}[\sqrt{-5}]$ en la sección 4. Dedekind observó que en muchos casos se podría obtener una nueva clase de factorización única, es decir en ideales primos. En esta sección discutiremos dominios Dedekind, que son dominios enteros D, en el cual cada ideal de D es igual a un producto finito de ideales primos de D.

Dedekind propuso la siguiente idea: Cuando se trabaja con los enteros ordinarios, muchas de las definiciones acerca de números pueden ser trasladados a las definiciones de los ideales principales que ellos generan. Así por ejemplo $6 = 2.3$ es equivalente a $\langle 6\rangle = \langle 2\rangle.\langle 3\rangle$ y $2 \mid 6$ es equivalente a $\langle 6\rangle \subset \langle 2\rangle$. Estas equivalencias son válidas en cualquier dominio entero. Recalcamos nuevamente: La idea de Dedekind fue estudiar ideales en vez de números.

Si D es un dominio de ideales principales, entonces cualquier ideal I distinto de cero en D tiene la forma $I = a.D = \langle a\rangle$ para algún $a \in D$, $a \neq 0$, como $a = p_1p_2...p_n$ donde $p_1, p_2, ..., p_n \in D$ son elementos irreducibles, entonces I es un producto de ideales primos, puesto que $\langle a\rangle = \prod_{i=1}^{n}\langle p_i\rangle = \prod_{i=1}^{n} p_i.D$. Así pues cada DIP es un dominio Dedekind, lo reciproco no siempre es cierto, como por ejemplo $\mathbf{Z}[\sqrt{-5}]$.

En esta sección demostraremos que un dominio Dedekind tiene algunas propiedades de un dominio de ideales principales. Específicamente que un dominio Dedekind debe ser un dominio Noetheriano y cualquier ideal primo distinto de cero de un dominio Dedekind debe ser maximal.

Definición 5.1. *Un domino entero D es un **Dominio Dedekind** si cada ideal propio de D es igual a un producto finito de ideales primos de D.* □

Demostraremos algunos resultados previos para dominios Dedekind usando la noción de la "inversa" de un ideal.

Definición 5.2. *Sea D un dominio entero con su campo de fracciones $F(F \supset D)$. Un **ideal fraccionario** de D es un D –submódulo I de F distinto de cero,*

tal que existe un elemento $a \in D, a \neq 0$, *con* $a.I \subseteq D$. □

Definición 5.3. *Sea* D *un dominio entero con su campo de fracciones* F. *Sea* I *es un ideal fraccionario de* D, *entonces su* ***inversa*** *se define como*:

$$I^{-1} = \{a \in F / a.I \subseteq D\}.$$ □

Definición 5.4. *Sea* D *un dominio entero con su campo de fracciones* F. *Sea* I *es un ideal fraccionario de* D, *entonces* I *es un* ***ideal inversible*** *si* $I.I^{-1} = D$. □

Corolario 5.1 Sea D un dominio entero *con su campo de fracciones* F.

a. *El conjunto de ideales fraccionarios de* D *es cerrrado bajo la adición, multiplicación e intersección, donde la multiplicación se define como*: $I_1 I_2 = \left\{\sum_{i=1}^{n} a_i b_i / a_i \in I_1,\ b_i \in I_2,\ n \in \mathbf{Z}^+\right\}$.

b. *Si* I *es un ideal fraccionario de* D, *entonces también lo es* $I^{-1} = \{a \in F / a.I \in D\}$.

c. *Para cada ideal fraccionario* I *de* D, $I.I^{-1} \subset D$.

d. *El conjunto de ideales fracionarios de* D *es un grupo bajo la multiplicación si y solo si cada ideal fraccionario de* D *es inversible*.

Ejemplo 5.1.

a. En el dominio entero **Z** con su campo de fracciones **Q**, el conjunto $I = \frac{1}{2}\mathbf{Z}$ que son todos los multiplos de $\frac{1}{2}$ es un ideal fraccionario de **Z**. Además este es un ideal fraccionario inversible, pues su inversa es $I^{-1} = 2\mathbf{Z}$.

b. Cada ideal principal distinto de cero $\langle a \rangle$ de un dominio entero D es inversible, su inversa es $D.\ 1/a = \langle 1/a \rangle$.

c. Sean I, J ideales fraccionarios de D, entonces $I.J$ también es un ideal fraccionario de D.

d. Sean I, J ideales fraccionarios de D, el cociente fraccionario se define como: $[I : J] = \left\{a \in F / aJ \subseteq I\right\}$, es claro que $[D : I] = I^{-1}$ y que en general $[I : J]$ es un ideal fraccionario de D. En efecto, sean $x, z \in [I : J]$, entonces $xJ \subseteq I$ y $zJ \subseteq I$, de donde $(x+z)J \subseteq xJ + zJ \subseteq I$; sea $d \in D$, entonces $dxJ \subseteq dI \subseteq I$, es

decir, $[I : J]$ es un submódulo de F. Sea $0 \neq d \in D$ tal que $dI \subseteq D$ y $a = t/s \neq 0$ en J, entonces $sa = t \in J \cap D$, luego para $x \in [I : J]$ se tiene que $xJ \subseteq I$ y $xt \in I$, de donde $tdx \in dI \subseteq D$. Sea $s = td \in D \setminus \{0\}$, entonces d es tal que $tdx \in D$ para cada $x \in [I : J]$, es decir, $td[I : J] \subseteq D$.

Lema 5.1. *Un ideal inversible de un dominio entero es finitamente generado.*

Demostración.

Sea I un ideal inversible de un dominio entero D. Entonces $I.I^{-1} = D$. Puesto que $1 \in D$, existe $b_i \in I^{-1}$, $a_i \in I$, $i = 1,2,...,n$. tal que $1 = \sum_{i=1}^{n} b_i.a_i$. Concluimos entonces que $I = \langle a_1, a_2, ..., a_n \rangle$. En efecto, para $a \in I$, $a = a.1 = \sum_{i=1}^{n} (a.b_i).a_i$, con $a.b_i \in D$.■

Lema 5.2. *Sea $\{I_i\}_{i=1}^{n}$ una familia finita de ideales de un dominio entero D. Si $\prod_{i=1}^{n} I_i$ es inversible, entonces también lo es I_i, para cada $i = 1,2,...,n$.*

Demostración.

Sea J un ideal fraccionario tal que $J.\prod_{i=1}^{n} I_i = D$. Entonces, para cada $i = 1,2,...,n$, $I_i(J.\prod_{j=1, j\neq i}^{n} I_j) = D$, de aquí I_i es inversible.■

Lema 5.3. *Sea I un ideal de un dominio entero D. y sean $I = \prod_{i=1}^{m} P_i$ e $I = \prod_{j=1}^{n} Q_j$ factorizaciones de I en producto de ideales primos de D, con $P_1, P_2, ..., P_n$ inversibles. Entonces $m = n$ y $P_i = Q_i$, para $i = 1,2,...,n$.*

Demostración.

La demostración es por inducción sobre m. Para el caso $m = 1$ es claro. Supongamos que el Lema es cierto si $m < r$. Supóngase que $I = \prod_{i=1}^{r} P_i = \prod_{j=1}^{n} Q_j$. De la familia $\{P_i\}_{i=1}^{r}$ elegimos un ideal P_1, el cual no contiene propiamente a ninguno de los otros ideales pertenecientes a la familia. Claramente $\prod_{j=1}^{n} Q_j \subset P_1$. De aquí algún Q_j, digamos Q_1, está contenido en el ideal P_1. Puesto que $\prod_{i=1}^{r} P_i \subset Q_1$, existe algún P_i, digamos P_2 tal que $P_2 \subset Q_1$. Luego $P_2 \subset Q_1 \subset P_1$ y, puesto que P_1 es minimal, $Q_1 = P_1$.

Concluimos entonces que $\prod_{i=2}^{r} P_i = P_1^{-1} \prod_{i=1}^{r} P_i = Q_1^{-1} \prod_{j=1}^{n} Q_j = \prod_{j=2}^{n} Q_j$.
Con un argumento similar se completa la demostración por inducción.■

Lema 5.4. *Sea D un dominio Dedekind. Entonces cada ideal primo propio de D es maximal e inversible.*

Demostración.

Demostraremos que cada ideal primo propio de D es maximal. Sea P un ideal primo propio de D, y sea $a \in D - P$. Denotamos por $\langle P, a \rangle$ y $\langle P, a^2 \rangle$ los ideales de D generados por P y a, y por P y a^2, respectivamente. Puesto que D es un dominio Dedekind, existen ideales primos $P_1, P_2, ..., P_m$ y $Q_1, Q_2, ..., Q_n$ de D tal que $\langle P, a \rangle = \prod_{i=1}^{m} P_i$ y $\langle P, a^2 \rangle = \prod_{i=1}^{n} Q_i$. Note que $P_i \supset P$ y $Q_j \supset P$ $(i = 1, 2, ..., m;$ $j = 1, 2, ..., n)$. Sea v el epimorfismo canónico de D sobre D/P. Entonces $\langle va \rangle = \prod_{i=1}^{m} vP_i$ y $\langle va^2 \rangle = \prod_{j=1}^{n} vQ_j = \langle va \rangle^2 = \prod_{i=1}^{m} [vP_i]^2$. Puesto que los ideales principales $\langle P, a \rangle$ y $\langle P, a^2 \rangle$ son inversibles, cada uno de los ideales vP_i y vQ_i son inversibles por el Lema 5.2. Luego por Lema 5.3. $2m = n$ y renumerando $vQ_{2i} = vQ_{2i-1} = vP_i$ $(i = 1, 2, ..., m)$. Luego $Q_{2i} = Q_{2i-1} = P_i$ para cada $i = 1, 2, ..., m$, y $\langle P, a^2 \rangle = \langle P, a \rangle^2$. De aquí $P \subset \langle P, a^2 \rangle = \langle P, a \rangle^2 = \langle P^2, a \rangle$ y cada elemento de P es la suma de un elemento de P^2 y un elemento de la forma da $(d \in D)$. Si $b = c + da \in P$ $(c \in P^2, d \in D)$, entonces $da \in P$. Puesto que $a \notin P$ y P es un ideal primo, $d \in P$, Esto implica que $P \subset \langle P^2, Pa \rangle \subset P$. Luego $P = \langle P^2, Pa \rangle = P.\langle P.a \rangle$. Puesto que P es por hipótesis es inversible, concluimos que $\langle P, a \rangle = P^{-1}.P = D$. Puesto que a fue un elemento arbitrario de D, que no está en P, implica que P es un ideal maximal.
Demostraremos ahora que cada ideal primo propio de D es inversible. Sea P un ideal primo propio de D. y sea $b \neq 0$ un elemento de P. Entonces existen ideales primos P_i $(i = 1, 2, ..., m)$ tales que $\langle b \rangle = \prod_{i=1}^{m} P_i \subset P$. Note que P contiene al menos a uno de los P_i digamos P_1. Puesto que $\langle b \rangle$ es inversible, lo es también P_1 por el Lema 5.2. Puesto que P_1 es un ideal primo e inversible entonces P_1 es maximal. Luego $P = P_1$ y así P es inversible.■

Teorema 5.1. *Las siguientes condiciones se cumplen para cualquier Dominio Dedekind D:*

a. *Cada ideal distinto de cero de D es inversible.*

b. *Cada ideal propio de D puede ser escrito en forma única (salvo el orden) como un producto finito de ideales primos de D.*

c. *D es un Dominio Noetheriano.*

d. *Cada ideal primo distinto de cero de D es maximal.*

Demostración.

a. Puesto que cada ideal distinto de cero de D es un producto finito de ideales primos, es suficiente probar que cada ideal primo distinto de cero es inversible. Sea P un ideal primo distinto de cero de D, y sea p un elemento distinto de cero de P. Entonces $pD = P_1P_2...P_n$ donde los P_i son ideales primos, y cada uno de estos ideales primos es inversible puesto que pD es inversible. Puesto que P es un ideal primo y $P_1P_2...P_n \subseteq P$, entonces $P_i \subseteq P$ para algún i. Por el Lema 5.4. P_i es maximal, entonces $P_i = P$. Así pues, P es inversible.

b. Se verifica por el Lema 5.3.

c. Se verifica por el Lema 5.1.

d. Se verifica por el Lema 5.4 ■

Teorema 5.2. *Sea D un dominio entero con su campo de fracciones F. Supongamos que D es Noetheriano y que cualquier ideal primo distinto de cero de D es maximal. Entonces para cualquier ideal propio distinto de cero I de D existe $q \in F \setminus D$ con $qI \subseteq D$.*

Demostración.

Sea I un ideal propio distinto de cero de D. Si I es un ideal principal, $I = aD$, entonces $a^{-1} \in F \setminus D$ y $a^{-1}I \subseteq D$. Supongamos que I no es un ideal principal. Sea a cualquier elemento distinto de cero de D, y sea P un ideal maximal de D con $I \subseteq P$. Por el Lema 2.1 existen ideales primos distintos de cero $P_1, P_2, ..., P_n$ de D con $P_1P_2...P_n \subseteq aD$, y al menos uno de estos ideales debe estar contenido en P, digamos $P_1 \subseteq P$, puesto que P es un ideal primo. Por hipótesis, cada ideal primo distinto de cero de D es maximal, esto implica que $P_1 = P$. Así tenemos

$PP_2...P_n \subseteq aD \subset I \subseteq P \subset D$,

y al omitir inneceriamente ideales primos, podemos asumir que $P_2...P_n$ no está

contenido en aD. Si elegimos un elemento $b \in P_2...P_n \setminus aD$, entonces $a^{-1}b \notin D$, puesto que $b \notin aD$. Tenemos

$^{-1}bI \subseteq a^{-1}bP \subseteq a^{-1}PP_2...P_n \subseteq a^{-1}aD = D$,

y esto completa la demostración.■

Teorema 5.3. *Sea D un dominio entero. Las siguientes afirmaciones son equivalentes*:

a. *D es un dominio Dedekind.*

b. *D es Noetheriano, integralmente cerrado en su campo de fracciones y cada ideal primo distinto de cero de D es maximal*

Demostración.

a.⇒**b**. Supongamos que D es un dominio Dedekind con su campo de fracciones F. Entonces por el teorema 5.1 D es Noetheriano, y cada ideal primo distinto de cero de D es maximal. Para mostrar que D es integralmente cerrado en F, sea $u \in F$ un elemento entero sobre D, y supongamos que u es una raíz de un polinomio mónico $f(x)$ en $D[x]$ de grado n. Sea I el $D-$*submódul o* de F generado por $\{1, u, ..., u^{n-1}\}$. Esto implica que la relación dada por $f(x)$, I contiene todas las potencias de u, y además $I^2 \subseteq I$. Puesto que I es un $D-$*submódul o*finitamente generado de F, este es un ideal fraccionario, el cual también debe ser inversible puesto que D es un dominio Dedekind. Esto implica que $I \subseteq D$, y así $u \in D$.

b.⇒**a**. Recíprocamente supongamos que D es Noetheriano, integralmente cerrado, y que cada ideal primo distinto de cero de D es maximal. Sea I cualquier ideal de D, y supóngase que $I^{-1}.I$ está contenido propiamente en D. Entonces $I^{-1}.I$ es un ideal de D, esto implica que por el Teorema 5.2 existe $u \in F \setminus D$ con $u(I^{-1}.I) \subseteq D$. Para cualquier elemento $q \in I^{-1}$, y cualquier $a \in I$, tenemos $(uq)a = u(qa) \in u(I^{-1}.I) \subseteq D$, y esto demuestra que $uq \in I^{-1}$, así $uI^{-1} \subseteq I^{-1}$. Debido a que D es Noetheriano, el ideal I es finitamente generado, y si d es el producto de estos generadores, entonces $dI^{-1} \subseteq D$, demostrando que I^{-1} es un ideal fraccionario. Además, dI^{-1} es un ideal de D, así que este también es finitamente generado, digamos $dI^{-1} = \sum_{i=1}^{n} Da_i$. Se puede verificar que $I^{-1} = \sum_{i=1}^{n} Da_i d^{-1}$. Así I^{-1} es un $D[u]-$*submódul o*sin divisores de cero de F que es finitamente generado como un $D-$*módul o*, luego u es entero sobre

D. Puesto que D es integralmente cerrado, esto implica que $u \in D$, en contradicción con la elección de u. Concluimos que $I^{-1}.I$ no está contenido propiamente en D, luego $I^{-1}.I = D$, y así I es inversible.■

6. ANOTACIONES Y EJEMPLOS.

Definición 6.1. *Sea* $d \in \mathbf{Z}$, $d \neq 0, \neq 1$ *un entero cuadrado libre* (*es decir*, $p^2 \nmid d$ *para cualquier* p *primo*), *entonces el conjunto*

$$\mathbf{Q}[\sqrt{d}\,] = \{a + b\sqrt{d} \,/\, a, b \in \mathbf{Q}\}$$

se llama ***campo cuadrático***, *donde la suma y la multiplicación se definen del siguiente modo*:

$$(a + b\sqrt{d}) + (a' + b'\sqrt{d}) = (a + a') + (b + b')\sqrt{d}$$
$$(a + b\sqrt{d}).(a' + b'\sqrt{d}) = (a.a' + b.b'd) + (a.b' + a'.b)\sqrt{d} \quad \square$$

Observaciones.

- El campo cuadrático $\mathbf{Q}[\sqrt{d}\,]$ es un aniilo con unidad con respecto a la suma y producto de números complejos **C**.
- El conjunto $\mathbf{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \,/\, a, b \in \mathbf{Z}\}$ es un subanillo contenido en $\mathbf{Q}[\sqrt{d}\,]$.
- El anillo $\mathbf{Z}[\sqrt{d}\,]$ es un dominio entero.

Determinación de la clausura integral de Z en $\mathbf{Q}[\sqrt{d}\,]$

Supóngase que $a + b\sqrt{d} \in \mathbf{Q}[\sqrt{d}\,]$ es entero sobre **Z**.

Si $d \equiv 1 (\text{mod } 4)$, entonces el polinomio mónico irreducible de $(1 + \sqrt{d})/2$ sobre **Q** es $x^2 - x + (1 - d)/4 \in \mathbf{Z}[x]$, así $(1 + \sqrt{d})/2$ es entero sobre.**Z**

La clausura integral de **Z** en $\mathbf{Q}[\sqrt{d}\,]$ contiene al subanillo $\mathbf{Z}[\sqrt{d}\,]$.

Un elemento $a + b\sqrt{d} \in \mathbf{Q}[\sqrt{d}\,]$ donde $a, b \in \mathbf{Z}$, es entero sobre **Z**, si $x^2 - 2a.x + (a^2 - d.b^2) \in \mathbf{Z}[x]$, Si $a = (2k + 1)/2$ para cualquier entero k, entonces $a^2 - d.b^2 \in \mathbf{Z}$ si y solo si $b = (2l + 1)/2$ donde l es un entero y $(2k + 1)^2 + d(2l + 1)^2$ es divisible por 4. Lo cual equivale a decir que d es un residuo cuadrático $(\text{mod } 4)$. Es decir $d \equiv 1 (\text{mod } 4)$. Así pues, si $d \equiv 1 (\text{mod } 4)$ entonces cada elemento $(2k + 1)/2 + (2l + 1)\sqrt{d}$ es entero sobre.

Así los elementos enteros de $\mathbf{Q}[\sqrt{d}\,]$ sobre **Z** son iguales a:

$\mathbf{Z}[\sqrt{d}\,]$ si $d \equiv 2, 3 (\text{mod } 4)$

$\mathbf{Z}[(1 + \sqrt{d})/2]$ si $d \equiv 1 (\text{mod } 4)$ ■

Algunos resultados del anillo: $\mathbf{Z}[\sqrt{-5}]$.

i. Los elementos $2, 3, 1 \pm \sqrt{-5}$ son elementos primos de $\mathbf{Z}[\sqrt{-5}]$.

ii Los ideales $\langle 2, 1+\sqrt{-5} \rangle$, $\langle 3, 1+\sqrt{-5} \rangle$, $\langle 3, 1-\sqrt{-5} \rangle$ son maximales.

iii. El ideal $\langle 3, 4+\sqrt{-5} \rangle$ es un ideal primo, pero no es un ideal principal.

iv. Como $6 = 2.3 = (1+\sqrt{-5}).(1-\sqrt{-5})$, entonces $\mathbf{Z}[\sqrt{-5}]$ no es un dominio de factorización única.

v. El ideal $\langle 3 \rangle = \langle 3, 4+\sqrt{-5} \rangle . \langle 3, 4-\sqrt{-5} \rangle$ es la factorización en producto de ideales primos.

vi. El ideal $I = \langle 3, 1+\sqrt{-5} \rangle$ generado sobre $\mathbf{Z}[\sqrt{-5}]$ por 3 y $1+\sqrt{-5}$ es inversible, cuya inversa es $I^{-1} = \langle 1, (1-\sqrt{-5})/3 \rangle$

vii. El anillo $\mathbf{Z}[\sqrt{-5}]$ es Noetheriano. En efecto, definiendo el siguiente homomorfismo : $f : \mathbf{Z}[x] \to \mathbf{C}$ por $p(x) \mapsto p(\sqrt{-5})$, se tiene que $\mathrm{Im}(f) = \mathbf{Z}[\sqrt{-5}] \cong \mathbf{Z}[x]/Ker(f) = \mathbf{Z}[x]/\langle x^2+5 \rangle$. Como $\mathbf{Z}$ es Noetheriano entonces $\mathbf{Z}[x]$ es Noetheriano, luego $\mathbf{Z}[x]/\langle x^2+5 \rangle$ también lo es. Así pues, $\mathbf{Z}[\sqrt{-5}]$ Noetheriano.

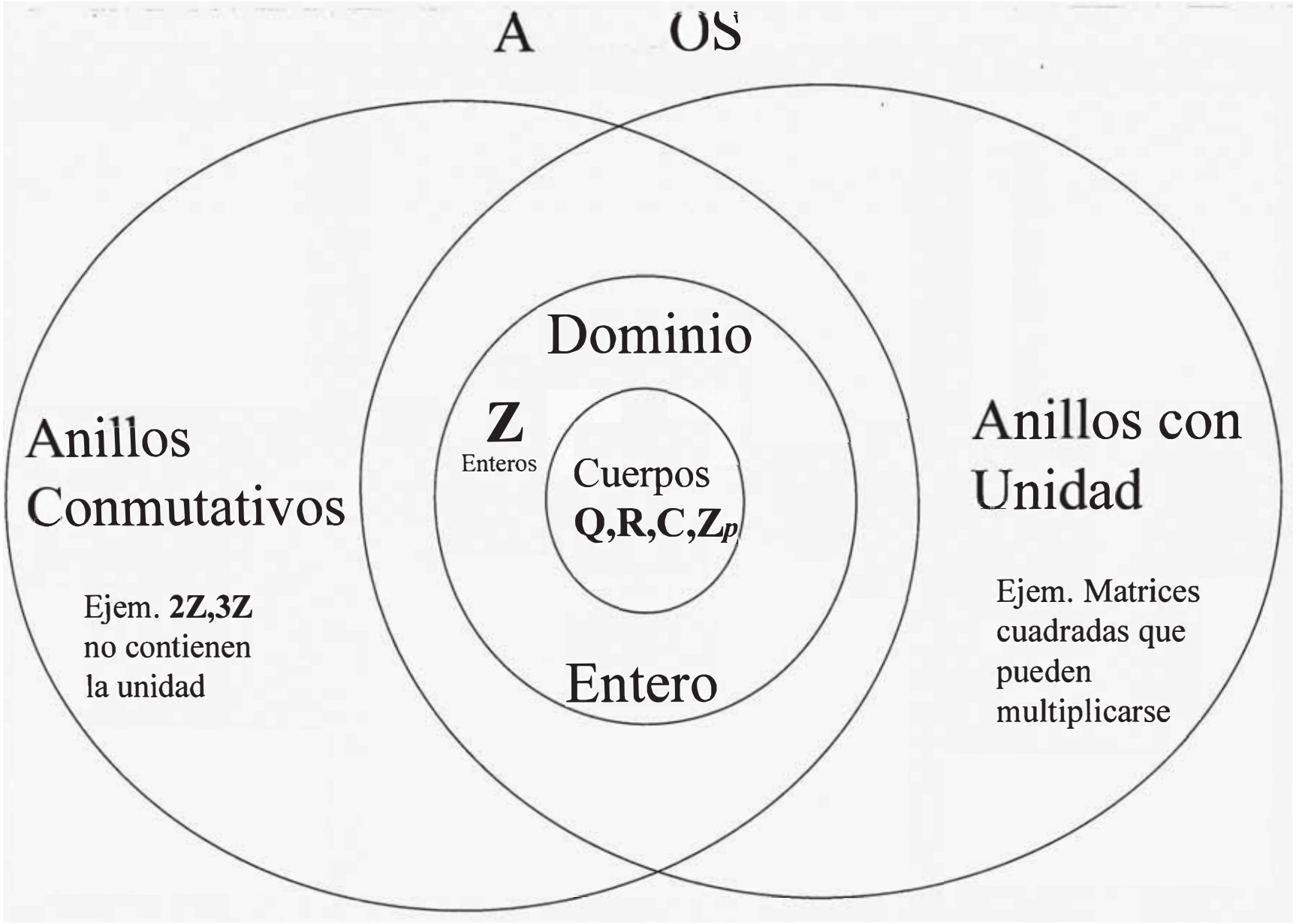
viii. $\mathbf{Z}[\sqrt{-5}]$ es la clausura integral de $\mathbf{Z}$ en $\mathbf{Q}[\sqrt{-5}]$ pues $-5 \equiv 1 (\mathrm{mod}.4)$

ix. Aplicando el teorema 5.3. $\mathbf{Z}[\sqrt{-5}]$ es un dominio Dedekind.

Notas Históricas.

El término “anillo” se debe a Dieudonné. El eligió esta palabra por el simple hecho de que un anillo esta ausente la división, lo que es un defecto como un anillo tiene un hoyo.

El término “álgebra” viene de la palabra árabe “Al-jabr”, se debe Khwarizmi, cuyo nombre completo es Abu Abd-Allah ibn Musa alKhwarizmi, nacido alrededor de 790AC en Baghdad.



Anillo conmutativo
Un anillo en el que la multiplicación es conmutativa

Anillo con unidad
Un anillo con la unidad multiplicativa

Unitario
Cualquier elemento de un anillo el cual tiene un inverso multiplicativo

1
lo que usualmente pensamos como 1

Dominio Entero
Anillo conmutativo con unidad que no contiene divisores de cero

Campo
Anillo conmutativo con unidad tal que cada elemento no cero tiene inverso multiplicativo

Anillo de división
Un anillo en el cual cada tiene elementos unitarios (ejem. Z_n)

7. DATOS BIOGRAFICOS

Richard Dedekind (1831-1916)

Nació en Braunschweig (Alemania). Su padre era abogado y su profesor de leyes en el colegio Carolinum de Braunschweig. Años más tarde Richard fue profesor de este colegio.

Dedekind permaneció soltero toda su vida, viviendo con su hermana Julie (novelista famosa), en su pueblo natal.

En 1850 entró en la universidad de Gotinga. Fueron profesores de Dedekind, Wilhelm Weber (famoso físico) y Gauss.

En 1858 fue nombrado profesor ayudante del politécnico de Zurich, por consejo de Weirstrass.

Dedekind fue uno de los mas grandes matemáticos de su tiempo, a pesar de que permaneció la mayor parte de su vida como profesor de secundaria. Se cree que Dedekind no quería salir de su pueblo, fue amigo de Cantor.

Murió en 1916 a los 85 años. Una publicación matemática le dió por muerto en 1899, lo que parece que le divirtió mucho. Dedekind trabajó en teoría de números.

Emmy Amalie Noether (1882-1935)

Nació en 1882 en Erlangen (Alemania). Su padre era profesor de matemáticas en Erlangen.

Estudió francés e inglés y aunque obtuvo el título de profesora de idiomas no llegó a ejercer en estas materias.

Se dice que ha sido la matemática mas grande de la historia de las matemáticas. Tuvo que vencer muchas dificultades para estudiar matemáticas, porque en ese tiempo a las mujeres no se les permitía estudiar, oficialmente, en las universidades alemanas. Cuando se doctoró en la universidad de Erlangen (1898) el senado académico declaró que la admisión de mujeres estudiantes "subvertía todo el orden académico". En 1915 Hilbert y Klein invitaron a Noether a volver a Gottingen y lucharon contra las autoridades universitarias para habilitar como profesora a Noether. No lo consiguieron hasta 1919. Es famosa por sus trabajos sobre la teoría de ideales. En 1921 publicó un artículo (Ideal Theory in Ring Bereichen) sobre teoría de anillos tan importante que, desde entonces, se llaman anillos

noetherianos a una determinada clase de anillos. En 1913 los nazis, provocaron su expulsión de Gottingen, porque era judía. se fue a USA. y murió en Pennsylvania, USA en 1935.

8. REFERENCIAS

[by Jacob K. Goldhaber and Gertrude Ehrlich] *Algebra*, *University of Maryland*

[M.A. Farinati A.L. Solotar] *Anillos y sus categorías de representaciones*, 26 *de Marzo* 2002.

[John A. Beachy] *Introductory Lectures on Ring and Modules*: *Suplement*, *Northern Illinois University* 1,999.

[M.F. Atiyah, I.G. MacDonald] *Introduction to Commutative Algebra*, *University of Oxford.*

[Francisco Cesar Polcino Milies] *Anéis e Módulos*, *Da Universidade de Sao Paulo*.

Links

http://www.math.niu.edu/~beachy/aaol/commutative.html

http://www.math.ksu.edu/~dbski/book.pdf

http://www.us.es/da/programas/progestructuras.html

http://d5.dir.dcx.yahoo.com/science/mathematics/algebra/

http://www.math.nmsu.edu/~pmorandi/math601f01/dedekinddomains.pdf

http://correio.cc.fc.ul.pt/~candre/numeros/Cap5.pdf

http://www.planetmath.org/

http://mathworld.wolfram.com/

http://dae.um.es:8019/docs/Matematicas.htm

http://www.math.hawaii.edu/~lee/book/

http://www.virtual.unal.edu.co/cursos/ciencias/15930/index.html.

UNIVERSIDAD NACIONAL DE INGENIERÍA
Facultad de Ciencias

ACTA DE SUSTENTACIÓN DEL INFORME DE SUFICIENCIA PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN MATEMÁTICA

Nombre: VILCA TOMAYLLA, EFRAIN

Título:

INTRODUCCION A LA TEORIA DE LOS ANILLOS CONMUTATIVOS

Miembros del Jurado:

Decano o su representante:

F. ESCALANTE _____ (firma)

Profesor Asesor:

G. Gómez _____ (firma)

Profesor Especialista:

Luis Gómez Sánchez A. _____ (firma)

Luego de sustentado el Informe de Suficiencia y absueltas las preguntas, el Jurado otorgó el calificativo de:

APROBADO

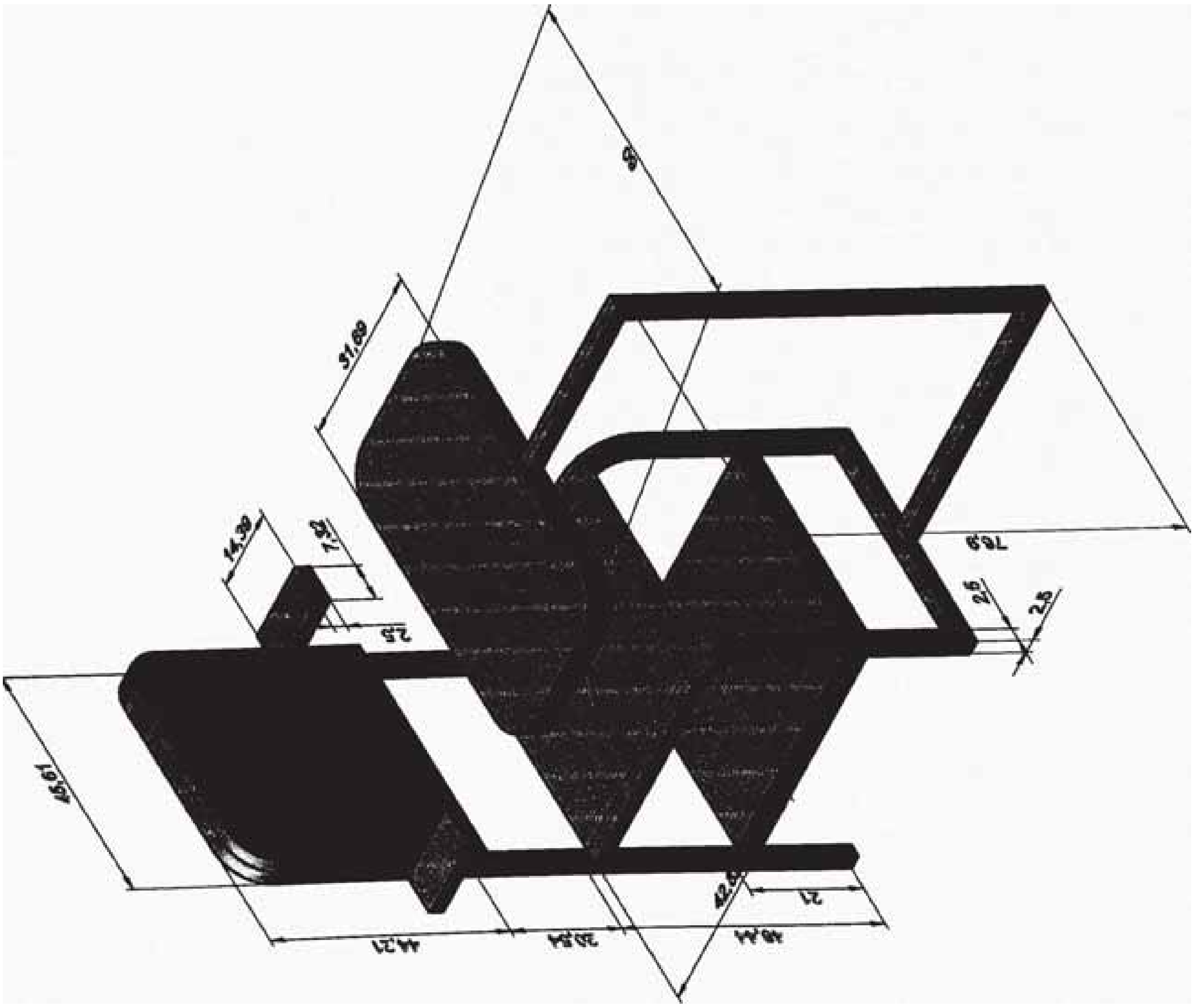
tal como consta en el Libro de Actas N° 208-408, Folio N° 341

Dado en la ciudad de Lima en la fecha: 19/01/03 a horas: 12.400

UNIVERSIDAD NACIONAL DE INGENIERIA FACULTAD DE CIENCIAS DECANO

Decano

Director de la Escuela Profesional


80
31,60
14,30
7,92
2,5
76,9
2,6
2,5
45,61
21
42,0
44,21
20,54
48,44

RESUMEN

La flotación de minerales es un proceso físico-químico el cual es realizado tanto en laboratorios como en plantas metalúrgicas, en dicho proceso intervienen variables las cuales afectan el proceso de recuperación cobre, es en ese sentido que algunas variables presentan mayor grado de afectación en la recuperaciones y leyes.

La presente tesis plantea establecer mediante modelos matemáticos y el software Minitab 17.0 a aquellas variables que presenten mayor grado de afectación en el proceso de recuperación de cobre y asimismo establecer las condiciones óptimas de las variables más representativas que maximicen el proceso de recuperación.

El desarrollo de este proceso plantea utilizar herramientas estadísticas que validen los modelos matemáticos, así como los diseños factoriales y Hexagonales para el desarrollo del diseño de Experimentos.

En la etapa de screening, la granulometría y espumante, fueron los más significativos, mientras que en la etapa de escalamiento, se identificó los niveles de máxima recuperación de cobre y finalmente en la etapa de optimización final, mostro una recuperación máxima de 80.75 % de Cu, demostrando así que para este tipo de mineral es posible incrementar la recuperación en más del 3.0 %.

ABSTRACT

Mineral flotation is a physical-chemical process, which is carried out in both laboratories and metallurgical plants, in the process-involved variables, which affect the process of copper recovery, is in the sense that some variables have a higher degree of involvement in the recoveries and laws.

This thesis presents set using mathematical models and software Minitab 17.0 for those variables that present greater involvement in the process of recovery of copper and establish the optimal conditions of the most representative variables that maximize the recovery process.

The development of this process poses to use statistical tools to validate the mathematical models and factorial designs and development Hexagonal Design of Experiments.

In the step of screening, particle size and foaming were the most significant, while in the scaling step, levels high copper recovery was identified and finally in the stage of final optimization, showed a maximum recovery of 80.75% of Cu, demonstrating that for this type of mineral is possible to increase recovery in most 3.0%

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABLAS