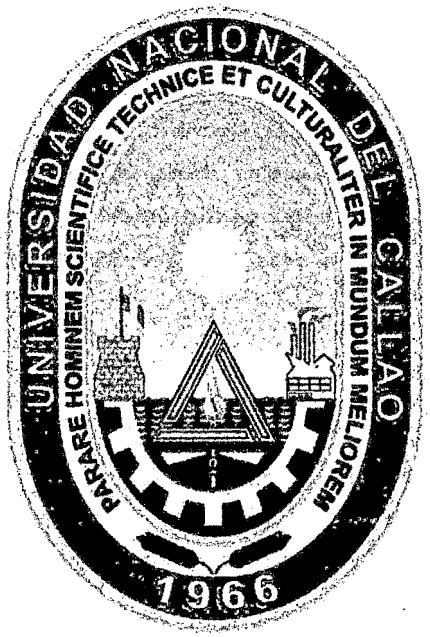
UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

ESCUELA PROFESIONAL DE MATEMÁTICA



UNA CARACTERIZACIÓN DE LOS DOMINIOS DE IDEALES PRINCIPALES Y DOMINIOS DE FACTORIZACIÓN ÚNICA

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN MATEMÁTICA

DENNIS ALBERTO ESPEJO PEÑA

BELLAVISTA – CALLAO

FEBRERO – 2013

HOJA DE PRESENTACIÓN

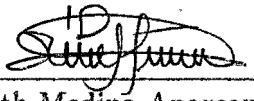
Una Caracterización de los Dominios de Ideales Principales y Dominios de Factorización Única

Dennis Alberto Espejo Peña

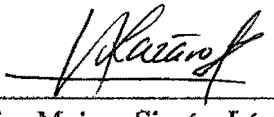
Tesis presentada a consideración del Cuerpo Docente de la Facultad de Ciencias Naturales y Matemática de la Universidad Nacional del Callao, como parte de los requisitos para obtener el Título Profesional de Licenciado en Matemática.

Aprobada por:

Lic. Absalón Castillo Valdivieso



Mg. Ruth Medina Aparcana



Lic. Moises Simón Lázaro Carrión

Lic. Herminia Bertha Tello Bedreñana

Callao - Perú
Febrero - 2013

FICHA CATALOGRÁFICA

ESPEJO PEÑA DENNIS ALBERTO

Una Caracterización de los Dominios de Ideales Principales y Dominios de Factorización Única, Callao [2012].
x, 71 p. 29,7 cm (UNAC, Licenciado en Matemática, 2012).

Tesis, Universidad Nacional del Callao, Facultad de Ciencias Naturales y Matemática.
Matemática.
I. UNAC / FCNM II. Título (Serie)

Dedicatoria

A mis padres Antonia y Primitivo,
por ser la motivación que me
impulsa a seguir día a día.

AGRADECIMIENTOS

- A Dios y a mis padres por ser mis guías en cada momento de mi vida.
- Al Lic. Marco Antonio Rubio Gallarday por ser mi asesor de tesis y ser parte de mi formación profesional orientandome hacia el estudio de esta área de la matemática, siendo él quien me impulso a trabajar esta tesis.
- Al Mg. Mario Santiago Saldaña por todo el tiempo brindado, su compromiso con este trabajo y con mi persona, por ser mi asesor y un amigo.
- Al Mg. Alex Molina por su amistad y apoyo en la revisión de esta tesis.
- Agradezco a todas las personas que me apoyaron de una u otra forma, amigos que hoy sienten este logro como suyo, gracias : Michael Gonzales Gargate, Jorge Luis Rojas, entre otros.

RESUMEN

UNA CARACTERIZACIÓN DE LOS DOMINIOS DE IDEALES PRINCIPALES Y DOMINIOS DE FACTORIZACIÓN ÚNICA

Dennis Alberto Espejo Peña

Enero - 2012

Asesor : Lic. Marco Antonio Rubio Gallarday.
Título Obtenido: Licenciado en Matemática.

En esta tesis, mostraremos una caracterización de los Dominios de Ideales Principales y Dominios de Factorización Única. Para tal efecto, se introduce primero las definiciones y nociones básicas de la Teoría de Números y del Álgebra, así como sus principales resultados necesarios para enfocarnos en los Dominios. Posteriormente se desarrollará los dos teoremas principales de este trabajo, donde con ayuda de normas e ideales fraccionarios, caracterizaremos los DIP y DFU, para luego presentar algunas aplicaciones usando los resultados obtenidos.

Palabras claves:
Dominios de Ideales Principales.
Dominios de Factorización Única.
Ideales Fraccionarios
Caracterización.

ABSTRACT

A CHARACTERIZATION OF DOMAINS PRINCIPAL IDEAL DOMAINS AND UNIQUE FACTORIZATION DOMAINS

Dennis Alberto Espejo Peña

January - 2012

Adviser : Lic. Marco Antonio Rubio Gallarday.
Obtained Degree: Mathematician.

In this thesis, we will show a characterization of principal ideal domains and unique factorization domains. For such an effect, one introduces first the definitions and basic notions of the Theory of Numbers and of the Algebra, as well as his principal results necessary to focus in the Domains. Later one will develop both principal theorems of this work, where with help of normas and ideal fractional, we will characterize the DIP and DFU, then to present some applications using the obtained results.

Keywords:
Principal Ideals Domains
Unique Factorization Domain
Ideal Fractional
Characterization.

Índice general

Introducción 1

1. Preliminares 4

1.1. Relación de equivalencia 4

1.2. Teoría de Anillos 7

1.3. Dominios de Integridad y Cuerpos. 13

1.4. Ideales 16

1.5. Homomorfismo de Anillos 17

1.6. Cuerpo de Fracciones 20

2. Dominios de Ideales Principales y de Factorización Única 25

2.1. Asociados y Divisores 25

2.2. Elementos Primos e Irreducibles 28

2.3. Máximo Común Divisor 29

2.4. DIP y DFU 36

3. Caracterización de los DIP y DFU 43

3.1. Norma en los DIP y DFU 43

3.2. Caracterización de los DIP 49

3.3. Caracterización de los DFU 52

4. Aplicaciones 60

4.1. $\mathbb{Z}$ es DFU. 61

4.2. $K[x]$ es un DIP. 62

4.3. $\mathbb{Z}[\sqrt{10}]$ no es un DIP. 63

4.4. $\mathbb{Z}[x]$ no es DIP. 65

Introducción

Como es sabido, Pierre Fermat(1601-1665) afirmó, que la ecuación diofántica

$$x^p + y^p = z^p$$

no tiene solución en los enteros positivos cuando $p > 2$
El intento de demostrar esta imposibilidad ofrece un ejemplo sorprendente del efecto inspirador que un problema, tan particular y aparentemente sin importancia, puede tener en el avance de la ciencia. Así, por ejemplo Ernest Kummer motivado por el problema de Fermat, se vio llevado a la introducción de los números ideales. En 1753, en la prueba del caso $p = 3$ del teorema de Fermat, Leonhard Euler(1707-1783) partió de la descomposición

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2)$$

Mientras que Dirichlet y Legendre en el año 1825, en sus pruebas para $p = 5$, consideraron la descomposición

$$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4)$$

El eje de los argumentos en las pruebas respectivas era determinar cuando los factores son primos entre sí, esto es, usaban un argumento de factorización única. Un paso importante fue dado por Lamé cuando consideró, como objeto donde intentar la prueba del teorema de Fermat, el anillo de los enteros ciclotómicos.

$$\mathbb{Z}[\omega] = \left\{ a_{p-1}\omega^{p-1} + ... + a_2\omega^2 + a_1\omega + a_0 \ / \ a_{p-1}, ..., a_o \in \mathbb{Z} \right\}$$

donde ω es una raíz p-ésima primitiva de la unidad, y utilizar la factorización

$$x^p - 1 = (x - 1)(x - \omega)(x - \omega^2)...(x - \omega^{p-1})$$

En el año 1839, Gabriel Lamé (1795-1870) conjeturó que si $\mathbb{Z}[\omega]$ tuviera factorización única se podría dar una prueba completa del teorema de Fermat. Fue en ese contexto, estudiando los enteros ciclotómicos que Kummer descubrió que estos anillos no siempre tienen factorización única, pero lo que la conjetura de Lamé era incorrecta.

Por ejemplo
Consideremos el anillo de enteros ciclotómicos $\mathbb{Z}[\sqrt{-3}]$ formados por los números complejos de la forma $a + b\sqrt{-3}$ donde $a, b \in \mathbb{Z}$.
Se puede observar que

$$4 = (1 + \sqrt{-3}) \times (1 - \sqrt{-3})$$

pero también

$$4 = 2 \times 2$$

donde los factores $2, 1 - \sqrt{-3}, 1 + \sqrt{-3}$ no se pueden descomponer nuevamente en factores irreducibles de $\mathbb{Z}[\sqrt{-3}]$, lo que nos indica que son elementos irreducibles, y asi el número 4 tiene dos factorizaciones distintas, en el anillo $\mathbb{Z}[\sqrt{-3}]$.
Por tanto en anillos de enteros ciclotómicos $\mathbb{Z}[\sqrt{-3}]$ no es de factorización única.

Para subsanar este problema Ernst Kummer en el año 1843 introdujo lo que él llamó números ideales , pero esto no lo llevo a la prueba teorema de Fermat. El concepto de números ideales fue luego generalizado por matemáticos de la talla de Richard Dedekind, Leopold Kronecker, Davis Hilbert y Emmy Noether, hasta llegar a la definición actual.

Así surgieron los problemas de los números primos y de los demás problemas de la teoría de números, la teoría de ecuaciones de Galois, la teoría de invariantes algebraicos, la teoría de funciones abeliana y automorfas, de hecho casi todas las más bellas cuestiones de la aritmética y la teoría de funciones modernas aparecen de esta manera y todas están relacionadas con la propiedad de poseer factorización única.

El trabajo está organizado de la siguiente manera:

En el primer capítulo, presentamos nociones básicas de Álgebra, desde la Teoría de Anillos hasta llegar al concepto de Cuerpo de fracciones así como las demostraciones de los resultados más importantes.

En el segundo capítulo, presentamos definiciones de la Teoría de Números, empezando por los elementos asociados y divisores que son nociones elementales para introducir las definiciones de los elementos primos e irreducibles y máximo común divisor hasta centrarnos en el concepto de Dominios de Ideales Principales y Dominios de Factorización Única que es donde nos centraremos de aquí en adelante.

En el tercer capítulo, estudiaremos la definición de norma y mostraremos que todo Dominio posee al menos una norma lo cual nos permitirá caracterizar los Dominios de Ideales Principales. Además introduciremos la definición de ideales divisoriales y sus propiedades, con esto caracterizaremos los Dominios de Factorización Única.

En el cuarto y último capítulo, desarrollaremos con detalle ejemplos y contraejemplos con los resultados obtenidos, demostrando así la importancia del presente trabajo.

Capítulo 1

Preliminares

En este capítulo enunciaremos y demostraremos los resultados fundamentales para la comprensión del presente trabajo .

1.1. Relación de equivalencia

Definición 1.1. Sea K un conjunto no vacío y R una relación binaria definida sobre K. Se dice que R es una relación de equivalencia si cumple las siguientes propiedades:

(i) Reflexividad:

Si todo elemento de K está relacionado consigo mismo.

$$\forall x \in K,\ xRx$$

(ii) Simetría:

Si un elemento de K está relacionado con otro, entonces ese otro elemento también se relaciona con el primero.

$$\forall x, y \in K,\ xRy \Rightarrow yRx$$

(iii) Transitividad:

Si un elemento de K está relacionado con otro, y este otro a su vez con un tercero, entonces el primero estará también relacionado con ese último.

$$\forall x, y, z \in K,\ xRy\ e\ yRz \Rightarrow xRz$$

Observación 1.1. *Una relación de equivalencia $\sim$ sobre un conjunto K se denotará con el par $(K, \sim)$*

Ejemplo 1.1.

Sea K el conjunto de todos los pares ordenados (a, b) con $a, b \in \mathbb{Z}$ y $b \neq 0$.
Definimos ahora la siguiente relación

$$(a, b) \sim (c, d) \quad \textit{si y sólo si} \quad a \cdot d = b \cdot c$$

Probaremos que $\sim$ es una relación de equivalencia sobre K.

En efecto

Veremos que dicha relación cumple con las tres condiciones que definen una relación de equivalencia:

Reflexividad

Si $(a, b) \in K$ y como $\mathbb{Z}$ es conmutativo bajo el producto usual, tenemos que $a \cdot b = b \cdot a$ entonces $(a, b) \sim (a, b)$

Simetría

Si $(a, b), (c, d) \in K$ y $(a, b) \sim (c, d)$ entonces $a \cdot d = b \cdot c$, de donde tenemos que $c \cdot b = d \cdot a$, por lo tanto $(c, d) \sim (a, b)$

Transitividad

Si $(a, b), (c, d), (e, f)$ están todos en K además $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$ entonces $a \cdot d = b \cdot c$ y $c \cdot f = d \cdot e$.
Luego $b \cdot c \cdot f = b \cdot d \cdot e$ y como $b \cdot c = a \cdot d$, se sigue que $a \cdot d \cdot f = b \cdot d \cdot e$.
Además como $\mathbb{Z}$ bajo el producto usual es conmutativo, podemos expresar la igualdad anterior como $a \cdot f \cdot d = b \cdot e \cdot d$; y como, $d \neq 0$ tenemos que $a \cdot f = b \cdot e$, por lo tanto $(a, b) \sim (e, f)$.

Las clases de equivalencia de (a, b) en K se denota como $[a, b]$.

Ejemplo 1.2.

Si $n > 1$ es un entero fijo y $a, b \in \mathbb{Z}$

Definimos $a \equiv b \ mod\ n$ si $n|(b-a)$, esta relación se llama congruencia módulo n y define una relación de equivalencia en el conjunto de los números enteros.

En efecto

Reflexividad

Como $n|0$, tenemos que $n|(a-a)$ de donde $a \equiv a \ mod\ n$, para todo $a \in \mathbb{Z}$.

Simetría

Si $a \equiv b \ mod\ n$ entonces $n|(b-a)$ es decir $n|-(a-b)$ de donde $n|(a-b)$; entonces $b \equiv a \ mod\ n$.

Transitividad

Si $a \equiv b \ mod\ n$ y $b \equiv c \ mod\ n$, entonces $n|(b-a)$ y $n|(c-b)$, de donde $n|(b-a)+(c-b)$, es decir $n|(c-a)$ por lo tanto $a \equiv c \ mod\ n$.

Denotamos a la clase de equivalencia por el símbolo $[a]$; y la llamaremos clase de congruencia (mod n) de a.

Afirmamos que:

Esta relación de equivalencia tiene "n" distintas clases de congruencias.

En efecto

Dado un entero cualquiera a, por el algoritmo de Euclides tenemos que $a = kn + r$ donde $0 \leq r < n$ entonces $a \equiv r \ mod\ n$ es decir

$$[a] = [r]$$

Por lo tanto, hay cuando más "n" distintas clases de congruencia, a saber:

$$[0], [1], ..., [n-1]$$

Pero éstas son distintas.

Pues si $[i] = [j]$, donde $0 \leq i < n$ y $0 \leq j < n$ tendríamos que $i = kn + j$, además digamos que $0 \leq j < i < n$, entonces $i - j = kn$.

Es decir, que $n|(i-j)$ donde $(i-j)$ es un entero positivo menor que n, lo que es obviamente imposible.

1.2. Teoría de Anillos

Definición 1.2. Un anillo es una terna $(A, +, \cdot)$ formada por un conjunto no vacío A y dos operaciones binarias, denotadas por $+$ y $\cdot$ respectivamente tales que para cualesquiera $a, b, c \in A$:

1. $a + b$ están en A.
2. $a + b = b + a$.
3. $a + (b + c) = (a + b) + c$.
4. Hay un elemento 0 en A tal que $a + 0 = a$, $\forall a \in A$.
5. Existe un elemento $-a$ en A tal que $a + (-a) = 0$.
6. $a \cdot b$ está en A.
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$ las dos leyes distributivas.

Observación 1.2. *La definición de un anillo nos permite deducir algunas características como:*

(i) Los axiomas (1) a (5)simplemente afirman que A es un grupo abeliano bajo la operación $+$ la que se llamará adición.

(ii) Los axiomas (6) y (7) nos dicen que A es cerrado bajo una operación asociativa, $\cdot$, la se llamará multiplicación.

(iii) El axioma (8) sirve para correlacionar las dos operaciones de A.

(iv) Siempre que hablemos de un anillo entenderemos que estamos hablando de un anillo asociativo.

Definición 1.3. Si $a \cdot b = b \cdot a$, $\forall a, b \in A$ diremos que A es un anillo conmutativo.

Definición 1.4. Sea A un anillo conmutativo.
A es un anillo unitario si existe $1_A \in A$ tal que

$$a \cdot 1_A = 1_A \cdot a = a.$$

Para todo $a \in A$, donde 1_A (o simplemente 1) es el elemento unitario de A.

Definición 1.5. Sea A un anillo conmutativo con 1 (Anillo unitario).
Un elemento $u \in A$ es una unidad de A si existe un $a \in A$ tal que

$$a \cdot u = 1.$$

Un anillo conmutativo con 1 que posee unidad se llamará anillo con unidad.
El inverso de un elemento a bajo la multiplicación se denotará como a^{-1}.

Observación 1.3.
Por simplicidad en la expresión, omitiremos de aquí en adelante el punto en $a \cdot b$ y escribiremos simplemente este producto como ab.

Ejemplo 1.3.
Los anillos más comunes son:

(i) $(\mathbb{Z}, +, .)$ *es un anillo conmutativo (bajo la suma y el producto usual) y con unidad 1.*

(ii) Dado un $n \in \mathbb{Z}$ *fijo. El conjunto* $n\mathbb{Z} = \{nx / x \in \mathbb{Z}\}$ *es un anillo conmutativo (bajo la suma y el producto usual) y sin unidad.*

(iii) Las clases de módulo n, $(\mathbb{Z}_n, +, .)$ *son anillos conmutativos y con unidad* $1_{\mathbb{Z}_n} = [1]$, *siendo* $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$

(iv) Los enteros de Gauss $(\mathbb{Z}[i], +, .)$ *son anillos conmutativos y con 1, donde* $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ *e* $i = \sqrt{-1}$

Ejemplo 1.4.

Si $K = \mathbb{Q}$, $\mathbb{R}$ *ó* $\mathbb{C}$

Llamaremos $K[x]$ *al conjunto de todos los polinomios con coeficientes en* K.

Los elementos de $K[x]$ *son expresiones de la forma*

$$f(x) = a_0 + a_1 x + ... + a_n x^n$$

con $a_j \in K$ *y* $n \geq 0$ *un entero.*

Dos polinomios $f(x) = a_0 + a_1 x + ... + a_m x^m$ *y* $g(x) = b_0 + b_1 x + ... + b_n x^n$ *en* $K[x]$, *son iguales y lo denotaremos como* $f(x) = g(x)$, *si y sólo si,* $a_i = b_j$ *para todo* $i, j \geq 0$. *De donde tenemos que* $m = n$.

En $K[x]$ *definimos la suma y producto usuales:*

SUMA:

Si $f(x) = a_0 + a_1 x + ... + a_m x^m$ *y* $g(x) = b_0 + b_1 x + ... + b_n x^n$ *son dos polinomios en* $K[x]$, *se define*

$$f(x) + g(x) := (a_0 + b_0) + (a_1 + b_1)x + ... + (a_i + b_i)x^i + ... \in K[x]$$

PRODUCTO:

Si $f(x), g(x) \in K[x]$ *son dos polinomios dados como antes, se define*

$$f(x) \cdot g(x) := c_0 + c_1 x + ... + c_i x^i + ... \in K[x]$$

donde

$$c_i := \sum_{r+s=i} a_r \cdot b_s$$

Entonces, $K[x]$ *resulta un anillo conmutativo con 1.*

Ejemplo 1.5.
Si A y B son anillos, definimos el producto cartesiano $A \times B$ como:

$$A \times B = \{(a,\ b);\ a \in A\ \ y\ \ b \in B\}$$

En $A \times B$ se define la suma y producto:

SUMA:

Si $(a_1,\ b_1)$ y $(a_2,\ b_2)$ son dos elementos de $A \times B$

$$(a_1,\ b_1) + (a_2,\ b_2) := (a_1 + a_2\ ,\ b_1 + b_2)\ \in A \times B$$

PRODUCTO:

Si $(a_1,\ b_1)$ y $(a_2,\ b_2) \in A \times B$

$$(a_1,\ b_1) \cdot (a_2,\ b_2) := (a_1 \cdot a_2\ ,\ b_1 \cdot b_2)\ \in A \times B$$

De donde $A \times B$ es un anillo, llamado producto directo de los anillos A y B.

Definición 1.6. Un subanillo S de un anillo A es un subconjunto no vacío $S \subset A$ que cumple que es cerrado para la adición y la multiplicación en el anillo, esto es:

(i) Si $a, b \in S$ entonces $a - b \in S$

(ii) Si $a, b \in S$ entonces $ab \in S$

Ejemplo 1.6. *Los ejemplos más comunes y sencillos de subanillos son:*

- $\mathbb{Z}$ *es un subanillo de* $\mathbb{Q}$
- $\mathbb{Q}$ *es un subanillo de* $\mathbb{R}$
- $\mathbb{R}$ *es un subanillo de* $\mathbb{C}$

Lema 1.1. *Si A es un anillo, entonces para todo $a, b \in A$*

1. $a0 = 0a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.

   Si, además, A tiene un elemento unitario, 1, entonces
4. $(-1)a = -a$.
5. $(-1)(-1) = 1$.

Demostración.

1. Dado un $a \in A$ tenemos que

$$a0 = a(0 + 0) = a0 + a0$$

   y como A es un grupo respecto a la adición obtenemos

$$a0 = 0$$

   Analogamente tenemos que $0a = 0$.

2. Haciendo uso de la parte 1 tenemos que

$$ab + a(-b) = a(b + (-b)) = a0 = 0$$

   Por tanto

$$a(-b) = -(ab)$$

   Análogamente $(-a)b = -(ab)$.

3. De la parte anterior tenemos que

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

4. Supongamos que A tiene un elemento unitario 1 entonces

$$a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$$

   de donde

$$(-1)a = -a$$

5. En particular, tomando $a = -1$ y por la parte 4 tenemos que

$$(-1)(-1) = -(-1) = 1$$

lo que deja establecido la parte 5.

□

1.3. Dominios de Integridad y Cuerpos.

Definición 1.7. Sea A un anillo conmutativo entonces si $a \neq 0 \in A$ se dice que es un divisor de cero si existe $b \in A$, $b \neq 0$, tal que $ab = 0$.

Definición 1.8. Un anillo conmutativo es un Dominio de integridad si no tiene divisores de cero.

Ejemplo 1.7.

- $\mathbb{Z}$ *y* $\mathbb{Q}$ *son Dominios de integridad.*
- $\mathbb{Z}_6$ *no es un Dominio de Integridad ya que* $[2] \neq 0$ *y* $[3] \neq 0$ *se tiene que*

$$[2] \cdot [3] = [6] = [0]$$

- $A \times B$ *no es un Dominio de Integridad ya que para* $a, b \neq 0$ *tenemos*

$$(a, 0)(0, b) = (0, 0)$$

Proposición 1.1. *A es un dominio de integridad, si y sólo si A es un anillo conmutativo y dado $a \neq 0$ y $ax = ay$ implica que $x = y$.*

Demostración.
$\Rightarrow$)
Como $ax = ay$ entonces $a(x - y) = 0$.
Por otro lado como A es un dominio de integridad, no tiene divisores de cero, y como $a \neq 0$ entonces $x - y = 0$
Por lo tanto

$$x = y.$$

$\Leftarrow$)
Sea $a \cdot b = 0$ con $a \neq 0$ luego tenemos que $a \cdot b = 0 = a \cdot 0$ entonces $b = 0$, es decir, no tiene divisores de cero.
Por lo tanto

A es un dominio de integridad.

□

Definición 1.9. Un anillo conmutativo se dice que es un anillo con división, si dado $a \neq 0$ entonces existe $b \neq 0$ tal que $a \cdot b = 1$.

Definición 1.10. Un cuerpo es un anillo de división conmutativo con al menos dos elementos distintos.

Ejemplo 1.8.

(i) Los números racionales $\mathbb{Q}$ *, los números reales* $\mathbb{R}$*, los números complejos* $\mathbb{C}$ *, son cuerpos*

(ii) El conjunto de las matrices de orden 2 con coeficientes en $\mathbb{Z}_3$*, de la forma* $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$ *es un cuerpo.*

Proposición 1.2. *El anillo de enteros módulo* p*,* $\mathbb{Z}_p$ *es un cuerpo si y sólo si,* p *es un número primo.*

Demostración.
$\Rightarrow$)
Supongamos que p no es un número primo, entonces existen $0 < a, b < p$ tales que

$$p = ab.$$

Entonces

$$[a] \cdot [b] = [a \cdot b] = [p] = [0]$$

Como $\mathbb{Z}_p$ es cuerpo, tenemos que $[a] = [0]$ o $[b] = [0]$. Pero eso se cumple si $p|a$ o $p|b$ lo que contradice la hipótesis.

$\Leftarrow$)

Probaremos que todo elemento no nulo tiene inverso multiplicativo.

En efecto

Consideremos $[q] \in \mathbb{Z}_p$ con $0 < q < p$.

Por ser p primo, tenemos que p y q son primos entre sí y por tanto, existen enteros $a, b \in \mathbb{Z}_p$ tales que $1 = aq + bp$, de donde

$$[1] = [a][q] + [b][p] = [a][q] + [b][0] = [a][q].$$

Luego $[q]$ tiene inverso en $\mathbb{Z}_p$. □

Proposición 1.3. *Todo cuerpo es un dominio de integridad.*

Demostración.

Sea A un cuerpo y sean $a, b \in A$ tal que $a \neq 0$ y $b \neq 0$.

Supongamos que $ab = 0$ entonces

$$1 = (ab)a^{-1}b^{-1} = 0$$

lo cual es absurdo ya que todo cuerpo tiene al menos dos elementos distintos $1 \neq 0$.

Entonces $ab \neq 0$, es decir,que A no tiene divisores de cero.

Por lo tanto

A es un dominio de integridad.

□

1.4. Ideales

Apartir de esta sección trabajaremos con anillos conmutativos con unidad.

Definición 1.11. Un subconjunto no vacío I de A se dice que es un ideal de A si:

(i) I es un subgrupo de A bajo la adición.

(ii) Para todo $u \in I$ y $r \in A$, ru está en I.

Ejemplo 1.9. *Veamos*

(i) 0 *y* A *son ideales triviales de* A.

(ii) Los conjuntos $n\mathbb{Z}$ *son ideales, para todo* $n \in \mathbb{Z}$.

(iii) Todos los conjuntos cuyos elementos son los múltiplos de $p(x) \in \mathbb{R}[x]$ *son ideales.*

Observación 1.4.
Sea A *un anillo,* A *es un cuerpo si y sólo si los únicos ideales son (0) y (1).*
En efecto
$\Rightarrow$)
Sea $I \subset A$ *ideal donde* $I \neq (0)$, *luego dado un* $b \neq 0$ *tal que* $b \in I$ *se tiene que* $b \cdot b^{-1} = 1 \in I$ *entonces* $I = A$.
$\Leftarrow$)
Sea $b \neq 0$ *entonces* $(b) = (1) = A$ *entonces existe* $c \in A$ *tal que* $b \cdot c = 1$.

1.5. Homomorfismo de Anillos

Definición 1.12. Una aplicación $\phi : A \to B$ donde A y B son anillos, se dirá un homomorfismo de anillos si

$$\phi(a+b) = \phi(a) + \phi(b) \quad \forall a, b \in A$$

$$\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in A$$

Lema 1.2.
Si $\phi : A \to B$ es homomorfismos de anillos, se verifica que:

(i) $\phi(0_A) = 0_B$ *o simplemente* $\phi(0) = 0$

En efecto

$\phi(0_A) = \phi(0_A + 0_A) = \phi(0_A) + \phi(0_A)$ *de donde* $\phi(0_A) = 0_B$

(ii) $\phi(-a) = -\phi(a)$

En efecto

$\phi(a) + \phi(-a) = \phi(a + (-a)) = \phi(0_A) = 0$ *entonces* $\phi(-a) = -\phi(a)$

(iv) $\phi(a - b) = \phi(a) - \phi(b)$

En efecto

$\phi(a) = \phi(a - b + b) = \phi(a - b) + \phi(b)$ *de donde* $\phi(a - b) = \phi(a) - \phi(b)$

Ejemplo 1.10. *Veamos*

- *La función inclusión $i : A \to B$ definida como $i(a) = a$, $\forall a \in A$ y $A \subset B$ es un homomorfismo de anillos.*
- *La aplicación $\phi : \mathbb{Z} \to \mathbb{Z}_n$ dado por $\phi(a) = [a]$, es un homomorfismo de anillos.*

Definición 1.13. *El núcleo de un homomorfismo de anillos* $\phi : A \to B$ *es el conjunto*

$$Ker(\phi) = \{x \in A \ / \ \phi(x) = 0\}$$

y la imagen de ϕ *es el conjunto*

$$Im(\phi) = \{\phi(x) \ / \ x \in A\}$$

Teorema 1.1. *Sea* $\phi : A \to B$ *un homomorfismo de anillos. Se cumplen:*

(i) $Ker(\phi)$ *es un ideal del anillo* A.

(ii) $Im(\phi)$ *es un subanillo del anillo* B.

Demostración.

(i) Sean $a \in Ker(\phi)$ y $b \in A$
$\phi(ab) = \phi(a) \cdot \phi(b) = 0 \cdot \phi(b) = 0$ de donde $ab \in Ker(\phi)$

(ii) Sean $\phi(a)$, $\phi(b) \in Im(\phi)$ tal que $a, b \in A$
$\phi(a) - \phi(b) = \phi(a - b) \in Im(\phi)$ puesto que $a - b \in A$
$\phi(a) \cdot \phi(b) = \phi(ab) \in Im(\phi)$ puesto que $ab \in A$

□

Definición 1.14. *Sea* $\phi : A \to B$ *es homomorfismos de anillos.*

(i) ϕ *es monomorfismo , si es homomorfismo inyectivo.*

(ii) ϕ *es epimorfismo , si es homomorfismo suprayectivo.*

(iii) ϕ *es isomorfismo , si es homomorfismo biyectivo.*

Proposición 1.4. *Dado un homomorfismo de anillos $\phi : A \to B$, diremos que es ϕ inyectivo si y sólo si $Ker(\phi) = 0$.*

Demostración.
$\Rightarrow$)
Sea $a \in Ker(\phi)$ entonces $\phi(a) = 0 = \phi(0)$ y como ϕ es inyectiva
entonces

$$a = 0$$

$\Leftarrow$)
Sea $\phi(a) = \phi(b)$ entonces $0 = \phi(a) - \phi(b) = \phi(a - b)$ es decir
$a - b \in Ker(\phi) = (0)$ entonces $a - b = 0$
luego

$$a = b$$

Por lo tanto

$$\phi \text{ es inyectivo.}$$

□

Lema 1.3.
Todo homomorfismo no nulo que parte de un cuerpo es inyectivo.

Demostración.
Sea A un cuerpo y dado un homomorfismo no nulo de anillos $\phi : A \to B$.
Por el Teorema 1.1 tenemos que $Ker(\phi)$ es un ideal en A, y como ϕ es no nulo tenemos que $Ker(\phi) \neq (1)$.
Por otro lado A es un cuerpo entonces los únicos ideales de A son (0) y (1).
es decir

$$Ker(\phi) = (0)$$

Por lo tanto

$$\phi \text{ es inyectiva.}$$

□

1.6. Cuerpo de Fracciones

A lo largo de esta sección A denotará un dominio de integridad y $A^* = A \setminus \{0\}$.

Dados $(a,b),(c,d) \in A \times A^*$ definiremos $(a,b) \sim (c,d)$ si $ad = bc$,
y como $\sim$ es una relación de equivalencia.

Escribiremos $K = \dfrac{A \times A^*}{\sim}$.

Denotaremos a/b la clase de equivalencia del elemento $(a,b) \in A \times A^*$.

Definiremos sobre K las operaciones

$$a/b + c/d = (ad + bc)/(bd)$$

$$(a/b)(c/d) = (ac)/(bd)$$

las cuales veremos que están bien definidas.
En efecto
Sean $a/b = a'/b'$ y $c/d = c'/d'$ de donde tenemos que $ab' = a'b$ y $cd' = c'd$

SUMA:

Debemos probar que

$$a/b + c/d = a'/b' + c'/d'$$

o lo que es equivalente a probar que

$$(ad + bc)/(bd) = (a'd' + b'c')/(b'd')$$

veamos

$$\begin{aligned}(ad + bc)b'd' &= adb'd' + bcb'd' \\ &= a'dbd' + c'dbb' \\ &= bd(a'd' + c'b')\end{aligned}$$

Por lo tanto la suma está bien definida.

PRODUCTO:

Debemos probar que

$$(a/b)(c/d) = (a'/b')(c'/d')$$

o lo que es equivalente a probar que

$$(ac)/(bd) = (a'c')/(b'd')$$

veamos

$$\begin{aligned}(ac)(b'd') &= acb'd' \\ &= a'bc'd \\ &= (a'c')(bd)\end{aligned}$$

Por lo tanto el producto esta bien definido.

Definimos

$$0/1 = \{(0,a)/a \in A^*\}$$

$$1/1 = \{(a,a)/a \in A^*\}$$

como neutro aditivo y el neutro multiplicativo respectivamente.

Además tenemos que:
$-(a/b) = \{(-a,b)/a,b \in A^*\}$ es la clase del inverso aditivo de a/b.
$(a/b)^{-1} = \{(b,a)/a,b \in A^*\}$ es la clase del inverso multiplicativo de a/b.

Veamos la ley distributiva

$$\begin{aligned}(a/b + c/d)(e/f) &= ((ad+bc)/bd)(e/f) \\ &= (ade+bce)/bdf \\ &= (adef+bcef)/bdff \\ &= ae/bf + ce/df \\ &= (a/b)(e/f) + (c/d)(e/f)\end{aligned}$$

Por lo tanto

K es el cuerpo de fracciones de A.

Por otro lado la función

$$\begin{aligned} i \ : \ A &\to K \\ a &\mapsto a/1 \end{aligned}$$

es un monomorfismo, así podemos identificar a A como subanillo de K.

El siguiente resultado nos dice que todo cuerpo que contenga a A como subanillo, debe contener al cuerpo de cocientes de A como subcuerpo.

Proposición 1.5. *Sea un A un Dominio de integridad y K su cuerpo de fracciones, sea L un cuerpo y $f : A \to L$ un monomorfismo, entonces existe un único homomorfismo $h : K \to L$ tal que es monomorfismo y $h \circ i = f$.*

Demostración.
Definamos h como

$$\begin{aligned} h \ : \ K &\to L \\ a/b &\mapsto f(a)(f(b))^{-1} \end{aligned}$$

ya que $b \neq 0$ entonces $f(b) \neq 0$ por tanto $(f(b))^{-1} \in L$.

Veamos que h esta bien definida
Sean $a/b = c/d$ de donde tenemos que $ad = bc$, luego

$$\begin{aligned} f(a)f(d) &= f(ad) \\ &= f(bc) \\ &= f(b)f(c) \end{aligned}$$

entonces

$$f(a)(f(b))^{-1} = f(c)(f(d))^{-1}$$

con lo cual h es bien definido.

Sean $a/b, c/d \in K$, luego

$$\begin{aligned} h\,(a/b + c/d) &= h\,((ad+bc)/(bd)) \\ &= f(ad+bc)(f(bd))^{-1} \\ &= (f(a)f(d)+f(b)f(c))(f(b))^{-1}(f(d))^{-1} \\ &= f(a)(f(b))^{-1} + f(c)(f(d))^{-1} \\ &= h(a/b) + h(c/d) \end{aligned}$$

$$\begin{aligned} h\,((a/b)(c/d)) &= h\,((ac)/(bd)) \\ &= f(ac)(f(bd))^{-1} \\ &= f(ac)(f(b))^{-1}(f(d))^{-1} \\ &= f(a)f(c)(f(b))^{-1}(f(d))^{-1} \\ &= f(a)(f(b))^{-1}f(c)(f(d))^{-1} \\ &= h(a/b)h(c/d) \end{aligned}$$

Con lo cual h es homomorfismo.

La inyectividad se deduce del Lema 1.3 ya que h es no nulo.

Por tanto h es monomorfismo.

También se cumple para todo $a \in A$

$$\begin{aligned} (h \circ i)(a) &= h(i(a)) \\ &= h(a/1) \\ &= f(a)(f(1))^{-1} \\ &= f(a)(1)^{-1} \\ &= f(a) \end{aligned}$$

Así $h \circ i = f$.

Por último veamos la unicidad de h

Sea $h' : K \to L$ otro monomorfismo tal que $h' \circ i = f$, entonces

$$\begin{aligned} h'(a/b) &= h'((a/1)(b/1)^{-1}) \\ &= h'(a/1)(h'(b/1))^{-1} \\ &= h'(i(a))(h'(i(b)))^{-1} \\ &= f(a)(f(b))^{-1} \\ &= h(a/b).\ \forall a/b \in K \end{aligned}$$

Por lo tanto

existe un único homomorfismo h tal que h es monomorfismo y $h \circ i = f$.

□

Capítulo 2

Dominios de Ideales Principales y de Factorización Única

A partir de este capítulo A denotará un dominio de integridad y K su cuerpo de fracciones.
Además dado cualquier subconjunto E de K, denotaremos $E^* = E \setminus \{0\}$.

2.1. Asociados y Divisores

Definición 2.1. *Sean $a, b \in A$. Diremos que a* divide a *b, si existe $c \in A$ tal que $b = ac$ y denotaremos $a|b$.*
En caso contrario diremos que a no divide a b y denotaremos $a \not| b$.

Definición 2.2. *Diremos que a y b son* asociados, *si existe $c \in A$ unidad tal que $a = bc$ y denotaremos $a \sim b$.*

Ejemplo 2.1. *Sea $a, b, c \in A$ arbitrario.*

1. *Para todo a se cumple que $a|0$ y $1|a$.*
   En efecto
   Este resultado es evidente debido a que $0 = a0 \quad y \quad a = a1$.

2. *Si* $0|a$ *entonces* $a = 0$.

   En efecto

   Como $0|a$, *existe* $b \in A$ *tal que* $a = 0b = 0$.

3. *Si* a *es unidad, entonces* $b|a$ *si y sólo si* b *es unidad.*

   En efecto

   Como $b|a$ *tenemos que existe* $d \in A$ *tal que*

   $a = bd$ *si y sólo si* $1 = (a^{-1}b)d = (a^{-1}d)b$ *si y sólo si* b *es unidad.*

4. *Para todo* $a \neq 0$, *entonces* $b|c$ *si y sólo si* $ab|ac$.

   En efecto

   Como $b|c$ *tenemos que existe* $d \in A$ *tal que*

   $c = bd$ *si y sólo si* $ac = a(bd) = (ab)d$ *si y sólo si* $ab|ac$.

Proposición 2.1.

1. *La relación "es asociado a" es una relación de equivalencia en* A.

2. *La relación "divide a" es reflexiva y transitiva en* A.

Demostración.

Sean $a, b, c \in A$.

1. Analicemos la relación "es asociado a":

   Reflexividad:

   $a \sim a$, debido a que $a = a1$.

   Simetría:

   Si $a \sim b$, existe $u \in A$ unidad tal que $a = bu$. Luego $b = au^{-1}$, y $b \sim a$.

   Transitividad:

   Si $a \sim b$ y $b \sim c$, existen $u, v \in A$ unidades tal que $a = bu, b = cv$. Luego $a = c(vu)$ con vu unidad, y $a \sim c$.

2. Analicemos la relación "divide a":

   Reflexividad:
   $a|a$ debido a que $a = a1$.

   Transitividad:
   Si $a|b$ y $b|c$, existen $u, v \in A$ tal que $b = au, c = bv$. Luego $c = a(uv)$, y $a|c$.

□

Proposición 2.2. *Dados $a, b \in A$, se cumple:*

1. *$a|b$ si y sólo si $bA \subseteq aA$,*

2. *$a \sim b$ si y sólo si $aA = bA$.*

Demostración.

1. Como $a|b$ tenemos que existe $c \in A$ tal que
   $b = ac$ si y sólo si $b \in aA$ si y sólo si $bA \subseteq aA$.

2. $\Rightarrow$)
   Como $a \sim b$ tenemos que existe $c \in A$ unidad tal que
   $b = ac$ o también $a = bc^{-1}$.
   Luego $a|b$ y $b|a$, y por el item anterior $bA \subseteq aA$ y $aA \subseteq bA$ respectivamente.
   Finalmente $aA = bA$
   $\Leftarrow$)
   Como $aA = bA$ tenemos que $a|b$ y $b|a$.
   Es decir, existen $u, v \in A$ tal que $a = bu$, $b = av$.
   Si $b = 0$, es inmediato que $a = 0$.
   Si $b \neq 0$, tenemos que $b = b(uv)$, de donde se sigue que $uv = 1$, es decir,
   u es unidad y por tanto $a \sim b$.
   En cualquier caso $a \sim b$. □

2.2. Elementos Primos e Irreducibles

Definición 2.3. *Sea $p \in A$. Diremos que p, no nulo y no unidad, es elemento* irreducible *siempre que $p = ab$ con $a, b \in A$, tenemos que a o b es unidad.*

Definición 2.4. *Sea $p \in A$, no nulo y no unidad. Diremos que p es elemento* primo *si en el caso que $p|ab$ con $a, b \in A$, tenemos que $p|a$ o $p|b$.*

Proposición 2.3. *Todo elemento primo es irreducible.*

Demostración.
Dado un elemento primo $p \in A$.
Sea además $p = ab$ con $a, b \in A$, donde ni a ni b son 0, entonces $a|p$ o $b|p$.
Supongamos que $a|p$ entonces $pA \subseteq aA$.
Por otro lado como p es primo y $p = ab$ tenemos que $p|a$ o $p|b$, tomando que $p|a$ tenemos que $aA \subseteq pA$ entonces

$$pA = aA$$

Lo que implica que $p \sim a$ de donde $p = au$ con u unidad.
Luego $au = ab$ y como A es un Dominio y $a \neq 0$ tenemos que $u = b$.
entonces b es unidad.
Por lo tanto

$$p \text{ es irreducible.}$$

De manera análoga tenemos $p|b$ entonces a sería unidad.

□

2.3. Máximo Común Divisor

Definición 2.5. *Sean $a, b, d \in A$. Diremos que d es un* máximo común divisor *(mcd) de a, b si:*

(i) $d|a \quad y \quad d|b$

(ii) Si $c|a$ *y* $c|b$ *entonces* $c|d$.

Usaremos la notación $d = mcd(a, b)$ *para indicar que* d *es un máximo común divisor de* a *y* b.

NOTA

Se dice que d es un máximo común divisor de a y b ya que cualquier asociado de un máximo común divisor es un máximo común divisor dicho resultado se probará en la Proposición 2.4 .

Observación 2.1.

Sean $a, b \in A$. *Entonces:*

(i) $a = mcd(a, 0)$.

En efecto

Es inmediato que $a|a$ *y* $a|0$; *si* $c|a$ *y* $c|0$, *entonces* $c|a$.

Por tanto

$$a = mcd(a, 0).$$

(ii) Si a *es unidad y* b *arbitario no nulo,* $1 = mcd(a, b)$.

En efecto

Si $c|a$ *y* $c|b$

Como $c|a$ *existe* $x \in A$, *tal que* $a = cx$ *y además como* a *es unidad tenemos que*

$$1 = c(xa^{-1})$$

de donde c *es unidad entonces*

$$c|1.$$

Por lo tanto

$$mcd(a,b) = 1$$

Proposición 2.4. *Sean $a, b \in A$ tal que existe $d = mcd(a,b)$. Entonces $c = mcd(a,b)$ (otro mcd) si y sólo si c y d son asociados.*

Demostración.

$\Rightarrow$)

Como $d = \text{mcd}(a,b)$ entonces $d|a$ y $d|b$ y como $c|a$ y $c|b$ tenemos que $c|d$ entonces $dA \subseteq cA$.

Por otro lado como $c = \text{mcd}(a,b)$ entonces $c|a$ y $c|b$ y como $d|a$ y $d|b$ tenemos que $d|c$ entonces $cA \subseteq dA$.

Lo que implica que

$$dA = cA$$

Por lo tanto

$$c \sim d$$

$\Leftarrow$)

Como $c \sim d$, existe $u \in A$ unidad tal que $c = ud$, es decir, $d|c$ y además como $d = u^{-1}c$ tenemos que $c|d$.

Luego dado que $d = \text{mcd}(a,b)$ tenemos que $d|a$ y $d|b$ y como $c|d$ entonces

$$c|a \text{ y } c|b.$$

Luego sea $e \in A$ tal que $e|a$ y $e|b$, tendriamos que $e|d$ y como $d|c$ implica que

$$e|c$$

Por lo tanto $c = \text{mcd}(a,b)$. □

Ejemplo 2.2.

Sean $a(x) = 48x^3 - 84x^2 + 42x - 36$ *y* $b(x) = -4x^3 - 10x^2 + 44x - 30$

entonces

$a(x) = 6(2x-3)(4x^2 - x + 2)$ *y*

$b(x) = -2(2x-3)(x-1)(x+5)$

Luego

- *En* $\mathbb{Z}[x]$, $mcd(a(x), b(x)) = 4x - 6$
  $g_1 = 4x - 6$ *y* $g_2 = -4x + 6$ *son divisores comunes de* $a(x)$ *y* $b(x)$
  pero g_1/g_2 *y* g_2/g_1, *es decir son asociados.*

- *En* $\mathbb{Q}[x]$, $mcd(a(x), b(x)) = x - 3/2$
  $g_1 = 4x - 6$ *y* $g_2 = x - 3/2$ *son divisores comunes de* $a(x)$ *y* $b(x)$
  pero g_1/g_2 *y* g_2/g_1, *es decir son asociados.*

Definición 2.6. *Diremos que A es un dominio con máximo común divisor (DMCD) si todo par de elementos de A tienen mcd.*

Ejemplo 2.3.

En el Dominio

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

los elementos

$$9 = 3 \times 3 = (2 + \sqrt{-5}) \times (2 - \sqrt{-5})$$

y

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

tienen como únicos divisores comunes (salvo asociados) a

$$3 \text{ y } 2 + \sqrt{-5}$$

Es decir que estos elementos son nuestros candidatos a ser mcd.

Supongamos que el $mcd(9, 6 + 3\sqrt{-5}) = 2 + \sqrt{-5}$

Luego como $3|9$ *y* $3|6+3\sqrt{-5}$ *entonces* $3|2+\sqrt{-5}$ *es decir, existe* $a+b\sqrt{-5}$ *donde* $a, b \in \mathbb{Z}$ *tal que*

$$3 \cdot (a + b\sqrt{-5}) = 2 + \sqrt{-5}$$

de donde $3a = 2$ *y* $3b = 1$ *es imposible ya que* $a, b \in \mathbb{Z}$

Ahora supongamos que el $mcd(9, 6 + 3\sqrt{-5}) = 3$
Luego como $2 + \sqrt{-5}|9$ *y* $2 + \sqrt{-5}|6 + 3\sqrt{-5}$ *entonces* $2 + \sqrt{-5}|3$ *es decir, existe* $a + b\sqrt{-5}$ *donde* $a, b \in \mathbb{Z}$ *tal que*

$$(2 + \sqrt{-5}) \cdot (a + b\sqrt{-5}) = 3$$

de donde $2a - 5b + (a + 2b)\sqrt{-5} = 3$ *es decir* $a + 2b = 0$ *y* $2a - 5b = 3$ *entonces* $a = 2/3$ *y* $b = -1/3$ *lo cual es imposible ya que* $a, b \in \mathbb{Z}$

Luego
Como dos elementos en el Dominio $\mathbb{Z}[\sqrt{-5}]$ *hemos visto que no tiene mcd.*
Por lo tanto

$$\mathbb{Z}[\sqrt{-5}] \text{ no es DMCD}$$

Es decir que, dos elementos de A no tienen porque tener mcd, y si lo tuvieran no tiene por que ser único.

Proposición 2.5. *Si A es DMCD y* $a, b, c \in A$. *Escribamos* $d = mcd(a, b)$. *Entonces:*

1. $mcd(ab, ac) = a \cdot mcd(b, c)$.
2. *Si* $d \neq 0$ *entonces* $mcd(a/d, b/d) = 1$.
3. *Si* $mcd(a, b) = mcd(a, c) = 1$, *entonces* $mcd(a, bc) = 1$.

Demostración.

1. Si $a = 0$, el resultado se sigue fácilmente.
   Si $a \neq 0$, sea $x = \text{mcd}(ab, ac)$.

Como $a|ab$ y $a|ac$, tenemos $a|x$, luego existe $y \in A$ tal que $x = ay$.
Como $x|ab$ y $x|ac$, existe $p, q \in A$ tal que

$$\begin{aligned} ab &= xp \\ &= (ay)p \\ &= a(yp) \end{aligned}$$

De manera análoga tenemos que

$$\begin{aligned} ac &= xq \\ &= (ay)q \\ &= a(yq) \end{aligned}$$

entonces $b = yp$ y $c = yq$, es decir,

$$y|b \text{ y } y|c.$$

Sea $z \in A$ tal $z|b$ y $z|c$, entonces $az|ab$ y $az|ac$, luego como $x = \text{mcd}(ab, ac)$ tenemos que $az|x$ y como $x = ay$ decimos que $az|ay$ es decir

$$z|y.$$

Entonces $y = \text{mcd}(b, c)$.
Luego

$$\begin{aligned} mcd(ab, ac) &= x \\ &= ay \\ &= a \cdot mcd(b, c) \end{aligned}$$

2. Como $d = mcd(a, b)$ y además $d \neq 0$ podemos afirmar que

$$\begin{aligned} d &= mcd(a, b) \\ &= mcd(d(a/d), d(b/d)) \\ &= d \cdot mcd(a/d, b/d) \end{aligned}$$

de donde $mcd(a/d, b/d) = 1$.

3. Sea $u \in A$ tal que $u|a$ y $u|bc$, entonces $u|ac$ y $u|bc$, entonces $u|mcd(ac, bc)$
Por otro lado tenemos que

$$\begin{aligned} mcd(ac, bc) &= c \cdot mcd(a, b) \\ &= c \cdot 1 \\ &= c \end{aligned}$$

Entonces $u|mcd(ac, bc)$, es decir, $u|c$ y como $u|a$ tenemos que $u|mcd(a, c)$ pero $mcd(a, c) = 1$ entonces $u|1$ implica que u es una unidad.
Por tanto

$$mcd(a, bc) = 1$$

□

Lema 2.1. *Si p es un elemento irreducible de A, entonces $p \nmid a$ si y sólo si $mcd(p, a) = 1$.*

Demostración.
$\Rightarrow$)
Sea $u \in A$ tal que $u|p$ y $u|a$ entonces existe $b, c \in A$ tal que $p = bu$, $a = cu$.
Como p es irreducible, b o u es unidad.
Supongamos que b es unidad, entonces $u = b^{-1}p$.
Luego

$$a = cu = (cb^{-1})p,$$

luego $p|a$, y como $p \nmid a$ tenemos una contradicción.
Así b no es unidad entonces u debe ser unidad, por tanto $mcd(p, a) = 1$.
$\Leftarrow$)
Supongamos $p|a$, entonces $p|mcd(p, a)$ de donde tenemos que $p|1$, así p es unidad, lo cual es una contradicción ya que p es irreducible.
Por tanto $p \nmid a$. □

Proposición 2.6. *Si A es un DMCD, todo elemento irreducible es primo.*

Demostración.
Sea p elemento irreducible de A.
Debemos probar que p es primo, es decir

$$\text{Si } p|ab \text{ entonces } p|a \text{ o } p|b$$

lo que es equivalente a probar que

$$\text{Si } p \not| a \text{ y } p \not| b \text{ entonces } p \not| ab$$

Supongamos que $p \not| a$ y $p \not| b$, con $a, b \in A$.
entonces

$$mcd(p, a) = mcd(p, b) = 1$$

Por la Proposición 2.5 tenemos que

$$mcd(p, ab) = 1$$

y por el Lema 2.1

$$p \not| ab$$

Por lo tanto

$$p \text{ es elemento primo de } A.$$

□

2.4. DIP y DFU

Definición 2.7. *Un ideal I de A se dice principal si tiene la forma aA con $a \in A$. Diremos que A es un dominio de ideales principales (DIP) si todo ideal de A es principal.*

Proposición 2.7. *Si A es DIP entonces es un DMCD. Además para $a, b \in A$ existen $\alpha, \beta \in A$ tal que $mcd(a, b) = \alpha a + \beta b$.*

Demostración.
Dado que A es un DIP tenemos que

$$aA + bA = cA$$

de donde $aA, bA \subseteq cA$, es decir

$$c|a \text{ y } c|b$$

Por otro lado, sea $u|a$ y $u|b$ entonces tenemos que $aA, bA \subseteq uA$ de donde

$$cA = aA + bA \subseteq uA$$

Por tanto $u|c$.
En conclusión

$$c = \text{mcd}(a, b).$$

Por lo tanto

$$A \text{ es un DMCD.}$$

Finalmente de

$$aA + bA = cA,$$

tenemos que existen $\alpha, \beta \in A$ tal que

$$mcd(a, b) = \alpha a + \beta b$$

□

Definición 2.8. *Diremos que A es un dominio de factorización única (DFU) si todo elemento no unidad y no nulo de A se puede expresar de manera única como producto finito de elementos irreducibles de A salvo asociados.*

Lema 2.2. *Sea A un DFU. Todo elemento irreducible es primo.*

Demostración.
Dado un $p \in A$ irreducible tal que $p|ab$ donde $a, b \in A$ entonces existe $t \in A$ tal que $a \cdot b = p \cdot t$.
Como A es un DFU tenemos que

$$a = a_1 \cdot a_2 \cdot \ldots \cdot a_r$$
$$b = b_1 \cdot b_2 \cdot \ldots \cdot b_s$$
$$t = t_1 \cdot t_2 \cdot \ldots \cdot t_n$$

entonces

$$a_1 \cdot a_2 \cdot \ldots \cdot a_r \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_s = p \cdot t_1 \cdot t_2 \cdot \ldots \cdot t_n$$

Luego p es asociado a algún a_i o b_j.
Supongamos que p y a_i son asociados entonces $a_i = u \cdot p$ donde u es una unidad.
De donde $p|a_i$ y como $a_i|a$ entonces

$$p|a$$

Por lo tanto

$$p \text{ es primo.}$$

□

Definición 2.9. *Diremos que A cumple la condición de cadena ascendente (CCA) para ideales pricipales, si para toda sucesión estrictamente creciente $(I_n)_{n\in\mathbb{Z}^+}$ de ideales principales existe $k \in \mathbb{Z}^+$ tal que $I_n = I_k$ para todo $n \geq k$.*

Proposición 2.8. *A es un DFU si y sólo si A es DMCD y cumple CCA para ideales principales.*

Demostración.

$\Rightarrow$)

Sean $a, b \in A^*$ no unidades.

Sea $a = p_1 \dots p_r$ y $b = q_1 \dots q_s$ escritos como producto de irreducibles de A.

Consideremos el conjunto D de los p_i tales que existe un q_j tal que $p_i \sim q_j$.

Primer Caso

Si $D = \emptyset$

Afirmamos que $\text{mcd}(a, b) = 1$, veamos

Sea $u \in A$ tal que $u|a$ y $u|b$ y supongamos que u no es unidad.

Luego sea $t \in A$ tal que $t|u$ y t es irreducible, entonces $t|a$ y $t|b$ y por lo tanto

$$t \text{ divide a algún } p_i \text{ y algún } q_j,$$

y como p_i, q_j, t son irreducibles, entonces tenemos que

$$t \sim p_i \text{ y } t \sim q_j$$

de donde sigue que $p_i \sim q_j$ y de la definición de D tenemos que $p_i \in D$,

lo cual es una contradicción.

Por tanto

$$u \text{ es unidad y } mcd(a, b) = 1.$$

Segundo Caso

Si $D \neq \emptyset$

Tomemos $d = \prod_{p \in D} p$, veamos

Como d está formado por algunos p_i, donde p_i y p_j no son asociados para todo $i \neq j$, entonces $d|a$, y como los $p_i \sim q_j$ para algunos q_j tenemos que $d|b$.

Es decir

$$d|a \text{ y } d|b$$

Sea $e \in A$ tal que $e|a$ y $e|b$.

Denotaremos $e = r_1 \dots r_t$ como producto de irreducibles, donde $t < r$.

Ahora $r_1|a$ y $r_1|b$, entonces r_1 divide a algunos p_i y q_j, y como r_1, p_i, q_j son irreducible tenemos que

$$r_1 \sim p_i \text{ y } r_1 \sim q_j.$$

Ahora $r_2 \dots r_t | p_1 \dots p_{i-1} p_{i+1} \dots p_r$ y $r_2 \dots r_t | q_1 \dots q_{j-1} q_{j+1} \dots q_s$, de donde r_2 divide a algunos p_k y q_l, con $p_k \neq p_i$ y $q_l \neq q_j$.
Además como r_2, p_k, q_l son irreducible tenemos que

$$r_2 \sim p_k \text{ y } r_2 \sim q_l.$$

Continuando así, cada r_i está asociado a algún $p_j \in D$
Es decir

$$\begin{aligned} r_1 &\sim p_1 \\ r_2 &\sim p_2 \\ r_3 &\sim p_3 \\ &\vdots \\ r_t &\sim p_t \end{aligned}$$

En conclusión

$$r_1 \cdot r_2 \cdot \ldots \cdot r_t \sim p_1 \cdot p_2 \cdot \ldots \cdot p_t$$

y como

$$p_1 \cdot p_2 \cdot \ldots \cdot p_t \mid p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

Entonces

$$e|d$$

Por tanto

$$d = mcd(a, b)$$

En consecuencia de la Proposición 3.3 sabemos que todo cuerpo de fracciones de un DFU posee al menos una norma y por la Proposición 3.2 tenemos que si existe una norma entonces se cumple la CCA para ideales principales.
Por lo tanto

A cumple la CCA para ideales Principales

$\Leftarrow$)

Sea $a \in A^*$ no unidad.

Probemos primero que a tiene al menos un factor irreducible.

En efecto

Si a es irreducible, hemos terminado.

Si a no es irreducible, entonces $a = a_1 b_1$ con $a_1, b_1 \in A$ no unidades.

Como $a_1 | a$ y no son asociados, tenemos

$$aA \subset a_1 A.$$

Siguiendo este procedimiento y comenzando ahora por a_1.

Si a_1 es irreducible, hemos terminado.

Si a_1 no es irreducible, entonces $a_1 = a_2 b_2$ con $a_2, b_2 \in A$ no unidades.

Como $a_2 | a_1$ y no son asociados, tenemos

$$aA \subset a_1 A \subset a_2 A.$$

De manera análoga obtenemos una cadena de ideales principales estrictamente creciente

$$aA \subset a_1 A \subset a_2 A \subset \ldots,$$

por la CCA, esta cadena termina en algún $a_r A$ y a_r debe ser irreducible.

Así a_r es factor irreducible de a.

Ahora probemos que a es producto de irreducibles.

Si a es irreducible, hemos terminado.

Si a no es irreducible, entonces decimos que $a = p_1 c_1$ con $p_1, c_1 \in A$, donde p_1 es irreducible y c_1 no es unidad.

Como $p_1 | a$ pero no son asociados, tenemos

$$aA \subset c_1 A.$$

Siguiendo con este procedimiento y comenzando ahora con c_1

Si c_1 es irreducible, hemos terminado.

Si c_1 no es irreducible, entonces decimos que $c_1 = p_2 c_2$ con $p_2, c_2 \in A$, donde p_2 es irreducible y c_2 no es unidad.

Como $p_2 | a$ pero no son asociados, tenemos

$$aA \subset c_1 A \subset c_2 A.$$

De manera análoga obtenemos una cadena de ideales principales estrictamente creciente

$$aA \subset c_1A \subset c_2A \subset \ldots,$$

Nuevamente por la CCA, esta cadena termina en algún c_rA, con c_r irreducible. Luego,

$$\begin{aligned} a &= p_1c_1 \\ &= p_1p_2c_2 \\ &= \vdots \\ &= p_1p_2\ldots p_{r-1}c_{r-1} \\ &= p_1p_2\ldots p_{r-1}p_rc_r. \end{aligned}$$

es producto de elementos irreducibles de A.

Ahora sea $a = p_1 \ldots p_r = q_1 \ldots q_s$ con p_i, q_j irreducibles.
Supongamos que $s > r$.
Como A es DMCD, y por la proposición 2.6 de la sección anterior sabemos que, todo elemento irreducible es primo, entonces p_i, q_j son elementos primos.
Inmediatemente tenemos que $p_1|(q_1 \ldots q_s)$, entonces $p_1|q_{j_1}$ para algún j_1.
Al intercambiar, si es necesario, el orden de las q_j, podemos suponer que $j_1 = 1$.
Entonces $q_1 = p_1u_1$ y como p_1 es un irreducible, u_1 es unidad, de modo que p_1 y q_1 son asociados.
Tenemos así

$$p_1p_2\ldots p_r = p_1u_1q_2\ldots q_s$$

entonces

$$p_2\ldots p_r = u_1q_2\ldots q_s$$

Al continuar este proceso, comenzando por p_2 y así sucesivamente, se obtiene

$$1 = u_1u_2\ldots u_rq_{r+1}\ldots q_s$$

donde $u_1, \ldots u_r$ son unidades.
Obtenemos así que q_s es unidad, lo cual es una contradicción ya que
q_s es irreducible.
Si suponemos que $r > s$, mediante el mismo procedimiento anterior, trabajando

con los q_j esta vez, obtenemos que p_r es unidad, lo cual tambien es una contradicón. Por tanto

$$r = s.$$

Mediante el mismo procedimiento obtenemos que $p_i \sim q_i$ (después de la reoordenación).

Por tanto A es un DFU. □

Corolario 2.1. *Todo DIP es DFU.*

Demostración.
Sea A un DIP, entonces por la proposición 2.7 de esta sección sabemos que todo DIP es un DMCD, es decir, A es DMCD.
Sea $(I_i)_{i\in\mathbb{Z}^+}$ cadena ascendente de ideales principales de A.
Consideremos $I = \bigcup_{i\in\mathbb{Z}^+} I_i$, es rutinario probar que I es ideal.
Además como A es un DIP y todo ideal de A es un ideal principal, tenemos que existe un $a \in A$ tal que $I = aA$.
Como $a \in I$ existe $r \in \mathbb{Z}^+$ tal que $a \in I_r$, entonces

$$aA \subseteq I_r \subseteq I_n \subseteq I = aA, \forall n \geq r,$$

Por lo tanto, para todo $n \geq r$, tenemos que

$$I_r = I_n$$

Así el conjunto de ideales principales (todos los ideales) de A cumple CCA.
Aplicando la proposicipn anterior tenemos que

$$A \text{ es un DFU.}$$

□

Capítulo 3

Caracterización de los DIP y DFU

A través del tiempo uno de los principales objetivos de la Matemática ha sido buscar varias formas de caracterizar un mismo objeto matemático, y por medio de estas caracterizaciones optimizar su uso y/o entendimiento. Aplicaremos este fructífero enfoque al estudio de los Dominios de Ideales Principales (DIP) y los Dominios de Factorización Única (DFU), los cuales serán caracterizados por medio de nociones equivalentes a sus conocidas definiciones.

3.1. Norma en los DIP y DFU

En ésta sección daremos algunas nociones de normas y presentaremos una norma en especial que nos permita caracterizar los DIP y DFU, y para ello tendremos que mostrar que dicha norma esta bien definida y algunos resultados previos que son vitales para nuestra caracterización.

Definición 3.1. *La aplicación $N : K \to \mathbb{Q}$ es llamado norma sobre K si:*

(i) $N(x) \geq 0$, $\forall x \in K$

(ii) $N(x) = 0$ *si y sólo si* $x = 0$

(iii) $N(xy) = N(x)N(y)$, $\forall x, y \in K$

(iv) $N(a) \in \mathbb{Z}$, $\forall a \in A$

(v) Para $a \in A$, *a es unidad de A si y sólo si* $N(a) = 1$

Proposición 3.1. *Sea N una norma sobre K. Se cumple:*

1. $N(x/y) = N(x)/N(y)$ *para cada* $x, y \in K^*$,
2. *si* $a, b \in A$ *y* $aA \subset bA$ *entonces* $N(b) < N(a)$.

Demostración.

1. Tenemos que

$$\begin{aligned} N(x) &= N((x/y)y) \\ &= N(x/y)N(y). \end{aligned}$$

   Entonces

$$N(x/y) = N(x)/N(y).$$

2. Como $aA \subset bA$ tenemos que $a \in bA$ entonces existe $c \in A^*$ no unidad tal que

$$a = bc$$

   además como c no es nulo ni unidad, tenemos que $N(c) > 1$.
   Entonces

$$\begin{aligned} N(a) &= N(b)N(c) \\ &> N(b) \cdot 1 \\ &= N(b) \end{aligned}$$

   Por lo tanto

$$N(a) > N(b).$$

□

Proposición 3.2. *Si existe una norma N sobre K, entonces A cumple CCA para ideales principales.*

Demostración.
Sea $(a_nA)_{n\in\mathbb{Z}^+}$ una familia creciente de ideales principales.
Es decir

$$a_1A \subset a_2A \subset a_3A \subset \ldots,$$

Luego por la Proposición anterior, tenemos la siguiente sucesión

$$\ldots \leq N(a_3) \leq N(a_2) \leq N(a_1),$$

donde $N(a) \in \mathbb{Z}^+$, para todo $a \in A^*$.
Por otro lado, sabemos que todo conjunto no vacío de enteros positivos posee un mínimo.
Entonces existe $k \in \mathbb{Z}^+$ tal que $N(a_k)$ es el menor término de dicha sucesión, pero como la sucesión es de infinitos términos tenemos que

$$N(a_n) = N(a_k) \text{ para todo } n \geq k.$$

Supongamos que $a_kA \subset a_nA$, con $n > k$
entonces

$$N(a_n) < N(a_k)$$

lo cual es imposible, dado que $N(a_n) = N(a_k)$.
entonces

$$a_nA = a_kA \text{ para todo } n \geq k.$$

Por lo tanto

$$A \text{ cumple CCA para ideales principales.}$$

□

Proposición 3.3. *Sea A un DFU, para cada $a \in A^*$ denotaremos $w(a)$ el total de factores irreducibles en su descomposición como producto de factores irreducibles. Entonces:*

1. *Para $a \in A^*$, $w(a) = 0$ si y sólo si a es unidad.*
2. *Para todo $a, b \in A^*$, $w(ab) = w(a) + w(b)$.*

Demostración.

1. Para cada $a \in A^*$, a es no unidad, si y sólo si, existe un irreducible que divide a a esto es, si y sólo si, $w(a) \geq 1$.
2. Sean $a = p_1 \cdot p_2 \ldots p_r$ y $b = q_1 \cdot q_2 \ldots q_s$ con p_i, q_j irreducibles de A y donde $w(a) = r$ y $w(b) = s$, entonces

$$ab = p_1 \ldots p_r q_1 \ldots q_s$$

luego

$$\begin{aligned} w(ab) &= r + s \\ &= w(a) + w(b). \end{aligned}$$

□

Proposición 3.4. *Todo cuerpo de fracciones de un DFU posee al menos una norma.*

Demostración.
Sea A un DFU y K su cuerpo de fracciones.
Definiremos la aplicación $N : K \to \mathbb{Q}$ como sigue: dado un $x \in K$.
Si $x = 0$, entonces $N(x) = 0$.
Si $x \neq 0$, entonces existen $a, b \in A^*$ tal que $x = a/b$, donde

$$N(x) = 2^{w(a)-w(b)}.$$

N es bien definida:
Si $x = a/b = a'/b' \in K^*$ con $a, b, a', b' \in A^*$, entonces $ab' = a'b$. De donde

$$\begin{aligned} w(ab') &= w(a'b) \\ \Rightarrow w(a) + w(b') &= w(a') + w(b) \\ \Rightarrow w(a) - w(b) &= w(a') - w(b') \\ \Rightarrow 2^{w(a)-w(b)} &= 2^{w(a')-w(b')} \end{aligned}$$

N es una norma sobre K:

1. Si $x = 0$ entonces $N(0) = 0$.
   Si $x = a/b \neq 0$ con $a, b \in A^*$, entonces

$$N(x) = 2^{w(a)-w(b)} \geq 0.$$

2. $\Rightarrow$)
   Si $x = a/b \neq 0$ con $a, b \in A^*$, entonces

$$N(x) = 2^{w(a)-w(b)} \neq 0.$$

   $\Leftarrow$)
   $N(0) = 0$.

3. Si $x = 0$ ó $y = 0$ tenemos

$$N(x) \cdot N(y) = N(xy) = 0$$

   Si $x \neq 0, y \neq 0$, existen $a, b, c, d \in A^*$ tal que $x = a/b,\ y = c/d$, luego

$$\begin{aligned} N(x)N(y) &= 2^{w(a)-w(b)}2^{w(c)-w(d)} \\ &= 2^{w(a)+w(c)-(w(b)+w(d))} \\ &= 2^{w(ac)-w(bd)} \\ &= N(ab/cd) \\ &= N((a/c)(b/d)) \\ &= N(xy) \end{aligned}$$

4. Como $a = a/1$, entonces

$$N(a) = 2^{w(a)-w(1)} = 2^{w(a)} \in \mathbb{Z}.$$

5. a es unidad si y sólo si $w(a) = 0$ si y sólo si $N(a) = 2^{w(a)} = 1$.

Por tanto N es una norma sobre K. □

3.2. Caracterización de los DIP

En esta sección caracterizaremos los Dominios de Ideales Principales, a través de condiciones necesarias y suficientes, con esto tendremos una herramienta que nos permite verificar o descartar que un dominio es un DIP.

Teorema 3.1. *Sea A un Dominio de Integridad y si existe una norma N sobre K tal que satisface la condición:*
Dado $x \in K \setminus A$ existen $\alpha, \beta \in A$ tal que

$$0 < N(\alpha x - \beta) < 1.$$

Entonces A es DIP.

Demostración.
Sea I ideal no nulo de A. Consideremos el conjunto

$$S = \{N(a),\ a \in I^*\}.$$

Sea $d \in I^*$ tal que $N(d) = \text{mín}\, S$.

Ahora probaremos que $dA = I$

Como $d \in I$ tenemos $dA \subseteq I$. Nos falta mostar que $I \subseteq dA$
Veamos dado un $e \in I$.
Supongamos que d " no divide a" e, es decir, no existe $c \in A$ tal que

$$e = dc,$$

entonces

$$e|d \notin A.$$

Por hipótesis existe $\alpha, \beta \in A$ tal que

$$0 < N\left(\left(\frac{e}{d}\right)\alpha - \beta\right) < 1,$$

luego

$$N\left(\left(\frac{e}{d}\right)\alpha - \beta\right) = N\left(\frac{e\alpha - \beta d}{d}\right) = \frac{N(e\alpha - \beta d)}{N(d)} < 1,$$

de donde

$$N(e\alpha - \beta d) < N(d)$$

y como $e\alpha - \beta d \in I$ ya que $e, d \in I$, contradice que

$$N(d) = \min S.$$

Así

$$d|e$$

Además tenemos que $e \in dA$ para todo $e \in I$, entonces

$$I = dA$$

Es decir, es un Dominio de Ideales Principales.
Por tanto

$$A \text{ es un DIP.}$$

□

Es importante mencionar que en la demostración de la condición necesaria, utilizamos la definición de norma en un sentido general, es decir no requerimos de una norma especifíca, para que este teorema tenga validez.

Teorema 3.2. *Si A es un DIP y $N : K \to \mathbb{Q}$ norma sobre K, entonces satisface la condición:*
Dado $x \in K \setminus A$ existen $\alpha, \beta \in A$ tal que

$$0 < N(\alpha x - \beta) < 1.$$

Demostración.
Como A es un DIP y por el Corolario 2.1 , tenemos que A es un DFU.
Dados $a, b \in A^*$ tal que

$$x = a/b \in K \setminus A$$

Luego de la Proposición 2.7 sabemos que A es un DMCD, es decir, que todo par de elementos de A tienen máximo común divisor.
Entonces diremos que

$$d = mcd(a, b)$$

de donde

$$\text{existen } u, v \in A^* \text{ tal que } a = du, b = dv.$$

Luego de la Proposición 2.5 tenemos que

$$1 = mcd(a/d, b/d) = mcd(u, v),$$

además

$$x = a/b = (du)/(dv) = u/v.$$

Supongamos que v fuese unidad de A, entonces tendríamos que

$$x = u/v = uv^{-1} \in A,$$

lo que contradice la hipótesis.
Por lo tanto $v \in A^*$ y como no es unidad, tenemos que dado una norma cualquiera

$$N(v) > 1.$$

Además gracias a la Proposición 2.7 sabemos que
Para $u, v \in A$ existen $\alpha, \beta \in A$ tal que

$$mcd(u, v) = \alpha u + (-\beta)v$$

y como el $mcd(u, v) = 1$, tenemos que

$$\alpha u + (-\beta)v = 1$$

De donde

$$\alpha x - \beta = \alpha\left(\frac{u}{v}\right) - \beta = \frac{\alpha u - \beta v}{v} = \frac{1}{v} \neq 0,$$

entonces

$$0 < N(\alpha x - \beta) = N\left(\frac{1}{v}\right) = \frac{N(1)}{N(v)} = \frac{1}{N(v)} < 1.$$

Por lo tanto

$$0 < N(\alpha x - \beta) < 1.$$

□

3.3. Caracterización de los DFU

En esta sección presentaremos algunas definiciones y propiedades de gran importancia en la caracterización de los Dominios de Factorización Única.

Definición 3.2. *Sea R un anillo cualquiera, un conjunto no vacío M se dice que es un R-módulo (o un módulo sobre R) si M es un grupo abeliano bajo la operación $+$, tal que para cada $r \in R$ y $m \in M$ existe un elemento $rm \in M$ de tal modo que se verifica:*

- $r(a+b) = ra + rb$
- $r(sa) = (rs)a$
- $(r+s)a = ra + sa$

Para cualquier $a, b \in M$ y $r, s \in R$.

Definición 3.3. *Un subgrupo aditivo A del R-módulo M se llama submódulo de M si siempre que $r \in R$ y $a \in A$ tenemos que $ra \in A$.*

Definición 3.4. *Sea I un A-submódulo no nulo de K, diremos que I es un ideal fraccionario de A si existe $d \in A^*$ tal que $dI \subseteq A$.*

Ejemplo 3.1.

- *Todo A-submódulo finitamente generado es un ideal fraccionario.*
  En Efecto
  Sea I un A-submódulo finitamente generado, y sea

$$\left\{\frac{a_1}{b_1}, \cdots, \frac{a_n}{b_n}\right\}$$

conjunto A-generador de I con $a_i, b_i \in A$, donde $b_i \neq 0$.

Tomemos $d = b_1 \cdot ... \cdot b_n \neq 0$.

Sea $\alpha \in I$ entonces existen $\alpha_1, ..., \alpha_n \in A$ tal que

$$\alpha = \sum_{i=1}^{n} \alpha_i \left(\frac{a_i}{b_i}\right)$$

luego

$$\begin{aligned} d\alpha &= d\sum_{i=1}^{n} \alpha_i \left(\frac{a_i}{b_i}\right) \\ &= \sum_{i=1}^{n} \alpha_i \left(\frac{da_i}{b_i}\right) \\ &= \sum_{i=1}^{n} \alpha_i b_1 ... b_{i-1} b_{i+1} ... b_n a_i \\ &\in A \end{aligned}$$

luego $dI \subset A$.

Por lo tanto

I es un ideal fraccionario

- *Todo ideal I (en el sentido usual) de A , es un A-submódulo debido a que $A \subseteq K$ y $1I = I \subseteq A$.*

De aqui en adelante los ideales fraccionarios serán llamados simplemente ideales.

Definición 3.5. *Dados I, J, I_α A-submódulos no nulos de K y $a \in K$ definiremos:*

$$\sum_\alpha I_\alpha = \left\{ \sum_\alpha a_\alpha \ / \ a_\alpha \in I_\alpha \text{ y } a_\alpha \neq 0 \text{ sólo para una cantidad finita de } \alpha's \right\}$$

$$IJ = \left\{ \sum_{\alpha}^{n} a_i b_i \ / a_i \in I, b_i \in I \text{ para todo } i = 1, 2, ..., n \text{ donde } n \in \mathbb{Z}^+ \right\}$$

$$aI = \{ab / b \in I\}$$

$$(I : J) = \{x \in K / xJ \subseteq I\}$$

Proposición 3.5. *Dados I, J, L A-submódulos no nulos de K y $a \in K^*$, entonces:*

1. *$(I : J)$ es un A-submódulo de K,*
2. *$L \subseteq (I : J)$ si y sólo si $LJ \subseteq I$*
3. *$(I : J)J \subseteq I$*
4. *Sea I un ideal de A y $J \neq 0$ entonces $(I : J)$ es un ideal de A*
5. *$(I : aA) = a^{-1}I$*
6. *$(I : aJ) = (a^{-1}I : J) = a^{-1}(I : J)$*
7. *Si $I \subseteq J$ entonces $(L : J) \subseteq (L : I)$*

Demostración.

1. Sea $x, y \in (I : J)$ y $\alpha \in A$ entonces $xJ, yJ \subseteq I$ de donde

$$(x + \alpha y)J = xJ + \alpha(yJ) \subseteq I + \alpha I \subseteq I.$$

2. Como $L \subseteq (I : J)$ si y sólo si $x \in (I : J)$ para todo $x \in L$ si y sólo si $xJ \subseteq I$ para todo $x \in L$ si y sólo si $LJ \subseteq I$

3. Del item anterior, con $L = (I : J)$

4. Tomemos $y \in J^*$ y como I es un ideal fraccionario de A tenemos que dado $x \in K^*$ se tiene que $xI \subseteq A$. Entonces $xy \neq 0$ tal que

$$(xy)(I : J) = x(I : J)y \subseteq xI \subseteq I \subseteq A.$$

   Por lo tanto $(I : J)$ es ideal A.

5. $x \in (I : aA) \iff a(xA) = x(aA) \subseteq I \iff xA \subseteq a^{-1}I \iff x \in a^{-1}I.$

6. Sea $x \in K^*$
   Veamos que $(I : aJ) = (a^{-1}I : J)$
   $x \in (I : aJ) \iff a(xJ) = x(aJ) \subseteq I \iff xJ \subseteq a^{-1}I \iff x \in (a^{-1}I : J).$
   Veamos que $(I : aJ) = a^{-1}(I : J)$
   $x \in (I : aJ) \iff a(xJ) = (ax)J \subseteq I \iff ax \in (I : J) \iff x \in a^{-1}(I : J).$

7. $x \in (L : J)$ entonces $xJ \subseteq L$ entonces $xI \subseteq xJ \subseteq L$ entonces $x \in (L : I)$

□

Definición 3.6. *Sea A es un Dominio e I un ideal de A. Definimos la clausura divisorial de I como $\bar{I} = (A : (A : I))$. Diremos que I es ideal divisorial si $I \neq 0$, $I \neq K$ y $\bar{I} = I$.*

Proposición 3.6. *Sean I, J ideales no nulos de A, entonces :*

1. $I \subseteq \bar{I}$
2. *Si $I \subseteq J$ entonces $\bar{I} \subseteq \bar{J}$*
3. $\bar{A} = A$
4. $\overline{aI} = a\bar{I}$ *para todo* $a \in K^*$
5. $\bar{\bar{I}} = \bar{I}$

Demostración.

1. $x \in I$ entonces $xy \in A$ para todo $y \in (A : I)$ entonces $x(A : I) \subseteq A$ entonces $x \in (A : (A : I)) = \bar{I}$.

2. Tenemos que $(A : J) \subseteq (A : I)$ luego

$$\bar{I} = (A : (A : I)) \subseteq (A : (A : J)) = \bar{J}$$

3. Ya tenemos que $A \subseteq \bar{A}$.
   Sea $x \in \bar{A} = (A : (A : A))$ entonces $xy \in A$ para todo $y \in (A : A)$,
   como $1a = a \in A$ para todo $a \in A$, esto es, $a \in (A : A)$, tomando $y = 1$ tenemos que $x \in A$, entonces $\bar{A} \subseteq A$.
   Por lo tanto

$$\bar{A} = A$$

4. $\overline{aI} = (A : (A : aI)) = (A : a^{-1}(A : I)) = (a^{-1})^{-1}(A : (A : I)) = a\bar{I}$

5. Como $(A : I) \subseteq \overline{(A : I)}$, se sigue

$$\bar{\bar{I}} = (A : (A : (A : (A : I)))) = (A : \overline{(A : I)}) \subseteq (A : (A : I)) \subseteq \bar{I}$$

Además $\bar{I} \subseteq \bar{\bar{I}}$.
Por lo tanto

$$\bar{\bar{I}} = \bar{I}$$

□

Teorema 3.3. *A es DFU si y sólo si existe una norma N sobre K que satisface la siguiente condición:*
Dados $a, b \in A^*$ tal que $a \not| b$ y $b \not| a$, entonces existe $c \in \left(\overline{aA + bA}\right)^*$ con

$$N(c) < \text{mín}\{N(a), N(b)\}.$$

Demostración.
$\Rightarrow$)
Como A es un DFU entonces por la Proposición 2.8 tenemos que A es un DMCD, de donde decimos que dados $a, b \in A^*$ tenemos que

$$c = \text{mcd}(a, b).$$

Es decir,

$$\text{existen } u, v \in A \text{ tal que } a = cu, b = cv.$$

Si u fuese unidad.
Tendríamos que $b = au^{-1}v$ lo que contradice que $a \not| b$ entonces u no es unidad.
De manera análoga, v no es unidad.
Es decir que

$$\text{ni } u \text{ ni } v \text{ son unidades.}$$

Por otro lado, como a, b no pueden ser nulos, entonces

$$\text{tampoco } u, v \text{ pueden ser nulos.}$$

De donde $u, v \in A^*$ y como son no unidades, tenemos que dada una norma cualquiera

$$N(u) > 1 \text{ y } N(v) > 1$$

Por lo tanto

$$\begin{aligned} N(a) &= N(cu) = N(c)N(u) > N(c) \\ N(b) &= N(cv) = N(c)N(v) > N(c) \end{aligned}$$

Así

$$N(c) < \text{mín}\{N(a), N(b)\}.$$

$\Leftarrow$)

Sean $a, b \in A^*$, luego

$$\overline{aA + bA} \subseteq \overline{A} = A,$$

así el conjunto

$$S = \left\{ N(x) \ / \ x \in \left(\overline{aA + bA}\right)^* \right\}$$

es un subconjunto no vacío de $\mathbb{Z}^+$.

Además como sabemos que todo conjunto no vacío de enteros positivos posee un mínimo.

Podemos tomar un $c \in \left(\overline{aA + bA}\right)^*$ tal que $N(c) = \text{mín}\, S$.

Probaremos que $\overline{aA + bA} = cA$.

Sea $e \in \overline{aA + bA}$.

Afirmaremos que $e \not| c$.

Pero si sucediera que $e|c$, por la Proposición 2.2 tendríamos que $cA \subset eA$ y por la Proposición 3.1 concluimos que $N(e) < N(c)$, lo cual es absurdo ya que $N(c) = \text{mín}\, S$.

Por lo tanto

$$e \not| c.$$

Supongamos que $c \not| e$

Por hipótesis tenemos que existe $f \in \left(\overline{eA + cA}\right)^*$ tal que

$$N(f) < \text{mín}\{N(e), N(c)\} = N(c).$$

Como $e, c \in \overline{aA + bA}$ y como $eA + cA \subseteq \overline{aA + bA}$ tenemos que

$$\overline{eA + cA} \subseteq \overline{\overline{aA + bA}}$$

Luego

$$f \in \overline{eA + cA} \subseteq \overline{\overline{aA + bA}} = \overline{aA + bA},$$

lo que es una contradicción con $N(c) = \text{mín}\, S$.

Por lo tanto

$$c|e$$

Es decir, para todo $e \in \overline{aA+bA}$ tenemos que $e \in cA$ entonces $\overline{aA+bA} \subset cA$
De donde tenemos que

$$\overline{aA+bA} = cA.$$

Probemos ahora que $c = \text{mcd}(a,b)$.
Como

$$aA \subseteq aA+bA \subseteq \overline{aA+bA} = cA,$$
$$bA \subseteq aA+bA \subseteq \overline{aA+bA} = cA$$

se tiene que $c|a$ y $c|b$.
Sea $d \in A$ tal que $d|a$ y $d|b$, luego $aA, bA \subseteq dA$, entonces

$$cA = \overline{aA+bA} \subseteq \overline{dA} = d\overline{A} = dA,$$

esto es $d|c$
Así

$$c = \text{mcd}(a,b).$$

Por tanto

$$A \text{ es un DMCD.}$$

Como N es una norma sobre K, por la Proposición 3.2 tenemos que A cumple CCA para ideales principales.
Finalmente gracias a la Proposición 2.8

$$A \text{ es un DFU.}$$

□

Capítulo 4

Aplicaciones

A modo de validar y mostrar la utilidad del presente trabajo las primeras aplicaciones serán dos resultados conocidos:

- $\mathbb{Z}$ es un Dominio de Factorización Única.
- $K[x]$, donde K es un cuerpo, es un Dominio de Ideales Principales.

Muchas de estas caracterizaciones son utilizadas no solo para probar que un Dominio es un Dominio de Ideales Principales o Dominio de Factorización Única sino para descartar que un Dominio no cumple dichas características.
Por ello presentamos los casos siguientes:

- $\mathbb{Z}[\sqrt{10}]$ no es un Dominio de Ideales Principales.
- $\mathbb{Z}[x]$ no es Dominio de Ideales Principales.

En esta última aplicación haremos una comparación entre el método usual y la caracterización de los DIP.

4.1. $\mathbb{Z}$ es DFU.

Como el cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.

Definimos la norma

$$\begin{aligned} N \ : \ \mathbb{Q} &\longrightarrow \mathbb{Q} \\ x &\longmapsto |x| \end{aligned}$$

Como el valor absoluto usual. Sean $a, b \in \mathbb{Z}^*$ tal que $a \not| b$ y $b \not| a$, es decir,

ni a ni b pueden ser unidades

Sea $\text{mcd}(a, b) = k > 0$

entonces existen $\alpha, \beta \in \mathbb{Z}$ tal que $k = \alpha a + \beta b$, de donde $a\mathbb{Z} + b\mathbb{Z} = k\mathbb{Z}$, luego

$$\overline{a\mathbb{Z} + b\mathbb{Z}} = \overline{k\mathbb{Z}} = k\overline{\mathbb{Z}} = k\mathbb{Z}$$

así tomamos $k \in k\mathbb{Z}^* = (\overline{a\mathbb{Z} + b\mathbb{Z}})^*$.

Por otro lado

$$a = a_1 k \ \text{ y } \ b = b_1 k \ \text{ con } a_1, b_1 \in \mathbb{Z}$$

entonces a_1 no divide b_1 y b_1 no divide a a_1, (por la propiedad de a y b).

Así a_1, b_1 no son unidades, tenemos que

$$N(a_1) > 1 \ y \ N(b_1) > 1$$

Entonces

$$\begin{aligned} \text{mín}\{N(a), N(b)\} &= \text{mín}\{N(a_1 k), N(b_1 k)\} \\ &= \text{mín}\{N(a_1)N(k), N(b_1)N(k)\} \\ &= N(k)\,\text{mín}\{N(a_1), N(b_1)\} \\ &> N(k) \end{aligned}$$

Por lo tanto

$\mathbb{Z}$ es un DFU.

4.2. $K[x]$ es un DIP.

Consideremos la siguiente norma en $K(x)$, el cuerpo de fracciones de $K[x]$:

$$\begin{array}{rccc} N & : & K(x) & \longrightarrow & \mathbb{Q} \\ & & \dfrac{f(x)}{g(x)} & \longrightarrow & 2^{grad\, f(x) - grad\, g(x)} \end{array}$$

Sea $\dfrac{f(x)}{g(x)}$ un elemento cualquiera de $K(x) \setminus K[x]$ con

$$f(x) = a_0 + ... + a_n x^n \ , \ a_n \neq 0$$
$$g(x) = b_0 + ... + b_m x^m \ , \ b_m \neq 0$$

Por el teorema 3.3 queremos hallar $\alpha(x)$, $\beta(x)$ en $K[x]$ tal que

$$0 < N\left(\alpha(x) \cdot \frac{f(x)}{g(x)} - \beta(x)\right) < 1$$

Luego por el algoritmo de la división existen únicos $q(x), r(x)$ en $K[x]$ tales que

$$f(x) = q(x) \cdot g(x) + r(x)$$

de donde

$$grad\, r(x) < grad\, g(x)$$

Tomando entonces

$$\alpha(x) = 1 \ y \ \beta(x) = q(x).$$

Asi

$$\begin{aligned} N\left(\alpha(x) \cdot \frac{f(x)}{g(x)} - \beta(x)\right) &= N\left(\alpha(x) \cdot \frac{q(x)g(x) + r(x)}{g(x)} - \beta(x)\right) \\ &= N\left(\frac{r(x)}{g(x)}\right) \\ &= 2^{grad\, r(x) - grad\, g(x)} \end{aligned}$$

entonces

$$0 < 2^{grad\, r(x) - grad\, g(x)} < 1$$

Por lo tanto

K[x] es DIP.

4.3. $\mathbb{Z}[\sqrt{10}]$ no es un DIP.

Como el cuerpo de fracciones de $\mathbb{Z}[\sqrt{10}]$ es $\mathbb{Q}(\sqrt{10})$.

Definimos la función

$$\begin{array}{rccc} N & : & \mathbb{Q}(\sqrt{10}) & \longmapsto & \mathbb{Q} \\ & & s+t\sqrt{10} & \longrightarrow & |s^2-10t^2| \end{array}$$

Veamos que N es una norma
En efecto.
Para todo $x, y \in \mathbb{Z}[\sqrt{10}]$ tenemos:

1. $N(x) = |x| \geq 0$
2. $N(x) = 0$ si y sólo si $|x| = 0$ si y sólo si $x = 0$
3. $N(xy) = |xy| = |x|\,|y| = N(x)N(y)$

Supongamos que $\mathbb{Z}[\sqrt{10}]$ es DIP.
Como $\sqrt{10}/2$ no esta en $\mathbb{Z}[\sqrt{10}]$, existen $x+y\sqrt{10}$ y $z+w\sqrt{10}$ en $\mathbb{Z}[\sqrt{10}]$ tal que

$$0 < N\left((\sqrt{10}/2)(x+y\sqrt{10}) - (z+w\sqrt{10})\right) < 1$$

$$0 < N(5y - z + (x/2 - w)\sqrt{10}) < 1$$

$$0 < |(5y-z)^2 - 10(x/2-w)^2| < 1$$

luego

$$0 < |2(5y-z)^2 - 5(x-2w)^2| < 2$$

entonces

$$2(5y-z)^2 - 5(x-2w)^2 = \pm 1.$$

Se sigue que

$$2z^2 = \pm 1 \bmod 5$$

Vemos que si:

$z = 0 \mod 5$ entonces $2z^2 = 0 \mod 5 \neq \pm 1 \mod 5$,
$z = 1 \mod 5$ entonces $2z^2 = 2 \mod 5 \neq \pm 1 \mod 5$,
$z = 2 \mod 5$ entonces $2z^2 = 8 \mod 5 = 3 \mod 5 \neq \pm 1 \mod 5$,
$z = 3 \mod 5$ entonces $2z^2 = 18 \mod 5 = 3 \mod 5 \neq \pm 1 \mod 5$,
$z = 4 \mod 5$ entonces $2z^2 = 32 \mod 5 = 2 \mod 5 \neq \pm 1 \mod 5$,

por tanto tal z no existe, y así

$$\mathbb{Z}[\sqrt{10}] \text{ no es un DIP.}$$

4.4. $\mathbb{Z}[x]$ no es DIP.

Método usual

Para esto consideremos el ideal

$$I = \{2p(x) + xq(x) \ : \ p(x), q(x) \in \mathbb{Z}[x]\}$$

es el ideal de todos los polinomios que tienen término constante par.
Supongamos que I es un ideal principal, digamos $I =< \alpha(x) >$, para algún $\alpha(x)$ no nulo en $\mathbb{Z}[x]$.
Como $2 \in I$, existe $\beta(x)$ en $\mathbb{Z}[x]$ tal que $2 = \beta(x)\alpha(x)$
donde

$$\begin{aligned} 0 &= grad(2) \\ &= grad(\beta(x)\alpha(x)) \\ &= \underbrace{grad(\beta(x))}_{\geq 0} + \underbrace{grad(\alpha(x))}_{\geq 0} \end{aligned}$$

Asi grad$(\alpha(x)) = 0$ y por tanto $\alpha(x)$ es una constante, más aún es par, luego $\alpha(x) \in I$, entonces $\alpha(x) = 2k$.
De otro lado, como $x \in I$, existe $\gamma(x)$ en $\mathbb{Z}[x]$ tal que

$$\begin{aligned} x &= \gamma(x)\alpha(x) \\ &= \gamma(x)(2k) \end{aligned}$$

de donde por cuestiones de grado

$$\gamma(x) = r + tx \ , \ t \neq 0$$

así

$$x = (2k)(r + tx) = 2kr + (2kt)x$$

de donde $2kt = 1$, es decir que, 2 pertenece a las unidades de $\mathbb{Z}[x]$, pero es conocido que las unidades de $\mathbb{Z}[x]$ son $\{1, -1\}$ entonces

$$2 \in \{1, -1\}$$

lo cual es absurdo. Por lo tanto

$$\mathbb{Z}[x] \text{ no es DIP}$$

$\mathbb{Z}[x]$ no es DIP .

Usando la Caracterización

Consideremos la siguiente norma en $\mathbb{Z}(x)$, el cuerpo de fracciones de $\mathbb{Z}[x]$:

$$\begin{array}{rccc} N & : & \mathbb{Z}(x) & \longmapsto & \mathbb{Q} \\ & & \dfrac{f(x)}{g(x)} & \longrightarrow & 2^{grad\, f(x) - grad\, g(x)} \end{array}$$

y $\dfrac{f(x)}{g(x)}$ en $\mathbb{Z}(x) \setminus \mathbb{Z}[x]$ donde

$$f(x) = a_0 + ... + a_n x^n \ , \ a_n \neq 0, \ a_n \in \mathbb{Z}$$
$$g(x) = b_0 + ... + b_m x^m \ , \ b_m \neq 0, \ b_m \in \mathbb{Z}$$

Supongamos que $\mathbb{Z}[x]$ es DIP.
Entonces, dado $\dfrac{1}{2} \in \mathbb{Z}(x) \setminus \mathbb{Z}[x]$, existen $\alpha(x)$ y $\beta(x) \in \mathbb{Z}[x]$ tal que

$$0 < N(\alpha(x)\frac{1}{2} - \beta(x)) < 1$$

$$0 < N(\frac{\alpha(x) - 2\beta(x)}{2}) < 1$$

esto es,

$$0 < 2^{grad(\alpha(x) - 2\beta(x)) - grad(2)} < 1$$

$$0 < 2^{grad(\alpha(x) - 2\beta(x))} < 1$$

pero como $grad(\alpha(x) - 2\beta(x)) \geq 0$ tenemos una contradicción.
Por lo tanto

$\mathbb{Z}[x]$ no es DIP.

Materiales y Métodos

- Con respecto a los materiales, se ha usado textos especializados del tema de dominios de ideales principales y dominios de factorización única, así como también textos de pregrado de teoría de números y álgebra abstracta. El servicio de internet fue un importante apoyo en la búsqueda de material bibliográfico y papers.

- Para la digitación se ha usado el sistema de composición de textos LATEX para Windows, que es un poderoso editor de textos matemáticos de calidad, cuyo uso es prácticamente obligatorio en la escritura de cualquier tesis, libro o artículo matemático.

- La metodología usada en este trabajo es de tipo inductivo-deductivo, tratando de ser lo más exhaustivo posible en cada demostración para el mejor entendimiento de cada punto de la tesis.

Resultados y Aportes

Los principales resultados de esta tesis son:

- Definir una norma adecuada en los Dominio de Ideales Principales y Dominio de Factorización Única y mostrar su existencia. (Ver Proposición 3.4)
- Caracterizar mediante normas cualesquiera y condiciones necesarias y suficientes, los DFU y DIP. (Ver Teoremas 3.1 , 3.2 y 3.3)

Los aportes de tesis son:

- Proponer y demostrar una equivalencia a los DFU (Ver la Proposición 2.8) en un sentido diferente a las otras equivalencias existentes a los DFU veamos:
  - (Kaplansky) Un dominio R es un DFU si y solo si todo ideal primo principal contiene un elemento primo.
  - (Nagata) Un dominio R es un DFU si y solo si R verifica la condición de cadena ascendente sobre sus ideales principales y la localización $S^{-1}R$ es DFU, donde S es un conjunto multiplicativo generado por elementos primos.

  Como vemos todas estas equivalencias utilizan el concepto de ideal principal y/o el concepto de elemento primo en R. Un aporte de este trabajo es que las caracterizaciones establecidas son independientes de estos conceptos lo que hace más viable probar si un dominio es o no es un DFU, ya que no tenemos que saber de antemano cuales son los elementos primos de dicho dominio ni sus ideales.
- Desarrollar con todo detalle ejemplos y contraejemplos que son de difícil acceso en los libros estandar de pregrado.

Discusiones

- El presente trabajo puede ser generalizado a Dominios de Krull, donde el concepto de elemento primo es extendido al concepto de ideal primario y la noción de factorización en primos se extiende como descomposición primaria. En este caso una norma es definida sobre el conjunto de los ideales divisoriales del dominio. Estos temas no son tocados en esta tesis pero pueden encontrarse en el trabajo de Clifford S. Queen titulado FACTORIAL DOMAINS.

- Es sabido que toda norma induce una topología, por tanto todo DFU y todo DIP poseen una topología inducida por la norma existente por la Proposición 3.4. El estudio de las propiedades topológicas de un DFU ó un DIP, según esta topología puede ser campo para futuros trabajos de investigación.

Conclusiones

- El estudio de los DFU, los DIP y estructuras más generales como Dominios de Krull y Dominios de Dedekin siguen siendo un fructífero campo de investigación dentro de la Teoría de Números, disciplina llamada por Gauss "La Reina de las Matemáticas".

- Dar diversas caracterizaciones de un mismo objeto matemático no solo sirve para identificar aquellas estructuras que verifican dichas caracterizaciones sino que nos sirve, en la práctica, para descartar aquellas estructuras que no cumplen con dicha características (Ver las aplicaciones 4.3 y 4.4) siendo este un argumento muy usado en matemática.

- Cada nueva caracterización de un objeto matemático nos permite conocer mejor las propiedades intrínsecas del objeto en estudio, en este caso los DFU y DIP, nos abren distintas lineas de investigación con los diferentes enfoques de un mismo tema.

- Una de mis principales motivaciones ha sido que esta tesis, sirva como iniciativa para futuros estudios en el área, para los que tengan a bien leer este trabajo, ya que lo que se ha mostrado es tan sólo un paso del gran camino que nos falta por recorrer en el estudio de la matemática.

Bibliografía

[1] P. Samuel, 'Lectures on Unique Factorization' Yaya Institute of fundamental Research, Bombay, 1964.

[2] R. M. Fossum, 'The divisor Class Group of a Krull Domain', Ergeb. Math. Grenzgeb, Springer, Berlin, 1973.

[3] N. Bourbaki, 'Elements de Mathematique, Fascicule XIV, Algebre- Charpite 6, Charpite 7.' Hermann, Paris, 1962.

[4] N. Bourbaki, 'Elements de Mathematique, Fascicule XXXI, Algebre Conmutative - Charpite 7.' Hermann, Paris, 1965.

[5] Patrick Suppes, Teoría Axiomática de Conjuntos, Editorial Norma Cali-Colombia 1968.

[6] I. N. Herstein, álgebra abstracta, editorial Iberoamérica 1988.

[7] I. N. Herstein, álgebra Moderna, editorial Iberoamérica 1988.