ALGUNAS OBSERVACIONES SOBRE ANILLOS EUCLIDIANOS

MARIELA DEL CARMEN PÉREZ AGUILAR.

UNIVERSIDAD DE CARTAGENA.

FACULTAD DE CIENCIAS EXACTAS Y NATURALES.

PROGRAMA DE MATEMÁTICAS.

CARTAGENA, D.T Y C.

Octubre, 2010

ALGUNAS OBSERVACIONES SOBRE ANILLOS EUCLIDIANOS

MARIELA DEL CARMEN PÉREZ AGUILAR.

TRABAJO DE TESIS PARA OPTAR POR EL TÍTULO DE MATEMÁTICO

NESTOR RODRÍGUEZ VEGA
Asesor

UNIVERSIDAD DE CARTAGENA.
FACULTAD DE CIENCIAS EXACTAS Y NATURALES.
PROGRAMA DE MATEMÁTICAS.
CARTAGENA, D.T Y C.
2010

Índice General

Dedicado a

Mis padres...mis más grandes inspiradores.

Agradecimientos

⋆ A Dios por ser mi guía, mi protector, mi fortaleza y mi refugio.

⋆ A mis padres por apoyarme y motivarme cada instante de mi vida a seguir perseverando.

⋆ A mis hermanas por enseñarme a que con costancia y disciplina se logra lo que se desea.

⋆ A el profe Nestor Rodríguez Vega por su asesoría y sus concejos.

⋆ A esa personita muy especial que ocupa un lugar importante en mi corazón quien con su apoyo constante y sus concejos me incentiva a lograr el objetivo trazado.

⋆ A mi gran amigo José de los Santos Marrugo Pérez por su incondicionalidad y su cola boración.

Introducción

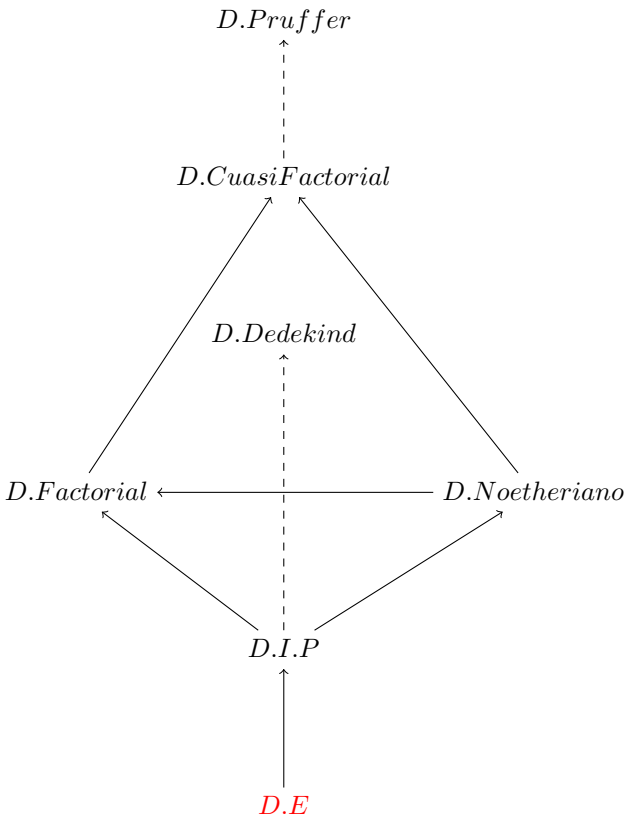
En el libro VII de los elementos de Euclides encontramos la siguiente proposición:

PROPOSICIÓN 1**:** " Dados dos números desiguales réstese sucesivamente el menor del ma yor. Si el número que queda separado no mide nunca al anterior hasta separar una unidad, los dos números son primos entre sí." Al hacer su demostración, Euclides empleó un método que hoy conocemos con el nombre de Algoritmo de la División, el cual posiblemente representa el primer algoritmo conocido en la historia de las matemáticas. Este ha sido el punto de partida de los Dominios Euclidianos.

Desde Euclides de Alejandría, son muchos los matemáticos que han contribuido al desarrollo de la teoría de Dominios Euclideanos. El profesor Hendrick W. Lenstra Jr, del instituto de matemáticas de la Universidad de Amsterdam presenta en el artículo titulado " Euclidean Number Fields 1" (Ver Matematical intelligenter Volumen 2. Número 1 de 1979 página 6), una lista de matemáticos que han hecho los aportes más significativos a esta rama del álgebra abstracta.

Como muchas otras teorías matemáticas, esta debe gran parte de su desarrollo a los intentos por resolver el último teorema de Fermat.

Consideremos el siguiente diagrama:



Obsérvese que los domínios euclidianos son el soporte de nuevas estructuras algebraicas que predominan en muchas ramas del álgebra moderna (álgebra conmutativa, álgebra homológica, geometría algebráica, teoría de números algebraicos, álgebra lineal sobre anillos) e investigaciones recientes sobre este campo.

Trabajar la teoría de módulo sobre dominios euclidianos (Ver [5], pág 279) nos permite visualizar con mayor claridad y estética muchos resultados del álgebra lineal clásica (Forma canónica de Jordan), de teoría de grupos (estructura de grupos abelianos) y teoría de anillos (ver [5], pág. 279).

Lo que hace realmente interesante e importante del diagrama descrito anteriormente es mirar y cuestionarse si las flechas(implicaciones) se pueden invertir, como por ejemplo se sabe que todo domínio euclidiano es un dominio de ideales principales, pero ¿ será un dominio de ideales principales un domínio euclidiano?, el tratar de invertir cada flecha, conlleva a teorias nuevas

o problemas (algunos aún no resueltos) que responden a esas inquietudes.
Este trabajo ha sido dividido en dos capítulos, el primero constituye el fundamento teórico necesario para comprender los resultados del capítulo 2. Dados dos elementos $a \neq 0$, $b \neq 0$ de un anillo euclidiano $(A, +, \cdot, \varphi)$, los comparamos , vía la función φ de A en $\mathbb{N}$ (con el orden usual).

En el capítulo 2, inspirados en el trabajo de Paul Samuel [12], se cambia a el anillo A por un módulo sobre un anillo arbitrario (no necesariamente conmutativo) y el codomínio sigue siendo un conjunto bien ordenado, Ver [2.1]; además se resaltan algunas propiedades de los módulos euclidianos y la construcción de algunos objetos matemáticos que sean euclidianos.

En textos introductorios al álgebra moderna es común probar que todo anillo euclidiano es un anillo de ideales principales, y es tambien usual decir que el recíproco tambien es falso, y se es referenciado en [12]. En la sección 2.2 se mostrará esto, soportado en el artículo [2].
Si K es un cuerpo, se sabe que $(K[x]$, grado) es un dominio euclidiano en el cual la división es única; es fácil mostrar que (K, función idénticamente nula) es un dominio euclidiano con la misma propiedad. Es posible demostrar que esos son los únicos dominios euclidianos donde la división es única, una prueba puede ser encontrada en [5] o en [10], aquí se considerará el problema en general, tomando un anillo conmutativo R, en vez de un cuerpo K. Ver sección [2.4].

No es difícil mostrar que $(\mathbb{Z}, |\cdot|)$ es un dominio euclidiano tal que para todo $a, b \in \mathbb{Z}$, $b \neq 0$, a no es múltiplo de b, exísten exactamente q_i, r_i, con $i = 1, 2$ tales que $a = q_i b + r_i$ con $g(r_i) < g(b)$. Es posible mostrar que es el único dominio euclidiano con esta propiedad. Ver sección [2.5].

CAPÍTULO 1

Preliminares

En este capítulo se comenzará con una revisión de la definición y propiedades elementales de anillos y módulos. Con esto se indica los conceptos básicos que debe conocer el lector y además servirá para fijar notaciones y convenios. Despues de ello, se pasará a discutir sobre conjuntos bien ordenados y ordinales.

Los libros [4], [9] y [11] son excelentes para este recuento.

1.1 ANILLOS

Sea A un conjunto no vacio. Se dice que A tiene una estructura de anillo, o simplemente A es un anillo, si en A se han definido dos operaciones binarias internas notadas $+$ y $\cdot$ (adición y multiplicación), tales que:

(i) $(A, +)$ es un grupo abeliano.

(ii) $(A, \cdot)$ es un semigrupo.

(iii) La multiplicación es distributiva con respecto a la adición, es decir, para todo $x, y, z \in A$ se tiene que,

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(y + z) \cdot x = y \cdot x + z \cdot x.$$

DEFINICIÓN 1.1.1:

Un anillo R es llamado un ***anillo conmutativo*** si

$$x \cdot y = y \cdot x \quad \text{para todo} \quad x, y \in A.$$

Un anillo conmutativo se denotará por R.

DEFINICIÓN 1.1.2:

Un anillo A es llamado un ***anillo con identidad*** o un ***anillo unitario*** si exíste un elemento $1_A \neq 0$ en A tal que

$$x \cdot 1_A = 1_A \cdot x = x \quad \text{para todo} \quad x \in A.$$

Se denota 1_A el elemento unidad del anillo.

Nota: Todos los Anillos a considerar tienen elemento unidad.

DEFINICIÓN 1.1.3:

Un ***Homomorfismo de anillos*** es una aplicación f de un anillo A en un anillo B tal que:

i)$f(x+y) = f(x) + f(y), \quad \forall x, y \in A.$

ii)$f(xy) = f(x)f(y) \quad \forall x, y \in A$

iii)$f(1_A) = 1_B$.

El ***Kernel*** $kerf$ y la ***Imagen*** $imgf$ son definidas por

$$kerf := \{a \in R \backslash f(a) = 0\} \qquad \text{y} \qquad imf := \{f(a) \backslash a \in A\}.$$

DEFINICIÓN 1.1.4:

Sea R un anillo con elemento identidad. La ***característica de un anillo***, denotado $charR$ esta definida como el $n \in \mathbb{N}$ mas pequeo tal que $n \cdot 1 = 0$;si no exíste tal número se dice que la $charR = 0$.

DEFINICIÓN 1.1.5: Sea A un anillo.

(a) Un elemento $x \neq 0$ en A es llamado ***un Divisor de cero*** si exíste un elemento $s \neq 0$ tal que $xs = 0$ o $sx = 0$.

(b) Un elemento $x \in A$ es llamado ***Nilpotente*** si $x^n = 0$ para algún $n \geq 1$.

DEFINICIÓN 1.1.6: Sea A un anillo con elemento identidad. Un elemento $x \in A$ es llamado ***Invertible*** o ***Unidad*** en R si exíste un elemento $s \in A$ tal que $xs = sx = 1$. Los elementos invertibles de un anillo A forman un grupo, que se denota A^*.

Ejemplo: Considérese el anillo $M_n(A)$ de las matrices de orden $n \times n$ sobre el anillo de A

$$M_n(A^*) := GL_n(A) = \{B \in M_n(A) \mid B \text{ es invertble}\}.$$

DEFINICIÓN 1.1.7: Sea R una anillo conmutativo.

Se dice que a divide a b o que b es divisible por a o que a es un factor o divisor de b, si exíste un elemento $r \in R$ tal que $b = ra$ y se denota $a \mid b$.

DEFINICIÓN 1.1.8:

Un ***Dominio de integridad*** es una anillo conmutativo sin divisores de cero.

Ejemplo 1: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son todos dominios de integridad.

Ejemplo 2: $K[x_1, x_2, ..., x_n]$ (K cuerpo, x_i indeterminadas),

$\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b, n \in \mathbb{Z}, \ n > 0\}$ son dominios de integridad.

DEFINICIÓN 1.1.9:

Un dominio de integridad R es llamado un ***campo*** si $a \mid b$ para cualesquiera dos elementos $a \in R - \{0\}$ y $b \in R$.

DEFINICIÓN 1.1.10

Un ***ideal a la derecha*** I de un anillo A es un subconjunto de A que es un subgrupo aditivo y $IA \subseteq A$.

DEFINICIÓN 1.1.11

Un ***ideal a la izquierda*** I de un anillo A es un subconjunto de A que es un subgrupo aditivo y $AI \subseteq A$.

DEFINICIÓN 1.1.12: *(Ideal)*

Un subanillo I de un anillo A es llamado un ***Ideal*** de A si $xy \in I$ y $yx \in I$ siempre que $x \in I$ y $y \in A$. Es decir, Un ideal I es un ideal a izquierda y a derecha de A. (Ideal Bilátero).

DEFINICIÓN 1.1.13

Sea A un anillo e I un ideal de A. El grupo cociente A/I hereda de A una multiplicación

$$(a+I)(b+I) := (ab+I)$$

unívocamente definida que lo convierte en un anillo, denominado ***Anillo Cociente.***

Ejemplo: Sea A un anillo y $a \in A$, entonces $Ann(a) := \{x \in A \mid x \cdot a = 0\}$ es un ideal a izquierda de A, llamado *el aniquilador de a.*

1.1.14 TEOREMA DE HOMOMORFISMO DE ANILLOS

Si $f : A \longrightarrow B$ es un homomorfismo cualquiera de anillos, el núcleo de f, $f^{-1}(\{0\})$ es un ideal de A, y la imagen de f, $f(A)$ es un subanillo de B, y f induce un isomorfismo de anillos $A/f^{-1}(\{0\}) \cong f(A)$.

DEFINICIÓN 1.1.15

Sea R un anillo. Un ideal $I \lhd R$ es llamado ***finitamente generado*** si I puede ser generado por un número finito de elementos. Un ideal I es llamado un ***ideal principal*** si puede ser generado por un solo elemento.

DEFINICIÓN 1.1.16

Un anillo donde todo ideal es principal es llamado un ***anillo de ideales principales.*** Un anillo de ideales principales que es también un dominio de integridad es llamado ***dominio de ideales principales.***

DEFINICIÓN 1.1.17

Los ***múltiplos*** xa de un elemento $x \in A$ forman un ideal principal a la izquierda, que se indica por xA, análogamente a la derecha.

Ejemplo: Sea $p \in \mathbb{N}$ primo, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo con p elementos, a veces notado $\mathbb{F}_p$.

Existen anillos exactamente con un ideal maximal; por ejemplo, los cuerpos.

DEFINICIÓN 1.1.18

Un anillo A que tiene exactamente un ideal maximal π se denomina ***Anillo local***.

DEFINICIÓN 1.1.19

Un ***Anillo Local Especial*** es un anillo local cuyo ideal maximal π es generado por un elemento nilpotente, esto es, $\pi = Ra$, con $a^n = 0$ para algún n.

Ejemplo: Un cuerpo es un anillo local especial.

1.2. MÓDULOS

Sea $(M, +)$ un grupo abeliano y A un anillo. Se dice que M tiene estructura de módulo a la izquierda sobre A , si se ha definido un producto entre elementos de M y A

$$A \times M \to M$$

$$(a, m) \mapsto a \cdot m$$

para el cual se cumplen las siguientes condiciones:

i)$a_1 \cdot (m_1 + m_2) = a_1 \cdot m_1 + a_1 \cdot m_2 \quad \forall a_1 \in A$ y $m_1, m_2 \in M$

ii)$(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m, \quad \forall a_1, a_2 \in A$y $m \in M$

iii)$(a_1 \cdot a_2) \cdot m = a_1 \cdot (a_2 \cdot m), \quad \forall a_1, a_2 \in A$ y $m \in M$

iv)$1_A \cdot m = m$.

De manera similar se definen los módulos a la derecha sobre el anillo A. Un módulo a la izquierda sobre A será denotado por M_A, también se dirá que M es un A-módulo.

Ejemplos:

1) Todo grupo abeliano es un $\mathbb{Z}$-módulo.

2) Si $\mathbb{K}$ es un anillo de división, entonces cada espacio vectotial sobre $\mathbb{K}$ es un $\mathbb{K}$-módulo izquierdo.

3) Sea A un anillo y $M_n(A)$ un anillo de matrices de orden n con entradas en A. El producto

$$aA := a(a_{ij}) = (aa_{ij})$$

da a $M_n(A)$ estructura de A- módulo izquierdo.

4)Cada anillo A tiene estructura de A-módulo izquierdo y A-módulo derecho:

$$ax := ax, \quad xa := xa; \quad a, x \in A$$

En general A presenta diferentes propiedades bajo estas dos estructuras, las denotaremos por A y A_A respectivamente.

5) Siendo A un anillo y un ideal izquierdo de A, entonces el grupo cociente A/I tiene estructura natural de A-módulo

$$a(x + I) = ax + I, \quad x, a \in A.$$

6) Sea I un conjunto no vacío, A un anillo, $\{M_i\}_{i\in I}$ una familia no vacia de A-módulos y $\prod_{i\in I} M_i$ el producto cartesiano de la familia dada. entonces $\prod_{i\in I} M_i$ es un A-módulo. Para su demostración ver [4,pág.173].

DEFINICIÓN 1.2.1

Sea M un A-módulo y N un subconjunto no vacío de M. Decimos que N es un ***A-submódulo*** de M, si N es un subgrupo del grupo $(M, +)$, y además $na \in N$ para cada $n \in N$ y cada $a \in A$.

Ejemplo: Sea M un A-módulo y $m \in M$. El conjunto $mA := \{ma : a \in A\}$ es un submódulo de M llamado *Submódulo cíclico* generado por m.

DEFINICIÓN 1.2.2

Se dice que M es un A-módulo ***Cíclico***, si exíste $m \in M$, tal que $mA = M$.

1.3. CONJUNTOS BIEN ORDENADOS

DEFINICIÓN 1.3.1

Se dice que un conjunto parcialmente ordenado S está ***bien ordenado***, si todo subconjunto no vacío de S posee un elemento mínimo, esto es, un elemento $a \in B$ tal que $a \leq x$ para todo $x \in B$.

Ejemplo: $\mathbb{Z}^+$ es un conjunto bien ordenado.

LEMA 1.3.1: Todo subconjunto de un conjunto bien ordenado es bien ordenado.

Demostración: Ver [11, pág.122].

DEFINICIÓN 1.3.2

Un conjunto α es un ***Número Ordinal*** (o simplemente un ordinal) si tiene las propiedades siguientes:

$P_1(\alpha)$: Si $\beta \in \alpha$ entonces $\beta \subset \alpha$.

$P_2(\alpha)$: $[(\beta \in \alpha) \wedge (\gamma \in \alpha)] \Longrightarrow [(\beta = \gamma) \vee (\beta \in \gamma) \vee (\gamma \in \beta)]$.

$P_3(\alpha)$: Si $\varnothing \neq A \subset \alpha$, entonces existe $\gamma \in A$ tal que $\gamma \cap A = \varnothing$.

2.1 Observación: Si en $P_3(\alpha)$ se toma $A = \alpha$ entonces

$$[(\gamma \in A) \wedge (\gamma \cap A = \varnothing)] \Longrightarrow \gamma = \varnothing$$

luego todo ordinal α, distinto del vacío, contiene al vacío como elemento.

Se asume conocidas las propiedades elementales de conjuntos bien ordenados y números ordinales, para tal fin, Ver [9].

El mínimo ordinal infinito es denotado por ω y $+$ denota la adición usual de ordinales (así $1 + \omega = \omega < \omega + 1$).

DEFINICIÓN 1.3.3

Dos funciones $\varphi : S \longrightarrow W$ y $\varphi' : S \longrightarrow W'$ desde un conjunto S a conjuntos bien ordenados W y W' son ***Equivalentes*** si existe un isomorfismo de conjuntos ordenados $\vartheta : \varphi(S) \longrightarrow \varphi'(S)$ tal que $\varphi' = \vartheta \circ \varphi$.

DEFINICIÓN 1.3.4

La ***Suma Herssenberg*** (denotada $\oplus$) de dos ordinales α y β pueden ser definidas inductivamente por:

$$\alpha \oplus \beta = min\{\nu : \nu \quad \text{es un ordinal}, \nu > \lambda + \beta \quad \text{para todo } \lambda \quad \lambda < \beta \quad \nu > \alpha + \lambda \quad \text{para todo} \quad \lambda < \beta\}$$

esta suma es asociativa y conmutativa.

CAPÍTULO 2

Módulos Euclidianos

2.1 MÓDULOS EUCLIDIANOS

En este capítulo se intoduce una definición muy general de anillo euclidiano, la introducción de una construcción euclídea de Samuel [11] y la deducción de algunas de sus consecuencias.

Sea A un anillo, M un A-módulo a la izquierda, S un conjunto bien ordenado y R un anillo conmutativo.

DEFINICIÓN 2.1.1: Una función $\varphi : M - \{0\} \longrightarrow S$ se dice que es un algoritmo de ***tipo I*** sobre M si para todo $a, b \in M$,$b \neq 0$ existe $q \in A$ y $c \in M$ tales que $a = qb + c$ y $c = 0 \quad$ o $\quad \varphi(c) < \varphi(b)$.

DEFINICIÓN 2.1.2: Una función $\varphi : M \longrightarrow S$ se dice que es un algoritmo de ***tipo II*** sobre M si para todo $a, b \in M$,$b \neq 0$ existe $q \in A$ y $c \in M$ tal que $a = qb + c$ y $\varphi(c) < \varphi(b)$.

DEFINICIÓN 2.1.3: Una función $\varphi : M \longrightarrow S$ se dice que es un algoritmo de ***tipo III*** sobre M si para todo $a, b \in M$, existe $q \in A$ y $c \in M$ tal que $a = qb+c$ y $c = 0 \quad$ o $\quad \varphi(c) < \varphi(b)$.

Se puede demostrar que las tres definiciones 2.1.1, 2.1.2 y 2.1.3 son equivalentes .Ver [1,pág.294].
En lo que sigue, cuando se diga un algoritmo se hara referencia al algoritmo de ***tipo III***, salvo previo aviso.
Sobre un A-módulo a izquierda la noción de algoritmo a izquierda es definido como una función $\varphi : A \times M \longrightarrow S$ tal que para todo $a, b \in M$ exísten $q \in A$ y $c \in M$ tales que $a = qb + c$ con $c = 0$ o $\varphi(c) < \varphi(b)$.

Sobre un A-módulo a la derecha la noción de un algoritmo derecho es definido similarmente remplazando $a = qb + c$ por $a = bq + c$.

DEFINICIÓN 2.1.4:

Sea **W** un conjunto bien ordenado. Un anillo A se dice ***Euclídeo*** con respecto a la función $\phi : A \longrightarrow \mathbf{W}$ si satisface la siguiente condición:

Dados $a, b \in A$, con $b \neq 0$, existen $q, r \in A$, con $a = bq + r$ y $\phi(r) < \phi(b)$.

En este caso, a ϕ lo llamamos un ***Algoritmo Euclídeo sobre A***. Además, es costumbre llamar a q ***cociente*** y a r ***resto*** que resultan de la aplicación de ϕ a la pareja (a, b).

DEFINICIÓN 2.1.5:

Un A-módulo M es llamado ***euclidiano*** si exíste un conjunto bien ordenado S y un algoritmo $\varphi : M \longrightarrow S$.

Diremos que un anillo es euclidiano o euclidiano a la izquierda si este es euclidiano como módulo a la izquierda sobre sí mismo.

Observación 2.1:

a) A es un anillo euclidiano a la derecha si exíste un algoritmo a la derecha sobre un A-módulo derecho A.

b) A es bieuclidiano si exíste una función φ desde A en un conjunto bien ordenado, el cual es a la vez un algoritmo a la izquierda y un algoritmo a la derecha.

EJEMPLOS DE MÓDULOS EUCLIDIANOS

1) Sea $|\cdot| : \mathbb{Z} \longrightarrow \mathbb{N}$, la función Valor absoluto. Entonces $(\mathbb{Z}, +, \cdot, |\cdot|)$ es un $\mathbb{Z}$-módulo euclidiano. (Ver [7], pág 19-20).

2) Sea $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $N(a + bi) = (a^2 + b^2)$, la función Norma. Entonces $(\mathbb{Z}[i], +, \cdot, N)$ es $\mathbb{Z}[i]$-módulo euclidiano.(Ver [7], pág 22-23).

3) Sea K un cuerpo y $\partial : K[x] \longrightarrow \mathbb{N}$ la función Grado, entonces $(K[x], \partial)$ es un $K[x]$-módulo euclidiano. (Ver[7], pág. 24-27).

4) Sea $n \geq 1$. Si A es un anillo euclidiano a izquierda entonces $M_n(A)$ tambien es un anillo

euclidiano a la izquierda.

Lema 2.1.1:

Sea M un módulo euclidiano $\varphi : M \longrightarrow S$ es un algorítmo sí y solo sí para todo $a, b \in M$ exíste $q \in A$ y exíste $c \in M$ tal que $a = qb + c$ y $c = b$ o $\varphi(c) < \varphi(b)$.

Demostración: $\Longrightarrow$) Supóngase que $\varphi : M \longrightarrow S$ es un algoritmo entonces para todo $a, b \in M$ exísten $q' = q + 1 \in A$ y $c \in M$ tal que $a = q'b + c$ tal que $c = 0$ ó $\varphi(c) < \varphi(b)$.
Si $\varphi(c) < \varphi(b)$ se tiene por definición.
Si $c = 0$ entonces $a = q'b + 0 = q'b = (q + 1)b = qb + b$. Así se tiene que $c = b$.

($\Longleftarrow$ Supóngase que para todo $a, b \in M$ exísten $q' \in A$ y $c \in M$ tal que $c = b$ ó $\varphi(c) < \varphi(b)$.
Si $\varphi(c) < \varphi(b)$ se tiene por definición.
Si $c = b$ entonces $a = q'b + b = (q + 1)b + 0$. Es decir, exíste $q' = q + 1 \in A$ y $c \in M$ tal que $a = q'b + c$ y $c = 0$ ó $\varphi(c) < \varphi(b)$.■

TEOREMA 2.1.1:

Si M es un A-módulo euclidiano entonces todo submódulo de M es cíclico.

Demostración: Sea M un A-módulo euclidiano con algoritmo φ y N un submódulo de M.

a) Si N=$\{0\}$=A_0

b) Si N$\neq \{0\}$, exíste $a \in N$ tal que $a \neq 0$. Sea $\Omega = \{\varphi(y) : y \in N, y \neq 0\}$. $\Omega \neq \varnothing$, pues $a \in \Omega$, y puesto que $\Omega \subseteq S$ y S es un conjunto bien ordenado entonces exíste $x \in M$, $x \neq 0$ tal que $\varphi(x) = min\Omega$. Veamos que $Ax = N$, en efecto: si $b \in N$ existe $q \in A$ y $r \in M$ tal que $b = qx + r$ y $r = 0$ o $\varphi(r) < \varphi(x)$.
Como N es un submódulo de M, entonces $r = b - qx \in N$. Si $r \neq 0$, $\varphi(r) \in \Omega$, lo cual es imposible por la minimalidad de $\varphi(x)$. Por lo tanto $r = 0$ y $b = qx \in Ax$.■

Corolario 2.1.1:

a) Todo ideal izquierdo de un anillo euclidiano es principal.

b) Todo dominio euclidiano es un dominio de ideales principales, y por lo tanto es un dominio

de factorización única.

c)Todo ideal bilátero I de un anillo A bieuclidiano contiene un elemento x tal que I=$Ax = xA$.

2.2 UN DOMINIO DE IDEALES PRINCIPALES QUE NO ES UN DOMINIO EUCLIDIANO

El recíproco del *Corolario 2.1.1* es falso, puesto que no todo dominio de ideales principales es un dominio euclidiano. Para tal efecto, Ver [2].

TEOREMA 2.2.1: El subanillo $\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}, \theta = (1 + \sqrt{-19})/2\}$
es un dominio de idelaes principales (D.I.P) pero no es un dominio euclidiano.

Demostración: Primero se demostarán las siguientes afirmaciones:

1.) $\bar{\theta} = 1 - \theta$.

2.) $\theta\bar{\theta} = 5$.

3.) $\theta^2 = \theta - 5$.

4.) Para cualquier $x = a + b\theta \in \mathbb{Z}[\theta], \theta x = -5b + (a + b)\theta$.

1.) $\bar{\theta} = \overline{\frac{1}{2} + \frac{i\sqrt{19}}{2}} = \frac{1}{2} + \overline{\frac{i\sqrt{19}}{2}} = \frac{1}{2} - \frac{i\sqrt{19}}{2} = \left(1 - \frac{1}{2}\right) - \frac{i\sqrt{19}}{2} = 1 - \left(\frac{1}{2} + \frac{i\sqrt{19}}{2}\right) = 1 - \theta.$

2.)$\theta\bar{\theta} = \left(\frac{1}{2} + \frac{\sqrt{-19}}{2}\right)\left(\overline{\frac{1}{2} + \frac{\sqrt{-19}}{2}}\right) = \left(\frac{1}{2} + \frac{\sqrt{-19}}{2}\right)\left(\frac{1}{2} - \frac{\sqrt{-19}}{2}\right) = \frac{1}{4} - \frac{1}{4}(-19) = \frac{1+19}{4} = \frac{20}{4} = 5.$

3.) De 1.) y 2.), $5 = \theta\bar{\theta} = \theta(1 - \theta) = \theta - \theta^2$, entonces $\theta^2 = \theta - 5$.

4.) Sea $x \in \mathbb{Z}[\theta]$ entonces $x = a + b\theta$, para todo $a, b \in \mathbb{Z}$, luego $\theta x = \theta(a + b\theta) = a\theta + b\theta^2 = a\theta + b(\theta - 5) = a\theta + b\theta - 5b = -5b + (a + b)\theta$, así $\theta x = -5b + (a + b)\theta$.

Considérese la función

$$N : \mathbb{Z}[\theta] \longrightarrow \mathbb{Z}$$

$$z \mapsto N(z) = z\bar{z}.$$

Luego se tiene la siguiente identidad:

5.) $N(a + b\theta) = (a + b\theta)\overline{(a + b\theta))} = (a + b\theta)(a + b\bar{\theta}) = a^2 + ab\bar{\theta} + ab\theta + b^2\theta\bar{\theta} = a^2 + ab(1 - \theta) + ab\theta + 5b^2 = a^2 + ab - ab\theta + ab\theta + 5b^2 = a^2 + ab + 5b^2$.

Además, la función $N : \mathbb{Z}[\theta] \longrightarrow \mathbb{Z}$ satisface:

a.)$N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[\theta]$

b.)$N(x) \geq 0$ para todo $x \in \mathbb{Z}[\theta]$

c.)$N(x) = 0$ sí y solo sí $x = 0$.

En efecto:

a.) $N(xy) = (xy)\overline{(xy)} = (xy)(\bar{x}\bar{y}) = (x\bar{x})(y\bar{y}) = N(x)N(y)$.

b.) Para $x = a + b\theta \in \mathbb{Z}[\theta]$, $N(x) = N(a + b\theta) = a^2 + ab + 5b^2 \geq a^2 + 5b^2 \geq 0$, para todo $a, b \in \mathbb{Z}$.

c.) $N(x) = N(a + b\theta) = a^2 + ab + 5b^2 = 0$ sí y solo sí $a^2 + ab + 5b^2 = 0$ sí y solo sí $a = 0 = b$ sí y solo si $x = 0$.

Ahora bien, probemos que $\mathbb{Z}[\theta]^* = \{1, -1\}$.

Si $\alpha = a + b\theta \in \mathbb{Z}[\theta]^*$, existe $\beta \in \mathbb{Z}[\theta]$ tal que

$$\alpha\beta = 1$$

entonces $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Como $N(\alpha) \in \mathbb{Z}^+$, esto es, $a^2 + ab + 5b^2 = N(a + b\theta) = 1$ y por lo tanto, si $ab \geq 0$, entonces $b = 0$ y $a = \pm 1$. Por otro lado, puesto que $a + b\bar{\theta} = a + b - b\theta$ y $1 = N(a + b\theta) = N(a + b\bar{\theta}) = (a + b)^2 - ab + 4b^2$, se tiene que, cuando $ab \leq 0$, entonces tambien $b = 0$ y $a = \pm 1$. Así que $\mathbb{Z}[\theta]^* = \{1, -1\}$.

Afirmación 1: $\mathbb{Z}[\theta]$ no es un dominio euclidiano.

Es suficiente probar que $\mathbb{Z}[\theta]$ no admite una función φ que sea un algoritmo. Supóngase lo contrario, esto es, asúmase que φ es un algoritmo en $\mathbb{Z}[\theta]$.

Supóngase que m es de norma mínima entre los elementos de A, esto es, $m \in A$ y $\varphi(m) \leq \varphi(a)$ para todo $a \in A, m \neq 0, 1, -1$. Por ser φ un algoritmo se tiene que:

$2 = qm + r$, con $\varphi(r) < \varphi(m)$; por lo tanto, r es $0, 1, -1$.

Si $r = 0$, entonces $2 = qm$, esto es, $m/2$.

Si $r = -1$, entonces $3 = qm$, así $m/3$.

Si $r = 1$ entonces $1 = qm$ entonces $q = m = 1$ ó $q = m = -1$. Contradicción. Por lo tanto, se tiene $m/2$ ó $m/3$.

Veamos que $m = \pm 2$ ó $m = \pm 3$. Esta afirmación es una consecuencia del hecho de que 2 y 3

son primos en $\mathbb{Z}[\theta]$, el cual se demuestra como sigue:

Supóngase que $2 = (a + b\theta)(c + d\theta)$. Entonces $4 = N(2) = N((a + b\theta)(c + d\theta)) = N(a + b\theta)N(c + d\theta)$.

Si $a + b\theta, c + d\theta \notin \mathbb{Z}[\theta]^*$, se tiene que: $2 = N(a + b\theta) = a^2 + ab + 5b^2 = N(a + b\bar{\theta}) = (a + b)^2 - ab + 4b^2$. Por lo tanto, considerando los casos cuando $ab \geq 0$ y $ab < 0$ se concluye que $b = 0 = d$.

Así $2 = (a + b\theta)(c + d\theta) = ac$, una contradicción, pues 2 es irreducible en $\mathbb{Z}$. Por lo tanto 2 es irreducible en $\mathbb{Z}[\theta]$, así es primo en $\mathbb{Z}[\theta]$.

Análogamente se demuestra que 3 es primo en $\mathbb{Z}[\theta]$.

Ahora bien, puesto que $m/2$ y 2 es primo, entonces m y 2 son asociados, luego $m = \pm 2$, de igual forma si $m/3$ y como 3 es primo, entonces $m = \pm 3$, ya que $\mathbb{Z}[\theta]^*$.

Ahora bien, nuevamente usando el hecho de que φ es un algoritmo, se tiene que $\theta \equiv 0(mod \pm 2 \quad ó \quad mod \pm 3)$, ó, $\theta \equiv 1(mod \pm 2 \quad ó \quad mod \pm 3)$, ó,$\theta \equiv (-1)(mod \pm 2 \quad ó \quad mod \pm 3)$; Por lo tanto, θ, ó, $(\theta+1)$, ó, $(\theta-1)$ es divisible por 2 ó 3, luego $N(\theta)$, $N(\theta-1)$ ó $N(\theta+1)$ es divisible por $N(2)$ ó $N(3)$. Pero esto es imposible puesto que $N(\theta) = 5 = N(\theta - 1)$ y $N(\theta + 1) = 7$, mientras que $N(2) = 4$ y $N(3) = 9$.

Afirmación 2: $\mathbb{Z}[\theta]$ es un dominio de ideales principales (D.I.P).

Sea I un ideal de $\mathbb{Z}[\theta]$. Si I=0, no hay nada que hacer. Supóngase que $I \neq 0$.

Considérese el conjunto

$$\Lambda = \{N(\alpha) \mid \alpha \in I - \{0\}\}$$

Este es un subconjunto no vacío de $\mathbb{N}$, luego por el principio de buena ordenación en $\mathbb{N}$, Λ posee un menor elemento $n \in \mathbb{N}$. Sea $\beta \in I - \{0\}$ tal que $N(\beta) = n$. Se ha de probar que $I = \beta\mathbb{Z}[\theta]$. En efecto, dado $\beta \in I$, se sigue que $\beta\mathbb{Z}[\theta] \subseteq I$.

Si $I \not\subseteq \beta\mathbb{Z}[\theta]$, exíste $\alpha \in I$ tal que β no divide a α, entonces $\alpha \neq 0$ y por lo tanto $N(\alpha) \geq N(\beta)$. Veamos que exísten ν y δ en $\mathbb{Z}[\theta]$ tal que

$$0 < N(\alpha\nu - \beta\delta) < N(\beta).$$

Sean $\alpha, \beta \in \mathbb{Z}[\theta]$, $\beta \neq 0$. Si β no divide a α y $N(\alpha) \geq N(\beta)$ escribamos

$$\frac{\alpha}{\beta} = a + b\theta$$

donde $a, b \in \mathbb{Q}$ y al menos a ó $b \notin \mathbb{Z}$. Esto es posible puesto que el inverso de β como un número complejo está en $\mathbb{Q}[\theta]$, el cual es un subcuerpo de $\mathbb{C}$.

Esto conlleva a considerar elementos ν y $\delta \in \mathbb{Z}[\theta]$ tales que

$$0 < N\left(\frac{\alpha}{\beta}\nu - \delta\right) < 1 \quad \text{de donde} \quad N(\alpha\nu - \delta\beta) < N(\beta)$$

Hay varios casos.

Caso 1:

$b \in \mathbb{Z}$. Entonces $a \notin \mathbb{Z}$ y se puede escoger $\nu = 1$ y $\delta = \{a\} + b\theta$ (aquí $\{\mathrm{x}\}$ denota el entero más próximo a x, con $\{n + 1/2\} = n$). Ahora bien,

$$0 < N(\frac{\alpha}{\beta}\nu - \delta) \leq \frac{1}{4} < 1.$$

Caso 2(a):

$a \in \mathbb{Z}$ y $5b \notin \mathbb{Z}$, entonces $\frac{\alpha}{\beta}\bar{\theta} = a + 5b - a\theta$ y podemos escoger $\nu = \bar{\theta}$, $\delta = \{a + 5b\} - a\theta$.

Caso 2(b):

$a \in \mathbb{Z}$ y $5b \in \mathbb{Z}$. Escogiendo $\nu = 1$, $\delta = a + \{b\}\theta$.

Caso 3(a):

$a, b \notin \mathbb{Z}$ y $2a, 2b \in \mathbb{Z}$, entonces como probamos (4) para $a, b \in \mathbb{Z}$ y está claro que tambien es válida para $a, b \in \mathbb{Q}$ y por lo tanto $\theta\alpha/\beta = -5b + (a + b)\theta$ y $a + b \in \mathbb{Z}$. Por lo tanto, podemos escoger $\nu = \theta$, $\delta = \{-5b\} + \{a + b\}\theta$.

Caso 3(b):

$a, b \notin \mathbb{Z}$ y $2a, 2b \notin \mathbb{Z}$, entonces $|b - \{b\}| \leq 1/3$ o $|2b - \{2b\}| \leq 1/3$. En la primera situación tome $\nu = 1$ y $\alpha = \{a\} + \{b\}\theta$ y estime $0 < N(\alpha/\beta\nu - \delta) \leq 35/36 < 1$.

En la segunda situación tome $\nu = 2$ y $\delta = \{2a\} + \{2b\}\theta$ con la misma estimación.

Caso 3(c):

$a, b \notin \mathbb{Z}$, $2a \in \mathbb{Z}$ y $2b \notin \mathbb{Z}$, donde $5b \in \mathbb{Z}$ tome $\nu = 5$ y $\delta = \{5a\} + 5b\theta$ y cuando $5b \notin \mathbb{Z}$ tome $\nu = 2\bar{\theta}$ y $\delta = \{2a + 10b\} - 2a\theta$.

Caso 3(d):

$a, b \in \mathbb{Z}$, $2b \in \mathbb{Z}$ y $2a \notin \mathbb{Z}$. Tome $\nu = 2$, $\delta = \{2a\} + 2b\theta$.

Así, encontramos un elemento no nulo $\alpha\nu - \beta\delta$ en I tal que $N(\alpha\nu - \beta\delta) < N(\beta)$, lo cual contradice la minimalidad de $N(\beta)$.
Por lo tanto $I = \beta\mathbb{Z}[\theta]$.

Corolario 2.2.1

Sea $\varphi : M \longrightarrow S$ un algoritmo. Para un submódulo $N \subseteq M$ coloque

$$\hat{\varphi}(N) = min\{\varphi(y) : y \in N\}$$

y para todo $x \in M$ sea $\varphi_*(x) = \hat{\varphi}(Ax)$. Entonces se tiene que:
a) $\hat{\varphi}(N) \leq \hat{\varphi}(N')$ para $N' \subseteq N$, y la igualdad se da sí y solo si $N' = N$.
b) $\varphi_*(x) \leq \varphi(x)$ para todo $x \in M$
c) φ_* es un algoritmo sobre M.
d) $\varphi_*(x) \leq \varphi_*(qx)$ para todo $x \in M$ y $q \in A$, y la igualdad se da sí y solo si $Ax = Aqx$.

Demostración: a) Como $\hat{\varphi}(N) = min\{\varphi(y) : y \in N\}$ entonces $\hat{\varphi}(N) \leq \varphi(y)$, para algún $y \in N$. Sea $\varepsilon = \{\varphi(y) : y \in N\}$ y $\varepsilon' = \{\varphi(y) : y \in N'\}$, veamos que $\varepsilon' \subseteq \varepsilon$, en efecto: sea $h \in \varepsilon'$ entonces $h = \varphi(y)$, tal que $y \in N'$, pero $N' \subseteq N$ esto implica que $h = \varphi(y)$ para algún $y \in N$, entonces $h \in \varepsilon$. Además, $\hat{\varphi}(N') = min\varepsilon'$ entonces $\hat{\varphi}(N') \in \varepsilon' \subseteq \varepsilon$ así se tiene que $\hat{\varphi}(N') \in \varepsilon$ y como $\hat{\varphi}(N)$ es menor o igual que todo elemento de ε, puesto que $\hat{\varphi}(N) = min\varepsilon$ se tiene en particular que $\hat{\varphi}(N) \leq \hat{\varphi}(N')$.
$\hat{\varphi}(N) \leq y$ para todo $y \in N$, en particular $\hat{\varphi}(N) \leq \varphi(N')$, ya que $\varphi(N') \in N' \subseteq N$. Si $\hat{\varphi}(N) = \varphi(N')$, entonces algún $x \in N' \subseteq N$ satisface $\varphi(x) = min\{\varphi(y) : y \in N\}$ por teorema 2.1, $N = Ax \subset N'$, así $N' = N$.

b) $\varphi_*(x) \leq \hat{\varphi}(Ax) \leq \varphi(x)$, para todo $x \in M$.

c) Sean $b \in M$ y $a \in M - Ab$. Escójase $r \in A$ tal que $\varphi_*(b) = \varphi(rb)$. Puesto que φ es un algorítmo, exíste $c \in a + Arb$ con $\varphi(c) < \varphi(rb)$, entonces $c \in a + Ab$ y $\varphi_*(c) \leq \varphi(c) < \varphi(rb) = \varphi_*(b)$, lo cual prueba que φ_* es un algoritmo.

d) Como $Aqx \subseteq Ax$, para todo $x \in M$ y $q \in A$ entonces por (a): $\hat{\varphi}(Ax) \leq \hat{\varphi}(Aqx)$ para todo $x \in M$ y $q \in A$, luego por definición, $\varphi_*(x) \leq \varphi_*(qx)$, para todo $x \in M$ y $q \in A$, nuevamente por a) se tiene la igualdad.

TEOREMA 2.2.2

Sea N un submódulo de un módulo euclidiano M. Entonces N y M/N son módulos euclidianos.

Demostración: Si φ es un algoritmo sobre M, entonces es fácil ver que $\varphi|_N$ es un algoritmo sobre N. Un algorítmo ϑ sobre M/N es dado por: $\vartheta(x + N) := min\{\varphi(y) \mid y \in x + N\}$ para $x + N \in M/N$.■

Corolario 2.2.2

Sea A un anillo euclidiano y $I \subseteq A$ un ideal bilátero. entonces A/I es un anillo euclidiano.

Observación 2.2 Los subanillos de un anillo euclidiano no son necesariamente euclidianos. Por ejemplo: $K[x^2, x^3] \subseteq K[x]$, donde K es un cuerpo, ó $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{Z}[e^{2\pi i/20}]$.

TEOREMA 2.2.3

Sea M_i un A_i- módulos euclidianos para $i = 1, 2$. entonces $M_1 \times M_2$ es un $A_1 \times A_2$-módulo euclidiano.

Demostración: Sea φ_i un algoritmo sobre M_i con valores ordinales, para $i = 1, 2$.

Afirmamos que un algorítmo φ sobre $M_1 \times M_2$ es dado por:

$$\varphi((m_1, m_2)) = \varphi_1(m_1) \oplus \varphi_2(m_2)$$

donde $\oplus$ es la suma de Hessemberg. Para probar esto, sea $a = (a_1, a_2)$, $b = (b_1, b_2)$ en $M_1 \times M_2$, para $i = 1, 2$, escójase $q_i \in A_i$, $c_i \in M_i$ tal que $a_i = q_i b_i + c_i$ y $\varphi_i(c_i) \leq \varphi_i(b_i)$, con la igualdad sí y solo si $c_i = b_i$.

Tomando $q = (q_1, q_2) \in A_1 \times A_2$ se tiene que $a = qb + c$. Además, si una de las últimas desigualdades $\varphi_1(c_1) \leq \varphi_1(b_1)$ y $\varphi_2(c_2) \leq \varphi_2(b_2)$ se cumple estrictamente, entonces $\varphi(c) = \varphi_1(c_1) \oplus \varphi_2(c_2) < \varphi_1(b_1) \oplus \varphi_2(b_2) = \varphi(b)$, y si $\varphi_1(c_1) = \varphi_1(b_1)$ y $\varphi_2(c_2) = \varphi_2(b_2)$ entonces $c_i = b_i$ para $i = 1, 2$ y $c = b$. Esto demuestra que φ es un algoritmo sobre $M_1 \times M_2$.■

TEOREMA 2.2.4

Sea M un R-módulo. Si $M \neq Rx$ para todo $x \in M$, entonces M no es euclidiano. Si $x \in M$ es tal que $M = Rx$, entonces M es euclidiano sí y solo sí el anillo $R/Ann(x)$ es euclidiano.

Demostración: Si M es euclidiano, entonces todo submódulo de M es cíclico, en particular M es cíclico, así que exíste $x \in M$ tal que $M = Rx$. Una contradicción.
Ahora bien, considerese la siguiente función

$$f_x : R \longrightarrow R_x$$

$$r \longmapsto f_x(r) := rx$$

con x fijo en M, y para todo $r \in R$. f_x es un R-homomorfismo de R-módulos sobreyectivos, entonces por el teorema de homomorfismo de módulos, $R/ker(f_x) \cong Rx$, como $ker(f_x) = Ann(x)$, entonces $R/Ann(x) \cong Rx = M$, y se tiene el teorema.■

2.3 EL ALGORITMO MÍNIMO

Lema 2.3.1

Sea M un módulo euclidiano, S un conjunto bien ordenado y Σ un conjunto no vacío de algoritmos $\varphi : M \to S$. Entonces la función $\phi : M \longrightarrow S$ dada por:

$$\phi(x) := min\{\varphi(x) \mid \varphi \in \Sigma\}$$

es un algorítmo sobre M.

Demostración: Sea $a, b \in M$ y escójase $\varphi \in \Sigma$ tal que $\phi(b) = \varphi(b)$. Puesto que φ es un algoritmo, existe $q \in A$ y $c \in M$ tal que $a = qb + c$, y $c = 0$ o $\varphi(c) < \varphi(b)$. Esto implica $c = 0$ o

$\phi(c) \leq \varphi(c) < \varphi(b) = \phi(b)$, como se quería.■

DEFINICIÓN 2.3.1

Sea $S_M = \{\text{ordinales de cardinalidad} \leq card(M)\}$ un conjunto bien ordenado. Ver[11,pág. 175].

Se dice que la función

$$\theta_M : M \longrightarrow S_M$$

dada por:

$$\theta_M := min\{\varphi(x) \mid \varphi : M \longrightarrow S_M \quad \text{es un algorítmo}\},$$

es un algorítmo es sí mismo denominado "***Algorítmo Mínimo*** " de M.

TEOREMA 2.3.1

Sea $\phi : M \longrightarrow S_M$ un algoritmo, entonces las siguientes afirmaciones son equivalentes:

a) $\phi = \theta_M$.

b) $\phi(x) \leq \varphi(x)$ para todo $x \in M$ y para todo algorítmo $\varphi : M \longrightarrow S_M$.

c) Para todo $b \in M$ y para todo $\lambda \in S_M$ satisfaciendo $\lambda < \phi(b)$, exíste $a \in M - Ab$ tal que $\phi(c) \geq \lambda$ para todo $c \in a + Ab$.

Demostración: $a) \Leftrightarrow b)$ Por la definición de θ_M.

$b) \Longrightarrow c)$ Supóngase que b) es cierta. Sea $b \in M$ y $\lambda < \phi(b)$. Defina $\varphi : M \longrightarrow S_M$,

$$\varphi(m) = \phi(m), \quad m \neq b$$

$$\varphi(b) = \lambda$$

entonces $\varphi(b) < \phi(b)$, así (b) implica que φ no es un algorítmo. Por lo tanto, existe $a, b' \in M$ con $a \notin Ab'$ tal que no exíste $c \in a + Ab$ con $\varphi(c) < \varphi(b')$. En el caso $b \neq b'$, esto contradice la suposición de que ϕ es un algoritmo. Por lo tanto $b = b'$, y concluimos que $\phi(c) = \varphi(c) \geq \varphi(b') = \lambda$ para todo $c \in a + Ab'$ como se queria.

$c) \Longrightarrow b)$ Sea $\varphi : M \longrightarrow S_M$ un algorítmo, y $b \in M$ suponiendo c), se probará que $\phi(b) \leq \varphi(b)$ por inducción sobre $\varphi(b)$.

Por lo tanto, se puede asumir que $\phi(x) \leq \varphi(x)$ para todo $x \in M$ con $\varphi(x) < \varphi(b)$. Aplicando c) con $\lambda = \varphi(b)$ se encuentra $a \in M - Ab$. En particular, si $c \in a + Ab$ tal que $\varphi(c) < \varphi(b) \leq \phi(c)$, pero esto contradice la hipótesis de inducción: $\phi(c) \leq \varphi(c)$.■

EJEMPLOS

1) Usando el teorema 2.3.1 (c), se observa que el grado usual es el algorítmo mínimo (de tipo I) sobre $K[x]$, con K un cuerpo. En efecto:

Veamos que la función grado $\partial : K[x] \longrightarrow \mathbb{N}$ satisface el teorema (2.3.1) parte (c).Sea $p(x) \in K[x]$ y $n \in \mathbb{N}$ tal que $n < \partial(p(x))$. Escójase $q(x) \in K[x]$ con $\partial(q(x)) = n$, entonces

$q(x) \notin < p(x) >$ y puesto que el único elemento $r(x)$ de $q(x) + < p(x) >$ satisfaciendo

$\partial(r(x)) < \partial(p(x))$ es dado por $r(x) = q(x)$, se tiene que

$\partial(r(x)) \geq n$ para todo $r(x) \in q(x) + < p(x) >$. Esto prueba que se verifica la parte (c) del teorema 2.3.1. Así se concluye $\partial = \theta_{K[x]}$.

2) Se puede demostrar que en $\mathbb{Z}$ el algorítmo mínimo está dado por $\theta_{\mathbb{Z}}(n = [log_2(n)] + 1)$, que no es otra cosa que el número de dígitos del desarrollo binario de n. Ver [6,pág. 39.]

3) Si K es un cuerpo finito, $\theta_{K[x]}(f(x)) = \partial(f(x)) + 1$.

Corolario 2.3.1

Si M es euclidiano y A es un anillo, entonces $\theta_M(x) \leq \theta_M(qx)$ para todo $x \in M$, $q \in A$, con la igualdad sí y solo sí $Ax = Aqx$.

Demostración: Como M es euclidiano admite una función algoritmo. Sean $\theta = \theta_M$. Por corolario 2.2.1 parte (b) se tiene que $\theta_*(x) \leq \theta(x)$ para todo $x \in M$, luego por la parte (c) se tiene que θ_* es un algorítmo sobre M. Ahora bien por el teorema 2.3.1 parte (b) se tiene que $\theta(x) \leq \theta_*(x)$ para todo $x \in M$ y para todo algorítmo $\theta_* : M \longrightarrow S_M$, así $\theta(x) = \theta_*(x)$ para todo $x \in M$ esto implica que $\theta = \theta_*$. Por tanto, por corolario 2.2.1 parte (d) se tiene que $\theta_*(x) \leq \theta_*(qx)$ para todo $x \in M$ y $q \in A$, esto es, $\theta_M(x) \leq \theta_M(qx)$ para todo $x \in M$ y $q \in A$, con la igualdad sí y solo sí $Ax = Aqx$.■

Corolario 2.3.2

Sea M_i un A_i-módulo euclidiano con algorítmo mínimo θ_i, $i = 1, 2$. entonces el algorítmo mínimo θ sobre el $A_1 \times A_2$-módulo, $M_1 \times M_2$ es dado por

$$\theta((m_1, m_2)) = \theta_1(m_1) \oplus \theta_2(m_2)$$

Demostración: Por la prueba del teorema 2.2.3 se sabe que la función $\psi : M \longrightarrow S_M$ definida por $\psi((m_1, m_2)) = \theta_1(m_1) \oplus \theta_2(m_2)$ es un algorítmo sobre $M_1 \times M_2$. Para probar que $\psi = \theta$ es sufieciente chequear que en el teorema 2.3.1 parte c) se cumple. Sea $b = (b_1, b_2) \in M_1 \times M_2$ y $\lambda < \varphi(b) = \theta_1(b_1) \oplus \theta_2(b_2)$ cualesquieras. La definición de la suma de Hessenberg implica que para $i = 1$ o para $i = 2$, existe un ordinal $\mu_i < \theta_i(b_i)$ tal que $\lambda \leq \mu_i \oplus \theta_{3-i}(b_{3-i})$. Sin pérdida de generalidad se puede suponer que $i = 1$. Aplicando el teorema 2.3.1 a M_1 se sabe que exíste $a_1 \in M_1 - A_1 b_1$ tal que $\theta_1 \geq \mu_1$ para todo c_1 y $a_1 + A_1 b_1$. Entonces los elementos $a = (a_1, b_1)$ de $M_1 \times M_2$ no está en $(A_1 \times A_2)b$, y para cada $c = (c_1, c_1) \in a + (A_1 \times A_2)b$ se tiene que $c_2 \in A_2 b_2$ y por lo tanto

$$\psi(c) = \theta_1(c_1) \oplus \theta_2(c_2) \geq \mu_1 \oplus \theta_2(b_2) \geq \lambda$$

Esto demuestra que la condición c) del teorema 2.3.1 se cumple.■

TEOREMA 2.3.2

Sea $\varphi : M \longrightarrow S_M$ un algoritmo, y sea $b \in M$ satisfaciendo $\varphi(b) = \varphi_*(b)$ (Ver colorario 2.2.1). Entonces $A/Ann(b)$ es un A-módulo euclidiano, y $\varphi(qb) \geq \varphi(q) + \theta_{A/Ann(b)}(q + Ann(b))$, para todo $q \in A$; donde $+$ denota la suma usual de ordinales.

Demostración: Para $b \in M$, $\varphi(b) = \varphi_*(b) = \hat{\varphi}(Ab) = min\{\varphi(y) : y \in Ab\}$.Luego $\varphi(b) \leq \varphi(y)$ para $y \in Ab$. Por tanto $\varphi(b) \leq \varphi(qb)$ para todo $q \in A$, asi que $\varphi(qb) = \varphi(b) + \rho(q)$, para alguna función $\rho : A \longrightarrow S_M$.

Ahora bien, defínase la función

$$\lambda : A/Ann(b) \longrightarrow S_M$$

$$r + Ann(b) = \bar{r} \longmapsto \lambda(r + Ann(b)) := \rho(r)$$

para todo $r \in A$.

Demostremos que λ esta bien definida, en efecto:

Sean $q + Ann(b), q' + Ann(b)$ en $A/Ann(b)$ tal que $q + Ann(b) = q' + Ann(b)$, entonces $(q - q') \in Ann(b)$, esto implica que $(q - q')b = 0$, esto es, $qb = q'b$, luego $\varphi(qb) = \varphi(b) + \rho(q)$ y $\varphi(q'b) = \varphi(b) + \rho(q')$,esto implica que $\rho(q) = \rho(q')$, esto es, $\lambda(q + Ann(b)) = \lambda(q' + Ann(b))$.

Ahora bien, demostremos que λ es un algoritmo, esto es, para todo $\bar{r_1}\bar{r_2} \in A/Ann(b)$ exísten $r \in A$ y $\bar{c} \in A/Ann(b)$ tal que $\bar{r_1} = r\bar{r_2} + \bar{c}$ con $\bar{c} = 0$ o $\lambda(\bar{c}) < \lambda(\bar{r_2})$. En efecto,

Sean $\bar{r_i}$ en $A/Ann(b), \bar{r_i} = r_i + Ann(b), i = 1, 2$ con $r_i \in A$.

Como $\varphi : M \longrightarrow S_M$ es un algorítmo entonces exísten $r \in A$ y $y := cb \in M$ con $c \in A$ tal que $r_1 = r(r_2b) + cb$ con $cb = 0$ o $\varphi(cb) < \varphi(r_2b)$.

Ahora bien, supóngase que $cb \neq 0$ entonces $c \notin Ann(b)$, esto es, $\bar{c} \notin Ann(b)$, luego $r_1b = r(r_2b) + cb$,así, $r_1b = (rr_2 + cb)$ lo que implica que $[r_1 - (rr_2 + c)]b = 0$, por tanto, $[r_1 - (rr_2 + c)] \in Ann(b)$, es decir, $\bar{r_1} = \overline{rr_2 + c}\, mod Ann(b)$, así, $\bar{r_1} = \overline{rr_2} + \bar{c} = r\bar{r_2} + \bar{c}$.

Además $\varphi(cb) < \varphi(r_2b)$ implica que $\varphi(b) + \rho(c) < \varphi(b) + \rho(r_2)$ por tanto $\rho(c) < \rho(r_2)$ esto es $\lambda(c + Ann(b)) < \lambda(r_2 + Ann(b))$, es decir $\lambda(\bar{c}) < \lambda(\bar{r_2})$.

Ahora bien, basta probar que $\varphi(qb) \geq \varphi(q) + \theta_{A/Ann(b)}(q + Ann(b))$, en efecto:

Se tiene que $\varphi(qb) = \varphi(b)+\rho(q)$, y $\theta_{R/Ann(b)} = min\{\lambda(\bar{x}) \mid \lambda : R/Ann(b) \longrightarrow S_{R/Ann(b)}$ es un algoritmo$\}$ con $\bar{x} := x + Ann(b)$. Como $\rho(q) = \lambda(\bar{x}) \geq \theta_{R/Ann(b)(\bar{x})}$ para todo $\bar{x} \in Ann(b)$ entonces $\varphi(qb) = \varphi(b) + \rho(q) \geq \varphi(b) + \theta_{R/Ann(b)(\bar{x})}$.■

Corolario 2.3.3

Sea A un anillo euclidiano sin divisores de cero, entonces

$$\theta_A(ab) \geq \theta_A(a) + \theta_A(b)$$

para todo $a, b \in A, b \neq 0$.

Demostración: Aplicando el teorema 2.3.2 con $A = M$ y $\varphi = \theta_A$.

Ahora bien consideremos la siguiente construcción transfinita.

Sea M un A-módulo, y sea S_M el conjunto de todos los ordinales cuyo cardinal no excede al car(M). Para $\lambda \in S_M$ se define inductivamente el conjunto M_λ:

$$M_\lambda := \{x \in M \mid \text{la aplicación natural } j : \Delta \longrightarrow M/Ax \quad \text{es sobreyectiva}\}$$

donde $\Delta := (\bigcup_{\alpha \in S_M, \alpha < \lambda} M_\alpha) \cup \{0\}$
Obsérvese que j satisface el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \Delta & \overset{i}{\hookrightarrow} & M \\ j \searrow & & \downarrow \pi \\ & & M/Ax \end{array}$$

se tiene que:

$$M_0 = \{x \in M : M = Ax\}$$

$$M_\alpha \subseteq M_\beta \quad \text{si} \quad \alpha \leq \beta$$

Si $M = R$ es un anillo conmutativo, entonces es facil chequear que

$$R_o = R^*$$

$R_1 = R^* \cup \{x \in R : R_x \quad$ es un ideal maximal en R, y la función $R^* \longrightarrow (R/R_x)^* \quad$ es sobreyectiva$\}$.

TEOREMA 2.3.3 (Motzkin [12], Samuel [10])
El A-módulo M es euclidiano sí y solo sí $\bigcup_{\lambda \in S_M} M_\lambda = M$. Si M es euclidiano entonces un algoritmo mínimo es dado por:

$$\theta_M(x) = min\{\lambda \mid x \in M_\lambda\} \qquad (1)$$

Demostración: Sea $\bigcup_{\lambda \in S_M} M_\lambda = M$ entonces la función $\psi : M \longrightarrow S_M$ dada por:

$$\psi(x) = min\{\lambda \mid x \in M_\lambda\} \qquad (2)$$

es un algorítmo. En efecto, sea $a,\ b \in M$. Ahora por la hipótesis a y b estan en M_λ, para algun $\lambda \in S_M$ y exísten q en A y c en M, por la tanto en M_λ, tales que: $a = qb + c$ o $c = 0$ o $\psi(c) < \psi(b) = min\{\lambda \mid b \in M_\lambda\}$ esto demuestra que $\psi : M \longrightarrow S_M$ es un algoritmo. Así que M es un $A-$módulo. Recíprocamente, asúmase que M es $A-$módulo euclidiano y sea $\varphi : M \longrightarrow S_M$ un algoritmo. Aquí $S_M = \{n \mid$ es un número ordinal y $Card\, n \leq Card\, M\}$.
Veamos ahora que

$$\{x \in M \mid \varphi(x) \leq \lambda\} \subset M_\lambda \qquad (3)$$

En efecto, considérese la condición $P(\lambda) : \{x \in M \mid \varphi(x) \leq \lambda\} \subset M_\lambda$ y hágase indicción sobre λ

(a) Ahora como φ es un algoritmo, entonces para todo a , b en M, existen q en R y x en M tales que $a = qb + x$, donde $x = 0$ o $\varphi(x) < \varphi(b)$. Luego basta con escoger b en M tal que $\varphi(b) \leq \lambda = 0$, (λ y $\varphi(b)$ están en S_M, que es bien ordenado). Asi que para $\lambda = 0$, se tiene que $P(0) : \{x \in M \mid \varphi(x) \leq 0\} = \phi \subset M_0$ y la condición es válida para $\lambda = 0$.

(b) Asúmase, hipotesis de inducción, que $P(\lambda) : \{x \in M \mid \varphi(x) \leq \lambda\} \subset M_\lambda$ es verdadera y demuéstrese que $P(\lambda + 1)$ es verdadera. En efecto, se tiene que

$$\{x \in M \mid \varphi(x) \leq \lambda\} \subseteq \{x \in M \mid \varphi(x) \leq \lambda + 1\} \subset M_{\lambda+1}.$$

Asi que $P(\lambda+1)$ es verdadera. Luego, $P(\lambda)$ es verdadera para todo λ en S_M por lo tanto $M = \bigcup_{x \in M} \left(\{x \in M \mid \varphi(x) \leq \lambda\}\right) = \bigcup_{\lambda \in S_M} M_\lambda$
Por último como M es euclidiano de (1) y (2) se sigue que
$\psi(x) = min\{\lambda \mid x \in M_\lambda\} \leq \varphi \leq \lambda$ para todo x en M y para todo algoritmo $\varphi : M \longrightarrow S_M$. Por lo tanto $\psi = \theta_M$ es su algoritmo menor■

Ahora se consideran algunas situaciones cuando el anillo A es conmutativo, por el teorma 2.2.3, en el caso conmutativo solo se necesita considerar el caso $M = R$.

TEOREMA 2.3.4 Sea R un anillo conmutativo. Si R no es un dominio de ideales principales, entonces R no es euclidiano. Si R es un dominio de ideales principales, entonces

$$R \cong \prod_{i=1}^{n} R_i$$

para algún $n \in \mathbb{Z}^+$, donde cada R_i o es un dominio de ideales principales el cual no es un cuerpo o es un anillo local especial. En este caso R es euclidiano sí y solo sí todos los R_i son euclidianos. Finalmente, si R es euclidiano entonces su algoritmo mínimo θ es dada por:

$$\theta(x) = \bigoplus_{i=1}^{n} \theta_i(x_i)$$

para $x = (x_i)_{i=1}^n \in \Pi_{i=1}^n = R$; aquí $\oplus$ denota la suma Hessenberg y θ_i es el algorítmo mínimo de R_i.

Demostracíon: La primera afirmacíon se sigue del corolario 2.1.1 para la descomposición de un anillo de ideales principales se hace uso del siguiente teorema:

"Una suma directa de anillos de ideales principales es un anillo de ideales principales. Todo anillo de ideales principales es una suma directa de dominios de ideales principales y de anillos de ideales principales especial". (Ver [13],IV,Sec.15.Teorema 3.3). Por el teorema 2.2.3 se tiene que el producto de módulos euclidianos es euclidiano, así por corolario 2.3.1 se tiene que $\theta_M \leq \theta_M(qx)$ para todo $x \in M$ y $q \in A$, con la igualdad sí y solo so $Ax = Aqx$. Por tanto, por colorario 2.3.2 el algoritmo mínimo θ sobre el producto de módulos esta dado por

$$\theta(x) = \bigoplus_{i=1}^{n} \theta_i(x_i).$$

2.4 UNICIDAD EN EL RESIDUO DEL ALGORITMO

Sea M un módulo sobre el anillo A, y S un conjunto bien ordenado. Una función $\varphi : M \longrightarrow S$ es llamado un ***Algoritmo con residuo único*** (a.r.u) si para todo $a, b \in M$ exíste un único elemento $r \in a + Ab$ tal que $r = 0$ o $\varphi(r) < \varphi(b)$.

Ejemplo: Sea $A = M = K[x]$, con K un semicuerpo, y $\varphi = grado$ cumple con con (a.r.u). (donde $\partial(0) = \omega$).

TEOREMA 2.4.1 Un algoritmo $\varphi : M \longrightarrow S$ es a.r.u sí y solo sí (a) y (b) se cumplen:
a) Para todo $x, y \in M$, $x \neq y$ implica $\varphi(x - y) \leq max\{\varphi(x), \varphi(y)\}$.
b) Para todo $x \in M$, y para todo $q \in R$, $\varphi(x) \leq \varphi(qx)$.
Demostración: $\Longrightarrow$) a) Tomando $a = x$ y $b = x - y$, se tiene que $x, y \in a + Ab$, por la unicidad no se puede tener $\varphi(x) < \varphi(b)$ y $\varphi(y) < \varphi(b)$. Por lo tanto, $\varphi(x) \geq \varphi(b)$ o $\varphi(y) \geq \varphi(b)$, como se queria.

b) Si $\varphi(qx) < \varphi(x)$ entonces $qx \neq 0$. Entonces $r = qx$ y $r = 0$ son dos elementos diferentes de $0 + Ax$, donde ambos satisfacen

$$r = 0 \quad \text{o} \quad \varphi(r) < \varphi(x)$$

contradiciendo la unicidad.
$\Longleftarrow$ Supóngase que (a) y (b) se cumplen, se debe probar probar que:

$$r \equiv s mod Ab$$

$$r = 0 \quad \text{o} \quad \varphi(r) < \varphi(b)$$

$$s = 0 \quad \text{o} \quad \varphi(s) < \varphi(b)$$

implica que $r = s$.
En el caso $r = 0$ se tiene que $s \in Ab$, así $\varphi(s) \geq \varphi(b)$ por (b), y $s = 0 = r$. Similarmente es tratado el caso $s = 0$. Si ambos $\varphi(r) < \varphi(b)$ y $\varphi(s) < \varphi(b)$ entonces se escoge $r - s = qb$ y se encuentra que:

$$max\{\varphi(r), \varphi(s)\} < \varphi(b) \leq \varphi(qb) = \varphi(r - s)$$

Corlario 2.4.1

Si φ es a.r.u sobre M, entonces $\varphi(x) = \varphi(-x)$ para todo $x \in M$, y $\varphi(x+y) = max\{\varphi(x), \varphi(y)\}$, si $\varphi(x) \neq \varphi(y)$, $x \neq 0 \neq y$.

Demostración: Por teorema 2.4.1 parte (b) se tiene que $\varphi(x) = \varphi(-x)$. Además, si $\varphi(x) > \varphi(y)$ entonces por parte (a) implica

$$\varphi(y) < \varphi(x) \leq max\{\varphi(x+y), \varphi(y)\}$$

y por lo tanto

$$\varphi(x+y) \geq \varphi(x) = max\{\varphi(x), \varphi(y)\}$$

La desigualdad es clara por (a) del teorema 2.4.1 y $\varphi(-y) = \varphi(y)$.■

TEOREMA 2.4.2

Sea φ un a.r.u sobre M tal que $\varphi[M]$ es un segmento principal de los números ordinales. Entonces φ es igual al algoritmo mínimo θ_M sobre M. Además, para $b \in M$ y $q \in A$ se tiene (Ver teorema 2.3.2)

$$\theta_M(qb) = \theta_M(b) + \theta_{A/Ann(b)}(q + Ann(b))$$

Demostración: Demostremos que $\varphi = \psi$ satisface la condiciones del teorema 2.3.1 parte (c). Sea $b \in M$ y $\lambda \in S_M$ tal que $\lambda < \varphi(b)$. Escójase $a \in M$ con $\varphi(a) = \lambda$. Entonces $a \notin Ab$, puesto que el único elemento r de $a + Ab$ satisfaciendo $\varphi(r) < \varphi(b)$ es dado por $r = a$, luego se tiene

$$\varphi(r) > \lambda \quad \text{para todo} \quad r \in a + Ab$$

Esto prueba teorema 2.3.1 parte (c) y se concluye que $\varphi = \theta_M$.

Por otro lado, sea $b \in M$. Como en la prueba del teorema 2.3.1 exíste un algorítmo

$$\lambda : A/Ann(b) \longrightarrow S_M \quad \text{tal que}$$

$$\theta_M(qb) = \theta_M(b) + \lambda(\bar{q})$$

donde $\bar{q} = q + Ann(b)$ se ha de probar que $\lambda = \theta_{A/Ann(b)}$.

(a) λ es a.r.u

(b) La imagen de λ es un segmento principal de los ordinales.

Para probar (b), sea $\bar{q} \in A/Ann(b)$ y $\mu \in S_M$ satisfaciendo $\mu < \lambda(\bar{q})$; se debe encontrar $\bar{r} \in A/Ann(b)$ tal que $\lambda(\bar{r}) = \mu$.

De $\theta_M(b) + \mu < \theta_M + \lambda(\bar{q}) = \theta_M(qb)$, se sabe que existe $c \in M$ tal que $\theta_M(c) = \theta_M(b) + \mu$.

si $c \notin Ab$, entonces $c = rb + d$ con $\theta_M(d) < \theta_M(b)$, y el corolario 2.4.1 implica $\theta_M(c) = \theta_M(rb)$, así $\mu = \lambda(\bar{r})$, y se tiene (b).■

Obsérvese que el teorema 2.4.2 implica que dos a.r.u cualesquiera sobre un módulo M son equivalentes.

Corolario 2.4.2

Sea A un anillo sin divisores de cero teniendo un a.r.u, entonces $\theta_A(ab) = \theta_A(a) + \theta_A(b)$ para todo $a, b \in A$, $b \neq 0$.

Para finalizar esta sección determinaremos todos los anillos A con a.r.u. Ver referencias [5] y [8].

TEOREMA 2.4.3

Sea R un anillo comutativo. Entonces R tiene a.r.u sí y solo sí $R \cong K[x]$ para algún cuerpo K, o R es un cuerpo, o $R \cong \mathbb{F}_2 \times \mathbb{F}_2$.

Demostración: Sea $\theta = \theta_R$ y póngase $K = \{0\} \cup R^* = \{0\} \cup \{x \in R : \theta(x) = 0\}$ (Ver teorema 2.3.3). Por teorema 2.4.1 parte (a) el conjunto K es cerrado bajo la suma, por tanto K es un cuerpo. Puesto que R es un anillo de ideales principales, por el teorema 2.3.3 se tiene que R es un dominio de ideales principales pero no es un cuerpo, o R es un anillo local especial o $R \cong R_1 \times R_2$ para ciertos anillos R_1 y R_2.

Caso I: R es un D.I.P pero no es un cuerpo.

Escójase $x \in R - K$ con $\theta(x) = 1$; se chequeará que $R = K[x]$. Supóngase que exíste $q \in R - K[x]$, y escójase q de tal forma que $\theta(q)$ sea mínimo. Entonces $q = ax + c$ con $a, c \in R$ y $c = 0$ o $\theta(c) < \theta(x) = 1$. Claramente $c \in K$, también, $\theta(ax) \geq \theta(x)$, del corolario 2.4.1 se concluye que $\theta(q) = \theta(ax)$. Usando conmutatividad y el corolario 2.4.2 se tiene que $\theta(q) = \theta(ax) = \theta(xa) = \theta(a) + \theta(x) > \theta(a)$. Por la minimalidad de de $\theta(q)$ se sigue que $a \in K[x]$ y por lo tanto tambien, $q = ax + c \in K[x]$, contradicción.

Por lo tanto $R = K[x]$, y puesto que R no es un cuerpo se tiene que $R \cong K[x]$.

Caso II: R es un anillo local especial.
Sea x en π, entonces $x = (1 + x) - 1 \in K + K = K = \{0\} \cup R^*$, pero $x \notin R^*$ así $x = 0$ y R es un cuerpo.

Caso III: $R = R_1 \times R_2$ con $R_1 \neq 0 \neq R_2$. Si $u \in R_1^*$ entonces $(u, 1) - (1, 1)$ esta en K pero no en R^* asi $(u, 1) = (1, 1)$ y $R_1^* = \{1\}$. Similarmente $R_2^* = \{1\}$, así $R_1^* = \{1\}$ y $K = \mathbb{F}_2$. Sea $x = (x_1, x_2) \in R$ satisfaciendo $\theta(x) = 1$, entonces $R \neq Rx$ y $K = \mathbb{F}_2$ mapeado sobre $R/Rx \cong (R_1/R_1x_1) \times (R_2/R_2x_2)$.

Por lo tanto $R/R_x \cong \mathbb{F}_2$ y despues reindizando se puede asumir que $R_1/R_1x_1 \cong \mathbb{F}_2$ y $R_2 = R_2x_2 \cong \mathbb{F}_2$.
Esto implica $x_2 \in R^*$ asi $x_2 = 1$.
Ahora bien, sea $y = x \cdot 1 = (x, -1, 0)$. Puesto que $\theta(y) = 1$ por corolario 2.4.1, se tiene de la misma forma $\mathbb{F}_2 \cong R/Ry \cong (R_1/R_1(x, -1)) \times R_2$. Asi se concluye $R_2 = \mathbb{F}_2$ y $(x, -1) \in R_1^* = \{-1\}$, asi $x_1 = 0$ y $R_1 = R_1/R_1x_1 \cong \mathbb{F}_2$, como se quería.■

2.5 UNA CARACTERIZACIÓN DE LOS ENTEROS COMO DOMINIOS EUCLIDIANOS

DEFINICIÓN 2.5.1:

Un ***Dominio euclidiano*** es un dominio de integridad junto con una función $g : R^* \longrightarrow N$, donde $R^* = R - \{0\}$ y N es el conjunto de los enteros no negativos, tal que:

(i) $g(ab) \geq g(a)$ para todo $a, b \in R^*$.

(ii) Si $a \in R, b \in R^*$, entonces exísten $q, r \in R$ tal que $a = qb + r$ donde $r = 0$ o $g(r) < g(b)$.

DEFINICIÓN 2.5.2:

Se dice que (R,g) tiene la propiedad del doble residuo (Abreviado **d.r.p**) si para cada par $a \in R, b \in R^*$ tal que b no divide a a, existe exactamente dos pares $q_i, r_i, i = 1, 2$, tal que $a = q_i b + r_i$ con $g(r_i) < g(b)$.Esta propiedad es equivalente a decir que para $a \in R, b \in R^*$ con b que no divide a a, existe exactamente dos elementos r_1, r_2 tales que $g(r_i) < g(b)$ y $a \equiv r_i mod(b), i = 1, 2$.

Ejemplo:$(\mathbb{Z}, |\quad|)$ es un **d.r.p.**

Acontinuación se demostrarán algunos lemas y corolarios que se emplearan para demostrar el teorema fundamental.Asumiremos de antemano que R no es un campo y se escribirá (R, g) para indicar que R es el dominio euclidiano y que g es la función algoritmo.

Para iniciar se fijará alguna terminología. Para un dominio euclidiano (R, g), sea

$$R_1 = \{x \in R^* \mid g(x) \leq g(y) \quad \text{para todo} \quad y \in R^*\}.$$

Por (i) y (ii) $R_1 = U(R)$, donde $U(R)$ es el grupo de las unidades de R. En efecto, Sea

$$R_1 = \{x \in R^* \mid g(x) \leq g(y) \quad \text{para todo} \quad y \in R^*\}.$$

veamos primero que $R_1 \subseteq U(R)$. Sea $x \in R_1$ entonces $x \in R^*$ y $g(x) \leq g(y)$ para todo $y \in R^*$, por (ii) se tiene que exísten $q, r \in R$ tales que

$$1 = xq + r, \quad r = 0 \quad \text{o} \quad g(r) < g(x)$$

Ahora bien, si $r = 0$ entonces se tiene que $1 = xq$ lo que implica que $x \in U(R)$.

Si $g(x) < g(y)$, como $g(x) \leq g(y)$ para todo $y \in R^*$, entonces $r = 0$. Por tanto se tiene que $R_1 \subseteq U(R)$.

Ahora veamos que $U(R) \subseteq R_1$.

Sea $y \in R^* \subseteq R$ arbitario, sea $x \in U(R) \subseteq R^*$ entonces exíste $z \in R^*$ tal que $xz = zx = 1$, asi para $r \in R^*$, $xzr = 1 \cdot r = r$, lo que implica por (i) que $g(x) \leq g(xzr) = g(r)$ para todo $x, y \in R^*$, asi se tiene que $g(x) \leq g(r)$ lo cual es absurdo.

Por tanto $r = 0$ y así $y = qx$, esto implica que $g(y) = g(qx) \geq g(x)$, y así se tiene que $x \in R_1$.

Por tanto $R_1 = U(R)$.

Para $n \geq 2$, sea

$$R_n = \{x \in R^* \mid g(x) \leq g(y) \quad \text{para todo} \quad y \in R^* - R_{n-1}\}.$$

Claramente, $R_n \subseteq R_{n+1}$ para todo $n \geq 1$ y $\bigcup_{n=1}^{\infty} R_n = R^*$,veamoslo por inducción sobre n. En efecto:

Es claro que $R_1 \subseteq R_2$. Supongamos que se cumple para $R_n \subseteq R_{n+1}$, y probemos que se cumple para $R_{n+1} \subseteq R_{n+2}$.

$R_{n+1} = \{x \in R^* \mid g(x) \leq g(y) \quad \text{para todo} \quad y \in R^* - R_n\}$, por hipótesis de inducción $R_n \subseteq R_{n+1}$, luego $-R_{n+1} \subseteq -R_n$, asi $R^* - R_{n+1} \subseteq R^* - R_n$, luego para todo $y \in R^* - R_{n+1}$, $y \in R^* - R_n$, asi las cosas $R_{n+1} = \{x \in R^* \mid g(x) \leq g(y) \quad \text{para todo} \quad y \in R^* - R_n \supseteq R^* - R_{n+1}\}$, esto es, $R_{n+1} \subseteq R_{n+2}$.

Para el resto del argumento, asumimos que (R, g) es un dominio euclidiano con **d.r.p.**

Lema 2.5.1

Si $u \in U(R)$ y $u = \pm 1$, entonces $1 + u \in U(R)$.

Demostración:

Sea $u \in U(R)$ y $u = \pm 1$, demostremos que $1 + u \in U(R)$. En efecto:

Recordemos que si $v \in U(R)$, entonces $g(v) < g(r)$ para $r \in R^* - U(R)$, ya que $R_1 = U(R)$, además es claro que $1, -u, u^2$ son unidades puesto que $1 \in U(R)$, como $u \in U(R)$, exíste $v \in R$ tal que $uv = 1$, así $(-u)(-v) = uv = 1$ por tanto exíste $-u \in U(R)$ y por ultimo como $u \in U(R)$, y $U(R)$ es un grupo bajo la multiplicación se tiene que $u^2 \in U(R)$, además son

distintos entre sí por hipótesis. Ahora bien,

$$1 \equiv 1(mod(1+u)$$

$$1 \equiv -u(mod(1+u))$$

$$1 \equiv u^2(mod(1+u))$$

Si $1+u \notin U(R))$ entonces $g(1) < g(1+u), g(-u) < g(1+u)$ y $g(u^2) < g(1+u)$, porque $1, -u, u^2 \in U(R)$ y $(1+u) \in R^* - U(R)$. Así para el par $1, 1+u$ se viola **d.r.p.**. Por tanto $1+u \in U(R)$.

Lema 2.5.2

$U(R) \cup \{0\}$ no es un campo con respecto a las operaciones de adición y multiplicación en R.

Demostración:

Razonemos por reducción al absurdo: Asumamos que $U(R) \cup \{0\}$ es un campo bajo las operaciones de R. Sea $r \in R_2 - R_1$. Puesto que R tiene la propiedad del doble residuo, exíste $u \in U(R), u \neq 1$ y $q \in R$ tal que $1 = qr + u$ por supuesto $qr = 1 - u \in U(r)$ pues por el lema 2, $1+u \in U(R)$ ya que $u \in U(R), u \neq 1$, además como $U(R)$ es el grupo de las unidades de R, $-u \in U(R)$,se tiene que $1 - u \in U(R)$ asi se tendría que $qr \in U(R)$, lo cual es una contradicción, por la escogencia de r.

Lema 2.5.3

Como un elemento de R, 2 no es cero ni unidad.

Demostración:

Si $2 \in U(R) \cup \{0\}$, entonces por el lema 2.5.1,nos asegura que para todo $u, v \in U(R)$, o $u+v = 0$ o $u + v = u(1+u)^{-1}v \in U(R))$. A consecuencia $U(R) \cup \{0\}$ es un campo bajo las operaciones de R, lo cual es absurdo por lema 2.5.2.

Corolario 2.5.1

La característica de R es cero.

Demostración: Como R es un dominio de integridad, entonces su característica es cero o un número primo. Por el lema 2.5.3 $char(R) \neq 2$ y $2 \notin U(R)$. Así se tiene lo que se quería.

Lema 2.5.4

Para cada n, R_n es un conjunto finito.

Demostración: Por el corolario 2.9, se tiene que R es finito. Asumamos que R_{n-1} es finito y sea $x \in R_n - R_{n-1}$. Por **d.r.p** cada clase lateral del ideal (x) distinto de cero contiene exactamente dos elementos de R_{n-1}. Así $R/(x)$ es una anillo finito con $k = 1 + \frac{1}{2}(\sharp R_{n-1})$ elementos. Puesto que $R/(x)$ es un grupo finito (bajo adición) con k elementos, se sigue que en $R/(x)$, $k(1 + (x)) = k + (x) = (x)$. sin embargo, $k = 1 + \frac{1}{2}(\sharp R_{n-1})$ es divisible por x.Porque R es un dominio de factorización única con un grupo finito de unidades, $k = 1 + \frac{1}{2}(\sharp R_{n-1})$ tiene solamente un número finito de divisores en R, asi se tiene el teorema.

Observación: Puesto que R es un conjunto finito y puesto que cada R_n es un conjunto finito, $R_n \subseteq R_{n+1}$ para $n \geq 1$.

La prueba del lema de 2.5.4 da el resultado siguiente:

Lema 2.5.5

Para $x, y \in R^*$, $N(xy) = N(x)N(y)$.

Demostración:

Puesto que R es un dominio de ideales principales, el mapeo $R/(x) \longrightarrow (y)/(xy)$ que envia $a + (x)$ a $ay + (xy)$ es una biyección. Puesto que

$$R/(y) \cong \frac{R/(xy)}{(y)/(xy)}.$$

Lema 2.5.6

Para $n \geq 2$, $R_n - R_{n-1} = \{x \in R^* \mid N(x) = 1 + \frac{1}{2}(\sharp R_{n-1})\}$.

Demostración: Por el lema 2.5.4 se sigue que

$$R_n - R_{n-1} \subseteq \{x \in R^* \mid N(x) = 1 + \frac{1}{2}(\sharp R_{n-1})\}$$

Sin embargo, los conjuntos $R_n - R_{n-1}$, para $n > 1$ son no vacios y su unión es $R^* - U(R)$, mientras que los conjuntos $\{x \in R^* \mid N(x) = 1 + \frac{1}{2}(\sharp R_{n-1})\}$ son disyuntos. Asi se tiene el lema.

Corolario 2.5.2

Para $x, y \in R^*$, $g(x) < g(y)$ sí y solo sí $N(x) < N(y)$. Por tanto el dominio euclidiano (R, N)

también tiene d.r.p. Por otra parte, para $y \in R^*$,

$$\sharp\{x \in R^* \mid N(x) < N(y)\} = 2(N(y) - 1). \qquad (*)$$

TEOREMA 2.5.1 Si (R, g) es un dominio euclidiano con **d.r.p.**, entonces $R = \mathbb{Z}$.

Demostración:Para demostrar el teorema se procedera de manera inductiva:
Primeramente, se probará que $R_2 - R_1 = \{r \mid N(r) = 2\} = \{\pm 2\}$. Sea $r \in R_2 - R_1$. Puetso que $N(r) = 2, rs = 2$ para algún $s \in R$. Veamos que $N(s) = 1$. Este hecho implica que s es una unidad, así $r = \pm 2$. Obsérvese que $N(r^2) = N(r)N(r) = 2 \cdot 2 = 4$ y que $1 \equiv r \equiv r^2(mod(r-1))$, esto es, $1 \equiv 1 mod(r-1), 1 \equiv r mod(r-1), 1 \equiv r^2 mod(r-1)$, luego, por **d.p.r** $N(r-1) \leq 4$ puesto que $r^2 > r^2 - 1$ así, $4 = N(r^2 \geq N(r^2 - 1) = N((r+1)(r-1)) = N(r+1)N(r-1)$, así, $N(r+1)N(r-1) \leq 4$. Similarmente, $N(\pm 1 \pm r) \leq 4$. Ahora, no hay dos $(\pm 1 \pm r)$ que sean iguales, pero son congruentes $mod 2$. Por **d.p.r** $N(2) \leq 4$ y así $N(s) \leq 2$. Si todos $\pm 1 \pm r$ tienen la norma menor que 4, entonces $N(2) < 4$, sino **d.p.r** es violado. y si $N(2) < 4$, entonces $N(s) = 1$ como se quería. Asúmase sin perder generalidad que $N(1 - r) = 4$, y que $N(s) = 2$. Puesto que todo elemento de norma 4 es un producto de irreducibles dividido por 2, y puesto que r no divide a $r - 1$ se debe tener $1 - r = \pm s^2$. Ahora

$$R_2 - R_1 = \{x \mid N(x) = 2\} = \{\pm r, \pm s\},$$

y

$$R_3 - R_2 = \{x \mid N(x) = 4\} = \{\pm r^2, \pm rs, \pm s^2\}.$$

Así, puesto que $N(r+1) \leq 4$, $1 + r = \pm s$. Sin embargo, $s^2 = (1+r)^2 = \pm(1-r)$. Si $(1+r)^2 = 1 - r$ entonces $r = -3$ y $s = \pm 2$ lo cual implica que $r = \pm 1$, lo cual es una contradicción. De aquí $(1+r)^2 = -1 + r$ o $r^2 + r + 2{=}0$; así $r = (-1 \pm \sqrt{-7})/2$, y $s = -1 - r = -(1 \pm \sqrt{-7})/2$. Sea $x \in R_4 - R_3 = \{y \backslash N(y) = 7\}$. Claramente x divide a $\sqrt{-7}$ y así x divide a $r - s = 1 + 2r = \pm\sqrt{-7}$. Sin embargo, $r^2 \equiv rs \equiv s^2(modx)$ el cual contradice **d.p.r**. Así se concluye que $N(s) = \pm 1$, y de aquí $R_2 - R_1 = \{\pm 2\}$.

Para concluir la prueba, se argumenta por inducción que $N(n) = n$ para todo n. Este resultado se ha demostrado para $n \leq 2$. Supóngase que $N(k) = k$ para $k < n$. Si n es compuesto,

entonces $N(n) = n$ por hipótesis de inducción.

Sea n un número primo impar, entonces

$$N(n+1) = N(2(n+1)/2) = 2(n+1)/2 = n+1$$

Puesto que $1 \equiv 1 - n \equiv n + 1(modn), N(n) \leq n + 1$. Pero 1 tiene orden n aditivo en $R/(n)$ y así n divide a $N(n)$ donde $N(n) = n$. Dejar que $y = n$ en (*) tenemos que

$$\{x \in R^* \mid N(x) < n\} = \{\pm 1, \pm 2, ..., \pm(n-1)\}$$

Tomando la unión para todos los n, se concluye que $R = \mathbb{Z}$

BIBLIOGRAFÍA

[1] *Ağargün*, A.C, Fletcher C.R. Euclideans Rings,Tr.J. of mathematics, 19,291-399 (1995).

[2] Cámpoli, O. A principal ideal domain that is not a eucludean domain, Amer. Math. Monthly. Nov, 1988, 868-871.

[3] Galovich,S. A charactization of the integers among euclidean domain, Americam Math.Soc.Monthy 85(1978), 572-575.

[4]Hungerford, T. Algebra, Springer-Verlag, New York,1974.

[5]Jodeit, M.A, Uniqueness in the division algorithm, American Math.Soc.Monthy 74(1967), P. 835-836.

[6] Lang S. Algebra, Springer-Verlang, New York 2002.

[7] Lenstra, H. W. Lectures on euclidean rings, Bielefeld, summer, 1974.

[8] Lequian Yves, García Arnaldo, Elementos de álgebra,IMPA, 2002, Rio de Janeiro.

[9] Motzkin, T. The euclidean algorithm, Bull. Amer. Math.Soc. 55, 1142-1146 (1949).

[10] Picavet, G. Caracterisation de certains type d'anneaux euclidiens enseignement math, 18 (1972), 245-254.

[11] Pinter Charles C. Set theory, addinson wesley publishing company,1971.

[12] Samuel P.About euclidean ring, J. alg-, 19, 282-301 (1971).

[13]Zariski, O, Samuel, P. Conmutative algebra I,Van Nostrand, New York.1958.