UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ALGUNOS EJEMPLOS EN TEORIA DE ANILLOS.

TESIS QUE PARA OBTENER EL

TITULO DE MATEMATICO

PRESENTA:

MARITZA SIRVENT DE HERNANDEZ.

MEXICO, D.F. 1982.

INTRODUCCION

En la sección 1, se da una clasificación de todos los anillos de orden menor que 8. En esta sección todos los anillos serán asociativos, no necesariamente conmutativos o con idéntico.

Los grupos aditivos de anillos son abelianos y por lo tanto, si el orden es menor que 8 todos son cíclicos, excepto el grupo de Klein $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ de orden 4. De aquí que tenga sentido discutir el caso cíclico por separado.

Observación: Todo anillo con grupo aditivo cíclico debe ser conmutativo. Si a es un generador del anillo, entonces cada elemento puede ser expresado en la forma:

$$a + \cdots + a = ka \quad , \quad k \in \mathbb{Z}.$$

$$\therefore (k_1 a)(k_2 a) = (k_1 k_2) a^2 = (k_2 a)(k_1 a)$$

Por lo tanto, todos los anillos por determinar serán conmutativos, excepto para algunos con grupo aditivo V.

En la sección 2, se generaliza para el caso no conmutativo el siguiente resultado de Camilo:
Si $R[x]$ es semihereditario con R conmutativo, entonces R es un anillo Von Neumann regular.

En la sección 3, se trata con el problema de cuándo un dominio LCM derecho, es un dominio LCM izquierdo.
El problema de si un dominio de ideales principales derecho (PRI) que cumpla la condición Ore izquierdo

es un dominio de ideales principales izquierdo (D.I.) está abierto.
Aquí se muestra que un dominio LCM derecho que cumple Ore izquierdo, no necesariamente es un dominio LCM izquierdo. Pero será cierto con la hipótesis adicional de que el anillo tenga la condición ascendente de cadena para ideales principales izquierdos.
De hecho, el ejemplo dado es de un dominio LCM derecho acotado (y por lo tanto Ore izquierdo) el cual no es un dominio LCM izquierdo.

En la sección 4, se dan respuestas a dos conjeturas de J.W. Fisher; así si R es un anillo semiprimo que satisface una identidad polinomial, entonces.

1) El anillo máximo de cocientes derecho de R, satisface una identidad polinomial.
2) El anillo máximo de cocientes derecho de R, coincide con el anillo máximo de cocientes izquierdo de R.

Esta tesis está basada en cuatro artículos de Colin R. Fletcher, P. Pillay, Raymond A. Beauregard y Wallace S. Martindale III, respectivamente.

AGRADECIMIENTOS.

Deseo agradecer al Dr. Francisco Raggi C., director de esta tesis y profesor de una gran parte de mis cursos, por su ayuda y atención para la elaboración de este trabajo.

Tambien agradezco al M. en C. José Ríos M., por el interés que mostró y por sus atinadas observaciones.

Por último, deseo expresar mi más profundo agradecimiento a Luis Hernández L., por su apoyo y comprensión.

ANILLOS DE ORDEN PEQUEÑO.

§1. ANILLOS CON GRUPO ADITIVO CICLICO.

Teorema 1.- Sean A y B anillos con grupos aditivos C_n generados por a y b respectivamente, donde $a^2 = ka$ y $b^2 = kb$ entonces A y B son isomorfos $\Leftrightarrow$ $(k,n) = (l,n)$.

Dem. $\Rightarrow$) Sea $\phi: A \longrightarrow B$ isomorfismo
donde $\phi(a) = mb$
ϕ es sobre $\therefore \exists\, k_1 a \in A \ni \phi(k_1 a) = b$
$b = \phi(k_1 a) = k_1 \phi(a) = k_1 mb$
entonces $k_1 m \equiv 1 \pmod{n}$
$nq = k_1 m - 1$
$\therefore 1 = k_1 m - nq$
$\therefore (m,n) = 1$

ϕ es homomorfismo de anillos
$\therefore kmb = \phi(ka) = \phi(a^2) = \phi(a)\phi(a) = m^2 b^2 = m^2 lb$
$\therefore km = m^2 l \pmod{n}$

Ahora $(k,n) \mid k, n$
$\therefore (k,n) \mid ml$, $(m,n) = 1$
$\therefore (k,n) \mid l$
$\therefore (k,n) \mid (l,n)$

Análogamente $(l,n) \mid (k,n)$
$\therefore (k,n) = (l,n)$ ∎.

Para demostrar la otra implicación, antes demostraremos el siguiente Lema:

Lema. $(k_1,n) = (l_1,n) \Leftrightarrow \exists\, x \ni k_1x \equiv l_1 \pmod n$ y $(x,n)=1$.

Dem. $\Rightarrow$) Vamos a encontrar todas las soluciones de la congruencia $k_1x \equiv l_1 \pmod n$.

$(k_1,n) \mid l$ $\therefore$ la congruencia tiene solución.
Sea m una solución de $k'x \equiv l' \pmod{n'}$, $0 \le m < n'$
donde $k_1 = dk'$, $l_1 = dl'$, $n = dn'$; $d = (k_1,n)$

Definimos para $j = 0, 1, \ldots, d-1$
$$m_j = m + jn'$$
ent. $m_j \equiv m \pmod{n'}$
$\therefore$ m_j es una solución de $k'x \equiv l' \pmod{n'}$
y es también solución de $k_1x \equiv l_1 \pmod n$

Además, puesto que:
$$0 \le m_0 < m_1 < m_2 < \ldots < m_{d-1} < n$$
se sigue que si $0 \le i < j \le d-1$, ent. $m_i \not\equiv m_j \pmod n$

Afirmación: $\{m_0, m_1, \ldots, m_{d-1}\}$ es el conjunto de soluciones de $k_1x \equiv l_1 \pmod n$.

dem. de la Af.:
$\forall\, t \ni k_1t \equiv l_1 \pmod n \Rightarrow m_r \equiv t \pmod n$ p.a. r
Sup. $k_1t \equiv l_1 \pmod n \Rightarrow k't \equiv l' \pmod{n'}$
además $(k',n') = 1$ $\therefore$ la sol. es única
$\therefore$ $t \equiv m \pmod{n'}$
$\therefore$ $t = m + rn'$ p.a. r
por el algoritmo de la división, $r = qd + r'$ $0 \le r' \le d-1$
$\therefore$ $t = m + r'n' + qn = m_r + qn \equiv m_r \pmod n$

$(k', n') = 1 \quad \therefore \exists\, m \;\ni\; k'm \equiv l' \pmod{n'}$

$(l', n') = 1 \quad \therefore \exists\, m' \;\ni\; l'm' \equiv k' \pmod{n'}$

$\therefore k'mm' \equiv k' \pmod{n'}$ y $(k', n') = 1$

$\therefore mm' \equiv 1 \pmod{n'}$

$\therefore (m, n') = 1$

Por Teorema de Dirichlet:

$A = \{m + n'j \mid j \in \mathbb{Z}\}$ contiene a una infinidad de primos.

$\therefore \exists\, p \in A \;\ni\; p \nmid n$

$\therefore k_1 p \equiv l_1 \pmod{n}$ y $(p, n) = 1$ ∎

$\Leftarrow$) $(l_1, n) \mid l_1, n$

$\therefore (l_1, n) \mid k_1 x$, $(x, n) = 1$

$\therefore (l_1, n) \mid k_1$

$\therefore (l_1, n) \mid (k_1, n)$

Análogamente $(k_1, n) \mid (l_1, n)$

$\therefore (k_1, n) = (l_1, n)$ ∎.

Ahora demostraremos $\Leftarrow$) del Teorema:

$(k_1, n) = (l_1, n)$, por el Lema $\exists\, m \;\ni\; l_1 m \equiv k_1 \pmod{n}$, $(m, n) = 1$

Sea $\phi : A \longrightarrow B$ dada por

$\phi(a) = mb$

y $\phi(ra) = r\phi(a)$

i) ϕ es morfismo de anillos.

Sean $ra, sa \in \Lambda$ con $0 \le r \le n-1$, $0 \le s \le n-1$

$\phi(ra \cdot sa) = rs\,\phi(a^2) = rs\,\phi(ka) = rsk\,\phi(a) = rskmb$

$\phi(ra)\,\phi(sa) = rs\,\phi(a)^2 = rs\,m^2 b^2 = rs\,m^2 \ell b$

como $km \equiv m^2 \ell \pmod n$

ent. $\phi(ra \cdot sa) = \phi(ra)\,\phi(sa)$. ∎

ii) ϕ es inyectiva.

Sean $ra, sa \in \Lambda$, $r, s \in \mathbb{Z}$ t.

$\phi(ra) = \phi(sa)$

$\therefore$ $rmb = smb$

$\therefore$ $rm = sm \pmod n$ y $(m,n) = 1$

$\therefore$ $r \equiv s \pmod n$

$\therefore$ $ra = sa$. ∎

iii) ϕ es suprayectiva.

Sea $tb \in B$, $t \in \mathbb{Z}$.

$\exists\ ra \in \Lambda$ t. $\phi(ra) = tb$ ya que $rm \equiv t \pmod n$.

$\therefore$ ϕ es isomorfismo. ∎.

Corolario. Existen tantos anillos distintos con grupo aditivo cíclico $\mathcal{C}_n$ como divisores de n.

Dem. Sean $n_1, \ldots, n_k$ los divisores de n
$\therefore (n_i, n) \neq (n_j, n)$ si $i \neq j$

$\therefore$ Existen al menos k anillos distintos con grupo aditivo cíclico $\mathcal{C}_n$.

Sea A un anillo con grupo aditivo cíclico $\mathcal{C}_n$ tal que $a^2 = ma$, sea $d = (m,n)$
como $d|n$ ent. $d = n_i$ p.a. $i \in \{1, \ldots, k\}$
$(n_i, n) = n_i = (m,n)$ $\therefore A_i \subseteq A$.

$\therefore$ Existen exactamente k anillos distintos con grupo aditivo cíclico $\mathcal{C}_n$. ∎.

Cualquier entero positivo n tiene los divisores 1 y n.
Supongamos primero que:

$$a^2 = 1a = a, \quad \text{ent.}$$
$$(k_1 a)(k_2 a) = (k_1 k_2) a^2 = (k_1 k_2) a = (\overline{k_1 k_2})\, a$$

donde $\overline{k_1 k_2}$ denota el residuo cuando $k_1 k_2$ es dividido por n.

$\therefore$ El anillo es isomorfo a $\mathbb{Z}_n$
(bajo el mapeo $ka \to k$).

Ahora supongamos que:

$$a^2 = na = 0, \quad \text{ent.}$$
$$(k_1 a)(k_2 a) = (k_1 k_2) a^2 = 0$$

y obtenemos el anillo trivial $\mathcal{O}_n$, donde el producto de elementos son siempre cero.

Notemos que $\mathbb{Z}_n$ es un anillo conmutativo con idéntico ($n \geq 2$)
Pero $\mathcal{O}_n$, claramente no tiene un idéntico.
Cuando $n=1$, el anillo consiste del elemento cero solamente y $\mathbb{Z}_n$ y $\mathcal{O}_n$ coinciden.
Cuando n es primo, 1 y n son los únicos divisores de n y entonces $\mathbb{Z}_n$ y $\mathcal{O}_n$ son los únicos anillos posibles con grupo aditivo cíclico C_n.
∴ Los casos cuando $n = 2, 3, 5$ y 7 han sido resueltos.

Cuando $n=4$, sus divisores son 1, 2 y 4
Ent. hay 3 anillos con grupo aditivo C_4.
Para los divisores 1 y 4 tenemos los anillos $\mathbb{Z}_4$ y $\mathcal{O}_4$.
El restante es formado del producto $a^2 = 2a$
(notemos que $(1,4) = (3,4)$ y ∴ $a^2 = 3a$ nos da $\mathbb{Z}_4$ otra vez).
Este tercer anillo es conmutativo (pues C_4 es cíclico), no trivial y no tiene idéntico. (ya que si tuviera, digamos ja ∴ $(ja)a = a$, ent. $a = ja^2 = 2ja$
∴ $2j \equiv 1 \pmod 4$ ∴ $4 \mid 2j - 1$ ↯).

Cuando $n=6$, hay 4 anillos: $\mathbb{Z}_6$, $\mathcal{O}_6$, $a^2 = 2a$, $a^2 = 3a$.
$a^2 = 2a$ lo podemos identificar con $\mathbb{Z}_3 \oplus \mathcal{O}_2 = \{(x,y) \mid x \in \mathbb{Z}_3, y \in \mathcal{O}_2\}$.
haciendo $a = (2,1)$, tenemos:
$(2,1)^2 = (2^2, 1^2) = (1,0) = (2,1) + (2,1)$
Análogamente, el anillo $a^2 = 3a$ nos da $\mathbb{Z}_2 \oplus \mathcal{O}_3$
donde $a = (1,1)$.

Y de estos cuatro anillos, $\mathbb{Z}_6$ es el único que tiene idéntico.

Teorema 2. Excepto por isomorfismo, el único anillo A con idéntico que tiene grupo aditivo $\mathcal{C}_n$ es $\mathbb{Z}_n$.

Dem. Sea a un generador de $\mathcal{C}_n$ donde $a^2 = ka$ y sea ja la identidad. Ent.

$$a = (ja)a = ja^2 = jka$$
$$\therefore jk \equiv 1 \pmod{n}$$
$$\therefore (j,n) = 1 = (1,n)$$
$$\therefore A = \mathbb{Z}_n.$$

Teorema 3. Excepto por isomorfismo, el número de anillos distintos con grupo aditivo $\mathcal{C}_n$ donde $n = p_1^{\alpha_1} \dots p_i^{\alpha_i}$ está dado por:

$$\varphi(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_i+1)$$

Dem. $\varphi(n)$ cuenta el número de divisores de n.

Por el Teorema 2, solo uno de estos anillos tiene idéntico.

§2. ANILLOS NO CONMUTATIVOS.

Teorema 4. Si $n \in \mathbb{N}$, $n>1$, entonces existe un anillo no conmutativo de orden $n \Leftrightarrow n$ tiene factores cuadrados.

Dem.

$\Rightarrow$) Supongamos que n no tiene factores cuadrados sea A el grupo aditivo de un anillo de orden n. Por el teorema fundamental de grupos abelianos finitamente generados, a A lo podemos expresar como sigue:

$A = C_{n_1} \oplus \dots \oplus C_{n_i}$ donde C_{n_j} es un grupo cíclico finito y $n_\alpha | n_{\alpha+1}$ para $1 \leq \alpha < i$ $n_1 > 1$.

Como $n = n_1 \dots n_i$, entonces
Si $i>1$, n tiene factores cuadrados ($n_1 | n_2 \therefore n_2 = n_1 q$
$\therefore n = n_1^2 q \dots n_i$)

$\therefore$ $i = 1$
$\therefore$ $A = C_{n_1}$
$\therefore$ A es cíclico
$\therefore$ El anillo debe ser conmutativo.

$\Leftarrow$) Sea p primo y formemos la suma directa C_p consigo mismo. donde $p^2 | n$.
$\therefore$ $C_p \oplus C_p$ es un grupo aditivo con p^2 elementos
Ahora construiremos un anillo no conmutativo R con $C_p \oplus C_p$ como grupo aditivo.

Sea a un generador de C_p
entonces $(a,0)$ y $(0,a)$ generan a R aditivamente.

Definimos la multiplicación como sigue:

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

En general

$$(ka, la)(ra, sa) = \{\overbrace{(a,0)+\dots+(a,0)}^{k\text{-veces}} + \overbrace{(0,a)+\dots+(0,a)}^{l\text{-veces}}\} \times \{\underbrace{(a,0)+\dots+(a,0)}_{r} + \underbrace{(0,a)+\dots+(0,a)}_{s}\}$$
$$= k(r+s)(a,0) + l(r+s)(0,a)$$
$$= (k(r+s)a,\ l(r+s)a)$$

Ahora,

$$(ra, sa)(ka, la) = r(k+l)(a,0) + s(k+l)(a,0)$$
$$= (r(k+l)a,\ s(k+l)a)$$

$$\therefore (ka, la)(ra, sa) \neq (ra, sa)(ka, la)$$

La asociatividad es fácil de checar.

$\therefore$ R es un anillo no conmutativo de orden p^2.

Finalmente, un anillo no conmutativo de orden kp^2 está definido, tomando:

$$\mathbb{O}_k \oplus R \quad \text{ó} \quad \mathbb{Z}_k \oplus R$$

Son no conmutativos ya que contienen un subanillo isomorfo a R.

Ejemplo. Sea $p = 2$

Sea R que consiste de los pares: $(0,0)$; $(a,0)$; $(0,a)$; (a,a) donde a es el generador de C_2.

+	$(0,0)$	$(a,0)$	$(0,a)$	(a,a)
$(0,0)$	$(0,0)$	$(a,0)$	$(0,a)$	(a,a)
$(a,0)$	$(a,0)$	$(0,0)$	(a,a)	$(0,a)$
$(0,a)$	$(0,a)$	(a,a)	$(0,0)$	$(a,0)$
(a,a)	(a,a)	$(0,a)$	$(a,0)$	$(0,0)$

•	$(0,0)$	$(a,0)$	$(0,a)$	(a,a)
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(a,0)$	$(0,0)$	$(a,0)$	$(a,0)$	$(0,0)$
$(0,a)$	$(0,0)$	$(0,a)$	$(0,a)$	$(0,0)$
(a,a)	$(0,0)$	(a,a)	(a,a)	$(0,0)$

§ 3. Anillos No conmutativos de orden 4.

El único grupo abeliano no-cíclico de orden menor que 8 es el grupo de Klein V de orden 4 $(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.

Sea R un anillo con grupo aditivo V y sean las siguientes tablas:

+	0	a	b	a+b
0	0	a	b	a+b
a	a	0	a+b	b
b	b	a+b	0	a
a+b	a+b	b	a	0

·	0	a	b	a+b
0	0	0	0	0
a	0	x_1	x_2	x_1+x_2
b	0	x_3	x_4	x_3+x_4
a+b	0	x_1+x_3	x_2+x_4	$x_1+x_2+x_3+x_4$

Este anillo está definido, únicamente cuando los valores x_1, x_2, x_3, x_4 han sido dados.

Denotamos a R por (x_1, x_2, x_3, x_4)
Para cada x_i, existen cuatro posibilidades.
∴ Existen 256 casos para formar R.
Sin embargo, este número se reduce con las leyes asociativas.
Las leyes distributivas, no reducen el número de casos, ya que R ha sido construido suponiendo que estas leyes se cumplen.

La Ley asociativa, $f(gh) = (fg)h \quad \forall f, g, h \in R$ claramente se satisface cuando cualquiera de los elementos es cero.
Si se satisface cuando $f, g, h \in \{a, b\}$ entonces se satisface en general.
Por ejemplo, consideremos el caso cuando

$f = a+b$, $g = a$, $h = b$

$(a+b)(ab) = a(ab) + b(ab)$ Ley distributiva
$= (aa)b + (ba)b$ " asociativa para $\{a,b\}$.
$= (aa+ba)b$ " distributiva
$= ((a+b)a)b$ " "

$\therefore$ La Ley asociativa se satisface para $a+b, a, b$.

En general la Ley asociativa puede ser reemplazada por las siguientes 8 condiciones:

$aaa = ax_1 = x_1a$ (1) $\quad baa = bx_1 = x_3a$ (2)
$aab = ax_2 = x_1b$ (3) $\quad bab = bx_2 = x_3b$ (4)
$aba = ax_3 = x_2a$ (5) $\quad bba = bx_3 = x_4a$ (6)
$abb = ax_4 = x_2b$ (7) $\quad bbb = bx_4 = x_4b$ (8)

Tomaremos los casos no conmutativos y conmutativos por separado.

Supongamos primero que R es no conmutativo.
Ent. existen $4\times4\times3\times4 = 192$ posibilidades para x_1, x_2, x_3, x_4.
(ya que $ba = x_3$, $ab = x_2$ y para que $ab \neq ba$ necesitamos que $x_3 \neq x_2$, i.e. para x_3 solo tenemos 3 posibilidades).

Si $x_1 = b$ ó $x_1 = a+b$ ent. R es conmutativo [de (1)]
Ent. $x_1 = 0$ ó $x_1 = a$ y análogamente [de (8)]
$x_4 = 0$ ó $x_4 = b$
entonces tenemos $2\times4\times3\times2 = 48$ casos.

Si $x_2 = a+b$ ent. (de (3))
$a(a+b) = x_1b$ $\therefore x_1+x_2 = x_1b$

Si $x_1 = 0$ ent. $x_2 = 0$ y $\therefore$ $a+b=0$ ↯.
Si $x_1 = a$ ent. $x_1 + x_2 = x_2$ y $\therefore$ $x_1 = 0 = a$ ↯.

$\therefore$ $x_2 \neq a+b$ y análogamente (de (6)) $x_3 \neq a+b$

Finalmente si $x_1 = x_4 = 0$ ent. (de (3) y (7))

$0 = ax_2 = x_2 b$ y la única solución de esta ecuación es $x_2 = 0$
ya que si $x_2 = a$ ent. $0 = ab$ y $\therefore$ $x_2 = 0$ ↯.
si $x_2 = b$ ent. $0 = ab$ ↯.

Análogamente $x_3 = 0$, lo cual haría a R conmutativo.

$\therefore$ Esto nos deja con: $2 \times 3 \times 2 \times 2 - 1 \times 3 \times 2 \times 1 = 18$ casos
hasta aquí, las posibilidades de x_1, x_2, x_3, x_4 se pueden resumir en la siguiente tabla:

x_1	0	a	a
x_4	b	0	b
x_2	0, a ó b		
x_3	pero no iguales.		

Supongamos $x_1 = 0$ y $x_4 = b$ ent. (de (2) y (3))
$ax_2 = 0 = x_3 a$ si $x_2 = b$ ent. $ab = 0$ $\therefore$ $x_2 = 0$ ↯.
si $x_3 = b$ ent. $ba = 0$ $\therefore$ $x_3 = 0$ ↯.

$\therefore$ las dos posibilidades restantes son:
$(0,0,a,b)$; $(0,a,0,b)$ y ambos nos dan anillos.

Análogamente si $x_1 = a$ y $x_4 = 0$, ent.

$x_2 b = 0 = b x_3$ (de (7) y (6))

Si $x_2 = a$ ent. $x_2 = 0$ C.

$x_3 = a$ ent. $x_3 = 0$ L.

∴ Aquí tenemos otra vez dos anillos:

$\underline{(a, b, 0, 0)}$; $\underline{(a, 0, b, 0)}$.

Los 6 casos finales son cuando:

$x_1 = a$, $x_4 = b$ (de (4) y (5)) $b x_2 = x_3 b$ y

$a x_3 = x_2 b$

Si $x_2 = 0$ ent. $x_3 b = 0 = a x_3$ y la única solución es $x_3 = 0$ lo cual no puede ser porque entonces R sería conmutativo.

Análogamente si $x_3 = 0$ es una contradicción

∴ los dos casos restantes son:

$\underline{(a, b, a, b)}$ y $\underline{(a, a, b, b)}$.

§ 4. Anillos isomorfos de orden 4.

Cualquier isomorfismo de anillos es un isomorfismo de grupos de los grupos aditivos fundamentales de los anillos. Y un isomorfismo de grupos del grupo de Klein debe tener la forma de una permutación de los elementos a, b y a+b.

Existen 6 de tales permutaciones, a saber (llamándola a+b=c y las permutaciones poniéndolas como ciclos):

La identidad ; (a,b); (bc); (ca); (abc); (acb).

Supongamos que (x_1, x_2, x_3, x_4) es un anillo R de orden 4. y sea:

$$\phi: R \longrightarrow R \quad \text{un isomorfismo}$$
$$x_i \longmapsto \phi(x_i) \quad \text{para } i = 1, 2, 3, 4.$$

Como un ejemplo, consideremos $\phi = (ca)$.
Esto es $\phi(a) = c$; $\phi(b) = b$; $\phi(c) = a$.

$\cdot$	$\phi(0)$	$\phi(a)$	$\phi(b)$	$\phi(c)$
$\phi(0)$	$\phi(0)$	$\phi(0)$	$\phi(0)$	$\phi(0)$
$\phi(a)$	$\phi(0)$	$\phi(x_1)$	$\phi(x_2)$	$\phi(x_1+x_2)$
$\phi(b)$	$\phi(0)$	$\phi(x_3)$	$\phi(x_4)$	$\phi(x_3+x_4)$
$\phi(c)$	$\phi(0)$	$\phi(x_1+x_3)$	$\phi(x_2+x_4)$	$\phi(x_1+x_2+x_3+x_4)$

=

	0	c	b	a
0	0	0	0	0
c	0	$\phi(x_1)$	$\phi(x_2)$	$\phi(x_1)+\phi(x_2)$
b	0	$\phi(x_3)$	$\phi(x_4)$	$\phi(x_3)+\phi(x_4)$
a	0	$\phi(x_1)+\phi(x_3$	$\phi(x_2)+\phi(x_4)$	$\phi(x_1)+\phi($ $+\phi(x_2)+\phi($

Ahora colocando la tabla en orden usual:

	0	a	b	c
0	0	0	0	0
a	0	$\phi(x_1)+\cdots+\phi(x_1)$	$\phi(x_2)+\phi(x_4)$	$\phi(x_1)+\phi(x_3)$
b	0	$\phi(x_3)+\phi(x_4)$	$\phi(x_4)$	$\phi(x_3)$
		$\phi(x_\cdot)$	$\phi(x_\cdot)$	$\phi(x_1)$

Y el anillo nos queda:

$$(\phi(x_1)+\phi(x_2)+\phi(x_3)+\phi(x_4),\ \phi(x_2)+\phi(x_4),\ \phi(x_3)+\phi(x_4),\ \phi(x_4)).$$

Sea $R = (a,b,a,b)$ el anillo encontrado antes.
ent. bajo (ca) este anillo es isomorfo a:
$(c+b+c+b,\ b+b,\ c+b,\ b)$ esto es

$(a,b,a,b) \cong (0,0,a,b)$ y este es el primer anillo encontrado.

De manera semejante, podemos determinar el anillo imagen de cada una de las permutaciones.

Identidad	$(\phi(x_1),\ \phi(x_2),\ \phi(x_3),\ \phi(x_4))$
(ab)	$(\phi(x_4),\ \phi(x_3),\ \phi(x_2),\ \phi(x_1))$
(bc)	$(\phi(x_1),\ \phi(x_1)+\phi(x_2),\ \phi(x_1)+\phi(x_3),\ \phi(x_1)+\phi(x_2)+\phi(x_3)+\phi(x_4))$
(ca)	$(\phi(x_1)+\phi(x_2)+\phi(x_3)+\phi(x_4),\ \phi(x_2)+\phi(x_4),\ \phi(x_3)+\phi(x_4),\ \phi(x_4))$.
(abc)	$(\phi(x_1)+\phi(x_2)+\phi(x_3)+\phi(x_4),\ \phi(x_1)+\phi(x_3),\ \phi(x_1)+\phi(x_2),\ \phi(x_1))$.
(acb)	$(\phi(x_4),\ \phi(x_3)+\phi(x_4),\ \phi(x_1)+\phi(x_4),\ \phi(x_1)+\phi(x_2)+\phi(x_3)+\phi(x_4))$.

De esto obtenemos los siguientes:

$(a,b,a,b) \cong (0,0,a,b)$ bajo (ca)
$\cong (a,b,0,0)$ bajo (bc)

$(a,a,b,b) \cong (0,a,0,b)$ bajo (ca)
$\cong (a,0,b,0)$ bajo (bc)

Por lo tanto, excepto por isomorfismos, existen solamente dos anillos no conmutativos de orden 1.:

$$(a, b, a, b) \quad \text{y} \quad (a, a, b, b)$$

El último es el anillo construido en § 2.
y el primero es el anillo construido en la misma forma, pero en vez de tomar los factores izquierdos, tomamos los factores derechos.

Cada uno de los anillos tiene identidad por un lado pero ninguno es por los dos lados.

§5 Anillos Conmutativos de orden 4.

Si ponemos $x_3 = x_2$, entonces tenemos un anillo conmutativo de la forma (x_1, x_2, x_2, x_4) y la ley asociativa nos da las dos condiciones:

$$ax_2 = x_1 b \qquad (\text{de } (3) \text{ y } (2)).$$
$$ax_4 = x_2 b$$

Supongamos primero que el anillo tiene un idéntico, digamos a.
Ent. $x_1 = a$
$x_2 = b$

y la ley asociativa se cumple.
Entonces cada uno de los cuatro valores posibles de x_4 nos da un anillo:

$x_4 = 0$ Nos Da un anillo de ideales principales

$x_4 = a$ Nos da el mismo anillo de ideales principales, ya que $(a, b, b, 0) \cong (a, b, b, a)$ bajo (bc).

$x_4 = b$ Nos da $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, otro anillo de ideales principales

$x_4 = a+b$ Nos da $GF(4)$; el campo de Galois de orden 4.

Finalmente, supongamos que los anillos no tienen idéntico. Entonces no son de la forma:

(a, b, b, x_4) con idéntico a.
(x_1, a, a, b) con idéntico b.
$(a+x_2, x_2, x_2, b+x_2)$ " " $a+b$.

Sea $x_1 = 0$, entonces de las leyes asociativas:

$$ax_2 = x_1 b$$
$$ax_4 = x_2 b$$

obtenemos que $ax_2 = 0$ lo cual implica $x_2 \neq b, a+b$

$ax_4 = x_2 b$; Si $x_2 = a$ entonces las únicas soluciones de esta ecuación son:
$x_4 = b$ ó, $x_4 = a+b$ lo cual no puede ser ya que supusimos que el anillo no tenía idéntico.

Entonces nos quedamos con anillos de la forma:

$$(0, 0, 0, x_4).$$

Análogamente:

$x_1 = a$ nos da $(a,0,0,0)$ y (a,a,a,a)
$x_1 = b$ nos da $(b,0,0,0)$ y (b,b,b,b)
y $x_1 = a+b$ nos da $(a+b,0,0,0)$ y $(a+b, a+b, a+b, a+b)$.

Usando los resultados previos sobre isomorfismos, podemos descomponer este conjunto en clases de isomorfismos.

$(0,0,0,0)$ el anillo trivial $\mathbb{O}_2 \oplus \mathbb{O}_2$

$(0,0,0,a) \cong (b,0,0,0)$ bajo (ab)
$\cong (a+b, a+b, a+b, a+b)$ bajo (ca)

$(0,0,0,b) \cong (a,0,0,0)$ bajo (ab)

$\cong (0,0,0,a+b)$ " (bc)

$\cong (b,b,b,b)$ " (ca)

$\cong (a+b,0,0,0)$ " (abc)

$\cong (a,a,a,a)$ " (acb)

Este tercer anillo $(0,0,0,b)$ es $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. $(a \leftrightarrow (0,1)$ y $b \leftrightarrow (1,0))$.

CONCLUSION: Podemos escribir ahora todos los anillos asociativos, incluyendo de orden 7.

En la siguiente hoja, presentamos una tabla con la clasificación de los anillos de orden menor que 8.

Tabla 1.

ORDEN	ANILLO	GRUPO ADITIVO	PROPIEDADES
1	$\mathcal{O}_1$	C_1	Anillo Conmutativo
2	$\mathcal{O}_2$	C_2	Anillo Conmutativo
2	$\mathbb{Z}_2$	C_2	Campo
3	$\mathcal{O}_3$	C_3	Anillo Conmutativo
3	$\mathbb{Z}_3$	C_3	Campo
4	$\mathcal{O}_4$	C_4	Anillo Conmutativo
4	$\mathbb{Z}_4$	C_4	Anillo de Ideales principales
4	$a^2=2a$	C_4	Anillo Conmutativo
4	(a,b,a,b)	V	Anillo no conm. con idéntico izq.
4	(a,a,b,b)	V	Anillo no conm. con " derecho
4	$\mathbb{Z}_2 \times \mathbb{Z}_2$	V	Anillo de ideales principales.
4	$GF(4)$	V	Campo
4	$(a,b,b,0)$	V	Anillo de ideales principales.
4	$\mathcal{O}_2 \oplus \mathcal{O}_2$	V	Anillo Conmutativo
4	$(0,0,0,a)$	V	Anillo Conmutativo
4	$\mathbb{Z}_2 \oplus \mathcal{O}_2$	V	Anillo Conmutativo
5	$\mathcal{O}_5$	C_5	Anillo Conmutativo
5	$\mathbb{Z}_5$	C_5	Campo
6	$\mathcal{O}_6$	C_6	Anillo Conmutativo
6	$\mathbb{Z}_6$	C_6	Anillo de ideales principales
6	$\mathbb{Z}_3 \oplus \mathcal{O}_2$	C_6	Anillo Conmutativo
6	$\mathbb{Z}_2 \oplus \mathcal{O}_3$	C_6	Anillo Conmutativo
7	$\mathcal{O}_7$	C_7	Anillo Conmutativo
7	$\mathbb{Z}_7$	C_7	Campo.

En las descripciones en el §5 y tabla 1, hemos adoptado la convención de que un anillo de ideales principales contiene un idéntico.

Obs. 1 El campo más chico es $\mathbb{Z}_2$ y éste es el dominio Euclidiano, de ideales principales y de - factorización única menor.

Obs. 2. Los anillos de factorización única, de ideales principales y Euclidianos menores que no son - dominios son: $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ y $(a,b,b,0)$.

Estas observaciones se siguen del hecho de que en un anillo finito (dominio finito) son equivalentes los conceptos de anillo de factorización única, - anillo de ideales principales y anillo Euclidiano.

El anillo no conmutativo menor es de orden 4. Este no es un dominio, ya que un anillo finito sin divisores de cero es un anillo con división y cualquier anillo finito con división es un campo (Teorema de Wedderburn).

Sin embargo, aún existen preguntas por hacerse:

1.- ¿Cuáles son los anillos no conmutativos más chicos i) Con un idéntico izquierdo y derecho?
ii) Sin ningún idéntico izquierdo ni derecho?

El único grupo abeliano no cíclico de orden menor que 8 es $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ y los anillos no conmutativos de orden menor que 8 no tienen idéntico por los dos lados, por lo tanto las respuestas para 1.i) y 1.ii) son anillos de orden 8.

Para 1.i) consideremos:

$$\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z}_2 \right\}$$

Para 1.ii) Podemos formar la suma directa de uno de nuestros anillos no conmutativos de orden 4 con D_2.
p.ej.

$$(a, b, a, b) \oplus D_2 .$$

Sabemos que para el grupo cíclico finito $\mathbb{Z}_n$ existen tantos anillos distintos como divisores de n.

Lo siguiente que nos podemos preguntar es cuáles son los anillos con grupo aditivo cíclico infinito, la respuesta es que son el trivial y los $n\mathbb{Z}$, ya que si A es un anillo con grupo cíclico infinito con a un generador, entonces $a \cdot a = ma$ para alguna $m \in \mathbb{Z}$ y por lo tanto $\varphi: A \longrightarrow m\mathbb{Z}$ $\ni$. $\varphi(a) = m$ es un isomorfismo de anillos.

SOBRE ANILLOS DE POLINOMIOS NO CONMUTATIVOS SEMIHEREDITARIOS.

Sea R un anillo asociativo con elemento unitario.

R es Von Neumann regular si $\forall\, a \in R$, $\exists\, a' \in R$ s.t. $aa'a = a$. entonces $e = aa'$ es idempotente y $aR = eR$

Un anillo S es semihereditario derecho si cada uno de sus ideales derechos finitamente generados es proyectivo como un S-mod.

Sea $S = R[x]$ el anillo de polinomios en la indeterminada x. (x conmuta con los elementos de S)

Teorema.- Son equivalentes:

a) R es Von Neumann regular
b) $\forall a \in R$, $aS + xS$ es un ideal derecho proyectivo de S.
c) $\forall a \in R$, $Sa + Sx$ es un ideal izquierdo proyectivo de S.

Dem.

a) $\Rightarrow$ b) Si $a \in R$, ent. $\exists\, a' \in R$ s.t. $aa'a = a$
Sea $e = aa'$
Como $a = (e + (1-e)x)a$;
$x = (e + (1-e)x)(1 - e + ex)$

$e + (1-e)x = aa' + x(1-e)$
Ent. tenemos que $aS + xS = (e + (1-e)x)S$

Sea $f = e + (1-e)x$

f no es un divisor de cero.

dem. Sea $g \in S$, $g = a_0 + a_1 x + \dots + a_n x^n$ $\quad a_i \in R$.

Supongamos $\quad 0 = fg = (e+(1-e)x)(a_0 + a_1 x + \dots + a_n x^n)$

$$= ea_0 + ea_1 x + \dots + ea_n x^n + (1-e)a_0 x + \dots + (1-e)a_{n-1} x^n + (1-e)a_n x^{n+1}$$

$$= ea_0 + (ea_1 + (1-e)a_0)x + \dots + (1-e)a_n x^{n+1}$$

$\therefore e(fg) = 0 \quad$ y $\quad (1-e)(fg) = 0$

$\therefore ea_i = 0 \quad$ y $\quad (1-e)a_i = 0 \quad \forall\, i \in \{1, \dots, n\}$

$\therefore ea_i + (1-e)a_i = 0 \quad \forall i$

$\therefore (e+(1-e))a_i = 0 \quad \forall i$

$\therefore a_i = 0 \quad \forall i$

$\therefore g = 0$

$\therefore$ Como f no es divisor de cero, el siguiente homomorfismo de módulos derechos:

$$\begin{aligned} S_S &\xrightarrow{\alpha} fS_S \\ h &\longmapsto fh \end{aligned}$$

es un isomorfismo. (claramente es epimorfismo.

Si $\alpha(h) = 0 \Rightarrow fh = 0 \Rightarrow h = 0$

$\therefore \alpha$ es monomorfismo).

Como S_S es libre

$\therefore$ Proyectivo

$\therefore fS_S$ es proyectivo

$\therefore aS + xS$ es proyectivo.

b) $\Rightarrow$ a) Supongamos que $\forall a \in R$, $aS + xS$ es proyectivo
Fijemos $a \in R$ y sea $K = aS + xS$
K es proyectivo.
Sea $g: S^2 \longrightarrow K$
$(1,0) \longmapsto a$.
$(0,1) \longmapsto x$
$\therefore \exists\ f: K \longrightarrow S^2$ $\ni$. $gf(a) = a$ y $gf(x) = x$ (pues K es proy.)
$f(k) = (1,0)\, s + (0,1)\, t$
Sean $\alpha(k) = s$; $\beta(k) = t$
$\therefore k = (gf)k = as + xt = a\alpha(k) + x\beta(k)$.
$\therefore$ hemos demostrado que si K es proyectivo, entonces existen S-homomorfismos $\alpha, \beta: K \longrightarrow S$ $\ni$. $\forall k \in K$
$k = a\,\alpha(k) + x\beta(k)$. En particular $a - a\alpha(a) = x\beta(a)$
Como x es central en S y α es S-homomorfismo
$x\alpha(a) = \alpha(a)x = \alpha(x)a$ $\therefore$ $ax - a\,\alpha(x)a = x^2\beta(a)$
$\alpha(x) \in S$ $\therefore \alpha(x) = a_0 + a_1 x + \cdots + a_n x^n$ con $a_i \in R$.

Igualando coeficientes de x en ambos lados, obtenemos:
$a = aa'a$ $\left(ax = a\alpha(x)a + x^2\beta(a) = aa_0a + aa'ax + \cdots + x^2\beta(a)\right)$.
donde a' es el coeficiente de x del polinomio $\alpha(x)$.

$\therefore$ R es Von Neumann regular.

a) $\Leftrightarrow$ c) Se sigue por simetría.

Corolario. Si $S = R[x]$ es semihereditario derecho ó izquierdo Entonces R es Von Neumann regular.

Dem. Si S es semihereditario derecho, entonces todo ideal derecho finitamente generado es proyectivo.

$\therefore \forall a \in R$, $aS + xS$ es un ideal proyectivo derecho de S.

$\therefore$ R es Von Neumann regular.

DOMINIOS LCM DERECHOS VS. IZQUIERDOS.

DEFINICIONES.

1.- Un dominio entero en el cual la intersección de dos ideales principales derechos distintos de cero es otra vez derecho se le llama un Dominio LCM derecho.

2.- R es un dominio derecho de Ore si la intersección de cualesquiera dos ideales principales derechos es distinto de cero.

3.- Para dos elementos $a, b \in R^*$ (donde R^* denota a los elementos distintos de cero); R dominio entero, el máximo común divisor izquierdo denotado por $(a,b)_l$ y el mínimo común múltiplo izquierdo denotado por $[a,b]_l$ se definen de la siguiente forma:

$d = (a,b)_l \Leftrightarrow dR$ es el ideal principal derecho menor distinto de cero que contiene a aR y bR.

$m = [a,b]_l \Leftrightarrow Rm$ es el ideal principal izquierdo mayor distinto de cero contenido en Ra y Rb.

4.- Un anillo se dice que es acotado derecho si todo ideal derecho contiene un ideal bilateral distinto de cero.

En lo que sigue, R denota un anillo con unitario y sin divisores propios de cero.

Para $x \in R^*$, sea $[xR, R] = \{aR \mid xR \subseteq aR,\ a \in R\}$.

$[xR, R]$ está parcialmente ordenado por inclusión.

Proposición 1. Para cada $x \in R^*$, la correspondencia $[xR, R] \longrightarrow [Rx, R]$ dada por $aR \longrightarrow Ra'$ es un anti-isomorfismo.

Dem. Sea $\varphi: [xR, R] \longrightarrow [Rx, R]$ tal correspondencia.

i) φ está bien definida:

Sea $aR \in [xR, R]$
$\therefore x \in aR$, $\therefore x = aa'$ p.a. $a' \in R$
$\therefore x \in Ra'$

Supongamos $aR = bR$
$\therefore x \in aR$ $\therefore x = aa'$
$x \in bR$ $\therefore x = bb'$

Puesto que $aR = bR$, $a = br$ p.a. $r, t \in R$
$b = at$

$x = aa' = bb'$, $a = br$
$\therefore bra' = bb'$
$\therefore ra' = b'$
$\therefore b' \in Ra'$

$x = aa' = bb'$ y $b = at$

$\therefore \; aa' = atb'$

$\therefore \; a' = tb'$

$\therefore \; a' \in Rb'$

$\therefore \; Ra' = Rb'$ ■.

ii) φ cambia el orden:

Sea $aR \subseteq bR$, $aR, bR \in [xR, R]$

$\therefore a = bc$ p.a. $c \in R$

$x \in aR \quad \therefore \; x = aa'$

$x \in bR \quad \therefore \; x = bb'$

$\therefore \; aa' = bb' = x$

$\therefore \; bca' = bb'$

$\therefore \; ca' = b'$

$\therefore \; b' \in Ra'$

$\therefore \; Rb' \subseteq Ra'$ ■.

iii) φ tiene inversa:

Sea $[Rx, R] \xrightarrow{\Psi} [xR, R]$ dada por

$Ra' \longmapsto aR$ donde $x = aa'$

Ψ está bien definida y

$\varphi\Psi(Ra') = \varphi(aR) = Ra'$

$\Psi\varphi(aR) = \Psi(Ra') = aR$ $\therefore \; \Psi = \varphi^{-1}$.

Proposición 2. Si el intervalo $[xR, R]$ es una red $\forall x \in R^*$ y si R es un dominio Ore derecho, entonces R es un dominio LCM derecho.

Dem. Sean $a, b \in R^*$ y supongamos $x_i \in aR \cap bR$, $x_i \neq 0$, $i = 1, 2$. (Por ser Ore derecho)

Sea $m_iR = aR \wedge_i bR$ (el ínfimo de aR, bR en $[x_iR, R]$).

Primero demostraremos que $m_1R = m_2R$:

Sea $0 \neq z \in m_1R \cap m_2R$

y sea $m_2R = aR \wedge_z bR$ en $[zR, R]$.

esto es $m_iR \subseteq m_zR$ ($z \in m_iR \therefore m_iR \in [zR, R]$ y $m_iR \subset aR, bR \therefore m_iR \subseteq m_zR$)

Entonces $x_iR \subset m_iR \subseteq m_zR \subseteq aR \cup bR$

Análogamente $x_i \in m_zR$

$\therefore m_zR \in [x_iR, R]$

y $m_zR \subseteq aR, bR$

$\therefore m_zR \subset m_iR$

$\therefore m_iR = m_zR$

$\therefore m_1R = m_2R$ ∎

Ahora mostraremos que $aR \cap bR = mR$, mR = ínfimo de aR, bR.

1) $mR \subseteq aR \cap bR$ es claro.

2) Sea $x \in aR \cap bR$,

ent. $m_xR = mR$ $\therefore x \in mR$

$\therefore aR \cap bR = mR$

$\therefore R$ es un dominio LCM derecho ∎.

Teorema. Sea R un dominio LCM derecho, si R tiene la condición ascendente de cadena para ideales principales izquierdos y satisface la condición Ore izquierda, entonces R es un dominio LCM izquierdo.

Dem. Sea $x \in R^*$, como $[{}_R x, R]$ tiene c.a.c., entonces $[{}_R xR, R]$ tiene la condición descendente de cadena por prop. 1.

Como R es un dominio LCM derecho $[{}_R xR, R]$ es una semi-red con ínfimo (pues $aR \cap bR \subseteq aR, bR \quad \forall aR, bR \in [{}_R xR, R]$ y claramente es la máxima cota inferior).

y como $[{}_R xR, R]$ tiene la c.d.c., debe ser una red, dem.: Sea $\mathcal{C} = \{{}_R cR = aR, bR\}$

Sean $c_0 R$, $c_0' R$ mínimos de $\mathcal{C}$,

$c_0 R \cap c_0' R \subseteq c_0 R, c_0' R$

$\therefore c_0 R \cap c_0' R = c_0 R = c_0' R$ (pues $c_0 R$, $c_0' R$ eran mínimos)

$\therefore c_0 R$ es el mínimo

$\therefore c_0 R$ es la mínima cota superior

$\therefore c_0 R$ es el supremo de $aR, bR \quad \forall aR, bR \in [{}_R xR, R]$.

Se sigue de la prop. 1 que $[{}_R x, R]$ es una red $\forall x \in R^*$.

Aplicando la analogía izq.-der. de la prop. 2, tenemos que R es un dominio LCM izquierdo.

En seguida daremos un ejemplo de un dominio LCM derecho, acotado (ent. Ore izq.) el cual no es un dominio LCM izquierdo.
Para esto, antes daremos un ejemplo de un dominio local PRI, Ore derecho, el cual no es Ore izquierdo, ni un dominio de ideales principales izquierdos (PLI), y un lema.

Ejemplo *. Sea $K = L\langle t,\rho\rangle = \{ \sum_{i\geq 0} t^i c_i \mid c_i \in L \}$

donde L es un campo y
$\rho : L \longrightarrow L$ un monomorfismo que no es isomorfismo.

Definimos la igualdad y la suma en la forma usual, y la multiplicación por la siguiente regla:

$$ct = t\rho(c) \qquad \forall\, c \in L$$

Suponemos también las leyes distributivas.
Esto define la estructura de un dominio entero sobre $L\langle t,\rho\rangle$.

i) K es un dominio de ideales principales derechos.

Si $\sum_{i\geq 0} t^i c_i$ es un elemento arbitrario de K con $c_0 \neq 0$

entonces $\forall\, n \geq 1$ tenemos que:

$$t^n = c_0 t^n \left[\rho^n(c_0)\right]^{-1} \qquad \forall n.$$

Sea $\mathcal{L}$ un ideal derecho distinto de cero de K.

$n = \min \{ \partial f(t) \mid f(t) \in \mathcal{L} ;\ f(t) \neq 0 \}$ y

$$T = \{ c \in L \mid t^n c + \sum_{i>n} t^i c_i \in \mathcal{L} \}$$

claramente T es un ideal derecho de L.
como L es un campo y $T \neq 0$ (pues $n = \min \{ \partial f(t) \mid f(t) \in \mathcal{L};\ f(t) \neq 0 \}$)

ent. $T = L$

Sea $f^*(t) = t^n + \sum_{i>n} t^i c_i \in \mathcal{L}$

Mostraremos que $\mathcal{L} = f^*(t) K$.

Sea $g(t) = \sum_{i \geq 0} t^i a_i$ un elemento arbitrario distinto de cero de $\mathcal{L}$ de grado m.

claramente $m \geq n$.
si $m = n$ entonces $a_n \in T = L$

Ahora consideremos $g(t) - f^*(t) a_n \in \mathcal{L}$ y es de grado mayor que n.
∴ basta considerar cuando $m > n$.

Si $m > n$ entonces $g(t) - f^*(t)\, t^{m-n} a_m \in \mathcal{L}$ y es de grado mayor que m.
Por lo tanto todas las series de potencia en $\mathcal{L}$ de grado m es congruente a una serie de potencia en $\mathcal{L}$ de grado mayor que m, módulo

el ideal derecho $f^*(t)K$. Por lo tanto $\mathcal{L}$ representa a la clase del cero.

$$\therefore \mathcal{L} = f^*(t)K.$$

ii) Todo ideal derecho de K es de la forma t^nK, $n \geq 0$.

Sea I ideal derecho de K.

$$\therefore I = f^*(t)K = t^nK.$$

$\therefore tK$ es el único ideal máximo de K.
(tK es un ideal bilateral.)

$\therefore$ K es local.

iii) K no es Øre izquierdo.

ρ no es epimorfismo,
$\therefore \exists\, a \in L \quad \ni \quad a \notin \rho(L)$

Consideremos $Kta \cap Kt$.
Sea $fta = gt$ un elemento de $Kta \cap Kt$ distinto de cero.
f y g tienen el mismo grado

$f = t^n a_n + t^{n+1} a_{n+1} + \dots \qquad a_n \neq 0$
$g = t^n b_n + t^{n+1} b_{n+1} + \dots \qquad b_n \neq 0$

$$fta = t^n a_n ta + t^{n+1} a_{n+1} ta + \dots$$
$$= t^n b_n t + t^{n+1} b_{n+1} t + \dots = gt$$

$$\therefore fta = t^{n+1} \rho(a_n) a + t^{n+2} \rho(a_{n+1}) a + \dots = t^{n+1} \rho(b_n) + t^{n+2} \rho(b_{n+1}) + \dots$$

$$\therefore \rho(a_{n+k}) a = \rho(b_{n+k}) \qquad k = 0, 1, \dots$$

$$\rho(a_n) a = \rho(b_n) \qquad \begin{matrix} a_n \neq 0 \\ b_n \neq 0 \end{matrix}$$

ρ es monomorfismo
$\therefore \rho(a_n) \neq 0$
$\rho(b_n) \neq 0$

$$\therefore a = \rho(b_n)\rho(a_n)^{-1}$$
$$= \rho(b_n a_n^{-1})$$
$$\therefore a \in \rho(L) \qquad \square.$$

$$\therefore fta = gt = 0$$

$$\therefore Kta \cap Kt = 0$$

$\therefore K$ no es Ore izquierdo.

v) K es Ore derecho.

Observación: Un elemento en $K = L\langle t, \rho\rangle$ es una unidad en $K \iff$ su término independiente es una unidad en L.
Puesto que L es un campo, todos los elementos de K de grado cero son unidades.

Si f, g son elementos de K distintos de cero, tal que uno de ellos es de grado cero, entonces claramente $fK \cap gK \neq 0$.

$\therefore$ Supongamos que $f = t^n a_n + t^{n+1} a_{n+1} + \dots$ con $a_n \neq 0$.
$g = t^m a'_m + t^{m+1} a'_{m+1} + \dots$ con $a'_m \neq 0$

$\therefore$ $f = t^n u(t)$ $\quad u(t)$ unidad en K.
$g = t^m u'(t)$ $\quad u'(t)$ unidad en K.

$\therefore$ $fK \cap gK = t^n K \cap t^m K \neq 0 \quad \forall f, g \in K^*$ ■.

Lema 1. Sea $ab' = ba' \in R^{**}$. Si $[a',b']_l$ existe, entonces $(a,b)_l$ existe y $ab' = ba' = (a,b)_l\,[a',b']_l$.

Dem. Sea $m = [a',b']_l$

$\therefore\ Rm = Ra' \cap Rb'$

$\therefore\ m = b_1a' = a_1b' \qquad b_1, a_1 \in R.$

ent. $ab' = d\,a_1b' \quad$ p.a. $d \in R \qquad (a'b \in Rm = Ra_1b' = Rb_1a')$

$\therefore\ a = da_1$ y

$b = db_1$

$\therefore$ d es un divisor común izquierdo de a y b.

Sea e cualquier otro divisor:

$a = ea_2$

$b = eb_2$

$\therefore\ eb_2a' = ba' = ab' = ea_2b'$

$\therefore\ b_2a' = a_2b'$

$\therefore\ b_2a' \in Ra' \cap Rb' = Rb_1a'$

$\therefore\ b_2a' = rb_1a' \quad$ p.a. $r \in R$

$\therefore\ b_2 = rb_1.$

$$b = db_1 = eb_2 = erb_1$$

$$\therefore d = er$$

$$\therefore d = (a,b)_l$$

y $\quad ab' = da_1b' = dm = (a,b)_l\,[a',b']_l.$

Ahora daremos el ejemplo de un dominio LCM derecho, acotado (ent. Ore izquierdo el cual no es un dominio LCM izquierdo.

Sea K el dominio del ejemplo $*$.

Sea $F = K(K^*)^{-1}$ el campo de cocientes derecho de K. Existe pues K es Ore derecho.

Sea $P = F[[x]]$ el anillo de series formales de potencia en la indeterminada central x.

El ejemplo que daremos es el siguiente subanillo de P:

$$R = \{ f(x) \in P \mid f(0) \in K \}.$$

i) R es un dominio LCM derecho.

Sean $f, g \in R$

podemos suponer que $fR \not\subseteq gR$, $gR \not\subseteq fR$
(pues si $fR \subseteq gR \Rightarrow fR \cap gR = fR$).
y $ord(g) \leq ord(f)$.

$\therefore$ $f = gh_0$ p.a. $h_0 \in P$.

Escogemos $d \in K$ tal que $fd \in gR$.
d no es unidad por las hipótesis anteriores.
De hecho escogemos d tal que dK es máximo.

Esta d existe ya que K tiene la c.a.c. para ideales derechos, por lo tanto $A = \{aK \mid fa \in gR\}$ tiene un máximo.

$$\therefore fdR \subseteq fR \cap gR.$$

Ahora mostraremos la inclusión inversa:

Sea $fh_1 = gh_2$ $h_i \in R$, un elemento de $fR \cap gR$ entonces $fh_1 = fdh_3$ p.a. $h_3 \in P$ ya que $fP \cap gP = fP = fdP$ pues d es unidad en F.

Si $h_3(0) = 0$ entonces $h_3 \in R$ y $fh_1 \in fdR$ ☐.

Si $h_3(0) \neq 0$ entonces escribimos $h_1 = au$ donde $u \in R$ y $u(0) = 1$.

$$\therefore fa = f(h_1 u^{-1}) = g(h_2 u^{-1}) \in gR.$$
$$\therefore aK \in A.$$

$dK \subseteq aK + dK = eK$, $e \in K$ (pues K es PRI)
$\therefore dK = aK + dK$ pues dK es máximo
$\therefore aK \subseteq dK$
$\therefore a = dc$ p.a. $c \in K$

y $fh_1 = fau = fd(cu) \in fdR$

$$\therefore fR \cap gR \subseteq fdR.$$

ii) R no es un dominio LCM izquierdo.

Por lema 1, en un dominio entero si $0 \neq (xa^{-1})a = (xb^{-1})b$ entonces la existencia del mínimo común múltiplo izquierdo $[a,b]_L$, implica la existencia del máximo común divisor izquierdo $(xa^{-1}, xb^{-1})_L$.

Por lo tanto es suficiente mostrar que el máximo común divisor izquierdo no existe en R.

Supongamos que $h = (xa^{-1}, xb^{-1})_L$ en R

$\therefore$ $xa^{-1}R$, $xb^{-1}R \subset hR$.
$\therefore$ $xa^{-1} = hf$ p.a. $f \in R$.
$\therefore$ $ord(hf) = 1 = ord(h) + ord(f)$
$\therefore$ $ord\, h = 0, 1$
y como $hf = xa^{-1}$, los coeficientes en h de x^n para $n > 1$ son cero
$\therefore$ $h = x^n s u$ donde $n = 0, 1$, $s \in F$, $u(0) = 1$

Como u es unidad en R, podemos omitirla
$hR = x^n s R$

$xa^{-1}, xb^{-1} \in tR$ $\forall\, t \in K^*$ $\left(\text{pues } xa^{-1} = t\left(0 + x\tfrac{1}{ta}\right)\right)$.

$\therefore$ $hR \subseteq tR$ $\forall\, t \in K^*$
Si $h \in K$ ent. $hR \subseteq h^2R$, $\therefore$ $h = h^2 s_1$, $s_1 \in K$
$\therefore$ $1 = hs$ $\therefore$ $hR = R$ lo cual no puede ser.

$\therefore$ h no puede estar en K.

Por lo tanto $h = xs$

$\therefore \quad xa^{-1} = xsr_1$

$xb^{-1} = xsr_2 \qquad r_1, r_2 \in K.$

$\therefore \quad s = a^{-1}r_1^{-1} = b^{-1}r_2^{-1}$

$\therefore \quad r_1 a = r_2 b \neq 0 \qquad \forall\ a, b \in K^*$

$\therefore \quad Ka \cap Kb \neq 0 \qquad \forall\ a, b \in K^*$

$\therefore$ K es Ore izquierdo $\square$.

$\therefore \quad (xa^{-1}, xb^{-1})_l$ no existe en R

$\therefore \quad [a, b]_l$ no existe en R.

$\therefore$ R no es un dominio LCM izquierdo.

iii) R es acotado (Ent. Ore izq.).

Si $f = x^n u a b^{-1}$ donde $a, b \in K$ y $u \in R$ con $u(0) = 1$

ent. $x^{n+1} = (x b a^{-1} u^{-1}) f \in Rf$.

Esto es, Rf contiene al ideal bilateral Rx^{n+1}.

$\therefore$ R es acotado izquierdo.

Análogamente R es acotado derecho. $\blacksquare$.

SOBRE ANILLOS SEMIPRIMOS CON IDENTIDAD POLINOMIAL.

DEFINICIONES

Sea R un anillo, no necesariamente con elemento unitario.

1.- Si S es un subconjunto de R

$$r(S) = \{x \in R \mid Sx = 0\}$$
$$\ell(S) = \{x \in R \mid xS = 0\}$$

son llamados el anulador derecho e izquierdo de R respectivamente.

2.- Un ideal derecho J de R es esencial, si para cualquier ideal derecho K, $J \cap K = 0$ implica $K = 0$.

3.- R es semiprimo si no tiene ideales nilpotentes distintos de cero.

Obs: Si R es semiprimo, un ideal bilateral I es esencial $\Leftrightarrow$ $r(I) = 0$ ó $\ell(I) = 0$.

$\Rightarrow$) $(I \cap r(I))^2 = 0$

$\therefore I \cap r(I) = 0$ pues R es semiprimo.

$\therefore r(I) = 0$.

$\Leftarrow$) Sup. $J \neq 0$ $\therefore$ $I \cap J = 0$

$\therefore IJ = 0$ $\therefore J \subset r(I)$

$\therefore r(I) \neq 0$.

4.- $Z(R) = \{x \in R \mid xJ = 0$ pa. J ideal derecho esencial en $R\}$ es un ideal bilateral de R, llamado el ideal singular derecho de R.

Análogamente se define el ideal singular izquierdo $Z'(R)$.

Obs. 1 Si R es un anillo no singular, i.e., $Z(R)=0$ entonces el anillo máximo de cocientes derecho Q de R coincide con la cápsula inyectiva derecha de R.

E se dice ser la cápsula inyectiva de R_R, si E es inyectivo y $R_R \longrightarrow E$ es un monomorfismo esencial. Además E está determinado en forma única.

Obs. 2 Si I es cualquier ideal derecho de R, entonces existe un ideal derecho I' máximo con respecto a la propiedad que no intersecta a I tal que $I \oplus I'$ es esencial en R_R.

5.- Por lo tanto, después de estas observaciones, al anillo máximo de cocientes derecho Q de R, lo podemos caracterizar de la siguiente forma:

a) R es un subanillo de Q

b) Si $f \in \mathrm{Hom}_R(J,R)$, donde J es un ideal derecho esencial en R, entonces $\exists\, q \in Q$ tal que $qx = f(x)$ $\forall\, x \in J$.

c) Si $q \in Q$, $\exists$ J ideal derecho esencial en R, tal que $qJ \subseteq R$

d) $\forall\, q \in Q$, $q=0$ si y sólo si $qJ=0$ p.a. J ideal esencial derecho en R.

6.- R se dice que satisface una identidad polinomial si existe un polinomio multilineal homogéneo

$$f(x_1, \ldots, x_n) = \sum_{\tau \in S^n} w_\tau\, x_{\tau(1)} \cdots x_{\tau(n)}$$

en indeterminadas que no conmutan $\{x_i\}$, $w_r \in End(G)$ donde G es el grupo aditivo de R y tal que $w_r(xy) = (w_r x)y = x(w_r y)$ $\forall x, y \in R$ y $\ker w_i = 0$.

7.- Un anillo R se llama localmente nilpotente si y sólo si, todo subconjunto finito F de R genera a un subanillo nilpotente.
Esto es equivalente a la siguiente condición:
$\exists\, N \in \mathbb{N}$ tal que cualquier producto $x_{i1} \cdots x_{iN} = 0$ para $x_{ij} \in F$.
Un ideal es llamado localmente nilpotente si es localmente nilpotente como anillo.

Lema 1. Si I es un ideal localmente nilpotente en R y R/I es localmente nilpotente entonces R es localmente nilpotente.

Dem. Sea $F = \{x_1, \ldots, x_n\}$ un subconjunto finito de R y sea $\bar{F} = \{\bar{x}_1, \ldots, \bar{x}_n\}$ donde $\bar{x}_i = x_i + I$
$\exists\, N \in \mathbb{N}$ s.t. $\bar{x}_{i1} \cdots \bar{x}_{iN} = 0$ para $i_j = 1, \ldots, n$.
El conjunto $G = \{x_{i1} x_{i2} \cdots x_{iN} \mid i_j = 1, 2, \ldots, n\}$ es finito y está contenido en I.
$\therefore \exists\, M$ tal que el producto de cualesquiera M de estos elementos es cero.
$\therefore$ $NM \in \mathbb{N}$ es tal que $x_{iN1} \cdots x_{iNM} = 0$
$\therefore$ R es localmente nilpotente.

8.- A la suma de todos los ideales localmente nilpotentes de R, se le llama el nilradical de Levitzki de R.

η = nilradical de Levitzki tiene las siguientes propiedades:
a) η es un ideal localmente nilpotente
b) η contiene a todos los ideales localmente nilpotentes.
c) El nilradical de Levitzki de $R/\eta = \{0\}$.

Teorema A. Todo nil anillo R con identidad polinomial es localmente nilpotente.

Dem. Sea R nilanillo con identidad polinomial y sea η el nilradical de Levitzki de R.
Entonces R/η es un nilanillo y $\eta(R/\eta) = \{0\}$.
Asegurámos que $R/\eta = \{0\}$, c.e., $R = \eta$ es localmente nilpotente, ya que en caso contrario, tenemos un nilanillo con identidad polinomial $\neq \{0\}$ el cual no tiene ideales unilaterales localmente nilpotentes.
Sea $S = R/\eta$ y obtendremos una contradicción probando que S contiene a un ideal derecho localmente nilpotente.
Sea $a \in S$, $a \neq 0$ tal que $a^2 = 0$ y consideremos el ideal derecho aS.
Si $aS = \{0\}$, entonces $L(S) \neq 0$ y $L(S)$ es nilpotente y $\therefore$ localmente nilpotente.
$\therefore$ Podemos suponer que $aS \neq \{0\}$.
Consideremos una identidad polinomial $f(e_1, \ldots, e_n) = 0$ en S
Podemos escribir $f(e_1, e_2, \ldots, e_n)$ en la forma:
$f_1(e_2, \ldots, e_n)e_1 + f_2(e_1, \ldots, e_n)$ donde e_1 no aparece en la última posición en los monomios de f_2. Reordenando las e_i, si es necesario, podemos suponer que $f_1(e_2, \ldots, e_n) \neq 0$

Sustituyendo $e_1 \longrightarrow a_1 = a$
$e_2 \longrightarrow a_2$
$\vdots$
$e_n \longrightarrow a_n$ donde $a_i \in aS$ $i \geq 1$.

Entonces $f_2(a_1, a_2, \ldots, a_n) = 0$ $\therefore$ $f_1(a_2, \ldots, a_n)a = 0$

$\therefore$ $f_1(a_2, \ldots, a_n) \in \ell_{aS}(aS)$

$\therefore$ $aS/\ell(aS)$ satisface una identidad polinomial de grado menor o igual que $n-1$ $[f_1(a_2 + \ell(aS) + \ldots + a_n + \ell(aS)) = 0]$

$\therefore$ Usando inducción en el grado de las identidades polinomiales, tenemos que $aS/\ell(aS)$ es localmente nilpotente.

$\ell(aS)$ es nilpotente $\therefore$ localmente nilpotente,

Por Lema 1 aS es localmente nilpotente ∎.

<u>Corolario A</u>. Si R es semiprimo con identidad polinomial f, entonces R no tiene nilideales distintos de cero.

Def. z es un elemento casi regular derecho de R si $(1-z)R = R$

z es casi regular $\Leftrightarrow$ $z \in (1-z)R$

$\Leftrightarrow$ $-z \in (1-z)R$

i.e. z es casi regular si existe $z' \in R$ tal que

$$z + z' - zz' = 0$$

Un ideal derecho I de R es casi regular si todo elemento de I es casi regular derecho.

Def. $R(R) = \cap \{ r(M) \mid M$ es un R-mod. derecho irreducible $\}$ es llamado el radical de R.
M es irreducible si M no tiene submódulos propios $\neq \{0\}$.

Def. R es primitivo $\Leftrightarrow$ existe un R-mod. M tal que M es irreducible y $r(M) = \{0\}$.

Def. Sea $I = \{ M \mid M$ es un R-mod. derecho irreducible $\}$
Si $r(I) = \{0\}$ entonces R es llamado semiprimitivo.

El radical R cumple con las siguientes propiedades:

a) $R/R(R)$ es semiprimitivo

b) R es un ideal de R casi regular, el cual contiene a todos los ideales derechos casi regulares.

Lema B. Sea I un ideal distinto de cero en $R[\lambda]$, donde $R[\lambda]$ es el anillo de polinomios con coeficientes en R y en la indeterminada central λ, y sea $p(\lambda) = a_0 + \cdots + a_n\lambda^n$ $a_n \neq 0$. Un polinomio de grado menor que pertenece a I
Sup. $r(\lambda)$ es un polinomio $\neq$ $a_n^{n} r(\lambda) = 0$ $p \neq 1$. Entonces
$a_n^{n-1} r(\lambda) \cdot r(\lambda) = 0$

Dem. $a_n^{n} r(\lambda)=0 \iff a_n^{n} r_i = 0$ donde r_i es el i-ésimo coeficiente de $r(\lambda)$, ∴ es suficiente probar el lema para $r(\lambda) = r$ de grado cero.

$a_n^{n-1} p(\lambda) r = a_n^{n-1} a_0 r + a_n^{n-1} a_1 \lambda r + \dots + a_n^{n-1} a_n \lambda^n r \in I$

∴ el coeficiente de λ^n es $a_n^{n} r = 0$

∴ $a_n^{n-1} p(\lambda) r$ es de grado menor que n.

∴ $a_n^{n-1} p(\lambda) r = 0$.

Teorema B. Si R no tiene nilideales distintos de cero, ent. $R[\lambda]$ es semiprimitivo

Dem. Por la propiedad a) del radical, basta demostrar que $R(R[\lambda]) = 0$.

Supongamos $R(R[\lambda]) \neq 0$

Sea $M = \{ f(x) \in R[\lambda] \mid f(x) \in R(R[\lambda]),\ f(x) \neq 0$ y $f(x)$ de grado menor $\}$.

Los coeficientes del término de mayor grado de estos polinomios y el cero forman un ideal $N \neq \{0\}$ de R.

Deseamos mostrar que N es un nilideal.

Sea $K(\lambda) = a_0 + a_1\lambda + \dots + a_n\lambda^n \in M$

∴ $p(x)\lambda a_n \in R$ y R es un ideal casi regular

∴ $p(\lambda)\lambda a_n$ es casi regular

∴ ∃ un polinomio $q(\lambda)$ tal que

(1) $p(\lambda)\lambda a_n + q(\lambda) - K(\lambda)\lambda a_n q(\lambda) = 0$

(2) $p(\lambda)\lambda a_n + q(\lambda) - q(\lambda) p(\lambda)\lambda a_n = 0$

Estas ecuaciones muestran que el término constante de $q(\lambda)$ es cero.

$\therefore$ (3) $s(\lambda) + t(\lambda) - \lambda\, s(\lambda)\, t(\lambda) = 0$

$s(\lambda) + t(\lambda) - \lambda\, s(\lambda)\, t(\lambda) = 0$

donde $s(\lambda) = p(\lambda) a_n$ y $t(\lambda)$ es obtenido reemplazando a λ^{i+1} por λ^i en la expresión para $q(\lambda)$.

Ahora mostraremos que $a_n^k\, t(\lambda) = 0$ para k suficientemente grande.

Supongamos que $a_n^k\, t(\lambda) \neq 0 \quad \forall\, k \in \mathbb{N}$

Sea ν el grado menor de estos polinomios y escribamos $t(\lambda) = t_1(\lambda) + \lambda^{\nu+1} t_2(\lambda)$, donde $t_1(\lambda) = b_0 + \cdots + b_\nu \lambda^\nu$

Entonces $a_n^k\, t_2(\lambda) = 0$ para k suficientemente grande ya que si $a_n^k\, t_2(\lambda) \neq 0 \quad \forall k$, ent. $\partial(a_n^k\, t(\lambda)) \geq \nu+1 \ \forall k$ contradiciendo la hipótesis de que hay alguno con grado ν.

y $a_n^k\, b_\nu \neq 0 \quad \forall k$.

$\therefore$ Por el lema y el hecho de que el coeficiente del término de mayor grado de $s(\lambda)$ es a_n^2, tenemos $a_n^l\, t_2(\lambda) = 0 = a_n^l\, s(\lambda)\, t_2(\lambda)$ para una l conveniente.

Multiplicando la ecuación (3) por a_n^l obtenemos:

(5) $a_n^l\, s(\lambda) + a_n^l\, t_1(\lambda) - a_n^l\, \lambda\, s(\lambda)\, t_1(\lambda) = 0$

el coeficiente de $\lambda^{l+\nu+1}$ en el lado izquierdo de (5) es $-a_n^{l+2} b_\nu$. $\therefore a_n^{l+2} b_\nu = 0$ contradiciendo que $a_n^k\, b_\nu \neq 0 \quad \forall k$.

$\therefore a_n^\mu\, t(\lambda) = 0 \quad$ p.a. $\mu \in \mathbb{N}$.

Multiplicando la ecuación (1) por a_n^μ obtenemos:

$a_n^\mu\, s(\lambda) = 0$

$\therefore a_n^{\mu+2} = 0$.

Esto muestra que η es un nilideal de $R + \{0\}$.

Lema C. Sea R semiprimitivo con centro C e identidad polinomial f. Sea I cualquier ideal de R distinto de cero, entonces $I \cap C \neq \{0\}$

Teorema C. Sea R semiprimo con centro C e identidad polinomial f. Sea I cualquier ideal de R distinto de cero, entonces $I \cap C \neq \{0\}$.

Dem. R es semiprimo con identidad polinomial f
$\therefore$ por corolario A, R no tiene nilideales distintos de cero, $\therefore$ $R[\lambda]$ es semiprimitivo (por teorema B)

El centro de $R[\lambda]$ es $C[\lambda]$ ya que si $c(\lambda) = \sum r_i \lambda^i$, es un elemento en el centro de $R[\lambda]$ entonces $\forall r \in R \quad c(\lambda) r = r c(\lambda)$.

$\therefore \sum (r_i r - r r_i) \lambda^i = 0$

$\therefore r_i \in C$

$\therefore c(\lambda) \in C[\lambda]$.

Sea I un ideal $\neq \{0\}$ de R
$\therefore$ $I[\lambda]$ es un ideal $\neq \{0\}$ de $R[\lambda]$
$R[\lambda]$ es semiprimitivo $\therefore$ Por Lema C
$I[\lambda] \cap C[\lambda] \neq \{0\}$
Comparando coeficientes, obtenemos:

$I \cap C \neq \{0\}$ ∎.

Lema 1. Sea R un anillo semiprimo con identidad polinomial con centro $\mathcal{C}$, y sea J un ideal derecho de R. Ent. el centro de J es igual a $J \cap \mathcal{C}$.

DEM. P.D. centro de $J \subseteq J \cap \mathcal{C}$

Sea a un elemento del centro de J, y sean $x, r \in R$ entonces

$$\begin{aligned}(ax - xa)r(ax - xa) &= (axr)ax - (axrx)a + x(arx)a - x(ar)ax \\ &= a(axr)x - a(axrx) + xa(arx) - xa(ar)x \\ &= 0\end{aligned}$$

R es semiprimo $\therefore ax - xa = 0$

$\therefore a \in \mathcal{C}$

$J \cap \mathcal{C} \subseteq$ centro de J obviamente. ∎.

En lo que sigue, R denotará un anillo semiprimo con identidad polinomial y con centro $\mathcal{C}$.

Teorema 1. $Z(R) = 0 = Z'(R)$

DEM. Supongamos $Z(R) \neq 0$

$\therefore Z(R) \cap \mathcal{C} \neq 0$

Sea $\lambda \in Z(R) \cap \mathcal{C}$, $\lambda \neq 0$.

$\therefore$ p.a. J ideal esencial derecho de R

$0 = \lambda J = J\lambda$ (pues $\lambda \in \mathcal{C}$)

$\therefore r(J) \neq 0$ contradicción, pues R es semiprimo.

Lema 2. Si J es un ideal derecho esencial en R, entonces J es semiprimo con identidad polinomial.

Dem. Supongamos $I^2 = 0$ donde I es un ideal de J entonces IJ es un ideal derecho de R

$(IJ)^2 \subseteq I^2 = 0$

$\therefore IJ = 0$ pues R es semiprimo

$\therefore I = 0$ por teorema 1.

$\therefore J$ es semiprimo y claramente es con identidad polinomial.

Teorema 2. Si R es un anillo semiprimo con identidad - polinomial (que satisface la identidad f) entonces el anillo máximo de cocientes derecho Q de R - satisface la misma identidad polinomial.

Dem. Sea $f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in S_n} w_\sigma \, x_{\sigma(1)} \ldots x_{\sigma(n)}$

Sean $q_1, q_2, \ldots, q_n \in Q$ y sea $q = f(q_1, \ldots, q_n)$

$q_i \in Q \quad \therefore \exists J_i$ ideal derecho esencial en R tal que $q_i J_i \subseteq R$

$\therefore$ tomando intersecciones finitas

$\exists J$ ideal derecho esencial en R tal que $q_i J$, qJ $i = 1, \ldots, n$ están contenidos en R.

Sea $a \in J$ y $qa = b \in R$ (p.d. $q = 0$).

(basta demostrar $b = 0$)

Supongamos $b \neq 0$

Ent. $U = RbR \cap J \neq 0$ ya que J es esencial y U es un ideal bilateral de J.

Por Lema 2, J es un anillo semiprimo con identidad polinomial y $\therefore$ podemos aplicar el Teorema A a J
$\therefore$ $\exists\ \lambda \neq 0$ un elemento de U que está en el centro de J.

$\therefore \lambda \in C$ (por Lema 1)

$$\therefore b\lambda^n = q a \lambda^n = \sum_\sigma w_\sigma q_{\sigma(1)} \dots q_{\sigma(n)}\, a \lambda^n$$

$$= \left\{ \sum w_\sigma (q_{\sigma(1)}\lambda) \dots (q_{\sigma(n)}\lambda) \right] a = 0$$

Pues cada $q_{\sigma(i)}\lambda \in R$ y $f(x_1, \dots, x_n) = 0\ \ \forall x_i \in R$

$$\therefore \lambda^{n+1} \in \lambda^n R b R = R\lambda^n b R = 0$$

$\therefore \lambda^{n+1} = 0$

$\therefore \lambda = 0$ ∎

$\therefore b = 0$

$\therefore qJ = 0$

$\therefore q = 0$ ∎.

Teorema 3. Sea J ideal derecho de R, entonces $\ell(J) \neq 0$ $\Leftrightarrow$ J contiene un ideal bilateral esencial de R.

Dem. Supongamos $\ell(J) = 0$

Sea I un ideal de J $\ni$ $I^2 = 0$

entonces $(IJ)^2 \subseteq I^2 = 0$ $\therefore IJ = 0$

$\therefore I \subseteq \ell(J)$ $\therefore I = 0$

$\therefore$ J es semiprimo

Sea U el ideal bilateral mayor de R que está contenido en J

Supongamos U no es un ideal esencial de R.

Ent. $\exists\ V \neq 0$ $\ni$ $UV = 0$ $(UV \subset U \cap V = 0)$.

$V \cap J \neq 0$ ya que si $V \cap J = 0$ entonces $JV = 0$

$\therefore VJ = 0$ (pues $(VJ)^2 = 0 \therefore VJ = 0$)

$\therefore \ell(J) \neq 0$ ↯

Aplicando el Teorema A y lema 1 a J

$V \cap J \cap C \neq 0$, Sea $\lambda \in V \cap J \cap C$, $\lambda \neq 0$

$\therefore$ Obtenemos un ideal $U + \lambda R$ de R tal que

$U \subsetneq U + \lambda R \subset J$ (pues $\lambda \notin U$) ↯.

$\therefore$ U es esencial.

EL teorema 1 y 3 implican al:

Teorema 4. Sea J un ideal derecho esencial en R, entonces J contiene un ideal bilateral de R.

Teorema 5. Q coincide con el anillo máximo de cocientes izquierdo de R.

Dem. Si $Z(R) = 0 = Z'(R)$ entonces el anillo máximo de cocientes derecho e izquierdo coinciden $\Leftrightarrow$ $\forall$ J ideal derecho de R no esencial, $\ell(J) \neq 0$ y el Teorema 3 precisamente asegura esta condición.

Teorema 6. J ideal derecho de R es esencial en R $\Leftrightarrow$ $J \cap C$ es esencial en C.

Dem. $\Rightarrow$) Si J es esencial en R, entonces por teo.4 J contiene un ideal bilateral esencial U de R. Sea $\lambda \in C$, $\lambda \neq 0$, λU es un ideal $\neq 0$ de R, ya que U es esencial.

Por Teorema Λ, $\exists\, \lambda u \in \mathcal{C}$, p.a. $u \in U$

Supongamos $\lambda(J \cap \mathcal{C}) = 0$
Ent. $\lambda(U \cap \mathcal{C}) = 0$ y en particular
$(\lambda u)^2 = u\,\lambda(\lambda u) = 0 \quad \therefore \lambda u = 0$ ↯.
$\therefore \lambda(J \cap \mathcal{C}) \neq 0$
$\therefore J \cap \mathcal{C}$ es esencial en $\mathcal{C}$.

$\Leftarrow$) Supongamos $J \cap \mathcal{C}$ es esencial en $\mathcal{C}$
sea U el ideal de R generado por $J \cap \mathcal{C}$
supongamos $r(U) \neq 0$
por Teo. Λ. $(r(U) \cap \mathcal{C}) \neq 0$
sea $\lambda \in r(U) \cap \mathcal{C}$, $\lambda \neq 0$
pero entonces $(J \cap \mathcal{C})\,\lambda = 0$ ↯.
$\therefore r(U) = 0$
$\therefore U$ es esencial en R y como $U \subset J$
$\therefore J$ es esencial en R.

BIBLIOGRAFIA

1.- Colin R. Fletcher, the structure of unique factorisation rings, Proc. Cambridge Philos. Soc. 67, 535-540 (1970).

2.- Colin R. Fletcher, Euclidean rings, J. London Math. Soc. 4 79-82 (1971)

3.- V. Camilo, Semihereditary polynomial rings, Proc. Amer. Soc. 45, 173-174 (1974).

4.- R.A. Beauregaid, right LCM domains, Proc. Amer. Math. Soc. 30, 1-7 (1971)

5.- P.M. Cohn, Free rings and their relations, Academic Press, London, 1971.

6.- A.V. Jategaonkar, left principal ideal domains, J. Algebra 8, 148-155 (1968).

7.- J.W. Fisher, Structure of semiprime P.I. rings, Proc. Amer. Math. Soc. 39, 465-467 (1973).

8.- Y. Utumi, Rings whose one-sided quotient rings are two sided, Proc. Amer. Math. Soc. 14, 141-147 - MR 26 # 137 (1963).

9.- N. Jacobson, Structure of rings, Amer. Math. Soc. Colloq. Publ. vol. 37, Amer. Math. Soc. Providende, R.I. MR 36 # 5158 (1964).

10.- L. Rowen, Some results on the center of a ring with polinomial identity, Bull. Amer. Math. Soc. 79 219-223 (1973).