26 2 ejem.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ALGUNOS RESULTADOS DE LA TEORIA DE ANILLOS

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A

HUGO ALBERTO RINCON MEJIA

MEXICO, D. F. 1981

TESIS CON FALLA DE ORIGEN

Indice .

Introducción .

En este trabajo estudiamos los principales resultados básicos acerca de anillos Regulares, anillos primitivos y Teorema de Densidad, anillos semiprimitivos y el Teorema principal de Wedderburn.

Es importante notar que casi todos los resultados aquí expuestos son para anillos que no necesariamente tienen unitario lo cual nos dá una generalización sobre la forma clásica de presentación de estos resultados.

Por ejemplo, en el último capítulo, abordamos el Teorema principal de Wedderburn en una forma poco usual, introducimos la hipótesis llamada SBI (Debida a Jacobson y Kaplansky) y nos concentramos en las implicaciones de esta hipótesis sobre el levantamiento de idempotentes y así obtenemos el Teorema mencionado.

Esta presentación fué tomada del libro de Irving Kaplansky, Fields and Rings (ver bibliografía).

Esta tesis fué dirigida por el Dr. Francisco Raggi Cárdenas, a quien agradezco además de la dirección de este trabajo, el apoyo brindado para mi superación académica, y gran parte de mi formación matemática.

El radical.

Definición.

Si A es un anillo, un A-módulo derecho M_A, es un grupo abeliano M, junto con una operación $M \times A \longrightarrow M$, denotada por yuxtaposición, tal que:

(1) $(x + y)\alpha = x\alpha + y\alpha$

(2) $x(\alpha + \beta) = x\alpha + x\beta$

(3) $x(\alpha \cdot \beta) = (x\alpha)\beta \quad \forall x, y \in M, \forall \alpha, \beta \in A$.

Si además A tiene Uno (neutro multiplicativo):

(4) $x1 = x \quad \forall x \in M$, y en este caso diremos que M_A es unitario.

Un A-módulo izquierdo ${}_AM$ se define simétricamente.

Notación:

Reservamos los símbolos M_A, ${}_AM$ para denotar A-módulos derechos, e izquierdos, respectivamente.

Definición.

Si $x \in M_A$, definimos el anulador de x, an x por:

$\text{an } x = \{\alpha \in A : x\alpha = 0\}$.

Si S es subconjunto de M, definimos el anulador de S, an S, por: $\quad \text{an } S = \bigcap_{x \in S} \text{an } x$.

Teorema 1 .

Sea M_A ; si $S \subset M$, entonces an S es un ideal derecho de A . Si además S es submódulo de M , an S es un ideal bilateral de A .

Prueba :

an $S \neq \emptyset$ pues $0 \in$ an S .

Si $s \in S$; $\alpha, \beta \in$ an S , entonces : $s(\alpha - \beta) = s\alpha - s\beta =$
$= 0 - 0 = 0$ $\therefore \alpha - \beta \in$ an S .

Si $s \in S$, $\alpha \in$ an S , $\gamma \in A$, entonces : $s(\alpha \cdot \gamma) = (s\alpha)\gamma =$
$= 0\gamma = 0$ $\therefore \alpha\gamma \in$ an S . $\therefore$ an S es un ideal derecho de A .

Si además S es submódulo de M_A , $s \in S$, $\alpha \in$ an S , $\gamma \in A$, entonces : $s(\gamma \cdot \alpha) = (s \cdot \gamma) \cdot \alpha = 0$ pues $s\gamma \in S$ cuando S es submódulo de M ; así que : S submódulo de $M_A \Longrightarrow$ an S es ideal bilateral de A .

Notas :

Si $I =$ an M_A , entonces M es también A/I-módulo . Más generalmente , si I es ideal bilateral de $A \ni MI = 0$ entonces M_A es también $M_{A/I}$. (Definiendo $x\bar{a} = xa$, $a \in \bar{a} \in A/I$) .

Definición .

Diremos que M_A es fiel si an $M = 0$.

Definición .

Diremos que M_A es irreducible si :

i) $MA \neq 0$.

ii) M_A no tiene submódulos distintos de 0 y M_A .

Definición .

El anillo A es primitivo derecho si existe M_A irreducible y fiel .

(Anillos primitivos izquierdos se definen similarmente) .

Notas :

1 . Un anillo trivial A ($ab = 0 \ \forall a , b \in A$) no admite módulos irreducibles .

2 . G. M. Bergman (Proc. Amer. Math. Soc. 15 (1964) , 473-5 , con corrección en pag. 1000) dió un ejemplo de un anillo primitivo derecho que no es primitivo izquierdo .

Teorema 2 .

Sea $x \in M_A$, $I = \text{an } x$. Entonces $xA \cong A/I$, isomorfismo de A-módulos .

Prueba :

(Notar que si I no es ideal bilateral de A , no podemos darle a A/I estructura de anillo ; sin embargo , damos a

A/I estructura de A-módulo derecho de la manera obvia) .

Definimos $h : A \twoheadrightarrow xA$

$\alpha \overset{h}{\longmapsto} x\alpha$, h es homomorfismo de A-módulos

$\operatorname{Ker} h = I = \operatorname{an} x$, $\therefore$ $\operatorname{Im} h = xA \cong A/I = A/\operatorname{an} x$.

Teorema 3 .

Si M_A es irreducible y $0 \neq x \in M$, entonces $xA = M$.

Prueba :

xA es submódulo de M . $\therefore$ $xA = 0$ ó $xA = M$. Así que basta probar $xA \neq 0$: Sea $S = \left\{ y \in M : yA = 0 \right\}$. Claramente , S es submódulo de M , y $S \neq M$ ya que $MA \neq 0$ por ser M irreducible , $\therefore$ $S = 0$, y en particular $0 \neq x \notin S$, es decir $xA \neq 0$.

Definición .

Si A es un anillo , el ideal derecho I de A es regular si $\exists e \in A$, $ea - a \in I$, $\forall a \in A$. Diremos que e es un elemento unitario izquierdo módulo I . Notar que si $e \in I$ entonces $I = A$.

Ejemplo .

En $2\mathbb{Z}$, el ideal (6) es regular con $e = 4$. El ideal (4) no es regular . ($4 \cdot 2n - 2n = 3 \cdot 2n = 6n \in (6)$; $e2n - 2n =$

$= (e - 1)2n \notin (4)$ para n impar pues e es par) .

<u>Teorema 4</u> .

Si M_A es irreducible y $0 \neq x \in M$, entonces $I = \text{an}\ x$ es un ideal derecho regular máximo de A .

Prueba :

Por el Teorema 1 . I es un ideal derecho , además :

(a) I es regular : Por el Teorema 3 , $xA = M \therefore \exists e \in A \ni xe = x$

Sea $a \in A$, entonces : $x(ea - a) = (xe)a - xa =$

$= xa - xa = 0 \quad \therefore ea - a \in I \quad \forall a \in A$.

(b) I es máximo : pues $A/I \cong xA = M$ (Teoremas 2 y 3) .

Si J fuera ideal derecho $\ni I \subsetneq J \subsetneq M$ entonces J/I sería un ideal de A/I distinto de 0 y de A/I , contradiciendo que M es irreducible .

<u>Teorema</u> 5

Si M_A es irreducible , entonces $\exists I \subset A$, un ideal derecho regular máximo $\ni M \cong A/I$, isomorfismo de A-módulos derechos.

Prueba :

Basta tomar $0 \neq x \in M$ (M es irreducible y $\therefore$ no trivial) e $I = \text{an}\ x$ por los teoremas 2 , 3 , 4 .

Definición .

Sea A un anillo . El ideal bilateral P de A es ideal primitivo derecho de A si A/P es un anillo primitivo derecho .

Nota :

Sea M_A , si $P = \text{an}\, M$, entonces M es también A/P-módulo fiel . (M es A/P-módulo por la primera nota en la pág. 2 . Además $0 = M(P+\alpha) = M\alpha \Rightarrow \alpha \in \text{an}\, M = P$, $\therefore \text{an}_{A/P}\, M = \{P\}$ el anulador de M en A/P. $\therefore M$ es A/P-módulo fiel) .

Así , un ideal bilateral P es ideal primitivo derecho $P = \text{an}\, M$, para algún M_A irreducible .

Teorema 6

Un ideal primitivo derecho P es la intersección de todos los ideales derechos regulares máximos que lo contienen .

Prueba :

Sea $R_p = \{ I \subset A : I \text{ es ideal derecho regular máximo} , I \supset P \}$

Por demostrar : $P = \bigcap R_p$.

$\subset$) $P \subset \bigcap R_p$, pues $P \subset I$, $\forall I \in R_p$.

$\supset$) Por la nota de arriba , $P = \text{an}\, M$ para algún M_A irreducible , así : $P = \text{an}\, M = \bigcap_{x \in M} \text{an}\, x = \bigcap_{0 \neq x \in M} \text{an}\, x$. Pero por el Teorema 4 an x es ideal derecho regular máximo de A ,

$x \neq 0$. $\therefore P = \bigcap_{0 \neq x \in M} \operatorname{an} x \supset \bigcap R_p$.

Teorema 7

Sea $\mathcal{P} = \{ P \subset A : P$ es ideal primitivo derecho $\}$ y

$S = \{ I \subset A : I$ es ideal derecho regular máximo $\}$

entonces : $\bigcap \mathcal{P} = \bigcap S$.

Prueba :

$\supset$) Por el Teorema 6 : $\bigcap \mathcal{P} = \bigcap_{P \in \mathcal{P}} \left[\bigcap R_p \right] \supset \bigcap S$.

$\subset$) Para probar $\bigcap \mathcal{P} \subset \bigcap S$, basta probar : $\forall I \in S$, $\exists P \in \mathcal{P} \ni P \subset I$.

Sea $I \in S$, como I es máximo , A/I es A-módulo derecho irreducible .

Por la nota en la pág. $P = \operatorname{an} A/I$ es un ideal primitivo derecho $\therefore P \in \mathcal{P}$. Además $P \subset I$: Pues si $p \in P$, sea e unitario izquierdo módulo I (I es regular) , entonces $\underline{ep - p \in I}$, $p \in P = \operatorname{an} A/I \Rightarrow I = (I + e)p = I + ep \therefore \underline{ep \in I}$.
Así $I = I + (ep - p) = (I + ep) - p = I - p \therefore -p \in I$, $\therefore p \in I$, es decir : $P \subset I$.

Definición

Sea A un anillo . $x \in A$ es casi-regular derecho si $\exists y \in A \ni x + y + xy = 0$, (abreviadamente diremos x es c.r.d.) .
Si A tiene 1 : x es c.r.d. $\Leftrightarrow (1 + x)$ es regular de-

recho : x c.r.d. $\Leftrightarrow x+y+xy=0$ p.a. $y \in A \Leftrightarrow$
$1+x+y+xy=1 \Leftrightarrow (1+x)(1+y)=1$.

<u>Notación</u> :

Denotamos $x \circ y = x+y+xy$. $(\circ)$ es asociativa y tiene 0 como neutro : $x \circ 0 = x+0+x\cdot 0 = x$, $0 \circ x = 0+x+0\cdot x = x$.
$(x \circ y) \circ z = (x+y+xy) \circ z = x+y+xy+z+xz+yz+xyz$.
$x \circ (x \circ z) = x \circ (y+z+yz) = x+y+z+yz+xy+xz+xyz$.

<u>Definición</u> .

Decimos que x es casi-regular (abreviamos c.r.) si x tiene casi-inverso derecho y casi-inverso izquierdo.

Nota :

Como $\circ$ es asociativa , ambos inversos coinciden , pues si $x\,y = 0$ y $z \circ x = 0$, entonces $z = z \circ 0 = z \circ (x \circ y) =$
$= (z \circ x) \circ y = 0 \circ y = y$.

Nota :

Si A tiene 1 , entonces $f : (A, \circ) \longrightarrow (A, \cdot)$
$x \stackrel{f}{\longmapsto} 1+x$ es un isomorfismo de monoides : $f(x \circ y) = f(x+y+xy) =$
$= 1+x+y+xy = (1+x)(1+y) = f(x)\cdot f(y)$, f es mono :
$f(z) = 1 \Rightarrow f(z) = 1+z = 1 \Rightarrow z = 0$.

f es epi : si $x \in A$, entonces $x = f(x - 1)$.

Notamos también que $(\{x \in A : x \text{ es c.r.}\}, \circ)$ es un grupo :

Ya notamos que $\circ$ es asociativa .

0 es c.r. : $0 + 0 + 0 \cdot 0 = 0$.

Si x es c.r. por definición $\exists\, y$ c.r. $\ni$ $x \circ y = 0$ y por la nota de la página anterior , $y \circ x = 0$.

x c.r. , y c.r. $\Longrightarrow \exists\, x'$, y' $\ni$ $x \circ x' = 0 = y \circ y'$, ahora

$(x \circ y) \circ (y' \circ x') = x \circ (y \circ y' \circ x') = x \circ (0 \circ x') = x \circ x' = 0$.

<u>Definición</u> .

Un <u>anillo radical</u> A es un anillo $\ni$ $\forall x \in A$, x es c.r.

Ejemplos de anillos radicales :

1) El anillo trivial .

2) Cualquier anillo <u>nil</u> : si $x^n = 0$, entonces

$(-x) \circ (x + \ldots + x^{n-1}) = 0$.

<u>Teorema 8</u>

Sea I un ideal derecho del anillo A, x casi regular derecho , $\forall x \in I \Longrightarrow I$ es un anillo redical (como subanillo de A)

Prueba :

Por demostrar $\forall x \in I$, $\exists\, y \in I$ $\ni$ $x \circ y = 0 = y \circ x$.

$x \in I \Rightarrow x$ c.r.d. por hipótesis , $\therefore \exists\, y \in A \ni 0 = x \circ y =$ $= x + y + xy \therefore y = -x - xy \in I$, $\therefore y$ es c.r.d. , repitiendo el argumento , $\exists\, z \in I \ni y \circ z = 0$. Pero entonces $x \circ y = 0 = y \circ z$, y por la primera nota de la pág. 8 $x = z$, $\therefore y \circ x = 0$ también, $\therefore x$ es c.r. con $y \in I$ como casi-inverso .

Definición .

Un ideal I (izquierdo , derecho ó bilateral) tal que $\forall\, x \in I$, x es c.r. se llamará ideal radical .

Teorema 9

Sea A un anillo . Si $I \subset A$ es un ideal derecho radical y $M \subset A$ es ideal derecho regular máximo entonces $I \subset M$.

Prueba :

Si $\exists\, x \in I \setminus M$, entonces $I + M = A$ (M máximo) $\therefore$ si e es unitario izquierdo módulo M (M regular) entonces

$\exists\, i \in I$, $\exists\, m \in M \ni e = i + m$.

Como I es radical , $\exists\, j \in I \ni -i + j - ij = 0$ (Teorema 8)

Como $e = i + m$, $ej = ij + mj$ sumando ésto a $-i + j - ij = 0$ tenemos : $-i + j + mj = ej \therefore i = mj - (ej - j) \in M$ (pues e es unitario izquierdo módulo M) $\therefore e = i + m \in M$ y por la nota en la definición de ideal regular (pág. 4) $M = A$ $\underset{\circ}{\nabla}$ (Pues $M \subset A$ es máximo) .

Teorema 10 .

Si $I \subsetneq A$ es un ideal regular con unitario izquierdo módulo I, e , entonces : $\exists M \subsetneq A$ ideal regular máximo $\ni M \supset I$.

Prueba :

Haremos uso del Lema de Zorn . Sea :

$$\mathcal{P} = \{ A_\alpha \subset A \ : \ A_\alpha \text{ es ideal regular } , A_\alpha \supset I \ , e \notin A_\alpha \}$$

Como $I \subsetneq A$, $e \notin I$ $\therefore I \in \mathcal{P} \therefore \mathcal{P} \neq \emptyset$. $\mathcal{P}$ está ordenado parcialmente por la inclusión . Sea $\{T_\alpha\}_{\alpha \in \mathcal{A}}$ una cadena en $\mathcal{P}$ entonces $C = \bigcup_{\alpha \in \mathcal{A}} T_\alpha \in \mathcal{P}$; C es un ideal por ser $\{T_\alpha\}_{\alpha \in \mathcal{A}}$ una cadena ; $e \notin C$ obviamente y C es regular : $\forall a \in A$, $ea - a \in I$ $I \subset T_\alpha$ $\forall \alpha \in \mathcal{A} \therefore ea - a \in \bigcup_{\alpha \in \mathcal{A}} T_\alpha = C$ $\forall a \in A$.

Así $C \in \mathcal{P}$, y C es cota superior para $\{T_\alpha\}_{\alpha \in \mathcal{A}}$. El Lema de Zorn nos dice que la familia $\mathcal{P}$ tiene un elemento máximo M , regular con unitario izquierdo módulo M , e , y como $e \notin M$, $M \subsetneq A$.

Teorema 11

Sea A un anillo y $\mathcal{R} = \{ I \subset A \ : \ I \text{ es ideal derecho regular máximo} \}$, entonces $N = \bigcap \mathcal{R}$ es un ideal radical .

Prueba :

Sea $x \in N$, probaremos que x es c.r.d. En otro caso , el ideal de A . $I = \{ xy + y \ : \ y \in A \}$ es propio pues $x \notin I$

($x+y+xy \neq 0 \quad \forall y \in A$) y regular con unitario izquierdo módulo I, $-x$: $-xy - y = x(-y)+(-y) \in I \quad \forall y \in A$.
Por el Teorema 10, $\exists M \subsetneq A$ ideal regular máximo $\ni$ $M \supset I$ y con unitario izquierdo módulo M, $-x$, $-x \notin M$.
$-x \notin M \Longrightarrow x \notin M \ \underline{\forall}$ ($x \in N$) . $\therefore x$ es c.r.d. $\forall x \in N$, ahora por el Teorema 8, N es ideal radical.

Teorema 12.

Los siguientes ideales son idénticos :

(1) La intersección de los ideales derechos regulares máximos.

(2) La intersección de los ideales izquierdos regulares máximos.

(3) La intersección de los ideales primitivos derechos.

(4) La intersección de los ideales primitivos izquierdos.

Prueba :

Por el Teorema 7, (1) y (3) son idénticos $= N$. Por simetría (2) y (4) son idénticos, llamémosle N' a este ideal. Por el Teorema 11, N es ideal radical, y por el Teorema 9 ("dual"), $N \subset M$ para cualquier ideal izquierdo regular máximo, $\therefore N \subset N'$. Similarmente $N' \subset N$, $\therefore N' = N$.

Nota :

El ideal $N = N'$ es un ideal radical que contiene todo otro ideal radical ; por lo tanto llamamos a N <u>el</u> radical de A . En particular N contiene a todo nilideal (izquierdo , derecho ó bilateral) .

<u>Definición</u> .

Un anillo A satisface la condición de cadena descendente (C.C.D.) en ideales derechos , si toda cadena propiamente descendente de ideales derechos es finita .

<u>Definición</u> .

Un álgebra A sobre el campo F , es un espacio vectorial (sobre F) que es también un anillo , y además

$\alpha(xy) = (\alpha x)y = x(\alpha y) \quad \forall x , y \in A , \forall \alpha \in F$.

Nota :

Si un álgebra tiene 1 , cualquier ideal derecho (o izquierdo) es automáticamente un subespacio . (Si D es ideal derecho de A , entonces : $\forall d \in D , \forall \lambda \in F , d\lambda = (d \cdot 1)\lambda = (d \cdot (1\lambda)) \in D$ aquí $1 \in A , 1\lambda \in A$.) . Además si A , álgebra con 1 es de dimensión finita , A satisface C.C.D. en ideales derechos (izquierdos) .

<u>Definición</u>.

Sea A un anillo . Si $I \subset A$ y J es ideal derecho de A . Denotaremos IJ el ideal derecho de A generado por

$\{ij : i \in I , j \in J\}$.

Definición.

Sea A un anillo. El ideal $I \subset A$ es nilpotente si $\exists n \in \mathbb{N} \ni I^n = 0$.

Si I es nilpotente $m = \min\{n \in \mathbb{N} : I^n = 0\}$ es el grado de nilpotencia de I.

Lema.

Si $ax = a$ y $-x$ es c.r.d. entonces $a = 0$.

Prueba :

Si $ax = a$ y $-x \circ z = 0$ entonces $0 = a(-x \circ z) = (a)(-x + z - xz) =$
$= -ax + az - axz = -a + az - az = -a$, $\therefore a = 0$.

Teorema 13.

Si el anillo A goza de C.C.D. en ideales derechos, entonces N = radical de A es nilpotente.

Prueba :

Consideramos $N \supset N^2 \supset \ldots\ldots$ por hipótesis, $\exists k \in \mathbb{N} \ni N^k = N^{k+1}$.
Sea $P = N^k$, probamos $P = 0$. En otro caso $0 \neq P = P^2$.
Sea $\mathcal{J} = \{I$ ideal derecho de $A : IP \neq 0\}$, $\mathcal{J} \neq \emptyset$
pues $P \in \mathcal{J}$; $P^2 \neq 0$ por hipótesis. Como A goza de C.C.D.
en ideales derechos, podemos escoger $I_0 \in \mathcal{J}$ mínimo.

Así , $I_0 P \neq 0$ y $\exists\, x \in I_0 \ni xP \neq 0$, ahora , $(xP)P = xP^2 =$ $= xP \neq 0$ $\therefore$ $xP \in \mathfrak{J}$ y $xP \subset I_0$; por la selección de I_0 , $xP = I_0$, así que $\exists\, a \in P \ni xa = x$, pero $a \in P \subset N$ y los elementos del radical son c.r.d. (Teorema 11) , $\therefore$ $xa = x$, y $-a \in N$ es c.r.d.; por el lema anterior ; $x = 0$ y así : $xP = 0$ $\lightning$. La contradicción viene de suponer $P \neq 0$. $\therefore$ $P = N^k = 0$.

Definición .

Un álgebra A (sobre el anillo con división F) es <u>algebráica</u> , si todo $x \in A$ satisface $P(x) = 0$ para algún polinomio $P \in F[x]$ no trivial .

Teorema 14

El radical N de un álgebra algebráica es nil .

Prueba :

Sea $x \in N$, entonces $x^n + \ldots\ldots + \alpha x^k = 0$ con $\alpha \neq 0$, así , $x^k = \beta_1 x^{k+1} + \ldots\ldots - \alpha^{-1} x^n = x^k(\beta_1 x + \ldots - \alpha^{-1} x^{n-k})$.

Ahora , $\beta_1 x + \ldots - \alpha^{-1} x^{n-k} \in N$ pues $x \in N$ y el radical es un ideal . Por el lema anterior al Teorema 13 y usando el Teorema 11 , $x^k = 0$, es decir x es nilpotente .

Anillos Primitivos y el Teorema de Densidad

Definición .

El anillo A es simple si :

(i) $A^2 \neq 0$.

(ii) Los únicos ideales bilaterales de A son (0) y A .

Definición .

Sea M_A , $\alpha : M \longrightarrow M$ es un A-endomorfismo de M si :

(i) $\alpha : M \longrightarrow M$ es homomorfismo de grupos .

(ii) $\alpha(ma) = (\alpha m)a \quad \forall m \in M , \forall a \in A$.

Denotaremos por $\mathrm{End}_A M$ al conjunto de los A-endomorfismos de M .

Bajo las operaciones $(\alpha + \beta)m = \alpha m + \beta m \quad \forall \alpha , \beta \in \mathrm{End}_A M , \forall m \in M$

$(\alpha\beta)m = \alpha(\beta m) \quad \forall \alpha , \beta \in \mathrm{End}_A M , \forall m \in M$

el conjunto $\mathrm{End}_A M$ es un anillo .

Ejemplos :

1 . Si $A = \mathbb{Z}$, todo endomorfismo de grupo de M es A-endomorfismo .

2 . Si M es espacio vectorial sobre el anillo con división A , los A-endomorfismos son las transformaciones lineales de M .

Teorema 15 . (Lema de Schur) .

Si M_A es irreducible entonces $End_A M$ es un anillo con división .

Prueba :

Como Id_M es el uno de $End_A M$, nos basta probar que $\forall \alpha \in End_A M \setminus \{0\}$, $\exists\, \alpha^{-1} \in End_A M \ni \alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = Id_M$:

Supongamos $0 \neq \alpha \in End_A M$; $Im\,\alpha$ y $Ker\,\alpha$ son submódulos de M, irreducible; como $\alpha \neq 0$, $0 \neq Im\,\alpha$ y $Ker\,\alpha \neq M$ $\therefore$ $Im\,\alpha = M$ y $Ker\,\alpha = (0)$ $\therefore$ α es sobre e inyectiva , por lo que $\exists\, \alpha^{-1} : M \longrightarrow M$, función $\ni \alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = Id_M$.

Probamos ahora que $\alpha^{-1} \in End_A M$:

Si $m , n \in M$:

$\alpha^{-1}(m+n) = \alpha^{-1}(\alpha(m')+\alpha(n')) = \alpha^{-1}(\alpha(m'+n')) = m'+n' =$
$= \alpha^{-1}(m)+\alpha^{-1}(n)$ donde $m' = \alpha^{-1}(m)$ y $n' = \alpha^{-1}(n)$;

Si $m \in M$ y $a \in A$:

$\alpha^{-1}(ma) = \alpha^{-1}(\alpha(m')a) = \alpha^{-1}(\alpha(m'a)) = m'a = \alpha^{-1}(m)a$.

Aquí $m' = \alpha^{-1}(m)$ $\therefore$ $\alpha^{-1} \in End_A M$.

Nota :

Si A es un anillo primitivo derecho y M_A es irreducible y fiel , entonces $\exists\, \varphi : A \longrightarrow End_D M$ monomorfismo , con $D = End_A M$, (Considerando M como espacio vectorial izquierdo sobre el anillo con división D (Teo. 15)) , dado por

$\varphi(a)(m) = am \ \forall\ m \in M$, $a \in A$.

Probamos que $\varphi(a) \in End_D M$:

$\varphi(a)(m+m') = (m+m')a = ma+m'a = \varphi(a)(m)+\varphi(a)(m')$

$\forall m$, $m' \in M$.

Si $\psi \in End_A M$: $\varphi(a)(\psi m) = (\psi m)a = \psi(ma) = \psi(\varphi(a)m)$;

además φ es mono : pues si $a \in Ker\,\varphi$, $\varphi(a) = 0 \in End_D M$ por lo que $0 = \varphi(a)(m) = ma \ \forall\ m \in M$ $\therefore$ $a \in an\ M = (0)$ pues M es fiel $\therefore$ $a = 0$ y $\therefore$ $Ker\,\varphi = (0)$.

<u>Definición</u> .

Sea V un espacio vectorial sobre el anillo con división D .
Diremos que $\mathcal{S} \subset End_D V$ es n-transitivo si para cualesquiera dos conjuntos $\{x_1, \ldots, x_n\}$ linealmente independiente y $\{y_1, \ldots, y_n\}$, $\exists\, S \in \mathcal{S} \ni x_i S = y_i$ $i \in \{1, \ldots, n\}$
Si $\forall\, n \in \mathbb{N}$, $\mathcal{S}$ es n-transitivo , entonces $\mathcal{S}$ se llamará denso (en $End_D V$) .

<u>Teorema 16</u> . (Teorema de densidad) .

Sea A un anillo primitivo derecho , M_A irreducible y fiel (M es espacio vectorial sobre $D = End_A M$) entonces $\exists\,\varphi: A \longrightarrow End_D M$ monomorfismo con $\varphi(A)$ denso .

Prueba :

Definimos $\varphi: A \longrightarrow End_D M$ por : $\varphi(a)(m) = ma \ \forall m \in M$, $a \in A$;

por la nota en la pág. 17 φ es mono . Para probar la densidad de $\varphi(A)$ probamos primero el siguiente

Lema : Para cualquier subespacio $E \subset M$ de dimensión finita y $\forall\ 0 \neq x \in M \setminus E$, $\exists a \in A \ni \varphi(a)(E) = 0$ pero $\varphi(a)(x) \neq 0$. (es decir $\exists\ a \in$ an $E \setminus$ an x) !.

Probamos el lema por inducción sobre dim(E) :

Base : Si $\dim(E) = 0$, $E = (0)$, si $0 \neq x \in M$ entonces $xA = M$ (Teorema 3) (y $M \neq (0)$ pues M es irreducible).

Supongamos el resultado válido para los subespacios de dimensión $n-1$; sea E subespacio de M de dimensión n , así $E = F + Dy$ con $\dim(F) = n-1$, sea $J =$ an F , J es ideal derecho de A y $\therefore$ yJ es submódulo de M !.

Por la hipótesis de inducción $(0) \neq yJ$ $\therefore$ $yJ = M$ (M es irreducible) !.

Si an $E \subset$ an x (contra la afirmación del lema) para $\underline{x \notin E}$, definimos $\alpha : M \longrightarrow M$ por $\alpha(yj) = xj$ (α está bien definida , pues si $yj_1 = yj_2$ entonces $y(j_1 - j_2) = 0$ $\therefore$ $j_1 - j_2 \in J$ anula F y también anula a y $\therefore$ $j_1 - j_2 \in$ an $E \subset$ an x $\therefore$ $j_1x = j_2x$) es fácil ver que $\alpha \in \mathrm{End}_A M$; ahora, por definición de α : $(\alpha y - x)J = 0$ y por la hipótesis de inducción $y - x \in F$ $\therefore$ $x \in F + Dy = E$! $\therefore$ an $E \not\subset$ an x , y así $\exists\ a \in$ an $E \setminus$ an x . Y aquí termina la demostración del lema !.

Ahora si $n \in \mathbb{N}$ y $\{x_1, \ldots, x_n\}$ es linealmente independiente y $\{y_1, \ldots, y_n\}$ son subconjuntos de M , entonces

$\exists\, a \in an\langle x_1 , \dots , x_{n-1}\rangle \setminus an\, x_n \therefore 0 \neq x_n a \therefore x_n aA = M$ (Teorema 3) $\therefore \exists\, a' \in A \ni x_n aa' = y_n$ hacemos $a_n = aa'$ y notamos que : $x_n a_n = y_n$, $x_i a_n = 0$ si $1 \leq i \leq n-1$, análogamente $\exists\, a_i \in A \ni$ $x_j ai = \begin{cases} y_i & \text{si } j = i \\ 0 & \text{si } j \neq i \end{cases}$

Tomando $\bar{a} = a_1 + a_2 + \dots + a_n$ tenemos que $\varphi(\bar{a})(x_i) = x_i\bar{a} = x_i a_i = y_i$ $i \in \{1 , \dots , n\} \therefore \varphi(A)$ es n-transitivo $\forall\, n \in \mathbb{N} \therefore \varphi(A)$ es denso '.

Teorema 17 .

Si el anillo primitivo A goza de C.C.D. en ideales derechos , entonces $\varphi : A \longrightarrow End_D M \ni \varphi(a)(m) = ma \ \forall m \in M$, $a \in A$, es un isomorfismo (M es espacio vectorial izquierdo sobre $D = End_A M$) . En particular , (Wedderburn-Artin) esto es cierto para A simple con C.C.D. en ideales derechos .

Prueba :

Por el Teorema 16 , basta probar que $\dim M < \infty$ '. En caso contrario , sea $\{x_n\}_{n \in \mathbb{N}}$ l.i. en M , sea $I_r = an\langle x_1 , \dots , x_r\rangle$ entonces $I_1 \supset I_2 \supset I_3 \supset \dots$ es una cadena estrictamente descendente (Teorema 16) γ .

Nota :

Una consecuencia particular del Teorema 17 es que todo anillo primitivo derecho con C.C.D. en ideales derechos tiene 1 .

Lema .

La única álgebra con división de dimensión finita sobre un campo F , algebráicamente cerrado es F .

Prueba :

Sea $F[x]$ el anillo de los polinomios con coeficientes en F , recordamos que $F[x]$ es un anillo euclidiano y por lo tanto , es de ideales principales . Sea $a \in D$, tomamos $I = \{ f(x) \in F[x] : f(a) = 0 \}$ notamos que I es un ideal de $F[x]$. Además $I \neq (0)$ pues si $n = \dim D$ entonces $\{ a , a^2 , \ldots , a^{n+1} \} \subset D$ es linealmente independiente y $\therefore \exists \lambda_1 , \ldots , \lambda_{n+1} \in F$, no todos cero , tales que : $0 = \sum_{i=1}^{n+1} \lambda_i a^i$ así $0 \neq \sum_{i}^{n+1} \lambda_i x^i = f(x) \in I$.

Como $F[x]$ es de ideales principales , $\exists\, p(x) \in I \ni I = (p(x))$. Afirmamos que $p(x)$ es irreducible , pues en otro caso , $p(x) = q(x)s(x)$ con grado($q(x)$) $<$ grado($p(x)$) y grado($s(x)$) $<$ grado($p(x)$) , ahora , $0 = p(a) = q(a)s(a)$ y $\therefore$ $q(a) = 0$ ó $s(a) = 0$ (D es anillo con división) , supongamos sin pérdida de generalidad $q(a) = 0$ así que $q(x) \in I = (p(x))$ $\therefore$ $q(x) = p(x)t(x)$ con $t(x) \in F[x]$ y $\therefore$ grado($q(x)$) $\geq$ grado($p(x)$) ∇_0 $\therefore$ $p(x)$ es irreducible en $F[x]$, pero como F es algebraicamente cerrado , los únicos polinomios irreducibles en $F[x]$ son de grado 1 $\therefore$ $p(x) = cx+d$ con $c,d \in F$ y $c \neq 0$ $\therefore$ $0 = p(a) = ca+d$ $\therefore$ $a = c^{-1}(-d) \in F$ $\therefore$ $D \subset F$ $\therefore$ $D = F$ ($D \subset F \Longrightarrow \dim D \leq 1$ $0 \neq D \Longrightarrow \dim D > 0$) .

Definición.

Sean F un campo , V_F y $A \subset \mathrm{End}_F V$. $W_F \subset V_F$ es invariante bajo A si $(W_F)A \subset W_F$.

Teorema 16°. (Teorema clásico de densidad) .

Sean F un campo algebráicamente cerrado y ${}_F V$ de dimensión finita . Si $(0) \neq A \subset \mathrm{End}_F V$ es un álgebra cuyos únicos subespacios invariantes son (0) y V entonces : $A \cong \mathrm{End}_F V$.

Prueba :

Usaremos el Teorema 16 . Notamos primero que V es A-módulo derecho . V_A es fiel pues $a \in an_A V \Longrightarrow (v)a = 0$ $\forall v \in V$ y así $a = 0 \in \mathrm{End}_F V$ $\therefore$ $an_A V = (0)$. Además V_A es irreducible , pues si $(0) \neq W_A \subset V_A$, tomamos $0 \neq x \in W_A$ y así : $xA \subset W_A \subset V_A$, pero xA es un subespacio vectorial de V ($\lambda(xa) = x(\lambda a) \in xA$, $\forall \lambda \in F$, $\forall x \in V$, $\forall a \in A$) $\therefore$ $xA = 0$ ó $xA = V$; si $xA = 0$ entonces $0 \neq x \in \langle x \rangle$ el subespacio generado por x , y $\langle x \rangle A = (0) \subset \langle x \rangle$ por lo que $\langle x \rangle$ sería invariante y distinto de (0), por lo que $\langle x \rangle = V$

y así: $(V)A = (0)$, por lo que $A = 0$, contra la hipótesis.
$\therefore xA = V$ y así $xA = V \subset W_A \subset V_A$ por lo que $W_A = V_A$.
$\therefore (0) \neq W_A \subset V_A \Longrightarrow W_A = V_A$, es decir V_A es irreducible.

Ahora $End_A V \subset End_F V$ pues si $\alpha \in End_A V$, $\lambda \in F$, $x \in V$ entonces $\forall y \in V \setminus \{0\}$, $\exists a \in A$ tal que $ya = x$, por el Teorema 16, así: $\alpha(\lambda x) = \alpha(\lambda(ya)) = \alpha((y)(\lambda a)) = [\alpha(y)](\lambda a) = \lambda[\alpha(y)a] = \lambda[\alpha(ya)] = \lambda[\alpha(x)]$ $\therefore \alpha \in End_F V$
$\therefore End_A V \subset End_F V$. $\therefore End_A V$ es un álgebra de transformaciones lineales de V, con división ya que V_A es irreducible (lema de Schur) y de dimensión finita. Así que por el lema anterior a este teorema, $End_A V \cong F$. Ahora, aplicando el Teorema 16, tenemos que A es un anillo denso de transformaciones lineales de V, pero como $\dim(V) < \infty$ ésto implica: $A \cong End_F A$.

Anillos semiprimitivos

Si A es un anillo , denotaremos con $R(A)$ al radical de A , o simplemente R , si no hay posibilidad de confusión .

Lema.

Si $\bar{x} \in A/R$ es casi-regular derecho , y $x \in \bar{x}$, entonces x es casi-regular derecho .

Prueba :

$\bar{x}$ c.r.d. $\Longrightarrow \exists\, \bar{y} \in A/R$ tal que $\overline{x \circ y} = 0$. Sea $y \in \bar{y}$ ahora , $\pi(x \circ y) = \overline{x \circ y} = \bar{0} \in A/R$ (donde $\pi : A \longrightarrow A/R$ es el epimorfismo canónico) $\therefore$ $x \circ y \in R$ y $\therefore$ $x \circ y$ es c.r.d. y $\exists\, z \in A$ tal que $0 = (x \circ y) \circ z = x \circ (y \circ z)$ de donde x es casi-regular derecho .

Teorema 10 .

Para cualquier anillo A , $R(A/R) = 0$.

Prueba :

Sea $A \xrightarrow{\pi} A/R$ el epimorfismo canónico . Si $R' = R(A/R)$ entonces $\pi^{-1}(R')$ es un ideal radical en A por el lema anterior (todos los elementos de $\pi^{-1}(R')$ son c.r.d.) . Pero te do ideal radical está incluído en R por lo que $\pi^{-1}(R')\subset R$ de donde $R'\subset\pi(R) = 0\in A/R$.

Nota :

Si $\varphi: A \twoheadrightarrow B$ es un epimorfismo de anillos , entonces $\varphi(R(A))\subset R(B)$.

<u>Lema 19.1 .</u>

Si A es un anillo y $-x^2 A$ es c.r.d. entonces x es c.r.d.

Prueba :

Si $-x^2\circ y = 0$ entonces $x\circ([-x]\circ y) = x\circ(-x)\circ y = (-x^2)\circ y = 0$.

<u>Lema 19.2 .</u>

Sea A un anillo y $x\in A$, entonces : xA es un ideal radical si y sólo si $x\in R(A)$.

Prueba :

Si $x\in R(A)$ entonces xA es un ideal radical ($R(A)$ es un ideal bilateral) . Recíprocamente , si xA es un ideal radical , sea J el ideal derecho generado por x ,

$J = \{nx+xa : n\in\mathbb{Z},\ a\in A\}$, probaremos que J es un ideal radical .

Si $y = nx+xa$ entonces
$$-y^2 = -n^2x^2 - nx^2a - nxax - xaxa$$
$$= x(-n^2x - nxa - nax - axa)\in xA ,$$

pero por hipótesis xA es un ideal radical $y \therefore -y^2$ es c.r.d. ahora, por el lema 19.1 tenemos que y es c.r.d. $\forall y \in J$ $\therefore J$ es un ideal radical, y así : $x \in J \subset R(A)$.

Teorema 19 .

Sea I un ideal derecho del anillo A, entonces $R(I) \supset I \cap R(A)$; y si además I es un ideal bilateral, entonces $R(I) = I \cap R(A)$.

Prueba :

Si $x \in I \cap R(A)$, entonces $\exists\, y \in A$ tal que $x \circ y = 0 = x + y + xy$, y así $y = -x - xy \in I$ de donde $I \cap R(A)$ es un ideal radical contenido en I, $\therefore I \cap R(A) \subset R(I)$. Si además I es bilateral, entonces $\forall x \in R(I)$ $\forall a \in A$, $-(xa)^2 = -x(axa) \in R(I)$ $\therefore -(xa)^2$ es c.r.d. y por el lema 19.1 xa es c.r.d. por lo que xA es un ideal derecho radical incluído en A ; por el lema 19.2, $x \in R(A)$, $\therefore R(I) \subset R(A)$, y así $R(I) \subset I \cap R(A)$ de donde $R(I) = I \cap R(A)$ (por la otra parte del teorema) .

Definición .

Sea A un anillo . Los ideales I_1, I_2 de A son primos relativos si : $I_1 + I_2 = A$.

Teorema chino del residuo.

Sea A un anillo con 1 . Si $I_1, \ldots, I_n$ son ideales bi laterales de A tales que I_i es primo relativo a $\bigcap_{j \neq i}^{n} I_j \quad \forall\, i \in \{1, \ldots, n\}$, entonces el homomorfismo natural $A \xrightarrow{\pi} A/I_1 \times \ldots \times A/I_n$ es sobre.

Prueba :

Por inducción sobre n. Para $n = 1$ es obvio. Si $n = 2$, sean $a + I_1 \in A/I_1$, $b + I_2 \in A/I_2$, por demostrar : $\exists\, x \in A$ tal que $x - a \in I_1$, $x - b \in I_2$.

Como $A = I_1 + I_2$, $1 = i_1 + i_2$ con $i_1 \in I_1$, $i_2 \in I_2$, y así :
$(b - a) = (b - a)i_1 + (b - a)i_2$ de donde :
$b = a + (b - a)i_1 + (b - a)i_2$.

Consideramos $x = a + (b - a)i_1 = b - (b - a)i_2$, tenemos que $(x - a) = (b - a)i_1 \in I_1$, $(x - b) = -(b - a)i_2 \in I_2$, de donde, el Teorema para $n = 2$ vale.

Ahora, sea $k \in \mathbb{N}$, $k > 2$, e $I_1, I_2, \ldots, I_k$ ideales bilaterales que satisfacen la hipótesis del Teorema, entonces :
$I_\ell + \bigcap_{j \notin \{\ell,k\}} I_j \supset I_\ell + \bigcap_{j \notin \{\ell\}} I_j = A$ de donde $I_\ell + \bigcap_{j \notin \{\ell,k\}} I_j = A$, y así por hipótesis de inducción el homomorfismo natural

$\varphi : A \longrightarrow A/I_1 \times \ldots \times A/I_{k-1}$ es sobre, con $\operatorname{Ker}\varphi = I_1 \cap \ldots \cap I_{k-1}$

Sean ahora : $a_1 + I_1 \in A/I_1, \ldots, a_k + I_k \in A/I_k$. $\exists\, x \in A$, tal que $\varphi(x) = (a_1 + I_1, \ldots, a_{k-1} + I_{k-1}) \in A/I_1 \times \ldots \times A/I_{k-1}$ (φ es sobre), y así : $x - a_1 \in I_1, \ldots, x - a_{k-1} \in I_{k-1}$.

Como por hipótesis $(I_1 \cap \ldots \cap I_{k-1}) + I_k = A$, tenemos que $1 = j + i_k$ con $j \in I_1 \cap \ldots \cap I_{k-1}$, $i_k \in I_k$ de donde :

$a_k - x = (a_k - x)j + (a_k - x)i_k$, tomando
$z = (x + (a_k - x)j) = a_k + (x - a_k)i_k$ tenemos :
$z - a_i = (x - a_i) + (a_k - x)j \in I_i + (I_1 \cap \ldots \cap I_{k-1}) \subset I_i$
$\forall i \in \{1 , \ldots , k-1\}$ y $z - a_k = (x - a_k)i_k \in I_k$, de
donde:
$\Pi(z) = (a_1 + I_1 , \ldots , a_{k-1} + I_{k-1} , a_k + I_k) \in A/I_1 \times \ldots \times A/I_k$
de donde $\Pi : A \longrightarrow A/I_1 \times \ldots \times A/I_k$ es sobre.

Nota:

Si A es un anillo con Uno , e $I_1 , \ldots , I_n$ son ideales bilaterales de A tales que son primos relativos dos a dos y además $A^2 + I_r = A$ $\forall r \in \{1 , \ldots , n\}$ (Es decir: $(A/I_r)^2 = A/I_r$ $\forall r \in \{1 , \ldots , n\}$) , entonces el homomorfismo natural $\Pi : A \longrightarrow A/I_1 \times A/I_2 \times \ldots \times A/I_k$, es sobre .

Prueba :

Como $I_1 + I_2 = A$, $I_1 + I_3 = A$ entonces :
$A^2 = (I_1 + I_2)(I_1 + I_3) \subset I_1 + I_2 I_3 \subset I_1 + (I_2 \cap I_3)$. Como
$A^2 + I_1 = A$, entonces $A = A^2 + I_1 \subset I_1 + (I_2 \cap I_3)$
$\therefore A = I_1 + (I_2 \cap I_3)$.
Repetimos esencialmente el mismo argumento , usando
$A = (I_1 + (I_2 \cap I_3))(I_1 + I_4)$ para concluir
$A = I_1 + (I_2 \cap I_3 \cap I_4)$. Iterando, $I_1 + (I_2 \cap \ldots \cap I_n) = A$. Un argumento análogo prueba que cada I_r es primo relativo a $\bigcap_{k \neq r} I_k$ y concluímos aplicando el Teorema anterior.

Teorema 20. (Wedderburn-Artin).

Sea A un anillo semiprimitivo con C.C.D. en ideales bilaterales. Supongamos además que para todo ideal primitivo derecho P, de A, A/P goza de C.C.D. en ideales derechos, entonces A es producto directo de un número finito de anillos simples, cada uno de ellos isomorfo a un anillo de matrices con coeficientes en un anillo con división.

Prueba:

Sea P un ideal primitivo derecho de A (por definición P es un ideal bilateral de A). Por el Teorema 17, A/P es isomorfo a un anillo de matrices con coeficientes en un anillo con división, en particular, A/P es simple y con 1, $\therefore A^2+P=A$. Notamos además que si $P_i \neq P_j$ son ideales primitivos derechos de A, entonces P_i, P_j son primos relativos (Si $P_i \neq P_j$ son ideales primitivos derechos de A, podemos suponer sin pérdida de generalidad: $P_i \not\subset P_j$, entonces, como A/P_j es simple y $P_i+P_j/P_j \neq (0)$ pues $P_i \not\subset P_j$ tenemos que $A/P_j = P_i+P_j/P_j$ de donde $A = P_i+P_j$).

Afirmamos que A contiene un número finito de ideales primitivos derechos. Pues en caso contrario, sea $\{P_1, P_2, \ldots\}$ una colección numerable de ideales primitivos derechos; notamos que la cadena $P_1 \supset P_1 \cap P_2 \supset \ldots \supset (P_1 \cap \ldots \cap P_n) \supset \ldots$ es estrictamente descendente, pues si $P_1 \cap \ldots \cap P_n = P_1 \cap \ldots \cap P_n \cap P_{n+1}$, entonces

$P_1 \cap \ldots \cap P_n \subset P_{n+1}$. (Como $(A/P_i)^2 = A/P_i$ para cada i , y además $P_i \neq P_j$ son primos relativos cuando P_i , P_j son ideales primitivos derechos , entonces por la demostración de la Nota anterior a este Teorema , P_{n+1} y $(P_1 \cap \ldots \cap P_n)$ son primos relativos) $\therefore P_{n+1} = A$ $\veebar$ ($A/P_{n+1} \cong (0)$ no es anillo primitivo) . $\therefore$ el conjunto de ideales primitivos derechos de A es finito $= \{P_1, \ldots, P_n\}$ p.a. $n \in \mathbb{N}$, ahora , $\bigcap_i^n P_i = R(A) = 0$ pues por hipótesis A es semiprimitivo (y usando la Nota siguiente al Teorema 12) , así que el epimorfismo natural $\pi : A \twoheadrightarrow A/P_1 \times \ldots \times A/P_n$ garantizado por el Teorema chino del residuo tiene núcleo $\operatorname{Ker}\pi = \bigcap_i^n P_i = 0$ $\therefore A \overset{\pi}{\cong} A/P_1 \times \ldots \times A/P_n$.

<u>Definición</u> .

Sea A un anillo . Decimos que $a \in A$ es Regular (en el sentido de Von Neumann) si $\exists x \in A$ tal que $axa = a$.
Si $\forall a \in A$, a es Regular entonces diremos que A es un anillo Regular .

Ejemplos de anillos Regulares :

1. Cualquier anillo con división .
2. Los productos dirctos de anillos Regulares .
3. El anillo de las matrices de $n \times n$ con coeficientes en un anillo Regular (ver el Teorema 24) .

4. $End_D V$, donde V es un espacio vectorial sobre un anillo con división D .

Notas .

1. (Von Neumann) . En un anillo Regular , el conjunto de los ideales derechos principales es una red modular con complementos .

2. Una imágen homomórfica de un anillo Regular es Regular .

Teorema 21 .

Cualquier anillo Regular es semiprimitivo .

Prueba :

Sea A un anillo Regular . Sea $a \in R(A)$ supongamos $axa = a$, entonces $(ax)^2 = axa \cdot x = ax$ $\therefore$ ax es un idempotente en $R(A)$ $\therefore$ $ax = 0$. (El radical no contiene elementos idempotentes distintos de 0 : si $0 \neq e \in R(A)$ es idempotente , entonces $-e$ es c.r.d. $\therefore \exists y \in A \ni -e + y - ey = 0$
$\therefore -ee + ey - eey = 0 = -e + ey - ey = -e \therefore -e = 0$ $\underset{\circ}{\nabla}$) .

Lema . (Mc Coy) .

Si $axa - a$ es Regular , entonces a es Regular .

Prueba :

$(axa - a)y(axa - a) = axa - a \Longrightarrow a = a(x - y - xayax + xay + yax) \cdot a$.

Teorema 22 .

Sea $0 \longrightarrow I \xrightarrow{i} A \xrightarrow{\pi} A/I \longrightarrow 0$ una sucesión exacta de anillos , entonces : A es Regular $\Longleftrightarrow I$, A/I son Regulares .

Prueba :

$\Rightarrow$) Supongamos que A es Regular . Si $y \in A/I$, sea $x \in A$ $\ni \pi(x) = y$, como A es Regular , $\exists z \in A \ni xzx = x$

$\therefore \; x = \pi(x)\pi(z)\pi(x)$

$= y\pi(z)y$ con $\pi(z) \in A/I$ $\therefore A/I$ es Regular . Ahora , si $a \in I_1$, $\exists z \in A \ni i(a)zi(a) = aza = i(a) = a$ pero entonces $a = (a)za = (aza)za = a(zaz)a$ con $zaz \in I$ (ideal bilateral de A) $\therefore I$ es Regular .

$\Leftarrow$) Recíprocamente , supongamos $0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$ es exacta con I , A/I Regulares . Si $x \in A$, $\exists \bar{z} \in A/I$ $\ni \pi(x) = \pi(x)\bar{z}\pi(x)$. Sea $z \in A \ni \pi(z) = \bar{z}$, entonces

$\pi(x) = \pi(x)\pi(z)\pi(x) = \pi(xzx) \;\therefore\; \pi(xzx - x) = 0$

$\therefore\; xzx - x$ es Regular y por el Lema de Mc Coy , a es Regular, $\therefore A$ es Regular .

Definición .

Si A es un anillo , el ideal bilateral $I \subset A$ es un ideal Regular si I es un anillo Regular como subanillo de A .

Teorema 23 .

Cualquier anillo A tiene un único ideal Regular máximo M , y A/M no tiene ideales Regulares distintos de cero .

Prueba :

Si I , J son ideales Regulares de A entonces $I+J$ es Regular : pues $I+J/J \cong I/I\cap J$ con $I/I\cap J$ Regular por ser cociente de I , Regular . Entonces tenemos la siguiente sucesión exacta : $0 \longrightarrow J \longrightarrow I+J \longrightarrow I/I\cap J \longrightarrow 0$ con J , $I/I\cap J$ Regulares , y así por el Teorema anterior $I+J$ es Regular . Inductivamente , $I_1+I_2+\ldots+I_m$ es Regular para cualquier colección $\{I_1 , \ldots , I_m\}$ de ideales Regulares . Ahora , si $\{I_\alpha\}_a$ es el conjunto de los ideales Regulares de A , entonces :

i) $\sum_a I_\alpha$ es Regular ; pues $x \in \sum_a I_\alpha \Longrightarrow (x = i_{\alpha_1}+\ldots+i_{\alpha_m}$ está en $I_{\alpha_1}+\ldots+I_{\alpha_m}$, que es un ideal Regular de $A) \Longrightarrow$ x es Regular .

ii) $M = \sum_a I_\alpha$ es el único ideal Regular máximo , obviamente . Ahora , si $J\subset A/M$ es un ideal Regular , entonces $J = I_0/M$ con I_0 ideal de A y así tenemos la sucesión exacta $0 \longrightarrow M \longrightarrow I_0 \longrightarrow J \longrightarrow 0$ con M y J Regulares por lo que I_0 es Regular y $\therefore$ $I_0\subset M$ por lo que $J = M/M = 0$.

__Lema 23.1 .__

Si $J\subset I\subset A$ con J ideal derecho de I e I ideal Regular de A , entonces J es ideal derecho de A .

Prueba :

Si $j\in J$, $a\in A$, entonces $\exists\, x\in I \ni jxj = j$ pero entonces $ja = (jxj)a = j(xja)$ con $xja\in I$ $\therefore$ $ja = j(xja)\in J(xja)\subset J$.

Lema 23.2 .

Sean A un anillo e I un ideal bilateral de A . Si I tiene neutro multiplicativo , entonces I es factor directo de A .

Prueba :

Sea e el neutro multiplicativo de I , entonces e conmuta con todo elemento de A pues $x \in A \Longrightarrow ex \in I$

$\therefore$ $exe = ex$, por otra parte $xe \in I$ $\therefore$ $exe = xe$ de donde $ex = exe = xe$ $\forall x \in A$.

Sea $J = \{ a - ea : a \in A \}$, J es ideal bilateral de A (usando que $ex = xe$ $\forall x \in A$) , $A = I + J$ pues :

$\forall a \in A$ $a = ae + (a - ea) \in I + J$.

$x \in I \cap J \Longrightarrow x = a'' - ea''$ con $a'' \in A$ $\therefore$ $x = ex = ea'' - eea'' =$

$= ea'' - ea'' = 0$

$\therefore I \cap J = 0$.

Y si $(x+y)$, $(x'+y') \subset I + J$, con x , $x' \in I$, y, $y' \in J$ entonces $(x+y)(x'+y') = xx' + xy' + yx' + yy'$ pero xy' , $yx' \in I \cap J = (0)$ $\therefore$ $(x+y)(x'+y') = xx' + yy'$.

$\therefore$ $A \cong I \times J$.

Teorema 23' .

Si A es un anillo con C.C.D. en ideales derechos , entonces $A \cong M \times N$ donde M es el ideal Regular máximo de A y

N no tiene ideales Regulares distintos de (0) .

Prueba:

Por el lema 23.1 M goza de C.C.D. en ideales derechos (los ideales derechos de M son ideales derechos de A) . Como cualquier anillo Regular es semiprimitivo (Teorema 21) , por el Teorema 20 M tiene neutro multiplicativo , (estamos dentro de las hipótesis del Teorema 20 , pues M goza de C.C.D. en ideales derechos , pues si $\pi : M \longrightarrow M/P$ es el epimorfismo canónico e $I_1 \supset I_2 \supset \ldots$ es una cadena de ideales derechos de M , estacionaria por hipótesis , y $\pi^{-1}(I_m) = \pi^{-1}(I_s) \Longrightarrow I_m = I_s$) . Ahora , como M tiene neutro multiplicativo , por el lema 23.2 tenemos que $A \cong M \times N$ y $N \cong A/M$ por lo que el único ideal Regular de N es (0) (Teorema 23) .

Teorema 24 .

Si $M_{n \times n}(R)$ es el anillo de las matrices de $n \times n$ con coeficientes en un anillo Regular R , entonces $M_{n \times n}(R)$ es Regular.

Prueba :

Consideramos primero el caso $n = 2$.

Si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{n \times n}(R)$ y $crc = c$ para r R , entonces :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} arc & ard-b \\ 0 & crd-d \end{pmatrix}$$ y así

por el Lema de Mc Coy basta probar que las matrices de la forma $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ son Regulares . Ahora si $axa = a$ y $dyd = d$ entonces :

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} - \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & axb-b \\ 0 & 0 \end{pmatrix}$$ y

de nuevo por el Lema de Mc Coy basta probar que las matrices de la forma $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ son Regulares , pero si $bzb=b$ entonces

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ z & 0 \end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & bzb \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$ y $\therefore$ $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ es

Regular , y hemos terminado el caso $n = 2$.

Para $n = 4$ observamos que las matrices en $M_{4\times 4}(R)$ son matrices en $M_{2\times 2}(M_{2\times 2}(R))$ es decir , de la forma $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$

con A , B , C , $D \in M_{2\times 2}(R)$ y aplicamos el argumento para el caso $n=2$. Inductivamente obtenemos el resultado para $n = 2^k$ con $k \in \mathbb{N}$ (los elementos de $M_{2^k \times 2^k}(R)$ son elementos en $M_{2\times 2}(M_{2^{k-1} \times 2^{k-1}}(R))$. Si $n \in \mathbb{N}$ es arbitraria tomamos $k \in \mathbb{N}$, $2^k \geq n$ y $\exists\, \varphi : M_{n\times n}(R) \rightarrowtail M_{2^k \times 2^k}(R)$ monomorfismo tal que para $A \in M_{n\times n}(R)$, $A \overset{\varphi}{\longmapsto} \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \in M_{2^k \times 2^k}(R)$ y observamos que $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$ y que $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$

es idempotente en $M_{2^k \times 2^k}(R)$. Y así el caso general se si gue de la siguiente :

Afirmación : Si A es un anillo Regular y $e \in A$ es idempotente , entonces eAe es Regular.

Prueba : $eae = eaexeae$ para alguna $x \in A$, así :

$eae = eae^2xe^2ae = eae(exe)eae$ y $exe \in eAe$ $\therefore$ eAe es Regular .

Definición .

Sea G un grupo y F un campo . El álgebra del grupo G sobre el campo F es el conjunto de todas las combinaciones lineales (formales) $\sum \lambda_i g_i$ de los elementos $g_i \in G$ donde $\lambda_i \in F$ y $\mathcal{N} \lambda_i$, $\lambda_i = 0$. Las operaciones algebráicas son las obvias.

Teorema 25 . (Maschke) .

Sea A el álgebra del grupo finito G sobre el campo F , entonces :

a) $car(F) = 0 \Longrightarrow R(A) = 0$

b) Si $car(F) = p$ entonces : $p \nmid o(G) \Longleftrightarrow R(A) = (0)$.

Prueba:

La prueba es en dos pasos :

I) Probamos primero la parte recíproca de b) :

Supongamos que $car(F) = p \mid n = o(G)$. Sea $\alpha = g_1 + \ldots + g_n$.

Como $g_iG = G = Gg_i$, evidentemente $g_i\alpha = \alpha = \alpha g_i$ $\forall i \in \{1, \ldots, n\}$.

De aquí que α está en el centro de A , que denotamos $Z(A)$. Además $\alpha^2 = \alpha\cdot\alpha = (g_1+\ldots+g_n)\alpha = g_1\alpha+\ldots+g_n\alpha = n\alpha$. Como $p|n$ tenemos que $0 = n\alpha = \alpha^2$.

Ahora , $\forall y \in A$ tenemos : $(\alpha y)^2 = \alpha y\alpha y = \alpha^2 y^2 = 0\cdot y^2 = 0$ pues $\alpha\in Z(A)$, $\therefore (\alpha A)^2 = (0)$. Es decir , αA es ideal nilpotente de A y : αA nilpotente $\Longrightarrow \alpha A \subset R(A)$. Y como $0 \neq \alpha = \alpha g_1 \in \alpha A \subset R(A)$ tenemos que $R(A) \neq 0$.

II) Probamos ahora las partes directas de a) y b) :

Supongamos $car(F) = 0$ o $car(F) = p$ con $p\nmid n$.

Consideramos el epimorfismo de álgebras $\varphi: A \twoheadrightarrow End_F A$, $End_F A$ el álgebra de las transformaciones lineales de A , donde $a \overset{\varphi}{\longmapsto} R_a$, R_a tal que $a'R_a = a'a$ $\forall a' \in A$.

Si $0 \neq \sum \lambda_i g_i \in R(A)$, multiplicando por un elemento apropiado de A , obtenemos un elemento $x \in R(A)$ ($R(A)$ es un ideal bilateral de A) de la forma $x = 1\cdot e + \mu_1 g_1 + \ldots + \mu_r g_r$, y $\varphi(x) = Id_A + \mu_1\varphi(g_1) + \ldots + \mu_r\varphi(g_r) = Id_A + \mu_1 R_{g_1} + \ldots + \mu_1 R_{g_r}$.

Tomando como base para A a los elementos de G , tenemos que R_{g_i} es una matríz de permutación , correspondiente a una permutación que no deja fijo ningún elemento de G . De aquí que R_{g_i} tiene ceros en la diagonal y $\therefore$ la traza $Tr(R_{g_i}) = 0$.

Por otra parte , x es nilpotente ($x \in R(A)$ y A goza de C.C.D. por ser $\dim(A) < \infty$) , $\therefore R_x$ es nilpotente , $\therefore Tr(R_x) = 0$. Pero $Tr(R_x) = n \neq 0$ pues $car(F) = 0$ o $car(F) = p$ y $p\nmid n$ por hipótesis ∇ . La contradicción viene de suponer $0 \neq \sum \lambda_i g_i \in R(A)$, $\therefore R(A) = 0$.

Del Teorema 25 podemos deducir un resultado acerca de la Regularidad de ciertas álgebras de grupo de dimensión infinita .

Definición .

Un grupo G es localmente finito si todo subgrupo de G finitamente generado es finito .

Teorema 26 .

Sea G un grupo localmente finito . Sea A el álgebra de grupo de G sobre un campo F . Entonces :

$car(F) = 0$ ó $(car(F) = p$ y $o(g) \neq p \ \forall g \in G) \Longrightarrow A$ es Regular.

Prueba :

Sea $x \in A$, $\exists g_1 , \ldots , g_n \in G$ tales que $x \in \langle g_1 , \ldots , g_n \rangle = B$, la subálgebra de A generada por $\{g_1 , \ldots , g_n\}$. Como G es localmente finito , $g_1 , \ldots , g_n$ generan un subgrupo finito G' de G . Ahora , B es el álgebra de grupo de G' sobre F , y por el Teorema 25 , $R(B) = 0$, pero B es también Regular ya que cualquier álgebra con radical 0 , y de dimensión finita es Regular , $\therefore$ x es Regular .

Este teorema estimuló una serie de investigaciones acerca de la validez del recíproco . M. Auslander , Mc Laughlin y Villamayor obtuvieron resultados parciales , posteriormente Villamayor probó completamente el recíproco : Si el álgebra de grupo de G sobre F, A, es Regular , entonces G es localmente finito ; y si $car(F) = p$, entonces $o(g) \neq p \ \forall g \in G$.

Recordemos el Teorema 1.6' (Teorema clásico de densidad) :
Si V es un espacio vectorial de dimensión finita sobre el campo F , algebráicamente cerrado , y A es un álgebra irreducible de transformaciones lineales de V entonces :
$A \cong End_F V$, el álgebra de transformaciones lineales de V .

Usando el Teorema 1.6' obtenemos :

<u>Teorema 1.6''</u> . (Teorema de Burnside) .
Sea S un subgrupo multiplicativo de transformaciones lineales de un espacio vectorial V de dimensión n , sobre el campo F algebráicamente cerrado . Supongamos que V es irreducible bajo S . Entonces S contiene n^2 transformaciones lineales linealmente independientes .

Prueba :
Sea A el álgebra generada por S . Aplicamos el Teorema 1.6' a A .

<u>Teorema A</u> .
Sea S un semigrupo multiplicativo irreducible de transforma

ciones lineales de un espacio vectorial V de dimensión n sobre un campo F, algebráicamente cerrado. Supongamos que las trazas de los elementos de S son exactamente k. Entonces S tiene a lo más k^{n^2} elementos.

Prueba :

Introducimos el producto interior $(A,B) = Tr(AB)$, en el álgebra de las transformaciones lineales de V, $End_F V$. $(\ ,\ )$ es no singular evidentemente. Sean $c_1, \ldots, c_k$ las trazas posibles. Sean A_i, $i \in \{1, \ldots, n^2\}$, n^2 elementos de S linealmente independientes (Teorema 16''). Cada $X \in S$ satisface ecuaciones $Tr(A_i X) = b_i$ donde $\{b_1, \ldots, b_n\} \subset \{c_1, \ldots, c_k\}$. Estas ecuaciones determinan X en forma única, así que hay a lo más k^{n^2} posibilidades para X. (Este uso del argumento de Burnside se debe a C. Procesi).

<u>Definición</u>.

Una matriz A es unipotente si todas sus raíces características son 1.

Equivalentemente, A es unipotente si $A = I + B$ donde I es la matriz identidad y B es nilpotente.

<u>Teorema B</u>. (Kolchin).

Sea S un semigrupo multiplicativo de matrices unipotentes, entonces los elementos de S se pueden triangular simultáneamente .

Prueba :

Por inducción sobre n = tamaño de las matrices . La base es trivial . Supongamos entonces que $n > 1$.

Caso I) . El campo F es algebráicamente cerrado .

Observamos que si $X \in S$, $X = I + B$ con I la matriz identidad y B matriz nilpotente ; como B es nilpotente $tr(B) = 0$ así que $tr(X) = tr(I) + tr(B) = tr(I) = n$. Así que la única traza posible para los elementos de S es n . Por el Teorema A , se tiene entonces : S irreducible $\Longrightarrow card(S) = 1^{n^2} = 1$. Pero una matriz de tamaño $n > 1$ siempre es reducible cuando el campo de escalares es algebráicamente cerrado (ver Lang, Algebra lineal) y $\therefore$ S es reducible . Entonces , escogiendo una base para el subespacio invariante de S , y extendiéndola a una base para todo el espacio , todos los elementos de S corresponden a matrices con forma de bloque :

$$\begin{pmatrix} B & C \\ 0 & D \end{pmatrix} .$$

Ahora , los conjuntos S_L , de las esquinas superiores izquierdas B , y S_K de las esquinas inferiores derechas D , forman semigrupos multiplicativos de matrices unipotentes de tamaños menores que n respectivamente . Por hipótesis de in ducción podemos triangular simultáneamente S_L , y simultánea mente S_K , y así todos los elementos de S se habrán triangulado simultáneamente .

Caso II) El campo de escalares F arbitrario .
Tomemos la cerradura algebráica de F y triangulemos los elementos de S simultáneamente , como matrices en la extensión de F . Entonces cualquier producto de n matrices de la forma $(T-I)$, donde $T \in S$ e I es la matriz identidad , tiene que ser 0 ($(T-I)$ tiene ceros en la diagonal y T es de tamaño n) . Sea r el mínimo natural tal que cualquier producto de r matrices de la forma $T-I$, $T \in S$, es 0 . Entonces $\exists\, T_1, \ldots, T_{r-1} \in S$ tales que $(T_1-I)(T_2-I)\ldots(T_{r-1}-I) \neq 0$, tomamos un vector x tal que $x(T_1-I)\cdot\ldots\cdot(T_{r-1}-I) = y \neq 0$, entonces , dada la selección de r , $y(T-I) = 0 \quad \forall T \in S$, es decir $yT = y \quad \forall T \in S$. Esto prueba que S es reducible . Terminamos la prueba repitiendo el argumento inductivo del caso I) .

Introducimos ahora el ideal de aumentación $N = \left\{ \sum \lambda_i g_i \in A \ : \sum \lambda_i = 0 \right\}$, donde A es el álgebra del grupo G sobre el campo F .

<u>Teorema 27</u> .
Si G es un p-grupo finito y $car(F) = p$, entonces N es nilpotente .

Prueba :

Fijamos una base para A (A vista como espacio vectorial sobre F) . Consideramos $\varphi : A \longrightarrow End_F A$, $a \overset{\varphi}{\longmapsto} R_a$ tal que $a'R_a = a'a$ $\forall a' \in A$, observamos que φ es mono , pues si $R_a = 0 \in End_F A$, entonces $0 = 1eR_a = 1e \cdot a = a$ y φ es un morfismo de álgebras . Como G es un p-grupo , $\forall g \in G$, $\exists k \in \mathbb{N}$ tal que $R_g^{p^k} = Id_A$ . .'. Las raíces características de R_g son raíces p^k-ésimas de 1 . Como $car(F) = p$, $x^{p^k} - 1 = (x-1)^{p^k}$, así que todas las raíces p^k-ésimas de 1 son iguales a 1 . Aplicando el Teorema de Kolchin concluímos que las matrices R_g , $g \in G$ se pueden triangular simultáneamente y así los elementos de la diagonal de una matriz R_g son todos de la forma $\sum \lambda_i = 0$, $\forall g \in G$, .'. $\{R_g : g \in G\}$ es nilpotente y como φ es mono , N es nilpotente .

<u>Corolario</u> .

Si G es un p-grupo localmente finito y $car(F) = p$ entonces N es un nilideal .

Prueba :

Sea $x = \sum \lambda_i g_i \in N$. Por demostrar : x es nilpotente . Consideremos el subgrupo finito de G generado por las g_i's para las cuales $\lambda_i \neq 0$ (G es localmente finito) . Aplicando el Teorema 27 , tenemos que x es nilpotente .

Teorema C . (O. Schmidt) .

Si $1 \longrightarrow H \longrightarrow G \xrightarrow{\pi} G/H \longrightarrow 1$ es una sucesión exacta de grupos (H normal en G) entonces :

H , G/H localmente finitos $\Longrightarrow$ G es localmente finito .

Prueba :

Sean $a_1 , \ldots , a_r$ elementos de G . Consideramos $a_1' = \pi(a_1) , \ldots , a_r' = \pi(a_r)$, que generan un subgrupo finito de G/H (G/H es localmente finito) con elementos $\pi(a_1) = a_1' , \ldots , \pi(a_r) = a_r' , a_{r+1}' , \ldots , a_n'$. Tomamos $a_{r+1} \in \pi^{-1}(a_{r+1}') , \ldots , a_{n+1} \in \pi^{-1}(a_n')$; para cada $\underset{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}{(i,j)}$,

$\pi(a_i a_j) = a_k' = \pi(a_k)$ por lo que $a_i a_j = h_{ij} a_k$ para alguna $k \in \{1, \ldots , n\}$ y alguna $h_{ij} \in H$.

Los elementos h_{ij} generan un subgrupo finito T de H (H es localmente finito) . Y así , cualquier producto finito de a_i's con $1 \leq j \leq r$ es de la forma ha_k con $h \in T$ y $k \in \{1, \ldots , n\}$ y hay a lo más $o(T)n$ elementos de esta forma $\therefore$ $o\langle a_1 , \ldots , a_r \rangle \leq o(T)n$.

Teorema Ch .

Un grupo de torsión soluble es localmente finito .

Prueba :

Sea $G = G_0 \supset G_1 \supset \ldots \supset G_n = 1$, con G_{i+1} normal en G_i y G_i/G_{i+1} abeliano . Consideramos $1 \longrightarrow G_n \hookrightarrow G_{n-1} \longrightarrow G_{n-1}/G_n \longrightarrow 1$

exacta, como G_{n-1}/G_n es localmente finito por ser abeliano y de torsión, entonces por el Teorema C, G_{n-1} es localmente finito. Consideramos ahora la sucesión exacta $1 \longrightarrow G_{n-1} \longrightarrow G_{n-2} \longrightarrow G_{n-2}/G_{n-1} \longrightarrow 1$, de nuevo, G_{n-2}/G_{n-1} es localmente finito por ser abeliano y de torsión; como ya vimos que G_{n-1} es localmente finito, por el Teorema C, G_{n-2} es localmente finito. Iterando: $G_{n-2}, G_{n-3}, \ldots, G_0 = G$ son localmente finitos.

Definición.

El A-módulo derecho M es semisimple (abreviadamente s. s.) si y sólo si M es suma directa de A-módulos derechos irreducibles.

Lema.

Si $M = N + \sum_S M_\alpha$ con M_α módulo irreducible $\forall \alpha \in S$, entonces $\exists R \in 2^S$ tal que $M = N \oplus \bigoplus_R M_\alpha$.

Prueba:

Haremos uso del lema de Zorn. Sea $\mathcal{A} = \{B \in 2^S : N + \sum_B M_\alpha$ es suma directa$\}$. Ordenamos $\mathcal{A}$ por inclusión. Como $\emptyset \in \mathcal{A}$, $\mathcal{A} \neq \emptyset$. Sea T una cadena en $\mathcal{A}$, afirmamos que $\bigcup T \in \mathcal{A}$; pues en otro caso existe $\{\alpha_1, \ldots \alpha_p\} \subset \bigcup T \ni 0 \neq n + m_{\alpha_1} + \ldots m_{\alpha_p}$ con $m_{\alpha_i} \neq 0$ $i \in \{1, \ldots, p\}$. Como T es una cadena, $\exists B_0 \in T$ tal que $\{\alpha_1, \ldots, \alpha_p\} \subset B_0$, y así:

$0 \neq n + m_{\alpha_1} + \ldots + m_{\alpha_p} \in N \oplus \bigoplus_{B_0} M_\alpha$ ∇ $\therefore \bigcup T \in \mathcal{A}$ y es cota superior para T. El lema de Zorn nos dice entonces que $\mathcal{A}$ tiene algún elemento máximo . Sea R máximo , $R \in \mathcal{A}$. Afirmamos que $N \oplus \bigoplus_R M_\alpha = M$. En caso contrario , $\exists q \in S \setminus R$, M_q $N \oplus \bigoplus_R M_\alpha$, por lo que $M_q \cap (N \oplus \bigoplus_R M_\alpha) \subsetneq M_q$, entonces como M_q es irreducible $(q \in S)$, $M_q \cap (N \oplus \bigoplus_R M_\alpha) = 0$, lo que prueba que $N \oplus \bigoplus_{R \cup \{q\}} M_\alpha$ es suma directa , y así : $R \subsetneq R \cup \{q\} \in \mathcal{A}$ (pues $q \notin R$, y por definición de $\mathcal{A}$) , contradiciendo la selección de R .

$\therefore N \oplus \bigoplus_R M_\alpha = M$ con $R \in 2^S$.

<u>Teorema 28</u> .

Sea A un anillo , y supongamos que A es la suma de sus ideales derechos mínimos . Si A no contiene ningún anulador distinto de (0) , entonces para cualquier A-módulo derecho M , tal que $MA = M$, M es s.s.

Prueba :

Si I es ideal derecho mínimo de A , y $x \in M$, consideremos el epimorfismo de A-módulos $\varphi : I \twoheadrightarrow xI$, $i \overset{\varphi}{\mapsto} xi$. Como I es mínimo , $\operatorname{Ker}\varphi = (0)$ o $\operatorname{Ker}\varphi = I$; si $\operatorname{Ker}\varphi = I$ entonces $xI = (0)$, si $\operatorname{Ker}\varphi = (0)$ entonces $I \overset{\varphi}{\cong} xI$ que es por lo tanto submódulo irreducible de M (I no es trivial , e.d. $IA \neq (0)$, pues por hipótesis A no contiene anuladores izquierdos $\neq (0)$) . Ahora , como $MA = M$, entonces $\sum_{x \in M} xI = MA = M$. Como en la suma anterior tenemos que $M = \sum_S M_\alpha$ con M_α irreducible $\forall \alpha \in S$. Aplicando el lema anterior , tenemos que M es s.s.

<u>Definición</u> .

Sea A un álgebra con 1 , de dimensión finita , sobre el campo F , sea V un espacio vectorial de dimensión finita sobre F . Una representación de A en V es un homomorfismo de álgebras $\varphi: A \longrightarrow End_F\ V$ tal que $\varphi(1) = Id \in End_F\ V$.

Nota :

Una representación de A en V , hace a V un A-módulo derecho (con la multiplicación $v \cdot a = (v)\varphi(a)$) . Cualquier submódulo S de V es automáticamente un subespacio . (Si $s \in S$, $\lambda \in F$, $s \cdot \lambda = ((s)\varphi(1)) = (S)\varphi(1 \cdot \lambda) \in S$) .

Teorema 29 .

Sea G un grupo de torsión y V un espacio vectorial de dimensión finita sobre F un campo . Si $car(F) = p$ y $o(g) \nmid p$ $\forall g \in G$, entonces : cualquier representación de G en V es completamente reducible .

Prueba :

(decir que la representación $\psi: G \twoheadrightarrow W$, W subgrupo multiplicativo de $End_F\ V$, es completamente reducible es decir que $V = \bigoplus_{\alpha \in I} V_\alpha$ donde V_α es irreducible e invariante bajo $W \subset End_F\ V$, $\forall \alpha \in I$) .

Sea $\varphi: A \twoheadrightarrow W$, $W \subset End_F\ V$ una representación de G en V . Notamos que podemos suponer que φ es fiel (es decir , un monomorfismo) pue si no fuera este el caso , considerarĺamos la representación inducida de $G/\mathrm{Ker}\,\varphi$. Como G es un grupo de torsión isomorfo a un grupo de matrices , por el Teorema de Burnside tenemos que G es localmente finito . Sea A el álgebra del grupo G sobre F . Por el Teorema 26 , A es Regular . Ahora , la representación de G induce una representación de A . Sea K el núcleo de la representación inducida . Entonces A/K es Regular . Pero A/K es de dimensión finita (A/K es isomorfo a una subálgebra de $\mathrm{End}_F\, V$ que es de dimensión finita , ya que V es de dimensión finita) $\therefore$ $R(A/K) = 0$ (la Regularidad implica $R = 0$) y satisface la C.C.D. en ideales derechos . La afirmación se sigue entonces , del lema y del Teorema 28 .

El Teorema Principal de Wedderburn.

Sea A un álgebra y R su radical. El Teorema principal de Wedderburn asegura que bajo hipótesis apropiadas, $A = R \oplus S$ suma directa de espacios vectoriales (aquí necesariamente $S \cong A/R$). Esto nos da una reducción para el estudio de las álgebras a los casos: $R = (0)$, $R = A$.

En esta sección introducimos una hipótesis llamada SBI. Nos concentraremos en las implicaciones de esta hipótesis para el levantamiento de idempotentes.

Definición.

Sea A un anillo con radical R. Decimos que A es un anillo SBI si $\forall y \in A$, $\exists x \in R$ tal que:

i) $x^2 + x = y$

ii) $xz = zx$, $\forall z \in R$ tal que $yz = zy$.

Teorema 30.

Si R es nil, entonces A es SBI.

Prueba:

Sea $y \in A$, escribimos la solución formal de la ecuación cuadrática $x^2 + x - y = 0$:

$$x = \frac{-1 + \sqrt{1 + 4y}}{2}.$$

Si desarrollamos $\sqrt{1+4y}$ por el teorema del binomio tenemos : $\sqrt{1+4y} = 1^{1/2} + 1/2\cdot 1^{-1/2}\cdot 4y - 1/8\cdot 1^{-3/2}\cdot (4y)^2 + \ldots$ (*)

Por lo que $x = y - y^2 + 2y^3 - 5y^4 + \ldots$ donde expresamos x como una serie de potencis de y con coeficientes enteros . Si y es nilpotente , esta serie tiene un número finito de sumandos distintos de 0 . Y así es claro que x conmuta con cualquier z R que conmute con y .

Notas :

1. Cualquier Algebra de Banach es SBI . Ya que si $y \in R$, la serie (*) converge .

2. Cualquier anillo topológico compacto es SBI, por la misma razón que en 1.

3. El siguiente es un ejemplo de un anillo que no es SBI : Sea A el anillo de los números racionales con denominador impar. A es un anillo de ideales principales en el que 2 es el único elemento primo . Como $-2/3$ es casi-inverso de 2 : $2 - 2/3 + 2\cdot(-2/3) = 0$, 2 es casi-regular $\therefore$ (2) es un ideal radical $\therefore (2) \subset R$; ahora , como 2 es primo , (2) es máximo , por lo que $(2) = R$. Sin embargo , para $y = -2 \in (2)$, no existe x tal que $x^2 + x = -2$.

<u>Teorema 31</u>.

Sea A un anillo SBI con radical R . Sean $u , v \in A/R$ idem potenes ortogonales (es decir $uv = 0 = vu$) . Si $\exists\, e \in A$, $e^2 = e$, tal que $\Pi(e) = u$. ($\Pi : A \longrightarrow A/R$ el epimorfismo canónico) Entonces $\exists\, f \in A$ tal que $f^2 = f$, $fe = 0$ y $\Pi(f) = v$.

Prueba :

(En lo que sigue haremos uso simbólico de un 1 . Si A no lo tuviera se lo podríamos adjuntar , ver p.ej. Mc Coy , The theory of Rings) .

Sea $b \in A \ni \Pi(b) = v$. Sea $a = (1-e)b(1-e)$, entonces : $\Pi(a) = v$ y : $ea = (e - ee)b(1-e) = 0 = ae$; $z = a^2 - a \in R$ pues $\Pi(a^2 - a) = \Pi(a)^2 - \Pi(a) = v^2 - v = 0$; $ez = 0 = ze$. Consideremos $(2a - 1)^2 = 4a^2 - 4a + 1 = 4z + 1$. Ahora , $z \in R \Longrightarrow 4z \in R \Longleftrightarrow 4z$ es casi regular $\Longleftrightarrow 4z + 1$ tiene inverso , además $(4z+1)^{-1}$ conmuta con z , $\therefore (4z+1)^{-1} = (2a - 1)^{-2}$ conmuta con z . Como A es SBI y $-z(2a - 1)^{-2} \in R$, $\exists\, w \in R$ tal que $w^2 + w = -z(2a - 1)^{-2}$, además como e , a , conmutan con z , w conmuta con e y con a (hipótesis SBI) .

Sea $x = (1 - e)w$, entonces :

$$(1) \quad x^2 + x + z(2a - 1)^{-2} = (1 - e)(w^2 + w + z(a - 1)^{-2}) = (1 - e)\cdot 0 = 0 \quad \text{y}$$

$ex = xe = 0$. Sea $r = x(2a - 1)$ y $f = a + r$. Como $ra = ar$ entonces : $f^2 = a^2 + 2ar + r^2 = a^2 + 2ax(2a - 1) + x^2(2a - 1)^2$.

Notando que por (1) $x^2(2a - 1)^2 + x(2a - 1)^2 + z = 0$, vemos que : $f^2 = (a^2 - z) + 2ax(2a - 1) - x(2a - 1) = f$.

Ahora : $er = re = 0$, así que $ef = fe = 0$. Como $r \in R$, $\Pi(f) = \Pi(a + r) = \Pi(a) = v \in A/R$.

Notas :

1. Respecto al Teorema 31 , decimos que v se ha <u>levantado</u> a un idempotente $f \in A$.

2. Si A es conmutativo , los levantamientos de idempotentes son únicos : Si e_1 y e_2 se levantaron del mismo idempotente , $e_2 - e_2e_1$ es un idempotente en el radical y $\therefore$ $e_2 - e_2e_1 = 0$ (ver Teorema 21) . Pero entonces $(e_1 - e_2)^2 =$ $= e_1^2 - 2e_1e_2 + e_2^2 = e_1 - e_1e_2 + e_2 - e_1e_2 = e_1 - e_1e_2 = e_1 - e_2 \in R$ $\therefore$ $e_1 - e_2 = 0$.

3. Más aún , cuando A es conmutativo , los levantados de idempotentes ortogonales son automáticamente ortogonales : si $\pi(e_1) = u_1$, $\pi(e_2)$, donde $u_1u_2 = 0$ y $u_1^2 = u_1$, $u_2^2 = u_2$, entonces e_1e_2 es un idempotente en el radical , $\therefore$ $e_1e_2 = 0$.

<u>Corolario</u> .

Si A es un anillo SBI , y u_1 , u_2 , ... es una colección numerable de idempotentes ortogonales en A/R , entonces u_1 , u_2 , ... se pueden levantar a idempotentes ortogonales en A .

Prueba :

Tomando $e = 0$ en el Teorema 31 , podemos levantar u_1 a un idempotente $e_1 \in A$. Con $e = e_1$ en el Teorema 31 , u_2 se puede levantar a e_2 , idempotente ortogonal a e_1 . Con $e = e_1 + e_2$, u_3 se puede levantar a $e_3 \in A$ idempotente ortogonal a $e_1 + e_2$ y $\therefore$ ortogonal a e_1 y a e_2 :

$$e_3(e_1 + e_2) = e_3e_1 + e_3e_2 = 0 \quad \text{de donde} \quad 0 = e_3e_1e_2 + e_3e_2e_2 = \\ = e_3 \cdot 0 + e_3e_2 = e_3e_2$$

$\therefore$ e_3 es ortogonal a e_2 y análogamente a e_1 .

Inductivamente : si $u_1 , \dots , u_k$ se han levantado a idempotentes ortogonales $e_1 , \dots , e_k$, haciendo $e = e_1 + \dots + e_k$, u_{k+1} se puede levantar a $e_{k+1} \in A$ idempotente ortogonal a $e_1 + \dots + e_k$ (usando el Teorema 31) . Así :

$$0 = e_{k+1}(e_1 + \dots + e_k) = e_{k+1}e_1 + \dots + e_{k+1}e_k$$

$\therefore$ $0 = 0 \cdot e_1 = e_{k+1}e_1e_1 + \dots + e_{k+1}e_ke_1 = e_{k+1}e_1$ $\therefore$ e_{k+1} es ortogonal a e_1 y análogamente , a cada una de las e_i con $1 \leq i \leq k$.

Nota .

El corolario anterior no es cierto en general , si la colección de idempotentes ortogonales no es numerable . Para anillos topológicos es cierto, sin embargo .

<u>Definición</u> .

Dos idempotentes e , f en un anillo A están <u>relacionados</u> si $\exists x \in eAf$ y $\exists y \in fAe$ tales que $xy = e$ y $yx = f$.

Notamos que e , f están relacionados $\iff eA \cong fA$, isomorfismo de A-módulos derechos .

Teorema 32 .

Sea $\pi: A \twoheadrightarrow A/R$, $e, f \in A$ idempotentes tales que $\pi(e) = u$, $\pi(f) = v$ (R el radical de A) . Entonces :

u , v relacionados $\Longrightarrow$ e , f relacionados .

Prueba :

Por hipótesis , $\exists\ \bar{x} \in u(A/R)v$, $\exists\ \bar{y} \in v(A/R)u$ $\ni$ $\overline{xy} = u$, $\overline{yx} = v$.

Sean $x_o \in \pi^{-1}(\bar{x})$, $y_o \in \pi^{-1}(\bar{y})$, (podemos suponer $x_o \in eAf$ y $y_o \in fAe$, pues en otro caso , tomamos ex_of y fy_oe) .

Ahora : $\pi(x_oy_o) = \bar{x}\bar{y} = u = \pi(e)$ $\therefore$ $x_oy_o - e \in R$ $\therefore$ $x_oy_o - e$ es casi regular y $\therefore$ $\exists t \in A$ $\ni$ $x_oy_o - e + t + (x_oy_o - e)t = 0$.

Multiplicando esta ecuación por e , por la izquierda (y notando que $ex_o = x_o$ pues $x_o \in eAf$ por hipótesis) tenemos :

$ex_oy_o - e^2 + ex_oy_ot = x_oy_o - e + x_oy_ot = 0$. $\therefore$ $x_oy_o + x_oy_ot = e$.

Ahora , sea $x = x_o$ y $y = y_o(e+t)e$. Claramente $x = x_o \in eAf$ (hipótesis) y $y = y_o(e+t)e \in fAe(e+t)e \subset fAe$.

También $xy = x_oy_oe^2 + x_oy_ote = (x_oy_o + x_oy_ot)e = ee = e$ e.d. $xy = e$.

Para ver que $yx = f$, procedemos como sigue :

$yx \in fAex \subset fAeeAf \subset fAf$ e.d. $yx \in fAf$ y es idempotente :

$yxyx = y(xy)x = yex = y(ex_o) = yx_o = yx$. Además :

$\pi(yx) = \pi(y_ox_o) = \pi(y_o)\pi(x_o) = \bar{y}\bar{x} = v$, por hipótesis . Así , $f - yx \in R$, pero $f - yx$ es idempotente $\therefore$ $f - yx = 0$ $\therefore$ $f = yx$.

Teorema 33 . (Teorema principal de Wedderburn) .

Sea A una SBI álgebra sobre un campo F tal que $A/R(A)$ es de dimensión finita ; supongamos además que todo factor directo de A/R tiene a F como su anillo con división asociado . Entonces existe una subálgebra $S \subset A$ tal que $A = S \oplus R$, suma directa de espacios vectoriales .

Prueba:

Sea $A/R = A_1 \times A_2 \times \dots \times A_r$, donde A_i es un álgebra de matrices sobre F , $i \in \{1, \dots, r\}$. Denotamos n_i el tamaño de las matrices en A_i y por $\mu_{ij}^{(k)} \in A_k$ la matriz con coeficiente ij igual a 1 y todos los otros coeficientes iguales a 0 , $i , j \in \{1 , \dots , n_k\}$ $k \in \{1 , \dots , r\}$.
Notamos que $\{\mu_{ii}^{(k)} \in A_k : i \in \{1 , \dots , n_k\}\}$ es un conjunto de idempotentes , ortogonales dos a dos en A/R que se pueden levantar a idempotentes ortogonales $e_{ii}^{(k)} \in A$, $i \in \{1, \dots , n_k\}$, $\forall k \in \{1 , \dots , r\}$ (Teorema 31) .
Ahora , los elementos $\mu_{11}^{(k)}$ y $\mu_{ii}^{(k)}$ están relacionados , usando $\bar{x} = \mu_{1i}^{(k)}$ y $\bar{y} = \mu_{i1}^{(k)}$ (con la notación del Teorema 32) , $\therefore$ por el Teorema 32 , $e_{11}^{(k)}$ y $e_{ii}^{(k)}$ están relacionados mediante alguna $x = e_{1i}^{(k)}$ y $y = e_{i1}^{(k)}$ (e.d. : $e_{1i}^{(k)} e_{i1}^{(k)} = e_{11}^{(k)}$ y $e_{i1}^{(k)} e_{1i}^{(k)} = e_{ii}^{(k)}$) . Ahora , definimos $e_{ij}^{(k)} = e_{i1}^{(k)} e_{1j}^{(k)}$.
Por definición de $e_{1i}^{(k)}$ y de $e_{i1}^{(k)}$ la definición anterior es consistente para $i = j$.
Afirmamos ahora que $e_{ij}^{(k)} e_{st}^{(k)} = \delta_{js} e_{it}^{(k)}$:

Por definición : $e_{ij}^{(k)} e_{st}^{(k)} = e_{i1}^{(k)} e_{1j}^{(k)} e_{s1}^{(k)} e_{1t}^{(k)}$, ahora ,

$e_{1j}^{(k)} = e_{11}^{(k)} e_{1j}^{(k)} e_{jj}^{(k)}$, $e_{ss}^{(k)} e_{s1}^{(k)} e_{11}^{(k)} = e_{s1}^{(k)}$. $e_{ij}^{(k)} e_{st}^{(k)} = e_{i1}^{(k)} (e_{11}^{(k)} e_{1j}^{(k)} e_{jj}^{(k)})\cdot$

$\cdot(e_{ss}^{(k)} e_{s1}^{(k)} e_{11}^{(k)}) e_{1t}^{(k)} =$

$$= \begin{cases} 0 = e_{i1}^{(k)} e_{11}^{(k)} e_{1j}^{(k)} \cdot 0 e_{s1}^{(k)} e_{11}^{(k)} e_{1t}^{(k)} & \text{si } j \neq s \\ e_{i1}^{(k)} e_{1j}^{(k)} e_{s1}^{(k)} e_{1t}^{(k)} = e_{i1}^{(k)} e_{11}^{(k)} e_{1t}^{(k)} = e_{it}^{(k)} & \text{si } j = s \end{cases}$$

Es decir : $e_{ij}^{(k)} e_{st}^{(k)} = \delta_{js} e_{it}^{(k)}$, de donde vemos que los elementos $e_{ij}^{(k)} \in A_k$ $i , j \in \{1 , \ldots , n_k\}$ se comportan como matrices de $n_k \times n_k$ con 1 en el coeficiente i,j y 0 en los demás .

Sea S el subespacio de A generado por $\{ e_{ij}^{(k)} : k \in \{1,\ldots,r\}$, $i , j \in \{1,\ldots,n_k\}\}$, claramente S es una subálgebra de A , y si $\pi : A \longrightarrow A/R$ es el epimorfismo canónico , vemos que $\pi(S) = A/R$ pues :

$$(\sum^{n_1} \lambda_{ij}^{(1)} \mu_{ij}^{(1)} , \ldots , \sum^{n_r} \lambda_{ij}^{(r)} \mu_{ij}^{(r)}) = \pi(\sum \lambda_{ij}^{(k)} e_{ij}^{(k)}) \in \pi(S) .$$

Además $0 = \pi(\sum_{i,j,k} \lambda_{ij}^{(k)} e_{ij}^{(k)}) = 0 \Longrightarrow \lambda_{ij} = 0 \ \forall i , j , k$.

$\therefore \pi|_S : S \rightarrowtail\!\!\!\twoheadrightarrow A/R$ es un isomorfismo, pero la sucesión exacta de espacios vectoriales sobre F : $0 \longrightarrow R \longrightarrow A \longrightarrow A/R \longrightarrow 0$ se escinde , de donde $A \cong R \oplus A/R \cong R \oplus S$.

Bibliografía .

1) Kaplansky Irving ; Fields and Rings ; The University of Chicago Press ; 2nd. edition , 1972 .

2) Lambek Joachim ; Lectures on Rings and Modules ; Chelsea ; 2nd. edition , 1976 .

3) Mc Coy H. Neal ; The theory of Rings ; Chelsea ; 1973 .

4) Lang Serge ; Algebra lineal ; Fondo educativo interamericano ; Seguna edición , 1975 .

5) Herstein N. Israel ; Topics in Algebra ; Wiley ; 2nd. edition , 1975 .