29
2Ej

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

" SISTEMAS DE ECUACIONES LINEALES SOBRE ANILLOS CONMUTATIVOS "

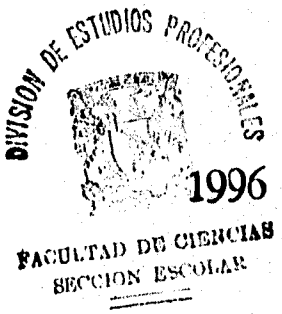
T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

MADELEINE | SANCHEZ LOPEZ



TESIS CON
FALLA DE ORIGEN

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

Comunicamos a usted que hemos revisado el trabajo de Tesis:

"Sistemas de Ecuaciones Lineales sobre Anillos Conmutativos"

realizado por Madeleine Sánchez López

con número de cuenta 7842760-4 , pasante de la carrera de Matemáticas.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Hugo Alberto Rincón Mejía
Propietario	Mat. César Alejandro Rincón Orta
Propietario	M. en C. Virginia Abrín Batule
Suplente	Mat. Alejandro [illegible] García
Suplente	Mat. Martín Cruz Cuevas

Consejo Departamental de Matemáticas

M. en C. ALEJANDRO BRAVO MOJICA

Et, peut-être, les mâts, invitant les orages
Sont-ils de ceux qu'un vent penche sur les naufrages
Perdus, sans mâts, sans mâts, ni fertiles îlots...
Mais, ô mon coeur, entends le chant des matelots! (*)

S. Mallarmé

Gracias quiero dar al divino
Laberinto de los efectos y de las causas
...
Por el álgebra, palacio de precisos cristales, ...

J.L.Borges

(*) Aunque, tal vez, los mástiles que invitan huracanes
Son aquellos que el viento doblega en los naufragios
Perdidos, sin mástiles, sin mástiles ni fértiles islotes...
¡Más, oh corazón mío, escucha la canción de los marinos!

A MIS PADRES

INDICE

	INTRODUCCION	 IV
CAPITULO I.	EL ANILLO DE POLINOMIOS	 1
CAPITULO II	IDEAS ELEMENTALES	 27
CAPITULO III	IDEALES EN $(R)_n$	 43
CAPITULO IV	EL DETERMINANTE	 52
CAPITULO V	MATRICES Y POLINOMIOS	 58
CAPITULO VI	SISTEMA DE ECUACIONES LINEALES	 67
	BIBLIOGRAFIA	 79

INTRODUCCION

El propósito de este trabajo es resumir y hacer accesible algunos de los resultados básicos de la Teoría de Matrices sobre un Anillo Conmutativo. Algunos de estos resultados son extensiones sencillas de resultados análogos para el caso en que el anillo es un Campo, otros se encuentran aún dispersos en la literatura y otros son de publicación reciente.

Se desarrollan los elementos de la Teoría de polinomios sobre Anillos Conmutativos, la cual juega un papel significativo en la Teoría de Matrices y en el Algebra Lineal, y que nos permiten resolver un ***Sistema de ecuaciones lineales sobre un Anillo Conmutativo.***

Contiene algunos ejercicios que son sencillos o de cálculo, otros que han sido seleccionados de varios artículos de investigación y otros que examinan la teoría para los casos particulares de Anillos Conmutativos.

El capítulo I reúne una serie de proposiciones sobre el Anillo de Polinomios R[x] con coeficientes en un Anillo Conmutativo R. Asimismo se dan algunas caracterizaciones de este anillo y del anillo de series de potencias formales R[[x]] demostrándose algunas de sus propiedades e incluye el Teorema de la Base de Hilbert.

En el capítulo II se define la función matriz con entradas en un Anillo Conmutativo y se analizan el Anillo de Matrices de mxn, denotado por $(R)_{m,n}$ y el

Anillo de matrices de nxn, denotado por $(R)_n$ con las operaciones suma y multiplicación. También se da una caracterización del centro de $(R)_n$ y se demuestran los siguientes isomorfismos de anillos: $(R[x])_n \cong (R)_n[x]$ y $(R)_n/(A)_n \cong (R/A)_n$ donde A es un ideal de R. Además se muestran algunas propiedades de la matriz transpuesta y de la traza de una matriz.

En el capítulo III se da una caracterización de los ideales del anillo de matrices cuadradas de orden n. $(R)_n$.

La función determinante y sus propiedades se analizan en el capítulo IV y se demuestra que el determinante de un subarreglo de una matriz es igual a la suma de productos de subarreglos. De este teorema se desprende que el det(A·B) = det(A)·det(B) donde A y B son matrices de orden n. Asimismo, en este capítulo se definen lo que son los *ideales determinantes*.

En el capítulo V se dan dos demostraciones del clásico teorema de Cayley-Hamilton y la demostración del teorema de McCoy utilizando los conceptos vistos en los capítulos anteriores.

Finalmente, en el capítulo VI se examinan las soluciones en un anillo conmutativo R para un sistema de ecuaciones lineales con coeficientes en un anillo R.

Por último, quiero hacer manifiesta mi infinita gratitud al Dr. Hugo A. Rincón Mejía por su paciente labor en la dirección de esta tesis.

I. El Anillo de Polinomios

Esta sección reúne la teoría elemental de polinomios que se necesitará a lo largo de este trabajo.

Sea R un anillo conmutativo y x una indeterminada sobre R. El anillo de polinomios $R[x]$ y el anillo de series de potencias formales $R[[x]]$ son fundamentales para el estudio de anillos conmutativos. La importancia de los polinomios está basada en el morfismo de sustitución:

Proposición: Supongamos que $\sigma: R \longrightarrow S$ es un morfismo de anillos y $\sigma(r)\lambda = \lambda\sigma(r)$ para alguna λ fija en S y para toda $r \in R$. Entonces existe un único morfismo de anillos $\sigma_\lambda: R[x] \longrightarrow S$ tal que:

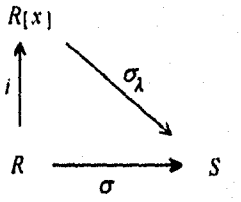
a) $\sigma_\lambda(r) = \sigma(r)$ para toda r en R

b) $\sigma_\lambda(x) = \lambda$

Precisando, $\sigma_\lambda: R[x] \longrightarrow S$ está dada por

$$\sigma_\lambda(\Sigma a_i x^i) = \Sigma \sigma(a_i)\lambda^i$$

y hace que el siguiente diagrama conmute:



Demostración:

$\sigma_\lambda \circ i(r) = \sigma_\lambda(i(r)) = \sigma_\lambda(r) = \sigma(r)$

Sean $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(r) = \sum_{j=0}^{m} b_j x^j$ en $R[x]$, entonces:

$$\sigma_\lambda(f+g) = \sigma_\lambda\left(\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j\right)$$

$$= \sigma_\lambda\left(\sum_{k=0}^{r} c_k x^k\right) \quad \text{donde } c_k = a_k + b_k,$$

$$k = 0, \ldots, r \quad \text{y} \quad r = \max\{n,m\}$$

$$= \sum_{k=0}^{r} \sigma(c_k)\lambda^k$$

$$= \sum_{k=0}^{r} \sigma(a_k + b_k)\lambda^j$$

$$= \sum_{k=0}^{r} (\sigma(a_k) + \sigma(b_k))\lambda^k$$

$$= \sum_{k=0}^{r} \sigma(a_k)\lambda^k + \sigma(b_k)\lambda^k$$

$$= \sum_{k=0}^{r} \sigma(a_k)\lambda^k + \sum_{k=0}^{r} \sigma(b_k)\lambda^k$$

$$= \sigma_\lambda\left(\sum_{k=0}^{r} a_k x^k\right) + \sigma_\lambda\left(\sum_{k=0}^{r} b_k x^k\right)$$

$$= \sigma_\lambda(f) + \sigma_\lambda(g).$$

$$\sigma_\lambda(f \cdot g) = \sigma_\lambda\left(\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right)\right)$$

$$= \sigma_\lambda\left(\sum_{k=0}^{r} c_k x^k\right) \quad \text{donde } c_k = \sum_{i=0}^{k} a_i b_{k-i} \quad \text{y } r = n + m$$

$$= \sum_{k=0}^{r} \sigma(c_k)\lambda^k$$

$$= \sum_{k=0}^{r} \sigma(\Sigma\, a_i b_{k-i})\lambda^k$$

$$= \sum_{k=0}^{t} \left(\sum_{i=0}^{k} \sigma(a_i)\sigma(b_{k-i}) \right) \lambda^k$$

$$= \sum_{i=0}^{n} \sigma(a_i)\lambda^i \sum_{j=0}^{m} \sigma(b_j)\lambda^j$$

$$= \sigma_\lambda\left(\sum_{i=0}^{m} a_i x^i \right) \sigma_\lambda\left(\sum_{j=0}^{m} b_j x^j \right)$$

$$= \sigma_\lambda(f)\sigma_\lambda(g) \quad \blacksquare$$

El morfismo de sustitución caracteriza a $R[x]$ salvo isomorfismo de anillos.

Ahora examinaremos algunos casos del morfismo de sutitución.

Primer caso. Supongamos $S = R$ y σ la función identidad. Entonces si $f(x) = \sum a_i x^i$, $\sigma_\lambda(f(x)) = \sigma_\lambda(\sum a_i x^i) = \sum \sigma(a_i)\lambda^i = \sum a_i \lambda^i = f(\lambda)$

$\sigma_\lambda(f)$ será denotado por $f(x)$.

El Kernel de σ_λ, $Ker(\sigma_\lambda)$, es un ideal en $R[x]$, llamado el ideal de relaciones satisfechas por λ. Para examinar los elementos en el ideal de relaciones de λ, recordemos que si $f(x)$ está en $R[x]$ es un polinomio mónico cuando su coeficiente principal es uno; y que si $g(x)$ está en $R[x]$ entonces, por el algoritmo de la división, existen $q(x)$ y $r(x)$ únicos en $R[x]$ con $g(x) = q(x)f(x) + r(x)$ donde $r(x) = 0$ ó grado $r(x) <$ grado $f(x)$.

Es fácil ver que el algoritmo de la división y el morfismo de sustitución están relacionados por el teorema del residuo:

$g(x) = (x - \lambda)q(x) + r(x)$ donde $r(x) = \sigma_\lambda(g) = g(\lambda)$. Esto nos lleva al siguiente teorema:

Teorema del factor: Las siguientes afirmaciones son equivalentes:

a) $g(x)$ está en el ideal de relaciones satisfechas por λ, es decir, $g(x) = 0$.

b) $g(x) = (x - \lambda)q(x)$ para algún $q(x)$ en $R[x]$, es decir, $x - \lambda$ es factor de $g(x)$.

Demostración:

Por el algoritmo de la división, existen $q(x)$ y $r(x)$ en $R[x]$, únicos tales que $g(x) = (x - \lambda)q(x) + r(x)$ donde grado $r(x) < 1$, ó $r(x) = 0$, por lo que $r(x)$ es una constante.

Como $g(\lambda) = 0$ entonces $r(x) = 0$

Por otro lado, $g(\lambda) = (\lambda - \lambda) = 0$. ■

Segundo caso. Sea σ: $R \longrightarrow T$ un morfismo de anillos. sea $S = T[x]$ y sea $\lambda = x$. Entonces $\sigma_x(\sum a_i x^i) = \sum \sigma(a_i)x^i$

Proposición: Si A= $Ker(\sigma)$ entonces $Ker(\sigma_x) = A[x] = \{\sum a_i x^i / a_i \in A\}$

Demostración:

Supongamos que $A = Ker(\sigma)$.

Sea $f(x) = \sum a_i x^i \in Ker(\sigma_x)$.

$0 = \sigma_x(f) = \sigma_x(\sum a_i x^i) = \sum \sigma(a_i)x^i$ por lo que $\sigma(a_i) = 0$ para toda i, asi $a_i \in A$ para toda i, por lo tanto:

$$\sum a_i x^i = f(x) \in A[x].$$

Sea $f(x) = \sum a_i x^i \in A[x]$

$\sigma_x(\sum a_i x^i) = \sum \sigma(a_i)x^i = 0$, por lo que $\sum a_i x^i \in Ker(\sigma_x)$

por lo tanto, $A[x] = Ker(\sigma_x)$.

Si σ es sobreyectiva entonces:

$T \cong R\ Ker(\sigma) = R/A$, ($1^{er}$ Teorema de isomorfismo)

σ_x es sobreyectiva por lo que:

$T[x] \cong R[x]\ Ker(\sigma_x) = R[x]/A[x]$

por lo tanto $R[x]/A[x] \cong (R/A)[x]$ ■

Proposición: σ es inyectiva (sobreyectiva) si y sólo si σ_x es inyectiva (sobreyectiva).

Demostración:

σ es inyectiva si y sólo si $Ker\sigma = A = 0$ por lo que $A[x] = Ker\sigma_x = 0$ si y solo si σ_x es inyectiva.

Ahora supongamos que σ es sobreyectiva

Sea $g(x) = \Sigma b_i x^i \in T[x]$ con $b_i \in T$.

Como $T = Im\sigma$, existe $a_i \in R$ tal que $\sigma(a_i) = b_i$ por lo que $g(x) = \Sigma b_i x^i =$

$= \Sigma\sigma(a_i)x^i = \sigma_x(\Sigma a_i x^i)$ por lo tanto σ_x es sobreyectiva.

Supongamos que σ_x es sobreyectiva.

Sea $b \in T \subseteq T[x]$, como σ_x es sobreyectiva, existe $f(x) = \Sigma a_i x^i \in R[x]$ tal que $\sigma_x(f) = \sigma_x(\Sigma a_i x^i) = \Sigma\sigma(a_i)x^i = b$, por lo que $\sigma(a_0) = b$, es decir, σ es sobreyectiva. ■

Proposición: R es un dominio entero si y sólo si $R[x]$ es un dominio entero.

Demostración:

Sean $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{j=0}^{m} b_j x^j$ en $R[x]$, donde $a_n \neq b_m$. Entonces:

$f(x)\, g(x) = \sum_{k=0}^{n+m} c_k x^k$, donde $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ y el coeficiente de x^{n+m} es $a_n b_m$ que es distinto de cero ya que R es un dominio entero.

Por lo tanto si $f(x)$ y $g(x)$ son distintos de cero, $f(x)g(x)$ es distinto de cero. Esto implica que $R[x]$ es un dominio entero. ■

Proposición: A es un ideal primo si y solo si R/A es un dominio entero.

Demostración:

Sean $r_1+A,\ r_2+A \in R/A,\ r_1, r_2 \in R$.

$(r_1 + A)(r_2 + A) = r_1 r_2 + A = A$, por lo que $r_1 r_2 \in A$.

Como A es un ideal primo, $r_1 \in A$ ó $r_2 \in A$, lo que implica que $r_1 + A = A$ ó $r_2 + A = A$.

Recíprocamente, supongamos que R/A es un dominio entero.

Sea $r_1 r_2 \in A$, entonces $r_1 r_2 + A = A$ y $r_1 r_2 + A = (r_1 + A)(r_2 + A)$ por lo que $r_1 + A = A$ ó $r_2 + A = A$ por lo tanto, $r_1 \in A$ ó $r_2 \in A$. ■

Proposición: A es un ideal primo si y solo si $A[x]$ es un ideal primo en $R[x]$.

Demostración: Si A es un ideal primo, entonces R/A es un dominio entero por lo que $(R/A)[x]$ es también un dominio entero y $(R/A)[x] \cong R[x]/A[x]$ por lo tanto $A[x]$ es un ideal primo en $R[x]$.

Analogamente se cumple el reciproco. ■

Proposición: Sea σ: $R \longrightarrow S$ un morfismo de anillos conmutativos. Entonces σ induce un morfismo de anillos σ_x en los anillos de series de potencias formales,

σ_x: $R[[x]] \longrightarrow S[[x]]$ dado por:

$$\sigma_x\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} \sigma(a_i)x^i$$

Demostración:

Sean $f(x) = \sum_{i=0}^{\infty} a_i x^i$ y $g(x) = \sum_{j=0}^{\infty} b_i x^j$ en $R[[x]]$.

$$\sigma_x(f+g) = \sigma_x\left(\sum_{i=0}^{\infty} a_i x^i + \sum_{j=0}^{\infty} b_j x^j\right)$$

$$= \sigma_x\left(\sum_{k=0}^{\infty} c_k x^k\right) \qquad \text{donde } c_k = a_k + b_k \qquad k = 0, 1, 2, \ldots$$

$$= \sum_{k=0}^{\infty} \sigma(c_k)x^k$$

$$= \sum_{k=0}^{\infty} (\sigma(a_k) + \sigma(b_k))x^i$$

$$= \sum_{k=0}^{\infty} \sigma((a_k)x^k + \sigma(b_k)x^k)$$

$$= \sum_{k=0}^{\infty} \sigma(a_k)x^k + \sum_{k=0}^{\infty} \sigma(b_k)x^k$$

$$= \sigma_x\left(\sum_{i=0}^{\infty} a_i x^i\right) + \sigma_x\left(\sum_{j=0}^{\infty} b_j x^j\right) \qquad = \sigma_x(f) + \sigma_x(g)$$

$$\sigma_x(f \circ g) = \sigma_x\left(\sum_{i=0}^{\infty} a_i x^i \sum_{j=0}^{\infty} b_j x^j\right)$$

$$= \sigma_x\left(\sum_{k=0}^{\infty} c_k x^k\right) \qquad \text{donde } c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

$$= \sum_{k=0}^{\infty} \sigma(c_k) x^k$$

$$= \sum_{k=0}^{\infty} \sigma_x\left(\sum_{i=0}^{\infty} a_i b_{k-i}\right) x^k$$

$$= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{\infty} \sigma(a_i)\sigma(b_{k-i})\right) x^k$$

$$= \sum_{i=0}^{\infty} \sigma(a_i) x^i \sum_{j=0}^{\infty} \sigma(b_j) x^j$$

$$= \sigma_x\left(\sum_{i=0}^{\infty} a_i x^i\right) \sigma_x\left(\sum_{j=0}^{\infty} b_j x^j\right) = \sigma_x(f)\,\sigma_x(g). \quad \blacksquare$$

Proposición: Sea $g = b_0 + b_1 x + \ldots + b_n x^n - \ldots$ en $R[[x]]$. g es una unidad en $R[[x]]$ si y sólo si b_0 es una unidad en R.

Demostración:

Como g es una unidad, existe $g'(x) = \sum_{k=0}^{\infty} b'_k x^k$ en $R[[x]]$ tal que $g(x)g'(x) = 1$ por lo tanto $b_0 b'_0 = 1$. Así, b_0 es una unidad en R.

Para el recíproco se procede inductivamente para definir los coeficientes de una serie de potencias $g'(x) = \sum_{k=0}^{\infty} b'_k x^k$ en $R[[x]]$ que será el inverso de $g(x)$.

Como b_0 es una unidad tomamos $b'_0 = b_0^{-1}$ y suponemos que los coeficientes $b'_1, b'_2, \ldots, b'_{k-1}$ han sido definidos previamente.

Sea $b'_k = -b_0^{-1}(b_1 b'_{k-1} + b_2 b'_{k-2} + \ldots + b_k b'_0)$

Entonces $g(x)\,g'(x) = \sum_{k=0}^{\infty} c_k x^k$ donde $c_k = \sum_{i=0}^{\infty} b_i b'_{k-i}$

Así, $b_0 b'_0 = 1$, mientras que para $k \geq 1$

$$c_k = b_0 b'_k + b_1 b'_{k-1} + b_2 b'_{k-2} + \ldots + b_k b'_0$$

$$= b_0(-b_0^{-1}(b_1 b'_{k-1} + b_2 b'_{k-2} + \ldots + b_k b'_0)) + b_1 b'_{k-1} + b_2 b'_{k-2} + \ldots + b_k b'_0$$

$$= -(b_1 b'_{k-1} + b_2 b'_{k-2} + \ldots + b_k b'_0) + b_1 b'_{k-1} + b_2 b'_{k-2} + \ldots + b_k b'_0$$

$$= 0$$

Por lo que se tiene $\left(\sum_{k=0}^{n} b_k x^k\right)\left(\sum_{k=0}^{n} b'_k x^k\right) = 1$, y así g tiene inverso en $R[[x]]$. ■

Proposición: La suma de una unidad más un elemento nilpotente es una unidad.

Demostración:

Sea u una unidad de R y n un elemento nilpotente de R, entonces existe $k \geq 0$ tal que $n^k = 0$. Ahora construiremos el inverso de $u + n$.

$$(u+n)(u^{-1} - nu^{-2} + n^2u^{-3} - n^3u^{-4} - \ldots - (-1)^{k-2}n^{k-2}u^{-(k-1)} + (-1)^{k-1}n^{k-1}u^{-k})$$

$$= u^{-1}u - nu^{-2}u - n^2u^{-3}u - n^3u^{-4}u + \ldots + (-1)^{k-2}n^{k-2}u^{-(k-1)}u + (-1)^{k-1}n^{k-1}u^{-k}u$$

$$+ nu^{-1} - nnu^{-2} - nn^2u^{-3} - nn^3u^{-4} + \ldots + (-1)^{k-2}nn^{k-2}u^{-(k-1)} + (-1)^{k-1}nn^{k-1}u^{-k}$$

$$= 1 - nu^{-1} + n^2u^{-2} - n^3u^{-3} + \ldots + (-1)^{k-2}n^{k-2}u^{-(k-2)} + (-1)^{k-1}n^{k-1}u^{-(k-1)}$$

$$+ nu^{-1} - n^2u^{-2} + n^3u^{-3} + \ldots + (-1)^{k-2}n^{k-1}u^{-(k-1)} + (-1)^{k-1}n^k u^{-k} = 1$$

Por lo tanto $u+n$ es una unidad en R. ■

Proposición: $f(x) = \sum_{i=0}^{n} a_i x^i$ es una unidad en $R[x]$ si y sólo si a_0 es una unidad en R y $a_1, a_2, \ldots, a_n$ son nilpotentes.

Demostración:

Supongamos que $f(x) = \sum a_i x^i$ es una unidad en $R[x]$. Entonces existe $g(x) = \sum b_j x^j$ en $R[x]$ tal que $f(x)g(x) = 1$, por lo que $a_0 b_0 = 1$ y así a_0 es una unidad en R.

Sea P un ideal primo de R, entonces $P[x]$ es un ideal primo en $R[x]$ y además $R[x]/P[x] \cong (R/P)[x]$.

Por lo que la imagen homomorfa de $f(x)$ en $(R/P)[x]$, $(a_0+P) + (a_1+P)x + \ldots + (a_n+P)x^n$ debe ser una unidad en $(R/P)[x]$.

Como R/P es un dominio entero, las únicas unidades de $(R/P)[x]$ son las unidades de R/P, es decir, los polinomios constantes diferentes de cero, lo que implica que $a_1+P = a_2+P = \ldots = a_n+P = P$.

Por lo tanto, $a_1, a_2, \ldots, a_n \in P$.

Como esta afirmación se cumple para todo ideal primo de R, se sigue que $a_1, a_2, \ldots, a_n \in radR$, por lo que $a_1, a_2, \ldots, a_n$ son nilpotentes.

Si a_0 es una unidad en R y los demás coenficientes $a_1, a_2, \ldots, a_n$ son nilpotentes, entonces el polinomio $f(x) = a_0 + a_1 x + a_2x^2 + \ldots + a_nx^n$ es la suma de una unidad más un elemento nilpotente por lo que $f(x)$ es una unidad en $R[x]$. ■

Definición: Sea R un anillo conmutativo. El radical primo de R, $radR$, es la intersección de todos los ideales primos de R.

Definición: Sea R un anillo conmutativo. El nil-radical de R es el conjunto que consiste de todos los elementos nilpotentes de R.

Proposición: R un anillo conmutativo. El radical primo de R coincide con el nil-radical de R.

Demostración:

Sea P un ideal primo de R y sea a un elemento del nil-radical de R, entonces existe $n > 0$ tal que $a^n = 0 \in P$. Como P es un ideal primo, $aa^{n-1} \in P$, se tiene que $a \in P$. Por lo tanto $a \in radR$.

Recíprocamente, sea $a \in radR$

Supongamos que a no es nilpotente.

Sea $\Sigma = \{I \leq R \mid n > 0 \Rightarrow a^n \notin I\}$ y Σ está ordenado por la inclusión.

Por el lema de Zorn, Σ tiene un elemento máximo. Sea P el elemento máximo de Σ. Ahora se mostrará que P es un ideal primo que no contiene a a, lo que contradice el hecho de que $a \in radR$.

Sea $xy \in P$.

Supongamos que $x \notin P$ y $y \notin P$, entonces los ideales $P+Rx$ y $P+Ry$ contienen estrictamente a P y además no pertenecen a Σ. Por lo tanto $a^m \in P+Rx$ y $a^n \in P+Ry$ para ciertas m y n. Esto implica que a^{m+n} está en $P+Rxy \subset P$ por lo que $a^{m+n} \in P$ lo cual es imposible, por lo tanto P es un ideal primo tal que $a \notin P$.

Así, a está en el nil-radical de R. ■

Proposición: $f(x) = \Sigma a_i x^i$ es un divisor de cero en $R[x]$ si y solo si existe $r \neq 0$ en R con $rf = 0$.

Demostración:

El proceso de la demostración se ilustrará con un ejemplo.

En particular, si el coeficiente de alguna potencia de x en $f(x)$ no es un divisor de cero en R, $f(x)$ no es un divisor de cero en $R[x]$.

Supongamos que $f(x)$ tiene grado positivo. Sean $f(x) = a_0+a_1x^1+a_2x^2+a_3x^3$ donde $a_3 \neq 0$, y $g(x) = b_0+b_1x^1+b_2x^2$ donde $b_2 \neq 0$, tal que $g(x)f(x) = 0$. Mostraremos que existe un polinomio $g'(x) \neq 0$ tal que grado $g'(x) <$ grado $g(x)$ y que además $g'(x)f(x) = 0$.

Como $0 = g(x)f(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 +$

$$+ (a_1b_2 + a_2b_1 + a_3b_0)x^3 + (a_3b_1 + a_2b_2)x^4 + a_3b_2x^5,$$

el coeficiente de x^5 en este producto debe ser cero, es decir, debemos tener que $a_3b_2 = 0$, esto implica que $(a_3g(x))f(x) = 0$.

$a_3g(x) = a_3(b_0 + b_1x + b_2x^2) = a_3(b_0 + b_1x)$, por lo que grado $(a_3g(x)) < 2$ ó $a_3g(x) = 0$.

Si $a_3g(x) \neq 0$ entonces definimos $g'(x) = a_3g(x)$.

Si $a_3g(x) = 0$ entonces $a_3b_0 = a_3b_1 = a_3b_2 = 0$, esto quiere decir que:

$g(x)f(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 +$

$$+ (a_1 b_2 + a_2 b_1)x^3 + a_2 b_2 x^4$$

$$= (b_0 + b_1 x + b_2 x^2)(a_0 + a_1 x + a_2 x^2) = 0,$$

por lo que $a_2 b_2 = 0$, esto implica que $(a_2 g(x))f(x) = 0$

$a_2 g(x) = a_2(b_0 + b_1 x + b_2 x^2) = a_2(b_0 + b_1 x)$ por lo que grado $(a_2 g(x)) < 2$ ó $a_2 g(x) = 0$.

Si $a_2 g(x) \neq 0$ entonces definimos $g'(x) = a_2 g(x)$.

Si $a_2 g(x) = 0$, entonces $a_2 b_0 = a_2 b_1 = a_2 b_2 = 0$, esto quiere decir que:

$g(x)f(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1)x^2 + a_1 b_2 x^3$

$= (b_0 + b_1 x + b_2 x^2)(a_0 + a_1 x) = 0$, por lo que $a_1 b_2 = 0$.

Esto implica que $(a_1 g(x))f(x) = 0$.

$a_1 g(x) = a_1(b_0 + b_1 x + b_2 x^2) = a_1(b_0 + b_1 x)$ por lo que grado $(a_1 g(x)) < 2$ ó $a_1 g(x) = 0$.

Si $a_1 g(x) \neq 0$, entonces definimos $g'(x) = a_1 g(x)$

Si $a_1 g(x) = 0$, entonces $a_1 b_0 = a_1 b_1 = a_1 b_2 = 0$, esto quiere decir que: $g(x)f(x) = a_0 b_0 + a_0 b_1 x + a_0 b_2 x^2 = (b_0 + b_1 x + b_2 x^2)a_0 = 0$, por lo que $g(x)f(x) = a_0 g(x) = 0$.

Si tenemos que $a_3 g(x) \neq 0$, $a_2 g(x) \neq 0$, $a_1 g(x) \neq 0$, $a_0 g(x) \neq 0$, entonces hemos encontrado un $g'(x)$ con las características que queríamos.

Si $a_3 g(x) = a_2 g(x) = a_1 g(x) = a_0 g(x) = 0$, se sigue que $a_3 b_2 = a_2 b_2 = a_1 b_2 = a_0 b_2 = 0$, esto es, $b_2 f(x) = 0$ y b_2 es distinto de cero y de grado cero.

Por lo tanto, en todos los casos existe un $g'(x)$ de grado menor que $g(x)$ tal que $g'(x)f(x) = 0$.

Si $g'(x)$ es de grado 1, repitiendo el argumento por el cual pasamos de $g(x)$ a $g'(x)$, mostraremos que existe un elemento diferente de cero, r en R tal que $rf(x) = 0$. ■

Proposición: $f(x) = \sum_{i=0}^{n} a_i x^i$ es nilpotente en $R[x]$ si y sólo si $a_0, a_1, a_2, \ldots, a_n$ son nilpotentes.

Demostración:

Sea P un ideal primo de R, entonces $P[x]$ es un ideal primo de $R[x]$. Como $f(x)$ es nilpotente, $f(x) \in P[x]$ y por lo tanto $a_i \in P$ para $i \geq 0$, a_i es nilpotente.

Recíprocamente, suma de nilpotentes es nilpotente. ■

Proposición: Si $g(x) = \sum_{i=0}^{\infty} b_i x^i$ es nilpotente en $R[[x]]$, entonces b_i es nilpotente para cada i, (el recíproco se cumple si R es noetheriano).

Demostración:

Sea P un ideal primo en R entonces $P[[x]]$ es un ideal primo en $R[[x]]$. Como $g(x)$ es nilpotente, $g(x) \in P[[x]]$ y por lo tanto $b_i \in P$ para $i \geq 0$. Como P es arbitrario, b_i es nilpotente. ■

Si S es un anillo conmutativo, denotamos por S^* el grupo de unidades de S.

Sea $\sigma_0: R[x] \longrightarrow R$ (Respectivamente $R[[x]] \longrightarrow R$) el morfismo "término constante", es decir, sustituir x por 0. Entonces σ_0 induce un morfismo sobreyectivo de grupos.

$\sigma_{0*}: R[x]^* \longrightarrow R^*$ (respectivamente $R[[x]]^* \longrightarrow R^*$).

Proposición: Sea $U_1 = ker\,\sigma_0$, $\sigma_0: R[x]^* \longrightarrow R^*$. $f(x) \in U_1$, es decir, $\sigma_0(f(x)) = f(0) = 1$, si y sólo si $f(x) = 1 + a_1 x + \ldots + a_n x^n$ donde $a_1, \ldots, a_n$ son nilpotentes. Sea $N = radR$. Entonces $rad(R[x]) = N[x]$ y $f(x) \in U_1$ si y sólo si $f(x) \in 1 + xN[x]$. Por lo tanto $U_1 = 1 + xN[x]$ y tenemos una sucesión exacta

$$1 \longrightarrow 1 + xN[x] \longrightarrow R[x]^* \longrightarrow R^* \longrightarrow 1$$

que se escinde bajo la inclusión natural $R^* \longrightarrow R[x]^*$ y por lo tanto, $R[x]^* \cong R^*[1+xN[x]]$.

Demostración:

Si $f(x) \in U_1$ entonces $\sigma_0(f(x)) = f(0) = 1$, lo que significa que el término constante es 1, por lo tanto $f(x) = 1 + a_1 x + \ldots + a_n x^n \in R[x]^*$, es decir, $f(x)$ es una unidad en $R[x]$ por lo que $a_1, \ldots, a_n$ son nilpotentes.

Si $f(x) = 1 + a_1 x + \ldots + a_n x^n$ entonces $\sigma_0(f(x)) = 1$ por lo que $f(x) \in U_1$.

Si $f(x) \in U_1$, entonces $a_1, \ldots, a_n$ son nilpotentes por lo que $a_1, \ldots, a_n \in N$, esto implica que $f(x)$ es de la forma $f(x) = 1 + \sum_{i=1}^{n} a_i x^i = 1 + x \sum_{n=0}^{n-1} a_i x^i$ en $1+xN[x]$.

Reciprocamente, si $f(x) \in 1 + xN[x]$, esto significa que $f(x) = 1+xq(x)$ donde $q(x) \in N[x]$ y $\sigma_0(f(x)) = \sigma_0(1) + \sigma_0(x)\sigma_0(q(x)) = 1$, por lo tanto, $f(x) \in U_1$, así $ker\ \sigma_0 = U_1 = 1+xN[x]$.

Para mostrar que $rad(R[x]) = N[x]$, sea $q(x) = \sum_{i=0}^{n} a_i x^i \in rad(R[x])$.

Entonces $q(x)$ es nilpotente si y sólo si $a_0, a_1, \ldots, a_n$ son nilpotentes si y sólo si $a_0, a_1, \ldots, a_n \in N$ si y sólo si $q(x) \in N[x]$.

La sucesión $1 \longrightarrow 1 + xN[x] \hookrightarrow R[x]^* \underset{i}{\overset{\sigma_0}{\rightleftarrows}} R^* \longrightarrow 1$

es exacta y se escinde bajo la inclusión natural i ya que $\sigma_0 i(r) = \sigma_0(r) = r$.

Por lo tanto, $R[x]^* \cong R^*(1 + xN[x])$. ■

Proposición: Sea $\bar{U}_1 = ker\sigma_0$, $\sigma_0 : R[[x]]^* \longrightarrow R^*$. Si $g(x) = \sum_{i=0}^{\infty} b_i x^i$ está en $R[[x]]$, entonces $1 + xg(x)$ es invertible.

Demostración:

Sea $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n + \ldots \in R[[x]]$, entonces:

$$1 + xg(x) = 1 + b_0x + b_1x^2 + b_2x^3 + \ldots + b_nx^{n+1} + \ldots$$

Como 1 es una unidad en $R[[x]]$, por lo tanto $1 + xg(x)$ es invertible.

Por lo tanto, $\bar{U}_1 = 1 + xR[[x]] = 1 + (x)$ y la sucesión

$1 \longrightarrow 1 + (x) \longrightarrow R[[x]]^* \underset{i}{\overset{\sigma_0}{\rightleftarrows}} R^* \longrightarrow 1$ es exacta y se escinde bajo la inclusión $i: R \longrightarrow R[[x]]$.

Por lo tanto, $R[[x]]^* \cong R^* x (1 + (x))$. ■

Definición: Sea R un anillo conmutativo. El radical de Jacobson de R, $Rad\ R$, es la intersección de todos los ideales máximos de R.

Definimos a N como el ideal de todos los elementos x en R tal que $1-xy$ es una unidad en R para toda y en R.

Proposición: El radical de Jacobson de R, coincide con N.

Demostración:

Sean $x \in Rad\ R$ y $y \in R$.

Supongamos que $1-xy$ no es una unidad en R, entonces $1-xy$ pertenece a algún ideal máximo M. Pero $x \in Rad\ R$ por lo que $x \in M$, así $xy \in M$ por ser M un ideal. Esto implica que $1 \in M$ lo que es imposible.

Por lo tanto $1-xy$ es una unidad en R.

Recíprocamente, sea $x \in N$.

Supongamos que existe un ideal máximo M tal que $x \notin M$. Entonces M y Rx generan al ideal unitario (1), por lo que tenemos que $m + xy = 1$ para alguna $m \in M$ y para alguna $y \in R$.

Por lo tanto, $m = 1-xy \in M$ y además no es una unidad, lo cual es falso ya que por hipótesis $x \in N$, es decir, $1-xy$ es una unidad. ∎

Proposición: $rad\ (R[x]) = Rad\ (R[x]) = (rad\ R)[x]$

Demostración:

Anteriormente se demostró que:

$rad\,(R[x]) = (rad\,R)[x]$. Falta mostrar que $rad\,(R[x]) = Rad\,(R[x])$.

Como todo ideal máximo es un ideal primo entonces $rad\,(R[x]) \subseteq Rad\,(R[x])$.

Para la otra inclusión

Sea $f(x) = a_0 + a_1x - \ldots + a_nx^n \in Rad\,(R[x])$.

Entonces $1 + f(x)x = 1 + a_0x + a_1x^2 + \ldots + a_nx^{n+1}$ es una unidad en $R[x]$, como $a_0, a_1, \ldots, a_n$ son nilpotentes en R y $f(x)$ es nilpotente en $R[x]$ para una potencia suficientemente grande.

Por lo tanto, $f(x) \in rad\,(R[x])$. ■

Definición: Se dice que R^M es noetheriano si todo submódulo de M es finitamente generado.

Proposición: Las siguientes afirmaciones son equivalentes para un anillo conmutativo R:

(1) Todo ideal de R es finitamente generable.

(2) Toda cadena ascendente de ideales $A_1 \subseteq A_2 \subseteq \ldots$ de R tiene sólo un número finito de términos distintos.

(3) Todo conjunto no vacío de ideales de R, parcialmente ordenado por la inclusión, tiene al menos un elemento máximo.

Demostración: (1) $\Rightarrow$ (2)

Sea $A_1 \subseteq A_2 \subseteq \ldots$ una cadena ascendente de ideales en R.

Sea $A = \cup A_i$ la unión de la familia $\{A_i\}$.

Como A no es un ideal de R, A es finitamente generado, es decir, $A = \langle a_1, a_2, \ldots, a_m \rangle$.

Como $a_1 \in \cup A_i$, se tiene $a_1 \in A_{i_1}$, $a_2 \in A_{i_2}$, $\ldots$, $\ldots$. Si existe $t \in N$ tal que $i_1 \leq t$, $i_2 \leq t$, $\ldots$, $i_m \leq t$, entonces $\langle a_1, a_2, \ldots, a_m \rangle \subset A_t$, con lo que $A = \langle a_1, a_2, \ldots, a_m \rangle \subset A_t$, con lo que $A = \langle a_1, a_2, \ldots, a_m \rangle \subset A_t \subset A_1$, por lo tanto $A = A_t$, lo que implica que $A_i \subset A_{i-1} \subset A \subset A_t$, para toda i.

Así, $A_t = A_{t-1}$ y la cadena $A_1 \subset A_2 \subset \ldots$ se estaciona.

(2) $\Rightarrow$ (3)

Sea C una colección de ideales de R.

Supongamos que C no tiene elemento máximo. Como C no es vacío, tomamos un ideal $I_1 \in C$. Por lo que supusimos anteriormente, I_1 no puede ser máximo en C, entonces I_1 está propiamente contenido en algún ideal $I_2 \in C$. Pero I_2 tampoco puede ser máximo, por lo que existe un ideal $I_3 \in C$ tal que $I_2 \subset I_3$. Continuando de esta manera, obtenemos una cadena ascendente infinita de ideales de R, $I_1 \subset I_2 \subset I_3 \subset \ldots$ y todas las inclusiones son propias, lo cual contradice la condición (2).

(3) $\Rightarrow$ (1)

Sea A un ideal de R.

Si $A = \{0\}$ entonces A está generado por 0.

Si $A \neq \{0\}$ entonces podemos elegir un elemento diferente de cero, $a_1 \in A$. Esto implica que $\langle a_1 \rangle = A$ y por lo tanto A es finitamente generado o $\langle a_1 \rangle \neq A$.

Si $\langle a_1 \rangle \neq A$, existe un elemento $a_2 \in A$ tal que $a_2 \notin \langle a_1 \rangle$ y con $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subseteq A$

Análogamente, si $\langle a_1, a_2 \rangle \neq A$, existe $a_3 \in A$ tal que $a_3 \notin \langle a_1, a_2 \rangle$ y $\langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle$.

Siguiendo este razonamiento, obtenemos una cadena ascendente de ideales de R $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset \ldots$

Por hipótesis, este conjunto de ideales posee un elemento máximo, digamos, el ideal $\langle a_1, a_2, \ldots, a_n \rangle$.

Si $A \neq \langle a_1, a_2, \ldots, a_n \rangle$ podríamos encontrar un elemento a en A tal que $a \notin \langle a_1, a_2, \ldots, a_n \rangle$ y $\langle a_1, a_2, \ldots, a_n \rangle$ estaría contenido propiamente en $\langle a, a_1, a_2, \ldots, a_n \rangle$, lo que es imposible. Por lo tanto, A está generada por $\langle a_1, a_2, \ldots, a_n \rangle$. ■

Proposición: R un anillo conmutativo.

Sea $O \longrightarrow A' \xrightarrow{i} A \xrightarrow{P} A'' \longrightarrow O$ una sucesión exacta corta de R-módulos. Entonces A' y A'' son noetherianos si y sólo si A es noetheriano.

Demostración:

Primero mostraremos que si A' y A'' son finitamente generados entonces A es finitamente generado.

Sean $A' = \langle a'_1, \ldots, a'_s \rangle$ y $A'' = \langle a''_1, \ldots, a''_t \rangle$. Como P es sobreyectiva, existen $a_k \in A$, $k = 1, \ldots, t$, tales que $P(a_k) = a''_k$.

Afirmamos que: $A = \langle i(a'_1), \ldots, i(a'_s), a_1, \ldots, a_t \rangle$.

En efecto, se tiene que si $a \in A$, entonces:

$$P(a) = \sum_{k=1}^{t} r_k a''_k \qquad r_k \in R, \qquad k = 1, \ldots, t$$

$$= \sum_{k=1}^{t} r_k P(a_k) = P\left(\sum_{k=1}^{t} r_k a_k \right)$$

$$P\left(a - \sum_{k=1}^{t} r_k a_k \right) = 0 .$$

Esto implica que $a - \sum_{k=1}^{t} r_k a_k \in ker P = i(A')$.

Por lo tanto, existe $x \in A'$ tal que: $i(x) = a - \sum_{k=1}^{t} r_k a_k$.

Como $x \in A'$, $x = \sum_{k=1}^{s} r'_k a'_k$, $r'_k \in R$.

Entonces $i(x) = i\left(\sum_{k=1}^{s} r'_k a'_k\right) = \sum_{k=1}^{s} r'_k i(a'_k) = a - \sum_{k=1}^{t} r_k a_k$.

Por lo tanto, $a = \sum_{k=1}^{s} r'_k i(a'_k) + \sum_{k=1}^{t} r_k a_k$.

Así, A es finitamente generado.

Sea B un submódulo de A. Entonces $A \cap B < A'$ y $P(B) < A''$ y además se tiene la siguiente sucesión exacta:

$$O \longrightarrow A \cap B \longrightarrow B \longrightarrow P(B) \longrightarrow O$$

Como A' y A'' son noetherianos, $A \cap B$ y $P(B)$ son finitamente generados y por la proposición anterior, B es finitamente generado. Por lo tanto A es noetheriano.

Recíprocamente, sea A noetheriano.

A' es isomorfo a un submódulo de A por lo que A' es noetheriano.

$A'' \cong A/A'$, entonces una cadena ascendente de submódulos de A que contienen a A' y como A es notheriano, A'' tambien lo es. ∎

Teorema de la base de Hilbert.

Si R es un anillo noetheriano entonces el anillo de polinomios $R[x]$ es noetheriano.

Demostración:

Sea I un ideal diferente de cero de $R[x]$. Para cada entero $k \geq 0$, consideramos al conjunto I_k que consiste del cero y aquellos elementos $r \in R$ que aparecen como el coeficiente principal de algún polinomio de grado k que pertenece a I.

$$I_k = \{r \in R \mid a_0 + a_1x + \ldots + rx^k \in I\} \cup \{0\}$$

I_k forma un ideal del anillo R con $I_k \subseteq I_{k+1}$ (que $I_k \subseteq I_{k+1}$ se sigue del hecho de que si $r \in I_k$, entonces r aparece como coeficiente principal de x^{k+1} cuando el correspondiente polinomio es multiplicado por x, por lo que $r \in I_{k+1}$).

Como por hipótesis se cumple la condición de cadena ascendente para R entonces existe un entero n tal que $I_k = I_n$ para toda $k \geq n$.

Además, cada ideal I_i ($i = 1, 2, \ldots, n$) es finitamente generado, es decir:

$$I_i = \langle a_{i1}, a_{i2}, \ldots, a_{im_i} \rangle \quad i = 0, 1, \ldots, n$$

donde a_{ij} es el coeficiente principal de $f_{ij}(x)$ un polinomio de grado i en I.

Ahora basta mostrar que los $m_0 + \ldots + m_n$ polinomios $f_{ij}(x)$ generan a I.

Sea $J = \langle f_{01}, \ldots, f_{0m_0}, \ldots, f_{n1}, \ldots, f_{nm_n} \rangle$.

El ideal J es finitamente generado y por la elección de los $f_{ij}(x)$, J debe estar contenido en I.

Para obtener la otra inclusión, sea $f(x) \in I$, digamos de grado r:

$$f(x) = b_0 + b_1x + \ldots + b_{r-1}x^{r-1} + bx^r$$

El argumento procede por inducción sobre r.

Si $r = 0$ entonces tenemos que $f(x) = b_0 \in I_0 \subseteq J$.

Por hipótesis de inducción suponemos que todo polinomio de grado r-1 que está en I también pertenece al ideal generado por los $f_{ij}(x)$.

Si $r > n$, entonces el coeficiente principal $b \in I_r = I_n$ y se podría expresar como $b = a_{n1}c_1 + a_{n2}c_2 + \ldots + a_{nm_n}c_{m_n}$ para alguna elección de $c_i \in R$.

Entonces el polinomio $f_1(x) = f(x) - x^{r-n}(c_1 f_{n1}(x) + c_2 f_{n2}(x) + \ldots + c_{m_n} f_{nm_n}(x))$ pertenece a I y tiene grado menor que r, ya que el coeficiente de x^r en este polinomio es $b - \sum_{i=1}^{m_n} c_i a_{ni} = 0$.

Por hipótesis de inducción, $f_1(x)$ y $f(x)$ están en el ideal J.

Si $r \leq n$, como $b \in I_r$, podemos encontrar elementos $d_1, d_2, \ldots, d_{m_r}$ en R tales que $b = a_{r1}d_1 + a_{r2}d_2 + \ldots + a_{rm_r}d_{m_r}$.

Entonces el polinomio $f_2(x) = f(x) - (d_1 f_{r1}(x) + d_2 f_{r2}(x) + \ldots + d_{m_r} f_{rm_r}(x))$ es un elemento de I con grado r-1 o menor por lo que $f_2(x)$ y $f(x)$ están en el ideal J. Por lo tanto, $I = J$. ■

Corolario: Si R es noetheriano entonces $R[x_1, \ldots, x_n]$ es noetheriano.

Demostración:

Demostración por inducción sobre n.

Si $n = 1$ entonces por el teorema anterior, $R[x_1]$ es noetheriano.

Como hipótesis de inducción, supongamos que para n-1 indeterminadas el anillo $R[x_1, \ldots, x_{n-1}]$ es noetheriano.

Como $(R[x_1, \ldots, x_{n-1}])[x_n] = R[x_1, \ldots, x_n]$ entonces el anillo de polinomios en n indeterminadas $R[x_1, \ldots, x_n]$ es noetheriano. ■

Proposición: Supongamos que R es un anillo noetheriano y $\sigma: R \longrightarrow S$ es un morfismo de anillos sobreyectivo. Entonces S es noetheriano. Por lo tanto, si A es un ideal de $R[x]$ (resp. $R[[x]]$) y R es noetheriano, entonces $R[x]/A$ (resp. $R[[x]]/A$) es noetheriano.

Demostración:

Sea I un ideal de S.

Como σ es sobreyectiva, se tiene que $R/ker\sigma \cong S$. Entonces $I \cong J/ker\sigma$ donde J es un ideal de R y $ker\sigma \subseteq J$.

Como R es noetheriano, J es finitamente generado, es decir, $J = \langle r_1, r_2, \ldots, r_n \rangle$. Por lo que $J/ker\sigma = \sigma(J) = \langle \sigma(r_1), \sigma(r_2), \ldots, \sigma(r_n) \rangle$. Así, I es finitamente generado y por lo tanto S es noetheriano.

Si R es noetheriano entonces $R[x]$ es noetheriano. Si A es un ideal de $R[x]$, se tiene la proyección natural $R[x] \xrightarrow{\pi} R[x]/A$. Por lo tanto, R/A es noetheriano.

Análogamente, si R es noetheriano entonces $R[[x]]$ es noetheriano. Si A es un ideal de $R[[x]]$, se tiene que $R[[x]]/A$. ■

Proposición: Si R es un anillo noetheriano y M es un R-módulo finitamente generado, entonces M es noetheriano.

Demostración:

Demostración por inducción sobre el número de generadores de M.

Si $M = \langle \alpha \rangle$ entonces M es isomorfo a un $R/An(\alpha)$ donde $An(\alpha)$ es el anulador de α.

Entonces se puede considerar a M como una imagen homomorfa de R como R-módulo. Como R es noetheriano entonces $R/An(M) \cong M$ es noetheriano.

Si $M = \langle a_1, a_2, \ldots, a_n, a_{n+1} \rangle$, supongamos que todo R-módulo generado por n elementos es noetheriano.

Sea $M' = \langle a_1, \ldots, a_n \rangle$. Entonces se tiene la sucesión exacta:

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{P} M/M' \longrightarrow 0$$

donde M/M' es cíclico, pues está generado por $P(a_{n+1})$. Por lo tanto, M es noetheriano. ∎

Proposición: Sea K un campo y $f(x)$ un polinomio en $K[x]$ de grado $n \geq 0$. Entonces $f(x)$ tiene a lo más n raíces en K.

Demostración:

Demostración por inducción sobre el grado de $f(x)$.

Si $gr(f(x)) = 0$ entonces el resultado es trivial, ya que $f(x)$ no puede tener raíces.

Si $gr(f(x)) = 1$, es de la forma $f(x) = ax + b$ $(a \neq 0)$, ya que si a es un elemento invertible, se tiene que $-a^{-1}b$ es la única raíz de $f(x)$.Como hipótesis de inducción, supongamos que la proposición se cumple para todos los polinomios de grado n-1.

Sea $gr(f(x)) = n$.

Si $f(x)$ tiene una raíz a, entonces $f(x) = (x-a)\,q(x)$, donde el polinomio $q(x)$ tiene grado n-1. Cualquier raíz a' distinta de a debe ser una raíz de q, ya que $0 = f(a') = (a-a')q(a')$ y como R no tienes divisores de cero, $q(a') \neq 0$. Por hipótesis de inducción, q tiene a lo mas n-1 raíces distintas. Como las únicas raíces de $f(x)$ son a y las raíces de $q(x)$. $f(x)$ no puede tener más de n raíces distintas en R. ■

II. Ideas elementales.

A lo largo de este capítulo, R denotará un anillo conmutativo con identidad 1.

Sean I y J conjuntos de índices de cardinalidad finita. Supongamos:

$$I = \{1, 2, 3, \ldots, m\}$$

$$J = \{1, 2, 3, \ldots, n\}.$$

Una matriz de $m \times n$ sobre R es una función $\sigma: I \times J \longrightarrow R$.

La función $\sigma: I \times J \longrightarrow R$ es identificada frecuentemente con su rango de valores en R, arreglados en la siguiente forma tabular:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ \vdots & & & & \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} \end{bmatrix} = [a_{ij}] \quad \text{donde } a_{ij} = \sigma(ij)$$

Se dice que el elemento a_{ij} en la tabla de valores de arriba tiene índice de renglón i e índice de columna j y se dice que ocupa la posición (i,j) ó está en la entrada (i,j) de la matriz.

Dos funciones $\sigma: I \times J \longrightarrow R$ y $\beta: I \times J \longrightarrow R$ son iguales, $\sigma = \beta$, si $\sigma(i,j) = \beta(i,j)$ para toda (i,j) en $I \times J$. Equivalentemente, si σ tiene un arreglo $[a_{ij}]$ donde $\sigma(i,j) = a_{ij}$ y β tiene un arreglo $[b_{ij}]$ donde $\beta(i,j) = b_{ij}$ entonces $[a_{ij}] = [b_{ij}]$ si $a_{ij} = b_{ij}$ para toda (i,j) en $I \times J$.

Desde ahora suprimimos la referencia al mapeo $\sigma: I \times J \longrightarrow R$ y usaremos la forma tabular para denotar matrices.

El conjunto de todas las matrices sobre R de tamaño $m \times n$ es denotado por $(R)_{m,n}$.

Si $m = n$ entonces $(R)_{m,n}$ se abrevia a $(R)_n$.

Una matriz en $(R)_{m,1}$ es llamada una columna de tamaño, dimensión o longitud m. Una matriz en $(R)_{1,n}$ es llamada un renglón de tamaño, dimensión o longitud n.

Nuestro primer propósito es dar a $(R)_{n,m}$ y $(R)_n$ operaciones algebraicas y consecuentemente, una estructura algebraica. La primera operación, la adición, es natural ya que es inducida por la adición en R y por la forma usual en que las funciones se suman.

Si $[a_{ij}]$ y $[b_{ij}]$ estan en $(R)_{m,n}$ entonces definimos la suma como:

$$[a_{ij}] + [b_{ij}] = [c_{ij}]$$

donde $c_{ij} = a_{ij} + b_{ij}$ para cada (i,j) en $I \times J$.

Claramente $(R)_{m,n}$ bajo la suma (+) es un grupo abeliano con identidad $0 = [0]$ (cero en todas las entradas), y el inverso aditivo de $[a_{ij}]$ es $-[a_{ij}] = [-a_{ij}]$.

Sea r en R. Definimos el producto escalar de r y $[a_{ij}]$ por $r[a_{ij}] = [ra_{ij}]$. Entonces $(R)_{m,n}$ bajo la suma y la multiplicación escalar es un R-módulo.

La siguiente operación es el producto de matrices. Esta no surge de manera natural de la consideración de las funciones $\sigma: I \times J \longrightarrow R$. En su lugar, ésta se deduce de la composición de funciones lineales entre módulos libres.

Sean $[a_{ij}]$ en $(R)_{m,n}$ y $[b_{jk}]$ en $(R)_{n,p}$. Definimos el producto de $[a_{ij}]$ por $[b_{jk}]$ como $[c_{ik}]$ donde $c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$.

El producto anterior es un "producto de convolución". La riqueza de la teoría de matrices y sus inherentes dificultades y misterios son resultado de este producto.

Es fácil ver que el producto induce una funcion: $(R)_{m,n} \times (R)_{n,p} \longrightarrow (R)_{m,p}$ que es bilineal, es decir,

$$A(B + C) = AB + AC$$

$$(A + B)C = AC + BC$$

$$r(AB) = (rA)B = A(rB).$$

donde A, B y C son matrices de tamaño apropiado. Además el producto es asociativo, es decir, $(AB)C = A(BC)$. En particular $(R)_n$ es una R-álgebra (no conmutativa si $n > 2$), bajo la suma, multiplicación y la multiplicación por escalares.

Históricamente, los términos "matriz" y "arreglo" fueron empleados indistintamente. El primer uso del término "matriz" ha sido atribuído a Sylvester

El álgebra $(R)_n$ tiene una identidad $I = [\delta_{ij}]$ donde $\delta_{ij} = 0$ si $i \neq j$ y $\delta_{ij} = 1$, $1 \leq i \leq n$. (δ_{ij} es llamada la delta de Kronecker).

La matriz $rI = [r\delta_{ij}]$ es llamada una matriz escalar y el conjunto de todas las matrices escalares forman un subanillo de $(R)_n$ que es isomorfo a R.

La matriz de $n \times n$ que tiene 1 en la posición (i,j) y 0 en todas las demás posiciones es llamada una matriz elemental unitaria y es denotada por E_{ij}.

Lema: Para un anillo conmutativo R, el centro de $(R)_n$, es decir, $C((R)_n) = \{A \in (R)_n \mid AB = BA \text{ para todo } B \text{ en } (R)_n\}$ es precisamente el conjunto de matrices escalares $\{rI \mid r \in R\}$.

Demostración:

Denotamos como $S = \{rI \mid r \in R\}$.

Sea $A \in S$ entonces A es de la forma $A = rI$ y sea $B \in (R)_n$.

$AB = (rI)B = r(IB) = r(BI) = B(rI) = BA$ por lo que $A \in C((R)_n)$

Para la otra inclusión, sea $A \in C((R)_n)$ y supongamos que A no es de la forma rI para alguna $r \in R$. Entonces existe un elemento a_{kl} no nulo de esta matriz que está fuera de la diagonal, es decir, $k \neq l$. Observamos que la matriz $E^{lk}A$ no es nula ya que a_{kl} está en la entrada (l,l) y es 0 en la entrada (k,k).

Ahora consideramos la matriz AE^{lk} que también es distinta de cero ya que a_{kl} está en la entrada (k,k) y es 0 en la entrada (l,l) por lo que $AE^{lk} \neq E^{lk}A$ lo cual es imposible ya que $A \in C((R)_n)$, por lo que A es una matriz diagonal.

Si A es una matriz diagonal en $C((R)_n)$ tal que existen elementos de esta matriz a_{kk} y a_{ll} no nulos y tales que $a_{kk} \neq a_{ll}$ entonces la matriz $E^{kl}A \neq 0$ ya que a_{ll} está en la posición (k,l) y la matriz $AE^{kl} \neq 0$ ya que a_{kk} está en la posición (k,l). Pero $A \in C((R)_n)$ por lo que $AE^{kl} = E^{kl}A$ y por lo tanto $a_{kk} = a_{ll}$ lo que es imposible.

Así, A es de la forma rI con $r \in R$, es decir, $A \in S$. ∎

El siguiente lema da las propiedades generales de las matrices elementales unitarias.

Lema: Sea $\{E_{ij}\}$, $1 \leq i,j \leq n$, el conjunto de matrices elementales unitarias en $(R)_n$. Entonces:

(*a*) $E_{ij} E_{pq} = \delta_{jp} E_{iq}$

(*b*) $\sum_i E_{ii} = I$

(*c*) $E_{ij} = E_{pq}$ si y solo si $i = p$ y $j = q$.

Demostración:

P.D. $[E_{ij}E_{pq}]_{rs} = [\delta_{jp}E_{iq}]_{rs}$

Sean $E_{ij} = [a_{rt}]$, $E_{pq} = [b_{ts}]$, entonces $E_{ij}E_{pq} = [c_{rs}]$ donde $c_{rs} = \sum_{t=1}^{n} a_{rt}b_{ts}$.

Así $c_{rs} = \delta_{ri}\,\delta_{jp}\,\delta_{qs}$ donde:

$$\delta_{ri} = \begin{cases} 1 \text{ si } r = i \\ 0 \text{ si } r \neq i \end{cases} \quad \delta_{jp} = \begin{cases} 1 \text{si } j = p \\ 0 \text{ si } j \neq p \end{cases} \quad \delta_{qs} = \begin{cases} 1 \text{ si } q = s \\ 0 \text{ si } q \neq s \end{cases}$$

$[\delta_{jp} E_{iq}] = [d_{rs}]$ donde $d_{rs} = \delta_{jp}\,\delta_{ri}\,\delta_{qs}$.

Por lo tanto, $E_{ij} E_{pq} = \delta_{jp} E_{iq}$.

Si $A = [a_{ij}]$ está en $(R)_n$, entonces $A = \sum_{ij} a_{ij} E_{ij}$ y esta expresión es **única**.

Las matrices elementales unitarias no son, obviamente, "unidades" en el sentido de la teoría de anillos. El origen del término parece tener su origen en el término "unidad basal" que era usado para designar a los elementos "base" del R-módulo libre. $(R)_n$

Sea $A = [a_{ij}]$ en $(R)_{m\,n}$. Entonces la transpuesta $A^t = [b_{ij}]$ es la matriz en $(R)_{n.m}$ dada por $b_{ji} = a_{ij}$ $(1 \le j \le m, \quad 1 \le i \le n)$.

Proposición:

a) $(A + B)^t = A^t + B^t$

b) $(AB)^t = B^t A^t$

c) $(A^{-1})^t = (A^t)^{-1}$

d) $t: (R)_{m.n} \longrightarrow (R)_{n.m}$

$A \longmapsto A^t$ es un morfismo de R-módulos con $t^2 = Id$.

Demostración:

Sean $A = [a_{ij}]$ y $B = [b_{ij}]$ en $(R)_{m.n}$.

Entonces $A+B = C$ donde $C = [c_{ij}]$ y $c_{ij} = a_{ij} + b_{ij}$.

$(A + B)^t = C^t = [c_{ij}]^t = [c_{ji}] = [a_{ji} + b_{ji}] = [a_{ji}] + [b_{ji}] = A^t + B^t$.

Sean $A=[a_{ij}]\in(R)_{m.n}$, $B=[b_{ik}]\in(R)_{n.p}$ y $A^t=[d_{ij}]\in(R)_{n.m}$, $B^t=[e_{jk}]\in(R)_{p.n}$ sus respectivas matrices transpuestas donde $d_{ij} = a_{ji}$ y $e_{jk} = b_{kj}$. Entonces:

$AB = C$ donde $C = [c_{ik}]$ en $(R)_{m.p}$ y $c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$.

Sea $C^t = [f_{ik}]$ la matriz transpuesta de C, donde $f_{ik} = c_{ki}$.

$(AB)^t = C^t = [f_{ik}]$

$$f_{ik} = c_{ki} = \sum_{j=1}^{n} a_{kj}b_{ji} = a_{k1}b_{1i} + a_{k2}b_{2i} + \ldots + a_{kn}b_{ni}$$

$$= b_{1i}a_{k1} + b_{2i}a_{k2} + \ldots + b_{ni}a_{kn} = e_{i1}d_{1k} + e_{i2}d_{2k} + \ldots + e_{in}d_{nk}$$

$$= \sum_{j=1}^{n} e_{ij}d_{jk} .$$

Por lo tanto, $(AB)^t = [f_{ik}] = [e_{ij}][d_{jk}] = B^t A^t$.

Para demostrar (e) tenemos que : $AA^{-1} = I$

$$\therefore (A^{-1})^t A^t = (AA^{-1})^t = I, \quad \text{y}$$

$$A^{-1}A = I$$

$$A^t(A^{-1})^t = (A^{-1}A)^t = I.$$

Por lo tanto $(A^t)^{-1} = (A^{-1})^t$.

(d) Si $t: (R)_{m,n} \longrightarrow (R)_{n,m}$

$A \longmapsto A^t$, entonces:

$t(A + B) = (A + B)^t = A^t + B^t = t(A) + t(B)$

$t(rA) = (rA)^t = rA^t = rt(A)$

$t^2(A) = t(t(A)) = t(A^t) = (A^t)^t = A.$

Por lo tanto, t es un morfismo de R-módulo con $t^2 = Id$. ■

Proposición: Sea R un anillo conmutativo y A un ideal en R. Entonces $(A)_n = \{[a_{ij}] \mid a_{ij}$ está en $A\}$ es un ideal bilateral de $(R)_n$. Además existe un isomorfismo natural: $\dfrac{(R)_n}{(A)_n} \cong \left(\dfrac{R}{A}\right)_n$.

Demostración:

$[0] \in (A)_n$ ya que $0 \in A$ por ser A un ideal en R.

Sean $[a_{ij}] \in (A)_n$ y $[b_{jk}] \in (R)_n$. Entonces $[a_{ij}][b_{jk}] = [c_{ik}]$ donde $c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$.

Para cada j, $a_{ij}b_{jx} \in A$ y por lo tanto $c_{ik} \in A$ para toda i,k, $1 \le i,k \le n$.

Análogamente, $[b_{ij}][a_{jk}] \in (A)_n$.

Sean $[a_{ij}], [a'_{ij}] \in (A)_n$.

$[a_{ij}] - [a'_{ij}] = [a_{ij} - a'_{ij}]$ donde $a_{ij} - a'_{ij} \in A$, así $[a_{ij}] - [a'_{ij}] \in (A)_n$.

Definimos $\frac{(R)_n}{(A)_n} \xrightarrow{\varphi} \left(\frac{R}{A}\right)_n$ como

$[r_{ij}] + (A)_n \longmapsto [r_{ij} + A]$ donde $r_{ij} \in R$.

Sea $[r_{ij}] + (A)_n \in Ker\ \varphi$.

$0 = \varphi([r_{ij}] + (A)_n) = [r_{ij} + A]$, entonces $r_{ij} \in A$ por lo que $[r_{ij}] \in (A)_n$, por lo tanto φ es inyectiva. ■

Sea R un anillo conmutativo. Un conjunto $\{F_{ij} \mid 1 \leq i,j \leq n\}$, de matrices en $(R)_n$ es un conjunto de matrices unitarias si:

a) $F_{ij} = F_{pq}$ si y sólo si $i = p$, $j = q$.

b) $F_{ij}F_{pq} = \delta_{jp}F_{iq}$ (δ = delta de Kronecker).

c) $\sum_i F_{ii} = I$

Proposición: Si Q es una matriz invertible fija, entonces $QE_{ij}Q^{-1} = F_{ij}$ da un conjunto de matrices unitarias donde $\{E_{ij}\}$ es el conjunto de matrices elementales unitarias.

Demostración:

a) Sea $F_{ij} = F_{pq}$.

$QE_{ij}Q^{-1} = QE_{pq}Q^{-1}$

$Q^{-1}QE_{ij}Q^{-1}Q = Q^{-1}QE_{pq}Q^{-1}Q$

$IE_{ij}I = IE_{pq}I$

$E_{ij} = E_{pq}$ si y sólo si $i = p$ y $j = q$.

b) $F_{ij}F_{pq} = (QE_{ij}Q^{-1})(QE_{pq}Q^{-1})$

$= QE_{ij}Q^{-1}QE_{pq}Q^{-1}$

$$= Q(\delta_{jp}E_{iq})Q^{-1}$$

$$= \delta_{jp}QE_{iq}Q^{-1}$$

$$= \delta_{jp}F_{iq}$$

c) $\sum_i F_{ii} = \sum_i QE_{ii}Q^{-1}$

$$= Q(\sum_i E_{ii})Q^{-1}$$

$$= QIQ^{-1}$$

$$= QQ^{-1}$$

$$= I\ .$$

Sea S un anillo (no necesariamente conmutativo) con identidad I. Supongamos que S contiene un conjunto de elementos $\{f_{ij}\}$, $1 \le i,j \le n$, que satisfacen que $\sum_i f_{ii} = I$, $f_{ij}f_{pq} = \delta_{jp}f_{iq}$. Entonces $f_{ij} \neq 0$ para toda i,j.

Sea $T = \{t \in S \mid tf_{ii} = f_{ij}t \text{ para toda } i,j\}$.

Si $s \in S$, definimos t_{ij}, para $1 \le i,j \le n$, por $t_{ij} = \sum_k f_{ki}sf_{jk}$. Entonces se satisfacen las siguientes proposiciones:

a) $t_{ij}f_{pq} = f_{pq}t_{ij}$ y por lo tanto $t_{ij} \in T$.

b) $s = \sum_{i,j} t_{ij}f_{ij}$.

c) $\Sigma t_{ij}f_{ij} = 0$ implica que $t_{ij} = 0$ para toda i,j. Por lo tanto, cada elemento de S tiene una única representación como $\Sigma t_{ij}f_{ij}$.

d) Definimos φ: $S \longrightarrow (T)_n$ (matrices de $n \times n$ sobre el anillo T no necesariamiente conmutativo) como $s = \Sigma t_{ij}f_{ij} \longmapsto [t_{ij}]$. Entonces φ es un isomorfismo de anillos.

e) T es isomorfo como anillo a $f_{11} S f_{11}$. Por lo tanto un anillo S es isomorfo a un anillo de matrices sobre un anillo T no necesariamente conmutativo, siempre que S contenga un conjunto de matrices unitarias.

Demostración:

a) $t_{ij} f_{pq} = (\sum_k f_{ki}\, s\, f_{jk}) f_{pq}$

$= \Sigma f_{ki}\, s\, f_{jk} f_{pq}$

$= \sum_k f_{ki}\, s\, (f_{jk} f_{pq})$

$= \sum_k f_{ki}\, s\, (\delta_{kp} f_{jq})$ $\quad \delta_{kp} = \begin{cases} 1 \text{ si } k = p \\ 0 \text{ si } k \neq p \end{cases}$

$= f_{pi}\, s\, f_{jq}$

$f_{pq} t_{ij} = f_{pq} (\sum_k f_{ki}\, s\, f_{jk})$

$= \sum_k f_{pq} f_{ki}\, s\, f_{jk}$

$= \sum_k (f_{pq} f_{ki})\, s\, f_{jk}$

$= \sum_k (\delta_{qk} f_{pi})\, s\, f_{jk}$ $\quad \delta_{qk} = \begin{cases} 1 \text{ si } q = k \\ 0 \text{ si } q \neq k \end{cases}$

$= f_{pi}\, s\, f_{jq}$

Por lo tanto, $t_{ij} f_{pq} = f_{pq} t_{ij}$ y $t_{ij} \in T$.

b) $t_{ij} = \Sigma f_{ki}\, s\, f_{jk}$

$t_{ij} f_{ij} = f_{ii}\, s\, f_{jj}$, ya que $t_{ij} f_{ij} = f_{ij} t_{ij}$

$= f_{ij} (\sum_k f_{ki}\, s\, f_{jk})$

$= \sum_k f_{ij} f_{ki}\, s\, f_{jk} = f_{ii}\, s\, f_{jk}$

$\sum_{i,j} t_{ij} f_{ij} = t_{11} f_{11} + \ldots + t_{1n} f_{1n} + t_{21} f_{21} + \ldots + t_{2n} f_{2n} + \ldots + t_{n1} f_{n1} + \ldots + t_{nn} f_{nn}$

$$= f_{11}\, s f_{11} + \dots f_{11}\, s f_{nn} + f_{22}\, s f_{11} + \dots + f_{22}\, s f_{nn} + \dots + f_{nn}\, s f_{11} + \dots + f_{nn}\, s f_{nn}$$

$$= (f_{11}\, s)(\sum_i f_{i1}) + (f_{22}\, s)(\sum_i f_{i1}) + \dots + (f_{nn}\, s)(\sum_i f_{i1})$$

$$= f_{11}\, s + f_{22}\, s + \dots + f_{nn}\, s$$

$$= (f_{11} + f_{22} + \dots + f_{nn})\, s$$

$$= (\sum_i f_{i1})\, s = 1 \cdot s = s$$

c) Si $\Sigma t_{ij} f_{ij} = 0$ entonces $t_{ij} = \sum_k f_{ki}\, s\, f_{jk} = \sum_k f_{ki} \cdot f_{jk} = 0$

por lo tanto $t_{ij} = 0$ para toda i,j.

d) Sea $s \in Ker\, \varphi$, entonces: $\varphi(s) = \varphi(\Sigma t_{ij} f_{ij}) = [t_{ij}] = 0$

por lo que $t_{ij} = 0$ para toda i,j, lo que significa que $s = \Sigma t_{ij} f_{ij} = 0$.

Sea $[t_{ij}]$ en $(\Gamma)_n$ con t_{ij} en T. Definimos $s = \Sigma t_{ij} f_{ij}$, por lo tanto $\varphi(s) = [t_{ij}]$.

Así. φ es un isomorfismo de anillos.

Sean s y r en S.

$$s = \Sigma t_{ij} f_{ij}, \quad r = \Sigma t'_{jk} f_{jk}$$

$$sr = (\Sigma t_{ij} f_{ii})(\Sigma t'_{jk} f_{jk})$$

$$= \sum_{i,j,k} \sum t_{ii}\, t'_{jk}\, f_{ij} f_{jk}$$

$$= \sum_{i,k} (\sum_j t_{ij}\, t'_{jk}) f_{ik}$$

$$\varphi(s \cdot r) = [\sum_j t_{ij}\, t'_{jk}]$$

$$= [t_{ij}][t'_{jk}]$$

$$= \varphi(s)\, \varphi(r)$$

Por lo tanto, φ es un morfismo de anillo. ■

Proposición: Sean R un anillo conmutativo y $\Lambda: (R)_n \longrightarrow (R)_n$ un antomorfismo de anillos. Sean $\{E_{ij}\}$ las matrices elementales unitarias.

Si $F_{ij} = \Lambda(E_{ij})$ entonces $\{F_{ij}\}$ es un conjunto de matrices unitarias.

Demostración:

Si $F_{ij} = F_{pq}$

$\Lambda(E_{ij}) = \Lambda(E_{pq})$

$\Lambda(E_{ij}) - \Lambda(E_{pq}) = 0$

$\Lambda(E_{ij} - E_{pq}) = 0$

$E_{ij} - E_{pq} = 0$

$E_{ij} = E_{pq}$ si y sólo si $i = p$, $j = q$.

$$F_{ij} F_{pq} = \Lambda(E_{ij}) \Lambda(E_{pq})$$

$$= \Lambda(E_{ij} E_{pq})$$

$$= \Lambda(\delta_{jp} E_{iq})$$

$$= \delta_{jp} \Lambda(E_{iq}) = \delta_{jp} F_{iq}.$$

$$\sum_i F_{ii} = \sum_i \Lambda(E_{ii}) = \Lambda(\Sigma E_{ii}) = \Lambda(I) = I.$$

Por lo tanto, $\{F_{ij}\}$ es un conjunto de matrices unitarias.

Proposición: Supongamos que R es un anillo finito y $|R| = t$. Entonces $|(R)_n| = t^{n^2}$.

Demostración:

Sea $A = [a_{ij}]$ en $(R)_n$.

$A = \sum_{i,j} a_{ij} E_{ij}$ donde E_{ij} es una matriz elemental unitaria.

$\{E_{ij}\}$ tiene cardinalidad n^2.

Cada elemento de $(R)_n$ se puede ver como una permutación de t elemento en n^2 posiciones, por lo que el número de permutaciones de t elementos en n^2 posiciones es t^{n^2}.

Por lo tanto $|(R)_n| = t^{n^2}$. ■

Proposición: Sea R un anilo conmutativo y $A = [a_{ij}]$ en $(R)_n$. La traza de A, denotada por $Tr(A)$, es la suma de los elementos de la diagonal de A, es decir, $Tr(A) = a_{11} + a_{22} + \ldots + a_{nn}$. Entonces se tiene que para A y B en $(R)_n$ se satisfacen las siguientes igualdades:

$$Tr(AB) = Tr(BA)$$

$$Tr(A - B) = Tr(A) - Tr(B)$$

$$Tr(\alpha A) = \alpha Tr(A)$$

Las últimas dos proposiciones muestran que la traza, como mapeo, $Tr: (R)_n \longrightarrow R$ es un morfismo de R-módulos.

Demostración:

Sean $A = [a_{ij}]$, $B = [b_{jk}]$ en $(R)_n$.

$AB = C$ donde $C = [c_{ik}]$ y $c_{ij} = \sum_{j=1}^{n} a_{ij} b_{jk}$. Entonces:

$Tr(AB) = Tr(C) = c_{11} + c_{22} + \ldots + c_{nn}$

$$= \sum_{j=1}^{n} a_{1j} b_{j1} + \sum_{j=1}^{n} a_{2j} b_{j2} + \ldots + \sum_{j=1}^{n} a_{nj} b_{jn}$$

$$= a_{11}b_{11} + \sum_{j=2}^{n} a_{1j} b_{j1} + a_{21} b_{12} + \sum_{j=2}^{n} a_{2j} b_{j2} + \ldots + a_{n1} b_{1n} + \sum_{j=2}^{n} a_{nj} b_{jn}$$

$$= a_{11}b_{11} + a_{21}b_{12} + \ldots + a_{n1}b_{1n} + \sum_{j=2}^{n} a_{1j} b_{j1} + \sum_{j=2}^{n} a_{2j} b_{j2} + \ldots + \sum_{j=2}^{n} a_{nj} b_{jn}$$

$$= \sum_{j=1}^{n} b_{1j} a_{j1} + \sum_{j=2}^{n} a_{1j} b_{j1} + \sum_{j=2}^{n} a_{2j} b_{j2} + \ldots + \sum_{j=2}^{n} a_{nj} b_{jn}$$

$$= \sum_{j=1}^{n} b_{1j} a_{j1} + a_{12} b_{21} + \sum_{j=3}^{n} a_{1j} b_{j1} + a_{22} b_{22} + \sum_{j=3}^{n} a_{2j} b_{j2} + \ldots + a_{n2} b_{2n} + \sum_{j=3}^{n} a_{nj} b_{jn}$$

$$= \sum_{j=1}^{n} b_{1j} a_{j1} + b_{21} a_{12} + a_{22} b_{22} + \ldots + b_{2n} a_{n2} + \sum_{j=3}^{n} a_{1j} b_{j1} + \sum_{j=3}^{n} a_{2j} b_{j2} + \ldots + \sum_{j=3}^{n} a_{nj} b_{jn}$$

$$= \sum_{j=1}^{n} b_{1j} a_{j1} + \sum_{j=1}^{n} b_{2j} a_{j2} + \sum_{j=3}^{n} a_{1j} b_{j1} + \sum_{j=3}^{n} a_{2j} b_{j2} + \ldots + \sum_{j=3}^{n} a_{nj} b_{jn}$$

$$= \sum_{j=1}^{n} b_{1j} a_{j1} + \sum_{j=1}^{n} b_{2j} a_{j2} + \sum_{j=1}^{n} b_{3j} a_{j3} + \ldots + \sum_{j=1}^{n} b_{nj} a_{jn}$$

$$= c'_{11} + c'_{22} + c'_{33} + \ldots + c'_{nn}$$

$$= Tr(c') = Tr(BA) \qquad \text{donde } c' = [c'_{ik}] \text{ y } c'_{ik} = \sum_{j=1}^{n} b_{ij} a_{jk}$$

$$Tr(A + B) = a_{11} + b_{11} + a_{22} + b_{22} + \ldots + a_{nn} + b_{nn}$$

$$= a_{11} + a_{22} + \ldots + a_{nn} + b_{11} + b_{22} + \ldots + b_{nn}$$

$$= Tr(A) + Tr(B)$$

$$Tr(\alpha A) = \alpha a_{11} + \alpha a_{22} + \ldots + \alpha a_{nn}$$

$$= \alpha \, (a_{11} + a_{22} + \ldots + a_{nn})$$

$$= \alpha Tr(A).$$

Por lo tanto, $Tr: (R)_n \longrightarrow R$ **es un morfismo de** R**-módulos.** ■

Proposición: El mapeo $Tr: (R)_n \longrightarrow R$ es sobreyectivo.

Demostración:

Sea $r \in R$.

Definimos $A = rE_{11}$, entonces $Tr(A) = Tr(rE_{11}) = r$, por lo tanto Tr es sobreyectivo. ■

Proposición: Los elementos que van a dar a cero bajo el mapeo $Tr:(R)_n \longrightarrow R$ son generados como un R-módulo por el conjunto $\{E_{ji} (j \neq i),\ E_{11}-E_{ii}, (i > 1)\}$ donde E_{ji} denota una matriz elemental unitaria.

Demostración:

Sea A en $(R)_n$ tal que $Tr(A) = 0$.

$A = [a_{ji}],\ a_{ji} \in R$.

$A = \sum_{j \neq i} a_{ji}E_{ji} + a_{11}E_{11} + a_{22}E_{22} + a_{33}E_{33} + \ldots + a_{nn}E_{nn}$

Como $Tr(A) = a_{11} + a_{22} + a_{33} + \ldots + a_{nn} = 0$, se tiene que:

$$a_{11} = -a_{22} - a_{33} - \ldots - a_{nn}.$$

Así, $a_{11}E_{11} = (-a_{22} - a_{33} - \ldots - a_{nn})\, E_{11}$ por lo que:

$$A = \sum_{j \neq i} a_{ji}E_{ji} + (-a_{22} - a_{33} - \ldots - a_{nn})\, E_{11} + a_{22}E_{22} + \ldots + a_{nn}E_{nn}$$

$$= \sum_{j \neq i} a_{ji}E_{ji} - a_{22}E_{11} - a_{33}E_{11} - \ldots - a_{nn}E_{nn} + a_{22}E_{22} + \ldots + a_{nn}E_{nn}$$

$$= \sum_{j \neq i} a_{ji}E_{ji} - a_{22}E_{11} + a_{22}E_{22} - a_{33}E_{11} - a_{33}E_{33} + \ldots - a_{nn}E_{11} + a_{nn}E_{nn}$$

$$= \sum_{j \neq i} a_{ji}E_{ji} - a_{22}(E_{11}-E_{22}) - a_{33}(E_{11}-E_{33}) + \ldots - a_{nn}(E_{11}-E_{nn}).$$

Por lo tanto A es generada por el conjunto $\{E_{ji} (j \neq i),\ E_{11}-E_{ii} (i > 1)\}$. ■

Proposición: $Tr(A^t) = Tr(A)$ y si Q es invertible, entonces $Tr(QAQ^{-1}) = Tr(A)$.

Demostración:

Sea $A = [a_{ij}]$ y $A^t = [b_{ij}]$ donde $b_{ij} = a_{ji}$.

Entonces: $Tr(A^t) = b_{11} + b_{22} + \ldots + b_{nn}$

$= a_{11} + a_{22} + \ldots + a_{nn} = Tr(A)$

$Tr(QAQ^{-1}) = Tr((QA)Q^{-1})$

$= Tr(Q^{-1}(QA))$

$= Tr(Q^{-1}QA)$

$= Tr(IA)$

$= Tr(A)$. ■

Proposición:

Si $A = \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix}$ donde A_1 y A_2 son bloques de matrices cuadradas, entonces $Tr(A) = Tr(A_1) + Tr(A_2)$.

Sea A_1 una matriz de $r \times r$ y sea A_2 una matriz de $s \times s$. Entonces:

$Tr(A_1) = a_{11} + \ldots + a_{rr}$

$Tr(A_2) = a_{r+1\,r+1} + \ldots + a_{r+s\,r+s}$

$Tr(A_1) + Tr(A_2) = a_{11} + \ldots + a_{rr} + a_{r+1\,r+1} + \ldots + a_{r+s\,r+s} = Tr(A)$. ■

III. Ideales en $(R)_n$.

Como en la sección anterior, R denota un anillo y $(R)_n$ la R-álgebra de matrices de $n \times n$ sobre R.

Proposición: Sea R un anillo conmutativo y A un ideal en R. Entonces: $(A)_n = \{[a_{ij}] \mid a_{ij} \in A\}$ es un ideal de $(R)_n$.

Demostración:

$(A)_n \neq \emptyset$ ya que $[0] \in (A)_n$.

Sean $[a_{ij}]$ y $[b_{ij}]$ en $(A)_n$. Entonces $[a_{ij}] - [b_{ij}] = [c_{ij}]$ donde $c_{ij} = a_{ij} - b_{ij}$ para toda (i,j) por lo que $[c_{ij}] \in (A)_n$.

Sean $[a_{ij}] \in (A)_n$ y $[b_{jk}] \in (R)_n$. Entonces $[a_{ij}][b_{jk}] = [c_{ik}]$ donde $c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$.

$a_{ij} b_{jk} \in A$ para $j = 1, \ldots, n$ ya que A es un ideal, por lo que $c_{ik} \in A$ para toda (i,k), por lo tanto $[c_{ik}] \in (A)_n$.

Análogamente se cumple que $[b_{ij}][a_{jk}] = [d_{ik}] \in (A)_n$.

Así, $(A)_n$ es un ideal de $(R)_n$. ■

Ahora demostraremos la proposición recíproca, es decir, que todo ideal en $(R)_n$ tiene la forma $(A)_n$ para algún ideal A en R. Este es un resultado útil e importante en la teoría de matrices sobre anillos y como se observará en la demostración, no depende de que R sea conmutativo.

Teorema: Cada ideal B de $(R)_n$ tiene la forma $B = (A)_n$ para un único ideal A de R.

Demostración:

Sea B un ideal de $(R)_n$.

Sea A el conjunto de todos los elementos en R que aparecen en las entradas de las matrices en B.

Si r aparece en la entrada (i,j) de una matriz X en B entonces por medio de operaciones con matrices elementales unitarias podemos hacer que r aparezca en la posición (1,1) de alguna matriz Y en B ya que $E^{1i}XE^{j1} = rE^{11} \in B$. Por lo que podemos suponer que los elementos de A se pueden encontrar en la entrada (1,1) de los elementos de B.

Primero mostraremos que A es un ideal en R.

$A \neq \varnothing$ ya que $0 \in A$.

Sean $a, b \in A$ entonces existen matrices $X, Y \in B$ tales que $x_{11}=a$ y $y_{11}=b$.

Así, $a-b$ aparece en la entrada (1,1) de la matriz $X-Y$ que está en B. Por lo tanto $a-b$ está en A.

Sean $a \in A$ y $r \in R$. Entonces existe una matriz Y en B tal que $y_{11}=a$.

Sea X una matriz en $(R)_n$ que tenga en la entrada (1,1) a r. Por lo tanto, ra aparece en la entrada (1,1) de la matriz XY que está en B.

Así, $ar \in A$. Por lo tanto A es un ideal en R.

Sea $\hat{B} = (A)_n$

Demostraremos que $B = \hat{B}$.

Sea $X \in B$, X es de la forma $X = \Sigma x_{ij} E^{ij}$. Entonces:

$$E^{1r} X E^{s1} = E^{1r} (\Sigma x_{ij} E^{ij}) E^{s1}$$

$$= x_{rs} E^{11} \in B \qquad 1 \leq r \leq n \quad y \quad 1 \leq s \leq n.$$

Por lo tanto, para cada x_{ij} existe una matriz en B tal que x_{ij} aparece en la entrada (1,1).

Así, $x_{ij} \in A$ para toda (i,j). Por lo tanto, $X \in \hat{B}$.

Para la otra inclusión, sea $[x_{ij}] \in \hat{B}$, entonces para cada x_{ij} existe una matriz $Y = [y_{ij}]$ en B con $y_{11} = x_{ij}$. Entonces:

$E^{i1} Y E^{1j} = y_{11} E^{ij} = x_{ij} E^{ij}$ está en B.

Así, $B = \hat{B}$. ■

Podemos observar que la clave de la demostración anterior fue que:

(1) Tenemos una descripción sencilla de la multiplicación de matrices unitarias, y

(2) Cada elemento de $(R)_n$ puede ser expresado de manera única como una suma $\Sigma a_{ij} E^{ij}$ para $a_{ij} \in R$ adecuados.

Sea $\{E_{ij}\}$ el conjunto de matrices elementales unitarias en $(R)_n$.

Proposición: Para $\lambda \in R$ y $i \neq j$, sea $T_{ij}(\lambda) = I + \lambda E_{ij}$. La matriz $T_{ij}(\lambda)$ es una transvección elemental. Entonces:

$T_{ij}(\lambda)\, T_{ij}(\beta) = T_{ij}(\lambda+\beta)$ y $T_{ij}(\lambda)$ es invertible con inversa $T_{ij}(-\lambda)$.

Demostración:

$$T_{ij}(\lambda)\, T_{ij}(\beta) = (I + \lambda E_{ij})(I + \beta E_{ij})$$

$$= I + \beta E_{ij} + \lambda E_{ij}(I + \beta E_{ij})$$

$$= I + \beta E_{ij} + \lambda E_{ij} + \lambda E_{ij}\beta E_{ij}$$

$$= I + \beta E_{ij} + \lambda E_{ij}$$

$$= I + (\lambda + \beta)E_{ij}$$

$$= T_{ij}(\lambda+\beta)$$

$$T_{ij}(\lambda)\, T_{ij}(-\lambda) = T_{ij}(\lambda - \lambda) = T_{ij}(0) = I$$

$$T_{ij}(-\lambda)\, T_{ij}(\lambda) = T_{ij}(-\lambda + \lambda) = T_{ij}(0) = I.$$

$$\therefore T_{ij}(\lambda)^{-1} = T_{ij}(-\lambda). \quad \blacksquare$$

Proposición: Sea $P_{ij} = I - E_{ii} - E_{jj} + E_{ij} + E_{ji}$ para $1 \leq i,j \leq n$. La matriz P_{ij} es una permutación elemental. Entonces P_{ij} es invertible con $P^{-1}{}_{ij} = P_{ij}$ y $E_{jj} = P^{-1}{}_{ij} E_{ii} P_{ij}$ para $1 \leq j \leq n$.

Demostración:

$$P_{ij} P^{-1}{}_{ij} = P_{ij} P_{ij}$$

$$= (I - E_{ii} - E_{jj} + E_{ij} + E_{ji})(I - E_{ii} - E_{jj} - E_{ij} + E_{ji})$$

$= (I-E_{ii} - E_{jj}+ E_{ij}+ E_{ji})-E_{ii}(I - E_{ii} - E_{jj} + E_{ii} + E_{ji})-E_{jj}(I - E_{ii} - E_{jj} + E_{ij} + E_{ji})$

$-E_{ij}(I-E_{ii} - E_{jj}+ E_{ij} +E_{ji}) - E_{ji}(I- E_{ii} -E_{jj}+ E_{ij}+E_{ji})+E_{ji}(I-E_{ii} - E_{jj} + E_{ii} + E_{ji})$

$= I - E_{ii} - E_{jj} + E_{ij} + E_{ji} - E_{ii} + E_{ii} - E_{ij} - E_{ij} + E_{ij} - E_{ji} + E_{ij} - E_{ij} + E_{ii} - E_{ji} -$

$E_{ji} + E_{jj}$

$= I - 2E_{ii} + 2E_{ii} - 2E_{jj} + 2E_{jj} + 2E_{ij} - 2E_{ij} + 2E_{ji} - 2E_{ji}$

$= I$. ■

Proposición: Sea $S_{ij} = I - E_{ii} - E_{jj} - E_{ij} + E_{ji}$ para $1 \le i,j \le n$, $i \ne j$. La matriz S_{ij} es una permutación "skew" elemental. Entonces S_{ij} es invertible con inversa $S^{-1}{}_{ij} = (I + E_{ij})(I - E_{ji})(I + E_{ij})$

Demostración:

$S_{ij} S^{-1}{}_{ij} = (I - E_{ii} - E_{jj} - E_{ij} - E_{ji})(I - E_{ii} - E_{jj} + E_{ij} - E_{ji})$

$= (I - E_{ii} - E_{ii} - E_{ij} + E_{ji}) + (-E_{ii} + E_{ii} - E_{ij}) + (-E_{jj} + E_{jj} + E_{ij}) + (E_{ji} - E_{ji} + E_{jj}) + (-E_{ij} + E_{ij} + E_{ii})$

$= I - E_{ii} - E_{jj} + E_{ij} - E_{ji} - E_{ij} - E_{ii} + E_{ji} + E_{ij}$

$= I$.

$(I + E_{ij})(I - E_{ji})(I + E_{ij}) =$

$= ((I + E_{ij})(I - E_{ji}))(I + E_{ij})$

$= ((I - E_{ji}) + E_{ij}(I - E_{ji}))(I + E_{ij})$

$= (I - E_{ji} + E_{ij} - E_{ii})(I + E_{ij})$

$= (I - E_{ji} + E_{ij} - E_{ii}) + (I - E_{ji} + E_{ij} - E_{ii})E_{ij}$

$= I - E_{ji} + E_{ij} - E_{ii} + E_{ij} - E_{jj} - E_{ij}$

$I - E_{ii} - E_{jj} - E_{ij} - E_{ji}$

$= S^{-1}{}_{ij}$. ■

Proposición: Sea $D_i(\lambda) = I - E_{ii} + \lambda E_{ii}$ (λ una unidad). La matriz $D_i(\lambda)$ es una dilatacion elemental. Entonces:

$D_i(\lambda)D_i(\beta) = D_i(\lambda\beta)$ y $D_i(\lambda)^{-1} = D_i(\lambda^{-1})$.

Demostración:

$$D_i(\lambda)\,D_i(\beta) = (I - E_{ii} + \lambda E_{ii})(I - E_{ii} + \beta E_{ii})$$

$$= (I - E_{ii} + \beta E_{ii}) + (-E_{ii} + E_{ii} - \beta E_{ii}) + (\lambda E_{ii} - \lambda E_{ii} + \lambda E_{ii}\beta E_{ii})$$

$$= I - E_{ii} + \beta E_{ii} - \beta E_{ii} + \lambda E_{ii}\beta E_{ii}$$

$$= I - E_{ii} + \lambda E_{ii}\beta E_{ii}$$

$$= I - E_{ii} + (\lambda\beta)E_{ii}$$

$$= D_i(\lambda\beta) .$$

$$D_i(\lambda)\,D_i(\lambda^{-1}) = D_i(\lambda\lambda^{-1}) = D_i(1) = I - E_{ii} + E_{ii} = I$$

$$D_i(\lambda^{-1})\,D_i(\lambda) = D_i(\lambda^{-1}\lambda) = D_i(1) = I - E_{ii} + E_{ii} = I$$

$$\therefore\ D_i(\lambda^{-1}) = D_i(\lambda)^{-1}$$

$$D_i(u_1)\,D_j(u_2) = (I - E_{ii} - u_1E_{ii})(I - E_{jj} - u_2E_{jj})$$

$$= I - E_{jj} + u_2E_{jj} - E_{ii} + u_1E_{ii}$$

$$= I - E_{ii} + u_1E_{ii} - E_{jj} + u_2E_{ii}$$

$$= (I - E_{jj} + u_2E_{jj})(I - E_{ii} + u_1E_{ii})$$

$$= D_j(u_2)\,D_i(u_1) . \quad ■$$

Proposición: Sea $T_{ij}(\lambda)$ en $(R)_n$. Entonces $T_{ij}(\lambda)T_{ik}(\beta) = T_{ik}(\beta)T_{ij}(\lambda)$.

Demostración:

$$\begin{aligned} T_{ij}(\lambda)T_{ik}(\beta) &= (I + \lambda E_{ij})(I + \beta E_{ik}) \\ &= (I + \beta E_{ik}) + \lambda E_{ij}(I + \beta E_{ik}) \\ &= I + \beta E_{ik} + \lambda E_{ij} + \lambda E_{ij}\beta E_{ik} \\ &= I + \lambda E_{ij} + \beta E_{ik} + \beta E_{ik}\lambda E_{ij} \\ &= (I + \lambda E_{ij}) + \beta E_{ik}(I - \lambda E_{ij}) \\ &= (I + \beta E_{ik})(I + \lambda E_{ij}) \\ &= T_{ik}(\beta) + T_{ij}(\lambda) . \blacksquare \end{aligned}$$

Proposición: Definimos $A(\lambda_2 , \dots , \lambda_n) = T_{12}(\lambda_2)\ T_{13}(\lambda_3) \dots T_{1n}(\lambda_n)$. Entonces existe un mapeo natural $\varphi: (R)_{n-1} \longrightarrow \{A(\lambda_2 , \dots , \lambda_n) \mid \lambda_i \in R\} \subset (R)_n$ dado por $[\lambda_2 , \dots , \lambda_n] \longmapsto A(\lambda_2 , \dots , \lambda_n)$ tal que φ es un isomorfismo de módulos.

Demostración:

Sea $[\lambda_2 , \dots , \lambda_n] \in ker\ \varphi$.

$0 = \varphi[\lambda_2 , \dots , \lambda_n] = A(\lambda_2 , \dots , \lambda_n) = T_{12}(\lambda_2)\ T_{13}(\lambda_3) \dots T_{1n}(\lambda_n)$ si y solo si $\lambda_2 = \lambda_3 = \dots = \lambda_n = 0$.

Por lo tanto $[\lambda_2 , \dots , \lambda_n] = 0$. Así, φ es inyectiva.

Sea $A(\lambda_2 , \dots , \lambda_n) \in (R)_n$

$$A(\lambda_2 , \dots , \lambda_n) = T_{12}(\lambda_2)\ T_{13}(\lambda_3) \dots T_{1n}(\lambda_n)$$

$$= \begin{bmatrix} 1 & \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Sea $[\lambda_2, \ldots \lambda_n] \in (R)_{1,n-1}$ tal que $\varphi([\lambda_2, \ldots \lambda_n]) = A(\lambda_2, \ldots, \lambda_n)$.

P.D. $\varphi(r[\lambda_2, \ldots \lambda_n]) = r\varphi([\lambda_2, \ldots \lambda_n])$

$$\varphi(r[\lambda_2, \ldots \lambda_n]) = \varphi([r\lambda_2, \ldots r\lambda_n])$$

$$= A(r\lambda_2, \ldots, r\lambda_n)$$

$$= T_{12}(r\lambda_2)\, T_{13}(r\lambda_3) \ldots T_{1n}(r\lambda_n)$$

$$= rA(\lambda_2, \ldots, \lambda_n)$$

$$= r\varphi([\lambda_2, \ldots \lambda_n]) \cdot \blacksquare$$

Definición: Una matriz A en $(R)_n$ es llamada una matriz unitriangular (inferior) si todos los elementos de la diagonal son 1 y todos los elementos de arriba de la diagonal son cero.

Proposición: Si $A = [a_{ij}]$ es unitriangular, entonces $A = \prod_{i>j} T_{ij}(a_{ij})$. Una expresión similar se cumple para una matriz unitriangular superior.

Demostración:

Cada renglón de A se puede escribir como un producto de transverceciones elementales.

$$T_{21}(a_{21}) = I + a_{21}E_{21}$$

$$T_{31}(a_{31})\ T_{32}(a_{32}) = I + a_{31}E_{31} + a_{32}E_{32}$$

$$T_{41}(a_{41})\ T_{42}(a_{42})\ T_{43}(a_{43}) = I + a_{41}E_{41} + a_{42}E_{42} + a_{43}E_{43}$$

$$\vdots$$

$$T_{n1}(a_{n1})\ T_{n2}(a_{n2})\ T_{n3}(a_{n3})\ \cdots\ T_{nn-1}(a_{nn-1}) = I + a_{n1}E_{n1} + \cdots + a_{nn-1}E_{nn-1}$$

Por lo que:

$$T_{21}(a_{21})(T_{31}(a_{31})T_{32}(a_{32}))(T_{41}(a_{41})T_{42}(a_{42})T_{43}(a_{43}))\ \cdots\ T_{n1}(a_{n1})T_{n2}(a_{n2})\cdots T_{nn-1}(a_{nn-1})$$

$$= (I+a_{21}E_{21})(I+a_{31}E_{31}+a_{32}E_{32})(I+a_{41}E_{41}+a_{42}E_{42}+a_{43}E_{43})\ \cdots\ (I+a_{n1}E_{n1}+\cdots+a_{nn-1}E_{nn-1})$$

$$= (I+a_{21}E_{21} + a_{31}E_{31} + a_{32}E_{32})(I+a_{41}E_{41}+a_{42}E_{42}+a_{43}E_{43})\ \cdots\ (I+a_{n1}E_{n1}+\cdots+a_{nn-1}E_{nn-1})$$

$$= (I+a_{21}E_{21} + a_{31}E_{31} + a_{32}E_{32} + a_{41}E_{41} + a_{42}E_{42} + a_{43}E_{43})\ \cdots\ (I+a_{n1}E_{n1}+\cdots+a_{nn-1}E_{nn-1})$$

$$= I + a_{21}E_{21} + a_{31}E_{31} + a_{32}E_{32} + \cdots + a_{n1}E_{n1} + \cdots + a_{nn-1}E_{nn-1}$$

$$= A\ .\ \blacksquare$$

VI. El Determinante.

El determinante es uno de los invariantes más útiles asociados a una matriz. En esta sección se da un desarrollo clásico matricial del determinante.

Sea $A = [a_{ij}]$ en $(R)_n$.

Definimos $det: (R)_n \longrightarrow R$ como:

$$det(A) = \sum_{\sigma} sgn(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

donde la suma se extiende sobre todas las permutaciones σ de $\{1,2, \ldots, n\}$, es decir, sobre todas las σ en el grupo simétrico S_n de n letras. El símbolo $sgn(\sigma)$ es el "signo de la permutación σ" -esto es, + o - de acuerdo a si σ es una permutación par o impar, respectivamente. Una permutación es par (impar) si puede ser escrita como un producto par (impar) de transposiciones.

El mapeo $det: (R)_n \longrightarrow R$ es llamado el determinante o el mapeo determinante y $det(A)$ es llamado el determinante de A.

A continuación se probará un viejo teorema que tiene muchas aplicaciones.

Sea A una matriz de $n \times m$ sobre R.

Sea $A \begin{bmatrix} r_1 & r_2 & \cdots & r_t \\ \vdots & & & \\ c_1 & c_2 & \cdots & c_t \end{bmatrix}$ $\qquad t \leq min\{n,m\}$

que denota el subarreglo cuadrado de $t \times t$ obtenido de A eliminando todos los renglones excepto los renglones $r_1, \ldots, r_t$ y eliminando todas las columnas $c_1, \ldots, c_t$. El determinante de la matriz de $t \times t$ resultante, es llamada un menor de A de orden t.

Teorema: Sea A una matriz de $m\times n$ sobre R y B una matriz de $n\times p$ sobre R. Sea $M\begin{bmatrix} r_1 & r_2 & \dots & r_t \\ c_1 & c_2 & \dots & c_t \end{bmatrix}$ una submatriz de $t\times t$ de $M = AB$ donde $1\le t \le min\{m,n,p\}$. Entonces:

$$det\left|M\begin{bmatrix} r_1 & r_2 & \dots & r_t \\ c_1 & c_2 & \dots & c_t \end{bmatrix}\right| = \Sigma det\left|A\begin{bmatrix} r_1 & \dots & r_s \\ s_1 & \dots & s_t \end{bmatrix}\right| det\left|B\begin{bmatrix} s_1 & \dots & s_t \\ c_1 & \dots & c_t \end{bmatrix}\right|$$

donde la suma se extiende sobre todas las $\binom{n}{t}$ selecciones de $\{s_1, s_2, \dots, s_t\}$ de $\{1,2,3, \dots, n\}$ con $1 \le s_1 < s_2 < \dots < s_t \le n$.

Demostración:

Sea $M' = M\begin{bmatrix} r_1 & \dots & r_t \\ c_1 & \dots & c_t \end{bmatrix} = \begin{bmatrix} \alpha_{r_1c_1} & \alpha_{r_1c_2} & \dots & \alpha_{r_1c_t} \\ \vdots & & & \\ \alpha_{r_tc_1} & \alpha_{r_tc_2} & \dots & \alpha_{r_tc_t} \end{bmatrix}$

donde $\alpha_{r_kc_l} = \sum_{l_k=0}^{n} a_{r_kl_k}b_{l_kc_l} \qquad k = 1, \dots, t$

$$detM' = \sum_{\sigma} sgn(\sigma)\alpha_{r_1,\sigma(c_1)}\alpha_{r_2,\sigma(c_2)}\dots\alpha_{r_t\sigma(c_t)}$$

donde $\sum_{\sigma}$ se extiende a todas las permutaciones de $\{c_1, c_2, \dots, c_t\}$.

$$detM' = \sum_{\sigma} sgn(\sigma)\left(\sum_{l_1=1}^{n} a_{r_1l_1}b_{l_1\sigma(c_1)}\right)\left(\sum_{l_2=1}^{n} a_{r_2l_2}b_{l_2\sigma(c_2)}\right)\dots\left(\sum_{l_t=1}^{n} a_{r_tl_t}b_{l_t\sigma(c_t)}\right)$$

donde σ corre sobre las permutaciones de $\{c_1, \dots, c_t\}$. Expandiendo, esta expresión puede ser escrita como una suma de n^t determinantes, como sigue:

$$= \sum_{\sigma} sgn(\sigma)a_{r_11}b_{1\sigma(c_1)}\,a_{r_21}b_{1\sigma(c_2)}\dots a_{r_t1}b_{1\sigma(c_t)} + \dots +$$

$$+ \sum_{\sigma} sgn(\sigma)a_{r_1n}b_{n\sigma(c_1)}\,a_{r_2n}b_{n\sigma(c_2)}\dots a_{r_tn}b_{n\sigma(c_t)}$$

$$= \sum_{l_1,l_2,\dots,l_t=1}^{n}\left(\sum_{\sigma} sgn(\sigma)(a_{r_1l_1}b_{l_1\sigma(c_1)}\,a_{r_2l_2}b_{l_2\sigma(c_2)}\dots a_{r_tl_t}b_{l_t\sigma(c_t)})\right)$$

Como las permutacines σ comprenden solo los subíndices b_{kl}

$$= \sum_{i_1,i_2,\ldots,i_t=1}^{n} a_{r_1 i_1} a_{r_2 i_2} \ldots a_{r_t i_t} \left(\sum_{\sigma} sgn(\sigma)(b_{i_1 \sigma(c_1)} b_{i_2 \sigma(c_2)} \ldots b_{i_t \sigma(c_t)}) \right)$$

Pero: $$det\left|B\begin{bmatrix} i_1 & i_2 & \ldots & i_t \\ c_1 & c_2 & \ldots & c_t \end{bmatrix}\right| = \sum_{\sigma} sgn(\sigma)(b_{i_1 \sigma(c_1)} b_{i_2 \sigma(c_2)} \ldots b_{i_t \sigma(c_t)})$$

por definición de determinante. Por lo tanto:

$$detM' = \sum_{i_1,i_2,\ldots,i_t=1} a_{r_1 i_1} \ldots a_{r_t i_t} det\left|B\begin{bmatrix} i_1 & i_2 & \ldots & i_t \\ c_1 & c_2 & \ldots & c_t \end{bmatrix}\right|$$

Consideremos la suma $\sum_{i_1,i_2,\ldots,i_t=1}^{n}$. Sabemos que si dos renglones de $B\begin{bmatrix} i_1 & i_2 & \ldots & i_t \\ c_1 & c_2 & \ldots & c_t \end{bmatrix}$ son idénticos, entonces $det\left|B\begin{bmatrix} i_1 & i_2 & \ldots & i_t \\ c_1 & c_2 & \ldots & c_t \end{bmatrix}\right| = 0$. Por lo tanto $det\left|B\begin{bmatrix} i_1 & i_2 & \ldots & i_t \\ c_1 & c_2 & \ldots & c_t \end{bmatrix}\right| = 0$ si los $i_1, \ldots, i_t$ no son distintos.

Así, la suma $\sum_{i_1,i_2,\ldots,i_t=1}^{n}$ podría ser reemplazada por la suma $\sum_{\beta}$ donde β se extiende a todas las permutaciones de $\{i_1, \ldots, i_t\}$ para todas (distintas y no ordenadas) selecciones de $\{i_1, \ldots, i_t\}$ de $\{1, 2, 3, \ldots, n\}$. Estas permutaciones podrían ser agrupadas en $\binom{n}{t}$ conjuntos de $t!$ permutaciones cada una. Por lo que, seleccionando combinaciones, denotadas por $[j_1, \ldots, j_t]$ de $\{1, 2, \ldots, n\}$ se tiene que:

$$detM' = \sum_{[j_1,\ldots,j_t]} \sum_{\rho} a_{r_1 \rho(j_1)} \ldots a_{r_t \rho(j_t)} det\left|B\begin{bmatrix} \rho(j_1) & \rho(j_2) & \ldots & \rho(j_t) \\ c_1 & c_2 & \ldots & c_t \end{bmatrix}\right|$$

donde $\sum_{\rho}$ se extiende a todas las permutaciones ρ de $\{j_1, \ldots, j_t\}$. Después, ordenamos $\{j_1, \ldots, j_t\}$ respecto a la condición de que $1 \le j_1 < j_2 < \ldots < j_n \le n$.

Entonces:

$$det\left|B\begin{bmatrix} \rho(j_1) & \cdots & \rho(j_t) \\ c_1 & \cdots & c_t \end{bmatrix}\right| = sgn(\rho)\, det\left|B\begin{bmatrix} j_1 & \cdots & j_t \\ c_1 & \cdots & c_t \end{bmatrix}\right|$$

Así,

$$detM' = \sum_{[j_1,\ldots,j_t]} \sum_{\rho} sgn(\rho) a_{r_1\rho(j_1)} \ldots a_{r_t\rho(j_t)} det\left|B\begin{bmatrix} j_1 & \cdots & j_t \\ c_1 & \cdots & c_t \end{bmatrix}\right|$$

$$detM' = \sum_{[j_1,\ldots,j_t]} \left(\sum_{\rho} sgn(\rho) a_{r_1\rho(j_1)} \ldots a_{r_t\rho(j_t)}\right) det\left|B\begin{bmatrix} j_1, & \ldots, & j_t \\ c_1, & \ldots, & c_t \end{bmatrix}\right|$$

$$= \sum_{[j_1,\ldots,j_t]} det\left|A\begin{bmatrix} r_1 & \cdots & r_t \\ j_1 & \cdots & j_t \end{bmatrix}\right| det\left|B\begin{bmatrix} j_1 & \cdots & j_t \\ c_1 & \cdots & c_t \end{bmatrix}\right|$$

donde $1 \le j_1 < j_2 < j_3 < \ldots < j_t = n$. ■

Observamos que en la demostración del teorema no se hace uso de m, el número de renglones de A ni de p, el número de columnas de B. Por lo tanto, m y p son arbitrarios.

Suponiendo que $m = n = p = t$, tenemos el siguiente corolario.

Corolario: Para A y B en $(R)_n$,

$$det(AB) = det(A)det(B).$$

Ejemplo:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 4 & 1 \\ 0 & 0 & 2 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 3 \\ 1 & 4 \\ 2 & 1 \end{bmatrix} \qquad M = AB = \begin{bmatrix} 9 & 14 \\ 11 & 32 \\ 4 & 2 \end{bmatrix}$$

Sea $M' = M\begin{bmatrix} r_1 & r_2 \\ c_1 & c_2 \end{bmatrix} = \begin{bmatrix} 9 & 14 \\ 11 & 32 \end{bmatrix}$

$$detM' = A\begin{bmatrix} r_1 & r_2 \\ s_1 & s_2 \end{bmatrix} B\begin{bmatrix} s_1 & s_2 \\ c_1 & c_2 \end{bmatrix} + A\begin{bmatrix} r_1 & r_2 \\ s_1 & s_3 \end{bmatrix} B\begin{bmatrix} s_1 & s_3 \\ c_1 & c_2 \end{bmatrix} + A\begin{bmatrix} r_1 & r_2 \\ s_2 & s_3 \end{bmatrix} B\begin{bmatrix} s_2 & s_3 \\ c_1 & c_2 \end{bmatrix}$$

la suma se extiende sobre 3 selecciones de $\{s_1, s_2\}$ de $\{1,2,3\}$ con $1 \le s_1 \le s_2 \le 3$

$$detM' = det\begin{vmatrix} 1 & 2 \\ 5 & 4 \end{vmatrix} det\begin{vmatrix} 1 & 3 \\ 1 & 4 \end{vmatrix} + det\begin{vmatrix} 1 & 3 \\ 5 & 1 \end{vmatrix} det\begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} + det\begin{vmatrix} 2 & 3 \\ 4 & 1 \end{vmatrix} det\begin{vmatrix} 1 & 4 \\ 2 & 1 \end{vmatrix}$$

$$= (-6)(1) + (-14)(-5) + (-10)(-7) = 134 .$$

Proposición: $det(A^t) = det(A)$.

Demostración:

Sea $A = [a_{ij}]$ en $(R)_n$ y sea $A^t = [b_{ij}]$ donde $b_{ij} = a_{ji}$. Entonces:

$det(A^t) = \Sigma sgn(\sigma) b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{n\sigma(n)}$ donde $b_{i\sigma(i)} = a_{\sigma(i)i}$.

Así, $det(A^t) = \Sigma sgn(\sigma)\, a_{\sigma(1)1}\, a_{\sigma(2)2} \cdots a_{\sigma(n)n}$.

Si $i = \sigma^{-1}(j)$ entonces $a_{\sigma(i)i} = a_{j\sigma^{-1}(j)}$, con lo que:

$a_{\sigma(1)1}\, a_{\sigma(2)2} \cdots a_{\sigma(n)n} = a_{1\sigma^{-1}(1)}\, a_{2\sigma^{-1}(2)} \cdots a_{n\sigma^{-1}(n)}$

Como $\sigma\sigma^{-1}$ es la permutación identidad $(sgn(\sigma))(sgn(\sigma^{-1})) = 1$ ó

$sgn(\sigma^{-1}) = sgn(\sigma)$.

Además como σ varía sobre todas las permutaciones de grado n, también lo hace σ^{-1}.

Por lo tanto,

$det(A^t) = \Sigma sgn(\sigma^{-1}) a_{1\sigma^{-1}(1)}\, a_{2\sigma^{-1}(2)} \cdots a_{n\sigma^{-1}(n)} = det(A)$.

Supongamos que $A = [a_{ij}]$ es una matriz de $n \times m$. Sea $F_k(A)$ el ideal generado por los determinantes de submatrices de $k \times k$ de A, es decir, el ideal generado por todos los menores de orden k, donde $k \le min\{n.m\}$. Definimos $F_0(A) = R$

y $F_k(A) = 0$ para $k > min\{n,m\}$. Entonces F_k es el k-ésimo ideal determinante de A. Observe que:

$$R = F_0(A) \supseteq F_1(A) \supseteq F_2(A) \supseteq \ldots \supseteq 0 = 0 = \ldots$$

Sea $A = [a_{ij}]$ una matriz de $n \times n$ sobre R.

Sea A_{ij} la matriz de $(n\text{-}1)\times(n\text{-}1)$ obtenida de A eliminando el i-ésimo renglón y la j-ésima columna.

Definimos $b_{ij} = (-1)^{i+j} det(A_{ij})$

$B = [b_{ij}]$

y $adj(A) = B^t$. $adj(A)$ es llamada la adjunta de A.

V. Matrices y Polinomios.

Se ha demostrado anteriormente que existe un isomorfismo natural de anillos entre $(R[x])_n$ (las matrices de $n \times n$ sobre el anillo de polinomios $R[x]$) y $(R)_n[x]$, el anillo de polinomios sobre el anillo de matrices $(R)_n$.

Ahora, si x es una indeterminada sobre R y $A = [a_{ij}]$ es una matriz en $(R)_n$ entonces $xI-[a_{ij}]$ está en $(R[x])_n$.

El polinomio $X(A,x) = det|xI-[a_{ij}]|$ es el polinomio característico de A.

El ideal $(X(A,x))$ en $R[x]$ es el ideal característico de A.

Notación: Usaremos el mismo símbolo x para denotar la indeterminada del anillo de polinomios $R[x]$ y del anillo de polinomios $(R)_n[x]$.

Teorema de Cayley-Hamilton:

Sea A una matriz en $(R)_n$. Entonces $X(A,A) = 0$, es decir, A satisface su polinomio característico.

Se darán dos demostraciónes de este teorema. La primera demostración es similar en estilo al método de identidades algebraicas y ha sido atribuida a L. Roberts; sin embargo, una demostración similar ha sido también dada por McCoy en 1939.

Primera Demostración:

Consideremos el siguiente diagrama conmutativo de morfismo de anillos:

$$\begin{array}{ccc} (Z[x_{11}, \ldots, x_{nn}])[x] & \xrightarrow{\alpha} & R[x] \\ \downarrow \gamma & & \downarrow \beta \\ (Z[x_{11}, \ldots, x_{nn}])_n & \xrightarrow[\delta]{} & (R)_n \end{array}$$

tales que:

a) $\alpha: x_{ij} \longmapsto a_{ij}$ donde $A = [a_{ij}]$ y $\alpha: x \longmapsto x$

b) $\delta: x_{ij} \longmapsto a_{ij}$

c) $\beta: x \longmapsto A$

d) $\gamma: x \longmapsto [x_{ij}]$

Sea $f = X([x_{ij}], x)$ el polinomio característico de $[x_{ij}]$ en $(Z[x_{11}, \ldots, x_{nn}])[x]$

$$f = X([x_{ij}], x) = det \begin{vmatrix} x - x_{11} & -x_{12} & \ldots & -x_{1n} \\ -x_{21} & x - x_{22} & \ldots & -x_{2n} \\ \vdots & & & \\ -x_{n1} & -x_{n2} & \ldots & x - x_{nn} \end{vmatrix}$$

Sea $\bar{f} = X(A,x)$ el polinomio característico de A en $R[x]$.

$$\bar{f} = X(A,x) = det \begin{vmatrix} x - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & x - a_{22} & \ldots & -a_{2n} \\ \vdots & & & \\ -a_{n1} & -a_{n2} & \ldots & x - a_{nn} \end{vmatrix}$$

Tenemos que $\alpha(f) = \bar{f}$ y $\bar{f}(A) = \beta(\bar{f}) = \delta\gamma(f)$,

pero $\gamma(f) = f([x_{ij}]) = 0$.

Por lo tanto $\bar{f}(A) = 0$

$$X(A,A) = 0. \blacksquare$$

La segunda demostración involucra morfismos de anillos y al anillo de polinomios no conmutativo $(R)_n[x]$, pero antes se discutirán algunas generalidades.

Supongamos que S es un anillo no conmutativo. Si x es una indeterminada conmutativa, podemos formar de manera estandar, el anillo de polinomios $S[x]$. Sin embargo, si λ está en S, el morfismo de sustitución $S[x] \longrightarrow S[\lambda]$ no está bien definido en general. Esto es porque si $f(x) = \Sigma a_i x^i$ entonces $f(x) = \Sigma x^i a_i$, pero generalmente $\Sigma a_i \lambda^i \neq \Sigma \lambda^i a_i$. Esta dificultad podría ser superada definiendo una sustitución derecha (izquierda) como

$$f_D(\lambda) = \Sigma a_i \lambda^i \qquad (f_I(\lambda) = \Sigma \lambda^i a_i)$$

Sin embargo surge otro problema. El mapeo $S[x] \longrightarrow S[\lambda]$ definido por $f(x) \longrightarrow f_D(\lambda)$, aún no es un morfismo de anillos. La dificultad es con la multiplicación. Para ilustrarlo, supongamos que $f(x) = \Sigma a_i x^i$ y $g(x) = \Sigma b_j x^j$. Entonces $h(x) = f(x)g(x) = \Sigma c_k x^k$ donde los coeficientes c_k están dados por el producto de convolución $c_k = \sum_{i+j=k} a_i b_j$. Por lo tanto $h_D(\lambda) = \sum_k \left(\sum_{i+j} (a_i b_j) \lambda^k \right)$. Por otro lado, $f_D(\lambda) g_D(\lambda) = (\Sigma a_i \lambda^i)(\Sigma b_j \lambda^j)$ que generalmente no es igual a $h_D(\lambda)$.

Afortunadamente, en muchas ocasiones la generalidad de la situación anterior no ocurre. Usualmente surgen dos tipos de morfismos:

Primero. Si R y S son anillos no necesariamente conmutativos y $\sigma: S \longrightarrow R$ es un morfismo de anillos, entonces σ se levanta a un morfismo de anillos

$$\bar{\sigma}: (S)_n \longrightarrow (R)_n, \quad \text{dado por:} \quad \bar{\sigma}([s_{ij}]) = [\sigma(s_{ij})]$$

Por ejemplo, la función δ en la demostración anterior es de este tipo.

Segundo. Usualmente estamos tratando no con $(R)_n[x]$ sino con una matriz A y con el subanillo conmutativo $R[A] = \{\Sigma a_i A^i \mid a_i \in R\}$ (R conmutativo) de $(R)_n$. Aquí por ejemplo, el morfismo de anillos

$$R[x] \longrightarrow R[A] \quad \text{dado por:}$$
$$x \longmapsto A$$

sí tiene sentido. Los mapeos β y γ de la demostración anterior son precisamente de este tipo.

Ahora comenzamos con los preliminares de la segunda demostración del Teorema de Cayley-Hamilton. La técnica es clásica y utiliza el algoritmo de la división para $(R)_n[x]$.

Recordamos de la sección I, que para un anillo conmutativo R, si f y g son polinomios en $R[x]$ donde el coeficiente principal de f es una unidad, entonces existen polinomios únicos q y r con $g = qf + r$ y grado(r) < grado(f) ó r=0. De este algoritmo de la división, es fácil deducir el teorema de factor, es decir, a es un cero de un polinomio si y sólo si x-a es un factor. Pero siendo a un cero de un polinomio es un resultado del morfismo de sustitución y hemos indicado

arriba las dificultades para $(R)_n[x]$ (no conmutativo) y el morfismo de sustitución.

Sea $f(x) = A_0 + A_1x + \ldots + A_mx^m$ un polinomio en $(R)_n[x]$. Diremos que f es regular si A_m es una matriz invertible. Una demostración análoga a la demostración usual del algoritmo de la división para $R[x]$ dará un algoritmo derecho e izquierdo de la división. Precisando, sean f y g en $(R)_n[x]$ con f regular. Entonces existen polinomios únicos q_1, q_2, r_1 y r_2 en $(R)_n[x]$ que satisfacen

$$g = q_1 f + r_1 \quad \text{y} \quad g = fq_2 + r_2$$

donde grado(r_i) < grado(f) ó $r_i = 0$ para $i = 1,2$. Nos referiremos a esto como el algoritmo de la división para $(R)_n[x]$.

Supongamos que $g(x) = B_0 + B_1x + \ldots + B_mx^m$ en $(R)_n[x]$ y A está en $(R)_n$. Observamos que:

$$x^1 - A^1 = (x - A)$$

$$x^2 - A^2 = (x + A)(x - A)$$

$$x^3 - A^3 = (x^2 + xA + A^2)(x - A)$$

$$x^4 - A^4 = (x^3 + x^2A + xA^2 + A^3)(x - A)$$

$$\vdots$$

$$x^i - A^i = (x^{i-1} + x^{i-2}A + \ldots + A^{i-1})(x - A)$$

Multiplicamos ambos lados de la identidad por B_i para $i = 1, 2, \ldots, m$

$$B_1(x^1 - A^1) = B_1(x - A)$$

$$B_2(x^2 - A^2) = B_2(x + A)(x - A)$$

$B_3(x^3 - A^3) = B_3(x^2 - xA + A^2)(x - A)$

$\vdots$

$B_i(x^i - A^i) = B_i(x^{i-1} + x^{i-2}A + \ldots + A^{i-1})(x - A)$

Sumamos las ecuaciones resultantes y obtenemos:

$$\sum_{i=1}^{m} B_i x^i - \sum_{i=1}^{m} B_i A^i = |Q(x-A)| \quad \text{donde } Q \in (R)_n[x].$$

Empleando la sustitución derecha $g_D(A) = B_0 + B_1 A + \ldots + B_m A^m$, la ecuación (1) se convierte en:

$$g(x) = Q(x - A) + g_D(A)$$

Un cálculo similar nos da $g_I(A)$ y la ecuación (1) se convierte en:

$$g(x) = Q(x - A) + g_I(A).$$

Esto nos lleva al siguiente teorema:

Teorema generalizado de Bézout.

Sean $g(x) = \sum_{i=0}^{m} B_i x^i$ en $(R)_n[x]$ y A en $(R)_n$. Entonces:

$$g(x) = Q_D(x-A) + g_D(A), \quad g(x) = Q_I(x-A) + g_I(A)$$

donde Q_D y Q_I están en $(R)_n[x]$ y

$$g_D(A) = \sum_{i=0}^{m} B_i A^i, \qquad g_I(A) = \sum_{i=0}^{m} A^i B_i$$

además Q_D, g_D y Q_I, g_I son únicos.

Demostración:

Sabemos que $B_i(x^i - A^i) = B_i(x^{i-1} + x^{i-2}A + \ldots + A^{i-1})(x - A)$

$\sum_{i=0}^{m} B_i x^i - \sum_{i=0}^{m} B_i A^i = Q_D(x-A)$ donde $Q_D \in (R)_n[x]$

Como $g_D(A) = \sum_{i=0}^{m} B_i A^i$, entonces $g(x) = Q_D(x-A) + g_D(A)$.

Análogamente, $(x^i - A^i)B_i = (x-A)(x^{i-1} + x^{i-2}A + \ldots + A^{i-1})B_i$

$\sum_{i=0}^{m} x^i B_i - \sum_{i=0}^{m} A^i B_i = (x-A)Q_I$ donde $Q_I \in (R)_n[x]$

Como $g_I(A) = \sum_{i=0}^{m} A^i B_i$, entonces $g(x) = (x-A)Q_I + g_I(A)$.

Q_D, g_D, Q_I, g_I son únicos por la unicidad del algoritmo de la división para $(R)_n[x]$. ■

En este teorema, $(R)_n$ podría ser remplazado por un anillo no conmutativo S y el resultado también se cumple.

Segunda demostración del Teorema de Cayley-Hamilton.

Sea A una matriz en $(R)_n$ y $X(A,x)$ su polinomio caracteristico.

Sea $X(A,x) = B_0 + B_1x + \ldots + B_mx^m \in (R)_n[x]$.

Dividimos por la derecha al polinomio $X(A,x)$ en $(R)_n[x]$ por $(x-A)$. Por la discusión anterior, tenemos que:

$$X(A,x) = Q(x-A) + X(A,A) \text{ donde } Q \in (R)_n[x]$$

Por otro lado, $X(A,x) = (adj(x-A))(x-A)$.

Por el algoritmo de la división y la unicidad del cociente y el residuo, tenemos que:

$$Q = adj(x-A) \quad \text{y} \quad X(A,A) = 0$$

Sea A en $(R)_n$. Hemos estudiado a A estudiando al anillo $R[A]$ que A genera en $(R)_n$. A su vez, nos hemos aproximado a $R[A]$, examinando el anillo de polinomios $R[x]$ y el morfismo de sustitución $R[x] \longrightarrow R[A]$ dado por

$x \longmapsto A$. El Kernel de este morfismo de sustitución es llamado el ideal de relaciones satisfechas por A y denotado por $I(A)$, es decir,

$$I(A) = \{f \in R[x] \mid f(A) = 0\}$$

Ahora nuestro propósito es determinar $I(A)$. La caracterización de $I(A)$ se debe a McCoy en 1939.

Recordemos que si S es un anillo conmutativo y J e I son ideales de S, entonces el ideal cociente de I y J es:

$$(I:J) = \{ s \in S \mid sJ \subseteq I\}$$

En particular, $(0:J)$ es el anulador de J.

Además, si $J = (f)$ es un ideal principal, entonces $(I:J)$ es denotado por $(I:f)$.

En la sección IV definimos los ideales determinantes de una matriz de $n \times n$. El $(n\text{-}1)$ ideal determinante de $X\text{-}A$, $F_{n-1}(X\text{-}A)$, es el ideal generado por los determinantes de las matrices de $(n\text{-}1)\times(n\text{-}1)$ de $X\text{-}A$.

El resultado de McCoy es que el ideal de relaciones satisfecho por A es precisamente el ideal cociente de $(X(A,x))$ y el $(n\text{-}1)$ ideal determinante de $X\text{-}A$.

Teorema de McCoy.

Sea $A \in (R)_n$. Entonces:

$I(A) = (X(A,x): F_n(X\text{-}A))$ en $R[x]$.

Demostración:

Sea $g(x) \in (X(A,x): F_n(x\text{-}A))$. Entonces $g(x)F_n(x\text{-}A) \subset X(A,x)$.

Los generadores de $F_n(x\text{-}A)$ son precisamente los elementos de $adj(x\text{-}A)$. Por lo que si $adj(x\text{-}A) = [f_{ij}(x)]$ entonces:

$$g(x)\, adj(x\text{-}A) = [g(x)f_{ij}(x)] = X(A,x)M, \quad \text{donde } M \in (R)_n[x].$$

Multiplicando por la izquierda por $x\text{-}A$, tenemos:

$$(x\text{-}A)g(x)\, adj(x\text{-}A) = (x\text{-}A)[g(x)f_{ij}(x)] = (x\text{-}A)X(A,x)M$$

$$g(x)X(A,x)I = X(A,x)(x\text{-}A)M$$

Como el coeficiente principal de $X(A,x)$ es uno, $X(A,x)$ no es un divisor de cero en $R[x]$ y $g(x) = (x\text{-}A)M$

$$g(A) = 0$$

Así, $g(x) \in I(A)$.

Reciprocamente, supongamos que $g(x) \in I(A)$, es decir, $g(A) = 0$. Entonces por el teorema del factor, $g(x) = (x\text{-}A)G(x)$ donde $G(x) \in (R)_n[x]$.

Multiplicando por $adj(x\text{-}A)$ se obtiene:

$$g(x)\, adj(x\text{-}A) = (x\text{-}A)\, adj(x\text{-}A)\, G(x)$$

$$= X(A,x)\, G(x)$$

por lo tanto, si $adj(x\text{-}A) = [f_{ij}(x)]$ entonces $g(x)f_{ij}(x) \in (X(A,x))$.

Como los $f_{ij}(x)$, $1 \le i,j \le n$, generan a $F_{n-1}(x\text{-}A)$, entonces:

$$g(x) \in (X(A,x):F_{n-1}(x\text{-}A)). \quad \blacksquare$$

VI. Sistemas de Ecuaciones Lineales.

Uno de los problemas más antiguos del álgebrea lineal fue la solución de ecuaciones lineales y de sistemas de ecuaciones lineales, sobre los racionales y los enteros.

Esta sección examina las soluciones $x_1, \ldots, x_n$ en un anillo conmutativo R de un sistema de ecuaciones lineales

$$a_{11}x_1 + \ldots + a_{1n}x_n = b_1$$
$$\vdots$$
$$a_{m1}x_1 + \ldots + a_{mn}x_n = b_m$$

donde los a_{ij} y b_i, $1 \le i \le m$, $1 \le j \le n$, están en R.

Sean $X = [x_1, \ldots, x_n]^t$, $B = [b_1, \ldots, b_m]^t$ y $A = [a_{ij}]$, el sistema anterior podría ser escrito en forma matricial como:

$$AX = B$$

Si $m > n$, podríamos introducir las variables $x_{n+1}, \ldots, x_m$ y definir $a_{ij} = 0$ para $1 \le i \le m$, $n+1 \le j \le m$. En consecuencia, podemos suponer sin pérdida de generalidad que $m \le n$ siempre que esto sea conveniente.

Para ilustrar el tratamiento de ideales determinantes que utilizamos, supongamos que A es una matriz cuadrada de tamaño n. Sea A_{ij} la submatriz de A que se obtiene eliminandio el renglón i y la columna j. Entonces de la fórmula de la adjunta se obtiene:

$$adj(A)AX = adj(A)B$$

$$det(A)IX = adj(A)B$$

$$det(A)\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} (-1)^2 \det(A_{11}) & \dots & (-1)^{m+1}\det(A_{m1}) \\ \vdots & & \\ (-1)^{1+n} \det(A_{1n}) & \dots & (-1)^{m+n}\det(A_{mn}) \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

$$= \begin{bmatrix} \sum_{j=1}^{n} (-1)^{j+1}\det(A_{j1})b_j \\ \vdots \\ \sum_{j=1}^{n} (-1)^{j+n}\det(A_{jn})b_j \end{bmatrix}$$

Esto es,

$$det(A)x_i = \sum_{j=1}^{n} (-1)^{j+i} det(A_{ji})b_j = \sum_{j=1}^{n} c_{ji}b_j = \sum_{j=1}^{n} b_j c_{ji} = detM_i$$

donde c_{ji} es el cofactor de a_{ji} y $\Sigma b_j c_{ji}$ es la expansión de la matriz M_i sobre la i-ésima columna.

$$det(A)x_i = detM_i = det\begin{bmatrix} a_{11}\dots a_{1i-1}b_1 a_{1i+1}\dots a_{1n} \\ \vdots \\ a_{n1}\dots a_{ni-1}b_n a_{ni+1}\dots a_{nn} \end{bmatrix}$$

para $1 \le i \le n$. En particular, si $det(A)$ es una unidad, entonces se podrá resolver de manera única para x_i, $1 \le i \le n$. La técnica anterior es llamada la Regla de Cramer o Método de Cramer.

Ahora se extenderá para el caso $m \times n$. Recordemos que anteriormente se definió a $F_t(A)$ como el ideal generado por todos los determinantes de las submatrices de $t \times t$ de A. $F_t(A)$ es el t-ésimo ideal determinante de A.

Teorema: Consideremos un sistema de ecuaciones $AX = B$ donde A es una matriz de $m \times n$. Si este sistema tiene una solución entonces los ideales determinantes de A son los mismos que los ideales determinantes de la matriz aumentada $[A,B]$.

Demostración:

Como las submatrices de A son también submatrices de $[A,B]$, tenemos que:

$$F_t(A) \subseteq F_t([A,B])$$

Ahora es necesario mostrar que $F_t([A,B]) \subseteq F_t(A)$, para lo cual se examinarán los generadores de $F_t(A)$ si éstos no involucran elementos de B. Consideraremos este caso. Como $AX = B$ tiene una solución, existen $x_1, \ldots, x_n$ en R con el i-ésimo renglón igual a:

$$(a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{it}x_t) + a_{it+1}x_{t+1} + \ldots + a_{in}x_n = b_i$$

Entonces,

$$\sum_{j=1}^{t} a_{ij}x_j = b_i - \sum_{j=t+1}^{n} a_{ij}x_j \quad \text{para } 1 \le i \le t$$

Sea $T_1 = det\bar{A}$ donde $\bar{A} = [a_{ij}]$ $1 \le i,j \le t$

Sea $L = det\,|[b_i,a_{ij}]| = det \begin{vmatrix} b_1 & a_{12} & a_{13} & \ldots & a_{1t} \\ b_2 & a_{22} & a_{23} & \ldots & a_{2t} \\ \vdots & & & & \\ b_t & a_{t2} & a_{t3} & \ldots & a_{tt} \end{vmatrix}$

$1 \le i \le t$, $2 \le j \le t$ y para $k = t+1, \ldots, m$ sea $T_k = det\,|[a_{ij}]|$ $1 \le i \le t$, $j = k, 2, 3, \ldots, t$ donde:

$$T_l = \begin{bmatrix} a_{1l} & a_{12} & a_{13} & \ldots & a_{1t} \\ a_{2l} & a_{22} & a_{23} & \ldots & a_{2t} \\ \vdots & & & & \\ a_{tl} & a_{t2} & a_{t3} & \ldots & a_{tt} \end{bmatrix} \qquad t+1 \le l \le m$$

Por el método de Cramer.

$$adj(\bar{A})\bar{A}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{bmatrix} = adj(\bar{A})\left(\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{bmatrix} - \sum_{j=t+1}^{n}\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{tj} \end{bmatrix} x_j\right)$$

$$det(\bar{A})I\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{bmatrix} = adj(\bar{A})\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{bmatrix} - adj(\bar{A})\sum_{j=t+1}^{n}\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{tj} \end{bmatrix} x_j$$

$$T_1\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{t}(-1)^{j+1}\det(A_{j1})b_j \\ \sum_{j=1}^{t}(-1)^{j+2}\det(A_{j2})b_j \\ \vdots \\ \sum_{j=1}^{t}(-1)^{j+t}\det(A_{jt})b_j \end{bmatrix} - \sum_{j=t+1}^{n} adj(A)\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{tj} \end{bmatrix} x_j$$

$$T_1\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{t}(-1)^{j+1}\det(A_{j1})b_j \\ \sum_{j=1}^{t}(-1)^{j+2}\det(A_{j2})b_j \\ \vdots \\ \sum_{j=1}^{t}(-1)^{j+t}\det(A_{jt})b_j \end{bmatrix} - \sum_{j=t+1}^{n}\begin{bmatrix} \sum_{k=1}^{t}(-1)^{k+1}\det(A_{k1})a_{kj} \\ \sum_{k=1}^{t}(-1)^{k+2}\det(A_{k2})a_{kj} \\ \vdots \\ \sum_{k=1}^{t}(-1)^{k+t}\det(A_{kt})a_{kj} \end{bmatrix} x_j$$

que da como primer renglón:

$$T_1x_1 = \sum_{j=1}^{t}(-1)^{j-1}det(A_{j1})b_j - \sum_{j=t+1}^{n}\left(\sum_{k=1}^{t}(-1)^{k-1}det(A_{k1})a_{kj}\right)x_j$$

$$= \sum_{j=1}^{t} c_{j1} b_j - \sum_{j=t+1}^{n} \left(\sum_{k=1}^{t} c_{k1} a_{kj} \right) x_j$$

$$= \sum_{j=1}^{t} b_j c_{j1} - \sum_{j=t+1}^{n} \left(\sum_{k=1}^{t} a_{kj} c_{k1} \right) x_j$$

$$= L - \sum_{j=t+1}^{n} \begin{bmatrix} a_{1\,t+1} & a_{12} & \dots & a_{1t} \\ & & \vdots & \\ a_{t\,t+1} & a_{2t} & \dots & a_{tt} \end{bmatrix} x_j$$

$$T_1 x_1 = L - \sum_{j=t+1}^{n} T_j x_j$$

Por lo tanto L (un generador de $F_t([A,B])$) es una combinación R-lineal de generadores de $F_t(A)$. El teorema se obtiene permutando los renglones y las columnas de A y aplicando el argumento anterior. ■

La condición del teorema anterior no es suficiente para asegurar una solución de $AX = B$. Camion. Levy y Mann han dado un ejemplo donde los ideales determinantes de A y los de la matriz aumentada $[A.B]$ coinciden para toda t, pero $AX = B$ no tienen solución.

El método de Cramer indica que la existencia de una solución depende en parte de la acción de $det(A)$ y de los menores de A sobre las x_i, $1 \le i \le n$. Esto ha dado origen a dos tipos de "rango" de una matriz.

Decimos que el rango de una matriz A de $m \times n$, $rank(A)$, es el entero no negativo más grande t tal que $F_t(A) \neq 0$. Recordamos que $F_t(A) = 0$ para $t > min\{m,n\}$. Por lo tanto, $0 \le rank(A) \le min\{m,n\}$.

El rango de McCoy de una matriz A de $m \times n$, es el entero más grande t tal que $A_{nn_R}(F_t(A)) = 0$ donde $A_{nn_R}(F_t(A)) = \{r \in R \mid rF_t(A) = 0\}$.

Sea A una matriz de $m \times n$. Consideremos la ecuación $AX = B$. Supondremos que $m \leq n$. Suponemos que el rango de McCoy es igual a m, sea F_m^* el ideal generado por todos los determinantes de las submatrices de $m \times m$ de $[A,B]$ que no son submatrices de A.

Teorema: (Camion, Levy, Mann)

Sea A una matriz de $m \times n$ donde $m \leq n$ y el rango de McCoy es igual a m. Si para algún ideal Q y algún α no divisor de cero se tiene:

$$QF_m(A) \supseteq (\alpha) \supseteq QF_m^* \quad ,$$

entonces $AX = B$ tiene solución.

Demostración:

Supongamos que $A = [a_{ij}]$.

Como el rango de McCoy es igual a m, existe un determinante distinto de cero

$$T^{(1)} = det\begin{bmatrix} a_{11} \dots a_{1m} \\ a_{m1} \dots a_{mm} \end{bmatrix} \neq 0$$

$$T^{(1)}\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{m} a_{1j}x_j^{(1)} \\ \sum_{j=1}^{m} a_{2j}x_j^{(1)} \\ \vdots \\ \sum_{j=1}^{m} a_{mj}x_j^{(1)} \end{bmatrix}$$

Lo que implica que $T^{(1)}b_i = \sum_{j=1}^{m} a_{ij}x_j^{(1)}$ donde $x_j^{(1)} \in F_m^*$, $1 \leq i \leq m$.

Haciendo $x_{m+1}^{(1)} = \ldots = x_n^{(1)} = 0$

$$T^{(1)} b_i = \sum_{j=1}^{n} a_{ij} x_j^{(1)} \qquad (1 \le i \le m)$$

Sean $T^{(1)} \ldots T^{(t)}$ los determinantes distintos de cero de submatrices de $m \times m$ de A. Como se hizo anteriormente se puede obtener las siguientes ecuaciones.

$$\sum_{j=1}^{n} a_{ij} x_j^{(s)} = T^{(s)} b_i \qquad 1 \le s \le t, \quad 1 \le i \le m.$$

donde cada $x_j^{(s)}$ está en F_m^*, y

$$\bar{A} = \begin{bmatrix} a_{11} \ldots a_{1m} \\ a_{m1} \ldots a_{mm} \end{bmatrix}$$

Entonces:

$$T^{(1)} = det(\bar{A}) I = \bar{A} adj(\bar{A})$$

$$T^{(1)} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = det(\bar{A}) \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \bar{A} adj(\bar{A}) \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

$$T^{(1)} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = det(\bar{A}) \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \bar{A} \left(adj\left(\bar{A}\right) \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_{11} \ldots a_{1m} \\ a_{m1} \ldots a_{mm} \end{bmatrix} \begin{bmatrix} \sum_{j=1}^{m} (1)^{j+1} \det A_{j1} b_j \\ \sum_{j=1}^{m} (1)^{j+m} \det A_{jm} b_j \end{bmatrix} = \begin{bmatrix} a_{11} \ldots a_{1m} \\ a_{21} \ldots a_{2m} \\ \vdots \\ a_{m1} \ldots a_{mm} \end{bmatrix} \begin{bmatrix} x_1^{(1)} \\ x_2^{(1)} \\ \vdots \\ x_m^{(1)} \end{bmatrix}$$

donde $x_j^{(1)} \in Fm^*$.

Como $(\alpha) \subseteq QF_m(A)$, existen $q_1, \ldots, q_t \in Q$ tales que $\sum_{s=1}^{t} q_s T^{(s)} = \alpha$.

$$\sum_{s=1}^{t} q_s T^{(s)} = \alpha$$

$$\sum_{s=1}^{t} q_s T^{(s)} b_i = \alpha b_i$$

$$\sum_{s=1}^{t} q_s \sum_{j=1}^{n} a_{ij} x_j^{(s)} = \alpha b_i$$

$$\sum_{s=1}^{t} \sum_{j=1}^{n} a_{ij} q_s x_j^{(s)} = \alpha b_i$$

$$\sum_{j=1} a_{ij} (\Sigma q_s x_j^{(s)}) = \alpha b_i, \qquad x_j^{(s)} \in F_m^*$$

Como $q_s x_j^{(s)} \in QF_m^* \subset (\alpha)$ entonces para alguna $\bar{x}_j$

$$\sum_{s=1}^{t} q_s x_j^{(s)} = \alpha \bar{x}_j .$$

Como α no divide a cero, se divide por α y se obtiene una solución

$$\sum_{j=1}^{n} a_{ij} \bar{x}_j = b_i .$$

Una aplicación del teorema anterior es dada por el siguiente corolario.

Supongamos que para un anillo conmutativo R, el m-ésimo ideal determinante de una matriz A de $m \times n$ es R, es decir, los $m \times m$ determinantes de A generan a R. Entonces claramente el rango de McCoy de A es igual a m y $F_m(A) = R = (1) \supset F_m^*$ donde $Q = (1)$. Esto da el siguiente resultado:

Corolario: Sea A una matriz de $m \times m$. Si $F_m(A) = R$ entonces $AX = B$ tiene solución.

Teorema (McCoy)

Sea A una matriz de $m \times n$ sobre R. La ecuación matricial $AX = 0$ tiene una solución no trivial $X = [x_1, \ldots, x_n]^t$ si y solo si el rango de McCoy de A es menor que n.

Demostración:

Supongamos que $AX = 0$ tiene una solución no trivial.

Supongamos $X = [\bar{x}_1, \ldots, \bar{x}_n]^t$ con $\bar{x}_i \in R$ y como alguna de las $\bar{x}_i$ es distinta de cero, podemos afirmar sin pérdida de generalidad que $\bar{x}_1 \neq 0$.

Se afirma que $A_{nn_R}(F_n(A)) \neq 0$. Se demostrará que al menos tiene un elemento $\neq 0$.

Si $n > m$ entonces $F_n(A) = 0$ por lo que $A_{nn_R}(F_n(A)) = R$.

Podemos suponer que $n \leq m$.

Sea D el determinante de la submatriz $T = \begin{bmatrix} a_{11} \ldots a_{1n} \\ \vdots \\ a_{n1} \ldots a_{nn} \end{bmatrix}$

$$D\bar{x}_1 = 0 \text{ ya que } T\bar{x} = 0$$

$$D\bar{x} = (adj(T))T\bar{x} = 0$$

Similarmente, si D es el determinante de cualquier submatriz de $n \times n$ de A, entonces $D\bar{x}_1 = 0$. Por lo tanto, $\bar{x}_1$ está en $A_{nn}(F_n(A))$.

Por lo tanto el Rango de McCoy $(A) < n$.

Supongamos que el Rango de McCoy $(A) = t$ y $t < n$.

$A_{nn_R}(F_{t-1}(A)) \neq 0$

Existe $y \in R$ con $y \neq 0$ y $F_{t-1}(A)y = 0$

Si $t = 0$ entonces $F_1(A)y = 0$.

$F_1(A)$ es el ideal generado por los determinantes de 1×1 que son las entradas de la matriz $[a_{ij}]$.

Por lo tanto $a_{ij}y = 0$ para toda a_{ij}, entonces $x_i = y$ para $1 \leq i \leq n$ da una solución no trivial.

Supongamos que $t > 0$. Entonces el producto de y y algún generador de $F_t(A)$ es diferente de cero.

Este generador es el determinante de alguna submatriz de $t \times t$ de A. Permutando renglones y columnas, podemos suponer que es la submatriz T donde

$$T = \begin{vmatrix} a_{11} & \cdots & a_{1t} \\ \vdots & & \vdots \\ a_{t1} & & a_{tt} \end{vmatrix} \qquad \text{y} \quad A = [a_{ij}].$$

Consideremos la submatriz

$$T = \begin{vmatrix} a_{11} & \cdots & a_{1t+1} \\ \vdots & & \vdots \\ a_{t+1} & & a_{t+1\,t+1} \end{vmatrix}$$

de $t+1 \times t+1$.

Para $1 \leq i \leq t+1$, sea D_i el determinante de la submatriz T obtenida de eliminar el renglón $t+1$ y la columna i.

Sea $e_i = (-1)^{(t+1)+i} D_i$

Hagamos $\bar{x}_i = ye_i$. $\qquad (1 \leq i \leq t+1)$

$\bar{x}_i = 0 \qquad (t+2 \leq i \leq n)$

Si $\bar{x} = [\bar{x}_1, \ldots, \bar{x}_n]^t$ enonces:

$$AX = \begin{bmatrix} \sum_{j=1}^{n} a_{1j}\bar{x}_j \\ \sum_{j=1}^{n} a_{2j}\bar{x}_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj}\bar{x}_j \end{bmatrix} = \begin{bmatrix} \left(\sum_{j=1}^{t+1} a_{1j}e_j\right)y \\ \left(\sum_{j=1}^{t+1} a_{2j}e_j\right)y \\ \vdots \\ \left(\sum_{j=1}^{t+1} a_{mj}e_j\right)y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

ya que $\sum_{j=1}^{t+1} a_{ij}e_j = 0$ para $1 \le i \le t$

y $\left(\sum_{j=1}^{t+1} a_{ij}e_j\right)y = 0$ para $t+1 \le i \le m$

ya que y está en el $A_{nn_R}(F_{t-1}(A))$ y $\sum_{j=1}^{t+1} a_{ij}e_j$ es un generador de $F_{t-1}(A)$, es decir, es un determinante de una submatriz de $(t+1)\times(t+1)$ de A.

Finalmente, $\bar{x} \neq 0$ puesto que $\bar{x}_{t+1} = ye_{t+1} = y\,det(T) \neq 0$.

Lo anterior muestra que si el rango de McCoy es menor que n. entonces $AX = 0$ tiene una solución no trivial.

Supongamos que $AX = 0$ tiene una solución no trivial, y supongamos que $X = [\bar{x}_1, \ldots, \bar{x}_n]^t$ con $\bar{x}_i$ en R y como alguna de las $\bar{x}_i$ es distinta de cero podemos afirmar sin pérdida de generalidad que $\bar{x}_1 \neq 0$.

Se afirma que $A_{nn_R}(F_n(A)) \neq 0$. Se demostrará que al menos tiene un elemento $\neq 0$.

Si $n > m$ entonces $F_n(A) = 0$ y por lo tanto $A_{nn_R}(F_n(A)) = R$. Podemos suponer que $n \le m$.

Sea D el determinante de la submatriz

$$T = \begin{bmatrix} a_{11} \dots a_{1n} \\ \vdots \\ a_{n1} \dots a_{nn} \end{bmatrix}$$

Entonces $D\bar{x}_i = 0$, ya que $T\bar{x} = 0$ implica que $D\bar{x} = adj(T)T\bar{x} = 0$.

Similarmente, si $\bar{D}$ es el determinante de cualquier submatriz de $n \times n$ de A, entonces $\bar{D}\bar{x}_i = 0$. Por lo tanto $\bar{x}_i$ está en $A_{nn_R}(F_n(A))$. Esto completa la demostración. ■

Corolario:

El sistema

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= 0 \\ \vdots \qquad\qquad & \quad \vdots \\ a_{n1}x_1 + \dots + a_{nn}x_n &= 0 \end{aligned}$$

tiene una solución no trivial si y sólo si el $det[a_{ij}]$ es un divisor de cero en R.

BIBLIOGRAFIA

Burton, David M.
A first course in Rings and Ideals.
Addison-Wesley Publishing Company, 1970.

Friedberg, Insel, Spence.
Algebra Lineal.
Publicaciones Cultural, S.A.

Gilmer, Robert.
On Polynomial and Power Series Rings over a Commutative Ring.
Rocky Mountain Journal of Mathematics.
Vol. 5. 1975.

Hoffman, K., Kunze, R.
Algebra Lineal.
Prentice Hall Hispanoamericana, México, 1973.

Kurosh, A. G.
Curso de Algebra Superior.
Editorial MIR, URSS, 1977.

Lang, Serge.
Algebra Lineal.
Fondo Educativo Interamericano, México, 1976.

MacLane, S., Birkoff, G.
Algebra.
Macmillan Publishing, New York, 1979.

Mc Coy, Neal Henry.
Rings and Ideals.
Mathematical Association of America, Washington, D.C., 1948.

Mc Donald, Bernard R.
Linear Algebra over Commutative Rings.
Marcel Dekker, Inc. New York, 1984.

FE DE ERRATAS

Al final de la demostración de la página 30 , se debe incluir la siguiente proposición:

Proposición: Sea R un anillo conmutativo y R[x] el anillo de polinomios. Entonces existe un isomorfismo natural de los siguientes anillos: $(R[x])_n \cong (R)_n[x]$.

Demostración:

Sean $f_{ij}(x) = \sum_{k=0}^{nij} a_{k(ij)}\, x^k$ y $g_{ij}(x) = \sum_{k=0}^{nij} b_{k(ij)}\, x^k$ en R[x] y definimos $\varphi : [f_{ij}(x)] \mapsto \sum_{k=0}^{n} [a_{k(ij)}]\, x^k$

donde $n = \max\{n_{ij}\}$, $a_{k(ij)}$ en R, $1 \le i,j \le n$, $0 \le k \le n$.

$\varphi(f+g) = \varphi([f_{ij}(x)] + [g_{ij}(x)]) = \varphi([h_{ij}(x)])$

donde $h_{ij}(x) = f_{ij}(x) + g_{ij}(x) = \sum_{k=0}^{nij} a_{k(ij)}\, x^k + \sum_{k=0}^{nij} b_{k(ij)}\, x^k = \sum_{k=0}^{n} (a_{k(ij)} + b_{k(ij)})\, x^k = \sum_{k=0}^{n} c_{k(ij)}\, x^k$

$\varphi([h_{ij}(x)]) = \sum_{k=0}^{n} [c_{k(ij)}]\, x^k = \sum_{k=0}^{n} [a_{k(ij)} + b_{k(ij)}]\, x^k = \sum_{k=0}^{n} [a_{k(ij)}]\, x^k + \sum_{k=0}^{n} [b_{k(ij)}]\, x^k = \varphi(f) + \varphi(g)$.

$\varphi(f \cdot g) = \varphi([f_{ij}(x)] \cdot [g_{jp}(x)]) = \varphi([h_{ip}(x)])$

donde $h_{ip}(x) = \sum_{j=1}^{n} f_{ij}(x) \cdot g_{jp}(x) = \sum_{j=1}^{n} \left(\left(\sum_{k=0}^{nij} a_{k(ij)}\, x^k \right) \left(\sum_{k=0}^{mjp} b_{k(jp)}\, x^k \right) \right) = \sum_{t=0}^{r} c_{t(ip)}\, x^t$, $r = n_{ij} + m_{jp}$

$\varphi([h_{ip}(x)]) = \varphi\left(\left[\sum_{t=0}^{r} c_{t(ip)}\, x^t \right] \right) = \sum_{t=0}^{r} [c_{t(ip)}]\, x^t$ donde $c_{t(ip)} = \sum_{s=0}^{t} [a_{s(ij)}][b_{t-s(jp)}]$,

$= \sum_{k=0}^{n} [a_{k(ij)}]\, x^k \cdot \sum_{k=0}^{n} [b_{k(jp)}]\, x^k = \varphi([f_{ij}(x)]) \cdot \varphi([g_{jp}(x)]) = \varphi(f) \cdot \varphi(g)$.

Supongamos $\varphi([f_{ij}(x)]) = \varphi([f'_{ij}(x)])$

$\sum_{k=0}^{n} [a_{k(ij)}]\, x^k = \sum_{k=0}^{n} [a_{k(ij)}]\, x^k$ *dos polinomios son iguales si sus correspondientes coeficientes son iguales*

$[a_{k(ij)}] = [a_{k(ij)}]$ *para toda k en* $\{0, 1, \ldots, n\}$

$f_{ij}(x) = f'_{ij}(x)$ *para toda* (i,j)

donde $f_{ij}(x) = \sum_{k=0}^{nij} a_{k(ij)}\, x^k$ y $f'_{ij}(x) = \sum_{k=0}^{nij} a_{k(ij)}\, x^k$

por lo tanto $[f_{ij}(x)] = [f'_{ij}(x)]$. ■