ANILLOS DE POLINOMIOS, ISOMORFOS

Por:

ROSA ANTONIA FRANCO ARBELAEZ

Trabajo presentado como requisito parcial para promoción a la categoría de Profesora Asociada.

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE MEDELLIN
DEPTO. DE BIBLIOTECAS
BIBLIOTECA "EFE" GOMEZ

FACULTAD DE CIENCIAS

DEPARTAMENTO DE MATEMATICAS

Julio de 1989

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL

UNAL-Medellín
6 4000 00060244 4

512.4
F71

CONTENIDO

	Pág.
INTRODUCCION	1
0. RADICAL DE JACOBSON DE ANILLOS DE POLINOMIOS....	4
1. ANILLOS INVARIANTES Y FUERTEMENTE INVARIANTES.....	17
2. LA IMAGEN DE X BAJO SOBREYECCIONES	19
3. UNIDADES DE UN ANILLO DE POLINOMIOS, A[X]	28
4. DOMINIOS FUERTEMENTE INVARIANTES	53
BIBLIOGRAFIA	60

UNIVERSIDAD NACIONAL
30288
BIBLIOTECA CENTRAL

BIBLIOTECA "EFE" GOMEZ

INTRODUCCION

En el mundo de las Matemáticas es bien conocida la importancia de poder estudiar una estructura matemática compleja a través de atra aparentemente más sencilla; este hecho motiva especialmente el estudio sobre isomorfismos (y sobre homeomorfismos). En este trabajo se pretende presentar como contenido central algunos resultados sobre anillos de polinomios isomorfos, anillos invariantes y anillos fuertemente invariantes, publicados en el artículo: Isomorphic Polynomial Rings -D.B. Coleman and E.E. Enochs-, basado en la siguiente pregunta: Pueden existir anillos no isomorfos A y B, tales que sus anillos de polinomios $A[X]$ y $B[X]$ sean isomorfos? En este estudio se han logrado establecer condiciones suficientes pora que A y B sean isomorfos cuando $A[X]$ y $B[X]$ lo son; pero no se ha encontrado un par de anillos A y B que tengan la prapiedad indicada en la pregunta anterior.

Un objetivo especial de este trabajo es el de lograr una mejor comprensión del tema, para lectares con conocimientas básicos en Algebra Abstracta; y se pretende alcanzar complementando con algunos conceptos teóricos y ejemplos y realizando una presentación más didáctica de algunas pruebas, con lo

ayuda de otros artículos y textos.

Se inicia con una parte del estudio sobre Radical de Jacobson de anillos de polinomios, presentado por S.A. Amitsur en [2], en la que aparecen algunos resultados que se usan más adelante.

En la sección 1 se presentan los conceptos de anillo invariante y anillo fuertemente invariante y una relación entre ellos.

En la sección 2 "La imagen de X bajo sobreyecciones", se hace una extensión del teorema 3 de [4], en el que Gilmer caracteriza los B-algebra homomorfismos del anillo de polinomios $B[X]$ en $B[X]$, como sobreyecciones o isomorfismos según los coeficientes de la imagen de la indeterminada X. Se concluye esta sección con un resultado muy útil en el estudio sobre anillos fuertemente invariontes (ver (2.5)).

En la sección 3 se establecen condiciones para que un anillo sea fuertemente invariante, con base en el conjunto de unidades del anillo y bajo la condición de no tener elementos nilpotentes diferentes de cero; se presenta en esta sección una caracterización de las unidades de $A[X]$, bajo condiciones especiales y una equivalencia de esta caracterización con la relación $J(A[X]) = \mathcal{N}[X]$, donde $J(A[X])$ es el radical de Jacobson del anillo

$A[X]$ y $\mathcal{N}$ el conjunto de elementos nilpotentes de A; se muestran además dos ejemplos para ver que dicha caracterización no se tiene para cualquier anillo A y además no es necesaria para que un anillo sea fuertemente invariante. Finalmente se prueba un teorema que usando el radical de Jacobson da condiciones para que un anillo A sea fuertemente invariante.

La sección 4 trata sobre dominios fuertemente invariantes, a partir de un dominio de integridad D se considera una cadena de extensiones que es usada para establecer una condición suficiente para que un dominio sea fuertemente invariante que finalmente se utiliza para probar que el anillo D, de los enteros algebraicos de un campo de números algebraicos L, es fuertemente invariante.

Con excepción de la sección 0, mientras no se indique lo contrario los anillos se consideran con unidad.

0. RADICAL DE JACOBSON DE ANILLOS DE POLINOMIOS

Sea R un anillo y $R[X]$ el anillo de polinomios en una indeterminada conmutativa X sobre R. El radical de Jacobson de R es:

$$J(R) = \left\{ \begin{array}{l} X \in R / \; xi + xy \text{ es cuasi-regular a la derecha} \\ \text{para toda } i \in \mathbb{Z} \text{ y todo } y \in R. \end{array} \right\}$$

(ver [6], prop. 3.7).

S.A. Amitsur probó en [2] que $J(R[X]) = N[X]$ donde $N = J(R[X]) \cap R$ y N es un nilideal en R. Presentamos a continuoción algunas proposiciones preliminares para concluír con la prueba de dicho resultado.

Proposición 1

Sean R y R' anillos cualesquiera y sea $\varphi : R \longrightarrow R'$ un homomorfismo sobreyectivo de anillos. Entonces $\varphi\langle J(R)\rangle \subseteq J(R')$.

Prueba

Para empezar veamos que la imagen, bajo el homomorfismo de anillos φ, de un elemento cuasi-regular a la derecha es también cuasi-regular a la

derecha: si a es cuasi-regular a la derecha en R, con cuasi-inverso a', se tiene $a + a' - aa' = 0$ y así $\varphi(a) + \varphi(a') - \varphi(a)\varphi(a') = \varphi(a + a' - aa') = \varphi(0) = 0$, luego $\varphi(a)$ es cuasi-regular a la derecha en R', con cuasi-inverso $\varphi(a')$.

Ahora: Si $u \in \varphi\langle J(R)\rangle$, sea $u = \varphi(x)$ con $x \in J(R)$ entonces $u = \varphi(x)$ y $xi + xy$ es cuasi-regular a la derecha para todo $i \in \mathbb{Z}$ y todo $y \in R$, así $ui + u\varphi(y) = \varphi(x)i + \varphi(x)\varphi(y) = \varphi(xi + xy)$ es cuasi-regular a la derecha para todo $i \in \mathbb{Z}$ y todo $y \in R$ y como φ es sobre, $ui + uv$ es cuasi-regular a la derecha para todo $i \in \mathbb{Z}$ y todo $v \in R'$, es decir $u \in J(R')$.

Nota:

Si además φ es inyectivo, se tiene $\varphi\langle J(R)\rangle = J(R')$:

Para ver que $J(R') \subseteq (J(R))$, sea $u \in J(R')$ y $x \in R$ tal que $u = \varphi(x)$; así, para todo $i \in \mathbb{Z}$ y todo $y \in R$, $\varphi(xi + xy) = \varphi(x)i + \varphi(x)\varphi(y) = ui + uv$ con $v \in R'$ y por tanto $\varphi(xi + xy)$ es cuasi-regular a la derecha en R'; sea $\varphi(z)$ su cuasi-inverso, entonces $\varphi((xi + xy) + z - (xi + xy)z) = \varphi(xi + xy) + \varphi(z) - \varphi(xi + xy)\varphi(z) = 0$ y como φ es inyectivo, se tiene que $(xi + xy) + z - (xi + xy)z = 0$, es decir que $xi + xy$ es cuasi-regular a la derecha en R, con cuasi-inverso z; por lo tanto $x \in J(R)$ y $u = \varphi(x) \in \varphi\langle J(R)\rangle$.

Corolario

$J(R)$ es invariante bajo automorfismos del anillo R. En particular: Si φ es un automorfismo de $R[X]$, se tiene:

$$\varphi < J(R[X]) > = J(R[X]).$$

Proposición 2

Sea R un anillo cualquiera, p un número primo y $R_p = \{ x \in R / px = 0 \}$.

Entonces:

i) R_p es un ideal de R y así $R_p[X]$ es un ideal de $R[X]$.

ii) R_p es un algebra sobre el campo finito $\mathbb{Z}_p$.

iii) En el anillo $R_p^{(1)}[X]$ donde $R_p^{(1)} = \mathbb{Z}_p \times R_p$ es el anillo obtenido por adjunción de una unidad a R_p (ver 7, p. 36) se verifica $(x+1)^p = x^p + 1$.

iv) Sea $g(x) \in R_p[X]$ tal que $g(x+1) = g(x)$; entonces: $g(x) \in R_p[X^p - X]$.

v) Si $h(x^p - x) \in J(R_p[X])$ entonces $h(x^p - x) \in J(R_p[X^p - X])$.

Prueba:

i) $0 \in R_p$; si $x, y \in R_p$ entonces $px = py = 0$, luego $p(x-y) = 0$ y $p(xy) = 0$; además para todo $x \in R_p$ y $r \in R$, $p(rx) = r(px) = r.0 = 0$ y $p(xr) = (px)r = 0r = 0$. Por lo tanto R_p es ideal de R y así $R_p[X]$ es ideal de $R[X]$.

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE MEDELLIN
DEPTO DE BIBLIOTECAS
BIBLIOTECA "EFE" GOMEZ

ii) R_p es un subanillo de R y puede ser considerado como $\mathbf{Z}_p$-módulo, ya que para $\lambda \in \mathbf{Z}_p$ y $a \in R_p$, $p(\lambda a) = (p\lambda)a = \lambda(pa) = 0$ y además si $\lambda \in \mathbb{Z}_p$ y $a,b \in R_p$ se tiene que $(\lambda a)b = a(\lambda b) = \lambda(ab)$; por lo tanto R_p es una $\mathbb{Z}_p$=algebra.

iii) En $R_p^{(1)} = \mathbb{Z}_p \times R$, la unidad es $(1,0)$ y se verifica: $p(1,0) = (p,0) = (0,0)$(ver 7 , p. 36); así en el desarrollo del binomio $(x + 1)^p$ los únicos términos que no anulan son x^p y 1, es decir $(x + 1)^p = x^p + 1$.

iv) Sea $g(x) \in R_p[X]$ tal que $g(x + 1) = g(x)$.

1) Supongamos que grad $g(x) = k < p$ y sea v elemento de $\mathbb{Z}_p$; entonces por inducción sobre v, se obtiene $g(x + v) = g(x)$

[$g(x + 1) = g(x) \Longrightarrow g(x + 2) = g((x + 1) + 1) = g(x+1) = g(x)$

Ahora:

$g(x + (v - 1)) = g(x) \Longrightarrow g(x + v) = g((x + (v - 1)) + 1)$

$= g(x + (v - 1)) = g(x)$].

Si $g(x) = b_o + b_1 x + \ldots + b_k x^k$, se sigue que para cada v elemento de $\mathbf{Z}_p$:

$$g(v) + g_1(v)x + \ldots + g_k(v)x^k$$
$$= b_o + b_1 x + \ldots + b_k x^k .$$

y por lo tanto $g(v) = b_o$ para todo v elemento de $\mathbb{Z}$, luego

$g(x) - b_o$ tiene al menos p raíces distintas (los elementos de $\mathbb{Z}_p$). Pero grad $(g(x) - b_o)$ = grad $g(x) = k < p$ luego $g(x) - b_o = 0$ y así $g(x) = b_o \in R_p$.

2) Ahora: Si $g(x)$ es un polinomio de grado arbitrario, entonces en $R_p^{(1)}[X]$, existen $h(x)$ y $k(x)$ tales que:

$$g(x) = h(x)(x^p - x) + k(x) \quad \text{con} \quad \text{grad } k(x) < p$$

(en realidad como $g(x)$ $R_p[X]$, se debe tener $h(x)$ y $k(x)$ en $R_p[X]$).

Entonces: $g(x + 1) = h(x + 1)((x + 1)^p - (x + 1)) + k(x + 1)$

$$g(x + 1) = h(x + 1)(x^p - x) + k(x + 1) \quad \text{(por iii)}.$$

Como $g(x + 1) = g(x)$, se tiene que:

$$[h(x + 1) - h(x)](x^p - x) = k(x) - k(x + 1)$$

El polinomio $k(x) - k(x + 1)$ es de grada menor que p y $[h(x + 1) - h(x)](x^p - x)$ es cero o de grada mayor o igual que p. Por lo tanta la igualdad anteriar se espera sólo si $h(x + 1) = h(x)$ y $k(x) = k(x + 1)$, luego por (1) puesto que grad $k(x) < p$, se sigue que $k(x) = k_o \in R_p$ y tenemos así que: $g(x) = h(x)(x^p - x) + k_o$

3) Probemos ahora por inducción que $g(x) \in R_p[x^p - x]$.

En efecta:

(i) Si grad $g(x) < p$, $g(x) = b_o \in R_p \subseteq R_p[x^p - x]$.

(ii) Supongamos que si $(n-1)p \leq \text{grad } g(x) < np$, $n \in \mathbb{N}$, entonces $g(x) \in R_p[x^p - x]$ (Hip. de inducción).

(iii) Si $np \leq \text{grad } g(x) < (n+1)p$ entonces, como:

$g(x) = h(x)(x^p - x) + k_o$, donde $h(x+1) = h(x) \in R_p[X]$ y además $(n-1)p \leq \text{grad } h(x) < np$, se concluye por hipótesis de inducción que $h(x) \in R_p[x^p - x]$ y por lo tanto $g(x) \in R_p[x^p - x]$.

v) Si $h(x^p - x) \in J(R_p[X])$, consideremos el ideal a derecha:

$$D = D_{h(x^p-x)} = \left\{ h(x^p-x)i + h(x^p-x)g(x) \quad i \in \mathbb{Z},\ g(x) \in R_p[x^p - x] \right\}$$

Sea $k(x) \in D$, entonces $k(x) = h(x^p - x)i + h(x^p - x)g(x)$ para algún $i \in \mathbb{Z}$ y algún $g(x) \in R_p[x^p - x]$, y así $k(x+1) = k(x)$ (ya que por (iii), $(x+1)^p - (x+1) = x^p - x$).

Como $h(x^p - x) \in J(R_p[X])$ y $k(x) \in D$, claramente $k(x) \in J(R_p[X])$ (por ser éste un ideal de $R_p[X]$); entonces su cuasi-inverso $k'(x)$ está determinado de manera única, el cuasi-inverso de $k(x+1)$ es $k'(x+1)$ y como $k(x+1) = k(x)$, se tiene $k'(x+1) = k'(x)$; además $k'(x) \in R_p[X]$ y por lo tanto $k'(x) \in R_p[x^p - x]$ (por (iv)).

De lo anterior se concluye que el ideal D es cuasi-regular en $R_p[x^p - x]$ y como $h(x^p - x) \in D$, se sigue que $h(x^p - x) \in J(R_p[x^p - x])$.

Lema 1:

Si $N = J(R[X]) \cap R$ entonces :

$J(R[X]) \neq \{0\}$ implica $N \neq \{0\}$

Prueba

Supongamos que $J = J(R[X]) \neq \{0\}$ y $N = J \cap R = \{0\}$.

Podemos elegir un polinomio $f(x) \in J$, diferente de cero y de grado mínimo; sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ tal polinomio, entonces $n \geq 1$ ya que $J \cap R = \{0\}$.

Consideremos el automorfismo de $R[X]$, $g(x) \xrightarrow{\psi} g(x+1)$, como $f(x) \in J$, entonces $\psi(f(x)) = f(x+1) \in J$ (ya que J es invarionte bajo automorfismos de $R[X]$), así $f_0(x) = f(x+1) - f(x) \in J$, pero grad $f_0(x) <$ grad $f(x)$ y así la minimalidad del grado de $f(x)$ implica $f_0(x) = 0$, es decir: $f(x+1) = f(x)$ y $f(x+1) - f(x) = n a_n x^{n-1} + \ldots + (a_1 + a_2 + \ldots + a_n) = 0$, de donde $n a_n = 0$.

Consideremos dos casos:

1) Si R es de característico cero, entonces $R_p = \{0\}$ para todo primo p, y así para todo entero $m \neq 0$ y todo elemento $a \neq 0$ en R, se tiene $ma \neq 0$, por lo tanto, si $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ con $a_n \neq 0$, y como $n a_n = 0$, se concluye $n = 0$, es decir $f(x) = a_0 \in R$ y $a_0 \neq 0$, pero $f(x) \in J$ luego $f(x) \in J \cap R$, y así $J \cap R \neq \{0\}$ Contradicción.

2) Si R no es de característica cero existe un primo p, tal que $R_p \neq \{0\}$ como $n a_n = 0$ y además $n > 1$ (ya que si $n = 1$, $a_1 = 0$, pero $J \cap R = \{0\}$, luego $f(x) = a_o = 0$, lo que contradice la elección de $f(x) \neq 0$).

Sea $m = \min \left\{ k \in \mathbb{Z}^+ / k a_n = 0 \text{ y } k > 1 \right\}$

Sea p un número primo que divide a m, entonces $(\frac{m}{p}) a_n \neq 0$ y claramente $(\frac{m}{p}) a_n \in R_p$, sea $h(x) = (\frac{m}{p}) f(x)$ entonces $h(x) \in J$ y grado de $h(x)$ = grado de $f(x)$.

Además $ph(x) \in J$ y el grado de $ph(x)$ es menor que el grado de $f(x)$, entonces, por la minimalidad del grado de $f(x)$ en J, $ph(x) = 0$ y así $h(x) \in R_p[X]$.

Se concluye entonces que $h(x) \in R_p[X] \cap J$, $h(x) \neq 0$ y el grado de $h(x)$ es mínimo con respecto a los elementos no nulos de J; pero $R_p[X] \cap J = J(R_p[X])$, luego $h(x)$ $J(R_p[X])$. Además como $h(x) \in J$ y J es invarionte bajo el outomorfismo φ de $R[X]$, tal que $g(x) \xrightarrow{\varphi} g(x+1)$, entonces $h(x+1) \in J$ y por lo tanto $h(x+1) - h(x) = h_o(x) \in J$ y el grado de $h_o(x)$ es menor que el grado de $h(x)$ y así la minimolidad del grado de $h(x)$ en J, implica $h_o(x) = 0$, es decir $h(x+1) = h(x)$; pero $h(x) \in R_p[X]$, luego por proposición 2 (iv), $h(x) \in R_p[x^p - x]$.

Ahora sabemos que $h(x) \in R_p[x^p - x]$ y $h(x) \in J(R_p[X])$, luego por proposición 2 (v), se tiene $h(x) \in J(R_p[x^p - x])$.

Consideremos el isomorfismo:

$$\varphi : R_p[X] \longrightarrow R_p[X^p - x]$$
$$g(x) \longmapsto g(x^p - x)$$

Según la proposición 1 y la nota que le sigue, tenemos:

$\varphi < J(R_p[X]) > = J(R_p[x^p - x])$, entonces $h(x) = \varphi(g(x)) = g(x^p - x)$ para algún polinomio $g(x) \in J(R_p[X]) = J \cap R_p[X] \subseteq J$, pero el grado de $g(x)$ es menor que el grado de $h(x)$ (pues grado de $h(x) \geq 1$) y se contradice así la minimalidad del grado de $h(x)$ en J.

Conclusión: $J(R[X]) \neq \{0\}$ implica $N \neq \{0\}$.

UNIVERSIDAD NACIONAL DE COLOMBIA
BIBLIOTECA

Lema 2:

$N = J(R[X]) \cap R$ es un nilideal de R.

Prueba

i) Como $J(R[X])$ es un ideal en $R[X]$, entonces $J(R[X])$ es un subgrupo aditivo del grupo aditivo $R[X]$, también R es subgrupo aditivo de $R[X]$. Además si $a \in J(R[X]) \cap R$ y $r \in R$, entonces:

$$ar \in J(R[X]) \cap R$$

y $$ra \in J(R[X]) \cap R$$

Luego $N = J(R[X]) \cap R$ es un ideal en R.

ii) Sea $r \in N \subseteq J$, entonces $r(rx) = r^2x \in J$. (Por ser J un ideal de $R[X]$).

Sea $g(x)$ el cuasi-inverso de r^2x, entonces:

$$g(x) + r^2x - g(x)(r^2x) = 0$$

Así: $$g(x) = -r^2x + g(x)(r^2x) \qquad (1)$$

de donde: $$g(x) = -r^2x + (-r^2x + g(x)(r^2x))(r^2x)$$

$$g(x) = -r^2x - (r^2x)^2 + g(x)(r^2x)^2$$

y sustituyendo sucesivamente (1) en cada nueva expresión de $g(x)$, se obtiene, para un entero $n >$ grad $g(x)$, la ecuación:

$$g(x) = -r^2x - (r^2x)^2 - (r^2x)^3 - \ldots - (r^2x)^n - (r^2x)^{n+1} + g(x)(r^2x)^{n+1}$$

y si comparamos coeficientes de x^n en la igualdad anterior, encontramos

que $r^{2n} = 0$ y por lo tanto r es nilpotente; concluimos entonces que N es un nilideal en R.

TEOREMA

$J(R[X]) = N[X]$ donde $N = J(R[X]) \cap R$.

Prueba

Como $N \subseteq J = J(R[X])$ y J es un ideal de $R[X]$, entonces $N[X] \subseteq J$.

Consideremos el homomorfismo canónico $\varphi: R[X] \longrightarrow R[X]/N[X]$, cuyo núcleo es $N[X] \subseteq J$, entonces:

$$J/N[X] = J(R[X])/N[X] = \varphi\langle J(R[X])\rangle \underset{\text{por Prop. 1.}}{\subseteq} J(R[X]/N[X])$$

Veamos que $J(R[X]/N[X]) \subseteq J(R[X])/N[X]$:

Si para cada anillo denotamos por $A^{(1)}$ el anillo obtenido por adjunción de unidad a A y si $N'[X] = \{0\} \times N[X]$, es fácil prabar que

$$(R[X])^{(1)}/N'[X] \cong (R[X]/N[X])^{(1)}$$

Además, en general $J(A^{(1)}) = J(A)$ (ver 6, Prop. I 4.3, p. 16).

Luego $J((R[X])^{(1)}) = J(R[X])$ y

$$J(R[X]/N[X]) = J((R[X]/N[X])^{(1)}) = J((R[X])^{(1)}/N'[X])$$

Como $N'[X] \cong N[X]$, se tiene que

$$J(R[X])^{(1)}/N'[X] \cong J(R[X]/N[X])$$

De lo anterior vemos que es suficiente probar que :

$$J((R[X])^{(1)}/N'[X]) \subseteq J(R[X])^{(1)}/N'[X]$$

Mostremos entonces esta última inclusión :

Si $\overline{r(x)} \in J((R[X])^{(1)}/N'[X])$, entonces $\overline{r(x)} \in \mathcal{A}$, para todo ideal $\mathcal{A}$ maximal a derecha de $R[X]^{(1)}/N'[X]$ y así $r(x) \in \mathcal{B}$ para todo ideal $\mathcal{B}$ maximal a derecha, de $(R[X])^{(1)}$ tal que $N'[X] \subseteq \mathcal{B}$, (por el teorema de correspondencia); pero como $N[X] \subseteq J(R[x]) = J(R[X]^{(1)})$, entonces $N'[X] \subseteq J(R[X]^{(1)}) \subseteq \mathcal{B}$ para todo ideal maximal a derecha $\mathcal{B}$ de $(R[X])^{(1)}$, luego $r(x) \in J(R[X]^{(1)})$ y por lo tanto : $\overline{r(x)} \in J(R[X]^{(1)})/N'[X]$.

Luego $J(R[X]/N[X]) = J(R[X])/N[X] = J/N[X]$

Sea $\bar{R} = R/N$ entonces $R[X]/N[X] \cong \bar{R}[X]$.

Además : Si

$$\psi : R \cup N[X] \longrightarrow R[X]/N[X]$$
$$p(x) \longrightarrow p(x) + N[X]$$

es la restricción a $R \cup N[X]$ del homomorfismo canónico ψ de $R[X]$ en

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL

$R[X]/N[X]$, se tiene $\text{Ker}\,\psi = \text{Ker}\,\gamma = N[X]$ y

$$\psi\langle R \cup N[X]\rangle = \left\{ \overline{p(x)} \in R[X]/N[X] : \; p(x) \in R \cup N[X] \right\}$$

Así: $\overline{p(x)} \in \gamma\langle R \cup N[X]\rangle$

$\iff \overline{p(x)} \in R[X]/N[X]$ y $p(x) \in R \cup N[X]$

$\iff p(x) \in R$ ó $\overline{p(x)} = 0$

$\iff \overline{p(x)} \in R/N$ ó $\overline{p(x)} = 0$

$\iff p(x) \in \overline{R}$

Por lo tanto $R \cup N[X]/N[X] \cong \overline{R}$

Ahora: $J/N[X] \cap ((R \cup N[X])/N[X]) = [J \cap (R \cup N[X])]/N[X]$

$= ((J \cap R) \cup N[X])/N[X]$ (pues $N[X] \subseteq J$)

$= N \cup N[X]/N[X]$

$= N[X]/N[X]$

$= \{\overline{0}\}$

Luego $J(\overline{R}[X]) \cap \overline{R} = \{\overline{0}\}$ y así $J(\overline{R}[X]) = \{\overline{0}\}$ (por Lema 1); pero $J(\overline{R}[X]) = J(R[X]/N[X]) = J/N[X]$. Por lo tanto $J/N[X] = \{\overline{0}\}$, de donde $J = N[X]$.

Conclusión: $J(R[X]) = N[X]$, donde $N = J(R[X]) \cap R$ y N es un nilideal en R.

1. ANILLOS INVARIANTES Y FUERTEMENTE INVARIANTES

(1.1) Un anillo A es llamado invariante si para cualquier anillo B tal que los anillos de polinomios $A[X]$ y $B[X]$ son isomorfos, se tiene que A y B son isomorfos.

(1.2) Un anillo A es fuertemente invariante si todo isomorfismo: $\sigma: A[X] \longrightarrow B[X]$ es tal que $\sigma(X)$ es un B-generador de $B[X]$.

Nota: Mientras no se indique lo contrario, se trabaja aquí con anillos que tienen identidad.

(1.3) Proposición: Todo anillo A fuertemente invariante, es invariante.

Prueba:

Sea A un anillo fuertemente invariante y B un anillo tal que $\sigma: A[X] \longrightarrow B[X]$ es un isomorfismo, entonces $\sigma(X)$ es un B-generador de $B[X]$ y así $B[\sigma(X)] = B[X]$.

Consideremos el B-algebra isomorfismo :

$$\varphi : B[X] \longrightarrow B[X]$$
$$\sigma(X) \longrightarrow X$$

entonces $\varphi \circ \sigma : A[X] \longrightarrow B[X]$ es tal que $(\varphi \circ \sigma)(X) = \varphi(\sigma(X)) = X$ y así la imagen bajo $\varphi \circ \sigma$ del ideal generado por X en $A[X]$ es igual al ideal generado por X en $B[X]$, entonces $A[X]_{/(X)} \cong B[X]_{/(X)}$

Luego : $A \cong A[X]_{/(X)} \cong B[X]_{/(X)} \cong B$

(1.4) Observación : El recíproco de la proposición (1.3) no es cierto :

En la proposición (2.6) y el corolario (2.8) de [3], Abhyankar, Heinzer and Eakin prueban que si K es un campo, entonces $K[X]$ es invariante, pero éste no es un anillo fuertemente invariante .

2. LA IMAGEN DE X BAJO SOBREYECCIONES

(2.1) Proposición :

Sea B un anillo y $B[X]$ un anillo de polinomios sobre B; $\varphi(x) = b_o + b_1 x + \ldots + b_n x^n$ induce un B-endomorfismo sobre (inyectivo) si y sólo si $\psi(x) = b_1 x + \ldots + b_n x^n$ induce un B-endomorfismo sobre (respectivamente inyectivo).

Prueba :

Consideremos la aplicación $\delta : B[X] \longrightarrow B[X]$ tal que $\delta(x) = b_o + x$ y sea $\gamma : B[X] \longrightarrow B[X]$ tal que $\gamma(x) = -b_o + x$, entonces :

$(\gamma \circ \delta)(x) = \gamma(\delta(x)) = \gamma(b_o + x) = -b_o + (b_o + x) = x$

por lo tanto δ admite inversa, es decir δ es biyectiva y $\delta^{-1} = \gamma$

Ahora : $(\psi \circ \delta)(x) = \psi(\delta(x))$

$= \psi(b_o + x)$

$= \psi(b_o) + \psi(x)$

$= b_o + b_1 x + \ldots + b_n x^n$

$= \varphi(x)$

Luego : $\psi \circ \delta = \varphi$.

Y en consecuencia : φ es sobre si y sólo si ψ es sobre ; φ es inyectivo si y sólo si ψ es inyectivo.

(2.2) Proposición :

El B-endomorfismo $h : B[X] \longrightarrow B[X]$ inducido por $h(x) = x + h_2 x^2 + h_3 x^3 + \ldots + h_n x^n$, con $h_i \in B$ es inyectivo.

Prueba :

Sea $p \in B[X]$ y $p = p_o + p_1 x + p_2 x^2 + \ldots + p_n x^n$. Entonces $h(p_o) = p_o$ y para todo $k \neq 0$,

$$h(p_k x^k) = p_k h(x^k) = p_k (h(x))^k$$
$$= p_k (x + h_2 x^2 + \ldots + h_n x^n)^k$$

luego $h(p_k x^k) = p_k x^k + \mathcal{Q}_k$, donde $\mathcal{Q}_k$ es un polinomio tal que el menor exponente de x en $\mathcal{Q}_k$ es mayor que k.

Se tiene entonces :

$$h(p) = h(\sum_{k=0}^{n} p_k x^k) = \sum_{k=0}^{n} p_k (h(x))^k = \sum_{k=0}^{n} (p_k x^k + \mathcal{Q}_k)$$

Si $p \in \text{Ker } h$, entonces $h(p) = 0$, es decir :

$$\sum_{k=0}^{n} (p_k x^k + \mathcal{Q}_k) = 0 .$$

Esto es :

$$(p_o + \mathcal{Q}_o) + (p_1 x + \mathcal{Q}_1) + (p_2 x^2 + \mathcal{Q}_2) + \ldots + (p_n x^n + \mathcal{Q}_n) = 0 \quad (1)$$

En consecuencia : $p_o = 0$ (por ser el único coeficiente de x^o en (1)) y así :

$0 = h(0) = h(p_o) = p_o x^o + \mathcal{Q}_o$, de donde $\mathcal{Q}_o = 0$.

De manera que el único coeficiente de x en (1) es p_1 y así $p_1 = 0$, y $0 = h(0) = h(p_1) = p_1 x + \mathcal{Q}_1$; luego $\mathcal{Q}_1 = 0$.

Sea $k \in \mathbb{Z}^+$, $k \leq n$;

Supongamos que para $1 \leq r < k$, $p_r = 0$ y $\mathcal{Q}_r = 0$; entonces $p_k = 0$ (por ser el único coeficiente de x^k en (1)) y $0 = h(0) = h(p_k) = p_k x^k + \mathcal{Q}_k$. Luego $\mathcal{Q}_k = 0$.

De lo anterior se deduce que $p = 0$ y así Ker h = 0 , es decir h es inyectivo.

(2.3) Proposición :

Si C es el centro de un anillo B, entonces $C[X]$ es el centro del anillo de polinomios $B[X]$.

(2.4) TEOREMA

Sea B un anillo, $b_o, b_1, \ldots, b_n$ elementos de B, $n \geq 1$. Entonces

UNIVERSIDAD NACIONAL DE COLOMBIA
FACULTAD DE CIENCIAS
BIBLIOTECA "ALEJANDRO ANGULO"

las siguientes afirmaciones son equivalentes :

(1) $b_o, b_1, \ldots, b_n$ pertenecen al centro del anillo B, b_1 es una unidad y $b_2, b_3, \ldots, b_n$ son nilpotentes.

(2) El B-algebra homomorfismo de $B[X]$ en $B[X]$ inducido por $x \longmapsto b_o + b_1 x + \ldots + b_n x^n$ es sobre.

(3) El B-algebra homomorfismo de $B[X]$ en $B[X]$ inducido por $x \longmapsto b_o + b_1 x + \ldots + b_n x^n$ es un isomorfismo.

Prueba :

[1) $\Longrightarrow$ 2)]. Sean $b_o, b_1, \ldots, b_n$ elementos del centro de B, tales que b_1 es una unidad y $b_2, \ldots, b_n$ son nilpotentes.

Sea $\varphi : B[X] \longrightarrow B[X]$ el B-algebra homomorfismo inducido por

$$x \longmapsto \varphi(x) = \sum_{i=0}^{n} b_i x^i,$$

veamos que φ es sobreyectivo : Sea C el centro de B y sea f la restricción de φ a $C[X]$; como $b_i \in C$ para todo $i \in \{0, 1, \ldots, n\}$ entonces $\varphi(x) = \sum_{i=0}^{n} b_i x^i \in C[X]$, además $f(C) = C$ y C es un anillo conmutativo con identidad (por ser el centro de B), entonces usando el teorema de Gilmer para el caso conmutativo (Teorema 3) en [4] concluimos que f es un isomorfismo de $C[X]$ en $C[X]$; por lo tanto existe $p \in C[X]$ tal que $\varphi(p) = f(p) = x$ y como $C[X] \subseteq B[X]$, entonces φ es sobre.

[1) $\Longrightarrow$ 3)]. Sean $b_o, b_1, \ldots, b_n$ elementos del centro de B, donde b_1 es una unidad y $b_2, b_3, \ldots, b_n$ elementos nilpotentes; como 1) $\Longrightarrow$ 2), φ es sobre.

Veamos ahora que φ es inyectivo. El endomorfismo h inducido por

$$x \longmapsto h(x) = x + (b_1^2)^{-1} b_2 x^2 + \ldots + (b_1^n)^{-1} b_n x^n$$

es inyectivo (ver proposición 2.2).

El endomorfismo g inducido por $x \longmapsto g(x) = b_1 x$, es biyectivo por ser b_1 una unidad ($g^{-1}(x) = b_1^{-1} x$).

Consideremos $\psi(x) = b_1 x + b_2 x^2 + \ldots + b_n x^n$ y veamos que $\psi = g_o h$:

$$(g_o h)(x) = g(h(x)) = g(x + (b_1^2)^{-1} b_2 x^2 + \ldots + (b_1^n)^{-1} b_n x^n)$$

$$= g(x) + (b_1^2)^{-1} b_2 (g(x))^2 + \ldots + (b_1^n)^{-1} b_n (g(x))^n$$

$$= b_1 x + (b_1^2)^{-1} b_2 b_1^2 x^2 + \ldots + (b_1^n)^{-1} b_n b_1^n x^n$$

$$= b_1 x + b_2 x^2 + \ldots + b_n x^n \quad \text{(por ser los } b_i \text{ centrales)}$$

$$= \psi(x).$$

Como g es biyectivo y h es inyectivo entonces $\psi = g_o h$ es inyectivo y por la proposición (2.1) concluímos que φ es inyectivo.

$[3) \Longrightarrow 2)]$. Es obvio.

$[2) \Longrightarrow 1)]$. Sea C el centro de B y supongamos que el B-algebra homomorfismo φ inducido por $x \longmapsto b_o + b_1 x + \ldots + b_n x^n$ es sobre, entonces:

i) $C[X]$ es enviado mediante φ en $C[X]$ (por ser $C[X]$ el centro de $B[X]$) y por lo tanto $b_o, b_1, \ldots, b_n$ son centrales.

ii) Veamos que b_1 es una unidad: Sea $\bar{B} = B/(b_1)$ y sea $b \in B$, entonces por 2), la aplicación $x \longmapsto \bar{b}_o + \bar{b}_1 x + \ldots + \bar{b}_n x^n$ induce un $\bar{B}$-homomorfismo sobre $\psi : \bar{B}[X] \longrightarrow \bar{B}[X]$; pero como $\bar{b}_1 = 0$, se tiene que $x \longmapsto \bar{b}_o + \bar{b}_2 x^2 + \ldots + \bar{b}_n x^n = \psi(x)$.

Si $\bar{b}_1$ no es una unidad, $B \neq (b_1)$; sea $b \in B$ tal que $b \notin (b_1)$, entonces por ser ψ sabreyectivo, existe
$g(x) = \bar{g}_o + \bar{g}_1 x + \ldots + \bar{g}_k x^k$ tal que $\psi(g(x)) = \bar{b}\, x$, es decir:

$$\bar{g}_o + \bar{g}_1 \psi(x) + \bar{g}_2 (\psi(x))^2 + \ldots + \bar{g}_k (\psi(x))^k = \bar{b}\, x$$

de donde $\bar{b} = 0$ (pues en el polinomio de la izquierda el coeficiente de x es cero); por lo tanto $b \in (b_1)$ (contradicción!). Luego b_1 es uno unidad.

iii) Veamos que $b_2, b_3, \ldots, b_n$ son nilpotentes: Sea:
$Y = b_o + b_1 x + \ldots + b_n x^n$, y

UNIVERSIDAD NACIONAL DE COLOMBIA
BIBLIOTECA

$$Z = x + b_1^{-1} b_2 x^2 + \ldots + b_1^{-1} b_n x^n$$

Puesto que el B-algebra homomorfismo φ, inducido por $x \longmapsto y$ es sobre, existe:

$$q(x) = \sum_{i=0}^{n} q_i x^i, \text{ tal que}$$

$$x = \varphi(q(x)) = \varphi\left(\sum_{i=0}^{n} q_i x^i\right) = \sum_{i=0}^{n} q_i (\varphi(x))^i = \sum_{i=0}^{n} q_i Y^i .$$

luego, $B[X] = B[Y]$; además por la proposición (2.1) y por ser b_1 una unidad, el homomorfismo inducido por $x \longmapsto z$ es sobre y por lo tanto $B[X] = B[Z]$; en consecuencia $B[Z] = B[X] = B[Y]$.

Ahora: Si $X = C_o + C_1 Z + C_2 Z^2 + \ldots + C_m Z^m$, con $C_i \in B$, $i \in \{0, 1, 2, \ldots, m\}$, entonces:

$$\begin{aligned} X = C_o &+ C_1 (x + b_1^{-1} b_2 x^2 + \ldots + b_1^{-1} b_n x^n) \\ &+ C_2 (x + b_1^{-1} b_2 x^2 + \ldots + b_1^{-1} b_n x^n)^2 \\ &+ C_3 (x + b_1^{-1} b_2 x^2 + \ldots + b_1^{-1} b_n x^n)^3 \\ &+ \\ &\vdots \\ &+ C_m (x + b_1^{-1} b_2 x^2 + \ldots + b_1^{-1} b_n x^n)^m \end{aligned}$$

Se obtiene de la anterior igualdad:

$C_o = 0$

$C_1 = 1$

$C_1 b_1^{-1} b_2 + C_2 = 0 \Longrightarrow C_2 = C_1 b_1^{-1} b_2 = - b_1^{-1} b_2$

$C_1 b_1^{-1} b_3 + 2 C_2 b_1^{-1} b_2 + C_3 = 0 \Longrightarrow C_3 = 2(b_1^{-1} b_2)^2 - b_1^{-1} b_3$

Como todos los b_i son elementos de C y C es un subanillo de B entonces C_o, C_1, C_2, C_3 están en C; y continuando el proceso se puede probar que paro todo $i \in \{0, 1, 2, \ldots, m\}$, $C_i \in C$; luego por la versión correspondiente para el caso conmutativo, se tiene que para $i \in \{2, 3, \ldots, n\}$, $b_1^{-1} b_i$ es nilpotente y como b_1 es central, se concluye que para $i \in \{2, 3, \ldots, n\}$, b_i es nilpotente.

(2.5) Corolario :

Sean A y B anillos con identidad y sea $\sigma : A[X] \longrightarrow B[X]$ un homomorfismo sobre, tal que $\sigma(A) \subseteq B$, entonces $\sigma(A) = B$.

Prueba :

Como σ es sobre, y $\sigma(A) \subseteq B$, se tiene :

$$B[X] = \sigma(A[X]) = (\sigma(A))[\sigma(X)] \subset B[\sigma(X)];$$

además como $\sigma(X) \in B[X]$, $B[\sigma(X)] \subset B[X]$; así que $B[\sigma(X)] = B[X]$; entonces el B-algebra endomorfismo :

$f : B[X] \longrightarrow B[X]$ inducido por $X \longmapsto \sigma(X)$ es sobre y por el

teorema anterior, f es un isomorfismo. Así $f^{-1} \circ \sigma : A[X] \longrightarrow B[X]$ es sobre y $(f^{-1} \circ \sigma)(A) \subset B$ y $(f^{-1} \circ \sigma)(x) = x$.

Entonces $(f^{-1} \circ \sigma)$ envía (x) en (x), luego $(f^{-1} \circ \sigma)(A) = B$ y como $f(B) = B$ entonces $f(f^{-1} \circ \sigma)(A) = f(B) = B$, ésto es:

$$\sigma(A) = B.$$

3. UNIDADES DE UN ANILLO DE POLINOMIOS, $A[X]$

Notación: Si B es un anillo, denotaremos por B^* el grupo de unidades de B.

(3.1) TEOREMA

Sea A un anillo. Entonces $(A[X])^* = A^*$ si y sólo si A no tiene elementos nilpotentes diferentes de cero.

Prueba

$[\Longrightarrow]$. Supongamos que A tiene elementos nilpotentes diferentes de cero; sea $a \in A$, $a \neq 0$ tal que $a^k = 0$ para algún entero positivo k, entonces $1 + ax$ es una unidad no constante de $A[X]$ ya que:

$$(1 + ax)(1 - ax + a^2x^2 - \ldots \pm a^{k-1}x^{k-1})$$

$$= 1 - ax + a^2x^2 - \ldots \pm a^{k-1}x^{k-1} + ax - a^2x^2 + \ldots \mp a^{k-1}x^{k-1} \pm 0$$

$$= 1$$

Luego $(A[X])^* \neq A^*$

$[\Leftarrow]$. Supongamos que A no tiene elementos nilpotentes diferentes de cero.

Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in A[X]$ una unidad $(n \geq 1)$ y sea

$g(x) = \sum_{i=0}^{m} b_i x^i$ el inverso de $f(x)$; entonces:

$$1 = f(x)g(x)$$

$$= a_o b_o + a_o b_1 x + a_o b_2 x^2 + \ldots + a_1 b_o x + \ldots + a_1 b_m x^{m+1} + \ldots + a_n b_m x^{n+m}$$

Como $n \geq 1$, $a_n b_m = 0$, veomos por inducción que:

$$a_n b_m = a_n b_{m-1} = \ldots = a_n b_o = 0.$$

En efecto:

Supongamos que $a_n b_m = a_n b_{m-1} = \ldots = a_n b_{m-s} = 0$ para $s \geq 0$

y veamos que: $a_n b_{(m-s)-1} = 0 = a_n b_{m-(s+1)}$.

Consideremos el coeficiente de $x^{n+m-(s+1)}$ en $f(x)g(x)$, éste es:

$$h = a_n b_{m-(s+1)} + a_{n-1} b_{m-s} + a_{n-2} b_{m-s+1} + \ldots + a_{n-(s+1)} b_m = 0$$

y como $a_n b_{m-k} = 0$ para $k \in \{0, 1, \ldots, s\}$, entonces:

$$(b_{m-k} a_n)^2 = (b_{m-k} a_n)(b_{m-k} a_n)$$

$$= b_{m-k}(a_n b_{m-k}) a_n$$

$$= 0$$

luego $b_{m-k} a_n$ es un elemento nilpotente, así que $b_{m-k} a_n = 0$,

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE MEDELLIN
DEPTO. DE BIBLIOTECAS
BIBLIOTECA "CARLOS GOMEZ"

para $k \in \{0, 1, \ldots, s\}$. Por lo tanto, multiplicando h por a_n, se obtiene:

$$0 = h\,a_n = a_n\,b_{m-(s+1)}\,a_n + a_{n-1}\,b_{m-s}\,a_n + \ldots + a_{n-(s+1)}\,b_m\,a_n$$

$$= a_n\,b_{m-(s+1)}\,a_n .$$

Así que:

$$(a_n\,b_{m-(s+1)})^2 = (a_n\,b_{m-(s+1)}\,a_n)\,b_{m-(s+1)}$$

$$= 0$$

luego $a_n\,b_{m-(s+1)} = 0$ pues A no tiene elementos nilpotentes diferentes de cero.

En consecuencia $a_n\,b_o = 0$ y como $a_o\,b_o = b_o\,a_o = 1$, es decir a_o es una unidad, entonces $a_n = 0$ para todo $n \geq 1$ y así las unidades de $A[X]$ son las triviales, es decir, $(A[X])^* = A^*$.

(3.2) Ejemplo 1

Si D es un dominio de integridad, entonces $(D[X])^* = D^*$.

(3,3) Ejemplo 2

Si A es un anillo conmutativo tal que para cada ideal primo P de A, el anillo local A_P no tiene elementos nilpatentes diferentes de cero, entonces $(A[X])^* = A^*$.

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL

Prueba :

Como A_p no tiene elementos nilpotentes diferentes de cero, cualquiera sea el ideal primo P de A, entonces $\mathcal{N}_{A_p} = \{0\}$; pero para toda parte multiplicativa S de A, se tiene que :

$S^{-1}\mathcal{N}_A = \mathcal{N}_{S^{-1}A}$ (ver [5], p. 48), así que para $S = A - P$, se tiene $(\mathcal{N}_A)_P = \mathcal{N}_{A_P} = \{0\}$, para todo ideal primo P de A, luego $\mathcal{N}_A = \{0\}$ (ver [5], p. 50). En consecuencia, por (3.1), $(A[X])^* = A^*$.

(3.4) Corolario :

Si A es un anillo sin elementos nilpotentes diferentes de cero y generodo como anillo por A^* entonces A es fuertemente invariante.

Prueba :

Sea σ: $A[X] \longrightarrow B[X]$ un isomorfismo de anillos. Sea $b \in B$ tal que existe $r \in \mathbb{Z}^+$ que satisface $b^r = 0$, entonces por ser un isomorfismo existe $a \in A$, tal que $\sigma(a) = b$, entonces $\sigma(a^r) = (\sigma(a))^r = b^r = 0$, y como σ es 1-1, se tiene que $a^r = 0$; pero A no tiene elementos nilpotentes diferentes de cero y por lo tanto $a = 0$, y así $b = \sigma(a) = \sigma(0) = 0$; se concluye entonces que B no tiene elementos nilpotentes diferentes de cero y por (3.1) $(B[X])^* = B^*$. Además, como σ es un isomorfismo, envía unidades en unidades, así que $\sigma(A^*) = B^*$ y ya que A^* ge-

MC 99746

nera a A como anillo, para todo $a \in A$, a es suma finita de productos finitos de unidades de A, entonces $\sigma(A) \subseteq B$ y por ser σ sobre, se concluye por (2.5) que $\sigma(A) = B$.

Así: $B[X] = \sigma(A)[\sigma(x)] = B[\sigma(x)]$; luego $\sigma(x)$ es un B-generador de $B[X]$ y por lo tanto A es fuertemente invariante.

(3.5) Ejemplo 3

El anillo $\mathbb{Z}$ de los números enteros es fuertemente invariante.

(3.6) Ejemplo 4

Todo anillo de división es fuertemente invariante.

(3.7) Ejemplo 5

El anillo $A = \mathbb{Z}(i) = \{a + bi / a, b \in \mathbb{Z}\}$ de los enteros Gaussianos, es fuertemente invariante.

En efecto, $A^* = \{1, -1, i, -i\}$

$A = \mathbb{Z}(i) = \langle A^* \rangle$ y además $\mathbb{Z}(i)$ no tiene elementos nilpotentes diferentes de cero.

(3.8) Corolario :

Todo anillo local, sin elementos nilpotentes diferentes de cero, es

fuertemente invariante.

Prueba

Basta demostrar que A es generado como anillo por A^*.

En efecto, si A es un anillo local y $\mathcal{M}$ su ideal maximal, entonces $A - A^* \subset \mathcal{M}$ (ver [5], prop. 1.5, pág. 4), además $\mathcal{M}$ no contiene unidades (ya que si $u \in \mathcal{M}$ y u es una unidad, $1 = uu^{-1} \in \mathcal{M}$, luego $\mathcal{M} = A$), entonces $\mathcal{M} = A - A^*$; y ya que $\mathcal{M}$ es el único ideal maximal de A, entonces el radical de Jacobson de A es $\mathcal{M}$ y se tiene que $x \in \mathcal{M}$, si y sólo si para todo $y \in A$, $1 - xy \in A^*$, entonces $1 - xy = u \in A^*$ para todo $y \in A$, en particular para $y = 1$, se tiene entonces $1 - x = u \in A^*$, luego $x = 1 - u$, es decir, x es generado por elementos de A^*.

Luego todo elemento de A es generado por elementos de A^* y como A no tiene elementos nilpotentes diferentes de cero, entonces por (3.4), A es fuertemente invariante.

(3.9) TEOREMA

Sea A un anillo con centro C. Si C no tiene elementos nilpotentes diferentes de cero y C es generado por C^* entonces A es fuertemente invariante.

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE MEDELLIN
SISTEMA DE BIBLIOTECAS
BIBLIOTECA "EFE" GOMEZ

Prueba

Sea σ: $A[X] \longrightarrow B[X]$ un isomorfismo y sea D el centro de B, entonces $\sigma(C[X]) = D[X]$. Ahora: Como C no tiene elementos nilpotentes diferentes de cero y C es generado por C^*, entonces por (3.4) C es fuertemente invariante y como: σ: $C[X] \longrightarrow D[X]$ es un isomorfismo, se tiene que $\sigma(x)$ es un D-generador de $D[X]$.

Veamos que $\sigma(x)$ es un B-generador de $B[X]$:

Como $\sigma(x)$ es un D-generador de $D[X]$, entonces el homomorfismo de $D[X]$ en $D[X]$ inducido por $x \longmapsto \sigma(x)$ es sobre, luego por el teorema (2.4) $\sigma(x) = b_o + b_1 x$, donde b_1 es una unidad y b_o y b_1 son centrales ($b_2 = b_3 = \ldots = b_n = 0$, ya que D no tiene elementos nilpotentes diferentes de cero, pues C no los tiene y $C[X]$ es isomorfo a $D[X]$); por lo tanto el homomorfismo de $B[X]$ en $B[X]$ inducido por $x \longmapsto \sigma(x)$ es un isomorfismo y así $\sigma(x)$ es un B-generador de $B[X]$. En consecuencia A es fuertemente invariante.

(3.10) Corolario:

Si A es un anillo, cuyo centro es un compo, entonces A es fuertemente invariante. En particular, todo anillo simple es fuertemente invariante.

Prueba

1) Si el centro C de A es un campo, entonces C no tiene elementos nilpotentes diferentes de cero y C es generado por C^*, luego por (3.9) A es fuertemente invariante.

2) Si A es un anillo simple entonces los únicos ideales de A son A y $\{0\}$, luego A es un anillo local y su único ideal maximal es $\{0\}$, así $A^* = A - \{0\}$, por lo tanto el centro C de A es un anillo conmutativo y todos sus elementos diferentes de cero son unidades, es decir C es un campo y por (1) A es fuertemente invariante.

(3.11) Corolario :

Todo anillo artiniano semisimple es fuertemente invariante.

(3.12) Ejemplo 6 :

El anillo $M_2(\mathbb{Z}_2)$, de las matrices 2 x 2 con componentes en $\mathbb{Z}_2$ es fuertemente invariante. También $M_2(\mathbb{Q})$: anillo de matrices 2 x 2 con componentes racionales es fuertemente invariante.

Prueba

Es suficiente probar que $M_2(\mathbb{Z}_2)$ es anillo simple.

Sea $\mathcal{L}$ un ideal de $M_2(\mathbb{Z}_2)$, $\mathcal{L} \neq \{0\}$ y sea $A \in \mathcal{L}$, tal que

$A \neq 0$, entonces A es equivalente por filas a una de las siguientes matrices :

$$F_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad F_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad F_3 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad F_4 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

Además si A es equivalente a F_i, $i \in \{1, 2, 3, 4\}$, existe una matriz P que es producto de matrices elementales tal que $PA = F_i$ y como $A \in \mathcal{L}$ entonces $F_i \in \mathcal{L}$.

i) Si A es equivalente a F_1, entonces $F_1 \in \mathcal{L}$ y así $I \in \mathcal{L}$, luego $\mathcal{L} = M_2(\mathbb{Z}_2)$.

ii) Si A es equivalente a F_2, entonces $F_2 \in \mathcal{L}$ y además :

$$F_2 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = F_3$$

luego $F_3 \in \mathcal{L}$ y si $F_5 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$F_5 \in \mathcal{L}$, luego $F_2 + F_5 = I \in \mathcal{L}$, luego $\mathcal{L} = M_2(\mathbb{Z}_2)$.

iii) Si A es equivalente a F_3, $F_3 \in \mathcal{L}$, entonces por ii) $F_5 \in \mathcal{L}$ y como :

$$F_2 = F_3 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{entonces} \quad F_2 \in \mathcal{L}.$$

y así $F_2 + F_5 = I \in \mathcal{L}$.

Por lo tanto $\mathcal{L} = M_2(\mathbb{Z}_2)$.

iv) Si A es equivalente a F_4, $F_4 \in \mathcal{L}$, entonces $F_2 \in \mathcal{L}$ pues:

$$F_2 = F_4 \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Ahora: $F_2 + F_4 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = F_3 \in \mathcal{L}$

y por ii) $F_5 \in \mathcal{L}$, luego: $F_2 + F_5 = I \in \mathcal{L}$.

Por lo tanto $\mathcal{L} = M_2(\mathbb{Z}_2)$.

Análogamente el anillo $M_2(\mathcal{Q})$ de las matrices 2 x 2 con componentes racionales es un anillo simple y por lo tanto es fuertemente invariante.

(3.13) A continuación extenderemos el teorema (3.1) y anotaremos condiciones necesarias para que $(A[X])^*$ conste de elementos de la forma: $a_o + a_1 x + \ldots + a_n x^n$, donde a_o es unidad y $a_1, a_2, \ldots, a_n$ son elementos nilpotentes.

(3.14) Lema 1:

Si $\mathcal{A}$ es un ideal de un anillo A, tal que $(A/\mathcal{A})$ no tiene elementos nilpotentes diferentes de cero, y si $a_o + a_1 x + \ldots + a_n x^n$ es

una unidad en $A[X]$, entonces a_o es una unidad y $a_1, a_2, \ldots, a_n$ están en $\mathcal{a}$.

Prueba

Si $p = a_o + a_1 x + \ldots + a_n x^n$ es una unidad en $A[X]$, entonces existe $q = b_o + b_1 x + \ldots + b_m x^m$, tal que:

$$1 = pq = (a_o + a_1 x + \ldots + a_n x^n)(b_o + b_1 x + \ldots + b_m x^m),$$

luego $a_o b_o = 1 = b_o a_o$, es decir a_o es una unidad.

Consideremos ahora el homomorfismo canónico:

$\gamma: A[X] \longrightarrow (A/\mathcal{a})[x]$ definido por:

$$\gamma\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} \bar{b}_i x^i \ ;$$

como γ envía unidades en unidades, $\gamma(p) = \sum_{i=0}^{n} \bar{a}_i x^i$ es una unidad en $(A/\mathcal{a})[x]$, pero por (3.1) $\left[(A/\mathcal{a})[x]\right]^* = (A/\mathcal{a})^*$ ya que $(A/\mathcal{a})$ no tiene elementos nilpotentes diferentes de cero, entonces $\sum_{i=0}^{n} \bar{a}_i x^i$ es una unidad de $A/\mathcal{a}$; así que: $\sum_{i=1}^{n} \bar{a}_i x^i = \bar{0}$ y por lo tanto $\bar{a}_1 = \bar{a}_2 = \ldots = \bar{a}_n = \bar{0}$, es decir, $a_1, a_2, \ldots, a_n$ están en $\mathcal{a}$.

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE MEDELLIN
DEPTO. DE BIBLIOTECAS
BIBLIOTECA "EFE" GOMEZ

(3.15) Corolario :

Si el conjunto $\mathcal{N}$ de los elementos nilpotentes de A, forma un ideal de A, entonces una unidad en $A[X]$ tiene la forma :

$a_o + a_1 x + \ldots + a_n x^n$, donde $a_a \in A^*$ y $a_1, a_2, \ldots, a_n \in \mathcal{N}$.

Prueba

Si $\mathcal{N}$ es un ideal de A, tómese $\mathcal{A} = \mathcal{N}$ en el lema (3.14), pues $A/\mathcal{N}$ no tiene elementos nilpotentes diferentes de cero.

(3.16) Proposición :

Sea A un anillo, tal que para x, y en A, $xy = 0$ implica $yx = 0$; entonces dado un elemento x en A, tal que para algún entero positivo k, $x^k = 0$ y $y_1, y_2, \ldots, y_n$ elementos de A, se verifica $xy_1\, xy_2 \ldots xy_k = 0$.

Prueba

Si $x^k = 0$, entonces $x^k y_1 = 0$ y esto por hipátesis implica : $x^{k-1} y_1 x = 0$ y $x^{k-1} y_1 x y_2 = 0$. Por lo tanto $x^{k-2} y_1 x y_2 x = 0$ y por inducción se llega a $xy_1 x y_2 \ldots x y_k = 0$.

(3.17) Lema 2 :

Sea A un anillo tal que para x, y en A, $xy = 0$ implica $yx = 0$. Entonces el conjunto $\mathcal{N}$ de los elementos nilpotentes de A es un ideal de A.

Prueba

i) Sean $x \in \mathcal{N}$, $y \in A$, entonces existe un entero positivo k, tal que $x^k = 0$ y por la proposición anterior se verifica $(xy)^k = 0$ es decir $xy \in \mathcal{N}$; además como $xy_1\, xy_2 \ldots xy_k = 0$ entonces $y_k x y_1 x y_2 \ldots x y_{k-1} x = 0$ y para $y_i = y$, $i \in \{1, \ldots, k\}$ se tiene $(yx)^k = 0$, y así $yx \in \mathcal{N}$.

ii) Sean $x, z \in \mathcal{N}$ y sean k y r enteros positivos tales que $x^k = 0$ y $z^r = 0$, entonces en la expansión de $(x - z)^{k+r}$, cada término es un producto en el que aparece x repetida como factor al menos k veces o z repetida al menos r veces y como consecuencia de la proposición anterior todos sus términos son iguales a cero, luego $(x - z)^{k+r} = 0$, es decir $x - z \in \mathcal{N}$.

(3.18) TEOREMA

Sea A un anillo que satisface las hipótesis de (3.17). Entonces $A[X]^*$ consta de elementos de la formo:

$$a_o + a_1 x + \ldots + a_n x^n,$$

con $a_o \in A^*$ y $a_1, \ldots, a_n$ elementos nilpotentes de A.

Prueba

Por (3.17) y (3.15), las unidades de $A[X]$ son de la forma indica-

da en el enunciado anterior.

Recíprocamente: Sea $y = a_o + a_1 x + \ldots + a_n x^n$, con $a_o \notin A^*$ y $a_1, a_2, \ldots, a_n$ nilpotentes; podemos asumir $a_o = 1$ y así el inverso de y en el anillo de series formales de potencias de x, $A[[x]]$, es $1 + b_1 x + \ldots + b_m x^m + \ldots$ donde $b_m = \sum_{\text{poten}} a_{i_1} a_{i_2} \ldots a_{i_k}$ y $i_1 + i_2 + \ldots + i_k = m$ y existe un entero positivo N suficientemente grande, tal que para todo $m \geq N$, en cada sumando de b_m aparece al menos un a_i repetido como factor k_i veces donde k_i es el orden de nilpotencia de a_i (es decir $a_i^{k_i} = 0$); luego por (3.16) se sigue que para todo $m \geq N$, $b_m = 0$ y por lo tanto el inverso de y pertenece a $A[X]$, es decir y es una unidad en $A[X]$.

Notación

En lo que sigue para un anillo A, $J(A)$ denota el radical de Jacobson de A y $N = J(A[X]) \cap A$.

(3.19) Nota:

De acuerdo con los resultados presentados en el Lema 2 y en el Teorema central de la sección 0, se tiene $J(A[X]) = N[X]$, donde $N = J(A[X]) \cap A$ y N es un nilideal en A; así resulta interesante el estudio de la siguiente proposición:

(3.20) Proposición :

Sea A un anillo cuyos elementos nilpotentes forman un ideal $\mathcal{N}$ de A. Entonces las siguientes afirmaciones son equivalentes :

i) $J(A[X]) = \mathcal{N}[X]$

ii) $A[X]^*$ consta de elementos de la forma $a_o + a_1 x + \ldots + a_n x^n$ donde $a_o \in A^*$ y $a_1, a_2, \ldots, a_n$ son elementos nilpotentes de A.

Prueba

[i) $\Longrightarrow$ ii)]. Es inmediato por (3.15).

[ii) $\Longrightarrow$ i)]. Supongamos que ii) es cierta y sea :

$$p(x) \in J(A[X]),\ p(x) = p_o + p_1 x + \ldots + p_n x^n,$$

entonces para todo $q(x) \in A[X]$, $1 - p(x)q(x)$ es una unidad en $A[X]$, en particular $1 + p(x).x$ es una unidad en $A[X]$, es decir $1 + p_o x + p_1 x^2 + \ldots + p_n x^{n+1}$ está en $A[X]^*$; luego por ii): $p_o, p_1, \ldots, p_n$ son elementos nilpotentes de A y así $p(x) \in \mathcal{N}[X]$.

Ahora : Sea $p(x) \in \mathcal{N}[X]$, es decir $p(x) = p_o + p_1 x + \ldots + p_n x^n$ donde para $i \in \{0, 1, \ldots, n\}$, $p_i \in \mathcal{N}$, y sea :

$q(x) = q_o + q_1 x + \ldots + q_m x^m$ elementos de $A[X]$, entonces como $\mathcal{N}$ es un ideal, los coeficientes de $p(x)q(x)$ son sumas finitas de productos $p_i q_j$ con $p_i \in \mathcal{N}$, $q_j \in A$ y como $\mathcal{N}$ es ideal de A, se tiene $p_i q_j \in \mathcal{N}$, es decir $p(x)q(x) \in \mathcal{N}[X]$, luego por ii)

$1 - p(x)q(x)$ es una unidad de $A[X]$ y así (por proposición 2.4 en [6], p. 5), $p(x) \in J(A[X])$.

(3.21) Consecuencios:

1) Si el conjunto $\mathcal{N}$ de elementos nilpotentes de un anillo A es un ideal de A, entonces por (3.15) la afirmación ii) en (3.20) es cierta y por consiguiente: $J(A[X]) = \mathcal{N}[X]$.

2) Si A es un anillo tal que $\mathcal{N} \subset J(A[X])$, entonces como $J(A[X])$ es un ideal de $A[X]$ (ver 3.8 en [6], p. 9), se tiene que $\mathcal{N}[X] \subset J(A[X])$, pero $J(A[X]) = N[X]$, donde $N = J(A[X]) \cap A$; además N es un nilideal de A y así $N \subseteq \mathcal{N}$ y por lo tanto $N[X] \subseteq \mathcal{N}[X]$, luego: $J(A[X]) = N[X] = \mathcal{N}[X]$.

En particular si A es conmutativo, $\mathcal{N} \subseteq J(A[X])$ y $\mathcal{N}$ es un ideal de A (ver [6], p. 23), entonces se satisface (3.20) y se tiene que $J(A[X]) = N[X]$ es equivalente a i) y a ii) de (3.20).

3) Si A es anillo conmutativo y $\mathcal{N}$ es el nilradical de A, entonces $\mathcal{N}[X]$ es el nilradical de $A[X]$ (ver [5], ej. 2ii), p. 12) pero por (2) $\mathcal{N}[X] = J(A[X]) = N[X]$, luego $N[X]$, es nilradical de $A[X]$.

UNIVERSIDAD DEL VALLE COLOMBIA

4) Si A es un anillo Artiniano, $\mathcal{N} = J(A)$ (ver prop. 6.8 en [6]), luego $\mathcal{N}$ es un ideal de A y por (3.15) las unidades de $A[X]$ tienen la forma $a_o + a_1 x + \ldots + a_n x^n$ con $a_o \in A^*$ y $a_1, a_2, \ldots, a_n$ nilpotentes; luego por (3.20) $J(A[X]) = (J(A))[X]$.

5) Si A es un anillo artiniano a derecha entonces $J(A)$ es un ideal nilpotente, luego $J(A) \subset \mathcal{N}$ y así $(J(A))[X] \subset \mathcal{N}[X]$ y si además $\mathcal{N}$ es un ideal de A, entonces por (3.15) y (3.20) $J(A[X]) = \mathcal{N}[X]$ y así $(J(A))[X] \subset J(A[X])$.

6) Si A es un anillo conmutativo con unidad tal que todo ideal no contenido en el nilradical, contiene un elemento idempotente diferente de cero, entonces $\mathcal{N} = J(A)$ (ver [6] prop. 6.10) y por (3.20): $J(A[X]) = (J(A))[X]$.

(3.22) Observación 1:

En general $A[X]^*$ y el conjunto de elementos de la forma $a_o + a_1 x + \ldots + a_n x^n$ con $a_o \in A^*$ y $a_1, a_2, \ldots, a_n$ nilpotentes no son comparables, ésto lo verificamos mediante los ejemplos siguientes:

Ejemplo 7:

Sea $M_2(\mathbb{Q})$ el anillo de las matrices de orden 2 x 2 con compo-

nentes en el conjunto de los números racionales. El elemento :

$$Y = A_o + A_1 x + A_2 x^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} x + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} x^2$$

es tal que A_o es una unidad de $M_2(\mathbb{Q})$, A_1 y A_2 son elementos nilpotentes; veamos que Y no es una unidad en $(M_2(\mathbb{Q}))[X]$.

Prueba

En el anillo de series formales $(M_2(\mathbb{Q}))[[X]]$, consideremos el inverso de Y como :

$$Y' = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + B_1 x + B_2 x^2 + \ldots + B_m x^m + \ldots$$

y veamos que para todo k,

$$B_k = \begin{cases} I_2 & \text{si} \quad k \equiv 0 \pmod 3 \\ -A_1 & \text{si} \quad k \equiv 1 \pmod 3 \\ -A_2 & \text{si} \quad k \equiv 2 \pmod 3 \end{cases}$$

Esto puede verificarse si igualamos YY' a $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ y comparamos coeficientes; antes efectuamos los productos $A_1 A_2$ y $A_2 A_1$.

$$A_1 A_2 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$A_2 A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL

y se tiene : $A_1 A_2 + A_2 A_1 = I_2$

además : $A_1^2 = 0$ y $A_2^2 = 0$

Consideremos ahora los coeficientes de YY'

$A_o B_o = (I_2)^2 = I_2$ (pues $A_o = I_2 = B_o$)

El coeficiente de x :

$0 = A_o B_1 + A_1 B_o = B_1 + A_1$ luego $B_1 = - A_1$

El coeficiente de x^2 :

$0 = A_o B_2 + A_1 B_1 + A_2 B_o = B_2 - A_1^2 + A_2 = B_2 + A_2$

luego $B_2 = - A_2$

El coeficiente de x^3 :

$0 = A_o B_3 + A_1 B_2 + A_2 B_1 = B_3 - A_1 A_2 - A_2 A_1 = B_3 - I_2$

luego $B_3 = I_2$

El coeficiente de x^4 :

$0 = A_o B_4 + A_1 B_3 + A_2 B_2 = B_4 + A_1 - A_2^2 = B_4 + A_1$

luego $B_4 = - A_1$

Generalicemos por inducción :

Supongamos que $B_k = \begin{cases} I_2 & \text{si} \quad k \equiv 0 \pmod 3 \\ -A_1 & \text{si} \quad k \equiv 1 \pmod 3 \\ -A_2 & \text{si} \quad k \equiv 2 \pmod 3 \end{cases}$

El coeficiente de x^{k+1} en YY' es:

$$0 = A_o B_{k+1} + A_1 B_k + A_2 B_{k-1} = B_{k+1} + A_1 B_k + A_2 B_{k-1}$$

y así $B_{k+1} = -A_1 B_k - A_2 B_{k-1}$

i) Si $k + 1 \equiv 0 \pmod 3$ entonces $k \equiv 2 \pmod 3$ y

$k - 1 \equiv 1 \pmod 3$, luego $B_k = -A_2$ y $B_{k-1} = -A_1$,

así que $B_{k+1} = A_1 A_2 + A_2 A_1 = I_2$

ii) Si $k + 1 \equiv 1 \pmod 3$ entonces $k \equiv 0 \pmod 3$ y

$k - 1 \equiv 2 \pmod 3$, luego $B_k = I_2$ y $B_{k-1} = -A_2$

por lo tanto $B_{k+1} = -A_1 + A_2^2 = -A_1$

iii) Si $k + 1 \equiv 2 \pmod 3$ entonces $k \equiv 1 \pmod 3$ y

$k - 1 \equiv 0 \pmod 3$, luego $B_k = -A_1$ y $B_{k-1} = I_2$

y así $B_{k+1} = -A_1^2 - A_2 I_2 = -A_2$

Así queda probado que $Y' \notin (M_2(\mathbb{Q}))[X]$, es decir Y no es una unidad en $(M_2(\mathbb{Q}))[X]$.

Ejemplo 8:

En el anillo $(M_2(\mathbb{Q}))[X]$, el elemento

$$Z = A_o + A_1 x = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} x$$

es una unidad y no tiene coeficientes nilpotentes.

Prueba

$$A_o^{-1} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

$$A_o^{-1} Z = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix} x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} x$$

$A_o^{-1} Z$ es una unidad ya que si $Y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix} x$,

se verifica $(A_o^{-1} Z) Y = I_2$

Ahora : $$Y A_o^{-1} = \frac{1}{2}\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix} x\right\}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0 & 0 \\ -1 & 1 \end{bmatrix} x$$

y $Z(Y A_o^{-1}) = I_2$

Luego $Y A_o^{-1}$ es el inverso de Z en $A[X]$, es decir Z es una unidad de $A[X]$.

Sin embargo A_1 no es nilpotente pues $A_1^2 = A_1$ y por lo tanto $A_1^k = A_1 \neq 0$ para todo entero positivo k.

(3.23) Observación 2 :

La condición ii) de (3.20) no es necesaria, para que un anillo sea

fuertemente invariante; se puede concluír fácilmente de los ejemplos 6, 7 y 8 que $M_2(\mathbb{Q})$ es fuertemente invariante y no verifica dicha condición.

Concluiremos esta sección con un teorema que establece condiciones para que un anillo sea fuertemente invariante mediante el radical de Jacobson y en este sentido la proposición (3.20) y en particular su condición ii) es útil.

(3.24) TEOREMA

Sea A un anillo y $R = J(A)$ si se verifica $J(A[X]) = R[X]$ y A/R es fuertemente invariante; entonces A es fuertemente invariante.

Prueba

Sea B un anillo cualquiera y sea $\sigma : A[X] \longrightarrow B[X]$ un isomorfisma de anillos, camo el radical de Jacobson es invariante bajo isomorfismos (ver proposición 1 y nota 1 en la sección 0), entonces $\sigma(J(A[X])) = J(B[X])$, pero por hipótesis $J(A[X]) = R[X]$ y además $J(B[X]) = M[X]$, donde $M = J(B[X]) \cap B$ es un nil-ideal en B (ver Lema 2 y teorema en la Sección 0), luego, $\sigma(R[X]) = M[X]$. Sea $\sigma(x) = b_o + b_1 x + \ldots b_n x^n$, $b_i \in B$ y consideremos el isomorfismo $\psi : (A/R)[X] \longrightarrow (B/M)[X]$ dado

por : $\psi = \gamma \circ \bar{\sigma} \circ \varphi$

$$\begin{array}{ccc} A[X]/R[X] & \xrightarrow{\bar{\sigma}} & B[X]/M[X] \\ \varphi \uparrow & & \downarrow \gamma \\ (A/R)[X] & \xrightarrow[\psi]{} & (B/M)[X] \end{array}$$

donde : $\bar{\sigma}$ es el isomorfismo inducido por σ .

$$\varphi : (A/R)[X] \longrightarrow \underline{A[X]/R[X]}$$

$$\sum_{i=0}^{n} \bar{a}_i x^i \longmapsto \sum_{i=0}^{n} a_i x^i$$

$$\gamma : \underline{B[X]/M[X]} \longrightarrow (B/M)[X]$$

$$\sum_{i=0}^{n} b_i x^i \longmapsto \sum_{i=0}^{n} \bar{b}_i x^i$$

Se tiene : $\psi(x) = \bar{b}_o + \bar{b}_1 x + \ldots + \bar{b}_n x^n$ donde $\bar{b}_i$ denota la clase $b_i + M$ en B/M. Como A/R es fuertemente invariante $\psi(x)$ es un (B/M)-generador de $(B/M)[X]$ y por lo tanto : $(B/M)[\psi(x)] = (B/M)[X]$; así el homomorfismo de : $(B/M)[X] \longrightarrow (B/M)[X]$ inducido por $x \longmapsto \psi(x) = \bar{b}_o + \bar{b}_1 x + \ldots + \bar{b}_n$ es sobre y por (2.4) $\bar{b}_1$ es una unidad en B/M y $\bar{b}_2, \ldots, \bar{b}_n$ son nilpotentes en B/M y $\bar{b}_o, \bar{b}_1, \ldots, \bar{b}_m$ son centrales. Como M es un nilideal en B, $M \subset J(B)$ y $\bar{b}_1$ es una unidad en B/M existe $c_1 \in B$ tal que $b_1 c_1 - 1 \in M \subset J(B)$; así que $b_1 c_1 - 1 = y \in J(B)$,

entonces $b_1 c_1 = 1 + y$ y $1 + y$ es una unidad en B (ver 2.4 en [6]), por lo tanto b_1 es una unidad en B.

Ahora: Como $\bar{b}_2, \ldots, \bar{b}_n$ son elementos nilpotentes en B/M, existen enteros positivos $r_2, \ldots, r_n$, tales que $b_2^{r_2}, \ldots, b_n^{r_n}$ pertenecen a M; y como M es un nilideal en B, se concluye que: $b_2^{r_2}, \ldots, b_n^{r_n}$ son elementos nilpotentes en B y por lo tanto $b_2, \ldots, b_n$ son elementos nilpotentes en B.

De lo anterior se puede concluir usando (2.4) que $\sigma(x)$ es un B-generador de $B[X]$ y así A es fuertemente invariante.

(3.25) Corolario:

Todo anillo artiniano (a izquierda o a derecha) es fuertemente invariante.

Prueba

Si A es artiniano (a izquierda o a derecha), entonces J(A) es un ideal nilpotente de A y $J(A) = \mathcal{N}$, donde $\mathcal{N}$ es el conjunto de elementos nilpotentes de A (ver 6.8 y 6.9 en [6]); así que por (3.15) y (3.20) se tiene $J(A[X]) = (J(A))[X]$. Además $A/J(A)$ es artiniano (a izquierda o a derecha) y por 6.12 en [6], $A/J(A)$ es semi-simple, luego $A/J(A)$ es fuertemente invariante (por 3.11).

De lo anterior se concluye, usando (3.24) que A es fuertemente invariante.

4. DOMINIOS FUERTEMENTE INVARIANTES

(4.1) Sea D un dominio de integridad y sea K el campo de fracciones de D.

Sea $S_o = \left\{ x \in \langle D^* \rangle / x \neq 0 \right\}$

donde $\langle D^* \rangle$: es el anillo generado por las unidades de D.

Definimos :

$$D_1 = S_o^{-1} D = \left\{ d/s \,/ s \in S_o \wedge d \in D \right\} \subseteq K \quad (\text{con } \frac{d}{s} = s^{-1} d)$$

y sea $S_1 = \left\{ x \in \langle D_1^* \rangle / x \neq 0 \right\}$

$$D_2 = S_1^{-1} D_1 = \left\{ d/s \,/ s \in S_1 \wedge \quad d \in D_1 \right\}$$

Para $n > 1$, definimos :

$$D_n = S_{n-1}^{-1} D_{n-1} = \left\{ d/s \,/ s \in S_{n-1} \wedge d \in D_{n-1} \right\}$$

y $$S_n = \left\{ x \in \langle D_n^* \rangle / x \neq 0 \right\}$$

(4.2) Observaciones:

1) Cada S_i, $i \in \{0, 1, 2, \ldots\}$, es un subconjunto multiplicativamente cerrado de D_i.

En efecto: $1 \in S_i$ y si s, s' son generados por las unidades de D_i, también ss' es generado por las unidades de D_i, es decir $ss' \in S_i$.

2) Para $n \geq 1$, $D_n = S_{n-1}^{-1} D_{n-1}$ es un dominio de integridad.

Por 1) $D_1 = S_o^{-1} D$ es anillo conmutativo con unidad;

además: $\frac{d_1}{s_1} \cdot \frac{d_2}{s_2} = 0 \implies \frac{d_1 d_2}{s_1 s_2} = 0$

$$\implies d_1 d_2 = 0 \implies d_1 = 0 \text{ ó } d_2 = 0$$
$$\implies \frac{d_1}{s_1} = 0 \text{ ó } \frac{d_2}{s_2} = 0$$

3) $D \subset D_1 \subset D_2 \subset \ldots \subset D_{n-1} \subset D_n \subset \ldots$.

4) $\tilde{D} = \bigcup_{n \in \mathbb{Z}^+} D_n$ es un dominio de integridad.

5) $\tilde{D}_1 = \tilde{D}$

Dm: $\tilde{D} \subset \tilde{D}_1$. Veamos que $\tilde{D}_1 = \tilde{D}$:

Sea $x \in \tilde{D}_1$ entonces $x = \frac{d}{S}$ donde S es suma finita de productos finitos de unidades de $\tilde{D}$ y $d \in \tilde{D}$;

Pero, dadas $u_1, u_2, \ldots, u_k$ unidades de $\tilde{D}$, existe $n \in \mathbb{Z}^+$ tal que $u_1, u_2, \ldots, u_k$ y $u_1^{-1}, u_2^{-1}, \ldots, u_k^{-1}$ están en D_n y como D_n es dominio de integridad, las sumas finitas de productos finitos de elementos de D_n están en D_n. Además existe $m \in \mathbb{Z}^+$, tal que $d \in D_m$ ya que $d \in \tilde{D}$, luego $\frac{d}{s} \in D_{N+1}$ donde $N = \text{máx}(n,m)$ y como $D_{N+1} \subset \tilde{D}$ se concluye que $\tilde{D}_1 = \tilde{D}$.

6) Si denotamos por K_n, $n \in \mathbb{N}_o$, el campo de fracciones de D_n, se tiene que $\forall\, n \in \mathbb{Z}^+$, $K \subseteq K_n \subseteq K_{n+1}$.

[Ya que: $D \subset D_n \subset D_{n+1} \subset K_{n+1}$ y K_n es el menor campo que contiene a D_n y K el menor campo que contiene a D].

Pero además: Como $D \subset D_1 \subseteq K$, entonces $K_1 \subseteq K$; luego $K = K_1$, análogamente para todo n,
$D = D_0 \subset D_1 \subset \ldots \subset D_{n-1} \subset D_n \subset K_{n-1}$, luego $K_n \subset K_{n-1}$ y así $\forall\, n$, $K_n = K_{n-1} = \ldots = K_1 = K$.

7) El campo de fracciones de $\tilde{D}$ es K (igual al campo de fracciones de D).

<u>En efecto</u>: Sea F el campo de fracciones de $\tilde{D}$; como para todo $n \in \mathbb{Z}^+$, $D_n \subset K$ entonces $\tilde{D} = \bigcup_{n \in \mathbb{Z}^+} D_n \subset K$.
Luego $F \subset K$.

UNIVERSIDAD DE COLOMBIA
BIBLIOTECAS

Además $\tilde{D} \subset F$ y $D \subset \tilde{D}$, luego $D \subset F$ y como K es el campo de fracciones de D, se tiene que $K \subseteq F$.

Conclusión: $F = K$.

(4.3) TEOREMA

Sea D un dominio de integridad tal que $\tilde{D} = K$. Entonces D es un anillo fuertemente invariante.

Prueba:

Sea E un anillo, tal que $D[X] \cong E[X]$; como D es un dominio de integridad, no tiene elementos nilpotentes diferentes de cero; entonces E no tiene elementos nilpotentes diferentes de cero, luego por (3.1) $E[X]^* = E^*$ (1)

Sea $\gamma: D[X] \longrightarrow E[X]$ un isomorfismo, por (1), si: $S_i \in \langle D^* \rangle$ entonces $\gamma(S_i) \in \langle E^* \rangle$, así:

$$\gamma_1: D_1[X] \longrightarrow E_1[X]$$

$$\sum_{i=0}^{n} \left(\frac{d_i}{S_i}\right) x^i \longmapsto \sum_{i=0}^{n} \frac{\gamma(d_i)}{\gamma(S_i)} (\gamma(x))^i$$

es un isomorfismo, extensión de γ. Inductivamente, cualquier iso-

morfismo $\gamma_n : D_n[X] \longrightarrow E_n[X]$ puede ser extendido a un isomorfismo $\gamma_{n+1} : D_{n+1}[X] \longrightarrow E_{n+1}[X]$.

Por lo tanto existe un isomorfismo $\sigma : \tilde{D}[X] \longrightarrow \tilde{E}[X]$. Como $\tilde{D} = K$, todas las constantes no nulas de $\tilde{D}[X]$ son unidades; además $E[X]^* = E^*$ y todo isomorfismo envía unidades en unidades, así $\tilde{E}[X]^* = \tilde{E}^*$ y se sigue que $\sigma(\tilde{D}) \subseteq \tilde{E}$.

Ahora, si $\sigma(D) \not\subseteq E$, existe $d \in D$ tal que $\sigma(d)$ es un polinomio no constante y por las extensiones, $\sigma(d) \in \sigma(\tilde{D})$ y así $\sigma(\tilde{D}) \not\subseteq \tilde{E}$ (contradicción!).

Luego $\sigma(D) \subseteq E$ y por el Corolario (2.5), $\sigma(D) = E$ y así $\sigma(x)$ es un E-generador de $E[X]$, luego D es fuertemente invariante.

(4.4) Un campo de números algebraicos es cualquier extensión finita del campo $\mathbb{Q}$ de los números racionales.

Sea L un campo de números algebraicos, $\mathbb{Z}$ el conjunto de los números enteros y I_L la clausura entera de $\mathbb{Z}$ en L. I_L es un

subanillo de L, llamado el anillo de enteros algebraicos de L.

Así que: α es un entero algebraico de L si existe un polinomio mónico irreducible $f(x) \in \mathbb{Z}[X]$, tal que $f(\alpha) = 0$.

(4.5) Corolario:

Sea D el anillo de los enteros algebraicos en un campo de números algebraicos L. Entonces D es fuertemente invariante.

Prueba

Sea K el campo de fracciones de D. Sea S el conjunto de elementos diferentes de cero en el anillo generado por las unidades de D, veamos que $D_1 = S^{-1} D = K$ y así $\tilde{D} = K$:

En efecto: Si $d \in D$ y $d \neq 0$, sea $f(x) \in \mathbb{Z}[X]$ el polinomio mónico irreducible tal que $f(d) = 0$ y $d = d_1, d_2, \ldots, d_n$ las raíces de f, entonces para $i \in \{1, 2, \ldots, n\}$, $d_i \in D$ y además $d_1 d_2 \ldots d_n = \pm a$ donde a es el término independiente de $f(x)$.

Sea $t = d_2 d_3 \ldots d_n$, entonces $dt = \pm a$, con $a \in \mathbb{Z}$ y $t \in D$, es decir $\frac{1}{d} = \pm \frac{t}{a}$ y así $\frac{1}{d} = \frac{t}{s}$ con $t \in D$, $s \in \mathbb{Z}$.
Luego para todo $d \in D$, $d \neq 0$, $\frac{1}{d} \in \mathbb{Z}^{-1} D$. Ahora: Sea $k \in K$, entonces $k = \frac{d_1}{d_2}$ con $d_1, d_2 \in D$, $d_2 \neq 0$, pero $\frac{1}{d_2} = \frac{t}{s}$ con $t \in D$ y $s \in \mathbb{Z}$, por lo tanto $\frac{d_1}{d_2} = \frac{d_1 t}{s} = \frac{d'}{s}$ con $d' \in D$ y $s \in \mathbb{Z}$; como consecuencia $K = \mathbb{Z}^{-1} D$; pero

$\mathbb{Z} \subset S$ y así $K = \mathbb{Z}^{-1} D \subseteq S^{-1} D$ y claramente $S^{-1} D \subseteq K$, luego $D_1 = S^{-1} D = K$.

Así $\tilde{D} = D_1 = K$ y por el teorema (4.3) D es fuertemente invariante.

Nota: Si L es un campo y A es un subanillo de L, tal que L es algebraico sobre el campo de fracciones de A, entonces para cualquier subanillo B de L tal que $A \subset B$, $\tilde{B}$ es el campo de fracciones de B. Por lo tanto cualquier subanillo de una extensión algebraica del campo de los números racionales es fuertemente invariante.

BIBLIOGRAFIA

[1] D.B. COLEMAN and E. ENOCH. "Isomorphic Polynomial Rings", Proc. Amer. Math. Soc. 27 (1971), pp. 247-252.

[2] S.A. AMITSUR. "Radicals of polynomial rings", Canad. J. Math. 8 (1956), pp. 355-361.

[3] S. ABHYANKAR, W. HEINZER and P. EAKIN. "On the uniqueness of the coefficient ring in a polynomial ring", Journal of Algebra 23 (1972), pp. 310-342.

[4] GILMER, R. "R-automorphisms of R[X]". Proc. London Math. Soc. (3) 18 (1968), pp. 328-336.

[5] ATHIYAH, M.F. & MAC DONALD, I.G. "Introducción al Algebra Canmutativa", Ed. Reverté S.A., Barcelona, 1975.

[6] TEJADA, D. "El radical de Jacobson", Publ. Universidad Nacional, Medellín, Abril de 1986.

[7] TEJADA, D. "Teoría de Algebras", Publ. Universidad Nacional, Medellín, Febrero 1986.

UNIV... NAC... BIBL... CENTR...