UN MODELO ELEMENTAL PARA LAS CLASES DE IDEALES DE UN ANILLO ALGEBRAICO. II

J. Ochoa

Recibido: 1-II-78

PRESENTADO POR EL ACADÉMICO EXCMO. SR. GERMÁN ANCOCHEA QUEVEDO

El Dr. Hans Peter Rehm, que tuvo la amabilidad de leer detenidamente la primera parte de mi trabajo «Un modelo elemental para las clases de ideales de un anillo algebraico» [1] y al que agradezco muy sinceramente su valiosa colaboración, demostró mediante un contraejemplo, que las condiciones exigidas en el enunciado del teorema 1-4 no son suficientes para la existencia de A-matrices semejantes a una matriz dada. Con posterioridad, publicó [2] un teorema en el que se dan condiciones suficientes para la existencia de dichas matrices. A continuación damos las condiciones necesarias y suficientes para la existencia de A-metrices y en particular, el teorema de Rehm. Añadimos algunos complementos y aclaraciones a [1].

1. Existencia de A-matrices

I-1. LEMA.—*Si la matriz M de orden* n, *tiene por ecuación mínima su ecuación característica y* $\overline{X} = (x_1, \ldots, x_n)$ *es un vector arbitrario, el máximo común divisor de los determinantes de los menores de orden* h + 1 *de la matriz,*

$$\begin{pmatrix} \overline{X} \\ \overline{X}M \\ \vdots \\ \overline{X}M^h \end{pmatrix} \tag{1.2}$$

es independiente de $\overline{X}$, *para todo* $h \leqslant n - 2$.

DEMOSTRACIÓN. — Procederemos por inducción sobre n. Para $n = 2$, el lema es evidente, lo supondremos cierto para toda matriz de orden inferior a n y para la matriz M de orden n, supondremos que sea h el menor número para el que no se cumple el lema. Indudablemente, $h > 2$. Si representamos por $F(x_j)$, $(j = 1, \ldots, n)$, la forma homogénea M. C. D. de los determinantes de los menores de orden $h + 1$ de la matriz 1.2, en virtud de las hipótesis admitidas, existirán polinomios

$$P_i(x_j) \quad (j = 1, \ldots, n, \quad i = 0,1, \ldots, h-1)$$

tales que se verifique:

$$\overline{X}\, M^h \equiv \sum_{i=0}^{h-1} P_i(X_j)\, \overline{X}\, M^i \quad \text{mod} \quad F(x_j). \tag{1.3}$$

Si representamos por M_0, la forma normal de Jordan correspondiente a la matriz M, existe una matriz unitaria B tal que,

$$M = B\, M_0\, B^{-1}$$

Sustituyendo esta expresión de M en (I-3) resulta,

$$\overline{X}\, B\, M_0^h\, B^{-1} \equiv \sum_{i=0}^{h-1} P_i(x_j)\, \overline{X}\, B\, M_0^i\, B^{-1} \quad \text{mod} \quad F(x_j). \tag{1.4}$$

Si hacemos $\overline{X}\, B = \overline{Y}$, por ser B unitaria, la correspondencia entre los vectores $\overline{X}$ e $\overline{Y}$ es biunívoca, $\overline{X} = \overline{Y}\, B^{-1}$, con lo cual $F(x_j)$ se transformará en $F(y_j)$, los $P_i(x_j)$ en $P_i(y_j)$ y la relación I-4, la podemos escribir en la forma,

$$\overline{Y}\left(M_0^h - \sum_{i=0}^{h-1} P_i(y_j) M_0^i\right) B^{-1} \equiv 0 \quad \text{mod} \quad F(y_j).$$

Como la matriz B es independiente de $\overline{Y}$, de la anterior resulta,

$$\overline{Y}\, M_0^h \equiv \overline{Y} \sum_{i=0}^{h-1} P_i(y_j)\, M_0^i \quad \text{mod} \quad F(y_j).$$

En consecuencia, *basta demostrar el lema para matrices M_0 de Jordan.*

La matriz M_0 podrá ponerse en la forma,

$$M_0 = \begin{pmatrix} r_1 & a_1 & 0 & \dots & 0 \\ 0 & & & & \\ \vdots & & M_1 & & \\ 0 & & & & \end{pmatrix}$$

con $a_1 = 0$ si la ecuación característica de la matriz M tiene, al menos, una raíz simple y $a_1 = 1$ si dicha ecuación carece de raíces simples. M_1 es matriz de Jordan de orden $n - 1$, con la propiedad de que su ecuación característica es también mínima. De la forma de M_0 se deduce,

$$M^i_0 = \begin{pmatrix} r^i_1 & a_1 & \dots & a_i & 0 & \dots & 0 \\ 0 & & & & & & \\ \vdots & & & M^i_1 & & & \\ 0 & & & & & & \end{pmatrix}$$

para $i = 1, \dots, n - 2$. Si $a_1 = 0$, todos los a_i son ceros.

Si suponemos que para todo $\overline{Y}$, el M. C. D. de los determinantes de los menores de orden $h + 1$ de la matriz,

$$\begin{pmatrix} \overline{Y} \\ \overline{Y} M_0 \\ \vdots \\ \overline{Y} M_0{}^h \end{pmatrix} \tag{1.5}$$

es $F(y_j)$ y consideramos el vector particular

$$\overline{Y} = (0, y_2, \dots, y_n),$$

todos los elementos de la primera columna de la matriz 1.5, son cero, en consecuencia, todos los determinantes de los menores de orden $h + 1$ de dicha matriz en los que intervenga la primera columna son iguales a cero, pero los determinantes de los menores de orden $h + 1$, en los que no intervenga la primera columna, seguramente existentes (para $h = n - 2$ hay uno), no pueden ser iguales a cero, ya que esto implicaría que para todo

$$\overline{Y}_2 = (y_2, \dots, y_n),$$

los determinantes de los menores de orden $h + 1$, de la matriz,

$$\begin{pmatrix} \overline{Y}_2 \\ \overline{Y}_2 M_1 \\ \vdots \\ \overline{Y}_2 M_1{}^h \end{pmatrix} \tag{1.6}$$

fuesen iguales a cero, lo cual equivale a que la ecuación mínima de la matriz M_1 es de grado menor o igual a $h \leqslant n - 2$, en contra de la hipótesis admitida de ser dicho grado igual a $n - 1$. Si $h = n - 2$, los determinantes de todos los menores de orden $h + 1$ de la matriz 1.6, por hipótesis, tendrán por M. C. D. F (y_j), con $j = 2, \ldots, n$, pero esto es imposible por la hipótesis inductiva de ser cierto el lema para todas las matrices de orden inferior a n. Por consiguiente, sólo queda por demostrar el caso en que $h = n - 2$ y el vector $\overline{Y}$ tiene $y_1 \neq 0$. En estas condiciones, los determinantes de los menores de orden $n - 1$ de la matriz 1.5, coinciden con los correspondientes de la matriz,

$$\left.\begin{matrix} \overline{Y} \\ \overline{Y}(M_0 - r_1 U) \\ \overline{Y} M_0 (M_0 - r_1 U) \\ \vdots \\ \overline{Y} M_0{}^{n-3} (M_0 - r_1 U) \end{matrix}\right\} \quad U = \text{matriz unitaria de orden n.}$$

La primera columna de esta matriz es, $(y_1, 0, \ldots, 0)'$, por lo tanto, el M. C. D. de los determinantes de los menores de orden $n - 2$, de la matriz,

$$\begin{pmatrix} \overline{Y}(M_0 - r_1 U) \\ \overline{Y} M_0 (M_0 - r_1 U) \\ \vdots \\ \overline{Y} M_0{}^{n-3} (M_0 - r_1 U) \end{pmatrix} \tag{1.7}$$

es F (y_j). Ahora bien, las matrices M_0 y $M_0 - r_1 U$ conmutan, por tanto, la matriz I-7 puede ponerse en la forma,

$$\begin{pmatrix} \overline{Y}(M_0 - r_1 U) \\ \overline{Y}(M_0 - r_1 U) M_0 \\ \vdots \\ \overline{Y}(M_0 - r_1 U) M_0{}^{n-3} \end{pmatrix} \tag{1.8}$$

Si hacemos $\overline{Y}\,(M_0 - r_1\,U) = \overline{Z}$, el vector $\overline{Z}$ es un vector arbitrario que cumple la condición $z_1 = 0$ y resulta que el máximo común divisor de los determinantes de los menores de orden $n-2$ de la matriz,

$$\begin{pmatrix} \overline{Z} \\ \overline{Z}\,M_0 \\ \vdots \\ \overline{Z}\,M_0^{n-3} \end{pmatrix}$$

es función del vector $\overline{Z}$, pero esto es imposible, ya que para la matriz I-5 vimos que para que esto fuera posible, necesariamente tenía que ser $h = n - 2$.

En la demostración se ha supuesto que la ecuación característica de la matriz M tiene una raíz distinta de cero, si no fuera así, M_0 tendría la forma,

$$\begin{pmatrix} 0\ 1\ 0\ \ldots\ 0 \\ 0\ 0\ 1\ \ldots\ 0 \\ \ldots\ldots\ldots\ldots \\ 0\ 0\ 0\ \ldots\ 0\ 1 \\ 0\ 0\ 0\ \ldots\ 0\ 0 \end{pmatrix}.$$

En este caso, el determinante del menor de orden $n-1$, constituido por las $n-1$ primeras columnas de la matriz 1.5, con $h = n - 2$, es igual a y_1^{n-1} y el determinante del menor constituido por las $n-1$ últimas columnas de dicha matriz no es múltiplo de y_1. En consecuencia, el M. C. D. de los determinantes de los menores de orden $n-1$ de la matriz es igual a uno. Queda así demostrado el lema en todos los casos posibles.

Ahora estamos en condiciones de demostrar:

I-9. TEOREMA.—*Si la matriz M tiene por ecuación mínima su ecuación característica, la condición necesaria y suficiente para que M sea semejante a una A-matriz es que las matrices,*

$$M^0 = U, M, \ldots, M^{n-1}$$

sean linealmente independientes sobre Z/p, para todo primo p, *o lo que es igual, que la ecuación mínima de M sobre Z/p, sea, al menos, de grado* $n-1$ *para todo primo* p.

DEMOSTRACIÓN.—La relación

$$\sum_{i=0}^{n-2} M^i \lambda_i \equiv 0 \mod p \quad \lambda_i \in Z, \quad 0 = \text{matriz nula}$$

es invariante en la semejanza de matrices. En efecto, si

$$B = X\,M\,X^{-1},$$

se verifica,

$$X\,(\Sigma \lambda_i M^i)\,X^{-1} \equiv X\,O\,X^{-1} \mod p$$

por tanto,

$$\Sigma \lambda_i\, X\, M^i X^{-1} \equiv 0 \mod p$$

es decir,

$$\Sigma \lambda_i B^i \equiv 0 \mod p.$$

Si A es A-matriz, las matrices: U, A, ..., A^{n-2}, son linealmente independientes sobre Z/p para todo primo p. En consecuencia, la condición es necesaria.

En virtud del teorema I-4 de [1], para demostrar la suficiencia basta demostrar que existe un vector entero X, tal que el M. C. D. de los determinantes de los menores de orden $n-1$ de la matriz,

$$\begin{pmatrix} \overline{X} \\ \overline{X}\,M \\ \vdots \\ \overline{X}\,M^{n-2} \end{pmatrix} \tag{1.10}$$

es igual a uno. Si dicho M. C. D. fuera múltiplo de un número primo p, para todo $\overline{X}$, existirían enteros λ_i tales que,

$$\sum_{i=0}^{n-2} \lambda_i \overline{X}\, M^i \equiv 0 \mod p$$

es decir,

$$\overline{X}\left(\sum_{i=0}^{n-2} \lambda_i M^i\right) \equiv 0 \mod p,$$

para todo $\overline{X}$, lo cual implica,

$$\sum_{i=0}^{n-2} \lambda_i M^i \equiv 0 \mod p,$$

en contra de la hipótesis.

Si el M. C. D. de los determinantes de los menores de orden $n-1$ de la matriz I-10, es un número $m \neq 1$ para todo $\overline{X}$ y m varía con $\overline{X}$, esto equivale a que considerado el problema formalmente, el M. C. D. de dichos determinantes es una función homogénea $F(x_j)$ de las componentes x_j del vector X, pero esto es imposible en virtud del lema I-1. Por tanto, queda justificada la suficiencia y con ella demostrado el teorema.

Si

$$N = \sum_{i=0}^{n-2} \lambda_i M^i \equiv 0 \mod p \qquad (\lambda_i \in Z, \lambda_i \not\equiv 0 \mod p, \text{ para todo } i),$$

la matriz N tendrá por ecuación característica,

$$Q(y) = \det(N - y U) = \sum_{i=n}^{0} a_{n-i} y^i = 0 \tag{1.11}$$

con

$$a_0 = (-1)^n, \quad a_i \equiv 0 \mod p^i \quad (i = 1, \ldots, n).$$

La anterior ecuación es la transformada de la ecuación característica de la matriz M,

$$P(x) = \det(M - x U) = 0,$$

mediante,

$$y = \sum_{i=0}^{n-2} \lambda_i x^i.$$

La ecuación,

$$Q(y) \equiv 0 \mod p,$$

tiene la única solución, $y \equiv 0 \bmod p$, con multiplicidad n. En consecuencia, dada la ecuación $P(x) = 0$, para que exista la transformación

$$y = \sum_{i=0}^{n-2} \lambda_i x^i,$$

de forma que la transformada $Q(y) = 0$, de $P(x) = 0$, sea de la forma I-11, es necesario y suficiente que se cumpla alguna de las dos condiciones siguientes:

a) $P(x) \equiv 0$ *mod* p, *tiene una raíz* x_1 *al menos triple.*

En efecto, si $P(x) \equiv (x - x_1)^3 P_1(x) \bmod p$, la transformada de $P(x) = 0$, mediante $y = (x - x_1) P_1(x)$, cumple la condición de que $Q(y) \equiv 0 \bmod p$, tiene la raíz $y \equiv 0$ con multiplicidad n.

b) $P(x) \equiv 0$ *mod* p *tiene, al menos, dos raíces* x_1, x_2 *dobles.*

En efecto, si

$$P(x) \equiv (x - x_1)^2 (x - x_2)^2 P_1(x) \mod p,$$

la transformada de $P(x) = 0$, mediante la transformación,

$$y = (x - x_1)(x - x_2) P_1(x)$$

cumple la condición de que $Q(y) \equiv 0 \bmod p$, tiene la raíz $y \equiv 0$. con multiplicidad n.

En estas condiciones podemos enunciar:

I-12. TEOREMA.—*Si la ecuación*

$$P(x) = (-1)^n x^n + \sum_{i=n-1}^{0} a_{n-i} x^i = 0,$$

$a_i \in Z$, *no tiene raíces múltiples, las condiciones necesarias y suficientes para que toda matriz entera M, de ecuación característica* $P(x) = 0$, *sea semejante a una A-matriz son:*

1.ª) *Para cada primo* p, *no existe un* $a \in Z$, *tal que*

$$P(x) \equiv 0 \mod p^2,$$

para todo $x \equiv a$ *mod* p.

2.ª) *Para cada primo* p, *no existen* a, b $\in Z$, *tales que,*

$$P(x) \equiv 0 \mod p^2 \text{ para todo } x \equiv a \mod p.$$
$$P(x) \equiv 0 \mod p^2 \text{ para todo } x \equiv b \mod p.$$

DEMOSTRACIÓN.—En efecto, si $P(x) = 0$ no tiene raíces múltiples y la matriz M tiene por ecuación característica $P(x) = 0$, forzosamente, su ecuación mínima es también $P(x) = 0$. Si se cumplen las condiciones 1.ª) y 2.ª), no puede existir ninguna relación de la forma,

$$\sum_{i=0}^{n-2} \lambda_i M^i \equiv 0 \mod p,$$

por lo tanto, en virtud de I·9, queda demostrado el teorema.

Si la ecuación,

$$P(x) \equiv 0 \mod p,$$

tiene raíces múltiples, p es divisor del discriminante de la ecuación $P(x) = 0$.

Si

$$P(x) \equiv (x - a)^2 P_1(x) \mod p$$

la transformada $Q(y) = 0$ de $P(x) = 0$, mediante $y = (x - a) P_1(x)$, cumple la condición,

$$Q(y) \equiv 0 \mod p^n \text{ para todo } y \equiv 0 \mod p,$$

por tanto, $Q(y)$ es de la forma

$$Q(y) = y^n + b_1 y^{n-1} + \ldots + b_n \quad \text{con, } b_i \equiv 0 \mod p^i.$$

Si en $Q(y) = 0$, hacemos, $y = p z$, se transforma en $R(z) = 0$, con

$$R(z) = z^n + b' z^{n-1} + \ldots + b'_n, \quad \text{con} \quad b_i' = b_i / p^i.$$

La ecuación $R(z) = 0$, tiene sus coeficientes enteros y es la transformada de $P(x) = 0$, mediante la transformación,

$$z = \frac{(x - a) P_1(x)}{p}$$

por tanto, el orden Z $[x]$, (P $(x) = 0$), no es maximal. Como consecuencia de esta observación y de los teoremas I-9, I-12, podemos enunciar:

I-13. TEOREMA DE REHM.—*Si la ecuación* $P(x) = 0$ *tiene sus coeficientes en* Z *y es irreducible sobre* Z, *es condición suficiente para que toda matriz* M *con elementos enteros racionales y ecuación característica* $P(x) = 0$, *sea semejante a una A-matriz, que el orden* $Z[x]$ *sea máximo.*

Si la ecuación mínima de la matriz M de orden n y elementos enteros es de grado $n - 1$, evidentemente la ecuación P $(x) = 0$, característica de M, tiene al menos una raíz doble que es un entero racional.

Si la matriz M de orden n y ecuación mínima de grado $n - 1$, es semejante a una A-matriz, en virtud de las I-5 de [1], $a_n = b_1 = 0$. En consecuencia, la A-matriz semejante a M es de la forma:

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & 0 \\ 0 & 0 & 0 & \dots & 0 & r \end{pmatrix}$$

en donde r es raíz doble de la ecuación característica P $(x) = 0$. De acuerdo con las I-11 de [1], las a_i $(i = 1, \dots, n - 1)$, están unívocamente determinadas por P (x) y r. En consecuencia, podemos enunciar:

I-14. TEOREMA.—*Si las matrices* M_1, M_2 *de polinomio característico* $P(x) = (x - r)^2 P_1(x)$ *y ecuación mínima* $(x - r)P_1(x) = 0$, *son semejantes a una M-matriz, son semejantes.*

I-15. TEOREMA.—*Dado el polinomio* $P(x) = (x - r)^2 P_1(x)$, *con coeficientes en* Z, *la condición necesaria y suficiente para que toda matriz entera* M, *de polinomio característico* $P(x)$ *y ecuación mínima* $(x - r) P_1(x) = 0$, *sea semejante a una A-matriz, es que dichas matrices pertenezcan a la misma clase.*

2. Construcción del modelo

Para poder garantizar la validez del teorema IV-6 (definición del modelo) de [1] es necesario comprobar que los ideales de grado superior a uno, cuya norma es menor que k, están incluidos en el grupo producto de los subgrupos cíclicos de clases engendradas por los elementos del conjunto local completo, reducido, del polinomio $P(x)$.

Sea G el grupo de clases de ideales del anillo $Z(\Theta)$ ($P(\Theta) = 0$) y h su orden. Representaremos por G_1 el grupo producto de los grupos cíclicos de clases engendrados por los elementos del conjunto local, completo, reducido, del polinomio $P(x)$ y por h_1 su orden. Evidentemente, se verifica: G_1 es subgrupo de G y, por tanto, h_1 divisor de h. La relación existente entre las clases c_i de ideales del anillo $Z(\Theta)$ ($P(\Theta) = 0$) y el subgrupo G_1, queda establecida del modo siguiente:

1) Si en la clase c_i existe un ideal de primer grado cuya norma sea menor que k, c_i pertenece a G_1.

2) Si en la clase c_i no existe ningún ideal de primer grado cuya norma sea menor que k, pero en la clase

$$c_i^r \ (r \in N, \text{M. C. D}(r, k) = 1),$$

existe un ideal de primer grado de norma menor que k, c_i pertenece a G_1.

3) Si la clase c_i no cumple las condiciones exigidas en 1) o 2), pero en c_i existe un ideal cuya norma sea un producto de potencias de elementos correspondientes al conjunto local completo, reducido, de $P(x)$, la clase c_i pertenece a G_1.

4) Si existe una clase de ideales c_i, que no cumpla las condiciones exigidas en 1), 2) o 3), entonces, evidentemente, c_i no pertenece a G_1 y G_1 es subgrupo propio de G. En este caso, en las $h - h/h_1$ clases de ideales c_i que no pertenecen a G_1, los ideales de norma menor que k, no son de primer grado. Es decir, existen $h - h/h_1$ números primos p, menores que K, que no pertenecen al conjunto local completo reducido de $P(x)$ y para los que el polinomio $P(x)$ se descompone en producto de factores no lineales.

En los cuerpos cuadráticos se cumple siempre la condición 1).

En los cuerpos cúbicos se cumple siempre la condición 2). En consecuencia podemos enunciar:

II-1. TEOREMA.—*En los cuerpos cuadráticos y cúbicos G_1 coincide con G.*

En los anillos cuyo grado de algebricidad sea mayor que tres, tendrá que tenerse en cuenta la posibilidad de que G_1 no coincida con G. Si

$$P(x) \equiv P_1(x) \cdot P_2(x) \ldots P_k(x) \mod p,$$

y los polinomios $P_i(x)$ $(i = 2, \ldots, k)$ son irreducibles mod p, para estudiar la clase del ideal de orden superior correspondiente al factor $P_i(x)$, basta efectuar en $P(x) = 0$ la transformación

$$y = P_i(x).$$

El polinomio $Q(y)$, transformado del $P(x)$, verifica:

$$Q(0) \equiv 0 \mod p^r \qquad (r = \text{grado de } P_i(x))$$

en consecuencia, p^r pertenece al conjunto de descomposición completo del polinomio $Q(y)$ y, por tanto, podremos determinar la clase a la que pertenece.

El teorema IV-8 de [1] se refiere a G_1.

Bibliografía

[1] OCHOA, J.: *Un modelo elemental para las clases de ideales de un anillo algebraico.* «Rev. de la Real Academia de Ciencias de Madrid», tomo LXVIII, cuaderno 4.°, 1974.

[2] REHM, HANS PETER: *On Ochoa's special matrices in matrix classes.* «J. Linear Algebra and Applications», 1977.