P-ANCESTRALIDAD EN CIERTOS ANILLOS

por

Rolando E. Peinado

1. Introducción

Todos los anillos aquí considerados serán asociativos. Un subanillo es propio, si es diferente del anillo y consta de más de un elemento. En este artículo se estudiarán ciertas condiciones en los subanillos propios que caracterizarán a los anillos que los contienen. Dada una propiedad P, un anillo es P-ancestral, si todos sus subanillos propios poseen la propiedad P. Por ejemplo, si P es la propiedad de ser un ideal, entonces los números enteros, $\mathbb{Z}$ (de ahora en adelante usaremos $\mathbb{Z}$ para denotar el anillo de los números enteros), es un anillo P-ancestral.

Sea (S_i), $i\in I$ (I un conjunto de índices) una familia de subanillos de un anillo A. La intersección de los S_i es el mayor subanillo de A que está contenido en cada uno de los S_i. El subanillo $\{US_i\}$ de A es el conjunto formado por sumas de productos finitos de elementos de S_i, es decir, por elementos de la forma $\Sigma \pm s_i$, $i=1,2,\ldots,n$, $s_i\in S_i$. Es fácil mostrar que $\{US_i\}$ es el menor subanillo que contiene los S_i. Sea ahora S un subanillo de A, y consideremos la familia (S_i) de todos los subanillos S_i que contienen a S como ideal propio; es claro que $\{US_i\}$ contiene a S como ideal propio, luego $\{US_i\}$ es el menor subanillo de A que contiene a S como ideal propio. Se acostumbra decir entonces que $\{US_i\}$ es el idealizador por la izquierda de S y se denota por I(S). Es fácil demostrar que

$$I(S) = \{ x : x \in A,\ xs \in S, \text{ para todo } s \in S \}.$$

En forma análoga, con los cambios apropiados, se puede definir el idealizador por la derecha de S y el idealizador bilátero de S.

S es un ideal por la izquierda en A sis (de ahora en adelante sis significa si y solamente si), $I(S) = A$. En el caso en que S sea un ideal por la derecha, el concepto de idealizador fue usado por ORE en [6, pág.242] (los números entre corchetes hacen referencia a la bibliografía dada al final) el cual lo llamó el «eigen ring» de un ideal por la derecha. JACOBSON en [2, pág. 236] lo llamó el normalizador del ideal por la derecha. Como se puede observar el concepto de idealizador es el análogo del normalizador de subconjuntos en Teoría de Grupos.

Los resultados de la sección 2 establecen relaciones entre condiciones entre idealizadores (de ahora en adelante diremos idealizador para referirnos a un idealizador por la izquierda) y algunos casos de P-ancestralidad. También se incluye otro resultado concerniente al radical de JACOBSON.

En la sección 3 se estudia una condición P la cual implica la conmutatividad en los anillos P-ancestrales.

2. Idealizadores y P-ancestralidad

En esta sección todos los anillos considerados tienen unidad, la cual escribiremos 1, y todos tienen subanillos propios. Si S y T son subanillos de un anillo A, las siguientes relaciones son fáciles de demostrar, haciendo uso de la definición de idealizador:

(i) $1 \in I(S)$ (ii) $S \subseteq I(S)$

(iii) $I(S) = I(I(S))$ (iv) $I(S) \cap I(T) \subseteq I(S \cap T)$

(v) $I(T \cup S) \subseteq I(T) \cup I(S)$ (vi) $I(S) \subseteq I(S^2)$.

Sea D el anillo completo de las matrices 2x2 con elementos en $\mathbb{Z}$, y sean

$$K = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{Z} \right\}$$

$$S = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} : x,y \in \mathbb{Z} \right\}$$

$$T = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x,y \in \mathbb{Z} \right\}.$$

Entonces $K \subset S$ y $I(K) \subset I(S)$, estrictamente (obsérvese que S es un ideal por la izquierda de D). Ahora bien, $S^2 \subseteq S$, siempre, y por (vi), $I(S) \subseteq I(S^2)$. Estas observaciones muestran que conocer la relación de inclusión entre dos anillos arbitrarios no es suficiente para determinar la relación de inclusión entre sus idealizadores respectivos. En D tenemos $I(T) \cap I(K) \subset I(T \cap K)$, estrictamente, y $I(T \cup S) \subset I(T) \cup I(S)$, estrictamente. Esto demuestra que las relaciones (iv) y (v) son los mejores resultados posibles.

LEMA 2.1 <u>Para todo subanillo propio</u> S <u>de un anillo</u> A, $I(S) = S$ <u>sis</u> $1 \in S$.

Demostración: Por (i), $1 \in I(S)$, y por (ii), $S \subseteq I(S)$. Así $I(S) = S$ implica $1 \in S$. Recíprocamente, si $1 \in S$ y $x \in I(S)$, entonces $x.1 \in S$, lo cual implica $I(S) \subseteq S$. Por consiguiente, $I(S) = S$.

LEMA 2.2 <u>Si</u> A <u>es un anillo con división</u>(1) <u>en el cual todos sus subanillos propios son anillos con división, entonces la caraterística de</u> A <u>es</u>

un número entero primo.

Demostración: Todo anillo con división tiene como característica a cero ó a un número entero primo. Si A tiene característica cero, entonces A tiene un subanillo propio isomorfo al cuerpo formado por los números racionales. Por consiguiente, un subanillo propio isomorfo a los números enteros $\mathbb{Z}$. $\mathbb{Z}$ no es un anillo con división. Se obtiene así una contradicción. Por lo tanto la característica de A es un número entero primo.

LEMA 2.3 Sea A un anillo con división en el cual todos los subanillos propios son anillos con división. Entonces A es un cuerpo, extensión algebraica del cuerpo primo de A.

Demostración: Sea S un subanillo propio de A, entonces, como S es un anillo con división, $1 \in S$. En particular, si S es el subanillo generado por un elemento $s \in S$, $s \neq 0$, es decir, $S = \langle s \rangle$, S consiste de los polinomios en s sobre el cuerpo primo de A. Obviamente, $s^{-1} \in S$ y s^{-1} es un polinomio en s; por consecuencia, s satisface una ecuación algebraica sobre el cuerpo primo de A. Esto además muestra que S es finito. Tenemos entonces que $s^{n(s)} = s$, donde $n(s)$ es el número de elementos de S; entonces, por resultados en [3, teorema 1, pág.217], A es un anillo conmutativo. Esto demuestra que A es un cuerpo algebraico sobre el cuerpo primo de A.

LEMA 2.4 En un anillo A, $I(S) = S$, S un subanillo propio de A, sis, S es un anillo don división.

Demostración: $I(S) = S$ implica (por el lema 2.1) $1 \in S$. Si L es un ideal por la izquierda de S, enton ces $S \subseteq I(L) = L$, por consiguiente, $S = L$. S no tiene ideales propios por la izquierda y $S^2 \neq 0$ $(1 \in S)$, por lo tanto, S es un anillo con división. Recíprocamente, si S es anillo con división, $1 \in S$, y el lema 2.1 implica $I(S) = S$.

Obsérvese que si el anillo A no tiene unidad, entonces es posible que $I(S) = S$, sin que A sea un anillo con división. Consideremos el siguiente ejemplo: sea A el anillo siguiente

$$A = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\},$$

suma y multiplicación de matrices con coeficientes enteros módulo dos. Como el único subanillo diferente de cero es A mismo, $I(A) = A$, pero A no es un anillo con división.

Notemos también que aún cuando cada subanillo sea un anillo con división, el anillo no es necesariamente un anillo con división. Un contra-ejemplo se obtiene considerando el anillo siguiente:

$$B = \{ (0,0),\ (1,0),\ (0,1),\ (1,1) \},$$

suma y multiplicación definidas componente a componente módulo dos. Aquí cada subanillo propio es un anillo con división; aún más, es un cuerpo. Cada elemento es idempotente, lo cual implica que B no puede ser un anillo con división.

LEMA 2.5 A <u>es un cuerpo en el cual cada elemento es de orden finito sis</u>, $I(S) = S$ <u>para todo subanillo propio</u> S <u>de</u> A.

Demostración: Sea A un cuerpo en el cual cada elemento es de orden finito. Si S es un subanillo propio en A, para todo $x \in I(S)$ y $s \in S$, $s \neq 0$, $xs = s'$ $\in S$. s de orden finito implica que existe $m \in \mathbb{Z}$ tal que $s^m = 1$, $0 < m$. Entonces

$$x = x.1 = xs^m = xss^{m-1} = s's^{m-1} \in S.$$

Por consiguiente, $I(S) \subseteq S$. Por (ii), $S \subseteq I(S)$, luego $I(S) = S$.

Por otro lado, si $I(S) = S$, el lema 2.4 implica que S es un anillo con división, y el lema 2.3, que A es un cuerpo, y, como en la demostración del mismo lema, cada elemento de A tiene orden finito, ya que genera un cuerpo finito. Además, A es una extensión algebraica de su cuerpo primo.

En los lemas anteriores hemos analizado la relación entre ciertos anillos P-ancestrales, para ciertas propiedades P, y la condición en el idealizador, $I(S) = S$ para todo subanillo propio de los anillos considerados; resumamos estos resultados en el siguiente

TEOREMA 2.1 <u>Los siguientes enunciados son equivalentes en un anillo</u> A:

(1) $I(S) = S$ <u>para todo subanillo propio</u> S <u>de</u> A.

(2) A <u>y todos sus subanillos propios son anillos con división. Además la característica de</u> A <u>es un número primo</u>.

(3) A <u>es un cuerpo, todos sus elementos son de orden finito y</u> A <u>es una extensión algebraica de su cuerpo primo</u>.

Volvamos ahora al caso en el cual $I(S) \neq S$ para todo subanillo propio de un anillo A.

LEMA 2.6 En un anillo A cada subanillo de A es un ideal en A por la izquierda sis A es imagen homomorfa de $\mathbb{Z}$.

Demostración: Sea S el subanillo de A generado por la unidad 1 de A. Entonces $S = \{1.n : n \in \mathbb{Z}\}$. Es obvio que $1 \in S$. El lema 2.1 implica $I(S) = S$; debido a que S es un ideal, tenemos $I(S) = A$ y $A = S$. Esto demuestra que A es imagen homomorfa de $\mathbb{Z}$. Recíprocamente, si A es imagen homomorfa de $\mathbb{Z}$, como cada subanillo de $\mathbb{Z}$ es un ideal, y esta propiedad se preserva por homomorfismos, cada subanillo de A es un ideal.

LEMA 2.7 Sea S un subanillo propio del anillo A. $I(S) \neq S$ sis $I(S) = A$.

Demsotración: Si $I(S) \neq S$, por (iii), $I(I(S)) = I(S)$, lo cual implica $I(S) = A$. Si $I(S) = A$ para todo subanillo propio $S \neq A$, $I(S) \neq S$.

TEOREMA 2.2 En un anillo A las siguientes afirmaciones son equivalentes:

(1) A es imagen homomorfa de $\mathbb{Z}$.

(2) Cada subanillo de A es un ideal por la izquierda en A.

(3) $I(S) \neq S$ para cada subanillo propio S de A.

Demostración: (1) implica (2) por el lema 2.6. (2) implica (3) es obvio, y (3) implica (1) se tiene por el lema 2.7.

TEOREMA 2.3 Sea A un anillo. S un subanillo propio de A. Para cada S, existe un número entero n, dependiente de S, tal que $I(S^n) = A$ sis $I(S) \neq S$.

Demostración: Sea S un subanillo propio de A. $I(S) = S$ implicaría $1 \in S$, por el lema 2.1, y, por consiguiente, $S^n = S$. Así $S = I(S) = I(S^n) = A$, lo cual es falso. Por consiguiente, $I(S) \neq S$. Recíprocamente, si $I(S) \neq S$, el lema 2.7 implica que $I(S) = A$.

El siguiente teorema relaciona la propiedad de ser anillo radical, en el sentido de JACOBSON, y los anillos de polinomios sobre el mismo anillo. Este resultado también aparece en [4], aún cuando la demostración es diferente.

TEOREMA 2.4 <u>Si</u> A <u>es un anillo y cada subanillo</u> S <u>es igual a su radical</u> (JACOBSON), <u>entonces existe un polinomio</u> $f(x)$ <u>en</u> $A[x]$ <u>tal que</u> $f(a) = 0$ <u>para todo</u> a <u>en</u> A <u>y</u> $f(1) = 1$.

Demostración: Existe un polinomio $g(x)$ en $A[x]$ tal que para todo a en A $a + g(a) - ag(a) = 0$. Construyamos $f(x) = x + g(x) - xg(x)$; entonces $f(a) = a + g(a) - ag(a)$ para todo a en A, $a \neq 1$, y $f(1) = 1$.

3. Conmutatividad de ciertos anillos

Sea A un anillo arbitrario, no necesariamente con unidad. El subanillo $nA = \{na: a \in A\}$, $n \in \mathbb{Z}$, es llamado un <u>múltiplo del anillo</u> A. nA se dice <u>S-máximal</u> si $n \in \mathbb{Z}$ es el menor entero positivo para el cual $nA \subseteq S$, S subanillo de A.

F.SZÁSZ consideró, en [8], anillos P'-ancestrales en donde, si S es un subanillo propio de A,

P' : $S = nA$ para algún $n \in \mathbb{Z}$.

El resultado principal allí obtenido es el siguiente: <u>un</u>

anillo A es P'-ancestral sis, el grupo aditivo de A es un grupo cíclico.

En esta sección se consideran anillos P-ancestrales, en donde, si S es un subanillo propio de A,

P : $0 \neq nA \subseteq S$, nA es S-maximal.

El principal resultado obtenido es que, en dicho caso, A es conmutatitvo.

Cada anillo P'-ancestral es necesariamente P-ancestral. Es fácil verificar que si A es un anillo P-ancestral, entonces:

(a) Cada subanillo propio de A es P-ancestral.

(b) Toda imagen homomorfa de A es P-ancestral.

Si A es un anillo arbitrario, se puede construir un anillo A' con unidad que contenga un subanillo isomorfo con A, de la siguiente manera:

$$A' = A \times \mathbb{Z} = \{ (a,n) : a \in A, n \in \mathbb{Z} \} ,$$

y definiendo la suma y la igualdad componenete a componente, y la multiplicación como sigue:

$$(a,n)(b,m) = (ab + ma + nb, mn),$$

de donde el subanillo $\{ (a,0) : a \in A \}$ es isomorfo a A. Es fácil verificar que A es P-ancestral sis, A' es P-ancestral. La anterior consideración demuestra que, sin perder generalidad, se puede suponer que A tiene unidad. Escribimos 1 como la unidad.

En un grupo abeliano G, cuya operación binaria se nota aditivamente, se dice que un elemento a de G es periódico ó de torsión si existe $n \in \mathbb{Z}$ tal que $na = 0$; si no existe un tal número entero, el elemento a se dice sin torsión. Un grupo G se dice que es periódico ó de torsión si cada elemento de G es periódico. Un grupo G se dice sin torsión, si ningún elemento de G es de torsión.

LEMA 3.1 Sea A un anillo P-ancestral cuyo grupo aditivo es sin torsión. Entonces A es un anillo conmutativo.

Demsotración: El centro C de un anillo A es un subanillo de A, y $C \neq 0$ ya que $1 \in C$. Siendo A un anillo P-ancestral, esto implica que existe $n \in \mathbb{Z}$ tal que $nA \subseteq C$. Para todo elemento a,b en A, $na, nb \in C$, por tanto:

$$n^2ab = nanb = nbna = n^2ba,$$

lo cual implica:

$$n^2ab - n^2ba = n^2(ab - ba) = 0;$$

debido a que A es sin torsión, como grupo aditivo, tenemos:

$$(ab - ba) = 0 \Rightarrow ab = ba$$

para todo $a,b \in A$, y A es, por lo tanto, conmutativo.

Sea A un anillo cuya estructura aditiva sea un grupo con torsión. Las q-componentes de A; digamos A_q, son no sólo subgrupos de A, sino al mismo tiempo ideales de A como anillo. Por consiguiente, A es suma directa de los A_q anillos, donde el grupo aditivo de A_q es un q-grupo.

LEMA 3.2 Sea A un anillo P-ancestral que es un q-anillo. Entonces A es conmutativo.

Demostración: Sea A_q un anillo P-ancestral. Cada subgrupo propio de A_q contiene un múltiplo del anillo nA_q, $n \in \mathbb{Z}$, y n es el menor entero para el cual esto es posible. Estas consideraciones y el ejercicio 19 de [5,pág.19] nos permiten demostrar que A_q está acotado, ya que de otra manera existiría un homomorfismo de A_q sobre $\mathbb{Z}(p^\infty)$. Por (a) y (b) cada subgrupo de $\mathbb{Z}(p^\infty)$ contiene un múltiplo de $\mathbb{Z}(p^\infty)$ diferente de cero. El subgrupo generado por $1/p$, p un número entero primo; no contiene un múltiplo de $\mathbb{Z}(p^\infty)$. Esta contradicción muestra que A_q está acotado.

Supongamos que $q^k A_q = 0$ y que $q^{k-1}A_q \neq 0$. Entonces qA_q, $q^2A_q, \ldots, q^{k-1}A_q$, son subanillos de A_q los cuales también son ideales de A_q. Consideremos los anillos cocientes

$$A_q^i = q^i A_q / q^{i+1} A_q, \quad i = 1, \ldots, k-2.$$

(b) implica que A_q^i es también un anillo P-ancestral. Sea S un subanillo propio de A_q^i, y $I(S) = A_q^i$. Entonces, existe $n \in \mathbb{Z}$ tal que nA_q^i es S-maximal en A_q^i. A_q^i como grupo aditivo está acotado, digamos $n=q^j$, $j \in \mathbb{Z}$, lo cual contradice la definición de A_q^i. Por consiguiente, A_q^i no tiene ideales propios por la izquierda y A_q^i es un cuerpo de característica prima o un cero anillo. De todas maneras, A_q^i es un grupo de orden q^k. Por consiguiente, A_q, como grupo, lo cual implica que A_q es un anillo conmutativo.

COROLARIO. Si A es un anillo P-ancestral cuyo g grupo aditivo es de torsión, A es conmutativo.

Demostración: A es la suma directa de q-anillos y por el teorema éstos son conmutativos, luego A es conmutativo.

LEMA 3.3 Sea A un anillo P-ancestral. A es la suma directa (como anillo), A = F ⊕ T, en donde el grupo aditivo de F es sin torsión y el grupo aditivo de T es de torsión.

Demostración: Por argumentos análogos a los del lema 3.2, el subgrupo máximo T de torsión está acotado. Resultados en [1,pág.183] implican que A es la suma directa de T y un subgrupo F sin torsión..Como F y T son ideales de A, la suma, como anillos, es directa.

TEOREMA 3.1 Todo anillo P-ancestral ,A, es conmutativo.

Demsotración: Por el lema 3.3, A = F ⊕ T; el lema 3.1 dice que F es conmutativo y el lema 3.2, que T es conmutativo, y como la suma es directa, A es conmutativo.

Nótese que el recíproco de este teorema no es necesariamente válido. Basta considerar un cuerpo de característica cero, para observar que existen anillos conmutativos que no son anillos P-ancestrales.

(1) El autor, siguiendo la costumbre anglosajona, llama a un cuerpo no necesariamente conmutativo, un anillo con división.

BIBLIOGRAFIA

[1] L.FUCHS : Abelian groups, Pergamon Press, 1960, Nueva York.

[2] N.JACOBSON : Structure Theory of simple Rings Without Finiteness Assumptions, Trans.Amer.Math.Soc., vol.57(1945) 228-245

[3] N.JACOBSON : Structure of Rings, Amer.Math.Soc., Colloq.Publ., Vol.37,1956,Providence,R.I.

[4] A.JONES y G.LUMER : Una nota acerca de anillos radicales, Bol.Fac.Ing.yAgr.,Montevideo 5(1956) 1-4.

[5] I.KAPLANSKY : Infinite Abelian Groups, University of Michigan Press,1960,Ann Arbor,Michigan.

[6] O.ORE : Formale Theoria der Linearen Differentialgleinchugen,II,J.für Mathematik 168(1932) 233-252.

[7] R.E.PEINADO : Ancestral Rings, Proc. Edinburgh Math.Soc.(1967)

[8] F.SZÁSZ : On rings every subring which is a multiple of the ring, Pub.Math.Debrecen 4(1956) 237-238.

Universidad de Puerto Rico
Mayagüez, Puerto Rico
Recibido en mayo de 1967.