ANILLOS DE JACOBSON

Juan Diego Vélez Caicedo.

Trabajo de grado presentado como requisito para optar el título de Magister en Matemáticas

Directora: Débora María Tejada J.
Doctora en Matemáticas

UNIVERSIDAD NACIONAL DE COLOMBIA
Seccional de Medellín
Facultad de Ciencias
Postgrado de Matemáticas
1985

T
512.4
V35

TABLA DE CONTENIDO

Pág

INTRODUCCION..... 1

APENDICE 1 6

APENDICE 2 13

1. ESTUDIO DE LA CONMUTATIVIDAD DE UN Jn-ANILLO A TRAVES DEL ANILLO $Z_p[x]\langle x^n - x\rangle$ 17

2. FACTORIZACION DEL POLINOMIO $x^n - x$ $(n>1)$ EN $\mathbb{Z}_p[x]$. 24

3. ESTUDIO DEL ANILLO $Z_{p,n}[x]$ 36

4. CONMUTATIVIDAD DE CIERTOS Jn-ANILLOS 41

BIBLIOGRAFIA..... 55

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL
R. 25648

INTRODUCCION

Un teorema de Jacobson establece que un anillo A , para el cual existe un entero $n > 1$, tal que para todo $a \in A$, $a^n = a$ (Anillos que denominaremos Jn-anillos), es necesariamente un anillo conmutativo. Como puede verse en el apendice 1, usando de manera estandar el lema de Zorn, se prueba que un Jn-anillo A posee ideales maximales bilaterales y que el radical de Jacobson de A (definido como la intersección de todos los ideales maximales de A) contiene solamente el elemento 0 . Lo anterior permite reducir el problema de demostrar la conmutatividad de A , al problema de demostrar la conmutatividad de Jn-anillos que son anillos de división. La conmutatividad de estos últimos anillos se prueba haciendo uso del teorema de Wedderburn, el cual establece que todo anillo de división finito es un campo.

En este trabajo se demostrará la conmutatividad de ciertos Jn-anillos con una técnica propia y completamente diferente. Se desarrollará un método que involucra el uso de anillos de polinomios y que permite reducir el problema de demostrar la conmutatividad de un Jn-anillo, al problema de probar que cierto subanillo, de un anillo cociente, en un anillo de polinomios, es igual a todo el anillo.

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL

Como puede verse en el apéndice 2, es posible demostrar de manera elemental la conmutatividad de un Jn-anillo cuando n es un entero pequeño, por ejemplo para $n = 2,3,4,6$. A partir de estas demostraciones se puede pensar hasta que punto es posible extender estos métodos de demostración, que no hacen uso del lema de Zorn ni tampoco del teorema de Wedderburn, para probar la conmutatividad de los Jn-anillos. Se han hecho algunos intentos en esta dirección. En [2] se prueba por ejemplo que todo Jn-anillo con $n = p + 1$ donde p es un número primo de la forma $2^k + 2^m - 1$ con $m,k \geqslant 0$ es conmutativo. En [11] se prueba que un Jp-anillo (con p un número primo), que tenga característica p, es conmutativo.

Las ideas que aparecen en este trabajo fueron sugeridas por las demostraciones que aparecen en el apéndice 2. En todas estas demostraciones el camino seguido ha sido similar. Se toma un elemento general x de un Jn-anillo A y se demuestra que x esta en $C(A)$, centro del anillo A, a partir del hecho de que $x^{n-1} \in C(A)$. Formalmente podríamos pensar que en vez de estar operando con elementos de A, estamos operando con polinomios en la variable x. Supongamos, por ejemplo, que se está tratando de probar la conmutatividad de un Jn-anillo A el cual tiene característica 2, ($2x = 0$ para todo $x \in A$), y supongamos, además, que de alguna manera hemos demostrado que para cualquier elemento $x \in A$ se tiene que $x^3 - x^2 + x \in C(A)$. Como x representa un elemento cualquiera de A, podemos cambiar a x por una expresión polinómica en x, digamos $x^5 + x^7$ y afirmar que

$$(x^5 + x^7)^3 - (x^5 + x^7)^2 + (x^5 + x^7) \in C(A) .$$

Esta expresión la podemos desarrollar pensando que estamos multiplicando polinomios en la variable x con coeficientes en el campo $\mathbb{Z}_2$ de los enteros módulo 2 (esto ya que $2x = 0$ pues A tiene característica 2) y después podemos usar la relación $x^n = x$ (ya que estamos en un Jn-anillo) para reducir cualquier polinomio en x a otro polinomio donde solo aparecen potencias de x menores que n. El objetivo final es demostrar que $x \in C(A)$; usando lo siguiente:

i) Siempre que tengamos que $p(x) \in C(A)$, podemos cambiar la variable x por un polinomio $g(x)$ y afirmar que $p(g(x)) \in C(A)$.

ii) Si $p_1(x) \in C(A)$ y $p_2(x) \in C(A)$, entonces se puede ver que $p_1(x) + p_2(x) \in C(A)$, $p_1(x) \cdot p_2(x) \in C(A)$.

iii) $x^{n-1} \in C(A)$.

Si denotamos por $\langle x^n - x \rangle$ el ideal de $\mathbb{Z}_2[x]$ generado por $x^n - x$ podemos pensar que las operaciones entre polinomios $p(x)$ se efectúan en el anillo cociente $\mathbb{Z}_2[x] \,/\, \langle x^n - x \rangle$ (ya que intuitivamente estamos identificando a x^n con x y a $2x$ con cero) y que en este anillo tenemos un cierto subanillo S_A con la siguiente propiedad: Si $\overline{p(x)} \in S_A$ entonces $p(a) \in C(A)$, es decir, si cambiamos a x por un elemento $a \in A$ la expresión resultante está en el centro de A. Así, si probamos que $x \in S_A$, o lo que es equivalente, que $S_A = \mathbb{Z}_2[x] \,/\, \langle x^n - x \rangle$, estaremos probando que A es conmutativo.

Teniendo en cuenta las consideraciones anteriores, en el primer capítulo, después de mostrar algunas propiedades elementales de los elementos de un Jn-anillo A, se define el subanillo S_A de $\mathbb{Z}_p[x] \big/ \langle x^n - x \rangle$ y en 1.7 se establece la propiedad fundamental de este subanillo, que es la de absorber las potencias $n - 1$ de los elementos de $\mathbb{Z}_p[x] \big/ \langle x^n - x \rangle$, finalmente en el teorema 1.8 se muestra que A es conmutativo si S_A es todo el anillo $\mathbb{Z}_p[x] \big/ \langle x^n - x \rangle$.

El segundo capítulo está dedicado a estudiar la factorización del polinomio $x^n - x$ en factores irreducibles en $\mathbb{Z}_p[x]$, (p un número primo). Cuando este polinomio se considera en $\mathbb{Z}[x]$ su factorización es bien conocida en términos de los polinomios ciclotómicos. Sin embargo, hasta donde nosotros sabemos, en los textos de álgebra no aparece el estudio de la factorización de este polinomio en el anillo $\mathbb{Z}_p[x]$. Como una aplicación de la teoría de Galois, en 2.16 se demuestra la manera como se descompone el polinomio $x^n - x$ en factores irreducibles en $\mathbb{Z}_p[x]$.

En el capítulo tercero usando nuestra factorización de $x^n - x$ en $\mathbb{Z}_p[x]$, se prueba que si $p \nmid n-1$, entonces $\mathbb{Z}_p[x] \big/ \langle x^n - x \rangle$ se puede descomponer como una suma de campos, y con este resultado se prueba, finalmente, en el capitulo 4, que un Jn-anillo A con característica prima p es conmutativo; siempre que n posea ciertas propiedades respecto al primo p, estos enteros los llamaremos **admisibles** para p. Para un primo fijo p, se prueba que $n = p$ resulta ser admisible, de donde se deduce la conmutatividad de los p-anillos (Anillos para los cuales $p.a = 0$ y $a^p = a$ para todo $a \in A$). Se muestra también cómo en algunos casos

especiales el problema de decidir cuando un entero n es admisible para un primo p está relacionado con el problema de determinar las raices primitivas del primo p.

Creemos que las ideas desarrolladas en este trabajo son nuevas herramientas para probar la conmutatividad de otros anillos o álgebras en donde todos sus elementos verificaran una cierta ecuación.

APENDICE 1

Un anillo R se llama un **J-anillo** si, para cada $x \in R$ existe un entero $n(x) > 1$ (dependiente de x) tal que $x^{n(x)} = x$. Presentaremos en lo que sigue la prueba tal como aparece en [3], capítulo 9 del siguiente teorema:

TEOREMA: (Jacobson). Si R es un J-anillo, entonces R es conmutativo.

Probaremos primero el teorema en el caso en que R es un anillo con unidad. La prueba se basa en el teorema de Wedderburn el cual establece lo siguiente:

TEOREMA: (Wedderburn): Si R es un anillo de división finito, R es conmutativo.

La prueba de este teorema puede verse en [3] pág. 194. Otra prueba diferente puede verse en [4] pág. 319.

En el lema siguiente denotaremos con D un anillo de división, con I_p el subcampo de D generado por la unidad de D y con $C(D)$ el centro de D.

LEMA 1. Sea D un anillo de división con característica $p > 0$, p un número primo. Supongamos que $a \in D$ es tal que $a^{p^m} = a$, para un cierto $m > 0$, y que $a \notin C(D)$. Entonces, existe un $x \in D$ tal que:

i) $xax^{-1} \neq a$

ii) $xax^{-1} \in I_p(a)$ ($I_p(a)$ denota el campo que resulta de extender a I_p adjuntando el elemento a)

En efecto, como $a^{p^m} - a = 0$, a es algebraico sobre I_p y el campo $I_p(a)$ es finito con p^n elementos, para algún entero $n > 0$, ([3] pág. 141), más aún, cada $r \in I_p(a)$ cumple que $r^{p^n} = r$.

Definamos la función $f: D \longrightarrow D$, para cada $x \in D$, como $f(x) = xa - ax$. Si para cada $k \geq 1$ definimos $f^k(x) = f(f^{k-1}(x))$ se verifica facilmente por inducción sobre k que:

$$f^k(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} a^i \, x \, a^{k-i}$$

Cuando $k = p$ la ecuación anterior se reduce a $f^p(x) = xa^p - a^p.x$, esto ya que $p \mid \binom{p}{i}$ para $0 < i < p$, y la característica de D es p.

Mediante un nuevo paso de inducción se verifica facilmente que $f^{p^n}(x) = x.a^{p^n} - a^{p^n}.x$, pero $a^{p^n} = a$ luego $f^{p^n}(x) = f(x)$, para todo $x \in D$, de donde se deduce que $f^{p^n} = f$.

Para cada elemento $r \in I_p(a)$, consideremos la función T_r definida en D como $T_r(x) = r.x$. Para cada $x \in D$ se tiene que:

$f.T_r(x) = f(rx) = (rx).a - a(r.x) = rxa - rax$ (ya que a y r conmutan por estar ambos en $I_p(a)$). Por otro lado se tiene que $T_r.f(x) = r(xa - ax)$ $= rxa - rax = f.T_r(x)$. Esto nos muestra que para todo $r \in I_p(a)$ $fT_r = T_r f$.

Como se ve en ([3] , pág. 188) el polinomio $y^{p^n} - y \in I_p[y]$ se factoriza completamente en factores lineales en $I_p(a)$, es decir, se tiene que:

$$y^{p^n} - y = \prod_{r \in I_p(a)} (y - r) = y. \prod_{0 \neq r \in I_p(a)} (y - r)$$

En virtud de que $T_r f = fT_r$ y usando la ecuación anterior, se sigue que:

$$0 = f^{p^n} - f = f. \prod_{0 \neq r \in I_p(a)} (f - T_r) \qquad (1) .$$

Mostremos ahora que existe un $x \neq 0$ en D y un $r \neq 0$ en $I_p(a)$ tal que $(f - T_r)(x) = 0$. Si este no fuera el caso, se tendría que para cualquier $r \neq 0$ si $(f - T_r)(x) = 0$ implicaría que $x = 0$. Sea $g_r = f - T_r$. Como $r^{p^n} = r$ y $f^{p^n} = f$ se tiene que $g_r^{p^n} = g_r$, o lo que es equivalente $g_r(g_r^{p^n-1} - T_1) = 0$. Si $x \in D$ se tiene que $g_r \left[(g_r^{p^n-1} - T_1)(x) \right] = 0$ de donde se deduce que $g_r^{p^n-1}(x) = x$ para

cualquier $x \in D$. Dado un $z \in D$ se tiene que $g_r(g_r^{p^n-2}(z)) = z$ lo cual muestra que g_r es sobreyectiva, para todo $r \neq 0$ y por lo tanto $\prod_{0 \neq r \in I_p(a)} g_r$ también lo es. De lo anterior y de la ecuación (1) se obtiene que $f(x) = 0$, para todo $x \in D$, lo que es equivalente a decir que $xa = ax$ para todo $x \in D$ lo cual contradice el hecho de que $a \notin C(D)$.

Sea $x \neq 0$ y $r \neq 0$ tales que $(f - T_r)(x) = 0$. Lo anterior significa que $xa - ax = rx$ o bien que $xax^{-1} = r + a \in I_p(a)$. Como $r \neq 0$ el producto $xax^{-1} \neq a$.

COROLARIO: En el lema anterior $xax^{-1} = a^k \neq a$ para un entero $k > 0$

En efecto, sea S el orden de a en el grupo multiplicativo de $I_p(a)$. En el campo $I_p(a)$ los S elementos $a, a^2, \ldots, a^s = 1$ son raices del plinomio $y^s - y \in I_p(a)[y]$. Como xax^{-1} es también raíz de dicho polinomio, deberá ser igual a uno de los elementos $a, a^2, \ldots a^s$, en consecuencia existe un k, $2 \leqslant k \leqslant s-1$ para el cual $xax^{-1} = a^k$.

LEMA 2. Sea R un J-anillo. Si R es un anillo de división, entonces R es conmutativo.

Mostremos en primer lugar que R tiene característica $p > 0$, p un primo. Si la característica de R es 2 no hay nada que probar. Si

$a \neq 0$ está en R por hipótesis existen dos elementos $h,k > 1$ para los cuales $a^h = a$, $(2a)^k = 2a$. Si hacemos $q = (h - 1)(k - 1) + 1 > 1$ se sigue que $a^q = a$ y $(2a)^q = 2a$ de donde obtenemos $(2^q - 2)a = 0$. Como R es un anillo de división, existe un entero positivo mínimo primo p , tal que $p.a = 0$, lo que implica que la característica de R es p. Si como en el lema 1 denotamos con I_p el subcampo de R generado por la unidad de R , como $a^h = a$ el elemento a es algebraico sobre I_p y la extensión de I_p adjuntando a , $I_p(a)$, es un campo, con digamos p^n elementos. Si asumimos que $a \notin C(R)$ como $a^{p^n} = a$ (ya que $a \in I_p(a)$) por el corolario del lema 1 se deduce que existe un $b \in R$ y un entero $k > 1$ tales que $bab^{-1} = a^k \neq a$. Un razonamiento similar aplicado a $I_p(b)$ muestra que existe un $m > 1$ tal que $b^{p^m} = b$.

Consideremos el siguiente conjunto de sumas:

$$W = \left\{ \sum_{i=0}^{p^n-1} \sum_{j=0}^{p^m-1} r_{ij}\, a^i.b^j \ , \ r_{ij} \in I_p \right\}$$

El conjunto anterior es finito, además como $a^k.b = b.a$ el conjunto W es cerrado bajo la multiplicación y es por lo tanto un subanillo de división de R . Por el teorema de Wedderburn W es conmutativo y $ab = ba$ contradiciendo la relación $bab^{-1} = a_k \neq a$. La contradicción proviene de suponer que $a \notin C(R)$. Luego $a \in C(R)$ para todo $a \in R$ y R es conmutativo.

LEMA 3. Sea R un J-anillo. Todo ideal a derecha I de R es un ideal bilateral.

En efecto, sea $a \in I$ con $a^n = a$ $(n > 1)$. En la proposición 1.1 del capítulo 1 mostramos que $e = a^{n-1}$ es idempotente y que $a^{n-1} \in C(R)$. Si $r \in R$ $ra = ra^{n-1}.a = a^{n-1}.ra = a(a^{n-2}.r.a) = ar'$, con $r' = a^{n-2}r.a$ Como $ar' \in I$ esto muestra que $ra \in I$ y I es bilateral.

Observación: Si R es un J-anillo con unidad un argumento estandar usando el lema de Zorn muestra que R posee ideales maximales a derecha los cuales son bilaterales según el lema anterior.

En el lema siguiente $rad(R)$ denota el radical de Jacobson de R el cual está definido como la intersección de todos los ideales maximales de R , recordemos que un elemento $a \in A$ pertenece a $rad(R)$ si y solo si $1 - ar$ es invertible para todo $r \in A$.

LEMA 4. Si R es un J-anillo con unidad R es semisimple, es decir, $rad(R) = \{0\}$.

En efecto, si suponemos que $Z \in rad(R)$ y si $Z^m = Z$ para un cierto $m > 1$ entonces $Z^{m-1} \in rad(R)$ y por la proposición 1.1 del capítulo 1, $Z^{m-1} = e$, es idempotente $(e^2 = e)$. Y como se tiene que $e \in rad(R)$, $(1 - e)$ es invertible. Si $w \in R$ es tal que $(1 - e).w = 1$, como $(e - e^2)w = e(1 - e).w = 0$ se deduce que $e = Z^{m-1} = 0$ y $Z = Z^{m-1}.Z = 0$.

TEOREMA: Si R es un J-anillo con unidad, R es conmutativo.

En efecto, si M es un ideal maximal de R por el lema 3 M es bilateral y anillo cociente R/M es un anillo de división por no tener ideales triviales. Como R es un J-anillo se verifica facilmente que R/M es también un J-anillo. Por el lema 2, R/M es conmutativo. Si $\bar{a},\bar{b} \in R/M$ se tiene que $\bar{a}.\bar{b} = \bar{b}.\bar{a}$ luego $a.b - b.a \in M$. Esta última relación se cumple para todo ideal máximal M de R, luego $ab - ba$ está en $rad(R)$ y como $rad(R) = \{0\}$, $ab - ba = 0$ luego $a.b = b.a$ y R es conmutativo.

En el siguiente teorema se establece la conmutatividad de un J-anillo R que no tenga necesariamente unidad.

TEOREMA: Si R es un J-anillo, R es conmutativo.

En efecto, Sean $a,b \in R$. Supongamos que $a.b - ba \neq 0$. Como $(ab - ba)^{n-1} = e \in C(R)$ y es idempotente, se tiene que $S = R.e = e.R$ es un J-subanillo de R con unidad (e es la unidad de S) y por el teorema anterior S es conmutativo, luego $(ab - ba).e = 0$. Pero $(ab - ba).e = (ab - ba)^n = ab - ba = 0$ lo cual contradice el hecho de que $ab - ba \neq 0$. Esto muestra que R es conmutativo.

APENDICE 2

0. Se reunen en este apendice algunas de las demostraciones que nos motivaron a realizar el trabajo de tesis.

1. Si A es un J_2-anillo, A es conmutativo

Si A es un J_2-anillo se tiene que $(-a)^2 = -a$. Por otro lado se tiene que $(-a)^2 = (-a)(-a) = a^2 = a$ luego $-a = a$ para todo $a \in A$ de donde se deduce que la característica de A es 2 , $2a = 0$ para todo $a \in A$. Si tomamos $b,c \in A$ se tiene que $(b+c)^2 = b^2 + bc + cb + c^2 = b + c$; de donde resulta que $bc + cb = 0$ ó $bc = -cb = cb$ para cualquier par de elementos b y c en A , esto muestra que A es conmutativo.

2. Si A es un J_3-anillo , A es conmutativo

En efecto, sean $a,b \in A$, observemos que si $ab = 0$ entonces $b.a = 0$. Esto ya que $b.a = (b.a)^3 = b.(ab)^2a = b.0.a = 0$. Si $x,y \in A$ como $x^4 = x^3.x = x^2$, se tiene que $x^2(x^2y - y) = 0$ y $(yx^2 - y)x^2 = 0$. Por la observación anterior se tiene que $(x^2y - y).x^2 = 0$ y $x^2(yx^2 - y) = 0$. Las dos últimas ecuaciones muestran que $x^2y = yx^2$ de donde concluimos que x^2 conmuta con cualquier elemento y de A . Si denotamos con

$C(A)$ el centro de A, hemos demostrado que el cuadrado de cualquier elemento de A está en $C(A)$, en especial, se tiene que $(x^2+x)^2 \in C(A)$ pero $(x^2+x)^2 = x^4 + 2x^3 + x^2 = 2x^2 + 2x \in C(A)$. Como $C(A)$ es un subanillo de A, y $2x^2 \in C(A)$ resulta que $2x \in C(A)$ (1).

Por otro lado tenemos que $(x^2 + x)^3 = x^2 + x$. Desarrollando la expresión $(x^2 + x)^3 = x^6 + 3x^5 + 3x^4 + x^3 = 4x^2 + 4x$ e igualando, obtenemos que $3x^2 + 3x = 0$ y por consiguiente $3x^2 + 3x \in C(A)$. Como $3x^2 \in C(A)$ se tiene que $3x \in C(A)$ (2). De (1) y (2) obtenemos que $x \in C(A)$ para cualquier $x \in A$; es decir, A es conmutativo.

En la demostración anterior lo primero que se hizo fue probar que $x^2 \in C(A)$. En general, puede demostrarse de manera sencilla, proposición 1.1, que si a está en un J_n-anillo cualquiera A, entonces $a^{n-1} \in C(A)$. Con base en esto veamos como puede demostrarse la siguiente afirmación

3. Si A es un J_6-anillo, A es conmutativo

En efecto, como para todo $a \in A$ se tiene que $a^6 = a$, entonces $(-a) = (-a)^6 = ((-a)(-a))^3 = (a^2)^3 = a^6 = a$ de donde se obtiene que $-a = a$, ó bien, que $2a = 0$ y A tiene característica 2. Si $x \in A$; $(x + x^2)^5 \in C(A)$. $(x + x^2)^5 = (x + x^2)(x + x^2)^4 = (x + x^2)(x^4 + x^3) =$ $= x^5 + x^4 + x + x^5 = x^4 + x \in C(A)$ (1). Como $x^4 + x$ está en el

centro de A su cuadrado también está, esto es, $(x^4 + x)^2 \in C(A)$ y $(x^4 + x)^2 = x^8 + x^2 = x^3 + x^2 \in C(A)$. Si en la expresión $x^3 + x^2$ cambiamos a x por $x + x^5$, obtenemos $(x + x^5)^3 + (x + x^5) \in C(A)$. Desarrollando la expresión anterior se obtiene que $x^3 + x \in C(A)$. Tomando cuadrado se tiene que $(x^3 + x)^2 = x + x^2 \in C(A)$ (2). De (1) y (2) se sigue que $(x^4 + x).(x^2 + x) \in C(A)$, desarrollando se obtiene que $x^5 + x + x^2 + x^3 \in C(A)$. Como x^5, x^3+x^2 están en $C(A)$ se tiene que $x^5 + x + x^3 + x^2 - (x^3 + x^2) - x^5 \in C(A)$ de donde resulta que $x \in C(A)$ y A es conmutativo.

Antes de pasar a probar que un J_4-anillo es conmutativo, probemos el siguiente lema.

4. LEMA: Si A es un anillo en donde para todo $a \in A$, $a^2 + a \in C(A)$, A es conmutativo.

Sean x,y un par de elementos cualquiera de A. Entonces $(x + y)^2 + (x + y) \in C(A)$ desarrollando lo anterior obtenemos $y^2 + x^2 + xy + yx + x + y \in C(A)$. Si de la expresión anterior restamos x^2+x y y^2+y obtenemos que $xy + yx \in C(A)$; y por lo tanto $(xy + yx).x = x.(xy + yx)$, de donde resulta $x^2.y = y.x^2$. Esto implica que $x^2 \in C(A)$ y como $x^2 + x \in C(A)$ se concluye que $x \in C(A)$ y A es conmutativo.

5. Si A es un J_4-anillo , A es conmutativo

En efecto, $(-a) = (-a)^4 = ((-a)(-a))^2 = a^4 = a$; de donde $2a = 0$ para todo $a \in A$. Si $x \in A$, $(x + x^3)^3 \in C(A)$. Desarrollando esta expresión resulta que $(x + x^3)^3 = 2x^3 + x^2 + x = x^2 + x \in C(A)$, para todo $x \in A$. Usando el lema anterior se concluye que A es conmutativo.

1. ESTUDIO DE LA CONMUTATIVIDAD DE UN Jn-ANILLO A TRAVES DEL ANILLO $Z_p[x] / \langle x^n - x \rangle$

1.0 Jn-ANILLOS

Diremos que un anillo no trivial A es un **Jn-anillo**, $n > 1$, si para todo elemento $a \in A$ se verifica la ecuación $a^n = a$. El objetivo principal de este trabajo es el de mostrar cómo la conmutatividad de un Jn-anillo se puede caracterizar a través de un anillo exterior a el.

La siguiente proposición nos muestra algunas de las propiedades que tiene el elemento a^{n-1} en un Jn-anillo.

Denotaremos por $C(A)$ el centro del anillo A y con (a) el subanillo de A generado por a ([3] pág. 14).

1.1 PROPOSICION: Sea A un Jn-anillo. Para todo elemento $a \in A$ se tiene que $a^{n-1} \in C(A)$ y a^{n-1} actúa como elemento unidad en el subanillo (a).

En efecto, observemos que si $a,b \in A$ y $ab = 0$ entonces $b.a = 0$, ya que $b.a = (b.a)^n = b(ab)^{n-1}.a = 0$. Además se tiene que

$a^{n-1}.a^{n-1} = (a^{n-1}.a).a^{n-2} = a^{n}.a^{n-2} = a.a^{n-2} = a^{n-1}$ de estas dos observaciones se sigue que $a^{n-1}.(a^{n-1}.y - y) = a^{n-1}.y - a^{n-1}.y = 0$ luego $(a^{n-1}.y - y).a^{n-1} = 0$ (1) para cualquier elemento $y \in A$. Similarmente, $(y - ya^{n-1})a^{n-1} = 0$ de donde $a^{n-1}(y - ya^{n-1}) = 0$ (2). De las ecuaciones (1) y (2) obtenemos $a^{n-1}.y = y.a^{n-1}$ para todo $y \in A$, esto nos muestra que $a^{n-1} \in C(A)$.

Probemos ahora que a^{n-1} es un elemento unidad en (a). En primer lugar $a^{n-1}.a^{j} = a^{n}a^{j-1} = a\ a^{j-1} = a^{j}$ y como todo elemento de (a) se puede escribir como una suma finita $\sum_{j>0} \pm a^{j}$, entonces

$a^{n-1}.\sum_{j>0} \pm a^{j} = \sum \pm a^{n-1}.a^{j} = \sum \pm a^{j}$. Similarmente se obtiene que $\left(\sum_{j>0} \pm a^{j}\right).a^{n-1} = \sum \pm a^{j}$, lo cual muestra que a^{n-1} es unidad en (a) ∎

Denotaremos por $\mathbb{Z}$ el anillo de los enteros, por $\overline{m}$ un elemento del campo $\mathbb{Z}_p$ de los enteros módulo p, con p un número primo.

1.2 Sea R un anillo cualquiera. Diremos que R tiene **característica** $n > 1$, si $n.a = 0$ para todo $a \in R$ y n es el mínimo entero positivo con esta propiedad.

1.3 PROPOSICION: Sea A un Jn-anillo con característica prima p. Para cada $a \in A$, $a \neq 0$ se pueden construir homomorfismos $\psi_a : \mathbb{Z}_p \longrightarrow A$, $\phi_a : \mathbb{Z}_p[x] \longrightarrow A$ tales que: $\psi_a(\bar{1}) = a^{n-1}$, $\phi_a(x) = a$ y ϕ_a restringida a $\mathbb{Z}_p$ coincide con ψ_a.

En efecto, para $\bar{m} \in \mathbb{Z}_p$ definimos $\psi_a(\bar{m}) = m.a^{n-1}$. La función ψ_a está bien definida ya que si $\bar{m}_1 = \bar{m}_2$, p divide a $m_1 - m_2$ y como Jn tiene característica p entonces $(m_1 - m_2)\, a^{n-1} = 0$; luego $\psi_a(\bar{m}_1) = \psi_a(\bar{m}_2)$. Esta claro que $\psi_a(\bar{m}_1 + \bar{m}_2) = \psi_a(\bar{m}_1) + \psi_a(\bar{m}_2)$. Como $a^{n-1}.a^{n-1} = a^{n-1}$ se tiene que $\psi_a(\bar{m}_1.\bar{m}_2) = m_1 m_2 a^{n-1} =$ $= m_1 a^{n-1}.m_2 a^{n-1} = \psi_a(\bar{m}_1).\psi_a(\bar{m}_2)$. Para construir a ϕ_a, extendamos el homomorfismo ψ_a al anillo de polinomios $\mathbb{Z}_p[x]$ enviando la variable x en a. Para un elemento $g(x) = \sum_{i=0}^{r} m_i\, x^i$ definimos

$$\phi_a(g(x)) = \sum_{i=0}^{r} \psi_a(\bar{m}_i)a^i$$

donde hacemos a^0 igual a a^{n-1}. Sea

$$h(x) = \sum_{i=0}^{s} \bar{h}_i\, x^i .$$

Es fácil ver que $\phi_a(g(x) + h(x)) = \phi_a(g(x)) + \phi_a(h(x))$.

Como $g(x).h(x) = \sum_{i=0}^{r+s} c_i\, x^i$ con $c_i = \sum_{j=0}^{i} \bar{m}_j\, \bar{h}_{i-j}$, se tiene que

$$\phi_a(g(x).h(x)) = \sum_{i=0}^{r+s} \psi_a(c_i)\, a^i = \sum_{i=0}^{r+s} \left[\sum_{j=0}^{i} \psi_a(\bar{m}_j).\psi_a(\bar{h}_{i-j}) \right] . a^i$$

ya que ψ_a es un homomorfismo. Por otro lado $\phi_a(g(x)).\phi_a(h(x)) =$

$$= \sum_{i=0}^{r} \psi_a(\overline{m}_i)\, a^i . \sum_{i=0}^{s} \psi_a(\overline{h}_i)\, a^i .$$ Reuniendo en este producto, para

cada $0 \leqslant i \leqslant r+s$, todos los términos que contienen a a^i obtenemos

$$\phi_a(g(x)).\phi_a(h(x)) = \sum_{i=0}^{r+s} \left[\sum_{j=0}^{i} \psi_a(\overline{m}_j).\psi_a(\overline{h}_{i-j}) \right] a^i = \phi_a(g(x).h(x)) \quad \text{|||}$$

1.4 OBSERVACION: Para cada $a \in A$, $a \neq 0$ el homomorfismo ϕ_a puede extenderse al anillo cociente $\mathbb{Z}_p[x] \,/\, < x^n - x >$, donde $< x^n - x >$ denota el ideal de $\mathbb{Z}_p[x]$ generado por el polinomio $\overline{1}\, x^n - \overline{1}\, x$, ya que si $p(x) \in < x^n - x >$, $p(x) = q(x).(x^n - x)$ y se tiene que $\phi_a(p(x)) = \phi_a(q(x)).\phi_a(x^n - x) = \phi_a(q(x)).(a^n - a) = 0$. El teorema de extensión a los cocientes (ver [6] pág. 70) nos garantiza la existencia de un homomorfismo $\overline{\phi}_a$ tal que el diagrama siguiente conmuta:

$$\begin{tikzcd}
\mathbb{Z}_p[x] \arrow[r, "\phi_a"] \arrow[d, "\eta"] & A \\
\mathbb{Z}_p[x] \,/\, < x^n - x > \arrow[ur, "\overline{\phi}_a"'] &
\end{tikzcd}$$

$$\phi_a = \overline{\phi}_a \circ \eta$$

donde η denota la aplicación canónica, $\eta(p(x)) = \overline{p(x)}$; $\overline{p(x)} \in \mathbb{Z}_p[x] / < x^n - x >$

1.5 PRECENTRO. Sea A un Jn-anillo con característica prima p.

Al conjunto $S_A = \bigcap_{a \neq 0} \phi_a^{-1}(C(A))$, la intersección de las imágenes inversas del centro de A bajo cada uno de los homomorfismos ϕ_a, la llamaremos **precentro de** $\mathbb{Z}_p[x] / \langle x^n - x \rangle$ **relativo a** A.

1.6 OBSERVACION: La imagen inversa de $C(A)$ bajo cada homomorfismo ϕ_a, $a \in A$, $a \neq 0$ es un subanillo de $\mathbb{Z}_p[x] / \langle x^n - x \rangle$; luego también lo es S_A por ser intersección de subanillos de $\mathbb{Z}_p[x] / \langle x^n - x \rangle$.

La proposición siguiente nos muestra que el precentro es un subanillo que tiene la propiedad de absorber los elementos elevados a la potencia $n - 1$.

1.7 PROPOSICION: Sea A un Jn-anillo con característica prima p.

Si $\overline{u(x)} \in \mathbb{Z}_p[x] / \langle x^n - x \rangle$ entonces $\overline{u(x)}^{n-1} \in S_A$.

En efecto, para cada homomorfismo ϕ_a se tiene que $\phi_a(\overline{u(x)}^{n-1}) = \left[\phi_a(\overline{u(x)}) \right]^{n-1}$. Si hacemos $b = \phi_a(\overline{u(x)})$, por la proposición 1.1 se tiene que $b^{n-1} \in C(A)$, luego $\phi_a(\overline{u(x)}^{n-1}) \in C(A)$ para todo homomorfismo ϕ_a con $a \in A$ $a \neq 0$. Esto nos muestra que

$$\overline{u(x)}^{n-1} \in \bigcap_{a \neq 0} \phi_a^{-1}(C(A)) = S_A \qquad \text{iii}$$

La proposición siguiente nos muestra como la conmutatividad de un Jn-anillo A con característica prima p se puede ver a través de un anillo exterior a él.

1.8 TEOREMA: Sea A un Jn-anillo con característica prima p. A es conmutativo si y solo si el precentro de $\mathbb{Z}_p[x] / \langle x^n - x \rangle$ relativo a A es igual a todo el anillo $\mathbb{Z}_p[x] / \langle x^n - x \rangle$

Supongamos que $S_A = \mathbb{Z}_p[x] / \langle x^n - x \rangle$ y veamos que A es conmutativo. Como el elemento $\bar{x} \in S_A$, se tiene que $a = \overset{T}{\phi}_a(\bar{x}) \in C(A)$ para todo $a \in A$, esto muestra que A es conmutativo.

Recíprocamente, si A es conmutativo y $p(\bar{x}) \in \mathbb{Z}_p[x] / \langle x^n - x \rangle$ se tiene que para todo $a \in A$, $a \neq 0$ $\overset{T}{\phi}_a(p(\bar{x})) \in A = C(A)$ luego $p(\bar{x}) \in \bigcap_{a \neq 0} \overset{T}{\phi}{}_a^{-1}(C(A)) = S_A$, lo cual prueba que $S_A = \mathbb{Z}_p[x] / \langle x^n - x \rangle$ ||||

Denotaremos en lo que sigue al anillo $\mathbb{Z}_p[x] / \langle x^n - x \rangle$ simplemente como $\mathbb{Z}_{p,n}[x]$. ||||

El teorema anterior muestra que es posible demostrar la conmutatividad de A probando que $S_A = \mathbb{Z}_{p,n}[x]$. La proposición 1.7 nos garantiza que para cualquier Jn-anillo A con característica prima p, S_A no es trivial ya que por ejemplo $\bar{1}, (\bar{x} + \bar{1})^{n-1}, \bar{x}^{n-1}$ son elementos de S_A. Veremos

más adelante que si n y p están relacionados de cierta manera es posible garantizar que un subanillo R de $\mathbb{Z}_{p,n}[x]$ que tenga la propiedad de absorber las potencias $n-1$, es necesariamente todo el anillo $\mathbb{Z}_{p,n}[x]$ y por lo tanto todos los Jn-anillos con característica prima p en donde n,p están en la relación mencionada serán anillos conmutativos.

Veremos en lo que sigue como es posible descomponer a $\mathbb{Z}_{p,n}[x]$ en una Suma de campos. Para ello necesitamos estudiar antes la factorización del polinomio $x^n - x$ en $\mathbb{Z}_p[x]$.

2. FACTORIZACION DEL POLINOMIO $x^n - x$ $(n > 1)$ EN $\mathbb{Z}_p[x]$

2.1 Es claro que el polinomio $x^n - x$ es igual a $x.(x^{n-1} - \overline{1})$; luego el estudio de la factorización de $x^n - x$ en $\mathbb{Z}_p[x]$ se reduce a ver como se puede descomponer el polinomio $x^{n-1} - \overline{1}$ en factores irreducibles en $\mathbb{Z}_p[x]$. El hecho de que los coeficientes de $x^{n-1} - \overline{1}$ estén en $\mathbb{Z}_p$ hace que la descomposición de este polinomio en factores irreducibles sea más compleja que en el caso en donde sus coeficientes están en $\mathbb{Z}$. Por ejemplo el polinomio $x^7 - 1$ en $\mathbb{Z}[x]$ se puede factorizar de la siguiente manera $x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ donde cada factor es irreducible, sin embargo en el anillo $\mathbb{Z}_2[x]$, por ejemplo, el segundo factor no es irreducible ya que $x^6 + x^5 + \ldots + x + \overline{1} =$

$= (\overline{1} + x^2 + x^3)(\overline{1} + x + x^3)$

2.2 CAMPO RAIZ DE $x^{n-1} - \overline{1}$

Denotaremos por E el campo raíz del polinomio $x^{n-1} - \overline{1}$. Recordemos que la caracterización de E está dada por las dos afirmaciones siguientes:

i) El campo E es una extensión de $\mathbb{Z}_p$ en donde el polinomio $x^{n-1}-\bar{1}$ se puede factorizar como producto de factores lineales. Es decir, existen $w_1, w_2, \ldots w_{n-1}$ en E tales que

$$x^{n-1} - \bar{1} = (x - w_1)(x - w_2) \ldots (x - w_{n-1})$$

ii) E es la mínima extensión de $\mathbb{Z}_p$ en donde $x^{n-1} - \bar{1}$ se puede factorizar como producto de factores lineales, es decir si $\mathbb{Z}_p \subset T \subset E$ y $x^{n-1} - \bar{1}$ tiene todas sus raices en T, entonces $T = E$.

2.3 OBSERVACION: El campo raíz E, de $x^{n-1} - \bar{1}$, se obtiene extendiendo sucesivamente a $\mathbb{Z}_p$ con campos de la forma $E_o = \mathbb{Z}_p$

$E_i = E_{i-1}[x]/\langle p_i(x)\rangle$, $E_m = E$, donde $\langle p_i(x)\rangle$ denota el ideal generado
$i=1,\ldots m$

por un polinomio $p_i(x)$ irreducible en $E_{i-1}[x]$, ([4] pág. 180). Cada uno de los campos E_i, $i=1,\ldots m$ es un campo finito como puede verse por inducción sobre i. Para $i=0$, $E_o = \mathbb{Z}_p$ es finito. Sea r_i = grado $p_i(x)$ y asumamos que E_{i-1} es finito. Los elementos de E_i son de la forma $a_o + a_1 z + \ldots + a_{r_{i-1}} z^{r_{i-1}}$ donde $a_o, a_1, \ldots a_{r_{i-1}} \in E_{i-1}$ y z es un cierto elemento en E_i, ([4] pág. 171), luego el número de elementos en E_i es igual al número de combinaciones lineales posibles de la forma antes indicada. Si denotamos por $|E_i|$ el orden del campo E_i, según

lo anotado antes $|E_i| = |E_{i-1}| \cdot \underbrace{|E_{i-1}| \cdots |E_{i-1}|}_{r_i} = |E_{i-1}|^{r_i}$. Esto muestra que E_i es finito.

Como E es un campo finito y es una extensión de $\mathbb{Z}_p$ la característica de E deberá ser igual a p.

2.4 Asumiremos de ahora en adelante que p es un primo que no divide a $n-1$. Esto implica que el polinomio $x^{n-1} - \bar{1} \in \mathbb{Z}_p[x]$ no tenga raices repetidas en E, lo cual se deduce del hecho de que él y su derivada $(n-1)\, x^{n-2}$ (que es distinta del polinomio nulo, ya que $p \nmid n-1$) no tienen factores no triviales en común. ([4] pág. 192).

2.5 Es claro que las raices de $x^{n-1} - \bar{1}$ en E forman un subgrupo del grupo multiplicativo de E, y que los elementos de dicho subgrupo son exactamente los elementos de $L_{n-1} = \left\{ z \in E \mid z^{n-1} = \bar{1} \right\}$. Como el grupo multiplicativo de E es cíclico, ya que E es un campo finito, el subgrupo L_{n-1} también lo es y por lo tanto existe un elemento $w \in L_{n-1}$ generador de L_{n-1}. Como $x^{n-1} - \bar{1}$ tiene $n-1$ raices distintas, el orden de w deberá ser $n-1$ y $L_{n-1} = \left\{ w, w^2, \ldots w^{n-1} = \bar{1} \right\}$.

2.6 En adelante la frase d divisor de $n-1$ indicará divisor positivo de $n-1$. Para cada divisor d de $n-1$ definamos

$H_d = \left\{ z \in L_{n-1} \mid o(z) = d \right\}$ (donde $o(z)$ denota el orden del elemento

z en $L_{n-1} = \left\{ z \in E \mid z^{n-1} = \overline{1} \right\}$) y $Gd = \left\{ z \in L_{n-1} \mid z^{d} = \overline{1} \right\}$.

Como puede verse facilmente Gd es un subgrupo de L_{n-1} mientras que Hd no lo es necesariamente. Si d_1, d_2 son dos divisores distintos de n-1 los conjuntos Hd_1 , Hd_2 son disjuntos. Como el orden de cualquier elemento de L_{n-1} es un divisor de n-1 , la unión de los conjuntos Hd es todo el grupo L_{n-1} , $L_{n-1} = \bigcup_{d \mid n-1} Hd$.

La proposición siguiente nos muestra que Gd es un grupo cíclico de orden d generado por el elemento $w^{\frac{n-1}{d}}$, lo que denotaremos como $Gd = (w^{\frac{n-1}{d}})$, donde w es el elemento generador de L_{n-1} .

2.7 PROPOSICION: Con la notación anterior, para cada divisor d de n-1 se tiene que:

i) $Hd \subset Gd \subset L_{n-1}$

ii) $Gd = (w^{\frac{n-1}{d}})$ y $|Gd| = d$

La primera afirmación es una consecuencia inmediata de la definición de Hd y Gd .

Para ver ii) , Sea $z \in Gd$, como $z \in L_{n-1}$ se tiene que $z = w^{\alpha}$ para un cierto α , $1 \leq \alpha \leq n-1$. Como $z^{d} = w^{\alpha d} = \overline{1}$ y como

$o(w) = n - 1$ se debe tener que $n - 1 \mid \alpha . d$ y en consecuencia α se puede escribir como $\alpha = \left(\frac{n-1}{d}\right) .k$ para un cierto entero $k > 0$, y por lo tanto $z \in \left(w^{\frac{n-1}{d}}\right)$. Por otro lado, si $z \in \left(w^{\frac{n-1}{d}}\right)$ es claro que $z^d = \overline{1}$, esto nos muestra que $Gd = \left(w^{\frac{n-1}{d}}\right)$.

Si β es un entero positivo tal que $w^{\frac{(n-1).\beta}{d}} = \overline{1}$ entonces $n - 1$ divide a $\frac{(n-1).\beta}{d}$ y en consecuencia $\frac{(n-1).\beta}{d} \geqslant (n-1)$, y por lo tanto $\beta \geqslant d$.

Esto nos muestra que $o\left(w^{\frac{n-1}{d}}\right) = d = |Gd|$ ||||

Recordemos que la función de Euler $\varphi(k)$ se define para $k = 1$ como $\varphi(1) = 1$ y para $k > 1$ como el número de enteros positivos menores que k y primos con él. Con esta notación se tiene la siguiente proposición:

2.8 PROPOSICION: Para cada divisor d de $n - 1$ los generadores del grupo cíclico Gd son los $\varphi(d)$ elementos del conjunto Hd, y solamente ellos.

En efecto, si $z \in Hd$, $o(z) = d = |Gd|$ y por lo tanto z genera a Gd. Recíprocamente, cada generador de Gd es un elemento de orden

d y por lo tanto está en Hd. Si denotamos por $\tau = w^{\frac{n-1}{d}}$ se tiene por la proposición 2.7 que $Gd = \{\tau, \tau^2, \ldots \tau^d = \bar{1}\}$. τ^r, $1 \leqslant r \leqslant d$, es un generador de Gd si y solo si $(r,d) = 1$ (máximo común divisor de r y d igual a 1) ([6] pág. 34) y por lo tanto Gd tiene exactamente $\varphi(d)$ generadores ||||

2.9 Sea τ como en la prueba de la proposición anterior, $u(d)$ el grupo de los enteros positivos menores o iguales a d y primos con d. Para cada divisor d de $n - 1$ definimos el polinomio ciclotómico $Cd(x)$ como:

$$Cd(x) = \prod_{r \in u(d)} (x - \tau^r)$$

Veamos a continuación como se factoriza $x^{n-1} - \bar{1}$ cómo producto de polinomios ciclotómicos.

2.10 PROPOSICION: El polinomio $x^{n-1} - \bar{1}$ se puede factorizar como:

$$x^{n-1} - \bar{1} = \prod_{d|n-1} Cd(x)$$

En efecto, sabemos que $x^{n-1} - \bar{1}$ se puede factorizar como el producto de sus raices en el campo E, $x^{n-1} - \bar{1} = \prod_{z \in L_{n-1}} (x - z)$. (1) Como se vió en 2.6 y en 2.8 $L_{n-1} = \bigcup_{d|n-1} Hd$ donde Hd_1, Hd_2 son disjuntos si

$d_1 \nmid d_2$, y $Hd = \left\{ \tau^r \,/\, r \in u(d) \right\}$, luego el producto en la derecha de (1) puede escribirse como $\prod_{d|n-1} \prod_{z \in Hd} (x - z)$ y en consecuencia:

$$x^{n-1} - \overline{1} = \prod_{d|n-1} \prod_{z \in Hd} (x - z) = \prod_{d|n-1} \prod_{r \in u(d)} (x - \tau^r) = \prod_{d|n-1} Cd(x) \quad \|$$

2.11 Antes de pasar a probar la siguiente proposición, recordemos la forma que tienen los automorfismos de un campo finito. Si F es un campo finito con característica prima p y de orden p^m , $m \geqslant 1$, entonces los únicos automorfismos de F son de la forma $f_k(a) = a^{p^k}$ $0 \leqslant k < m$, para todo $a \in F$. Es claro que los automorfismos de F forman un grupo cíclico de orden m que es generado por el automorfismo $f_1(a) = a^p$.

2.12 Sea d un divisor de $n - 1$, como $p \nmid n-1$ (2.4) p y d son primos entre si ya que de lo contrario p dividiría a d y por consiguiente a $n - 1$. Si denotamos por $\overline{p}$ la clase de p modulo d, $d \neq 1$, por lo observado antes $\overline{p} \in u(d)$. Cuando $d = 1$ convenimos en que $\overline{p} = 1$. Denotaremos por $(\overline{p})$ el subgrupo de $u(d)$ generado por $\overline{p}$, y con $Od(\overline{p})$ su orden. Las clases laterales de $(\overline{p})$ en $u(d)$ las denotaremos con $(\overline{p})_1 = (\overline{p}), (\overline{p})_2, \ldots (\overline{p})_{ld}$ en donde $ld = \dfrac{\varphi(d)}{Od(\overline{p})}$, es decir, el número de clases laterales de $(\overline{p})$ en $u(d)$. Nótese que para cada

i tal que $1 \leqslant i \leqslant ld$ existe $V_i \in u(d)$ tal que $(\bar{p})_i = (\bar{p}).V_i$.

Para cada $d \mid n-1$ sea $Cd(x)$ el polinomio ciclotómico definido en 2.9 y sea $\tau = w^{\frac{n-1}{d}}$, donde w es el generador del subgrupo L_{n-1} .

2.13 PROPOSICION: Para cada divisor d de $n-1$ se tiene que:

$$Cd(x) = \prod_{i=1}^{ld} Cd,i(x)$$ en donde para cada i , $1 \leqslant i \leqslant ld$ definimos

$$Cd,i(x) = \prod_{r \in (\bar{p})_i} (x - \tau^r) .$$

En efecto, las clases $(\bar{p})_1, \ldots (\bar{p})_{ld}$ constituyen una partición de $u(d)$ y por consiguiente:

$$Cd(x) = \prod_{r \in u(d)} (x - \tau^r) = \prod_{i=1}^{ld} \left(\prod_{r \in (\bar{p})_i} (x - \tau^r) \right) \qquad \text{iiii}$$

2.14 OBSERVACION: Sea E el campo raiz de $x^{n-1} - \bar{1}$; si denotamos por $G(E\ \mathbb{Z}_p)$ el grupo de automorfismos de E que dejan fijo a $\mathbb{Z}_p$, como E es una extensión normal de $\mathbb{Z}_p$ ya que E es el campo raiz de un polinomio en $\mathbb{Z}_p[x]$ ([4] , pág. 204) se tiene que el campo fijado por $G(E\ \mathbb{Z}_p)$ es exactamente $\mathbb{Z}_p$. En otras palabras, si $z \in E$ y $f(z) = z$ para todo $f \in G(E\ \mathbb{Z}_p)$ entonces $z \in \mathbb{Z}_p$. Además, si f es un automorfismo cualquiera de E entonces $f(\bar{1}) = \bar{1}$,

y si $\overline{m} \in \mathbb{Z}_p$ $f(\overline{m}) = f(\underbrace{\overline{1} + \dots + \overline{1}}_{m}) = mf(\overline{1}) = \overline{m}$ luego f deja fijo

a todo elemento de $\mathbb{Z}_p$ y por consiguiente $G(E\ \mathbb{Z}_p)$ **coincide con todo el grupo de automorfismos de** E **,** que como se anotó en 2.11 es cíclico y generado por f_1, donde $f_1(a) = a^p$, para todo $a \in E$.)

Sea Id como en 2.12 , $Cd,i(x) = \prod_{r \in (\bar{p})_i} (x - \tau^r)$, $1 \leqslant i \leqslant Id$.

2.15 PROPOSICION: Cada uno de los polinomios $Cd,i(x)$ tiene sus coeficientes en $\mathbb{Z}_p$ y es irreducible en $\mathbb{Z}_p[x]$.

Si $f \in G(E\ \mathbb{Z}_p)$ podemos extender f a un homomorfismo $\hat{f}$,

$\hat{f} : E[x] \longrightarrow E[x]$ de la manera natural, si $p(x) \in E[x]$, $p(x) = \sum_{i=0}^{m} a_i x^i$

definimos $\hat{f}(p(x)) = \sum_{i=0}^{m} f(a_i)\ x^i$. Es fácil ver que $\hat{f}$ es un homomorfismo de $E[x]$ a $E[x]$ y que $\hat{f}$ restringido a E coincide con f . Para mostrar que $Cd,i(x)$ tiene sus coeficientes en $\mathbb{Z}_p$ basta ver que $Cd,i(x)$ es invariante bajo todos los homomorfismos $\hat{f}$ con $f \in G(E\ \mathbb{Z}_p)$ ya que si suponemos que $Cd,i(x) = b_0 + \dots + b_k x^k + \dots + b_m x^m$ con $b_k \notin \mathbb{Z}_p$ por lo anotado en 2.14 existe un $f' \in G(E\ \mathbb{Z}_p)$ tal que

$f'(b_k) \neq b_k$ y por consiguiente $\hat{f}'(Cd,i(x))$ tendría su término k-ésimo diferente del de $Cd,i(x)$ lo cual traería una contradicción con la invarianza de $Cd,i(x)$.

Para mostrar que $Cd,i(x)$ es invariante bajo todos los $\hat{f}$ con $f \in G(E\ \mathbb{Z}_p)$ basta ver que lo es bajo $\hat{f}_1$ donde f_1 es el generador del grupo $G(E\ \mathbb{Z}_p)$. Por definición $Cd,i(x) = \prod_{r \in (\bar{p})_i} (x - \tau^r)$ (1) luego aplicando $\hat{f}_1$ obtenemos $\hat{f}_1(Cd,i(x)) = \prod_{r \in (\bar{p})_i} (x - f_1(\tau^r)) = \prod_{r \in (\bar{p})_i} (x - \tau^{r.p})$ (2) . Para mostrar que (1) es igual a (2) basta mostrar la igualdad de los conjuntos $C_1 = \left\{ \tau^r \mid r \in (\bar{p})_i \right\}$, $C_2 = \left\{ \tau^{p.r} \mid r \in (\bar{p})_i \right\}$ donde, recordemos, $\tau = w^{\frac{n-1}{d}}$, siendo w el generador de L_{n-1} (2.5) . Como puede verse $\tau^{k_1} = \tau^{k_2}$ si y solo si $k_1 = k_2$ modulo (d) . Si $r \in (\bar{p})_i$ existe $r' \in (\bar{p})_i$ tal que $\bar{p}.r' = r$ en $u(d)$ y por consiguiente $pr' \equiv r \bmod (d)$ y $\tau^{pr'} = \tau^r$ teniéndose que $C_1 \subset C_2$. Si $r \in (\bar{p})_i$ es claro que $\tau^{p.r} = \tau^{\bar{p}.r}$ y como obviamente $\bar{p}.r \in (\bar{p})_i$ se tiene también la inclusión en el otro sentido. Hemos demostrado que $Cd,i(x) \in \mathbb{Z}_p[x]$.

Mostremos ahora la irreducibilidad. Supongamos que $Cd,i(x) = h(x).g(x)$, $h(x),g(x) \in \mathbb{Z}_p[x]$.

Como se anotó en 2.12 para cada i, $1 \leqslant i \leqslant Id$ existe un v_i tal que $(\bar{p})_i = (\bar{p}).v_i$. Como τ^{v_i} es raíz de $Cd,i(x)$, lo es de $h(x)$ ó bien de $g(x)$. Supongamos que es raíz de $h(x)$. Por tener $h(x)$ todos sus coeficientes en $\mathbb{Z}_p$, es invariante bajo todos los homomorfismos $\hat{f}$, $f \in G(E\ \mathbb{Z}_p)$ en especial, bajo $\hat{f}_1$. Mostremos a continuación que para todo $r \in (\bar{p})_i$, τ^r es raíz de $h(x)$. En efecto, si

$h(x) = (x - \tau^{v_i}).q(x)$, $q(x) \in E[x]$ se tiene que:

$h(x) = \hat{f}_1(h(x)) = (x - \tau^{p.v_i})\ \hat{f}_1(q(x))$ de donde se sigue que $\tau^{p.v_i}$ es raíz de $h(x)$. Repitiendo el razonamiento anterior vemos que

$\tau^{p^k.v_i}$ $k \in \mathbb{Z}$, $k \geqslant 0$ es raíz de $h(x)$ y en consecuencia si $r \in (\bar{p})_i$

$r = \bar{p}^k.v_i$ para algún $k \geqslant 0$ luego $\tau^r = \tau^{p^k.v_i}$ es raíz de $h(x)$.

Como $h(x)$ contiene las raices del polinomio $Cd,i(x)$, su grado deberá ser igual o mayor que el de éste y $g(x)$ deberá ser por consiguiente un polinomio constante; esto nos muestra que $Cd,i(x)$ es irreducible ||||

2.16 OBSERVACION: De las proposiciones 2.10 , 2.13 y 2.15 concluimos que si $n \in \mathbb{Z}$, $n > 1$ y p es un primo tal que $p \nmid n-1$ entonces $x^n - x$ se puede factorizar en $\mathbb{Z}_p[x]$ en factores irreducibles de la siguiente manera:

$$x^n - x = x. \prod_{d|n-1} \prod_{i=1}^{ld} C_{d,i}(x) \quad , \quad ld = \frac{\varphi(d)}{Od(\bar{p})}$$

Para cada divisor d de $n-1$, los polinomios $C_{d,i}(x)$, $1 \leqslant i \leqslant ld$, son polinomios irreducibles en $\mathbb{Z}_p[x]$ y de igual grado, ya que por definición $C_{d,i}(x) = \prod_{r \in (\bar{p})_i} (x - \tau^r)$ luego el grado de $C_{d,i}(x)$ es igual al número de elementos en la clase lateral $(\bar{p})_i$, igual para cada i , al orden del subgrupo $(\bar{p})$ que habíamos denotado por $Od(\bar{p})$.

3. ESTUDIO DEL ANILLO $\mathbb{Z}_{p,n}[x]$

3.0 Recordemos que $\mathbb{Z}_{p,n}[x]$ es el anillo $\mathbb{Z}_p[x] \big/ \langle x^n - x \rangle$.

3.1 En lo que sigue mostraremos como $\mathbb{Z}_{p,n}[x]$, con p primo y $p \nmid n-1$, puede descomponerse en una suma directa de campos. La siguiente proposición nos muestra cuando un anillo conmutativo con unidad se puede escribir como suma de campos.

3.2 PROPOSICION: Si R es un anillo conmutativo con unidad y M_i $i=1,2,\ldots k$ son ideales maximales de R tales que $\bigcap_{i=1}^{k} M_i = \{0\}$ y para cada i_o, $1 \leq i_o \leq k$ $\bigcap_{i \neq i_o} M_i \neq \{0\}$ entonces R es isomorfo a la suma directa de campos R/M_i

$$R \simeq R/M_1 \oplus R/M_2 \oplus \ldots \oplus R/M_k$$

Para la demostración de esta proposición ver ([9] pág. 59)

El resultado anterior puede usarse para descomponer un anillo de la forma

$\mathbb{Z}_p[x] \,/\, \langle f(x) \rangle$ en suma de campos como lo muestra la siguiente proposición.

3.3 PROPOSICION: Sea $f(x) = p_1(x) \cdot \ldots \cdot p_k(x)$ donde $p_i(x)$ $i=1,2,\ldots,k$ **son polinomios distintos dos a dos e irreducibles en** $\mathbb{Z}_p[x]$. **El anillo** $\mathbb{Z}_p[x] \,/\, \langle f(x) \rangle$ **se puede escribir de la siguiente manera:**

$$\mathbb{Z}_p[x] \,/\, \langle f(x) \rangle \simeq \mathbb{Z}_p[x] \,/\, \langle p_1(x) \rangle \oplus \ldots \oplus Z_p[x] \,/\, \langle p_k(x) \rangle$$

En efecto, si hacemos $M_i = \langle p_i(x) \rangle / \langle f(x) \rangle$, para $i=1,2,\ldots k$, entonces cada M_i es un ideal maximal del anillo $R = \mathbb{Z}_p[x] \,/\, \langle f(x) \rangle$. Esto lo podemos probar mostrando que R/M_i es un campo no trivial. Como $R/M_i = (\mathbb{Z}_p[x] \,/\, \langle f(x) \rangle) \,/\, (\langle p_i(x) \rangle / \langle f(x) \rangle)$ es isomorfo a $\mathbb{Z}_p[x] \,/\, \langle p_i(x) \rangle$ ([3] pág. 46) basta ver que $\mathbb{Z}_p[x] \,/\, \langle p_i(x) \rangle$ es un campo no trivial, pero esto último se da, ya que $\langle p_i(x) \rangle$ es un ideal maximal de $\mathbb{Z}_p[x]$ por ser $p_i(x)$ irreducible.

Mostremos ahora que $\bigcap_{i=1}^{k} M_i = \{0\}$. Si denotamos con $\overline{q(x)}$ un elemento de R que está en la intersección de todos los ideales M_i , se tiene que existen elementos $\overline{g_i(x)}$, $i=1,2,\ldots k$, en R tal que para cada i $\overline{q(x)} = \overline{g_i(x)}.\overline{p_i(x)}$, o lo que es equivalente a decir que $f(x)$ divide a

$q(x) - g_i(x).p_i(x)$. Como para cada $i=1,2,\ldots k$, $p_i(x) \mid f(x)$, se tiene que $p_i(x) \mid \left(q(x) - g_i(x).p_i(x)\right)$ y por lo tanto $p_i(x) \mid q(x)$ para todos los $i=1,2,\ldots k$, y en consecuencia $f(x) \mid q(x)$ de donde $\overline{q(x)} = 0$.

Probemos finalmente que dado un i_o , $1 \leqslant i_o \leqslant k$, se tiene que $\bigcap_{i \neq i_o} M_i \neq \{0\}$

Sea $u(x) = \prod_{i \neq i_o} p_i(x)$ es claro que $\overline{u(x)} \in M_i$ para $i \neq i_o$, además, $\overline{u(x)} \neq 0$ en R ya que si fuera cero $f(x)$ dividiría a $u(x)$ y en consecuencia $p_{i_o}(x)$ dividiría a $u(x)$. Como $u(x)$ es un producto de factores irreducibles distintos dos a dos y $p_{i_o}(x)$ divide dicho producto, debe dividir al menos uno de los factores $p_i(x)$ $i \neq i_o$ ([4] pág. 108) pero esto es imposible por ser cada $p_i(x)$ irreducible. ∎

3.4 Sea n un entero mayor que 1 , p un primo tal que $p \nmid n-1$. Para cada divisor positivo d de $n-1$ denotaremos por $F_{d,i}$ $1 \leqslant i \leqslant I_d$, $I_d = \dfrac{\varphi(d)}{O_d(\bar{p})}$ cada uno de los campos $\mathbb{Z}_p[x] / \langle C_{d,i}(x) \rangle$ donde $C_{d,i}$ son polinomios irreducibles en $\mathbb{Z}_p[x]$ dados en 2.13, y por $\mathbb{Z}_p \oplus \left(\bigoplus_{\substack{d \mid n-1 \\ i=1,\ldots I_d}} F_{d,i} \right)$

la suma directa de $\mathbb{Z}_p$ y todos los campos $F_{d,i}$.

3.5 TEOREMA: Con esta notación, para $n > 1$ y p un primo tal que $p \nmid n-1$ se tiene que:

i) $$\mathbb{Z}_{p,n}[x] \simeq \mathbb{Z}_p \oplus \Big(\bigoplus_{\substack{d \mid n-1 \\ i=1,\dots,I_d}} F_{d,i} \Big)$$

ii) Para cada d divisor de $n-1$ todos los campos $F_{d,i}$ $1 \leqslant i \leqslant I_d$ tienen orden $|F_{d,i}|$ igual a $p^{O_d(\bar{p})}$

En efecto, por la observación 2.16, $x^n - x = x. \prod_{d \mid n-1} \prod_{i=1}^{I_d} C_{d,i}(x)$. Cada par de factores en este producto son distintos, ya que de ser iguales el polinomio $x^n - x$ tendría raices repetidas en el campo raiz E lo cual es imposible ya que las raices de este polinomio son: cero, junto con las raices de $x^{n-1} - \bar{1}$ que como se vió (2.4) son todas distintas. Aplicando la proposición 3.3 con $f(x) = x^n - x$ obtenemos:

$$\mathbb{Z}_{p,n}[x] = \mathbb{Z}_p[x] \big/ \langle x^n - x \rangle \simeq \mathbb{Z}_p[x] \big/ \langle x \rangle \oplus \Big(\bigoplus_{\substack{d \mid n-1 \\ i=1,\dots,I_d}} \mathbb{Z}_p[x] \big/ \langle C_{d,i}(x) \rangle \Big)$$

pero es claro que $\mathbb{Z}_p[x] \big/ \langle x \rangle \simeq \mathbb{Z}_p$ por ser campos de igual orden

luego $$\mathbb{Z}_{p,n}[x] \simeq \mathbb{Z}_p \oplus \Big(\bigoplus_{\substack{d \mid n-1 \\ i=1,\dots,I_d}} F_{d,i} \Big)$$

Ahora bien, para cada d divisor de $n-1$ se tiene que

grado $(C_{d,i}(x)) = O_d(\bar{p})$ y el campo cociente $\mathbb{Z}_p[x] \big/ \langle C_{d,i}(x) \rangle$ tiene por lo tanto $p^{O_d(\bar{p})}$ elementos ([3] pág. 156), de donde concluimos ii) ∎

3.5 EJEMPLO: Para $n=13$ y $p=5$, $5 \nmid 13-1$. Los divisores de 12 son 1,2,3,4,6,12. Recordemos que $O_d(\bar{p})$ es el orden de $\bar{p}$ en $u(d)$. Como puede verse $O_1(\bar{5}) = 1$, $O_2(\bar{5}) = 1$, $O_3(\bar{5}) = 2$, $O_4(\bar{5}) = 1$, $O_6(\bar{5}) = 2$, $O_{12}(\bar{5}) = 2$.

$$\mathbb{Z}_{5,13}[x] \simeq \mathbb{Z}_5 \oplus F_{1,1} \oplus F_{2,1} \oplus F_{3,1} \oplus F_{3,2} \oplus F_{4,1} \oplus F_{6,1} \oplus F_{6,2} \oplus F_{12,1} \oplus F_{12,2}$$

$$|F_{1,1}| = 5 , \quad |F_{2,1}| = 5 , \quad |F_{3,1}| = |F_{3,2}| = 5^2 , \quad |F_{4,1}| = 5 ,$$

$$|F_{6,1}| = |F_{6,2}| = 5^2 \qquad |F_{12,1}| = |F_{12,2}| = 5^2 .$$

4. CONMUTATIVIDAD DE CIERTOS Jn-ANILLOS

4.0 En este capítulo probaremos el resultado principal de este trabajo. Veremos que si p es un primo, para ciertos enteros n que llamaremos admisibles para el primo p, los Jn-anillos correspondientes, si tienen característica p, son conmutativos.

De igual manera que como se hizo en 2.8, el símbolo (a,b) denotará en lo que sigue el máximo común divisor de a y b.

4.1 Sea p un número primo. Diremos que un entero $n > 1$ es admisible para p si se satisface que:

i) $p \nmid n-1$

ii) Para cada divisor positivo d de $n-1$ para el cual $Od(\bar{p}) > 1$ se verifica que:

$$(n-1,\ p^{Od(\bar{p})} - 1) < p^{\frac{Od(\bar{p})}{2}} + 1$$

Sea A un Jn-anillo con característica prima p, y n un entero admisible para p. La proposición siguiente nos muestra que en este caso el precentro de $Z_{p,n}[x]$ relativo a A, es igual a todo el anillo $Z_{p,n}[x]$

y por 1.7 el anillo A es conmutativo.

4.2 TEOREMA: Sea A un Jn-anillo con característica prima p. Si n es admisible para p entonces A es conmutativo.

En efecto, como se demostró en 3.4, existe un isomorfismo ψ de $\mathbb{Z}_{p,n}[x]$ a una suma finita de campos que por brevedad escribiremos como $\sum_{k=1}^{m} F_k$. $\psi : \mathbb{Z}_{p,n}[x] \longrightarrow \sum_{k=1}^{m} F_k$. Para mostrar que A es conmutativo, por 1.7, basta mostrar que $S_A = \mathbb{Z}_{p,n}[x]$ lo cual es equivalente a demostrar que $\psi(S_A) = \sum_{k=1}^{m} F_k$ (1). Para cada k, $1 \leqslant k \leqslant m$ las funciones $P_k : F_k \longrightarrow \sum_{k=1}^{m} F_k$ y $\pi_k : \sum_{k=1}^{m} F_k \longrightarrow F_k$ denotarán la inclusión y la proyección canónica respectivamente. Como se sabe P_k y π_k son homomorfismos y si $r \in \sum_{k=1}^{m} F_k$ entonces $r = P_1 \circ \pi_1(r) + \ldots + P_m \circ \pi_m(r)$ (2). Si demostramos que para cada k, $P_k(F_k) \subset \psi(S_A)$ habremos demostrado (1). En efecto, si $r \in \sum_{k=1}^{m} F_k$ $\pi_k(r) \in F_k$ y por lo tanto $P_k(\pi_k(r)) \in \psi(S_A)$ para todo $1 \leqslant k \leqslant m$

y en consecuencia cada uno de los sumandos en (2) es un elemento de $\psi(S_A)$. Como $\psi(S_A)$ es un subanillo de $\sum_{k=1}^{m} F_k$, la suma (2) es también un elemento de S_A, es decir, $r \in \psi(S_A)$ y se da (1). Veamos entonces que $P_k(F_k)$ si es subconjunto de $\psi(S_A)$. Sea $1k$ la unidad del campo F_k, y $q_k = \psi^{-1}(P_k(b_k))$ donde b_k es el elemento generador del grupo multiplicativo del campo F_k. Si hacemos $e_k = \psi^{-1}(P_k(1k))$, como se vió en 1.7, $e^{n-1} \in S_A$ y $\psi(ek^{n-1}) \in \psi(S_A)$ pero

$$\psi(ek^{n-1}) = \left[\psi(\psi^{-1}P_k(1k))\right]^{n-1} = P_k(1k), \text{ luego } P_k(1k) \in \psi(S_A) \quad (3).$$

Similarmente $\psi(q_k^{n-1}) = P_k(b^{n-1}) \in \psi(S_A)$ (4). Como nuestro propósito es demostrar que para cada k, $1 \leqslant k \leqslant m$, $P_k(F_k) \subset \psi(S_A)$ por (3) y (4) bastará demostrar que el subanillo de F_k generado por $1k$ y b_k^{n-1}, que denotaremos por $\left[1k, b_k^{n-1}\right]$ es igual a F_k.

Como $\left[1k, b_k^{n-1}\right]$ es un subanillo que contiene la unidad de F_k y F_k es un campo finito, $\left[1k, b_k^{n-1}\right]$ es un dominio entero finito y por lo tanto un subcampo de F_k. Distingamos dos casos: Si $|F_k| = p$ ó bien $|F_k| > p$. En el primer caso F_k es isomorfo a $\mathbb{Z}_p$ y en este caso

$\left[1k, b_k^{n-1}\right] = F_k$ ya que el subcampo generado por la unidad de F_k es igual a F_k y este subcampo está obviamente en $\left[1k, b_k^{n-1}\right]$. Si $|F_k| > p$ como con F_k representamos uno de los campos dados en 3.4 se tiene que $F_k = Fd,i$ d divisor de n-1 y $1 \leqslant i \leqslant Id = \dfrac{\ell(d)}{Od(\bar{p})}$.

Como $|F_k| = p^{Od(\bar{p})}$ entonces $Od(\bar{p}) > 1$ ya que estamos suponiendo que $|F_k| > p$. El número de potencias distintas de b_k^{n-1} en $\left[1k, b_k^{n-1}\right]$ es igual a:

$$\frac{p^{Od(\bar{p})} - 1}{u} \qquad \text{donde} \quad u = (n-1,\ p^{Od(\bar{p})} - 1)$$

Esto último ya que el grupo multiplicativo del campo Fd,i tiene $p^{Od(\bar{p})}-1$ elementos, igual al orden de bk en este grupo. ([6] pág. 34). Como $\left[1k, b_k^{n-1}\right]$ contiene el subgrupo generado por b_k^{n-1} y contiene además el elemento cero, entonces:

$$\left|\left[1k, b_k^{n-1}\right]\right| > \frac{p^{Od(\bar{p})} - 1}{u}$$

Ambos lados de la desigualdad anterior son números enteros luego

$$\left|\left[1k, b_k^{n-1}\right]\right| - 1 \geq \frac{p^{Od(\bar{p})} - 1}{u} \qquad (5).$$

Como $\left[1k, b_k^{n-1}\right]$ es un subcampo de F_k se deberá tener que

$\left|\left[1k,b_k^{n-1}\right]\right| = P^s \quad s \in \mathbb{Z}\ ,\ s > 0$. Además, como el orden del grupo multiplicativo de $\left[1k,b_k^{n-1}\right]$ es $P^s - 1$ y divide al orden del grupo multiplicativo de $F_{d,i}$ entonces $P^s - 1 \mid P^{Od(\bar{p})} - 1$ y en consecuencia $s \mid Od(\bar{p})$ ([4] pág. 325). Como s es un divisor de $Od(\bar{p})$, es igual a $Od(\bar{p})$ o bien tiene que ser menor o igual que su mitad, $s \leqslant \frac{Od(\bar{p})}{2}$. Esto último no puede suceder ya que si $s \leqslant \frac{Od(\bar{p})}{2}$ entonces por (5) tenemos que:

$$u \geq \frac{P^{Od(\bar{p})} - 1}{P^s - 1} \geq \frac{P^{Od(\bar{p})} - 1}{P^{\frac{Od(\bar{p})}{2}} - 1} = P^{\frac{Od(\bar{p})}{2}} + 1$$

Esta última desigualdad contradice el hecho de ser n admisible para p .

Luego $s = Od(\bar{p})$ y $\left[1k,b_k^{n-1}\right] = F_k$ ⁞⁞

La proposición siguiente nos proporciona algunas condiciones suficientes para ver que un entero n es admisible para un primo p .

4.3 PROPOSICION: Sea n un entero $n > 1$ y p un primo tal que $p \nmid n-1$. Si $n-1 = q_1 \cdot q_2 \cdots q_r$ es la factorización de $n-1$ en primos (no necesariamente distintos) y si para cada q_i se da que $n-1 < P^{\frac{O_{q_i}(\bar{p})}{2}} + 1$ entonces n es admisible para p .

En efecto, si d es un divisor positivo de $n-1$ con $Od(\bar{p}) > 1$, como por definición $Od(\bar{p})$ es igual al orden de $\bar{p}$ en el grupo $u(d)$ entonces $p^{Od(\bar{p})} \equiv 1 \mod(d)$ y $d \mid p^{Od(\bar{p})} - 1$. Si q_i es un divisor de d se tiene que $q_i \mid p^{Od(\bar{p})} - 1$ y por lo tanto en el grupo $u(q_i)$ se da que $\bar{p}^{Od(\bar{p})} = \bar{1}$ y en consecuencia el orden de $\bar{p}$ en $u(q_i)$ divide a $Od(\bar{p})$; teniéndose que $O_{q_i}(\bar{p}) \leq Od(\bar{p})$ para cada divisor d de $n-1$. Obviamente $(n-1, p^{Od(\bar{p})} - 1) \leq n-1$ y como $p^{\frac{O_{q_i}(\bar{p})}{2}} + 1 \leq p^{\frac{Od(\bar{p})}{2}} + 1$ se tiene que:

$$(n-1, p^{Od(\bar{p})} - 1) \leq n-1 < p^{O_{q_i}(p)/2} + 1 \leq p^{Od(\bar{p})/2} + 1$$ lo cual muestra que n es admisible para p.

4.4 Diremos que un anillo A es un **p-anillo**, p un número primo, si A es un Jp-anillo con característica p. (Ver [9] pág. 61)

4.5 PROPOSICION: Todo p-anillo es conmutativo

En efecto, veamos que p es admisible para p. Claramente $p \nmid p-1$. Si d es un divisor de $p-1$, $p \equiv 1 \mod d$ luego $Od(\bar{p}) = 1$ y no existe ningún divisor d de $p-1$ para el cual $Od(\bar{p}) > 1$ luego la

condición ii) de 4.1 se da vaciamente, y p es admisible para p, luego el teorema 4.2 nos da la conmutatividad de A ∎

En ([11]) puede verse otra prueba de la proposición 4.5 .

4.6 Estudiaremos a continuación Jn-anillos con n un entero par. En estos Jn-anillos la característica es igual a 2 ya que si $n = 2k$, $k \in \mathbb{Z}$ $k \geqslant 1$ se tiene que

$$(-a) = (-a)^n = [\,(-a)(-a)\,]^k = [\,a.a\,]^k = a^n = a \quad \text{luego}$$

$-a = a$ y por lo tanto $2a = 0$ para todo a en el anillo. Veremos ahora cuando un entero $n > 1$ es admisible para 2.

4.7 Un entero $k \in u(d)$ se llama una raíz primitiva de d si k es un generador del grupo $u(d)$ ([1] pág. 256) en otras palabras, si $Od(k) = \varphi(d)$.

4.8 PROPOSICION: Sea A un Jn-anillo donde $n = q + 1$ con $q > 5$ un número primo. Si q es un primo para el cual 2 es una raíz primitiva, se tiene que A es conmutativo.

Veamos que n es admisible para 2 . Obviamente $2 \nmid n-1$. Como $n-1 = q$ por la proposición 4.3 basta ver que $q < 2^{O_q(\bar{2})/2} + 1$ (1). Como 2 es raíz primitiva de q se tiene que $O_q(\bar{2}) = q-1$ y (1) se

transforma en $q < 2^{\frac{q-1}{2}} + 1$. La desigualdad $m < 2^{\frac{m-1}{2}} + 1$ es válida para todo entero $m \geqslant 6$. En efecto, $1 + 2^m \geqslant m^2$ para todo entero positivo m , y claramente $1 + 2^{\frac{m-1}{2}} \geqslant \left(\frac{(m-1)}{2}\right)^2 = \frac{(m-1)^2}{4}$ para todo $m \geqslant 3$. Ahora, $\frac{(m-1)^2}{4} > m$ si $m \geqslant 6$, ésto ya que

$\frac{(m-1)^2}{4} - m = \frac{m^2 - 6m + 1}{4}$ y $m^2 - 6m + 1 > 0$ si $m \geqslant 6$ lo cual puede observarse de la gráfica de la ecuación cuadrática $x^2 - 6x + 1$.

Como por hipótesis $q > 5$ se tiene que $q < 2^{\frac{q-1}{2}} + 1$ y n es admisible para 2 ⁞⁞

4.9 En [1] pág. 266 puede encontrarse una lista de números primos para los cuales 2 es una raíz primitiva. Ejemplos de estos primos son: 11, 13, 19, 29, 37, 53, 59, 61, 83, 97, 101. Así, por ejemplo anillos en donde para todos sus elementos x se da que $x^{102} = x$ son necesariamente anillos conmutativos.

4.10 OBSERVACION: Nótese que en la demostración de 4.8 para mostrar que A era un anillo conmutativo, bastaba ver que se satisfacía la desigualdad: $q < 2^{O_q(\bar{2})/2} + 1$.

Esta desigualdad puede verificarse aun en el caso en que 2 no sea una

raíz primitiva de q , por ejemplo para $q = 71$, $O_{71}(\bar{2}) = 35$ y $71 < 2^{35/2} + 1$.

El teorema 4.2 y la proposición 4.3 pueden usarse para demostrar que para ciertos primos q y Jn-anillos en donde $n = q^2 + 1$ se tiene también la conmutatividad. Por ejemplo, para $q = 19$ $2 \nmid n-1$ y $O_{19}(\bar{2}) = 18$ luego $n-1 = 19^2 < 2^{\frac{18}{2}} + 1 = 513$ luego un anillo para el cual $x^{19^2+1} = x$ es conmutativo.

4.11 Estudiaremos a continuación Jn-anillos, donde n es impar. En el teorema 4.2 se probó que si A es un Jn-anillo con característica prima p y n era admisible para p , entonces A era conmutativo. Nuestro paso siguiente será mostrar que todo Jn-anillo A tiene característica finita (Cuando n era par, se vió que 2 era la característica) y que además, A se puede escribir como una suma de Jn-anillos con característica prima.

4.12 PROPOSICION: Si A es un Jn-anillo, A tiene característica finita. Además si c es la característica de A , no existe ningún primo q tal que $q^2 | c$.

En efecto, si $k \in \mathbb{Z}$ y $a \in A$ se tiene que $(ka)^n = ka$ de donde $(k^n - k).a = 0$; lo cual muestra que existe al menos un entero que anula

todos los elementos de A. Sea c el mínimo entero positivo tal que $c.a = 0$ para todo $a \in A$. Si m es cualquier otro entero tal que $m.a = 0$ para todo $a \in A$, se tiene que $c|m$ ya que si c no dividiera a m, existirían enteros s_1, s_2, $0 < s_2 < c$ tales que $m = c.s_1 + s_2$ de donde $s_2.a = (m - cs_1).a = 0$ para todo $a \in A$, lo cual estaría en contradicción con la minimalidad de c.

Sea q un primo y veamos que $q^2 \nmid c$. Si este no fuera el caso, como $(q^n - q).a = 0$, para todo $a \in A$, por lo arriba discutido se tendría que $c \mid q(q^{n-1} - 1)$ y como $q^2 \mid c$ se tiene que $q^2 \mid q.(q^{n-1} - 1)$ de donde $q \mid q^{n-1} - 1$ lo cual es absurdo ⁞⁞

Si c es la característica de A la proposición anterior nos muestra que c se puede escribir como $c = q_1 \dots q_r$ donde los q_i son primos distintos dos a dos.

4.13 PROPOSICION: Sea A un Jn-anillo con característica $c = q_1 \dots q_r$ donde los q_i son números primos distintos dos a dos. Entonces, existen Jn-anillos A_i, $1 \leqslant i \leqslant r$, con característica prima q_i, tal que A es isomorfo a la suma directa de los anillos A_i.

En efecto, como se puede ver en ([10] , teorema 29) A se puede

escribir como suma directa de anillos $A_1, A_2, \ldots A_r$ con característica $q_1, q_2, \ldots q_r$ respectivamente, y claramente si se tiene que $A \cong A_1 \oplus \ldots \oplus A_r$, cada uno de los anillos A_i debe ser un Jn-anillo ∎

Como corolario inmediato de 4.13 y 4.2 se tiene que si n es admisible para todos los q_i $i = 1, \ldots r$ entonces A es conmutativo.

Las dos siguientes proposiciones fueron tomadas de ([2] pág. 270) y nos muestran en un Jn-anillo con característica p como se relacionan los enteros n y p.

4.14 PROPOSICION: Si A es un Jn-anillo con característica prima p; Entonces $p-1 \mid n-1$.

En efecto, sea t una raíz primitiva de p. Como se vió en la prueba de la proposición 4.12 se tiene que $p \mid t(t^{n-1} - 1)$ pero como p y t son primos entre si se tiene que $p \mid t^{n-1} - 1$, luego $t^{n-1} \equiv 1 \bmod p$. Como t es raíz primitiva de p, el orden de t en el grupo $u(p)$, de los enteros modulo p, es $p-1$ y como $t^{n-1} = 1$ en $u(p)$ se sigue que $p-1 \mid n-1$ ∎

En la proposición siguiente diremos que A es un Jn-anillo con n minimal,

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL

si la relación $a^n = a$ $(n > 1)$ se da para todo $a \in A$ y n es el mínimo exponente con esta propiedad.

4.15 PROPOSICION: Sea A un Jn-anillo con n minimal y con característica prima p. Entonces $n-1$ no es divisible por p.

En efecto, si suponemos que $p \mid n-1$, existiría un $m \in \mathbb{Z}$ tal que $n-1 = p.m$. Si $a \in A$ se tiene que $(a^{n-1})^p = a^{n-1} = (a^m)^p$ y por lo tanto $(a^{n-1} - a^m)^p = a^{n-1} - a^{n-1} = 0$. Si hacemos $b = a^{n-1} - a^m$, se tiene que $b = b^n = b^{n-1}.b = b^{m.p}.b = 0.b = 0$; es decir, $a^{n-1} = a^m$ y en consecuencia $a^n = a^{m+1} = a$ pero $m+1 < n$ lo cual está en contradicción con el hecho de que n es minimal.

Las proposiciones 4.12, 4.13, 4.14 y 4.15 permiten aplicar el teorema 4.2 a Jn-anillos con n un entero impar, como se muestra a continuación.

4.16 EJEMPLO: Si A es un J_7-anillo con 7 minimal, A es conmutativo.

De acuerdo a la proposición 4.13 basta considerar el caso en que A tiene característica prima. Sea p la característica de A. De acuerdo a 4.14 y 4.15 $p-1 \mid 6$ y $p \nmid 6$ lo cual obliga a que $p = 7$ de donde A resulta ser un 7-anillo el cual es conmutativo como se vió en 4.5. $\square$

4.17 EJEMPLO: Si A es un J_{15}-anillo , con 15 minimal, A es conmutativo

De acuerdo a 4.13 basta considerar el caso en que la característica de A es prima. Si p es la característica de A , $p-1 \mid 14$ luego $p = 2$ ó $p = 3$. Como $p \nmid 14$ se tiene necesariamente que $p = 3$. Veamos ahora que 15 es admisible para 3 . Como $n = 15$, se tiene que $3 \nmid n-1 = 14$ dándose la condición i) de 4.1 . Los divisores de 14 son 1,2,7,14 para los cuales se tiene que:

$O_1(\bar{3}) = 1$, $O_2(\bar{3}) = 1$, $O_7(\bar{3}) = 6$, $O_{14}(\bar{3}) = 6$, además :

$$(14, 3^6 - 1) = 14 < 3^{6/2} + 1 = 3^3 + 1 = 28$$

Lo cual nos muestra que se satisface ii) de la definición 4.1 y por lo tanto 15 es admisible para 3 . El teorema 4.2 nos da la conmutatividad de A .

NOTA: Nuestro trabajo termina aquí, sin embargo creemos que los resultados podrían mejorarse investigando en las siguientes direcciones: En primer lugar, se podría continuar por la misma línea buscando criterios que permitan caracterizar todos los enteros admisible para un primo p dado.

Una segunda línea de investigación podría seguirse a partir de la siguiente propiedad del precentro de A : Si $\overline{p(x)} \in S_A$ y $q(x)$ es un elemento cualquiera de $\mathbb{Z}_{p,n}[x]$ entonces $\overline{p(q(x))} \in S_A$. Esto último se da ya que si $a \in A$, $\overline{\phi_a(p(q(x)))} = p(q(a))$ si $b = q(a)$ se tiene que

$p(b) \in C(A)$ ya que $\overline{p(x)} \in S_A$.

La propiedad anterior probablemente obligue en muchos casos a que $S_A = \mathbb{Z}_{p,n}[x]$. Nótese que la propiedad de S_A , de absorber potencias $n-1$ de elementos de $\mathbb{Z}_{p,n}[x]$, es un caso particular de la propiedad arriba mencionada, haciendo $\overline{p(x)} = \overline{x}^n$ y $\overline{q(x)}$ cualquier elemento en $\mathbb{Z}_{p,n}[x]$. En el apéndice 2 cuando se demostró que un J_6-anillo es conmutativo, se usó implícitamente la propiedad de poder substituir en un $\overline{p(x)} \in S_A$ la variable x por otro polinomio cualquiera, y obtener un nuevo elemento de S_A ; lo cual nos muestra que para este caso especial de $n = 6$, en donde lo desarrollado en este trabajo no es suficiente para garantizar la conmutatividad de un J_6-anillo (ya que 2 no es admisible para $n = 6$), la propiedad más fuerte arriba mencionada es suficiente para garantizar la conmutatividad del J_6-anillo.

BIBLIOGRAFIA

1. T.M. APOSTOL. "Introducción a la teoría analítica de números". Ed. Reverté S.A. Barcelona 1980.

2. R. AYOUB and C. AYOUB. "On the commutativity of rings". The American Mathematical Monthly. (71) 3 (1964), 267 a 271.

3. D.M. BURTON. "Anillos e Ideales". Addison-Wesley Publ. Massachusetts 1970.

4. I.N. HERSTEIN. "Topics in Algebra". Blaisdell Publ. Co., Waltham, Massachusetts, 1964.

5. I.N. HERSTEIN. "Wedderburn's theorem and a theorem of Jacobson". The American Mathematical Monthly. (68) 3 (1961), 249 a 251.

6. N. JACOBSON. "Lectures in abstract Algebra". Vol. I, Springer Verlag New York, 1964.

7. J. LUH. "On the commutativity of J-rings". Canadian Journal of Mathematics. (19) 6 (1967), 1289 a 1292.

8. J. LUH. "On the structure of J-rings". The American Mathematical Monthly. (74) 2 (1967), 164 a 166.

9. N.H. Mc COY. "The theory of rings". Chelsea Publ. Co., Bronx New York, 1970.

10. N.H. Mc COY. "Rings and Ideals". The Mathematical Association of America. (Carus Monograph) 1948.

11. A. YAQUB. "Elementary proofs of the commutativity of p-rings". The American Mathematical Monthly. (64) 4 (1957), 253 a 254.