UNIVERSIDAD DE CANTABRIA
Facultad de Ciencias
Departamento de Matemáticas,
Estadística y Computación.

Algunos aspectos de la teoría de casi-anillos de polinomios.

Memoria presentada por JAIME GUTIERREZ
para optar al grado de Doctor en Ciencias
Matemáticas.

Santander, Enero de 1988.

Esta memoria ha sido realizada en el departamento de Matemáticas, Estadística y Computación de la Universidad de Cantabria, bajo la dirección del Prof. Dr. C. Ruiz de Velasco y Bellas.

Quiero agradecer a Carlos Ruiz de Velasco y Bellas, sus orientaciones y ayudas que han hecho posible la realización de este trabajo.

INDICE

INTRODUCCION

De todos es conocido que los polinomios constituyen el núcleo del álgebra. Estos pueden ser estudiados desde distintos puntos de vista, sin duda el más tratado es el estudio del anillo de polinomios $(R[X_1,\ldots,X_n], +, .)$ con la adición y la multiplicación de polinomios.

La presente memoria trata de casi-anillos de polinomios sobre un anillo R commutativo y con unidad; es decir, estudiamos algunos aspectos de la estructura algebraica (R[X], + , o) donde " + " es la adición de polinomios y " o " es la composición o sustitución de polinomios.

El punto de referencia obligado siempre que se estudian casi-anillos o siempre que esta estructura se emplea como herramienta, es el libro de Günter Pilz " *Near-Rings* " [P], contiene un buen sumario sobre los resultados de esta materia asi como una bibliografía completa.

Los casi-anillos son una generalización de los anillos. En términos coloquiales un casi-anillo es un "" anillo (N, +, .), donde la adición " + " puede no ser conmutativa y donde sólo se exige una ley distributiva "".

Estos aparecen de forma natural; considerar el conjunto M(G) de todas las aplicaciones de un grupo G en sí mismo, (M(G), +, o) es un casi-anillo, donde " + " es la adición de aplicaciones y " o " es la composición de aplicaciones.

Historicamente, la primera etapa hacia la axiomatización de los casi-anillos fue dada por L. E. Dickson [D] en 1.905. Dickson encontró "cuerpos con una sola ley distributiva ", llamados hoy casi-cuerpos. Una veintena de años más tarde éstos fueron usados para introducir coordenadas en un plano afín " no Desarguesiano "; es decir, un plano afín que no verifique el axioma de Desargues es "equivalente" al producto cartesiano K x K donde K es un casi-cuerpo y las rectas son las combinaciones lineales con coeficientes en K . Reciprocamente: dado un casi-cuerpo K , el par $\mathcal{A}_2$= (K x K, $\mathcal{F}$) es un plano afín, (en general no desarguesiano si K no es un cuerpo), donde r ∈ $\mathcal{F}$ si y solamente si r = {(x,y) ∈ K x K / aX + by + c = 0, para algún (a, b) ≠ (0, 0) } . H. Zassenhaus [Z] fue el que caracterizó todos los casi-cuerpos finitos. En 1938 H. Wielandt [W] comenzo a estudiar los casi-anillos, obteniendo unos interesantes resultados; también en estos trabajos es la primera vez que aparece la palabra "casi-anillo". Años más tarde H. Neumann [N], en [1954, 1956] y A. Fröhlich [F1] [F2], en [1958-1962] publican una serie de articulos sobre casi-anillos estrechamente ligados con la teoria de grupos, relacionando la resolubilidad del grupo del casi-anillo y la distributividad del casi-anillo.

A. Fröhlich es el pionero en el estudio de los casi-anillos distributivamente generados, obteniendo como consecuencia unos generosos resultados en teoria de grupos. Como continuación a los trabajos de A. Fröhlich podemos destacar entre otros a J. D. P. Meldrum [M], y a uno de sus alumnos Ian Roberts [R]; usaremos resultados obtenidos por estos en el segundo capítulo. Parte de estos trabajos se encuentran en el

interesante y reciente libro de J.D.P. Meldrum, [M] " *Near-rings and their links with groups*", publicado a finales de 1.985.

Por otro lado, siempre que se trabaje con la sustitución de polinomios, el punto de referencia mas extendido es el libro de H. Lausch y W. Nöbauer "*Algebra of polynomials*" (1.973)[L-N].

Entre todos los aspectos en el estudio de polinomios, nosotros pensamos que uno de los más importantes es la conexión entre polinomio y función polinómica. De todos es conocido que dos polinomios pueden definir la misma función polinómica, (p. e. en cuerpos finitos) en este sentido los casi-anillos de polinomios parecen ser un buen contexto para este fin [P], [L-N] (por ejemplo, el conjunto de polinomios que definen la función polinómica cero es un ideal en el casi-anillo de polinomios R[X])

Por otra parte, la sustitución de polinomios fue usada para resolver ecuaciones de grado tres y cuatro, haciendo sustituciones lineales de la forma $aX+b$ o sustituciones cuadraticas de la forma aX^2+bX+c. Ecuaciones de grado mayor que cuatro son costosas de resolver incluso si el polinomio es resoluble por radicales. A menudo la tecnica más usada es encontrar los factores irreducibles del polinomio, asi las raices constituyen la unión de las raices de los factores irreducibles. Ahora bien, existen polinomios irreducibles que, sin embargo, son descomponibles en el casi-anillo de polinomios de una forma no trivial.

Por ejemplo, el polinomio f(X) con coeficientes en el cuerpo de los números racionales:

$f(X) = X^6 + 6X^4 + X^3 + 9X^2 + 3X - 5$ es irreducible .

Sin embargo

$f(X) = g(X)$ o $h(X)$, con $g(X) = X^2 + X - 5$ y $h(X) = X^3 + 3X$.

Luego para computar las raíces de f(X), primero computamos las raíces de el polinomio cuadrático g(X) , digamos a_1 , a_2 . Entonces los ceros de f(X) son los ceros de los polinomios

$h_1(X) = X^3 + 3X - a_1$ y $h_2(X) = X^3 + 3X - a_2$.

En general, supongamos que f(X)= g(X) o h(X); las raíces de f(X) son las raíces de los polinomios $h_i(X)= h(X) - a_i$ donde los a_i son los ceros del polinomio g(X).

Estas ideas, ya recogidas desde hace mucho tiempo, están teniendo en estos momentos un gran interes, como muestra el reciente artículo *"Polynomial decomposition algotithms"* publicado en " *J. Symbolic Computation*" (1.985) por David R. Barton y Richard Zippel [B-Z] en orden a obtener algoritmos que permitan descomponer un polinomio en "componentes indescomponibles". Muchos resultados relacionados con la descomposición de polinomios se pueden encontrar en el libro antes citado *"Algebra of polynomials"* de H. Lausch and W. Nöbauer [L-N] y en el interesante libro " *Selected topics on polynomials* " (1.982) de Andrzej Schinzel [S]. Parte de estos resultados serán utilizados en el apéndice de la memoria.

Pasamos ahora a describir el contenido estricto de la presente memoria.

Hemos incluido en el capítulo cero de la memoria el material introductorio de la teoría básica de casi-anillos con objeto de hacerla lo más autocontenida posible y podernos situar con comodidad en el resto de

los capitulos. Este capitulo, divido en dos párrafos, contiene la definición de casi-anillo y en él establecemos distintos conceptos y resultados que nos recuerdan a los ya conocidos de la teoria de anillos. El párrafo dos está dedicado a los conceptos y resultados clásicos sobre casi-anillos distributivamente generados. En todos los resultados y definiciones daremos las fuentes de los mismos.

El capitulo primero esta centrado en el estudio de los elementos distributivos del casi-anillo de polinomios y del casi-anillo de series de potencias formales. En el párrafo uno damos una descripción explicita de los elementos distributivos de R[X] y $R_0[X]$. Como consecuencia obtenemos que $R[X]_d$ coincide con $R_0[X]_d$. En el párrafo dos estudiamos el anillo de los elementos distributivos de R[X] obteniendo algunas caracterizaciones de este anillo. El resultado más importante de este párrafo es

$$R[X]_d=(\oplus_{p\in P} I_p[X]) \oplus RX$$

donde P es el conjunto de todos los numeros primos y los $I_p[X]$ son ideales del anillo $R[X]_d$, en particular si la caracteristica de R es un número primo p, el conjunto de los elementos distributivos de (R[X], +, o) es

$$R[X]_d = \{a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \ldots\ldots\ldots + a_1 X^{p^1} + a_0 X^{p^0} / a_i \in R, n \geq 0\}$$

Antecedentes al estudio de $R[X]_d$ no los hemos encontrado en los "casi-anilleros" sino en los trabajos acerca de la teoría de cuerpos

finitos y por lo tanto en otro contexto. Así O. Ore [O] define " polinomio aditivo " o "p-polinomio " sobre un cuerpo, como un polinomio f(X) satisfaciendo la siguiente identidad:

$$f(X + Y) = f(X) + f(Y),$$

donde X e Y son variables algebraicamente independientes. Ore demuestra que si la característica del cuerpo es cero, entonces los polinomios aditivos son todos triviales; es decir, lineales; sin embargo, si la característica del cuerpo es un primo p, entonces son todos de la forma descrita arriba.

Parte de los resultados de estos dos párrafos se encuentran en [G-R].

Cerramos este capítulo encontrando todos los elementos distributivos de los casi-anillos de series de potencias formales sobre un anillo conmutativo y con identidad, caracterizando el anillo de dichos elementos, Los resultados obtenidos en este caso son análogos al caso de polinomios. La técnica para la demostración es inversa a la de los polinomios, en el sentido de que en el caso de polinomios atacamos el problema por el grado del polinomio y en el caso de serie de potencias formales por el orden de la serie. Ambas técnicas son de tipo elemental, puesto que no presuponen un gran conocimiento de conceptos de álgebra. El casi-anillo de serie de potencias formales ha sido considerado por A. Fröhlich [F3], Cartan [C], H. Kautschitsch [K1] y W. Muller [K-M] entre otros. H. Kautschitsch en [K1] encontró todos los ideales maximales de este casi-anillo.

Parte de los resultados de este último párrafo se encuentra en [G1].

En el capítulo dos abordamos el estudio de los subanillos y anillos cocientes de un casi-anillo de polinomios. Ciertamente el parrafo uno

también hubiera podido estar ubicado en el primer capítulo pues en él investigamos qué subcasi-anillos gozan de la propiedad distributiva a ambos lados. El resultado más destacable al respecto es el siguiente :

Si R es un dominio de integridad " Todo subanillo de R[X] (no necesariamente unitario) está contenido en el anillo de los elementos distributivos. "

Como corolario del resultado anterior obtenemos que los anillos del casi-anillo $Z_{/pZ}[X]$ son los subanillos (salvo isomorfismo) del anillo de polinomios ($Z_{/pZ}[X]$, +, .)

La complejidad del problema se agudiza cuando el anillo R no es un dominio de integridad, en este caso ponemos unos ejemplos ilustrativos.

Parte de los resultados de este párrafo se encuentran en [G-R].

En el párrafo dos de este capítulo nos dedicamos al estudio de anillos cocientes de casi-anillos N; es decir, buscamos ideales I de N tales que $N_{/I}$ sea anillo. Definimos el radical-anillo (el menor ideal de N que contiene a todos los conmutadores y distribuidores), obtenemos algunas caracterizaciones de este ideal que relacionan el ideal distribuidor y el ideal conmutador, en particular en los casi-anillos distributivamente generados. Justificamos también el término " radical " del radical anillo, demostrando que define una aplicación $\mathcal{A}$ que es radical. En el párrafo tres estudiamos el radical anillo en los casi-anillos de polinomios, que obviamente coincide con el ideal distribuidor $D_1[X]$. El resultado más notable es quizás que $D_1[X]$ es un ideal principal; es decir, como en teoría de anillos, generado por un único elemento ($D_1[X] = \mathfrak{I}(1)$). También

encontramos los ideales distribuidores para una clase muy amplia de anillos R . Por último, algunas consideraciones sobre el ideal distribuidor de $R_0[X]$ nos permitirán concluir que los casi-anillos $R_0[X]$ nunca son $\mathcal{A}$-radicales. Apenás hay antecedentes de trabajos relativos al estudio del ideal distribuidor de R[X]. Sin embargo en el estudio de $\mathfrak{I}(1)$ debemos citar a J. L. Brenner , [J1] [J2] (1.974-1.985) y a J. Clay y D.Doi (1.973). Estos últimos encuentran $\mathfrak{I}(1)$ para todos los F[X] donde F es un cuerpo de cardinal mayor que dos, y J. L. Brenner lo hace para Z[X] y $Z_{/2Z}[X]$. En particular, $\mathfrak{I}(1)$ en $Z_{/2Z}[X]$ es fundamental para una parte amplia de los resultados obtenidos en el párrafo tres. J. L. Brenner en su articulo "*Algebras of polynomials* " (1.985) sugiere algunas técnicas de demostración para atacar el problema de encontrar $\mathfrak{I}(1)$ para algunos anillos R muy particulares.

Parte de los resultados de los párrafos 2 y 3 se encuentran en [G 2].

El capitulo tres se aparta del contenido de los otros dos capitulos, sin embargo los tópicos que tratamos son muy extendidos y han sido abordados por varios especialistas. En este capitulo estudiamos los ideales de Z[X] y $Z_{/nZ}[X]$ y de los ideales del anillo de composición (R[X], +, .,o).

En el libro " *Near- rings*" de Günter Pilz, en la pagina 228, dice " *All maximal ideals or all full ideals of Z[X] are not Known* "

J. L. Brenner en su articulo " *Algebras of polynomials*" (1.985) dice encontrar todos los ideales de Z[X]. En el párrafo uno investigamos los ideales de Z[X], en particular damos una descripción completa de los

ideales maximales. Apareciendo ideales no mencionados por Brenner.

Aplicando los teoremas de isomorfía obtenemos como consecuencia los ideales maximales de $Z_{/nZ}[X]$ para todo n . Esto contituye el párrafo dos.

Al principio de la introdución comentábamos que el estudio de los polinomios es la mayor parte el del anillo (R[X], +, .), sin enbargo parece interesante estudiar la estructura con las tres operaciones , obteniendo así (R[X], +, . , o) que en términos algebraicos es conocida como un anillo de composición. En el párrafo tres destacamos los ideales del casi-anillo R[X] que son ideales del anilo de polinomios R[X], conocidos en la literarura como ideales completos (full) o ideales de composición (puesto que son los ideales del anillo de composición (R[X], +, . , o)). En este párrafo encontramos todos los ideales completos maximales de R[X] que estan estrechamente ligados a los ideales maximales del anillo R. Obtenemos de esta forma el radical de Jacobson del anillo de composición. Antecedentes a estos tópicos les encontramos en J. Clay y K. Doi [C-D] , Lausch y Nöbauer [L-N].

En particular H. Kautschitsch [K2] en " *Maximal ideals in the near-rings of polynomials* " (1.985) en un resultado obtiene todos los ideales maximales para una clase muy amplia de anillos, en particular todos los cuerpos de cardinal mayor que 2 y todos los anillos de característica un número positivo impar .

Acaba la memoria con un interesante algoritmo para la descomposicion de polinomios.

En el apéndice hemos considerado el siguiente problema : Dado un polinomio $f(X) \in F[X]$, F un cuerpo, encontrar una descomposición completa de f(X) de la forma :

$f(X) = g_1(X) \circ g_2(X) \circ \ldots\ldots \circ g_n(X)$ donde los $g_i(X)$ son polinomios indescomponibles.

Los únicos algoritmos que se conocen al respecto son debidos a David R. Barton y Richard Zippel [B-Z] (1.985). En estos dos algoritmos en alguna etapa necesitan de la factorización de un polinomio, en uno de los algoritmos de todos los factores irreducibles de un polinomio en dos variables y en el otro de todos los factores irreducibles de un polinomio en una única variable. Barton y Richard Zippel comentan que los algoritmos gastan el mayor tiempo en la etapa de la factorización. En este apéndice presentamos un algoritmo para determinar una descomposición completa de un polinomio f(X), con técnicas elementales que no hace uso de la factorización de polinomios. La complejidad de este algoritmo que presentamos, parece ser bastante menor que los debidos a David R. Barton y Richard Zippel [B-Z] fundamental porque en este, no hacemos uso de la factorización de polinomios. Obtenemos también algunas aplicaciones al calculo de los factores irreducibles de un polinomio .

CAPITULO 0. CASI-ANILLOS

En este capitulo introducimos parte de la teoria básica de casi-anillos ya que, aunque puede ser conocida, servirá para situar mejor el contenido del resto de los capitulos. En el párrafo 1, además de introducir - como es obvio- la definición de casi-anillo, establecemos distintos conceptos y resultados que nos recuerdan a los ya conocidos de la teoria de anillos. El párrafo 2 está dedicado al estudio de los casi-anillos distributivamente generados.

§ 1. CASI-ANILLOS.

Definición 1.1 [P]

Un conjunto N junto con dos operaciones binarias " + " y " . " es un casi-anillo si :

(a) (N, +) es un grupo (no necesariamente abeliano)

(b) (N , .) es un semigrupo.

(c) Para todo $n_1, n_2, n_3 \in N$: $(n_1 + n_2) n_3 = n_1 n_3 + n_2 n_3$ (propiedad distributiva a la derecha).

Nota 1.2.

Puesto que en la definición anterior se hace uso de la distributividad a la derecha , parecería más preciso hablar de " casi-anillos a la derecha" los que verifiquen (c) y de " casi-anillos a la izquierda " aquellos que verifiquen (c´) en lugar de (c), donde :

(c') Para todo $n_1, n_2, n_3 \in N$: $n_1(n_2 + n_3) = n_1 n_2 + n_1 n_3$.

Ambos conceptos desarrollan teorías paralelas.

Como dice G. Pilz en su libro " Near-rings " [P] " *The "religious war", if right or left near-rings are "better", is still unsettled* ". Sin embargo podríamos decir, a la vista de una bibliografía básica que dicha " religious war " podría terminar en un amigable empate, ya que por ejemplo, mientras G. Pilz en el libro antes citado utiliza casi-anillos a la derecha, J.D.P. Meldrum [M] en su libro " Near- rings and their links with groups " usa casi-anillos a la izquierda . No obstante en la teoría de casi-anillos de polinomios se trabaja siempre con " casi-anillos a la derecha " , es decir con casi-anillos.

A lo largo de este capítulo N = (N, +, .) denotará un casi-anillo. El elemento neutro de (N, +) será denotado por 0.

Ejemplos 1.3.

(a) Todo anillo es un casi-anillo.

(b) Sea (G, +) un grupo escrito aditivamente (no necesariamente abeliano). El conjunto de todas las aplicaciones de G en G, con la " suma " y la " composición " de aplicaciones, es un casi-anillo.

Si M(G): = { f : G → G }, el casi-anillo (M(G), +, o) será denotado por M(G). (ver [M], [P])

(c) (Casi-anillos de polinomios) [L-N], [P].

Los polinomios pueden ser definidos sobre cualquier estrucutura algebraica A en un conjunto X ($A \cap X = \emptyset$) de " indeterminadas " en una variedad $\boldsymbol{v}$ conteniendo A . Denotamos a este conjunto por A(X, $\boldsymbol{v}$).

Rudamente hablando, A(X, $\boldsymbol{v}$) es el " conjunto de todas las palabras

en $A \cup X$, donde la igualdad esta definida de acuerdo con las leyes que definen $\boldsymbol{\nu}$. Otra caracterización de $A(X, \boldsymbol{\nu})$ es la siguiente : $A(X, \boldsymbol{\nu})$ es la unión libre del algebra A y del algebra libre $F(X,\boldsymbol{\nu})$, sobre X en $\boldsymbol{\nu}$.

En el caso de algunas variedades $\boldsymbol{\nu}$, los elementos de A(X,V) se escriben de una forma mas conocida. (por ejemplo para el caso de anillos conmutativos y con identidad y para grupos).

Sin embargo aqui nos restringiremos al caso de una única " variable " $X = (X)$ y a la variedad $\mathfrak{R}$, de todos los anillos conmutativos y con identidad.

Sea R un anillo conmutativo y con identidad 1. El conjunto R[X] de todos los polinomios con coeficientes en R, es un casi-anillo con las operaciones :

" + " suma usual de polinomios y

" o " sustitución de polinomios (f(X) o g(X) = f(g(X)), - sustituir el polinomio g(X) en la variable X del polinomio f(X) -). (ver [La-N])

Definición. 1.4.[P]

Un subconjunto M de N es un subcasi-anillo si :

(M, +) es un grupo y (M, .) es un subsemigrupo.

Proposición 1.5.

En un casi-anillo N se tiene

$$0n = 0 \text{ y } (- n) n' = - (n n'), \text{ para todo } n, n' \in N .$$

Demostración

Se demuestra igual que en anillos. (ver [M], [P]). ◆.

En general no tenemos que $n0 = 0$ o que $n(-n') = -(nn')$, por lo tanto tiene sentido la siguiente definición.

Definición 1.6.[P]

(a) $N_0 := \{ n \in N / n0 = 0 \}$ es llamada la parte cero-simétrica de N.

(b) $N_c := \{ n \in N / n0 = n \}$ es llamada la parte constante de N.

Es inmediato comprobar que N_0 y N_c son subcasi-anillos de N y que N es suma directa de N_0 y N_c.

Definiciones 1.7.[P]

En los casi-anillos se definen identidades (derecha, izquierda), elementos inversibles (izquierda , derecha), elementos cancelables (derecha , izquierda) y divisores de cero de forma similar a como se definen en teoría de anillos.

Definiciónes 1.8.[P]

Sea N un casi-anillo.

Si (N, +) es un grupo abeliano, diremos que N es un casi-anillo abeliano.

Si (N, .) es un semigrupo conmutativo, diremos que N es un casi-anillo conmutativo.

Si (N, .) tiene identidad, diremos que N es un casi-anillo unitario.

Si $N = N_0$ diremos que N es un casi-anillo cero-simétrico.

Si N no tiene divisores de cero diremos que N es un casi-anillo íntegro.

Si (N^*: = N - { 0 }, .) es un grupo, diremos que N es un casi-cuerpo.

Definición 1.9.[P],[M]

Sean N, N' dos casi-anillos,

Una aplicación $f : N \to N'$ es un homomorfismo de casi-anillos si :

$f(m + n) = f(m) + f(n)$ y $f(mn) = f(m)f(n)$, para todo $m,n \in N$.

Los conceptos : isomorfismo, monomorfismo y epimorfismo de casi-anillos se definen de forma análoga a como se definen en álgebra universal.

Es conocido que para todo anillo A existe un grupo abeliano G y un monomorfismo $i : A \to End(G)$, es decir A es un subanillo de End(G) para algún grupo abeliano G. Se demuestra un resultado paralelo en teoría de casi-anillos : para todo casi-anillo N existe un grupo G y un monomorfismo $i : N \to M(G)$, es decir N es un subcasi-anillo de M(G) para algún grupo G.

J. Meldrum, G. Pilz y Yong So, [M-P-S] en " *Embeding near-rings into polynomial near-rings*" demuestran que para cada casi-anillo N existe una variedad $\boldsymbol{\nu}$ de Ω- Grupos y un $G \in \boldsymbol{\nu}$ tal que N se sumerge en G[X].

Definición 1.10.[P]

Un subgrupo normal I de (N, +) es un ideal de N , si verifica :

(a) IN esta contenido en I.

(b) Para todo n, $m \in N$ y para todo $i \in I$: $n(m + i) - nm \in I$.

Un subgrupo normal J de (N, +) diremos que es un ideal a la derecha de N si verifica (a).

Un subgrupo normal L de (N, +) diremos que es un ideal a la izquierda de N si verifica (b).

Nota 1.11.

Un subgrupo normal I de (N, +) es un ideal si y sólo si el conjunto cociente $N_{/I}$ puede dotarse de estructura de casi-anillo con las operaciones inducidas por las de N.

$N_{/I} = \{ i + N;\ i \in I \}$

$(i_1 + N) + (i_2 + N) = (i_1 + i_2) + N$

$(i_1 + N) (i_2 + N) = (i_1 i_2) + N$

para todo $i_1 , i_2 \in N$.

Claramente el { 0 } y N son ideales de N , llamados los ideales triviales de N.

Teorema 1.12.[P] [M] (Teorema del homomorfismo)

(a) Si I es un ideal de N entonces la aplicación canónica

$f: N \rightarrow N_{/I}$ es un epimomorfismo de casi-anillos.

(b) Reciprocamente, si N, N' son casi-anillos y $h : N \rightarrow N'$ es un epimorfismo, entonces Ker(h) es un ideal de N y $N_{/Ker(h)} \equiv N'$.

Demostración.

[P], [M] la demostración es análoga al caso de grupos o anillos. ♦.

Nota 1.13.

Como es usual en algebra, un ideal es el núcleo de un homorfismo. Esta definición aparece por primera vez en un articulo de G. Birkhoff en 1.934 de titulo " On the combination of subalgebras " publicado en " Proceedings of the Cambridge Philosophical Society ".

Teorema 1.14 [P] [M](Segundo teorema de isomorfia)

Sea h un epimorfismo de un casi-anillo N a un casi-anillo N´ . Entonces hay una correspondencia 1-1 entre los subcasi-anillos (resp. ideales a la izquierda, derecha, ideales) de N conteniendo Ker(h) y los subcasi -anillos (resp. ideales a la izquierda, derecha, ideales) de N´. Esta correspondencia preserva y refleja las inclusiones y está definida por :

A (contenido en N) → h(A).

Además para todo ideal I de N conteniendo Ker(h) se tiene que :

$$N_{/I} \equiv h(N)_{/h(I)}.$$

Si $f : N \to N_{/I}$ es el epimorfismo canónico, se tiene que para todo ideale J de N conteniendo I,

$$(N_{/I}) / (J_{/I}) \equiv N_{/I}.$$

Demostración

[P], [M]. ♦.

Es necesario recordar algunos conceptos del Algebra Universal relativos a " objetos generados ", para poder hablar de ciertos subconjuntos notables de N generados por una familia de partes de N.

Definición 1.15.[Gr],[P]

Sea A un conjunto .

Un subconjunto ϑ de $2^A = \{ f: A \to \{0,1\} \}$ se dice que es un sistema de Moore (Dubreil- Dubreil- Jacotin) en A si:

(a) $A \in \vartheta$.

(b) ϑ es cerrado con respecto a intersecciones.

Proposición 1.16.[Gr],[P]

Sea A un conjunto

Si ϑ es un sistema de Moore en A y B un subconjunto de A, entonces $[B]_{\vartheta} := \bigcap\{M / M \in \vartheta$ y B contenido en M $\}$ es el menor elemento de ϑ (con respecto a la inclusión) que contiene a B.

Demostración

[Gr], [P]. ◆.

Definición 1.17.[Gr],[P]

(a) El elemento $[B]_{\vartheta}$ de ϑ de la proposición anterior se dice que está generado por B.

(b) Sea $T \in \vartheta$. Se dice que T está finitamente generado si existe un subconjunto finito B de T tal que $T = [B]_{\vartheta}$.

Definición 1.18.[Gr],[P]

Un sistema de Moore ϑ se dice que es inductivo si ϑ contiene la unión de cada cadena de elementos de ϑ.

Retornando a casi-anillos tenemos la siguiente proposición que nos permitirá hablar del ideal generado por un subconjunto.

Proposición 1.19.[P]

El conjunto de todos los ideales (resp. ideales a la derecha, ideales a la izquierda) forma un sistema de Moore inductivo en N.

Demostración.

[P]. ♦.

Notación 1.20.

A lo largo de toda la memoria denotaremos por $\mathfrak{I}(S)$ el menor ideal de N que contiene a S, donde S es cualquier subconjunto de N, es decir

$\mathfrak{I}(S) = \bigcap \{ I \ / \ I$ es un ideal de N y S contenido en I $\}$.

Definición. 1.21.[Gr],[P]

Un ideal maximal de N es un ideal que es maximal en el conjunto de ideales de N distintos de N. Similarmente se define ideal a la derecha maximal e ideal a la izquierda maximal.

Dualmente se definen los conceptos minimales.

Teorema 1.22.

Si N es finitamente generado (ver 1.17) como ideal , cada ideal (ideal a la derecha) distinto de N está contenido en un ideal maximal.

Nótese que todo casi-anillo unitario es, evidentemente, finitamente generado como ideal.

Demostración

[P]. ♦.

Teorema 1.23.

Sea $(I_k)_{k\in \mathcal{K}}$ una familia de ideales de N, entonces los siguientes subconjuntos de N coinciden :

(i) El conjunto de todas las sumas finitas de elementos de los I_k's.

(ii) El subgrupo de (N, +) generado por $\bigcup (I_k / k\in \mathcal{K})$.

(iii) El ideal de N generado por $\bigcup (I_k / k\in \mathcal{K})$.

Demostración

[P]. ♦.

Definición. 1.24[P]

1.24-1. El conjunto del teorema anterior es llamado la suma de ideales $I_k (k\in \mathcal{K})$ y denotada por $\Sigma I_k (k\in \mathcal{K})$.

1.24-2. Se dice que la suma de ideales $\Sigma I_k (k\in \mathcal{K})$ es una suna directa si cada elemento de $\Sigma I_k (k\in \mathcal{K})$ tiene una única representación como suma finita de elementos de diferentes I_k's.

§ 2. CASI-ANILLOS DISTRIBUTIVAMENTE GENERADOS.

Hay dos axiomas que se verifican en anillos pero no necesariamente en casi-anillos. Son la conmutatividad de la suma y la segunda ley distributiva. Estos dos axiomas no son completamente independientes, como hemos observado. En casi-anillos distributivamente generados esta relación se agudiza.

Los casi-anillos distributivamente generados son los que más se parecen a los anillos. Su estudio comienza en 1.958 y es realizado por A. Fröhlich [F1],[F2]. Estos trabajos son realmente el comienzo de la teoría de casi-anillos distributivamente generados.

Definición 2.1.

Diremos que $d \in N$ es un elemento distributivo si :

$d(n + n') = dn + dn'$, para todo $n, n' \in N$.

El conjunto de los elementos distributivos será denotado por N_d, es decir

$N_d := \{ d \in N / \ d(n + n') = dn + dn' \text{ , para todo } n, n' \in N \}$.

Se dice que un casi-anillo N es distributivo si $N_d = N$.

Nota 2.2.

La definición de elemento distributivo describe una relación entre un elemento y el casi-anillo al cual pertenece. Un elemento puede ser distributivo en un subcasi-anillo pero sin embargo no ser distributivo en el casi-anillo total. Incluso se podría definir de forma obvia elemento distributivo en un subconjunto de N.(ejemplos de estos les veremos en los Cap. I y II).

Ejemplos 2.3.

(a) En un anillo R todos los elementos son distributivos.

(b) Dado un grupo (G, +), los endomorfismos de G , que denotaremos por End(G) , son precisamente los elementos distributivos de M(G), es decir $M(G)_d = End(G)$.

Además también se tiene $(M(G)_0)_d = End(G)$.

(c) Los elementos distributivos de R[X] y $R[X]_0$ son parte de los objetivos del Capítulo I, párrafos 1 y 2.

Lema 2.4.

Sea N un casi-anillo. Se tiene :

(i) (N_d, .) es un subsemigrupo de (N, .)

(ii) $0t = 0$ y $(-n)t = -(nt)$, para todo $t \in N_d$ y todo $n \in N$.

Demostración

[M]. ♦.

Definición 2.5. [M], [F 1] y [P]

Se dice que un casi-anillo N es distributivamente generado, generalmente abreviado por d.g., si el grupo (N, +) está generado por un subsemigrupo (S , .) de N_d.

Algunos autores llaman casi-anillo distributivamente generado a los casi-anillos generados , como casi-anillos, por un subsemigrupo (S, .) de N_d. Se demuestra que estas dos definiciones coinciden.

Los casi-anillos distributivamente generados son cero-simétricos. (ver [M], [F I] y [P]).

Ejemplos 2.6.

(a) Los anillos son obviamente casos especiales de casi-anillos distributivamente generados.

(b) Sea (G, +) un grupo y sea S un subsemigrupo de End(G), entonces S es un subsemigrupo de elementos distributivos del casi-anillo M(G). De esta forma surgen tres casi-anillos d.g. de especial interes :

(i) S = End(G), el grupo generado por todos los endomorfismos denotado por E(G).

(ii) S = Aut(G), el grupo generado por todos los automorfismos de G, denotado por A(G).

(iii) S = Inn(G), el grupo generado por todos los automorfismos internos de G, denotado por I(G). [M], [P].

Definiciónes 2.7.[M]

2.7-1. Se definen los conmutadores del grupo (N, +) como es usual en teoria de grupos, inductivamente :

$$(a, b) = a + b - a - b$$

$$(a,\ldots\ldots,d,e) = ((a,\ldots\ldots,d), e), \text{ para todos } a,b,\ldots\ldots, d,e \in N.$$

2.7-2. Si A y B son subconjuntos de N, definimos

$$(A, B) = Gp\langle (a, b) / a \in A \text{ y } b \in B \rangle,$$

es decir, (A, B) es el grupo generado por los conmutadores (a, b) con $a \in A$ y $b \in B$.

2.7-3. La serie derivada de N, se define inductivamente por :

$$\delta_0(N) := N \quad \delta_{i+1}(N) := (\delta_i(N), \delta_i(N)), \quad i = 0, 1,\ldots\ldots$$

2.7-4. $\mathfrak{I}(\delta_1(N))$ es el ideal conmutador de N.

Proposición 2.8. [M]

Si N es un casi-anillo distributivamente generado se tiene :

$\delta_i(N)$ es un ideal de N, para todo i.

Demostración

[M], [F1] [R]. ♦.

Hemos definido ciertos conceptos relacionados con la conmutatividad de la suma . Introducimos a continuación distintas nociones conectadas con la distributividad.

Definiciónes 2.9. [M] [R] [F1]

2.9-1. Sea N un casi-anillo y sean a, b, x ∈ N. Definimos el distribuidor de x con respecto a a y b por :

$|x; a, b| = x(a + b) - (xa + xb)$.

2.9-2. Si A, B , X son subconjuntos de R, definimos

$|X; A, B| = Gp\langle x(a + b) - (xa + xb) / a \in A, b \in B, x \in X \rangle$,

es decir, $|X; A, B|$ es el grupo generado por todos lo distibuidores

$x(a + b) - (xa + xb) / a \in A, b \in B, x \in X$.

2.9-3. La serie distribuidora se define inductivamente :

$D_0(N) := N$, $D_{i+1}(N) = Gp\langle N; D_i(N), D_i(N) \rangle^N$,

es decir, $D_{i+1}(N)$ es el grupo normal de N generado por $|N; D_i(N), D_i(N)|$.

2.9-4. $\mathfrak{I}(D_1(N))$ es el ideal distribuidor de N.

Nota 2.10.

Notar que un casi-anillo N es distributivo si y sólo si $\mathfrak{I}(D_1(N)) = (0)$.

Similar resultado al 2.8 para el caso de la serie derivada en casi-anillos d.g. lo tenemos en la serie distribuidora.

Lema 2.11.

Si N es un casi-anillo distributivamente generado entonces :

$D_i(N)$ es un ideal de N, para todo i .

Demostración

[M], [R], [F1] . ◆.

Para establecer la relación entre la serie distribuidora y la serie derivada en los casi-anillos d.g resta por introducir la siguiente notación :

Definiciónes. 2.12. [M], [R]

2.12-1. Sean A, B dos subconjuntos de N, definimos :

$$AB = Gp < ab \ / \ a \in A, b \in B >.$$

2.12-2. Denotamos por $N^{[m]}$ el subgrupo normal de (N, +) definido inductivamente como sigue :

$$N^{[1]} := N, \quad N^{[i+1]} := Gp < N^{[i]}N >^{N}.$$

Enunciamos ahora los resulatdos más importantes que ligan a los conmutadores y distribuidores en casi-anilos d.g.

Teorema 2.13.

Sea N un casi-anillo distributivamente generado. Entonces para todo entero $n > 1$, tenemos :

$D_n(N)$ está contenido en $N^n \cap \delta_n(N)$,

y para todos los enteros $n \geq 1$, $m \geq 0$, tenemos :

$D_{n+m}(N)$ está contenido en $\delta_{m+1}(N^n)$.

Demostración

[M], [F1] y [R] . ♦.

Acabamos este párrafo con un interesante resultado:

Teorema 2.14.

Sea N un casi-anillo distributivamente generado con $N^2 = N$, entonces

$D_n(N) = \delta_n(N)$, para todo $n \geq 0$.

Demostración

[M] ,[F1] y [R]. ♦♦.

CAPITULO I. LOS ELEMENTOS DISTRIBUTIVOS EN LOS CASI-ANILLOS DE POLINOMIOS Y EN LOS CASI-ANILLOS DE SERIES DE POTENCIAS FORMALES.

En este capítulo describimos los elementos distributivos del casi-anillo de polinomios. Estudiamos algunas propiedades del anillo formado por estos elementos distributivos obteniendo algunas caracterizaciones de este anillo. Por último en el parrafo 3, obtenemos resultados similares en el casi-anillo de series de potencias formales.

A lo largo de toda la memoria, R denotará un anillo conmutativo y con identidad 1, y $R[X] = (R[X], +, o)$ denotará el casi-anillo de polinomios con coeficientes en R.

§1. ELEMENTOS DISTRIBUTIVOS EN CASI-ANILLOS DE POLINOMIOS.

Si $N = (N, +, .)$ es un casi-anillo, el conjunto de los elementos distributivos $N_d = \{ d \in N / d(r+s) = dr + ds$, para todo $r, s \in N \}$ es un subsemigrupo de (N, .) (Cap.0-2.4), pero en general N_d no es un subcasi-anillo. Por lo tanto el teorema siguiente tiene sentido.

Teorema 1.1.

Si N es un casi-anillo abeliano entonces $N_d = (N_d, +, .)$ es un anillo.

Demostración.

Basta demostrar que (N_d, +) es un subgrupo de (N,+), por (Cap.0-2.4)

Sean $d_1, d_2 \in N_d$ y a, b ∈ N , entonces : ($d_1 - d_2$)(a + b) =

= ($d_1 - d_2$)a + ($d_1 - d_2$)b = $d_1a - d_2a + d_1b - d_2b$ = (Cap.0-1.5,2.4)

= d_1(a + b) - d_2(a + b). (por hipótesis),

luego $d_1 - d_2 \in N_d$ ◆.

Proposición 1.2.

Se tiene :

(i) $R_0[X]$: = { f(X) / f(X)oO = f(0) = 0 } (es decir el conjunto de polinomios con término constante cero) es un subcasi-anillo de (R[X], +, o) y coincide con $R[X]_0$, la parte cero-simétrica de (R[X], +, o).(Cap.0-1.6)

(ii) Los subcasi-anillos ($R[X]_d$, +, o) y ($R_0[X]_d$, +, o) son anillos con identidad y $R[X]_d$ es un subanillo de $R_0[X]_d$.

(iii) ($R[X]_d$, +) y ($R_0[X]_d$, +) son R-módulos de R[X] y $R_0[X]$ respectivamente.

(iv) ($R[X]_d$, +, o) y ($R_0[X]_d$, +, o) son subanillos de (End(R[X]), +, o) y (End(R_0[X]), +, o) respectivamente; (se entiende que los endomorfismos de R[X] (resp. R_0[X]) sólo se refieren a la estructura aditiva de R[X] (resp. R_0[X]) y en donde " o " es la composición de endomorfismos).

Demostración:

(i) Es inmediata

(ii) Las dos primeras afirmaciones son consecuencias inmediatas de

1.1 y del hecho que el polinomio X es un elemento distributivo.

Para probar que $R[X]_d$ es un subanillo de $R_0[X]_d$,

sea $f(X) \in R[X]_d$, digamos $f(X) = a_nX^n + \ldots\ldots + a_1X + a_0$ entonces :

$a_0 = f(X) \circ 0 = f(X) \circ (0+0) = f(X) \circ 0 + f(X) \circ 0 =$

$= a_0+a_0$, por lo tanto $a_0 = 0$.

(iii) Sea $r \in R$ y $f(X) \in R[X]_d$, entonces $rf(X) \in R[X]_d$. En efecto, para todo $g(X)$ y $h(X) \in R[X]$; $rf(X) \circ (g(X) + h(X)) =$

$= (rX \circ f(X)) \circ (g(X) + h(X)) = rX \circ (f(X) \circ g(X) + f(X) \circ h(X)) =$

$= rf(X) \circ g(X) + rf(X) \circ h(X)$, aplicando la asociatividad.

(iv) Consideramos la aplicación $i : R[X]_d \rightarrow End(R[X])$ definida de la forma siguiente:

$i(f(X))(g(X)) = f(X) \circ g(X)$, donde $f(X) \in R[X]_d$ y $g(X) \in R[X]$;

i está bien definida y es un homomorfismo de anillos. Además $Ker(i) = [0]$; en efecto si $f(X) \in Ker(i)$ entonces $f(X) = f(X) \circ X = 0$.♦.

Consecuencia 1.3.

El conjunto $RX: = \{aX / a \in R\}$ es un subanillo de $R[X]_d$ (respectivamente de $R_0[X]_d$) isomorfo a R.

Demostración.

Como $X \in R[X]_d$ y $R[X]_d$ es R-módulo, se tiene que $R[X]_d \supseteq RX$. Claramente $aX \circ bX = abX$, y por lo tanto RX es un subanilo de $R[X]_d$. La aplicación : $i: aX \rightarrow a$, de RX en R es un isomorfismo de anillos. ♦.

El objetivo de este párrafo es encontrar los elementos distributivos de $R[X]_d$ y $R_0[X]_d$. Las demostraciones de los distintos resultados son similares para ambos casos, así que daremos una demostración bien para $R[X]_d$ o bien para $R_0[X]_d$.

Comenzamos reduciendo el problema al caso de monomios, para lo cual necesitamos el siguiente:

Lema 1.4.

Sea a un elemento no nulo de R y n un número entero $n \geq 2$.

(i) Si $aX^n \notin R_0[X]_d$ (resp. $aX^n \notin R[X]_d$), existe un entero i, $1 \leq i \leq n-1$ tal que $a\binom{n}{i} \neq 0$ y para todo $t \geq 0$: $aX^n \circ (X^t + X^{t+1}) \neq aX^n \circ X^t + aX^n \circ X^{t+1}$.

(ii) Si $aX^n \in R[X]_d$ ($aX^n \in R_0[X]_d$) entonces el orden de a (denotado por O(a)) es finito.

Demostración

(i) Si $aX^n \notin R_0[X]_d$, existen $f(X), g(X) \in R_0[X]$ tal que:

$aX^n \circ (f(X) + g(X)) \neq a(f(X))^n + a(g(X))^n$, por lo tanto para algún i, $1 \leq i \leq n-1$, luego $a\binom{n}{i} \neq 0$.

Sea j = máximo { i / $1 \leq i \leq n-1$, $a\binom{n}{i} \neq 0$ }. Entonces:

$$aX^n \circ (X^t + X^{t+1}) = a(X^t(1 + X))^n = aX^{tn}(1 + X)^n =$$

$$=aX^{tn} + anX^{tn+1} + \ldots\ldots + a\binom{n}{j}X^{tn+j} + aX^{n(t+1)},$$

con $a\binom{n}{j}X^{tn+j} \neq 0$; luego $aX^n \circ (X^t + X^{t+1}) \neq aX^{tn} + aX^{n(t+1)}$.

(ii) Si O(a) fuese infinito se tendría $aX^n \circ (X + X^2) =$

$$=aX^n + anX^{n+1} + \ldots\ldots + anX^{2n-1} + aX^{2n} \neq aX^n \circ X + aX^n \circ X^2 = aX^n + aX^{2n}$$

puesto que por hipótesis $anX^{2n-1} \neq 0$, lo que es una contradición. ♦.

La siguiente proposición es fundamental en orden a caracterizar los elementos de $R[X]_d$ y $R_0[X]_d$.

Proposición 1.5.

Dado $f(X) = a_nX^n + \ldots\ldots + a_1X \in R[X]$; entonces $f(X) \in R[X]_d$ (respec. $R_0[X]_d$) si y solamente si $a_iX^i \in R[X]_d$ para todo $i = 1, \ldots\ldots, n$.

Demostración

Supongamos $f(X) \in R[X]_d$ y $a_nX^n \notin R[X]_d$. Consideramos :

j = máximo $\{ i \ / \ 1 \leq i \leq n-1, a_n\binom{n}{i} \neq 0 \}$ (ver Lema 1.4.) y t un entero ≥ 1; entonces $f(X) \circ (X^t + X^{t+1}) = f(X^t) + f(X^{t+1}) =$

$$= a_nX^{tn} + \ldots\ldots + a_1X^t + a_nX^{(t+1)n} + \ldots\ldots + a_1X^{t+1} \equiv (*).$$

Por otro lado $f(X) \circ (X^t + X^{t+1}) = a_n(X^t + X^{t+1})^n + a_1(X^t + X^{t+1}) \equiv (**)$.

Además el primer sumando de $(**)$ es :

$$a_n(X^t + X^{t+1})^n = a_n X^{tn} + \ldots\ldots + a_n\binom{n}{j}X^{tn+j} + a_n X^{n(t+1)},$$

con $a_n\binom{n}{j}X^{tn+j} \neq 0$ y es el monomio de grado más alto (claro está, distinto del $a_n X^{n(t+1)}$) que aparece en el desarrollo de $a_n(X^t + X^{t+1})^n$.

Ahora probamos que para un entero suficientemente grande t, $a_n\binom{n}{j}X^{tn+j} \neq 0$ es el monomio de grado más alto (distinto del $a_n X^{n(t+1)}$) en el polinomio f(X) o ($X^t + X^{t+1}$).

En efecto, los monomios de f(X) o ($X^t + X^{t+1}$) son todos de la forma $a_m\binom{m}{K}X^{tm+k}$ con $0 \leq k \leq m < n$, excepto los monomios proporcionados por $a_n X^n$ (caso que ya hemos estudiado al principio). Ahora podemos elegir un entero t suficientemente grande para que $tn + j > tm + k$, puesto que j y k no dependen del t y $m < n$.

Por otro lado se debe verificar que $(**) = (*)$, contradición. Se acaba la demostración usando inducción. ♦.

Esta última proposición nos permite demostrar de una forma cómoda el siguiente resultado, cuya demostración se puede atacar directamente.

Teorema 1.6.

Si todos los elementos no nulos de R tienen orden infinito (es decir el anillo R es libre de torsión), entonces :

$$R[X]_d = R_0[X]_d = RX.$$

Demostración

Es una consecuencia de 1.3 , 1.4.ii y 1.5. ♦.

Probamos ahora una serie de lemas preliminares para dar una descripción explícita de los elementos de $R[X]_d$ y $R_0[X]_d$ en los casos que restan.

Comenzamos enunciando un resultado conocido de la teoría elemental de números.

Lema 1.7.

Sean n y p dos números enteros tal que $n \geq 1$ y p un número primo. Supongamos $n = p^a r$, donde a es un entero no negativo y r es un entero positivo tal que p no divide a r. En estas condiciones, si $t \leq a$, el entero $\binom{n}{p^t}$ es divisible por p^{a-t} pero no lo es por p^{a-t+1}.

Demostración

[J]. ♦.

Haciendo uso del resultado anterior es fácil probar el siguiente lema de teoría elemental de números, del cual no hemos encontrado referencias en la literatura.

Lema 1.8.

Sea un entero $n > 1$. El máximo común divisor (mcd) de

$\{ \binom{n}{i} / i = 1, \ldots, n-1 \}$ es p, si n es una potencia de un número primo p, y es

1 en caso contrario.

Demostración.

Sea d = mcd ({ $\binom{n}{i}$ / i = 1,....., n-1 }).

Supongamos primero que n es una potencia de un primo p, digamos $n=p^a$, entonces d divide a p^a, luego d es de la forma, $d = p^b$.

Por otro lado d divide a $\binom{n}{p^{a-1}}$ y por el lema anterior, $\binom{n}{p^{a-1}}$ no es divisible por p^2.

Ahora, si $n = p_1^{a_1} \ldots\ldots p_t^{a_t}$, con $t \geq 2$, entonces d es de la forma $d = p_1^{\alpha_1} \ldots\ldots p_t^{\alpha_t}$ con $0 \leq \alpha_i \leq a_i$, para i = 1,.....,t. Como d divide a $\binom{n}{p_i^{a_i}}$ para todo i, d divide a $\binom{n}{p_1^{a_1}}$. Usando de nuevo el lema 1.7., $\binom{n}{p_1^{a_1}}$ no es divisible por p_1, y concluimos que $\alpha_1 = 0$. Así sucesivamente, demostramos que $\alpha_i = 0$, para i = 1,.....,t. ♦.

Proposición 1.9.

Sea a un elemento no nulo de R y n un entero, $n \geq 2$. Entonces :

$aX^n \in R[X]_d$ (resp. $aX^n \in R_0[X]_d$) si y solamente si el orden de a divide a $\binom{n}{i}$ para i = 1,....., n-1.

Demostración.

Supongamos que $aX^n \in R[X]_d$, tenemos

$aX^n (1 + X)^n = a(X(1 + X))^n =$

$= a(X + X^2)^n = aX^n \circ (X + aX^2) = aX^n + aX^{2n}$.

Desarrollando $a(X + X^2)^n$, obtenemos que $a\binom{n}{i}X^{n+i} = 0$ para todo i,

i=1,2,.....,n-1; luego necesariamente $a\binom{n}{i} = 0$.

El reciproco es inmediato. ◆.

El siguiente resultado caracteriza los monomios distributivos de los casi-anillos de polinomios $R[X]_d$ y $R_0[X]_d$ y por lo tanto todos los elementos (ver 1.5).

Teorema 1.10.

Sea a un elemento no nulo de R y n un entero ≥ 2, entonces:

$aX^n \in R[X]_d$ ($aX^n \in R_0[X]_d$) si y solamente si existe un primo p y un entero positivo α tal que $n = p^\alpha$ y $O(a) = p$.

Demostración

Supongamos que $aX^n \in R[X]_d$, por la proposición 1.9. O(a) divide a

$\binom{n}{i}$ para i = 1,....., n-1, luego divide a mcd ($\{\binom{n}{i} / i = 1,....., n-1\}$).

Como O(a) > 1, usando el Lema 1.8. tenemos que $n = p^\alpha$ para algún primo p y para algun entero $\alpha > 0$.

El reciproco es obvio. ◆.

Ejemplo 1.11.

Tomamos como R, el anillo de los enteros módulo 6, $Z_{/6Z}$.

En este caso los monomios distributivos de grado mayor que 1, de $(Z_{/6Z})[X]_d$ y $(Z_{/6Z})_0[X]_d$: (6 = 2.3) son

Para p = 2, $3X^{2^n}$ para todo n ≥ 1.

Para p = 3, $2X^{3^n}$, $4X^3$, para todo n ≥ 1. ♦.

Como consecuencia de 1.5 y 1.10., obtemos el siguiente resultado, cuya demostración se puede abordar directamente .

Teorema 1.12.

Se tiene:

$$R[X]_d = R_0[X]_d .$$

Demostración.

Se deduce de 1.5. y 1.10. ♦.

Recordemos que este resultado tiene su correspondiente en el caso del casi-anillo M(G), puesto que $M(G)_d = (M(G)_0)_d$. (ver Cap.0-2.3).♦♦.

§2. EL ANILLO DE LOS ELEMENTOS DISTRIBUTIVOS EN CASI-ANILLOS DE POLINOMIOS.

En este párrafo daremos una descrpición explícita del anillo $R[X]_d$.

Definición 2.1.

Para cada número primo p, definimos los siguientes subconjuntos de R y de $R[X]_d$ respectivamente.

$$I_p := \{ a \in R / O(a) = p \} \cup \{ 0 \},$$

$$I_p[X] := \{ a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \ldots\ldots\ldots + a_1 X^{p^1} / a_i \in I_p, n \geq 1 \}.$$

Proposición. 2.2.

(i) Para cada primo p, I_p es un ideal de R.

(ii) Si p y q son primos distintos, $I_p I_q := \{ ab / a \in I_p , b \in I_p \} = \{ 0 \}$.

(iii) Para todo primo p, $I_p[X]$ es un ideal de $R[X]_d$.

(iv) $I_p[X] \circ I_q[X] := \{ f(X) \circ g(X) / f(X) \in I_p[X] , g(X) \in I_p[X] \} = \{ 0 \}$, donde p y q son primos distintos.

Demostración.

(i) Es comprobación rutinaria.

(ii) Sea $ab \in I_p I_q$, con $a \in I_p$ y $b \in I_p$, entonces el O(ab) es finito;

además O(ab) divide a p y a q, luego ab = 0

(iii) Sea q un número primo y sean $cX^{q^r} \in R[X]_d$ y $aX^{p^n} \in I_p[X]$.

Se tienen $M_1 := cX^{q^r} \circ aX^{p^n} = ca^{q^r}X^{p^n q^r}$ y $M_2 := aX^{p^n} \circ cX^{q^r} = ac^{p^n}X^{p^n q^r}$

Si r = 0, entonces c puede ser cualquier elemento de R y queda $M_1 = caX^{p^n} \in I_p[X]$ por (i) y $M_2 = ac^{p^n}X^{p^n} \in I_p[X]$.

Suponer r distinto de cero, entonces por 1.10. O(c) = q.

Si $p \neq q$, $M_1 = M_2 = 0$ por (ii).

Si $p = q$, $M_1, M_2 \in I_p[X]$ por (i).

(iV) Esto se sigue de (i) y (ii).

Para el resto de la demostración observar que basta con considerar monomios. . ♦.

El importante resultado que veremos a continuación describe el anillo de los elementos distributivos como una suma directa de subcasi-anillos.

Teorema 2.3.

Se tiene:

$$R[X]_d = \left(\bigoplus_{p \in P} Ip[X] \right) \oplus RX.$$

donde P denota el conjunto de todos los números primos.

Demostración

(Cap.0-1.24) 1.3, 1.5, 1.10 y 2.2. ♦.

Ejemplos 2.4.

(a) Tomemos $R = Z_{/12Z}$, el anillo de los enteros módulo 12, cuya característica es $12 = 3.2^2$.

Entonces $I_2 = \{ 0, 6 \}$, $I_3 = \{ 0, 4, 8 \}$ y $I_p = \{ 0 \}$ para todo primo $p \neq 2, 3.$, con lo que $Z_{/12Z}[X]_d = (I_2[X] \oplus I_3[X]) \oplus Z_{/12Z}X$.

(b) Sea ahora $R = K[Y]$, el anillo de polinomios sobre un cuerpo finito de característica un primo p, asi $R[X]_d = I_p[X] \oplus RX$. con $I_p = R = K[Y]$.

(c) Tomemos $R = Z \times Z_{/pZ}$, R es directo del anillo de los enteros y del anillo de los enteros módulo el número primo p. Notar que, en este caso, la caracteristica de R es cero. Por lo tanto $I_q = \{ 0 \}$ si q es un primo distinto de p.

Todos los elementos de la forma (a,b) con $a \neq 0$ tienen orden infinito, luego por el lema 1.4. : $(a,b)X^n \notin R[X]_d$ si $n > 1$.

Los elementos de la forma (0 , b) tienen orden p, luego

$I_p = \{ (0,0), (0,1), \ldots\ldots\ldots, (0, p-1) \}$, en consecuencia

$$R[X]_d = I_p[X] \oplus RX.$$

(d) Tomemos $R = \prod p \ (Z_{/pZ})$, el producto directo de los anillos de enteros modulo p, donde p recorre el conjunto de todos los primos. Mediante un razonamiento similar al empleado en el ejemplo (c), se observa que para cada p, el anillo R tiene un ideal I_p isomorfo al cuerpo primo $Z_{/pZ}$ De ahi que en la expresión del anillo $R[X]_d$, apareceran infinitos sumandos $I_p[X] \neq 0$.

(e) Por último, tomemos $R = Z_{/15Z}$ de característica $15 = 5.3$

Para todo primo $p \neq 5,3$; tenemos que $I_p = \{ 0 \}$ e $I_5 = \{ 0, 3, 6, 9, 12 \}$, $I_3 = \{ 0, 5, 10 \}$. Nétese que $1 = 6 + 10$, luego todo elemento de R se expresa como suma de uno de I_5 y uno de I_3 . Además, esa esprexión es única por la Proposición 2.2 . Como también $X = 10X + 6X$; tenemos :

$$R[X]_d = (I_5[X] \oplus I_3[X]) \oplus RX = (I_5[X] + I_5X) \oplus (I_3[X] + I_3X),$$

(aqui $I_5X = \{ aX / a \in I_5 \}$, análogo para I_3X.) ◆.

Los ejemplos vistos y otros que se pueden poner para ilustrar el teorema 2.3, son interesantes y exóticos. El último ejemplo y el hecho de que RX es un subanillo pero no un ideal nos sugiere las siguientes definiciones.

Definición 2.5.

Para cada primo p, definimos :

$$I_p^*[X] := \{ a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \ldots\ldots\ldots + a_1 X^{p^1} + a_0 X^{p^0} / a_i \in I_p, n \geq 0 \}$$

El lema siguiente muestra que son unos nuevos ideales de $R[X]_d$ distintos de los $I_p[X]$.

Lema 2.6.

Para cada primo p :

(i) $I_p^*[X]$ es un ideal del anillo $R[X]_d$.

(ii) $I_p^*[X]$ o $I_q^*[X]$:= {f(X)og(X) / f(X) $\in I_p^*[X]$, g(X) $\in$ $I_p^*[X]$ } = {0}, donde p y q son primos distintos.

Demostración

La demostración es esencialmente la misma que la dada en 2.2 (iii) y 2.2 (iv) y por lo tanto la omitimos. ♦.

Nota 2.7.

En general, dado un ideal J de R, se define J[X] como el conjunto de polinomios a_nX^n +.....+ a_1X + a_0, donde los a_i $\in$ J para todo i = 0,1,....,n y n es un entero positivo. Se demuestra que J[X] es un ideal del casi-anillo de polinomios R[X]; más aún, es un ideal también del anillo de polinomios R[X] (ver Capítulo III). Notar que en nuestro caso $I_p[X]$ está estrictamente contenido en $I_p^*[X]$ y éste a su vez está estrictamente contenido en $I_p(X)$. Por otra parte es fácil comprobar que ni $I_p[X]$ ni $I_p^*[X]$ son ideales del casi-anillo R[X].

Definición 2.8.

Diremos que un anillo R commutativo y con identidad satisface la "propiedad de primos " si existen números primos p_1,.....,p_S y elementos a_1 en I_{p1}, ..., a_S en I_{ps} tales que 1 = a_1 + a_2 +.....+ a_S.

Corolario 2.9.

Sea R es un anillo que satisface la " propiedad de primos " . Se tiene

$$R[X]_d = \left(\bigoplus_{p \in P} Ip^*[X] \right)$$

donde P denota el conjunto de todos los números primos.

Demostración

Usar 2.3, 2.5,2.6 y 2.8. ♦.

La " propiedad de primos " de un anillo, requerida en el corolario 2.9 no la satisfacen todos los anillos, como se ilustra en los siguientes ejemplos:

Ejemplos 2.10.

(i) Si R es un anillo de característica nula, entonces R no satisface la "propiedad de primos " .

(ii) Si R es un anillo de característica un entero $n > 1$ tal que $n = p_1 p_2 \ldots\ldots p_r$, donde $r > 1$ y $p_1, p_2, \ldots\ldots, p_r$ primos distintos, se tiene que $p_1 p_2 \ldots\ldots \hat{p}_i \ldots\ldots p_r \in I_{pi}$ para $i = 1,2,\ldots\ldots,r$ (donde $\hat{p}_i$ denota la omision de p_i.) Como mcd($p_2 \ldots p_r$, $p_1 p_3 \ldots\ldots p_r$, ..., $p_1 p_2 \ldots\ldots p_{i-1} p_{j+1} \ldots\ldots p_r$, ..., $p_1 p_2 \ldots\ldots\ldots p_{r-1}$) = 1 , llegamos a que $1 = a_1 + a_2 + \ldots\ldots + a_s$ donde los $a_i \in I_{pi}$, concluimos que esta clase de anillos tienen la " propiedad de primos ".

Notar que la " propiedad de primos " de R es una condición necesaria y suficiente para que $R[X]_d$ sea suma directa de los $Ip^*[X]$

Corolario 2.11.

Si R es un anillo de característica un primo p, entonces:

$$R[X]_d = \{ a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \ldots\ldots\ldots + a_1 X^{p^1} + a_0 X^{p^0} / a_i \in R, n \geq 0 \}$$

Demostración

Usar 2.3 y 2.9. ♦.

Si R es un cuerpo finito, los elementos de $R[X]_d$ coinciden con los llamados " p-polinomios " - también conocidos como "polinomios aditivos " - introducidos y estudiados por O. ORE [O], aunque esto fue en un contexto distinto . Ore define polinomio aditivo sobre un cuerpo como un polinomio satisfaciendo la siguiente identidad :

$$f(X + Y) = f(X) + f(Y) ,$$

donde X y Y son variables algebraicamente independientes. El demuestra que si la característica del cuerpo es cero, entonces los polinomios aditivos son todos triviales, es decir, polinomios lineales; y que si la característica del cuerpo es un primo p, entonces son de la forma descrita arriba, (Corolario 2.11.) .

Se obtiene como consecuencia inmediata del corolario anterior la equivalencia entre las definiciones de " polinomio distributivo en casi-anillos de polinomios con coeficientes en un cuerpo " y " polinomio aditivo "

Los polinomios aditivos o p-polinomios, (sobre cuerpos de característica positiva) tienen unas interesantes propiedades Citemos alguna de ellas. Si K es un cuerpo finito , entonces K es, para algún primo p, un $Z_{/pZ}$ - espacio vectorial de dimension finita . En este caso los

polinomios aditivos pueden considerarse como endomorfismos de K, como Z/pZ-espacio vectorial; y sus raices podrán ser calculadas entonces resolviendo un sistema de ecuaciones lineales.

Esta y otras propiedades han sido estudiadas entre otros por O. Ore,[O], Waples [W], J. Carcanague [Ca] y muchos de estos resultados y aplicaciones acerca de los p-polinomios pueden encontrarse en el interesante libro " Finite Fields " de Lidl, R., y Neiderreiter, H. [L-N].

El comentario anterior sugiere extender la definición de polinomio aditivo al conjunto de polinomios con coeficientes en un anillo R .

Definición 2.12.

Diremos que un elemento $f(X) \in R[X]$ es un polinomio aditivo si :

$$f(X) \circ (X + Y) = f(X + Y) = f(X) + f(Y),$$

donde X e Y son variables algebraicamente independientes.

Claro está, todo polinomio aditivo es un elemento distributivo. El reciproco también es cierto, y se obtiene como consecuencia de 2.3.

Teorema 2.13.

Si $f(X) \in R[X]$ es un polinomio aditivo , entonces $f(X) \in R[X]_d$.

Demostración

Usar 2.3.◆.

Acabamos este párrafo con algunos importantes resultados relativos a la estructura del anillo $R[X]_d$, en el caso en que R es un cuerpo finito.

Corolario 2.14.

(i) $(Z_{/pZ}[X]_d, +, o)$ es isomorfo al anillo de polinomios $(Z_{/pZ}[X], +, .)$.

(ii) Si K es un cuerpo finito no primo de característica p, entonces $(K[X]_d, +, o)$ es un anillo no commutativo y su centro es isomorfo al anillo de polinomios $(Z_{/pZ}[X], +, .)$ y $(K[X]_d, +, o)$ contiene un anillo isomorfo al anillo de polinomios $(K[X]_d, +, .)$.

Demostración.

(i) La aplicación , $\Psi : (Z_{/pZ}[X], +, .) \rightarrow (Z_{/pZ}[X]_d, +, o)$,

dada por :

$$\Psi (a_n X^n + \ldots\ldots + a_1 X + a_0) = a_n X^{p^n} + \ldots\ldots + a_1 X^{p^1} + a_0 X,$$

es biyectiva. Por otro lado es un homomorfismo de anillos, puesto que para todo $a \in Z_{/pZ}$ se tiene que $a^p = a$;

(ii) Se tiene Cardinal(K) = p^n, para algún $n \geq 2$, y $K-\{ 0 \} = \{ 1, a , a^2, \ldots\ldots\ldots, a^{p^n - 2} \}$ para algún $a \in K$.

Calculemos el centro de $K[X]_d$, que lo denotaremos por $C(K[X]_d)$.

Si $bX^p \in C(K[X]_d)$, $b \neq 0$ tenemos

$abX^{p^r} = aX \text{ o } bX^{p^r} = bX^{p^r} \text{ o } aX = ba^{p^r} X^p$, luego $a^{p^r} = a$, por tanto $a^{p-1} = 1$ de donde $p^n - 1$ divide a $p^r - 1$. Lo que nos permite concluir que $r = nt$, para algún t .

Además, tenemos $bX^{p^{r+1}} = b(X^{p^r})^p = bX^{p^r} \text{ o } X^p = X^p \text{ o } bX^{p^r} = b^p X^{p^{r+1}}$, de donde $b^p = b$ con lo que $b^{p-1} = 1$.

Como $K-\{0\}$ y $Z_{/pZ}^{*} = Z_{/pZ} - \{ 0 \}$ es el único subgrupo de de orden $p-1$ y puesto que $K-\{ 0 \}$ es cíclico, con lo que los únicos elementos de K

que verifican $c^p = c$ son los de $Z_{/pZ}$.

Sea B el grupo generado por $cX^{p^{nt}}$ para todo t entero positivo y para todo elemento c de $Z_{/pZ}$, es decir $B = Gp\langle\ cX^{p^{nt}} / t \in N, c \in Z_{/pZ}\ \rangle$.

Demostremos que B coincide con $C(K[X]_d)$, lo cual prueba en particular que el anillo $K[X]_d$ no es conmutativo.

Es inmediato comprobar que B es un subanillo de $K[X]_d$ y arriba hemos demostrado que $C(K[X]_d)$ está contenido en B, puesto que

$f(X) = a_m X^{p^m} + \ldots\ldots + a_1 X^{p^1} + a_0 X^{p^0} \in C(K[X]_d)$ si y sólo si $a_i X^{p^i} \in C(K[X]_d$ para todo i.

La otra inclusión es una comprobación rutinaria.

Por último la aplicación $\Phi: (B, +, o) \rightarrow (Z_{/pZ}[X], +, .)$, determinada por

$\Phi(cX^{p^{nt}}) = cX^t$, para todo $t \in N$ y para todo $c \in Z_{/pZ}$, y extendida de forma lineal es un isomorfismo de anillos.

Cardinal(K) = $p^n = m$ Construimos el siguiente subconjunto de $K[X]_d$:

$$S := \{ a_t X^{m^t} + a_{t-1} X^{m^{t-1}} + \ldots\ldots + a_1 X^{m^1} + a_0 X^{m^0} / a_i \in K, t \geq 0 \}$$

que es un subanillo de $K[X]_d$.

La aplicación, $\Psi: (S, +, o) \rightarrow (K[X], +, .)$ determinada

$$\Psi(aX^{m^t}) = aX^t, \text{ para todo } t \in N \text{ y para todo } a \in K,$$

y extendida de forma lineal, es un isomorfismo de anillos. La comprobación resulta rutinaria (basta observar que para todo $a \in K$ y para todo $t \in N$; $a^{m^t} = a$). ◆◆.

§3. EL ANILLO DE LOS ELEMENTOS DISTRIBUTIVOS EN CASI-ANILLOS DE SERIES DE POTENCIAS FORMALES.

Cerraremos este capitulo buscando todos los elementos distributivos de los casi-anillos de series de potencias formales sobre un anillo comumutativo y con identidad, caracterizando el anillo de dichos elementos.

Los resultados a obtener van a ser análogos a los obtenidos en el caso de polinomios. Muchos de ellos sólo necesitarán trasladar, de forma natural, los conceptos definidos en los dos párrafos precedentes a este que iniciamos. Parte de las demostraciones se basan en resultados ya obtenidos con anterioridad.

Así como en el caso de polinomios atacábamos el problema por el grado del polinomio en el caso de series de potencias formales atacaremos el problema por el orden de la serie, llegando a resultados paralelos.

Definición. 3.1.

Una serie de potencias formales sobre R es un sucesión infinita $f = (f_0, f_1, \ldots\ldots, f_n, \ldots\ldots)$ de polinomios homgéneos f_n con coeficientes en R, de forma que cada polinomio f_n es el polinomio cero o es un polinomio homogéneo de grado n; el índice más pequeño n, para el cual el polinomio f_n es distinto de cero, es llamado el orden de la serie f y lo denotaremos por O(f). Como es habitual se denota al conjunto de las series formales por R[[X]]. Se definen una adición y una multiplicación de forma

obvia,que dotan a este conjunto de estructura de anillo. (ver [Z-S]).

Cada serie de potencia formales f, se puede escribir como una serie de potencias en X, $f = \sum a_i X^i$ con $a_i \in R$ y $i \geq 0$. (ver [Z-S]).

Identificaremos el anillo de polinomios R[X] con el subanillo obvio del anillo R[[X]].

Se demuestra que el conjunto, $R_+[[X]]$ de todas las series de potencias formales de orden no nulo junto a la serie cero, con las operaciones :

" + " suma usual de series y

" o " sustitución de series de potencias :

$$\sum a_i X^i \, o \, \sum b_j X^j = \sum a_i \left(\sum b_j X^j\right)^i$$

es un casi-anillo con identidad X, (ver por ejemplo [C]).

Esta operación de sustitución en principio no la podemos definir para todas las series de potencias formales, pues nos topamos en medio con sumas infinitas de elementos de R, que sólo tendrán sentido si trabajamos con alguna topologia en el anillo R .

Sea N el conjunto de todos los elementos nilpotentes de R. Si nos restringimos al conjunto de series de potencias formales con coeficiente inicial un elemento de N y denotamos este conjunto por $R_N[[X]]$, puede demostrarse que ($R_N[[X]]$, +, o) es un casi-anillo con identidad (ver, [K_1], [K-M]) .

Proposición 3.2.

(i) $R_+[[X]]$ es un subcasi-anillo de $R_N[[X]]$.

(ii) ($R_N[[X]]_d$, +, o) y ($R_+[[X]]_d$, +, o) son anillos con identidad. Además $R_N[[X]]_d$ es un subanillo de $R_+[[X]]_d$.

(iii) ($R_N[[X]]_d$, +) y ($R_+[[X]]_d$, +) son R-submódulos de R[[X]].

(iv) ($R_N[[X]]_d$, +, o) y ($R_+[[X]]_d$, +, o) son subanillos del anillo (End($R_N[[X]]_d$), +, o) y (End($R_+[[X]]_d$), +, o) respectivamente .

(v) $R_0[X]$ es un subcasi-anillo de de $R_+[[X]]$.

Demostración

(i) Obvio.

(ii) Las dos primeras afirmaciones son inmediatas usando 1.2. Para la tercera, sea $f = \sum a_i X^i \in R_N[[X]]_d$, entonces:

$a_0 = f \circ 0 = f \circ (0+0) = f \circ 0 + f \circ 0 = a_0 + a_0$, por lo tanto $a_0 = 0$.

(iii) Se demuestra igual que en el caso de polinomios.(ver 1.2).

(iv) Basta considerar la aplicación $i : R_+[[X]]_d \rightarrow End(R_+[[X]])$ definida de la siguiente forma : $i(f)(g) = f \circ g$, donde $f \in R_+[[X]]_d$ y $g \in R_+[[X]]$; que es un monomorfismo de anillos.

El resto de la prueba no reviste dificultad. ♦.

Proposición 3.3.

Sea a un elemento no nulo de R y n un entero con $n \geq 2$. Se tiene :

$aX^n \in R_+[[X]]_d$ ($aX^n \in R_+[[X]]_d$) si y solamente si $aX^n \in R_0[X]_d$.

Demostración

Una implicación es inmediata, por 3.2. (v).

Demostremos el reciproco. Sea $aX^n \in R_0[X]_d$; por el teorema 1.10 existen un primo p y un entero positivo r, tales que $n = p^r$ y $O(a) = p$. Sean

f, g elementos de R[[X]], tenemos:

$aX^{p^r} \circ (f + g) = a(f + g)^{p^r} = af^{p^r} + ag^{p^r} = aX^{p^r} \circ f + aX^{p^r} \circ g$,

puesto que (R[[X]], + , .) es un anillo commutativo. ♦.

El siguiente paso es reducir el problema de encontrar los elementos distributivos al caso de monomios.

Teorema 3.4.

Sea $f = \sum a_i X^i \in R[[X]]$. Entonces $f \in R_+[[X]]_d$,(resp. $f \in R_N[[X]]_d$) si y solamente si $a_i X^i \in R_+[[X]]_d$ (resp. $a_i X^i \in R_N[[X]]_d$).

Demostración

Tomamos k = mínimo (i / $a_i X^i \notin R_+[[X]]_d$). Ya que $R_N[[X]]_d$ es un subanillo de $R_+[[X]]_d$ y ($R_N[[X]]_d$, +) y ($R_+[[X]]_d$, +) son R-submódulos de R[[X]] , usando 3.2., concluímos que $k \geq 2$.

Sea $f = a_1X + a_2X^2 + \ldots\ldots + a_kX^k + \ldots\ldots$, definimos g :

$g := f - (a_1X + a_2X^2 + \ldots\ldots + a_{k-1}X^{k-1})$ que es un elemento de $R_+[[X]]_d$ (hacemos uso de nuevo de 3.2.)

La última proposición nos permite afirmar que $a_kX^k \notin R_0[X]_d$. Ahora usando el Lema 1.4. , podemos elegir j :

$$j = \text{mínimo} \{ i \ / \ 1 \leq i \leq k-1, a_k\binom{k}{i} \neq 0 \}.$$

Consideramos $h_1 = X^t$, $h_2 = X^{t+1} \in R[[X]]$, con $t \geq 1$; tenemos :

$$(*) \equiv g \circ h_1 + g \circ h_2 =$$

$(a_k X^{tk} + a_{k+1} X^{t(k+1)} + \ldots\ldots) + (a_k X^{(t+1)k} + a_{k+1} X^{(t+1)(k+1)} + \ldots\ldots)$

Por otro lado,

$g \circ (h_1 + h_2) = a_k (X^t + X^{t+1})^k + a_{k+1} (X^t + X^{t+1}) + \ldots\ldots\ldots\ldots =$

$= a_k X^{tk} + a_k \binom{k}{j} X^{tk} X^j + \ldots\ldots + a_k X^{(t+1)k} + a_{k+1} X^{t(k+1)} + \ldots\ldots\ldots\ldots \equiv (**)$

observamos que $a_k \binom{k}{j} X^{tk+j} \neq 0$ y que los monomios de los sumandos de los polinomios de la forma $a_m (X^t + X^{t+1})^m$ tienen grado mayor o igual que tm. Eligiendo un entero suficientemente grande t, tenemos, que para todo $m > k$ se verifica $tk + j < tm$. Además $a_k \binom{k}{j} X^{tk+j} \neq 0$ es el monomio de grado más bajo (distinto de $a_k X^{tk}$) que aparece en el desarrollo del polinomio $a_k (X^t + X^{t+1})^k$; por último como $(*) = (**)$, $a_k \binom{k}{j} X^{tk+j} + \ldots\ldots\ldots\ldots$ debe ser 0., lo cual es una contradición; concluyendo entonces que $a_k X^k \in R_+[[X]]_d$. ♦.

Obtenemos los primeros corolarios como consecuencia de los resultados anteriores.

Corolario 3.5.

Se tiene :

$$R_+[[X]]_d = R_N[[X]]_d.$$

Demostración.

Usar 1.6, 3.3 y 3.4. ◆

Corolario 3.6.

Si todos los elementos no nulos de R tienen orden infinito (es decir el anillo R es libre de torsión), entonces :

$$R_+[[X]]_d = RX.$$

Demostración

3.1, 3.3 y 3.4. ◆ .

Nota 3.7.

La hipótesis introducida en el corolario anterior es una condición necesaria como ilustra el siguiente ejemplo : tomando $R = Z_{/4Z}$.

$$R_+[[X]]_d = \{ b_iX + \sum a_iX^{2^i} \ / \ b_i \in R \, , a_i \in \{ 0, 2 \}, y \ i \geq 1 \} \, ,$$

luego RX está estrictamente contenido en $R_+[[X]]_d$.

En orden a dar una descripción explícita del anillo $R_+[[X]]_d$, introducimos las siguientes definiciones, de forma similar al caso de polinomios.

Definición 3.8.

Para cada primo p, definimos los siguientes subconjuntos de $R_+[[X]]_d$:

$$I_p[[X]] := \{ \sum a_iX^{p^n} \ / \ , a_i \in I_p \, , \ \text{con} \ n \geq 1. \}$$

$$I_p^*[[X]] := \{ \sum a_iX^{p^n} \ / \ , a_i \in I_p \, , \ \text{con} \ n \geq 0. \}$$

Lema 3.9.

Para cada primo p, se verifican

(i) $I_p[[X]]$ y $I_p^*[[X]]$ son ideales de $R_+[[X]]_d$.

(ii) Los subconjuntos de $R_+[[X]]_d$, $I_p[[X]]$ o $I_q[[X]]$ y $I_p^*[[X]]$ o $I_q^*[[X]]$ son la serie 0, cuando p y q son primos distintos.

Demostración

La demostración es similar a la dada para el caso de polinomios en 2.2. y 2.6. y por lo tanto la omitimos . ◆.

En este caso tampoco $I_p[[X]]$ y $I_p^*[[X]]$ son ideales del casi-anillo $R_+[[X]]$.

A continuación enunciamos el resultado más notable de este párrafo.

Teorema 3.10.

Se tiene:

$$R_+[[X]]_d = \left(\bigoplus_{p \in P} Ip[[X]] \right) \oplus RX,$$

donde P denota el conjunto de todos los números primos.

Demostración

Es inmediata usando Cap.0-1.23, 1.10, 3.3., 3.4. y 3.9. ◆.

Notemos que RX es un subanillo de $R_+[[X]]_d$ pero no un ideal. En el

siguiente corolario expresamos $R_+[[X]]_d$ como suma directa de ideales, en algunos casos particulares.

Corolario 3.11.

Sea R es un anillo que satisface la " propiedad de primos " (ver 2.8.) entonces:

$$R_+[[X]]_d = \left(\bigoplus_{p \in P} Ip^*[[X]] \right)$$

donde P denota el conjunto de todos los números primos.

Demostración

Cap.0-1.24, 2.8 , 3.9 y 3.10. ♦.

Una vez más, en el siguiente resultado, se pone de manifiesto el paralelismo existente entre las conclusiones obtenidas para el caso del casi-anillo de polinomios y el de series de potencias formales.

Corolario 3.12.

Si la característica de R es un número primo p, entonces:

(i) $R_+[[X]]_d = \{ \sum a_i X^{p^n} / \ , a_i \in R, \text{ con } n \geq 0. \}$.

(ii) El casi-anillo $R_+[[X]]$ contiene un subanillo B, isomorfo al anillo de series de potencias formales $(Z_{/pZ}[[X]], +, .)$. En particular $((Z_{/pZ})_+[[X]]_d, +, o)$ es isomorfo al anillo de series de potencias formales $(Z_{/pZ}[[X]] , +, .)$.

Demostración.

Basta considerar la aplicación, $\Psi : (Z_{/pZ})_+[[X]]_d \rightarrow Z_{/pZ}[[X]]$ definida de la siguiente forma :

$$\Psi(\sum a_i X^{p^i}) = \sum a_i X^i .$$

Un razonamiento análogo al llevado a cabo para el caso de polinomios completa la demostración. (ver 2.12.). ◆.

Todos los resultados obtenidos en el párrafo 2, pueden trasladarse al caso de series de potencias formales, con un poco de cuidado y teniendo en cuenta las definiciones de este párrafo.◆◆.

CAPITULO II. ANILLOS Y ANILLOS COCIENTE EN CASI-ANILLOS DE POLINOMIOS

En el primer párafo de este capítulo abordaremos el estudio de los subcasi-anillos de casi-anillos de polinomios que cumplan la propiedad distributiva a los dos lados.

En el resto del capítulo nos dedicaremos al estudio de anillos cocientes de casi-anillos N; es decir, buscaremos ideales I de N para los cuales $N_{/I}$ sea un anillo. En el segundo párrafo trataremos dicho estudio en el caso general, y en el tercer párrafo se trata el caso concreto de casi-anillos de polinomios.

S 1 ANILLOS EN CASI-ANILLOS DE POLINOMIOS

Nuestro propósito es el de investigar aquí cuáles son los anillos contenidos en R[X]. Puesto que todos los anillos son casi-anillos cero-simétricos, sólo necesitamos buscarlos en la parte cero-simétrica de R[X], es decir en $R_0[X]$.

El siguiente teorema, que demostraremos en sucesivas etapas y que

será el resultado más destacable de cuantos se vean en este párrafo, pondrá de manifiesto que la complejidad del problema se agudiza cuando el anillo R de los coeficientes no es íntegro.

Teorema 1.1.

Sea R un dominio de integridad. Todo subanillo (no necesariamente unitario) de R[X] está contenido en $R[X]_d$.

Algunos de los resultados vistos en el Capítulo I junto con otros que vamos a obtener a continuación van a hacer factible la demostración del teorema precedente.

Comenzamos enunciando un resultado conocido en casi-anillos de polinomios,

Lema 1.2. [La- N] [P]

(i) Para todo p(X), q(X) ∈ R[X], se tiene

grado(p(X) o q(X)) ≤ grado(p(X)) grado(q(X)) . (Grado(0) = 0)

y si R es un dominio de integridad ,se verifica la igualdad.

(ii) Si R es un dominio de integridad, entonces cada p(X) ∈ R[X] con grado(p(X)) > 0, es un elemento cancelable a la derecha, es decir si : f(X),g(X),p(X) ∈ R[X] son tales que f(X) o p(X) = g(X) o p(X) entonces

f(X) = g(X).

Demostración.

[P]. ♦.

Lema 1.3.

Sea R un dominio de integridad y S un subanillo de R[X] (no necesariamente unitario), se verifica ,

$$f(X) \circ (X + f(X)) = f(X) + f(X) \circ f(X), \text{ para todo } f(X) \in S.$$

Demostración

Sea $0 \neq f(X) \in S$, entonces $0 \neq f(X) \circ f(X) \in S$. Se tiene

$f(X) \circ (f(X) + f(X) \circ f(X)) =$

$= f(X) \circ f(X) + f(X) \circ f(X) \circ f(X) = (f(X) + f(X) \circ f(X)) \circ f(X)$

y por otro lado

$f(X) \circ (f(X) + f(X) \circ f(X)) = f(X) \circ (X + f(X)) \circ f(X)$.

Usando 1.2 - (i) . acaba la demostración.◆.

Distinguiremos los casos en los que la característica del dominio de integridad R sea 0 o un primo p.

Trataremos estos casos separadamente y comenzamos con la siguiente,

Proposición 1.4.

Sea R un dominio de integridad de característica 0 . . Todo subanillo (no necesariamente unitario) de R[X] está contenido en $R[X]_d$.

Demostración

Sea S un subanillo de R[X] y sea $f(X) = a_n X^n + \ldots + a_1 X \in S$, por el lema 1.3,

$f(X) \circ (X + f(X)) = f(X) + f(X) \circ f(X)$,

entonces ,

$a_n(X + f(X))^n + \ldots\ldots + a_1(X + f(X)) =$

$= a_n X^n + \ldots + a_1 X + a_n f(X)^n + \ldots + a_1 f(X)$,

llegando a que $n = 1$ o $a_n = 0$, para todo $n \geq 2$.

Se acaba la demostración haciendo uso del teorema 1.6. del capítulo I. ◆ .

Corolario 1.5.

Sea R un dominio de integridad de característica 0. Los subanillos de R[X] son (salvo isomorfismos) subanillos del anillo R y recíprocamente todo subanillo de R (salvo isomorfismo) es un subanillo de R[X].

Demostración.

Es inmediata usando 1.3., 1.6. del capítulo I y 2.4. ◆.

Queda probado el teorema 1.1 para el caso de característica(R) = 0. Ahora consideramos el caso más complicado, cuando la característica de R es p.

Definición 1.6.

Sea R un anillo commutativo y con identidad, definimos :

$R'[X]_0 := \{ f(X) \in R_0[X] \ / \ f'(X) \in R \}$,

($f'(X)$ denota la derivada formal de $f(X)$).

Nota 1.7.

La derivada formal en los polinomios verifican las siguientes propiedades :

$(f(X) + g(X))' = f'(X) + g'(X)$.

$(f(X).g(X))' = f'(X)g(X) + g'(X)f(X)$.

$(f(X) \circ g(X))' = (f'(X) \circ g(X)) g'(X)$.

En términos algebraicos, la derivada formal es una derivación en el anillo de composición, $(R[X], +, o, .)$ (ver Cap III)

Estudiemos algunas propiedades de $R'[X]_0$.

Lema 1.8.

(i) $R'[X]_0$ es un subcasi-anillo de R[X] que contiene a $R[X]_d$.

(ii) Sea a un elemento no nulo de R y n un entero, $n \geq 2$. Entonces $aX^n \in R'[X]_0$ si y solamente si O(a) divide a n.

Demostración

(i) El probar que $R'[X]_0$ es un subcasi-anillo de R[X]es tarea rutinaria. Para la segunda afirmación, es suficiente observar que $f(X) = a_nX^n + \ldots + a_1X \in R'[X]_0$ si y solamente si $a_iX^i \in R'[X]_0$, para $i = 1, \ldots, n$. El resto se obtiene directamente empleando el teorema 1.10.

(ii) Es inmediata. Como corolario podemos deducir que en un dominio de integridad R de característica un p , $aX^n \in R'[X]_0$ si y sólo si p divide a n. ♦.

Teorema 1.9.

Es condición necesaria y suficiente para que $R'[X]_0 = R[X]_d$ que R sea un anillo libre de torsión .

Demostración

Si R es un anillo libre de torsión, usando el lema 1.8. (ii) tenemos que $aX^n \in R'[X]_0$ si y solamente si a = 0 o n = 1. Entonces concluimos que $R'[X]_0 = R[X]_d = RX$.

Reciprocamente, suponer que $R'[X]_0 = R[X]_d$ y que R no es libre de torsión. Sea a un elemento no nulo de R y n un entero, $n \geq 2$,tales que na = 0 , pongamos $n = p_1^{r}1.....p_t^{r}t$. Distingamos dos casos :

Si $t \geq 2$, entonces $aX^n \in R'[X]_0$ (ver lema anterior) pero $aX^n \notin R[X]_d$ (ver teorema 1.10).

Si t = 1, digamos $n = p^r$, consideramos un primo $q \neq p$. Entonces $aX^{p\,q} \in R'[X]_0$, y $aX^{p\,q} \notin R[X]_d$. (1.8 y 1.10). ◆.

Lema 1.10.

Sea R un dominio de integridad de caracteristica p . Todo subanillo de R[X] está contenido en $R'[X]_0$.

Demostración

Sea S un subanillo de R[X] y sea $f(X) = a_nX^n + ... + a_1X \in S$.

Si n =1 entonces S está contenido en $R'[X]_0$, trivialmente.

Supongamos $n \geq 2$. Primero probaremos, por reducción al absurdo, que p divide a n.

Supongamos que mcd(n, p) = 1, por el lema 1.3.,

$(a_nX^n + ... + a_1X) \circ (X + f(X)) = a_n(X + f(X))^n + ... + a_1(X + f(X))$.

Como $a_n(X + f(X))^n = a_nX^n + ... + na_nf(X)^{n-1}X + a_nf(X)^n$, con

$na_nf(X)^{n-1}X = na_nX^{n(n-1)+1} + \ldots\ldots$ y $na_nX^{n(n-1)+1} \neq 0$,

deducimos

$$f(X) \circ (X + f(X)) - (f(X) + f(X) \circ f(X)) =$$

$$= na_nX^{n(n-1)+1} + \ldots\ldots \neq 0 .$$ Contradición.

Por lo tanto p divide a n.

Sea r = máximo { i / i = 1,2,.....,n, con $a_i \neq 0$ y mcd(i, p) = 1 }.

Aparecen dos casos :

i) Si r = 1, usando el lema 1.8 tenemos que $f(X) \in R'[X]_0$, y por lo tanto S está contenido en $R'[X]_0$.

ii) Si $r \geq 2$, tenemos que $f(X) = a_nX^n + \ldots\ldots + a_rX^r + \ldots\ldots + a_1X$ con las siguientes características : $a_r \neq 0$, mcd (r, p) = 1 y $r < n$ (porque p divide a n). Por 1.3 , $f(X) \circ (X + f(X)) = f(X) + f(X) \circ f(X)$ y aplicando las propiedades de la derivada (ver 1.7),se tiene

(*) ----------(*)

$$(f'(X)(\circ (X + f(X))) (1 + f'(X)) = f'(X) + (f'(X) \circ f(X)) f'(X) , (*)$$

en el lado derecho de la igualdad, tenemos:

$$(f'(X) \circ (X + f(X))) (1 + f'(X)) =$$

$$= ((ra_rX^{r-1} + \ldots\ldots + a_1) \circ (X + f(X))) (1 + f'(X)) =$$

$$= ra_r(X + f(X))^{r-1} + \ldots\ldots + a_1 + [ra_r(X + f(X))^{r-1} + \ldots\ldots + a_1] f'(X).$$

Sea $g(X) = ra_r(X + f(X))^{r-1} + \ldots\ldots + a_1 - f'(X)$, entonces $g(X) \neq 0$ y el grado de g es n(r-1).

Sea $h(X) = (ra_r(X + f(X))^{r-1} + \ldots\ldots + a_1) f'(X) - (f'(X) \circ f(X))f'(X)$, tenemos que grado(h(X)) < n(r - 1), puesto que los grados de los monomios

de h(X) son de la forma $i + m(r - i - 1) + r - 1$ (para $i = 1,..., r$ y $m \leq n$) y estos son todos menores que $< n(r-1)$. Así de (*) resulta

$$(f'(X) \circ (X + f(X)))(1 + f'(X)) - [f'(X) + (f'(X) \circ f(X)) f'(X)] =$$

$$= h(X) + g(X) \neq 0$$

y esto es una contradición. Por lo tanto el caso ii) no se puede presentar, así que $r = 1$ y $f(X) \in R'[X]_0$. ♦ .

(*) ----------(*)

Nota 1.11.

El lema anterior no se verifica en el caso general, es decir,si R no es un dominio de integridad.

Tomemos $R = Z_{/4Z}$ y $B := Gp \langle X, 2X^{3^i} / i \geq 0 \rangle$

Demostremos que B es un anillo.

Primero probaremos que B posee la propiedad distributiva; para lo cual basta probar que $r(X) \circ (s(X) + t(X)) = r(X) \circ s(X) + r(X) \circ t(X)$. (*) es cierto cuando r(X) es un monomio de B y s(X), t(X) $\in$ B.

Distinguiremos diferentes casos :

i) Si $r(X) = aX$ donde $a \in Z_{/4Z}$, entonces $aX \in Z_{/4Z}[X]_d$.(ver Cap I-1.3).

ii) Si $r(X) = 2aX^{3^i}$, donde $a \in Z_{/4Z}$ y $i \geq 1$, analizaremos distintos subcasos :

ii-1) $r(X) = 2aX^{3^i}$, $s(X) = bX$ y $t(X) = 2g(X)$, con $g(X) \in Z_{/4Z}[X]$ de grado ≥ 1, $a,b \in Z_{/4Z}$. Entonces

$$r(X) \circ (s(X) + t(X)) = 2aX^{3^j} \circ (bX + 2g(X)) = 2a(bX + 2g(X))^{3^i} =$$

$$= 2a(b^{3^i} X^{3^i} + 2\square + \ldots\ldots\ldots\ldots + 2\square + 2^{3^i} g(X)^{3^i}) =$$

(donde los $\square$ representan polinomios)

$= 2ab^{3^i}X^{3^i} + 4\square + \ldots\ldots\ldots\ldots + 4\square + 4\square) =$

$= 2ab^{3^i}X^{3^i} = r(X) \circ s(X) + r(X) \circ t(X) = 2ab^{3^i}X^{3^i} + 0 = 2ab^{3^i}X^{3^i}.$

ii-2) $s(X) = bX$ y $t(X) = cX$, donde b y c son unidades en el anillo $Z_{/4Z}$. Entonces $r(X) \circ (s(X) + t(X)) =$

$= 2aX^{3^i} \circ (bX + cX) = 2aX^{3^i} \circ (b + c)X =$

$= 2a(b + c)^{3^i}X^{3^i} = 0\,X^{3^i} = 0.$

(puesto que b + c no es una unidad y por lo tanto es múltiplo de 2.)

Por otro lado, tenemos

$r(X) \circ s(X) + r(X) \circ t(X) = 2aX^{3^i} \circ bX + 2aX^{3^i} \circ cX =$

$= 2ab^{3^i}X^{3^i} + 2ac^{3^i}X^{3^i} = 2a(b^{3^i} + c^{3^i})X^{3^i} = 0\,X^{3^i} = 0.$

Para estudiar el caso general, si $s(X), t(X) \in B$, podemos escribir

$s(X) = b_1X + 2g_1(X)$ y $t(X) = b_2X + 2g_2(X)$,

donde $b_1, b_2 \in Z_{/4Z}$ y $g_1(X), g_2(X) \in Z_{/4Z}[X]$.

Entonces

$s(X) + t(X) = bX + 2g(X)$, donde $b = b_1 + b_2$ y $g(X) = g_1(X) + g_2(X)$.

Así $r(X) \circ (s(X) + t(X)) = 2aX^{3^i} \circ (bX + g(X)) = 2ab^{3^i}X^{3^i}$.(usando ii-1)

y por otro lado $r(X) \circ s(X) + r(X) \circ t(X) =$

$= 2aX^{3^i} \circ (b_1X + 2g_1(X)) + 2aX^{3^i} \circ (b_2X + 2g_2(X)) =$

$= 2ab_1{}^{3^i}X^{3^i} + 2ab_2{}^{3^i}X^{3^i} = 2ab^{3^i}X^{3^i}$

(usando ii-1 y distinguiendo las distintas posiblidades de b_1 y b_2)

Con esto queda probado que B es distributivo.

Resta probar que B es un subcasi-anillo, es decir, que B es cerrado para la composición. Veámoslo para los monomios de B, lo cual es suficiente al haber probado que B es distributivo. Sean f(X) y g(X) monomios de B. Distingamos varios casos:

a-1) $f(X) = aX$, $g(X) = 2bX^{3^i}$ con $a, b \in Z_{/4Z}$ y $i \geq 1$. Entonces

$f(X) \circ g(X) = aX \circ 2bX^{3^i} = 2abX^{3^i} \in B$.

a-2) $f(X) = 2aX^{3^i}$, $g(X) = 2bX^{3^j}$, con $a,b \in Z_{/4Z}$ y $i \geq 1$ y $j \geq 1$. Entonces

$f(X) \circ g(X) = 2aX^{3^i} \circ 2bX^{3^j} = 0$.

El resto de los casos son inmediatos.

Así B es un anillo (infinito) con identidad, X.

Veamos que B no está contenido en $R'[X]_0$.

El polinomio $f(X) = 2X^3 \in B$, pero $f'(X) = 3.2X^2 = 2X^2 \neq 0$, por lo tanto $f(X) = 2X^3 \notin B$. ♦.

Para finalizar la demostración del teorema 1.1 necesitamos este interesante resultado.

Proposición 1.12.

Sea R un dominio de integridad. Sea $f(X) \in R[X]_d$, con grado de $f(X) \geq 1$. Si $h(X)$, $g(X) \in R[X]$ tales que $f(X) \circ g(X) = f(X) \circ h(X)$, entonces :

$g(X) - h(X) = r \in R$ y r es una raiz del polinomio f(X).

Demostración

Puesto que $f(X) \circ g(X) = f(X) \circ h(X)$, se tiene

$f(X) \circ g(X) - f(X) \circ h(X) = 0 = f(X) \circ (g(X) - h(X))$ $(f(X) \in R[X]_d)$

como R es un dominio de integridad, usando 1.2-(i) tenemos que ,

grado(f(X)) grado (g(X) - h(X)) = grado(0) = 0, y puesto grado(f(X) $\geq$ 1, existe una constante $r \in R$, con $g(X) - h(X) = r \in R$.♦.

Corolario 1.14.

Sea R un dominio de integridad de característica p , y sea a un elemento no nulo de R, entonces aX^{p^r} es un elemento cancelable a la izquierda, para todo $r \geq 1$.

Demostración

Es inmediata de 1.13, puesto que aX^{p^r} tiene como única raíz la 0. ♦.

Proposición 1.13.

Sea R un dominio de integridad de característica p . Todo subanillo de R[X] está contenido en $R[X]_d$.

Demostración

Sea S un subanillo y sea $f(X) = a_nX^n + \ldots + a_1X \in S$.

Entonces existen h(X), g(X) ∈ R[X] tal que f(X) = h(X) + g(X), con las siguientes particularidades :

$g(X) \in R[X]_d$ y $h(X) = b_mX^m + \ldots\ldots\ldots + b_tX^t$, con $b_iX^i \notin R[X]_d$ para i = 1,....., m y t > 1.

Si h(X) = 0, hemos concluido.

Supongamos $h(X) \neq 0$. Por el lema 1.12., $f(X) \in R'[X]_0$ y puesto que $g(X) \in R[X]_d$, $g(X) \in R'[X]_0$ (1.8). Al ser $R'[X]_0$ un subcasi-anillo, $h(X) \in R'[X]_0$. Usando de nuevo el lema 1.8, podemos escribir :

$h(X) = b_mX^{p^r mkm} + \ldots\ldots\ldots + b_tX^{p^r tkt}$, con las siguientes particularidades :

$r_i \geq 1$, $b_i \neq 0$, $k_i > 1$, $mcd(p, k_i) = 1$ y $p^{r_j} k_j > p^{r_i} k_i$ para todo $i, j = t,.....,m$, con $j > i$ ##.

Sea r_h = minimo $\{ r_i \ / \ i = t,.....,m \}$. (para simplificar la notación escribimos $k_h = k$ y $r_h = r$), entonces existe un número natural s tal que :

$$h(X) = (b_m X^{p^s mkm} + ... + b_h X^k + ... + b_t X^{p^s tkt}) \circ X^{p^r}.$$

Sea F el cuerpo cociente de R y sea $\bar{F}$ la clausura algebraica de F. Entonces existen elementos $c_i \in \bar{F}$ con $c_i \neq 0$ verificando que :

$$h(X) = X^p \circ (c_m X^{p^s mkm} + ... + c_h X^k + ... + c_t X^{p^s tkt}).$$

Podemos escribir $h(X) = X^p \circ c(X)$, donde $c(X) \in F[X]$ y

$$c(X) = c_m X^{p^s mkm} + ... + c_h X^k + ... + c_t X^{p^s tkt}.$$

Tenemos que : $f(X) \circ (X + f(X)) =$

$= (g(X) + h(X) \circ (X + f(X)) = g(X) \circ (X + f(X)) + h(X) \circ (X + f(X)) =$

$= g(X) + g(X) \circ f(X) + h(X) \circ (X + f(X))$. ($g(X) \in R[X]_d$)

Por otro lado :

$f(X) + f(X) \circ f(X) = g(X) + h(X) + (g(X) + h(X)) \circ f(X) =$ (1.3.)

$= g(X) + g(X) \circ f(X) + h(X) + h(X) \circ f(X)$, deducimos que h(X) es distributivo con respecto a X y a f(X), es decir :

$(X^{p^r} \circ c(X)) \circ (X + f(X)) = X^{p^r} \circ c(X) + (X^{p^r} \circ c(X)) \circ f(X) =$

$= X^{p^r} \circ (c(X) + c(X) \circ f(X)) =$ ($X^{p^r} \in \bar{F}[X]_d$)

$= X^{p^r} \circ ((c(X) \circ (X + f(X)))$ (aplicando la asociativa), deducimos (usando el lema 1.12.) que:

$c(X) \circ (X + f(X)) = c(X) + c(X) \circ f(X)$ (*), puesto que estamos en las hipótesis del corolario anterior, así que X^{p^r} es cancelable a la izquierda.

Haciendo uso de las propiedades de la derivada (ver nota 1.7.) en (*), tenemos que :

$(c'(X) \circ (X + f(X)))\,(1 + f'(X) = c'(X) + (c'(X) \circ f(X))\, f'(X)$.

y utilizando el mismo razonamiento que en el lema 1.10 en la demostración indicada entre (*) ----------(*)) llegariamos a que $k = 1$ o $mcd(k, p) \neq 1$, pero en ambos casos obtenemos una contradición con la elección de los k_i . La contradicción esta en suponer que $h(X) \neq 0$ luego $h(X) = 0$ y por lo tanto $f(X) = g(X) \in R[X]_d$. Concluimos que S está contenido en $R[X]_d$. ♦.

Esto completa la demostración del teorema 1.1.

Nota 1.13.

Si R no es un dominio de integridad el teorema 1.1, no es cierto. El contraejemplo dado en la nota 1.11 ilustra este hecho. Recordemos que en ese caso $R = Z_{/4Z}$ y $B := Gp < X,\ 2X^{3^i} / i \geq 0 >$.

Además podemos encontrar subanillos de B que son finitos (no necesariamente unitarios), por ejemplo $B_1 = \{ 0, 2X^3 \}$.

Sea n un número natural y

$B_n := Gp < X,\ 2X^{3^i} / i = 0, 1, \ldots\ldots, n >$ entonces B_n es un subanillo finito y unitario de R[X] , que no está contenido en $R[X]_d$.

Par finalizar este párrafo establecemos un nuevo enunciado que se deduce del teorema 1.1 y de ciertos resultados vistos en el capítulo I.

Corolario 1.14.

Sea R un dominio de integridad de característica p, se tiene :

(i) R[X] tiene un único subanillo maximal.

(ii) R[X] tiene un subanillo S isomorfo al anillo de polinomios $Z_{/pZ}[X]$, ,+, .). En particular, tenemos que los subanillos de $Z_{/pZ}$ [X] son subanillos (salvo isomorfismo) del anillo de polinomios $(Z_{/pZ}[X], ,+, .)$ y recíprocamente todo subanillo del anillo de polinomios $(Z_{/pZ}[X], ,+, .)$ es un subanillo (salvo isomorfismo) de $Z_{/pZ}$ [X] .

Demostración

(i) Es inmediata.

(ii) $Z_{/pZ}$ es un subanillo de R, por lo tanto $Z_{/pZ}[X]_d$ es un subanillo de $R[X]_d$, ahora aplicar Cap.I- 2.12. y la proposición 1.12. ◆◆.

§ 2. EL RADICAL ANILLO

En este párrafo N denotará un casi-anillo.

Investigamos aquí anillos cociente de casi-anillos. Lo que es equivalente a estudiar ideales I de N tal que el casi-anillo cociente $N_{/I}$ sea un anillo. Esto sugiere encontrar (si existe) el menor ideal de N, entre los ideales de N, cuyo cociente sea anillo.

Notas 2.1.

(*) Si I es un ideal de N tal que $N_{/I}$ es un anillo, entonces :

(a) $(N_{/I}, +)$ es un grupo abeliano , por lo tanto I contiene todos los conmutadores de N, luego el grupo derivado de N, $\delta_1(N) = (N , N)$ está contenido en I.

(b) $(N_{/I}, +, .)$ es un casi-anillo distributivo, por lo tanto I contiene todos los distribuidores de N, luego el grupo $I N; N, N I$ está contenido en I.

(**) Reciprocamente, si I es un ideal de N que contiene los grupos $\delta_1(N)$ y $IN; N, N I$, entonces obviamente $N_{/I}$ es un anillo.

Esta nota sugiere la siguiente definición.

Definición. 2.2.

El menor ideal de N que contiene a todos los conmutadores y a todos los distribuidores de N, le llamaremos el radical-anillo de N y le

denotaremos por $\mathfrak{R}(N)$, es decir:

$$\mathfrak{R}(N) = \mathfrak{I}(S) \text{ donde } S = \delta_1(N) \cup \{ N; N, N \}.$$

Corolario 2.3.

Sea J un ideal de N, se tiene:

$N_{/J}$ es un anillo si y solamente si J contiene a $\mathfrak{R}(N)$.

Demostración

Se sigue de 2.1 y 2.2. ◆.

Seguidamente introduciremos distintos enunciados que posibilitarán caracterizar el radical-anillo.

Definición 2.4.

Para cada casi-anillo N, definimos la siguiente familia de ideales:

$\Omega = \{ I / I \text{ ideal de N y } N_{/I} \text{ es anillo} \}$.

Proposición 2.5.

Se tiene:

(i) $\Omega \neq \emptyset$

(ii) Si W es una subfamilia no vacia de Ω, entonces:

$w(N) := \cap \{ I / I \in W \}$ pertenece a Ω.

Demostración

(i) En efecto, N es un ideal de N y $N_{/N} = \{ 0 \}$ que es un anillo.

(ii) Puesto que W es no vacía, tenemos que w(N) es un ideal (Cap.0 1.19). Sea $J \in W$, entonces $J \in \Omega$, luego J contiene por 2.3. a $\mathfrak{A}(N)$ y por lo tanto w(N) contiene $\mathfrak{A}(N)$. Concluímos, de nuevo por 2.3 , que $N_{/w(N)}$ es anillo. ♦.

Corolario 2.6.

Se tiene :

$$\mathfrak{A}(N) = \bigcap \{ I \ / \ I \in \Omega \}.$$

Demostración

Es inmediata de 2.3 y 2.5.

Justificaremos ahora el término " radical " del ideal radical anillo.

Definición 2.7. [P], [M].

2.7-1 Una aplicación $\mathfrak{R}$ que asigna a cada casi-anillo N un ideal $\mathfrak{R}(N)$ se dice que es una aplicación radical si para cada casi-anillo N y para cada homomorfismo $f : N \to N'$, se cumple :

(i) $\mathfrak{R}(N_{/\mathfrak{R}(N)}) = \{ 0 \}$.

(ii) $f(\mathfrak{R}(N))$ está contenido en $\mathfrak{R}(f(N))$.

2.7-1 Un casi-anillo N es $\mathfrak{R}$-semisimple si $\mathfrak{R}(N) = \{ 0 \}$ y es $\mathfrak{R}$-radical si $\mathfrak{R}(N) = N$.

Proposición 2.8.

Sean N y N' dos casi-anillos , $f: N \to N'$, un homomorfismo e I un ideal de N conteniendo a Ker(f), entonces :

$I \in \Omega$ si y solamente si $f(I) \in \Omega$.

Demostración

Supongamos que $I \in \Omega$.

Sea c un commutador de f(N),entonces:

$c = f(a) + f(b) - f(a) - f(b)$, para algunos a, b ∈ N, luego

$c = f(a + b - a - b)$, y puesto que $I \in \Omega$, tenemos que f(I) contiene a todos los commutadores de f(N).

Sea d un distribuidor de f(N), $d = f(r)(f(s) + f(t)) - f(r)f(t) - f(r)f(s)$ donde r, s, t ∈ N, $d = f(r(s + t) - rt - rs)$ y puesto que $I \in \Omega$, tenemos que f(I) contiene a todos los distribuidores de f(N)., luego por 2.3. , $f(I) \in \Omega$.

Reciprocamente, supongamos que $f(I) \in \Omega$.

Sea c un commutador de N, $c = a + b - a - b$, donde a, b ∈ N. Por ser f homomorfismo, $f(c) = f(a) + f(b) - f(a) - f(b) \in f(I)$, pues $f(I) \in \Omega$, luego $f(a + b - a - b) = f(i)$ donde i ∈ I, por tanto $a + b - a - b = i + e$, con e ∈ Ker(h) . Concluimos que $a + b - a - b \in I$, porque por hipótesis Ker(h) esta contenido en I

Análogamente se demuestra que todos los distribuidores están contenidos en I; aplicando de nuevo 2.3. se concluye que $I \in \Omega$. ◆ .

Teorema 2.9.

La correspondencia $\mathcal{A}$ que asocia a cada casi-anillo N el radical anillo $\mathcal{A}(N)$, es una aplicación radical.

Demostración.

$\mathcal{A}$ es una aplicación, usar 2.6.

Como $N/\mathcal{A}(N) = N/\mathcal{A}(N)$ y $\mathcal{A}(N) \in \Omega$ (2.5), $N/\mathcal{A}(N)$ es un anillo, y por tanto $\mathcal{A}(N/\mathcal{A}(N)) = \{ 0 \}$. quedando demostrada la primera condición de 2.7.

Demostramos ahora (ii) de 2.7. Sea $f : N \to N'$ un homomorfismo, entonces :

$f(\mathcal{A}(N)) = f(\cap \{ I / I \in \Omega \})$ que está contenido en

$f(\cap \{ I / I \in \Omega$ e I conteniendo a $Ker(f) \} =$

$= \mathcal{A}(f(N))$,

usando la proposición 2.8. y el teorema de homomorfismo. Así $\mathcal{A}$ es una aplicación radical. ♦.

El radical anillo mide la " anillez " de un casi-anilo N, así como el ideal distribuidor mide la distributividad y el ideal conmutador la conmutatividad del casi-anillo .

A. Fröhlich publicó entre 1.958 y 1.960 una serie de artículos sobre casi-anillos distributivamente generados, relacionando la distributividad y la conmutatividad de los casi-anillos, obteniendo interesantes resultados (ver Cap. 0- § 2).

Corolario 2.10

(a) Si N es un casi-anillo distributivo, entonces:

$$\mathcal{A}(N) = D_1(N).$$

(b) Si N es un casi-anillo abeliano, entonces:

$$\mathcal{A}(N) = \mathfrak{I}(\delta_1(N)).$$

(c) Si N es un casi-anillo distributivamente generado, entonces:

$$\mathcal{A}(N) = \delta_1(N).$$

Demostración

Para (a) y (b) usar 2.1 y 2.2, (c) consecuencia inmediata de (Cap.0- 2.8 y 2.13). ♦ .

Nota 2.11

Los ejemplos que damos a continuación ponen de manifiesto la necesidad de las hipótesis .

(a) Si $N = R[X]$, $\delta_1(N) = \{0\}$ y $R[X]_{/\{0\}} = R[X]$, que no es un anillo.

(b) Basta tomar un casi-anillo distributivo que no sea un anillo.

(c) Como en el caso (a).

El siguiente resultado es debido a A. Frölichs,

Corolario 2.12.

Sea N un casi-anillo distributivamente generado, tal que $N^2 = N$, entonces $\mathcal{A}(N) = \delta_1(N) = D_1(N)$

Demostración

(Cap. 0- 2.14) y 2.2.◆ .

En casi-anillos en general no se conocen grandes resultados relacionando el ideal distribuidor y el ideal conmutador. EL siguiente lema técnico nos permitirá relacionarlos en algunos casos .

Lema 2.13.

Sea N un casi-anillo y H, K subgrupos de (N, +), entonces :

$(NH, NK)^N$ está contenido en $| N; H, K |^N$.

Demostración

Sean h ∈ H, k ∈ K y a, b ∈ N, entonces :

ah + bk =

= -bh + (bh + ah + bk + ak) - ak =

= -bh + ((b + a) h + (b + a) k) - ak =

= -bh + ((b + a) (h + k)) - ak = (mod ($| H, K, N |^N$)

= -bh + ((b(h + k) + a(h + k)) -ak =

= -bh + (bh + bk + ah + ak) -ak = (mod ($| H, K, N |^N$)

= bk + ah.

Luego (ah, bk) = 0 (mod ($| H, K, N |^N$) y por lo tanto (NH, NK) esta contenido en $| H, K, N |^N$. ◆ .

Teorema 2.14.

Sea N un casi-anillo tal que $N^2 = N$, entonces:

$$\mathcal{A}(N) = D_1(N).$$

Demostración.

Puesto que $N^2 = N$, usando el lema anterior, tenemos:

$(NN, NN)^N = (N, N)^N$ está contenido en $|N, N, N|^N$, luego $\delta_1(N)$ está contenido en $D_1(N)$. ♦.

Acabamos con un corolario interesante de 2.14.

Corolario 2.15.

Si N es un casi-anillo unitario, entonces:

$$\mathcal{A}(N) = D_1(N).$$

Demostración.

Pues en este caso $N^2 = N$. ♦♦.

§ 3. EL IDEAL DISTRIBUIDOR EN CASI-ANILLOS DE POLINOMIOS

En este párrafo estudiamos el radical anillo de R[X]. Puesto que R[X] es un casi-anillo con identidad, tenemos como consecuencia de 2.15 que $\mathcal{A}(R[X]) = D_1(R[X])$, es decir, que el radical anillo en R[X] es precisamente el ideal distribuidor.

Demostramos que $D_1(R[X])$ es un ideal principal, es decir, como en teoría de anillos, generado por un único elemento. Es precisamente ese resultado el más importante de cuantos vamos a ver en este párrafo, que es adelantado en el siguiente teorema :

Teorema 3.1.

Se tiene :

$$D_1(R[X]) = \mathfrak{I}(\mid R[X], R[X], R[X] \mid) = \mathfrak{I}(1).$$

La demostración requiere una serie de lemas así como una buen número de resultados en casi-anillos de polinomios.

Lema 3.2.

(i) R está contenido en $D_1(R[X])$, (por lo tanto $\mathfrak{I}(1)$ está contenido en $D_1(R[X])$)

(ii) Los conjuntos 2R[X] y R están contenidos en $\mathfrak{I}(1)$.

Demostración.

(i) Sea $a \in R$, se tiene

$a \circ (0 + 0) - a \circ 0 + a \circ 0 = a - a - a = - a \in D_1(R[X])$,

en particular $1 \in \mathfrak{I}(1)$.

(ii) Puesto que $1 \in \mathfrak{I}(1)$, tenemos

$X^2 \circ (X + 1) - X^2 \circ X = 2X + 1 \in \mathfrak{I}(1)$, luego $2X \in \mathfrak{I}(1)$. Si $f(X) \in R[X]$, $2X \circ f(X) = 2f(X) \in \mathfrak{I}(1)$.

Sea $a \in R$, $aX \circ (1 + 0) - aX \circ 0 = a \in \mathfrak{I}(1)$. ♦.

Notas 3.3

- J.R. Clay y D.K. Doi,[C-D] han probado que

Si R = F es un cuerpo y L un ideal a la izquierda de F[X] con $L \cap F \neq (0)$,

(a) F está contenido en L

(b) Si cardinal de F es mayor que 2, entonces L = F[X].

Por lo tanto en estos casos tenemos que $\mathfrak{I}(1) = D_1(F[X]) = F[X]$. En terminos de radicales, el casi-anillo F[X] es $\mathcal{A}$-radical.

- J. L. Brenner [Br 1] ha probado que si $R = Z_{/2Z}$, $\mathfrak{I}(1)$ es el módulo sobre $Z_{/2Z}$ con base :

$$\mathfrak{I}(1) := \langle 1,\ X^{3n+1} + X,\ X^{3n-1} + X,\ X^{3n} + X^3 \ /\ n = 1,2,\ldots\ldots,\ \rangle.$$

Es fácil comprobar que el conjunto cociente tiene cardinal 4,

$$Z_{/2Z}[X] \ /\ \mathfrak{I}(1) = (\ \underline{0},\ \underline{X},\ \underline{X^3},\ \underline{X + X^3}\ )$$

y además

$$Z_{/2Z}[X] \ /\ \mathfrak{I}(1) \equiv Z_{/2Z} \oplus Z_{/2Z}.$$

Concluimos en este caso (usar 2.2.) que $\mathfrak{I}(1) = D_1(Z_{/2Z}[X]) \neq Z_{/2Z}[X]$ y por lo tanto el teorema en este caso.

El siguiente resultado es debido a J. L. Brenner [Br.2], y en él se describe $\mathfrak{I}(1)$ del casi-anilo Z[X]. Nosotros damos aquí una demostración mucho más corta, usando el segundo teorema de isomorfia, que la que aparece en [Br. 2].

Proposición 3.4.[Br. 2]

Si R = Z, se tiene:

$\mathfrak{I}(1)$ es el módulo sobre Z con base:

$$\mathfrak{I}(1) := \langle\ 1,\ 2X^n,\ X^{3n+1} + X,\ X^{3n-1} + X,\ X^{3n} + X^3 \ /\ n = 1,2,\ldots\ldots,\ \rangle.$$

Demostración

Es inmediato comprobar que la aplicación $f : Z[X] \to Z_{/2Z}[X]$ es un homomorfismo de casi-anillos, de hecho en [P-S] se demuestra :

Teorema.

(a) Sea $\phi : R_1[X] \to R_2[X]$ un homomorfismo de casi-anillos. Entonces ϕ / R_1 (ϕ restringido a R_1) es un homomorfismo de anillos $R_1 \to R_2$.

(b) Recíprocamente, si $\phi : R_1 \to R_2$., es un homomorfismo de anillos, entonces

$\Phi : R_1[X] \to R_2[X]$, definida

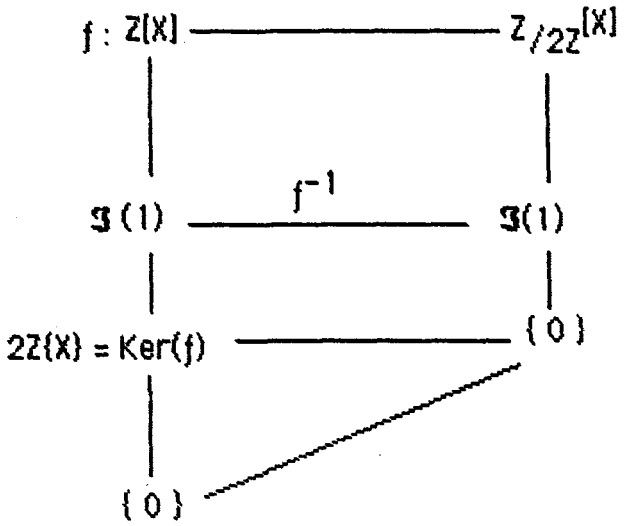
$\Phi(a_nX^n + \ldots\ldots + a_1X + a_0) = \phi(a_n)X^n + \ldots\ldots + \phi(a_1)X + \phi(a_0)$ es un homomorfismo de casi-anillos.

Es inmediato comprobar que Ker(h) = 2Z(X), donde

$2Z(X) = \{ a_nX^n + \ldots\ldots + a_1X + a_0 , a_i \in 2Z$, para todo $i = 0,1,\ldots,n$ y $n \geq 0 \}$

(ver Cap. III - § 1)

La correspondencia entre ideales que conserva las inclusiones que aparece en el segundo teorema de isomorfía y el hecho de que $\mathfrak{I}(1)$ de Z[X] es la imagen inversa completa de $\mathfrak{I}(1)$ en $Z_{/2Z}[X]$.



garantizan la tesis del teorema . ◆ .

Nota 3.5.

También en el caso R = Z es fácil comprobar que el cociente tiene cardinal 4: $Z[X] / \mathfrak{I}(1) = \{ \underline{0}, \underline{X}, \underline{X^3}, \underline{X + X^3} \}$

y además

$$Z[X] / \mathfrak{I}(1) \equiv Z_{/2Z} \oplus Z_{/2Z}.$$

Concluimos (usar 2.2.) que :

$\mathfrak{I}(1) = D_1(Z[X]) \neq Z[X]$ y por lo tanto el teorema 3.1 está probado para Z[X].

Distinguiremos los casos en los que la caracteristica del anillo R sea : 1) Un entero positivo impar. 2) Cero 0 3) Un entero positivo par. Comenzamos con :

Proposición 3.6.

Si $1 + 1 = 2$ es una unidad en R,

$$\mathfrak{I}(1) = D_1(R[X]) = R[X].$$

Demostración

Por el lema 3.2, $2X \in \mathfrak{I}(1)$, por hipotesis 2 es una unidad, llegamos a que $X \in \mathfrak{I}(1)$. ♦.

El recíproco de la proposición anterior no es cierta: basta tomar R =F, donde F es un cuerpo de característica 2 y de cardinal > 2, (ver 3.3)

El teorema 3.1 está probado cuando la característica de R es un entero positivo impar. Ahora consideraremos los otros casos.

El siguiente lema generaliza la proposición anterior.

Lema 3.7.

Para todo $a, b \in R$ se tiene

$$(a^2b + b^2a)X \in \mathfrak{I}(1).$$

Demostración

Por el lema 3.2 tenemos que $b \in \mathfrak{I}(1)$. Así

$X^3 \circ (aX + b) - X^3 \circ aX = (aX + b)^3 - a^3X^3 =$

$= 3a^2bX^2 + 3b^2aX + b^3 \in \mathfrak{I}(1)$. Nuevamente por 3.2, tenemos que $b^3, 3(a^2bX^2 + b^2aX) \in \mathfrak{I}(1)$, de donde $a^2bX^2 + b^2aX \in \mathfrak{I}(1)$.(*)

En particular $X^2 + X \in \mathfrak{I}(1)$. (tomar a = b = 1). Por lo tanto :

$a^2bX \circ (X^2 + X) = a^2bX^2 + a^2bX \in \mathfrak{I}(1)$. (* *) . Sumando (*) y (**) , tenemos :

$a^2bX^2 + b^2aX + a^2bX^2 + a^2bX = 2a^2bX^2 + a^2bX + b^2aX \in \mathfrak{I}(1)$.

Así que $(a^2b + b^2a)x \in \mathfrak{I}(1)$ ◆.

Nota 3.8.

El lema anterior puede ser utilizado para dar condiciones suficientes sobre R que garanticen que el casi-anillo R[X] sea $\mathcal{A}$- radical.

Denotemos por $\mathfrak{H}$ la clase de todos los anillos R para los cuales existen dos elmentos a, b tales que $a^2b + b^2a$ es una unidad en R.

En la clase $\mathfrak{H}$ están, por ejemplo, los anillos de característica un positiva impar y todos los cuerpos de cardinal > 2.

Así si $R \in \mathfrak{H}$, el casi-anillo R[X] es $\mathcal{A}$-radical, como de forma inmediata se prueba. ◆.

Tratamos ahora el caso de característica 0.

Observación 3.9.

Si la característica de R es cero, entonces:

$\mathfrak{I}(1) = D_1(R[X])$.

Demostración

Puesto que R es de característica 0, Z es un subanillo de R, por lo tanto $\mathfrak{I}(1) = D_1(Z[X])$ (ver 3.5) que es el Z-módulo de base:

$\mathfrak{I}(1)_{Z[X]} := \langle 1, 2X^n, X^{3n+1} + X, X^{3n-1} + X, X^{3n} + X^3 / n = 1,2,\ldots\ldots, \rangle$.

está contenido en $\mathfrak{I}(1)$.

Tenemos que probar que $D_1(R[X])$ está contenido en $\mathfrak{I}(1)$. Para ello, es suficiente comprobar que:

$X^n \circ (f(X) + g(X)) - (X^n \circ f(X) + X^n \circ g(X)) -$

$(f(X) + g(X))^n - f(X)^n - g(X)^n \in \mathfrak{I}(1)$, para todo $n \geq 1$ y para todo $f(X)$, $g(X) \in R[X]$.

Distinguimos dos casos :

A) Si 3 no divide a n.

Puesto $X^n + X \in \mathfrak{I}(1)$, $(X^n + X) \circ f(X) = f(X)^n + f(X) \in \mathfrak{I}(1)$. Similarmente obtenemos $g(X)^n + g(X)$, $[f(X)+g(X)]^n + [f(X) + g(X)] \in \mathfrak{I}(1)$. Sumando, $[f(X)+g(X)]^n + [f(X) + g(X)] - [f(X)^n + f(X) + g(X)^n + g(X)] =$

$= (f(X) + g(X))^n - f(X)^n - g(X)^n \in \mathfrak{I}(1)$.

B) Si 3 divide a n.

Primero lo demostramos para n = 3.

Sean $f(X) = a_r X^r + \ldots\ldots + a_i X^i + \ldots\ldots + a_1 X + a_0$,

$g(X) = b_m X^m + \ldots\ldots + b_j X^j + \ldots\ldots + b_1 X + b_0$ elementos de R[X], tenemos :

$(f(X) + g(X))^3 - (f(X)^3 + g(X)^3) =$

$3(a_r X^r + \ldots\ldots + a_i X^i + \ldots\ldots + a_1 X + a_0)^2 (b_m X^m + \ldots\ldots + b_j X^j + \ldots\ldots + b_1 X + b_0)$ **(1º)**

$+$

$3(b_m X^m + \ldots\ldots + b_j X^j + \ldots\ldots + b_1 X + b_0)^2 (a_r X^r + \ldots\ldots + a_i X^i + \ldots\ldots + a_1 X + a_0)$, **(2º)**

Es suficiente demostrar que :

(*) $a_i^2 b_j X^{2i+j} + b_j^2 a_i X^{2j+i} \in \mathfrak{I}(1)$, para $i \in \{ 0, \ldots\ldots, r \}, j \in \{ 0, \ldots\ldots, m \}$

Puesto que $2s(X) \in \mathfrak{I}(1)$ para cada $s(X) \in R[X]$.

Demostramos (*).

Observemos que $2i + j$ y $2j + i$ son ambos primos a 3 o ambos son divisibles por 3 ya que su suma es $(2i + j) + (2j + i) = 3(i + j)$, luego

$X^{2i+j} + X^{2j+i} \in \mathfrak{I}(1)$, entonces $(a_i^2 b_j X) o (X^{2i+j} + X^{2j+i}) =$

$= a_i^2 b_j X^{2i+j} + a_i^2 b_j X^{2j+i} = [+] \in \mathfrak{I}(1)$.

Por otro lado de 3.7.,

$(a_i^2 b_j + b_j^2 a_i) X o (X^{2j+i}) = a_i^2 b_j X^{2j+i} + b_j^2 a_i X^{2j+i} = [++] \in \mathfrak{I}(1)$.

Sumando [+] y [++], se tiene

$a_i^2 b_j X^{2i+j} + b_j^2 a_i X^{2j+i} \in \mathfrak{I}(1)$,

concluimos

$(f(X) + g(X))^3 - (f(X)^3 + g(X)^3) \in \mathfrak{I}(1)$,

y esta demostrado para n =3.

Si n = 3t.

Puesto que $X^n + X^3 \in \mathfrak{I}(1)$, tenemos :

$f(X)^n + f(X)^3$, $g(X)^n + g(X)^3$ y $[f(X)+g(X)]^n + [f(X)^3 + g(X)^3] \in \mathfrak{I}(1)$

por lo tanto :

$[f(X)+g(X)]^n + [f(X)^3 + g(X)^3] - [(f(X) + g(X))^3 - (f(X)^3 + g(X)^3)] +$

$+ [f(X)^n + f(X)^3] + [g(X)^n + g(X)^3] =$

$= (f(X) + g(X))^n - f(X)^n - g(X)^n \in \mathfrak{I}(1)$. ♦.

Nos queda por analizar cuando la característica de R es 2m, con m un entero positivo. Necesitamos la siguiente

Proposición 3.10.

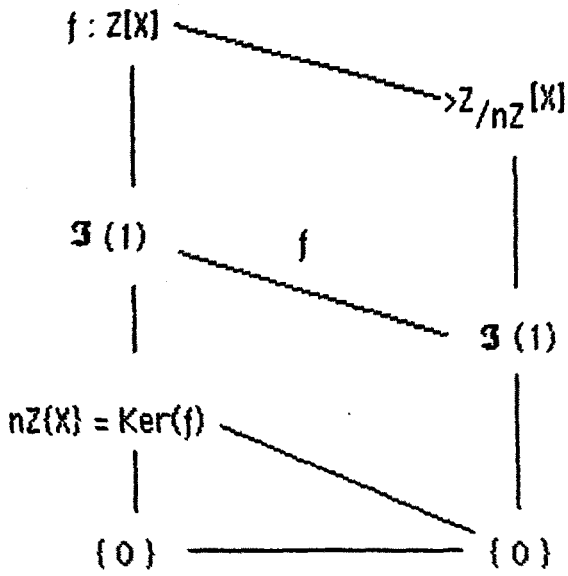
Sea $R = Z_{/nZ}$ donde n un entero positivo par. Entonces $\mathfrak{I}(1)$ es el módulo sobre $Z_{/nZ}$ con base :

$\mathfrak{I}(1) := \langle 1, 2X^n, X^{3n+1} + X, X^{3n-1} + X, X^{3n} + X^3 / n = 1,2,\ldots\ldots, \rangle$.

Demostración.

Consideramos el homomorfismo $f : Z[X] \to Z_{/nZ}[X]$ (3.4.)

Puesto que n es par el $Ker(f) = nZ[X]$ esta contenido en $\mathfrak{I}(1)$, usar el segundo teorema de isomorfia :



Ahora el resultado es inmediato. ♦ .

Observación 3.11.

Si La caracteristica de R es un entero positivo par, entonces :

$\mathfrak{I}(1) = D_1(R[X])$.

Demostración.

El razonamiento para la prueba es análogo al hecho en 3.9 y en este caso utilizar 3.10 . ♦ .

Esto completa la demostración del teorema 3.1.

Observamos que la clase de anillos R, para los cuales los casi-anillos R[X] son $\mathcal{A}$-radicales (es decir $R[X]_{/\mathfrak{J}(1)} = (0)$) es una clase muy amplia (ver 3.8).

Sin embargo, si nos restringimos a la parte zero-simétrica de R[X], es decir a $R_0[X]$, nos encontramos con la sorprendente respuesta de que nunca los casi-anillos $R_0[X]$ son $\mathcal{A}$-radicales. Para demostrar esto necesitamos las siguientes :

Definición 3.12.

Para cada entero no negativo, n, pongamos

$J_n[X]_0 = (a_m X^m + \ldots\ldots + a_n X^n \,/\, m \geq n \text{ y los } a_i \in R)$

Proposición 3.13.

Se tiene :

(i) $J_n[X]_0$ es un ideal de $R_0[X]$.

(ii) $D_1(R_0[X])$ esta contenido en $J_2[X]_0$.

Demostración

(i) Es una simple comprobación.

(ii) Basta observar que la aplicación, $F : R_0[X] \to R$,

definida de la forma siguiente :

$F(a_m X^m + \ldots\ldots + a_2 X^2 + a_1 X) = a_1$, es un epimomorfismo de casi-anillos, aplicando el teorema del homomorfismo :

$R_0[X]_{/\ Ker(\ F)} \equiv R$, pero el Ker(F) es exactamente $J_2[X]_0$. La demostración acaba usando 2.3. ♦ .

Terminamos este párrafo y así el capítulo con un resultado acerca del ideal distribuidor en $R_0[X]$.

Proposición 3.14.

Sea R un anillo tal que $1 + 1 = 2$ es una unidad de R entonces :

$$J_2[X]_0 = D_1(R_0[X])$$

Demostración.

Es suficiente probar que $X^n \in D_1(R_0[X])$, para $n \geq 2$.

Para $n \geq 1$, tenemos :

$X^2 \circ (X + X^n) - (X^2 + X^{2n}) = 2X^{n+1} \in D_1(R_0[X])$.

Por hipótesis llegamos a que $X^{n+1} \in D_1(R_0[X])$. ◆◆.

CAPITULO III.

IDEALES DE Z[X] Y DE $Z_{/nZ}[X]$. IDEALES COMPLETOS DE R[X].

En el libro Near- Rings de Gunter Pilz, en la pagina 228, dice : " All maximal ideals or all full ideals of Z[X] are not known ".

En este capítulo investigamos los ideales de Z[X], dando una descripción completa de los ideales maximales . Aplicando los teoremas de isomorfía obtenemos como consecuecia los ideales maximales de $Z_{/nZ}[X]$.

Por último, en el párrafo tres, estudiamos los ideales completos y describimos cómo son todos los ideales maximales del anillo de composición (R[X], + , o, .).

§ 1. IDEALES EN Z[X].

Comenzamos este párrafo con algunas definiciones y resultados conocidos en la literatura.

Definición. 1.1. [P]

1.1-1 Todo polinomio f(X) $\in$ R[X], f(X) define una aplicación de R en

R,

$$\underline{f}(X) : R \to R$$

$$a \dashrightarrow f(X) \circ r .$$

$\underline{f}(X)$ es conocida como la función polinómica inducida por f(X).

1.1-2 Se define $P(R) := \{ \underline{f}(X) \ / \ f(X) \in R[X] \}$. (P(R), +, o) es un subcasi-anillo de (M(R), +, o).

Definición y Proposición. 1.2. [P]

La correspondencia $h : R[X] \to P(R)$, definida

$h(f(X)) = \underline{f}(X)$ es un homomorfismo de casi-anillos. En general de núcleo no trivial.

Demostración

[P]. ◆.

Los primeros pasos en orden a encontrar los ideales maximales del casi- anillo R[X] fueron dados por J.R. Clay y K. Doi en 1973.

Teorema 1.3. (J.R. Clay y K. Doi) [C-D]

(a) Si R = F es un cuerpo infinito, [0] es el único ideal maximal de F[X].

(b). Si R = F es un cuerpo finito no isomorfo a $Z_{/2Z}$, entonces $Ker(h) = \{ f(X) \ / \ \underline{f}(X) = \underline{0} \}$ es el único ideal maximal de F[X].

Además J.R. Clay y K. Doi dieron una descripición de estos ideales $Ker(h) = \{ (X^p - X) f(X) / f(X) \in F[X] \}$ donde el cardinal(F) = p^k

Demostración

[C-D], [P]. ◆ .

Trabajos contemporáneos a los de J.R. Clay y K. Doi son los publicados en 1.974 por J.L.Brenner [Br1] y por G.Strauss, [S]. J.L.Brenner determinó los ideales maximales de $Z_{/2Z}[X]$.

Como es usual en Algebra la característica 2 en un anillo es causa casi siempre de complicaciones. La estructura de los ideales maximales en el cuerpo finito $Z_{/2Z}$ no es tan simple como en los otros cuerpos, como así lo muestra el siguiente resultado.

Teorema 1.4. (J.L.Brenner)[Br 1]

$Z_{/2Z}[X]$ tiene exactamente dos ideales maximales :

$V(1) := \{ f(X) / \underline{f}(X)$ es una aplicación constante $\} = \{ p(X) / p(0) = p(1) \}$.

Se demuestra que V(1) es un ideal principal generado por $X^3 + X + 1$,

$$V(1) = \Im(X^3 + X + 1).$$

T(1) , el ideal generado por X^3 . $T(1) = \Im(X^3)$.

Ademas T(1) y V(1) son módulos sobre $Z_{/2Z}$ con la siguientes bases:

$$T(1) = < 1, X^{3n+1} + X, X^{3n-1} + X, X^3 / n = 1,2,..... > \text{ y}$$

$$V(1) = < 1, X^n + X / n = 1,2,..... >$$

Otras caracterizaciones de V(1) y T(1) pueden verse en [St] .

Demostración.

[Br 1] . ◆ .

Nota 1.5.

Es inmediato comprobar que $\mathfrak{J}(1)$, el ideal distribuidor de $Z_{/2Z}[X]$ (Cap. II), es precisamente la interseción de los ideales maximales de $Z_{/2Z}[X]$, $\mathfrak{J}(1) = T(1) \cap V(1)$. Como observamos en Cap.II- 3.4, se tiene :

$$Z_{/2Z}[X]/\mathfrak{J}(1) \equiv Z_{/2Z} \oplus Z_{/2Z}$$

y además

$$Z_{/2Z}[X]/V(1) \equiv Z_{/2Z} \text{ y } Z_{/2Z}[X]/T(1) \equiv Z_{/2Z}$$

luego

$$Z_{/2Z}[X]/T(1) \cap V(1) \equiv Z_{/2Z}[X]/T(1) \oplus Z_{/2Z}[X]/V(1),$$

concluímos que el anillo cociente con respecto al ideal distribuidor es isomorfo a la suma directa de los anillos cocientes por los ideales maximales.

En el caso general la observación de arriba no es cierta : basta tomar $R = Z_{/pZ}$, donde p es un primo distinto de 2, $\mathfrak{J}(1) = R[X]$ (Cap.II-3.2) ; por otra parte R[X] tiene en este caso un único ideal maximal (1.3) .

Establecemos ahora algunos ideales conocidos en la literatura.

Definición. 1.6. [L-N] [P]

Para cada ideal I de R, definimos :

(a) $I(X) := \{ a_n X^n + \ldots\ldots + a_i X^i + \ldots\ldots + a_1 X + a_0 \;/\; a_i \in I,\ n \geq 0. \}$

(b) $I\langle X\rangle := \{ f(X) \ / \ f(X) \circ r = f(r) \in I$, para todo $r \in R \}$

Es comprobación elemental demostrar que $I[X]$ y $I\langle X\rangle$ son ideales de $R[X]$.

La siguiente interesante proposición será muy usada en lo sucesivo del capítulo.

Proposición 1.7.

Sea I un ideal de R, se tiene :

(i) $I[X]$ está contenido en $I\langle X\rangle$.

(ii) Sean I_1, I_2 ideales de R tal que I_1 está contenido en I_2. Entonces $I_1[X]$ está contenido en $I_2[X]$ e $I_1\langle X\rangle$ está contenido en $I_2\langle X\rangle$. Además, si I_1 está estrictamente contenido en I_2, lo mismo sucede con los ideales $I_1[X]$ e $I_1\langle X\rangle$ de $R[X]$.

(iii) Si $R = Z$ e I es un ideal propio de Z, entonces $I[X]$ está estrictamente contenido en $I\langle X\rangle$.

(iv) Si I es un ideal de Z, entonces $I[X]$ es un ideal principal de $Z[X]$.

Demostración

(i) Sea $f(X) = a_nX^n + \ldots\ldots + a_iX^i + \ldots\ldots + a_1X + a_0 \in I[X]$ y sea $r \in R$, entonces $f(X) \circ r = f(r) = a_nr^n + \ldots\ldots + a_ir^i + \ldots\ldots + a_1r + a_0 \in I$, puesto que los $a_i \in I$.

(ii) La primera afirmación es una comprobación rutinaria. Para la segunda, supongamos que I_1 está estrictamente contenido en I_2. Sea $a \in$

I_2 pero $a \notin I_1$, entonces $aX \in I_2(X)$, pero $aX \notin I_1(X)$. El mismo elemento sirve para demostrar lo restante.

(iii) Sea I un ideal de Z, entonces $I = nZ$ para algún n natural .

Distinguiremos varios casos para demostrar (iii) a la vez que ilustraremos el contenido estricto con ejemplos variados.

1º) Si $n = p$ donde p es un número primo, $X^p - X \in pZ< X >$; en efecto , para todo $a \in Z$, se tiene que $a^p - a \equiv 0(\text{mod } p)$. Por otra parte $X^p - X \neq p(f(X))$, para todo $f(X) \in pZ[X]$, puesto que $X^p - X$ es monico, luego $X^p - X \notin pZ(X)$.

2º) Si $n = p^r$, con $r \geq 1$. . Es conocido que el grupo de las unidades de $Z_{/p^rZ}$ tiene cardinal $\Phi(p^r)$, donde Φ es la función de Euler.

Todo elemento $a \in Z_{/p^rZ}$ satisface una de las dos ecuaciones $X^r = 0$ o $X^{\Phi(p)} - 1 = 0$ en el anillo $Z_{/p^rZ}$, luego para todo $a \in Z_{/p^rZ}$ tenemos que $a^r(a^{\Phi(p)} - 1) \equiv 0(\text{mod } p^r)$. Concluimos $X^r(X^{\Phi(p)} - 1) \in p^rZ < X >$, pero obviamente $X^r(X^{\Phi(p)} - 1) \notin p^rZ(X)$ pues es un polinomio mónico.

3º) Si $n = p_1^{r_1} \ldots\ldots p_k^{r_k}$, con $k \geq 2$. El polinomio

$[p_1^{(r_1-1)} \ldots\ldots p_k^{r_k}] X^{p_1} - [p_1^{(r_1-1)} \ldots\ldots p_K^{r_k}] X =$

$= [p_1^{(r_1-1)} \ldots\ldots p_k^{r_k}] (X^{p_1} - X)$, es obvio que no pertenece a nZ(X). Si $a \in Z_{/nZ}$, tenemos que $[p_1^{(r_1-1)} \ldots\ldots p_k^{r_k}] (a^{p_1} - a) = [p_1^{(r_1-1)} \ldots\ldots p_k^{r_k}] t p_1 \equiv 0(\text{mod } n)$.

(iii) Sea $I = nZ$ un ideal de Z, tenemos que $nX \in nZ(X)$. Demostramos que todo elemento de nZ(X) está en $\mathfrak{I}(nZ)$.

Sea $r(X) \in Z[X]$, entonces $nX \circ (r(X) + 0) - nX \circ 0 = nr(X) - n0 = nr(X) \in g(nZ)$. ♦ .

Lema 1.8.

Los módulos sobre Z con las siguiente bases :

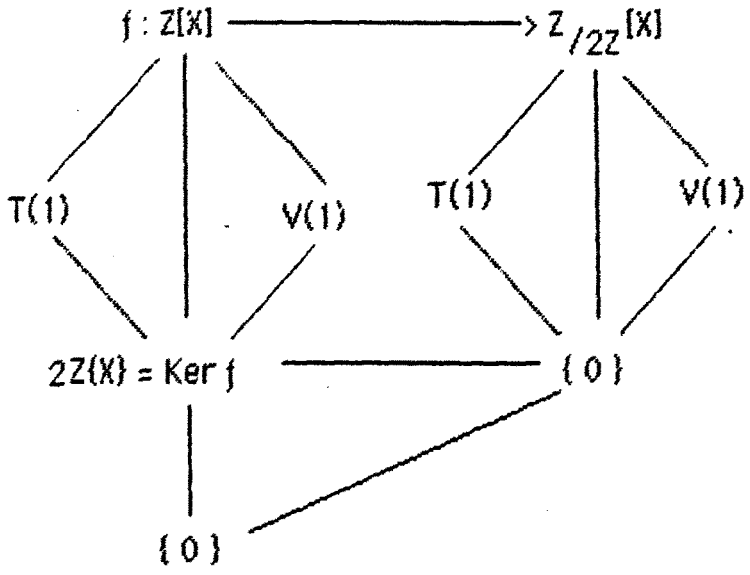
$V(1) := \langle 1,\ 2X^n,\ X^n + X \ / \ n = 1, 2, \ldots\ldots\ldots \rangle$

$T(1) := \langle 1,\ 2X^n,\ X^{3n+1} + X,\ X^{3n-1} + X,\ X^{3n} \ / \ n = 1, 2, \ldots\ldots \rangle$

son ideales de Z[X].

Demostración

Considerar la aplicación canónica $f : Z[X] \to Z_{/2Z}[X]$ que es un homomorfismo y aplicar el 2º teorema de isomorfía . Notemos ahora que V(1) y T(1) son las imagenes inversas de los ideales V(1) y T(1) de $Z_{/2Z}[X]$, (ver 1.4.)



Con esto se acaba la demostración. ♦ .

Nota 1.9.

J. L. Brenner en su articulo " Composition algebras of polynomials " aparecido a finales de 1.985, obtiene una serie de resultados a cerca de la estructura ideal de Z[X]. Entre otros el siguiente :

Teorema :

Los ideales de Z[X] son :

para cada $c \in Z$, $cZ[X]$, $T(c)$, $V(c)$, $J(c)$ donde

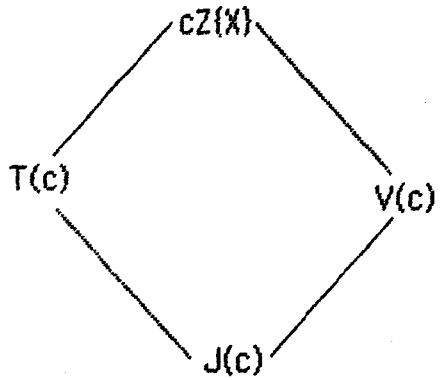
$T(c) = cT(1)$, $V(c) = cV(1)$ ($T(1)$ y $V(1)$ son los dados en lema 1.8). Con las siguiente relaciones de inclusiones :

Si c y d $\in Z$ tal que c divide a d, entonces :

J(d) está contenido en J(c),

T(d) está contenido en T(c),

V(d) está contenido en V(c) , junto con las relaciones de inclusión del diagrama siguiente :

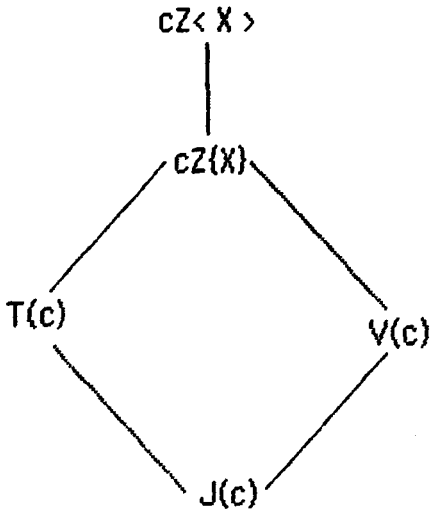


J. L. Brenner, en su articulo no da la demostración, dejándola para el lector.

El ideal $cZ< X >$ no aparece entre los que enumera el teorema anterior, de hecho, por la proposición 1.8., tenemos que cZ[X] esta estrictamente contenido en $cZ< X >$. Quiza el teorema deba decir :

¿ Los ideales de Z[X] son :

Para cada $c \in Z$, $cZ[X]$, $T(c)$, $V(c)$, $J(c)$, con las relaciones de inclusión dadas en el teorema junto con la relación de inclusión dada por el diagrama siguiente :



??

Aún no se conoce la estructura ideal de Z[X].

Pasamos ahora al estudio de los ideales maximales de Z[X].

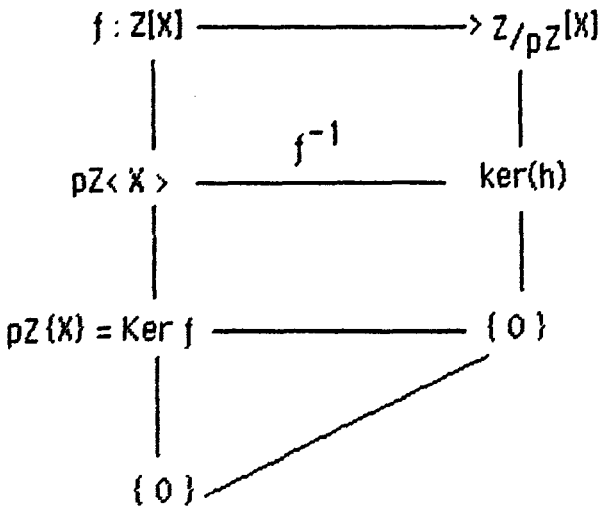
Proposición. 1.10.

(a) Sea p un primo impar hay un único ideal maximal de Z[X] que contenga al ideal $pZ[X]$: $pZ< X >$.

(b) Hay exactamente dos ideales maximales de Z[X] que contengan al ideal $2Z[X]$: $V(1)$ y $T(1)$.

Demostración

(a) Basta considerar el homomorfismo canónico de casi-anillos ƒ,



Téngase en cuenta el segundo teorema de isomorfía y que la imagen inversa del único ideal maximal de $Z_{/pZ}[X]$ (ver 1.3.) es precisamente pZ< X >.

(b) Considerar ahora , tambien , el homomorfismo canónico ƒ, ƒ : $Z[X] \to Z_{/2Z}[X]$, usar de nuevo el segundo teorema de isomorfía y el hecho que $Z_{/2Z}[X]$ tiene dos únicos ideales maximales (1.4). Para acabar, usar 1.8. ♦ .

En orden a encontrar todos los ideales maximales de Z[X], necesitamos la siguiente definición.

Definición 1.11.

Para cada ideal I de R[X], definimos :

I_C : = { f(X) o r = f(r) / para todo f(X) ∈ I y para todo r ∈ R }

Proposición 1.12.

Para cada ideal I de R[X], se tiene :

(i) $I_c = I \cap R$ es un ideal de R.

(ii) El ideal I está contenido en $I_c < X >$.

(iii) Sean I_1 y I_2 ideales de R[X], tal que I_1 esta contenido en I_2 , entonces $(I_1)_c < X >$ lo está en $(I_2)_c < X >$.

Demostración

(i) Sea $r \in I_c$, entonces $r = f(X) \circ s \in I$, par algun $f(X) \in I$ y para algún $s \in R$. Reciprocamente, sea $a \in I \cap R$, entonces $a \circ 0 = a \in I_c$. Por último I_c es un ideal. En efecto, si $a \in I_c$ y $b \in R$,

$bX \circ (0 + a) - bX \circ 0 = ba \in I_c$.

(ii) Sea $f(X) \in I$, entonces $f(X) \in I_c < X >$ si y solo si para toda $a \in R$ $f(X) \circ a = f(a) \in I_c$.

(iii) Es inmediata. ◆ .

Nota 1.13.

El contenido en (ii) de la proposición anterior es, en general, un contenido estricto. En efecto, si $R = Z$ e $I = pZ[X]$, entonces $I_c = pZ$, pero $pZ<X>$ contiene estrictamente a $pZ[X]$.

Además no hay ninguna relación de contenido entre I y $I_c[X]$, los ejemplos anteriores sirven para ilustrar este hecho.

Lema 1.14.

Sea I un ideal maximal de Z[X], entonces $I_c \neq 2Z$.

Demostración

En efecto si se verificára que $I_c = 2Z$, por la proposición 1.12. tendríamos que $I = I_c< X > = 2Z < X >$, que no es un ideal maximal usando 1.10- (b). ♦.

Teorema 1.15.

Cada ideal maximal de Z[X] contiene un ideal de la forma pZ(X), donde p es un número primo.

Demostración

Sea I un ideal maximal de Z[X], enonces $I_c = I \cap Z = nZ$, para algún n; Distinguimos casos:

(a) Si n = 0, entonces $I_c = \{ 0 \}$; sea $f(X) \in I$, $f(X) \circ r \in I_c = \{ 0 \}$, para todo $r \in Z$, luego $f(X) = 0$ y $I = \{ 0 \}$, contradición.

(b) Si n = 1, entonces $I_c = Z$ luego $1 \in I$ así :

$X^2 \circ (X + 1) - X^2 = 2X \in I$, luego 2Z(X) esta contenido en I.

(c) Si $n \neq 0$, $n \neq 1$ y $n \neq 2$ (ver lema 1.14), tenemos que I esta contenido en $nZ< X >$, puesto que I maximal $I = nZ< X >$, pero n es necesariamente primo; en efecto si n = st, entonces nZ esta contenido en tZ, usando la proposición 1.8. tendríamos que I esta contenido en $tZ< X >$, contradición. Luego n es primo . ♦.

Obtenemos todos los ideales maximales de Z[X].

Corolario 1.16.

Los ideales maximales de Z[X] son : $pZ< X >$, para todo primo $p \neq 2$, $V(1)$ y $T(1)$.

Demostración

1.11 y 1.15. ♦.

Definición. 1.17.

El radical de Jacobson del R[X] es la interseción de todos los ideales maximales y le denotaremos por Rad(R[X]).

Corolario 1.18.

Se tiene:

$$Rad(Z[X]) = \{ 0 \}.$$

Demostración

Sea $f(X) \in Rad(Z[X])$, entonces $f(X) \circ a = f(a) \in pZ$ para todo p , $p \neq 2$, y para todo $a \in Z$, luego $f(X) = 0$. ♦♦.

§ 2. IDEALES MAXIMALES DE $Z_{/nZ}[X]$.

En este párrafo determinamos todos los ideales maximales del casi-anillo $Z_{/nZ}[X]$.

El siguiente resultado, debido a H. Kautschitsch, encuentra los ideales maximales para algunos $Z_{/nZ}[X]$.

Teorema 2.1.(H. Kautschitsch)

Sea R un anillo satisfaciendo la siguiente propiedad : (p*)

" Existen unidades u, v de R tal que u + v o u - v es una unidad " .

Entonces los ideales maximales de R[X] son todos de ls forma $J< X >$ donde J es un ideal maximal de R.

Demostración.

[K2.] . ◆ .

Nota 2.2.

El resultado anterior determina todos los ideales maximales para una extensa clase de anillos. Así por ejemplo todos los cuerpos de cardinal mayor que 2, satisfacen la propiedad (P*).

Si n es un número impar, es inmediato comprobar que $Z_{/nZ}$ satiaface la propiedad (P*).

Si n es un número par, entonces $Z_{/nZ}$ no satisface la propiedad (P*).

El siguiente resultado encuentra todos los ideales maximales de $Z_{/nZ}[X]$ para todo n

Teorema. 2.3.

(a) Si $n = p_1^{r_1}.....p_k^{r_k}$, donde todos los primos $p_i \neq 2$, para todo i, entonces los ideales maximales de $Z_{/nZ}[X]$ son :

$p_i Z_{/nZ}< X >$ para todo i= 1,.....,k.

(b) Si $n = 2^s p_1^{r_1}.....p_k^{r_k}$ donde todos los primos $p_i \neq 2$, para todo i, y donde $s \geq 1$, entonces los ideales maximales de $Z_{/nZ}[X]$ son:

$p_i Z_{/nZ}< X >$ para i= 1,.....,k. y los módulos V(1), T(1) sobre $Z_{/nZ}$ con las siguientes bases :

$V(1) : = < 1, 2X^n , X^n + X \ / n = 1, 2, ... >$

$T(1) : = < 1, 2X^n, X^{3n+1} + X , X^{3n-1} + X , X^{3n} \ / n = 1, 2, ... >$.

Demostración

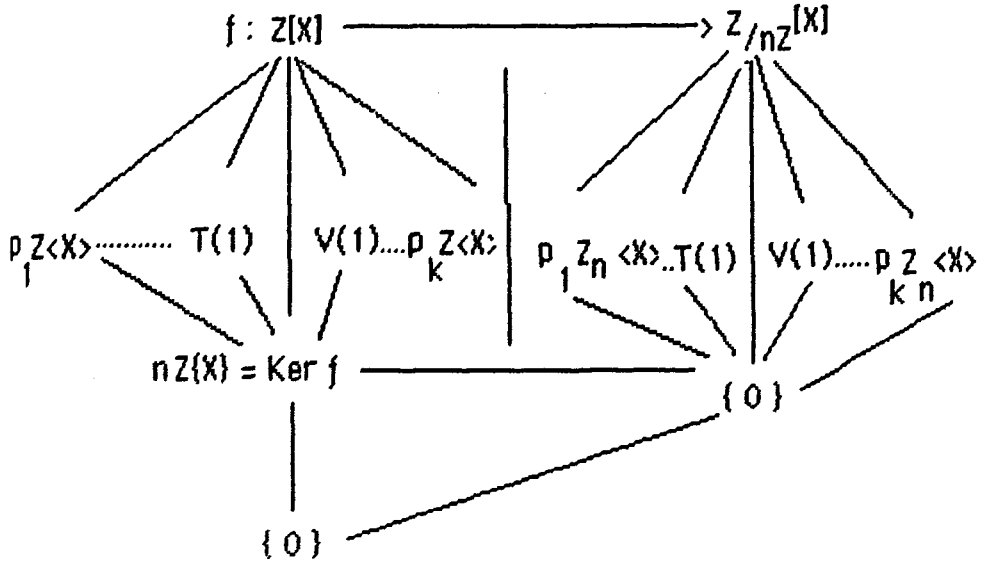
Hacemos el caso (b), el caso (a) se demuestra de forma analoga. Si $n = 2^s p_1^{r_1}.....p_k^{r_k}$ donde todos los primos $p_i \neq 2$, para i =1,..., k, y donde $s \geq 1$, los ideales maximales de Z[X] que contienen al ideal nZ[X] (ver parrafo 1) son todos de la forma :

$p_i Z< X >$ para i = 1,.....,k. y los módulos V(1), T(1) sobre Z con las siguientes bases :

$V(1) : = < 1, 2X^n , X^n + X \ / n = 1, 2, ... >$

$T(1) := \langle\ 1,\ 2X^n,\ X^{3n+1} + X,\ X^{3n-1} + X, X^{3n} \ /\ n = 1, 2, \ldots\ldots \rangle$.

Considerando el homomorfismo canonico f, y aplicando el segundo teorema de isomorfía :



Sea acaba la demostración aplicando la correspondencia entre los ideales. ◆ .

Similar al caso de Z[X], obtenemos el corolario en relación con el radical de Jacobson, ahora mientras que Rad(Z[X]) = { 0 } demostramos que en este caso siempre es distinto del ideal { 0 }.

Corolario 2.5.

Se tiene:

Rad($Z_{/nZ}[X]$) ≠ { 0 }, para todo n ≥ 2.

Demostración

Si $n = p_1^{r1}.....p_k^{rk}$, donde todos los primos $p_i \neq 2$, para i=1,.., k,

entonces el polinomio:

$f(X) = (p_1^{r_1-1} \ldots\ldots p_k^{r_k}) X^p - (p_1^{r_1-1} \ldots\ldots p_k^{r_k}) X \in p_i Z_{/nZ}\langle X \rangle$ para todo i= 1,.....,k. y $f(X) \neq 0$.

Si $n = 2^s p_1^{r_1} \ldots\ldots p_k^{r_k}$ donde todos los primos $p_i \neq 2$, para i=1,..., k, y donde $s \geq 1$; el polinomio :

$f(X) = (2^s p_1^{r_1-1} \ldots\ldots p_k^{r_k})X^p - (2^s p_1^{r_1-1} \ldots\ldots p_k^{r_k}) X \in p_i Z_{/nZ}\langle X \rangle$ para i= 1,.....,k.

Además $f(X) \neq 0$ y $f(X) = 2g(X)$ con $g(X) \in Z_{/nZ}[X]$, luego :

$f(X) = 2g(X) \in \mathfrak{I}(1) = V(1) \cap T(1)$. ◆◆ .

§ 3. IDEALES DEL ANILLO DE COMPOSICION (R[X], +, ., o)

Dentro de los ideales de R[X], destacamos aquellos que son ideales en el anillo de polinomios (R[X], +, .).

Definición. 3.1. [P]

Sea I un ideal de R[X], diremos que es un ideal completo si es un ideal en el anillo de polinomios (R[X], +, .).

Algunos autores a los ideales completos les llaman ideales de composición, esto viene determinado por la siguiente :

Definición 3.2. [P]

Un conjunto A dotado de tres operaciones binarias " + ", " . ", " o " se dice que es un anillo de composición (algunos autores dicen algebra tri-operación) si verifica :

(a) (A, +, .) es un anillo.

(b) (A, +, o) es un casi-anillo.

(c) Para todo $a_1, a_2, a_3 \in A$: $(a_1 . a_2) \circ a_3 = (a_1 \circ a_3).(a_2 \circ a_3)$.

Los siguientes ejemplos ilustran estan definición.

Ejemplos 3. 3.

(a) El conjunto de todas las aplicaciones de un anillo R en R, junto con la adición, la multiplicación y la composición de aplicaciones es un anillo

de composición.

(b) El casi-anillo de polinomios R[X] , junto con la multiplicación de polinomios forma un anillo de composición, que le denotaremos por (R[X], +, . o).

Nótese que los ideales completos de R[X] son precisamente los ideales del anillo de composición (R[X], +, ., o).

Definición 3.4.

Un ideal de (R[X], +, . o) es maximal si es un elemento maximal en el conjunto de los ideales de (R[X], +, ., o) distintos de R[X].

Damos ahora unos ejemplos de ideales completos.

Ejemplos 3.5. [L - N]

Para cada ideal I de R, los ideales de R[X] : I< X > , I(X) son ideales completos .

A partir de estos ideales construimos los siguientes interesantes ideales completos.

Proposición 3.6.

Sea I un ideal de R y t ∈ R, entonces t(I(X)) = (tI)(X) y t(I< X >) son ideales completos de R[X].

Demostración

La igualdad de la proposición es una comprobación rutinaria. Demostramos que t(I< X >) es un ideal.

Demostraremos que $t(I< X >)$ es un ideal de R[X], puesto que es elemental que es un ideal del anillo de polimomios (R[X], +, .)

Sea $tf(X) \in t(I< X >)$ y sea $g(X) \in R[X]$, entonces :

$tf(X) \circ g(X) = t(f(X) \circ g(X)) \in t(I< X >)$.

Sean $g(X)$, $h(X) \in R[X]$ y $tf(X) \in t(I< X >)$, tenemos que demostrar :

$$g(X) \circ (h(X) + tf(X)) - g(X) \circ h(X) \in t(I< X >) ,$$

Sea $g(X) = a_n X^n + \ldots\ldots\ldots + a_1 X + a_0$, demostramos que para todo m = 1,....,n , se verifica $a_m X^m \circ (h(X) + tf(X)) - (a_m X^m \circ h(X)) \in t(I< X >)$,

$a_m X^m \circ (h(X) + tf(X)) - (a_m X^m \circ h(X)) =$

$= a_m (h(X) + tf(X))^m - a_m(h(X))^m =$

$= a_m(h(X))^m + [tf(X) \square + \ldots\ldots + tf(X) \square + \ldots\ldots + t^m(f(X))^m] - a_m(h(X))^m =$

$= tf(X) \square + \ldots\ldots + tf(X) \square + \ldots\ldots + t^m(f(X))^m$, donde los $\square$ son polinomios de R[X].

Puesto que $I< X >$ es un ideal completo y $f(X) \in I< X >$, concluimos que $a_m (h(X) + tf(X))^m - a_m(h(X))^m \in t(I< X >)$ para todo m y como consecuencia obtenemos que $t(I< X >)$ es un ideal completo para todo $t \in R$. ♦ .

Nota 3.7.

Está claro que $t(I< X >)$ está contenido en $I< X >$ con contenido estricto si $t \neq 1$. Por otra parte no es cierto en general que se tenga una igualdad entre los ideales $t(I< X >)$ y $(tI)< X >$; siempre $t(I< X >)$ está contenido en $(tI)< X >$, pero la otra inclusión no es cierta : tomar como R = Z, I = 3Z , t = 2, tenemos que tI= 6Z , el polinómio mónico $f(X) = X (X - 1) \ldots\ldots(X - 5) \in (tI)< X >$ pero no está en $t(I< X >)$, de hecho $t(I< X >)$ siempre

está contenido en (tR)[X].

Existen ideales de R[X] que no son ideales completos. Por ejemplo, si tomamos en R = Z, los ideales J(1), V(1) y T(1) no son ideales completos , pues el 1 pertenece a todos, pero todos son distintos del total.

Reciprocamente, existen ideales del anillo de polinomios que no son ideales de R[X]. (por ejemplo el ideal generado por X). .

El siguiente resultado conocido relaciona los ideales del anillo de polinomios con los ideales a la izquierda de R[X].

Teorema 3.8. [L-N]

Cada ideal del anillo de polinomios (R[X], +, .) es un ideal a la izquierda de R[X].

Demostración

[L - N], [P]. ♦.

Teorema 3.9.

Sea R un anillo de característica positiva distinta de 2 . Los ideales a la izquierda de R[X] son exactamente los ideales del anillo de polinomios (R[X], +, .).

Demostración

Sea I un ideal de R[X] y sean $f(X) \in I$, $g(X) \in R[X]$, entonces tenemos

$X^2 \circ (g(X) + f(X)) - X^2 \circ g(X) = 2f(X)g(X) \in I$, por hipotesis $1/2 \in R$,

luego $1/2 X \circ 2f(X)g(X) = f(X)g(X) \in I$, para acabar usar el teorema 3.8.♦.

Nota 3.10.

E. G. Strauss fue el referee del artículo de J. L. Brenner (2). El publicó a continuación unos interesantes resultados en relación con los ideales completos sobre cuerpos :

Teorema(S)

Sea F un cuerpo finito. Cada ideal de F[X] es un ideal completo si y solamente si la característica de F es distinta de 2. (La demostración que aparece en [P] tiene una errata).

En orden a llegar a una respuesta acerca de la representación del anillo de composicion (R[X], +, ., o) como un producto subdirecto de anillos de composición simples, tendremos que determinar los ideales maximales.

Pasamos ahora a estudiar los ideales maximales del anillo de composición (R[X], +, ., o)

Lema 3.11.

Todo ideal de composición de (R[X], +, . o) distinto de R[X] esta contenido en un ideal maximal.

Demostración

La demostración es la tipica, usando el lema de Zorn. ♦.

Establecemos el resultado mas destacable de este párrafo acerca de los ideales maximales completos de R[X].

Teorema 3.12.

Los ideales maximales del anillo de composición (R[X], +, ., o) son todos de la forma $I\langle X\rangle$ donden I es un ideal maximal de R.

Demostración

Sea I un ideal maximal de R, demostramos que $I\langle X\rangle$ es maximal. En efecto, si J es un ideal que contiene estrictamente a $I\langle X\rangle$, tomamos un $f(X) \in J$ con $f(X) \notin I\langle X\rangle$, luego existe un $r \in R$ tal que $f(r) \notin I$. Por 1.12. J_C contiene a $(I\langle X\rangle)_C = I$, ademas $f(r) \in J_C$, por la maximidad de I, tenemos que $J_C = R$, luego $1 \in J_C$, $J_C = J \cap R$, tenemos que $1 \in J$, concluimos que J = R[X].

Reciprocamente sea J un ideal maximal del anillo de composición R[X], por 1.12. tenemos que J esta contenido en $J_C\langle X\rangle$; J maximal tenemos que $J_C\langle X\rangle = R[X]$ o $J_C\langle X\rangle = J$.

Si $J_C\langle X\rangle = R[X]$, tenemos que $1 \in J_C = J \cap R$ por lo tanto J = R[X], contradición.

Si $J_C\langle X\rangle = J$, tendremos que demostrar que J_C es un ideal maximal de R. En efecto, sea I un ideal de R que contiene estrictamente a J_C, entonces $J_C\langle X\rangle = J$ esta contenido en $I\langle X\rangle$, de nuevo haciendo uso de la maximidad de J, tenemos que $I\langle X\rangle = R[X]$, por lo tanto $1 \in I$, de donde I = R; concluyendo que J_C es maximal. ♦.

El siguiente corolario contiene algunos resultados ya conocidos para el caso de cuerpos.

Corolario 3.13.

(i) Si R = F, un cuerpo. El anillo de composición (F[X], +, ., o) tiene un único ideal maximal que es precisamente :

$$Ker(h) = \{ f(X) / \underline{f}(X) = \underline{0} \}$$

(ii) Si R = Z. Los ideales maximales del anillo de compósición son todos de la forma : $pZ< X >$, donde p recorre el conjunto de los números primos.

(iii) Si $R = Z_{/nZ}$ donde $n = p_1^{r1}.....p_k^{rk}$. Los ideales maximales del anillo de composición ($Z_{/nZ}[X]$, +, ., o), son :

$$p_i Z_{/nZ}< X >, \text{ para todo } i = 1, 2,....., k$$

Demostración

[3.9] . ◆ .

Nota 3.14.

El ideal maximal $2Z< X >$ del anillo de composición no es un ideal maximal ni del casi-anillo de polinomios (Z[X], +, o) ni del anillo de polinomios (Z[X], +, .), de hecho ningún ideal maximal del anillo de composición es un ideal maximal del anillo de polinomios (Z[X], +, .) como es facil de comprobar.

J. L. Brenner asegura que el casi-anillo Z[X] es un casi-anillo principal es decir todos sus ideales son generados por un elemento, ¿ cual es el

generador de los ideales $pZ\langle X\rangle$?.

El conocimiento de los ideales maximales de los anillos de composición $(R[X], +, ., o)$ nos permiten calcular el radical de Jacobson.

Definición 3.15.

El radical de Jacobson del anillo de composición está definido como la interseción de todos los ideales maximales. Será denotado por :

$$Rad\,((R[X], +, ., o))$$

Nota 3.16.

Los ideales completos de R[X] forman un sistema de Moore inductivo en R[X].

El siguiente resultado determina el radical de Jacobson, una vez conocido el de el anillo R.

Teorema 3.17.

Se tiene :

$Rad\,((R[X], +, ., o)) = Rad(R)\langle X\rangle$. (donde Rad(R) es el radical de Jacobson del anillo R)

Demostración.

$$Rad\,((R[X], +, ., o)) = \bigcap \{ J\langle X\rangle / J \text{ es un ideal maximal de } R \}$$

$$= \left(\bigcap J , J \text{ maximal} \right)\langle X\rangle = Rad(R)\langle X\rangle . \blacklozenge .$$

Acabamos este parrafo y asi el capitulo con un corolario inmediato del teorema 3.14.

Corolario. 3.18.

Se tiene :

(i) Si R = F, donde F es un cuerpo infinito, entonces :

$$Rad((F[X], +, ., o)) = \{ 0 \}.$$

(ii) Si R = F , cuerpo finito, entonces

$$Rad((F[X], +, ., o)) = Ker(h) \neq \{ 0 \}.$$

(iii) Si R= Z, entonces:

$$Rad((Z[X], +, ., o)) = \{ 0 \}.$$

(iv) Si R = $Z_{/nZ}$, con $n \geq 2$, entonces :

$$Rad((Z_{/nZ}[X], +, ., o)) \neq \{ 0 \}.$$

Demostración

3.17. ♦♦♦.

APENDICE

ALGORITMO PARA LA DESCOMPOSICION DE POLINOMIOS

En este apendice consideraremos el siguiente problema :

" *Dado un polinomio $f(X) \in F[X]$, F un cuerpo , encontrar una descomposición completa de $f(X)$ de la forma siguiente .*

$f(X) = g_1(X)$ o $g_2(X)$ o.....o $g_n(X)$ donde los $g_i(X)$ son polinomios indescomponibles "

INTRODUCCION.

Comenzamos dando las definiciones y resultados básicos que necesitaremos para concretar el problema.

Definición. 1. [L-N] [P] [S]

Se dice que un polinomio $f(X) \in R[X]$ de grado positivo es indescomponible sobre R si siempre que

$f(X) = g(X)$ o $h(X)$ con $g(X), h(X) \in R[X]$, entonces

$$\text{Grado}(g(X)) = 1 \quad \text{o} \quad \text{Grado}(h(X)) = 1.$$

Definición 2. [L-N] [P] [S]

(i) Sea $f(X) \in R[X]$ (R dominio de integridad) y $Grado(f(X)) > 1$ y $g_1(X), g_2(X), \ldots\ldots, g_n(X) \in R[X]$, polinomios indescomponibles con :

$$f(X) = g_1(X) \circ g_2(X) \circ \ldots\ldots \circ g_n(X) .$$

Diremos que $[g_1(X), g_2(X), \ldots, g_n(X)]$ es una descomposición completa de $f(X)$.

(ii) A los $g_i(X)$ les llameremos componentes de la descomposición.

Proposición 3.

Sea R un dominio de integridad y $f(X) \in R[X]$.

Si $Grado(f(X)) > 1$, entonces existe una descomposición completa de $f(X)$.

Demostración

(ver [L-N] [P] [S] .). ♦ .

Nota 4.

Resultados relativos a la " unicidad " de la descomposición completa de un polinomio f(X) pueden encontrarse en [D-W] [L-N] [P] [S] . En particular F. Dorey y G. Whaples en "*Prime and Composite Polynomials*" (1974) [D-W], demuestran que cada descomposición de $f(X) \in F[X]_d$ (F un cuerpo de característica p) es equivalente a una descomposición en polinomios aditivos (esto es inmediato si $F = Z_{/pZ}$, ver Cap.I- 2.14). Entre otras propiedades relativas a la " unicidad " de la descomposición de un polinomio, destacamos:

Si $f(X) \in F[X]$ con m.c.d(grado(f(X), car.(F)) = 1 o car(F) = 0 y

$f(X) = g_1(X) \circ g_2(X) \circ \ldots\ldots \circ g_r(X) = h_1(X) \circ h_2(X) \circ \ldots\ldots \circ h_s(X)$, donde $g_i(X)$, $h_i(X)$ son polinomios indescomponibles de grado > 1. Entonces r = s y los grados de las componentes son las mismos salvo permutación.

Los dos únicos algoritmos que se conocen al respecto son debidos a David R. Barton y Richard Zippel . [B-Z] (1.985) . Encuentran una descomposición completa de $f(X) \in F[X]$, donde F es un cuerpo de característica 0, en ambos algoritmos necesitan de todos los factores irreducibles de un polinomio; en uno de ellos de los factores de un polinomio en una variable y en otro de los factores irreducibles de un polinomio en dos variables .

Aunque los autores no lo advierten, estos algoritmos sirven también para un polinomio f(X) con coeficientes en cuerpo de característica positiva (con algunos pequeños matices), en concreto para ciertos polinomios se necesita en algún momento de una etapa encontrar (no solamente los factores irreducibles) las raíces de un cierto polinomio.

En este apéndice presentamos un algoritmo para la descomposición de un polinomio que no hace uso de la factorización de polinomios.

ALGUNOS RESULTADOS

A lo largo de este apéndice F denotará un cuerpo.

Teorema 5.

Sea $f(X) \in F[X]$ con Grado(f(X)) > 1. Entonces existe una descomposición completa $[h_1(X), h_2(X) , \ldots\ldots, h_r(X)]$ de f(X) con las siguientes características :

(a) Grado($h_i(X)$) > 1 para i = 1,....., r.

(b) Los $h_i(X)$ son polinomios mónicos para i = 2,....., r.

(c) Los $h_i(X) \in F_0[X]$ para i =2,.....,r.

Demostración

Necesitamos este resultado :

Lema

Supongamos que $h(X) \in F[X]$ con Grado(h(X)) >1 es un polinomio indescomponible. Entonces p(X) = l(X) o h(X) es indescomponible para todo $l(X) \in F[X]$ con Grado(l(X)) = 1 .

Demostración. En efecto l(X) = aX + b, con $a \neq 0$, tenemos $h(X) = (1/a X - b/a)$ o p(X), el resto es elemental.♦.

Haciendo uso de este lema podemos encontrar una descomposición completa que verifique (a).

Supongamos que f(X) = g(X) o h(X), con $h(X) = c_m X^m + \ldots\ldots + c_1 X + c_0$, y $c_m \neq 0$, tenemos que $h(X) = c_m X$ o h'(X) con

$$h'(X) = X^m + (c_m)^{-1} c_{m-1} X^{m-1} + \ldots\ldots + (c_m)^{-1} c_1 X + (c_m)^{-1} c_0 ,$$

luego tenemos que f(X) = g(X) o $c_m X$ o h'(X) = g'(X) o h'(X) con h'(X) mónico.

Así conseguimos una descomposición completa de f(X) que verifique (a),(b) .

Para conseguir que satistaga (c) . Sea f(X) = g(X) o h(X) con h(0) = a tenemos f(X) = g(X) o (X + a) o (X - a) o h(X) =

(g(X) o (X + a)) o ((X - a) o h(X)) = g'(X) o h'(X) con h'(0) = 0. Esta claro que haciendo uso de esta pequeña nota y del lema conseguimos la tesis del teorema. ♦.

Notar que no se pierde generalidad al suponer que el polinomio de partida f(X), es un polinomio mónico, (ver teorema 4).

Notación.6

El polinomio f(X) ∈ F[X], para el cual queremos encontrar una descomposicón completa, (Grado(f(X)) > 1) le escribiremos a lo largo de este apéndice de la siguiente forma :

$$f(X) = X^n + A^0_1X^{n-1} + A^0_2X^{n-2} + \ldots\ldots + A^0_iX^{n-i} + \ldots + A^0_{n-1}X + A^0_n$$

Definición 7.

Diremos que un polinomio h(X) ∈ K[X] (K es una extensión de F) con 1< Grado(hX)) < n es un " candidato bueno " si existe un g(X) ∈ K[X] tal que

$$f(X) = g(X) \circ h(X).$$

El siguiente teorema esta basado en las ideas de David R. Barton y Richard Zippel . [B-Z] (1.985) para la computación de g(X) una vez que se parte de un candidato h(X).

Notar, también que no se pierde generalidad en suponer que el posible "candidato bueno" no tiene término constante.(ver teorema 4)

Teorema 8.

Un polinomio $h(X) \in K_0[X]$ es un " candidato bueno " si y solamente si los restos de las divisiones p-ádicas de f(X) en h(X) son constantes, es decir : En las divisiones euclideas

$$f(X) = q_1(X)\, h(X) + r_0(X)$$

$$q_1(X) = q_2(X)\, h(X) + r_1(X)$$

.

. $\qquad\qquad$ Grado$(r_i(X)) <$ Grado$(h(X))$

. $\qquad\qquad$ para todo i

$$q_{t-1}(X) = q_t(X)\, h(X) + r_{t-1}(X)$$

$$q_t(X) = 0\, h(X) + r_t(X).$$

Los $r_i(X)$ son polinomios constantes $r_i(X) = r_i \in K$.

Demostración

Tenemos :

$$f(X) = r_t(X)\, h(X)^t + \ldots\ldots\ldots\ldots + r_1(X)\, h(X) + r_0(X).$$

Supongamos que los $r_i(X) = r_i$. Entonces $f(X) = g(X)$ o $h(X)$, donde

$$g(X) = r_t X^t + \ldots\ldots + r_1 X + r_0$$

Reciprocamente, sea $g(X) = c_s X^s + \ldots + c_1 X + c_0$ tal que $f(X) = g(X)$ o $h(X)$, $f(X) = c_s h(X)^s + \ldots\ldots + c_1 h(X) + c_0 = [\, c_s h(X)^{s-1} + \ldots\ldots + c_1\,]\, h(X) + c_0$ por otro lado $f(X) = q_1(X)\, h(X) + r_0(X)$, luego tenemos que

$q_1(X) = c_s h(X)^{s-1} + \ldots\ldots + c_1]$ y $r_0(X) = c_0$ analogamente demostramos que los $r_1(X) = c_1$ luego $s = t$ y los $r_i(X)$ constantes para $i = 1, \ldots, t$.

Además, puesto que h(0) = 0, tenemos

$$f(0) = q_1(0)\, h(0) + r_0(0) = r_0$$

$$q_1(0) = q_2(0)\, h(0) + r_1(0) = r_1$$

.

.

$$q_{t-1}(0) = q_t(0)\, h(0) + r_{t-1}(0) = r_{t-1}$$

$$q_t(0) = 0\, h(0) + r_t(0) = r_t .$$

Luego si qeremos saber si un polinomio h(X) es un " candidato bueno " habrá que computar las siguientes divisiones :

$$q_1(X) = f(X) - f(0)/\, h(X).$$

$$q_2(X) = q_1(X) - q_1(0)/\, h(X).$$

.

.

$$q_t(X) = q_{t-1}(X) - q_{t-1}(0)/\, h(X).$$

Si en alguna división no es exacta, h(X) no es un " candidato bueno " y si todas son exactas, h(X) es un "candidato bueno" ; además

$$f(X) = (r_t X^t + \ldots\ldots + r_1 X + r_0) \circ h(X) ,$$

luego, como ya anotaron David R. Barton y Richard Zippel [B-Z], esta observación servirá también para calcular los coeficientes de g(X) . ♦ .

El siguiente teorema es fundamental para la determinación del candidato h(X).

Teorema 9.

Sea m un número natural divisor propio de n = Grado(fX)) , n = mt con m.c.d(t , Caracteristica(F)) = 1 o car(F) = 0. Entonces:

Si existe un " candidato bueno " $h(X) \in K_0[X]$, (K es una extensión cualquiera de F) mónico, con Grado(h(X)) = m, entonces h(X) es único; y en este caso ambos h(X) y g(X) pertenecen a F[X].

Demostración.

Sea $h(X) = X^m + b_1X^{m-1} + b_2X^{m-2} + \ldots\ldots\ldots + b_{m-1}X \in K_0[X]$ y supongamos que h(X) es un " candidato bueno ", tenemos

$$f(X) = q_1(X)\, h(X) + r_0(X) \quad \text{con}$$

$$q_1(X) = X^{n-m} + A^1{}_1X^{n-m-1} + \ldots + A^1{}_iX^{n-m-i} + \ldots + A^1{}_{m-1}X^{n-m-(m-1)} + M_1(X)$$

donde $\text{Grado}(M_1(X)) < n-2m+1$ y los coeficientes $A^1{}_i$ estan calculados de forma recurrente aplicando el algoritmo de la división euclídea :

$$A^1{}_1 = A^0{}_1 - b_1$$

$$A^1{}_2 = A^0{}_2 - b_1 A^1{}_1 - b_2$$

$$A^1{}_3 = A^0{}_1 - b_1 A^1{}_2 - b_2 A^1{}_1 - b_3$$

.....

.....

$$A^1{}_i = A^0{}_i - b_1 A^1{}_{i-1} - b_2 A^1{}_{i-2} - \ldots\ldots\ldots - b_{i-2} A^1{}_2 - b_{i-1} A^1{}_1 - b_i$$

.....

$$A^1{}_{m-1} = A^0{}_{m-1} - b_1 A^1{}_{m-2} - b_2 A^1{}_{m-3} - \ldots\ldots\ldots - b_{m-2} A^1{}_1 - b_{m-1}$$

Por el mismo procedimiento tenemos

$$q_{k-1}(X) = q_k(X)\, h(X) + r_{k-1}(X) \text{ con}$$

$$q_k(X) = X^{n-km} + A^k{}_1 X^{n-m-1} + \ldots + A^k{}_i X^{n-km-i} + \ldots + A^k{}_{m-1} X^{n-km-(m-1)} + M_k(X)$$

donde Grado($M_k(X)$) $< n - (k+1)\, m + 1$ y los coeficientes $A^k{}_i$ de $q_k(X)$ vienen dados :

$$A^k{}_i = A^{k-1}{}_i - b_1 A^k{}_{i-1} - b_2 A^k{}_{i-2} - \ldots\ldots\ldots - b_{i-2} A^k{}_2 - b_{i-1} A^k{}_1 - b_i$$

para $i = 1, \ldots\ldots, m-1$ y pra $k = 1, \ldots, t-1$.

Tenemos

$q_{t-1}(X) = q_t(X)\, h(X) + r_{t-1}(X)$ donde

$$q_{t-1}(X) = X^m + A^{t-1}{}_1 X^{m-1} + \ldots + A^{t-1}{}_i X^{m-i} + \ldots\ldots\ldots + A^{t-1}{}_{m-1} X + M_{t-1}(X)$$

luego

$$r_t(X) = q_t(X) = 1 \qquad y \qquad M_{t-1}(X) = r_{t-1}(X) = r_{t-1} \in K.$$

Se tiene

$A^{t-1}{}_i = b_i$ para $i = 1, \ldots\ldots, m-1$.

Si denotamos

$C_i = A^1{}_i + A^2{}_i + \ldots\ldots\ldots + A^{t-1}{}_i$ para $i = 1, \ldots, m-1$.

Obtenemos:

$tb_1 = A^0{}_1$,

$$b_1 = A^0{}_1 / t$$

$tb_2 = A^0{}_2 - b_1 C_1$

$$b_2 = A^0{}_2 - b_1 C_1 / t$$

$$tb_3 = A^0{}_3 - b_1c_2 - b_2c_1$$

$$b_3 = A^0{}_3 - b_1c_2 - b_2c_1 / t$$

.....

$$tb_j = A^0{}_j - b_1c_{j-1} - b_2c_{j-2} - \ldots\ldots - b_{j-1}c_1$$

$$b_j = A^0{}_j - b_1c_{j-1} - b_2c_{j-2} - \ldots\ldots - b_{j-1}c_1 / t$$

Para $j = 1, 2, \ldots\ldots, m-1$

Concluimos que podemos encontrar todos los b_i y además obviamente todos los $b_i \in F$, luego $r_i(X) = r_i \in F$ y por lo tanto $g(X) \in F[X]$.

El algoritmo básico para la computación de h(X) dado f(X) en las condiciones del teorema es el siguiente:

Queremos computar los coeficientes b_i de h(X), el problema se traduce en encontar los elementos $A^k{}_i$ de la matriz $\underline{A}$ de t filas y de m-1 columnas.

$$\underline{A} = \begin{pmatrix} A^0{}_1 & A^0{}_2 \ldots\ldots & A^0{}_i \ldots\ldots & A^0{}_{m-1} \\ A^1{}_1 & A^1{}_2 \ldots\ldots & A^1{}_i \ldots\ldots & A^1{}_{m-1} \\ \ldots\ldots & & & \\ A^k{}_1 & A^k{}_2 \ldots\ldots & A^k{}_i \ldots\ldots & A^k{}_{m-1} \\ \ldots\ldots & & & \\ A^{t-1}{}_1 & A^{t-1}{}_2 \ldots\ldots & A^{t-1}{}_i \ldots\ldots & A^{t-1}{}_{m-1} \end{pmatrix}$$

Conocemos t y la primera fila (A^0_1 , A^0_2 ,..... A^0_i ,..... , A^0_{m-1})

1º etapa.

Computar b_1, $b_1 = (A^0_1) / t$

Computar la primera columna, $A^1_1 = A^0_1 - b_1$ y para todo k,

$$A^k_1 = A^{k-1}_1 - b_1.$$

Computar $C_1 = A^1_1 + A^2_1 + \ldots\ldots + A^{t-1}_1$

2º etapa.

Computar b_2, $b_2 = (A^0_2 - b_1 C_1) / t$

Computar la segunda columna, $A^1_2 = A^0_2 - b_1 A^1_1 - b_2$ y para todo k,

$$A^k_2 = A^{k-1}_2 - b_1 A^k_1 - b_2.$$

Computar $C_2 = A^1_2 + A^2_2 + \ldots\ldots + A^{t-1}_2$

.....

1º etapa.

Computar b_i, $b_i = (A^0_i - b_1 C_{i-1} - b_2 C_{i-2} - \ldots\ldots - b_{i-1} C_1) / t$

Computar la iº columna ,

$A^1_i = A^0_i - b_1 A^1_{i-1} - \ldots\ldots - b_{i-2} A^1_2 - b_{i-1} A^1_1 - b_i$, y para todo k,

$A^k_i = A^{k-1}_i - b_1 A^k_{i-1} - \ldots\ldots - b_{i-2} A^k_2 - b_{i-1} A^k_1 - b_i.$

Computar $C_i = A^1_i + A^2_i + \ldots\ldots + A^{t-1}_i$

así computamos todos los b_i, para i = 1,....., m-1 .♦.

Establecemos el algoritmo que nos da una descomposición completa del polinomio f(X).

ALGORITMO

El esquema del algoritmo para encontar una descomposición de un polinomio $f(X) \in F[X]$, será el siguiente :

I. Computar un polinomio h(X) indescomponible de grado menor que el de f(X) como una componente candidata de la descomposición.

II. Computar g(X) , si existe para que f(X) = g(X) o h(X) .

III. Recursivamente descomponer g(X) .

Una forma de atacar el problema, sería intentando resolver un sistema de ecuaciones :

Sean g(X) y h(X) con Grado(g(X)) = r y Grado(h(X)) = s. Determinar los coeficientes de g(X) y h(X) para que f(X) = g(X) o h(X), se traduce en resolver un sistema no lineal con coeficientes en F, de rs + 1 ecuaciones en r + s + 2 incognitas. Entonces cualquier solución de este sistema daria una descomposición de f(X). La técnica no es muy recomendable incluso en polinomios de grado muy bajo, porque las ecuaciones se van complicando rapidamente y así la complejidad de este problema es mas grande que el de partida.

Algoritmo.

Sea f(X) un polinomio mónico en F[X] de grado, n, primo con la carcterística de F o característica 0.

M1. Sea m el menor divisor propio de n, n = mt.

M2. Encontrar los coeficientes b_i para i = 1,....., m-1, del polinomio (teorema 9), $h(X) = X^m + b_1X^{m-1} + b_2X^{m-2} + \ldots\ldots + b_{m-1}X \in F[X]$.

M3. División p-ádica de f(X) en h(X) , comprobar si h(X) es un "candidato bueno " (teorema 8).

M4. Si h(X) es un " candidato bueno", encontrar los coeficientes de g(X) para que f(X) = g(X) o h(X). (teorema 8).

M5. Aplicar de nuevo **M1** al polinomio $g(X) = X^t + \ldots\ldots + r_1X + r_0$.

M6. Si h(X) no es un " candidato bueno " , tomar m' el siguiente divisor propio de n y distinto de m; aplicar **M2** para m'.

El algoritmo nos da una descomposición completa del polinomio f(X) en componentes indescomponibles.

En efecto si m es el menor divisor propio de n, n = mt para el cual existe :

$h(X)= X^m + b_1X^{m-1} + b_2X^{m-2} + \ldots\ldots + b_{m-1}X \in F[X]$ un " candidato bueno " entonces h(X) es obviamente un polinomio indescomponible.

Puesto que el número de divisores de n es finito , el número de etapas es también finito.

Por último, si para todo divisor l de n no existe un "candidato bueno " de grado l, entonces f(X) es indescomponible ; por lo tanto sólo aparece una única componente en la descomposición de f(X) .◆◆.

Corolario 11.

Sea $f(X) \in F[X]$ con Grado($f(X) > 1$ y m.c.d (Grado($f(X)$, Caract(F)) = 1 o característica 0. Supongamos que $f(X)$ es descomponible. Entonces existe una única descomposición completa de $f(X)$,

[$h_1(X)$, $h_2(X)$,....., $h_r(X)$] con las siguientes características :

(a) $f(X) = h_1(X)$ o $h_2(X)$ o.....o $h_r(X)$

(b) Grado($h_i(X)$) > 1 para i = 1,....., r.

(c) Los $h_i(X)$ son polinomios mónicos para i = 2,....., r.

(d) Los $h_i(X) \in F_0[X]$ ($h_i(0) = 0$) para i =2,.....,r.

(e) Grado($h_i(X)$) =Mínimo { Grado($h(X)$ / $h(X)$ es un "candidato bueno" para el polinomio $h_1(X)$ o $h_2(X)$ o.....o $h_i(X)$ }, para i=1,...r .

Demostración

Es inmediata usando el Algoritmo y el teorema 5. ♦ .

Definición 12.

Sea $f(X) \in F[X]$ con Grado($f(X) > 1$ y m.c.d (Grado($f(X)$, Caract(F)) = 1.

Si $f(X)$ es indescomponible a la descomposición completa de $f(X)$, [$f(X)$] diremos que es la " descomposición ideal " de $f(X)$.

Si $f(X)$ es descomponible, a la descomposición completa de $f(X)$, [$h_1(X)$, $h_2(X)$,....., $h_r(X)$] de la forma del corolario anterior diremos que es la " descomposición ideal " de $f(X)$.

Notar que la definición de " descomposición ideal " de un polinomio $f(X) \in F[X]$ con Grado($f(X) > 1$ y m.c.d (Grado($f(X)$, Caract(F)) = 1, esta bien definida (existe y es única) .

Ejemplos 13.

Encontrar la " descomposición ideal" de los siguientes polinomios sobre Q[X].

(a) $f(X) = X^6 + 6X^4 + X^3 + 9X^2 + 3X - 5$.

Aplicamos el algoritmo :

M1. n = 6, luego m = 2 , t = 3.

M2. Tenemos, $h(X) = X^2 + b_1X$, luego $b_1 = A^0{}_{1/3} = 0$.

M3. $h(X) = X^2$, $f(X) = q_1(X)\, X^2 + r_0(X)$, donde

$q_1(X) = X^4 + 6X^2 + X + 9$ y $r_0(X) = 3X - 5$.

Puesto que $r_0(X) \notin Q$, h(X) no es un " candidato bueno ".

M6. m = 3, t = 2.

M2. $h(X) = X^3 + b_1X^2 + b_2X$. tenemos :

$b_1 = A^0{}_{1\,/2} = 0$.

$2b_2 = A^0{}_2 - b_1C_1$, luego $b_2 = A^0{}_{2\,/2} = 3$.

M3. $h(X) = X^3 + 3X$, división p-ádica

$f(X) = (X^3 + 3X + 1)(X^3 + 3X) + 5$, luego $r_0 = 5 \in Q$.

$X^3 + 3X + 1 = 1\,(X^3 + 3X) + 1$, luego $r_1 = 1 \in Q$. Por lo tanto h(X) es un "candidato bueno ".

M4. Los coeficientes de g(X), son 1, r_1 y r_0 , luego $g(X) = X^2 + X - 5$.

M5. El grado del polinomio g(X) es primo, por lo tanto indescomponible. La " descomposición ideal " $f(X) = (X^2 + X - 5)\, o\, (X^3 + 3X)$.

(b)

$f(X) = X^{12} + 3X^{11} + 3X^{10} - 5X^9 - 12X^8 - 6X^7 + 12X^6 + 12X^5 - X^4 - 9X^3 + 2X + 5$.

M1. m = 2 , t = 6.

M2. $h(X) = X^2 + b_1X$, $b_1 = A^0{}_{1\,/6} = 1/2$.

M3. $h(X) = X^2 + 1/2X$. Tenemos $f(X) = q_1(X)\,h(X) + r_0(X)$, donde

$r_0(X) = 465/2048\,X + 5 \notin Q$, luego $X^2 + 1/2X$ no es un "candidato bueno".

M6. El siguiente divisor de 12 distinto de 2 es 4, luego m = 4, t = 3.

M2 Sea $h(X) = X^4 + b_1X^3 + b_2X^2 + b_3X$.

$b_1 = A^0{}_{1\,/3} = 1$.

$tb_2 = A^0{}_2 - b_1C_1$ donde $C_1 = A^1{}_1 + A^2{}_1 = (A^0{}_1 - b_1) + (A^0{}_1 - 2b_1) = 2 + 1 = 3$.

$3b_2 = 3 - 1.3 = 0 = b_2$.

$tb_3 = A^0{}_3 - b_1C_2 - b_2C_1$ donde $C_2 = A^1{}_2 + A^2{}_2 = 1 + 0 = 1$.

$3b_3 = -5 - 1.1 = -6$, entonces $b_3 = -2$.

M3. $h(X) = X^4 + X^3 - 2X$. División p-ádica de f(X) en h(X),

$f(X) = q_1(X)\,h(X) + r_0(X)$, donde

$q_1(X) = X^8 + 2X^7 + X^6 - 4X^5 - 4X^4 + 4X^2 - 1$ y $r_0(X) = 5 \in Q$.

$q_1(X) = q_2(X)\,h(X) + r_1(X)$, donde

$q_2(X) = X^4 + X^3 - 2X$ y $r_1(X) = -1 \in Q$.

$q_2(X) = q_3(X)\,h(X) + r_2(X)$, donde

$q_3(X) = 1$ y $r_2(X) = 0 \in Q$.

Por lo tanto $X^4 + X^3 - 2X$ es un "candidato bueno ".

M4. Los coeficientes de g(X) son $1, r_2(X)$, $r_1(X)$ y $r_0(X)$, luego

$g(X) = X^3 - X + 5$.

M5. El grado de g(X) es primo, luego g(X) es indescomponible.

La " descomposición ideal " de f(X) :

$[\,X^3 - X + 5,\ X^4 + X^3 - 2X\,]$.

Como consecuecia inmediata del teorema 9 obtenemos el siguiente

Teorema. 14. [F-R]

Sea $f(X) \in F[X]$ con el m.c.d (Grado(f(X)) = n , Carcteristica(F)) = 1 y f(X) indescomponible sobre F . Entonces f(X) es indescomponible sobre cualquier extensión K de F.

Demostración

Ver Teorema 9. ♦ .

Nota 15.

El teorema anterior no es cierto si la Carcteristica(F) divide al Grado(f(X)).

Sea $F = Z_{/2Z}$. Entonces $f(X) = X^4 + X^2 + X$ es indescomponible sobre F como de forma inmediata se comprueba, (notar que $f(X) \in F[X]_d$ así $\Psi(f(X) = X^2 + X + 1$ (Ψ es el isomorfismo del cap. I-2.14) que es un polinomio irreducible en el anillo (F[X], +, .). Sin embargo ,

$f(X) = (X^2 + \alpha^{-1}X) o (X^2 + \alpha X)$ donde

$\alpha^3 - \alpha + 1 = 0$ y $\alpha \in F_8$.

Sea $F = Z_{/pZ}$ y F la clausura algebraica de F. Sea $a \in F$, $a \neq 1$ con $a^{p+1} = 1$ y $h(X) = X^p + aX^{p-1} + \ldots\ldots + a^{p-1}X$. Es posible elegir g(X), $g(X) = a_pX^p + \ldots\ldots + a_1X$ tal que $f(X) = g(X)$ o $h(X) \in F[X]$. Basta elegir los a_i tales que $a_i(a^p)^i = a(-1)^i$. Así tenemos que

$f(X) = -(X^p + X^{p-1} + \ldots\ldots + X)(X^p + X^{p-1} + \ldots\ldots + X + 1)^{p-1}$.

Por otra parte f(X) es indescomponible sobre F, como de forma inmediata se comprueba.

Notemos entonces que en el Algoritmo necesitamos la condición de m.c.d (Grado(f(X)) = n , Carcteristica(F)) = 1, para poder determinar los coeficientes b_i del polinomio h(X)

APLICACIONES

Resolución de ecuaciones polinómicas

La aplicación más inmediata es para el cálculo de raices de un polinomio. Si f(X) es un polinomio descomponible, f(X) = g(X) o h(X). Entonces para computar los ceros de f(X), primero computamos los ceros de g(X), z_i; así los ceros de f(X) son los ceros de los polinomios

$h_i(X) = h(X) - z_i$.

Asi en los ejemplos 13 los dos polinomios son irreducibles sobre Q, sin embargo son descomponibles luego hemos reducido el problema de computar las raices de un polinomio irreducible de grado 12 a computar las raices de polinomios de grados 3 y 4 .

El operador SOLVE en el REDUCE no da ninguna solución al los ejemplos 13, pero si los resuelve aplicando el comentario de arriba.

Determinación de factores.

Sea f(X) ∈F[X] tal que Xf(X) es descomponible, entonces f(X) es reducible,

Existen g(X) y h(X) tal que Xf(X) = g(X) o h(X).

$Xf(X) = c_0h(X)^t + c_1h(X)^{t-1} + c_2h(X)^{t-2} + \ldots\ldots + c_{t-1}h(X)$, luego h(X) es un factor de Xf(X) y puesto que Grado(h(X)) ≥ 2, podemos conseguir de forma obvia un factor de f(X). En este sentido podemos aplicar el algoritmo para obtener factores de f(X).

Sea f(X) $\in$F[X] tal que una primitiva p(X) de f(X) (p'(X) = f(X), p'(X) es la derivada formal de p(X)) es descomponible entonces f(X) es reducible, Existen g(X) y h(X) tal que p(X) = g(X) o h(X), tenemos
f(X) = (g'(X) o h(X)) h'(X) y puesto que grado(h(X)) ≥ 2, grado(h'(X)0 ≥ 1.

Finalmente para determinar cuando el polinomio $(f(X) - f(Y))/ X- Y$ es un polinomio irreducible en F[X,Y](ver F-M]).◆◆◆...

BIBLIOGRAFIA

[B-Z] Barton, D. R., y Zippel, R. " *Polynomial decomposition algorithms*" J. Symbolic Computation, No.1, 1.985,(159-168).

[Br 1] Brenner, Joel L., " *Maximals ideals in the near-ring of polynomials mod 2*", Pacific J. Math. 52, 1.974 .

[Br 2] Brenner, Joel L., " *Composition algebras of polyomials* ", Pacific J. Math. 118, Nº 2, 1.985.

[C] Cartan, H. " *Theory of analytic functions*", Addison- Wesley, 1.963.

[Ca] Carcanague, Jean.," *q-polynomes abéliens sur un corps K*", 496- Série A, C.R. Acad. Sc. Paris, t. 265 (1.967).

[C-D] Clay, James R., y Doi, Donna K. " *Maximal ideals in the near-ring of polynomials over a field*", Colloq. Math. Soc. Janus Bolyai 6, Rings, Modules and Radicals, Keszthely (Hungary)1.971.,North-Holland , (117-133). 1.973

[D] Dickson, Leonard E. " *Definitions of a group and a field by independent postulates* " , Tans. Amer. Math. Soc.6. (1.905) (198-204).

[D-W] Dorey, F y Whaples, G., " *Prime and composite polynomials*" Journal of Algebra 28, 88-101- (1.974).

[F 1] Fröhlich, Albrecht. "*Distributively generated near-rings I. Ideal theory*", Procc. London Math. Soc. 8, (76-94). 1.958.

[F 2] Fröhlich, Albrecht. "*Distributively generated near-rings II. Representarion theory*", Proc. London Math. Soc. 8, 1.958, (95-108).

[F 3] Fröhlich, Albrecht. " *Some examples of near-rings* Oberwolfach, 1.968 .

[F-M] Fried, Michael y MacRae, R., " *On the invariance of chains of fields*" , III. J. Math. 13. (165-171) (1.969).

[Gr] Grätzer, George, " *Universal algebra*", Van Nostrand, 1.968.

[G 1] Gutiérrez, Jaime, " *The ring of the distributive elements in the near-rings of formal power series*" Com. XII Jornadas Luso-Espanholas de matemática . Braga, Portugal. 1.987

[G 2] Gutiérrez, Jaime, "*Distributor ideal in the near-ring of polynomials* " Com. Conference on near-rings and near-fields. Teeside Polytechnic, Middlesbrough, U. K. 1.987.

[G-R] Gutiérrez, Jaime, y Ruiz de Velasco y Bellas, Carlos. *"Distributive elements in the near-ring of polynomials* " Aceptado en Proc. of the Edinburgh Math. Soc. 1.987.

[J] Jacobson, N., " *Basic algebra*" Vol.1 Freeman, San Francisco, 1974.

[K 1] Kautschitsch, Herman. " *Maximal ideals in the near-ring of the formal power series* ", Proc. Conf en Near-rings and near-fields. San Benedetto del Tronto, 1.981 (101 -108).

[K 2] Kautschitsch, Herman. " *Maximal ideals in the near-ring of polynomials*" Colloq. Math. Soc. Janus Bolyai 38, Conf. on Radical Theory, Keszthely (Hungary)1.982.,North-Holland 1.985, (183-194).

[K-M] Kautschitsch, Herman, y Muller, Winfried, " *Ideale in kompositionsringen formaler potenzreihen mit nilpotent anfangskoeffizienten*", Arch. Math. 34 1.980, (517-525),

[L-N] Lausch, Hans, y Nöbauer, Winfried, " *Algebra of polynomials*" North-Holland, Amsterdam, 1.973.

[Li-N] Lidl, R y Neiderreiter, H, " *Finite fields*" Addison-Wesley, Reading, Massachusetts, 1.983.

[M] Meldrum, Jhon D.P. " *Near-rings and their links with groups*", Pitman Publ. Co. (Research Note Series No. 134), 1.985.

[M-P-S] Meldrum,J., Pilz, G. y So, Yong-Sian., " *Embedding near-rings into polynomials near-rings*" , Proc. of the Edinburgh Math. Soc, 25, 73-79 (1.982).

[N] Neumann, H., " *On varieties of groups and their associated near-rings*", Math. Z. 65, 36-69, (1.956).

[O] Ore, Oystein, " *On a special class of polynomials*", Trans. Amer. Math. Soc. vol. 35 , 1933 ,(539-584).

[P] Pilz, Günter, " *Near-rings* " North-Holland /American Elsevier, Amsterdam, Second, revised edition, 1.983.

[P-S] Pilz, Günter y So, Yong-Sian, " *Near-rings of polynomials and polynomial functions*", J. Austral. Math. Soc. (Series A) 29, 1.980 ,(61-70).

[R] Roberts, Ian , " *Generalized distributive near-rings*", Diss. Univ. Edinburgh., 1.983.

[S] Schinzel, Andrzej, " *Selected Topics on Polynomials*" Ann Arbor, The Univ. of Michigan Press, 1.982.

[St] Straus, Ernest, G. " *Remark on the precedings paper, ideals in near-rings of polynomials over a field*" Pacif. J. Math. No. 52, 1.974 , (601-603).

[W] Whaples, G. , " *Additive polynomials*", Duke Math. J. vol. 21 , 1954, (55-65).

[Wi] Wielandt, Helmut., " *Über bereiche aus gruppenabbildungen*" , Deutsche Mathematik, 3, 9-10, (1.938).

[Z-S] Zariski, O., y Samuel, P., " *Commutative algebra II*", D. Va. Nostrand Co., New York-Heidelberg-Berlin, 1975.

[Z] Zassenhaus, Hans., " *Über endliche fastkörper*", Abh. Math. Sem. Unv. Hamburg 11, 187-220, (1.935/1.936).