ANILLOS DE INVARIANTES DE GRUPOS DE R-AUTOMORFISMOS

Margarita María Toro Villegas

Trabajo de Grado presentado como requisito para optar el Título de Magister en Matemáticas.

Director: Debora María Tejada Jiménez
Doctora en Matemáticas

UNIVERSIDAD NACIONAL DE COLOMBIA
Seccional de Medellín
Facultad de Ciencias
Posgrado de Matemáticas
1.985

T
55

AGRADECIMIENTOS

A todas las personas que colaboraron conmigo en la realización de este trabajo y muy especialmente:

A la profesora Débora María Tejada por su excelente labor como directora de tesis.

A los profesores Miriam Campos, Gilberto García y Volker Stallbohm por su trabajo como jurados.

Al profesor Carlos Enrique Mejía por su inmejorable compañía y ayuda.

A la señora Miryam Lucia Patiño de Núñez por su paciente trabajo de mecanografía y escritura de signos especiales.

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL
D 95553

TABLA DE CONTENIDO

pág.

INTRODUCCION 1

1. NOCIONES TOPOLOGICAS 6

2. TEOREMA DE PREPARACION 24

3. GRUPO FINITO DE R-AUTOMORFISMOS DE $R[x]$ 49

4. GRUPO FINITO DE R-AUTOMORFISMOS DE $R[[x]]$ 68

5. GRUPO INFINITO DE R-AUTOMORFISMOS 90

APENDICE 104

REFERENCIAS BIBLIOGRAFICAS 111

INTRODUCCION

Dado un anillo R conmutativo decimos que un automorfismo ϕ del anillo de polinomios $R[x]$ (respectivamente del anillo de series formales $R[[x]]$) es un R-automorfismo de $R[x]$ (respectivamente de $R[[x]]$) si ϕ deja invariantes todos los elementos de R. El objetivo de este trabajo es estudiar el anillo de invariantes de un grupo G de R-automorfismos de $R[x]$ (resp. $R[[x]]^G$) que notaremos $R[x]^G$ (respectivamente $R[[x]]^G$), por tanto

$$R[x]^G = \left\{ p \in R[x] \ / \ \phi(p) = p \quad \forall \phi \in G \right\}$$

$$\text{(respectivamente } R[[x]]^G = \left\{ p \in R[[x]] \ / \ \phi(p) = p \quad \forall \phi \in G \right\} \text{)}$$

Cuando R es un anillo entero, conmutativo con unidad y G es un grupo finito obtenemos un resultado análogo en ambos casos, a saber:

$$R[x]^G = R[f] \quad \text{donde} \quad f = \prod_{\phi \in G} \phi(x) \quad \text{y}$$

$$R[[x]]^G = R[[f]] \quad \text{donde} \quad f = \prod_{\phi \in G} \phi(x)$$

El método que usamos para probar el resultado en el caso del anillo de polinomios es el empleado por Castillon en (4), y lo elegimos por ser el más simple que conocemos.

En el caso del anillo de las series formales empleamos el método seguido por O'Malley en (21). En artículos anteriores al de O'Malley fueron

suprimiéndose hipótesis, y el resultado fue evolucionando de la siguiente forma:

1- SAMUEL 1966 (**24**). En este artículo se trata el tema por primera vez, exigiéndole al anillo R que sea conmutativo, entero, con unidad, local, Noetheriano y completo.

2- CASTILLON 1970 (**4**), quien emplea un método más simple que el de Samuel, y exige al anillo R que sea conmutativo, entero, con unidad, separable y completo con la topología m-ádica, siendo m el ideal maximal de R.

3- O'MALLEY 1971 (**19**). Prueba el resultado bajo las hipótesis de que R sea un anillo conmutativo, entero, con unidad, noetheriano y tal que su clausura íntegra sea un R-módulo finito.

Y llegamos por fin al resultado más general que exige solo que R sea conmutativo, entero con unidad.

El esfuerzo que se requiere para poder suprimir tantas hipótesis justifica plenamente todo el trabajo previo que hay que hacer, el cual se encuentra en los dos primeros capítulos.

En el primer capítulo hacemos una recopilación de los resultados netamente topológicos que emplearemos posteriormente.

En el segundo capítulo estudiamos un resultado importante en el álgebra conmutativa, llamado Teorema de Preparación de Weierstrass.

Aunque estos dos capítulos surgieron durante el estudio como una herramienta, constituyen una parte fundamental del presente trabajo por su importancia en el desarrollo del resultado mencionado inicialmente. Por este motivo hacemos todas las pruebas en detalle, haciendo caso omiso de su longitud.

En el tercer capítulo estudiamos el anillo de invariantes de un grupo finito de R-automorfismos de anillo $R[x]$. Hacemos la prueba del resultado enunciado al principio de esta introducción, pero también investigamos y encontramos algunos resultados nuevos acerca de lo que sucede si debilitamos la hipótesis. De esta forma encontramos que si suprimimos la unidad, pero conservamos que el anillo sea conmutativo y entero obtenemos que $R[x]^G = K[f] \cap R[x]$, donde K es el campo de fracciones de R y $f = \prod_{\phi \in G} \phi(sx)$, y $s \in R$. Pero damos un ejemplo que prueba que la hipótesis de integridad no puede ser suprimida. En la última sección de este capítulo exponemos una serie de ejemplos de grupos finitos de R-automorfismos del anillo de polinomios $R[x,y]$, y hacemos algunas consideraciones acerca del anillo de invariantes de estos grupos. Es importante anotar que hasta el momento no se conoce ninguna extensión del resultado obtenido para el caso de una sola variable.

En el capítulo cuarto nos ocupamos del anillo de invariantes de un grupo finito de R-automorfismos de $R[[x]]$ y obtenemos como resultado

central el ya mencionado al comienzo. En la segunda sección consideramos qué sucede si se trabaja con un anillo entero, conmutativo sin unidad y nos encontramos con la imposibilidad de extender el método de trabajo que habíamos empleado para el anillo de polinomios y solamente podemos dar un resultado parcial.

En el quinto capítulo estudiamos el anillo de invariantes de un grupo infinito de R-automorfismos.

En el caso de considerar un grupo infinito de R-automorfismos de $R[x]$ obtenemos un resultado completo, que nos permite decir que si R es un anillo conmutativo y entero entonces $R[x]^G = R$, independientemente de que R tenga o no unidad. Damos ejemplos que nos muestran que si R no es entero no se cumple el resultado; y que si estamos considerando un grupo infinito de R-automorfismos del anillo de polinomios en varias variables tampoco se cumple el resultado, aunque el anillo R sea entero.

Damos también una caracterización de los R-automorfismos de $R[x]$ cuando R es entero y como aplicación estudiamos la forma de los grupos finitos de $\mathbb{Z}$-automorfismos de $\mathbb{Z}[x]$.

Al final de este capítulo estudiamos el anillo de invariantes de un grupo infinito de R-automorfismos de $R[[x]]$. Se tiene la conjetura de que si R es entero, conmutativo con unidad, entonces $R[[x]]^G = R$, pero encontramos un error en la única demostración que conocemos (Castillon (5)); y aunque intentamos métodos de trabajo diferentes para superar este

problema, solo obtuvimos resultados parciales. Lo que sucede en el caso general queda también como interrogante.

Concluímos el trabajo con un apéndice en el que hacemos un esbozo de una técnica original que diseñamos para construir grupos finitos de R-automorfismos del anillo de polinomios en varias variables. Hacemos este apéndice para ampliar la información acerca de algunos de los ejemplos que habíamos dado en la sección 3.3.

1. NOCIONES TOPOLOGICAS

El objetivo de este trabajo es obtener unos resultados netamente algebraicos, pero la única manera de obtenerlos es empleando conceptos topológicos, asi es que nos enfrentamos con la grata empresa de no poder desligar nuestro trabajo algebraico de la topología.

En este capítulo hacemos un recuento de los resultados topológicos que serán empleados posteriormente.

Por su importancia preferimos presentarlos todos en un capítulo independiente en lugar de irlos enunciando en el momento de usarlos.

Además, creemos que para una persona que no esté especializada en topología, este capítulo le será de gran utilidad, no solo en la lectura de este trabajo, sino también si desea profundizar en el tema.

1.1 IDEALES

Sea R un anillo conmutativo con unidad y $R[[x]]$ el anillo de las series formales con coeficientes en R. Si $@$ es un ideal de R, $@\,R[[x]]$ es la extensión de $@$ a $R[[x]]$, es decir:

$$@\,R[[x]] = \left\{ \sum_{\text{finitos}} a_i\, f_i \;\; / \;\; a_i \in @,\; f_i \in R[[x]] \right\}$$

Y notaremos $@[[x]]$ al ideal de $R[[x]]$ formado por todas las series formales con coeficientes en $@$, o sea

$$@[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i \;/\; a_i \in @ \right\}$$

En general estos dos ideales no son iguales, pero si $@$ es finitamente generado se tiene la igualdad, ya que siempre se cumple que $@\,R[[x]] \subset @[[x]]$ y si $@$ es un ideal generado por $a_1, a_2, \dots, a_n$ (hecho que notaremos por $@ = (a_1, a_2, \dots, a_n)$), entonces si $f \in @[[x]]$ tenemos que $f = \sum_{i=0}^{\infty} b_i\, x^i$ con $b_i \in @$ es decir, $b_i \underset{(1)}{=} \sum_{j=1}^{n} a_j\, b_j^{(i)}$ para todo $i \geqslant 0$, $j = 1, \dots n$

luego $f = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{n} a_j\, b_j^{(i)} \right) x^i = \sum_{j=1}^{n} a_j \left(\sum_{i=0}^{\infty} b_j^{(i)}\, x^i \right)$

donde $\sum_{i=0}^{\infty} b_j^{(i)}\, x^i \in R[[x]]$, por tanto $f \in @\,R[[x]]$ y asi

$$@\,R[[x]] = @[[x]]$$

Nota: Esta igualdad será fundamental en algunos teoremas posteriores. En el paso (1) vemos que la hipótesis de que el ideal sea finitamente generado es esencial. Sabemos además que si $@$ es finitamente generado entonces $@\,R[[x]]$ también lo es, precisamente por los mismos elementos, con la diferencia que la generación en este último caso tendrá como coeficientes elementos de $R[[x]]$ en lugar de elementos de R. Se cumple entonces también que $(@\,R[[x]])^n = @^n\,R[[x]]$ y por tanto $@^n\,R[[x]] = @^n[[x]]$.

1.2 ANILLOS TOPOLOGICOS

Dado un anillo R dotado de una estructura topológica, decimos que R es un anillo topológico si las dos estructuras son compatibles, es decir si las operaciones:

$$\begin{array}{ccc} R \times R \longrightarrow R & R \longrightarrow R & R \times R \longrightarrow R \\ (x,y) \longmapsto x+y & x \longmapsto -x & (x,y) \longmapsto x\,y \end{array}$$

son funciones continuas.

En este trabajo nos limitaremos únicamente a un tipo de anillos topológicos, que son aquellos en los cuales la topología sobre R está inducida por una sucesión de ideales $\{B_k\}_{k \in \mathbb{N}}$, tal que $B_k \subset B_n$, $\forall_{n,k} \in \mathbb{N}$, $k > n$. A este tipo de sucesión se le llama d-sucesión. Un sistema fundamental de vecindades de cero es precisamente la sucesión de ideales $\{B_k\}_{k \in \mathbb{N}}$. Fácilmente se prueba que en efecto R es un anillo topológico si se considera sobre R la topología inducida por este sistema fundamental de entornos de cero.

Una clase especial de estas topologías es cuando la sucesión está formada por potencias de un ideal $@$, es decir por $\{@^k\}_{k \in \mathbb{N}}$. Estas topologías se llaman $@$-ádicas, y serán las que más estudiaremos. Usaremos la notación $(R, @)$ para referirnos al anillo R con la topología $@$-ádica.

1.3 LEMA: Sea R un anillo y consideremos $\mathcal{T}$ la topología inducida sobre R por la sucesión de ideales $\{B_k\}_{k \in \mathbb{N}}$, entonces $\mathcal{T}$ es Hausdorff si y solo si $\bigcap_{k=0}^{\infty} B_k = (o)$

Para una demostración de este lema ver (**1**) pág. 113.

Veamos un ejemplo de topologías ádicas.

1.4 EJEMPLO: Consideremos el anillo $\mathbb{Z}$ de los enteros con la topología (p)-ádica, donde p es un número primo. Es decir, que las vecindades de cero serán de la forma (p^k) para $k \in \mathbb{N}$.

Como $\bigcap_{k=0}^{\infty} (p^k) = (o)$ entonces tenemos que $\mathbb{Z}$ es un espacio Hausdorff con la topología p-ádica. . Veamos que sin embargo no es un espacio completo.

Consideremos la sucesión $\left\{\sum_{k=0}^{i} p^k\right\}_{i \in \mathbb{N}}$. Esta es una sucesión Cauchy en $(\mathbb{Z}, (p))$ pues: $\sum_{k=0}^{m} p^k - \sum_{k=0}^{n} p^k = \sum_{k=n+1}^{m} p^k \in (p^n) \subset (p^k)$ siempre que $k \leqslant n \leqslant m$.

Supongamos que exista $a \in \mathbb{Z}$ tal que $\lim_{i \to \infty} \sum_{k=0}^{i} p^k = a$; como $\mathbb{Z}$ es un dominio de factorización única, entonces $a = \eta\, p^i$ para $i \in \mathbb{N}$ y $\eta \in \mathbb{Z}$ y $p \nmid \eta$

Luego para este i existe un valor $S_i > i$ tal que si $\eta > S_i$ se

cumple que $\sum_{k=0}^{n} p^k - a \in (p^i)$ es decir $\sum_{k=0}^{n} p^k = y\, p^i + a = y\, p^i + \eta\, p^i$ con $y \in \mathbb{Z}$ y por tanto $1 = p\,(\, p^{i-1}\, \eta + y\, p^{i-1} - \sum_{k=2}^{n} p^{k-1}\,)$ es decir que $1 \in (p)$ ¡Absurdo! , porque p es primo, es decir que $(\mathbb{Z}\,,\,(p)\,)$ es un espacio Hausdorff no completo, y precisamente su completación es la que llamamos **los enteros p-ádicos.**

Dada una serie formal $f = \sum_{i=0}^{\infty} a_i\, x^i$ nos referimos frecuentemente a las siguientes topologías:

$(R\,,\,a_i\,)$ para indicar precisamente la topología (a_i) -ádica

$(R\,,\,@\,)$ para la topología @-ádica, donde $@ = (a_0, \dots, a_n\,)$

$(R[[x]]\,,\,@[[x]]\,)$ para la topología $@[[x]]$ -ádica

$(R[[x]]\,,\,f\,)$ para la topología (f)-ádica, con $f \in R[[x]]$.

En esta sección nos interesa especialmente dar resultados que nos permitan relacionar estas diferentes topologías.

1.5 **PROPOSICION: Si $(R\,,\,@\,)$ es un espacio Hausdorff completo en la topología @-ádica entonces $(R\,,\,b)$ es un espacio Hausdorff completo para todo $b \in @$**

El hecho de que (R,b) sea Hausdorff se obtiene fácilmente porque como $(b)^n \subset @^n$ entonces si $\bigcap_{n=1}^{\infty} @^n = (0)$ se cumple también que $\bigcap_{n=1}^{\infty} (b)^n = (0)$ y por tanto (R,b) es Hausdorff. Veamos ahora que es completo.

Sea $\{n_j\}_{j \in \mathbb{N}}$ una sucesión Cauchy de (R,b). Esta sucesión tiene una subsucesión $\{C_j\}_{j \in \mathbb{N}}$ tal que $C_j = \sum_{k=0}^{j} S_k\, b^k$ con $S_k \in R$. Esta sucesión también es Cauchy en (R,b) y por tanto es Cauchy en $(R, @)$, tenemos entonces que converge a un único elemento C de R, que se nota precisamente por $C = \sum_{k=0}^{\infty} S_k\, b^k$ por ser $(R, @)$ Hausdorff completo (si no fuera Hausdorff podrían existir muchos más límites).

Veamos ahora si $\{C_j\}_{j \in \mathbb{N}}$ converge a C en (R,b), es decir, que para $h \in \mathbb{N}$ existe $n \in \mathbb{N}$ tal que si $J \geqslant n$ entonces $C - C_j \in (b^h)$

como $C - C_j = \sum_{k=0}^{\infty} S_k\, b^k - \sum_{k=0}^{j} S_k\, b^k = \sum_{k=j+1}^{\infty} S_k\, b^k = b^{j+1} \sum_{k=j+1}^{\infty} S_k b^{k-j-1}$

es decir que $(C - C_j) \in (b^{j+1}) \subset (b^h)$ si $j > h$. Por tanto dado h basta tomar $n = h$ y se tiene el resultado. ||||

1.6 **OBSERVACION:** El recíproco de este enunciado no es cierto. Ni siquiera en el caso en el que $@ = (a_1, \dots, a_n)$ y (R,a_i) sea un espacio Hausdorff completo se puede asegurar que $(R,@)$ sea Hausdorff completo. En **(9)**, ejemplo 2.4, se da un ejemplo donde se tiene esta situación.

Tampoco se cumple la proposición anterior si suprimimos que $(R,@)$ sea Hausdorff, es decir, que no es cierto que si $(R,@)$ es completo entonces (R,b) es completo para todo $b \in @$.

Ejemplo: Sea $R = \mathbb{Z} \times \mathbb{Z}$, y consideremos el ideal $@ = \mathbb{Z} \times (o)$.

R es completo en su topología $@$-ádica, pues si $\{(N_i , S_i)\}_{i \in \mathbb{N}}$ es una sucesión Cauchy en $(R,@)$ entonces para todo $k > 0$ existe $N \in \mathbb{N}$ tal que si $i,j > N$ entonces $(N_i , S_i) - (N_j , S_j) \in @^k$

pero $@^k = (\mathbb{Z} \times (o))^k = \mathbb{Z} \times (o)$ es decir $N_i - N_j \in \mathbb{Z}$ y $S_i - S_j \in (o)$ y por tanto cualquier elemento de la forma (N,o) es un límite de esta sucesión (precisamente el espacio no es Hausdorff y por eso puede haber varios valores para este límite).

Tomemos ahora el elemento $b = (2,o) \in @$ y la topología b-ádica, y consideremos la sucesión $\{C_i\}_{i \in \mathbb{N}} = \left\{ \left(\sum_{k=0}^{i} 2^k, o \right) \right\}_{i \in \mathbb{N}}$

Esta es una sucesión Cauchy en R con la topología $(2,o)$-ádica porque para $j > o$, si $m > n \geqslant j+1$ entonces

$$(C_m - C_n) = \left(\sum_{k=0}^{m} 2^k,o \right) - \left(\sum_{k=0}^{n} 2^k,o \right) = \left(\sum_{k=n+1}^{m} 2^k,o \right)$$

y como $2^{n+1} \left(\sum_{k=0}^{m-n-1} 2^k \right) \in (2^j)$ entonces $C_m - C_n \in ((2,o))^j$

Sin embargo esta sucesión no converge a ningún valor de R en la topología $(2,o)$-ádica, pues si existiera algún $(C,o) \in R$ tal que

$\lim_{i \to \infty} C_i = (C,o)$ entonces existiría $C \in \mathbb{Z}$ tal que $\lim_{i \to \infty} \sum_{k=0}^{i} 2^k = C$ en la topología (2)-ádica. Y sabemos que las topologías (p)-ádicas no son completas, y precisamente las sucesiones de la forma $\left\{ \sum_{k=0}^{i} p^k \right\}_{i \in \mathbb{N}}$

son sucesiones Cauchy que no convergen, como ya lo habíamos visto.

El siguiente resultado es el más cercano que tenemos al recíproco de la proposición anterior.

1.7 PROPOSICION: Sea R un anillo, $@$ un ideal finitamente generado, $@ = (a_1, \dots, a_n)$; si (R,a_i) es un espacio completo para todo $i = 1, \dots, n$ entonces R es un espacio completo en la topología $@$-ádica.

Consideremos la sucesión de ideales $B_k = (a_1^k, \dots, a_n^k)$ para todo $k \in \mathbb{N}$. Esta sucesión satisface $B_{j+1} \subset B_j$, es decir, $\{B_k\}_{k \in \mathbb{N}}$ es una d-sucesión e induce entonces una topología sobre R. Veamos que esta topología es equivalente a la topología $@$-ádica, es decir, que dada cualquier vecindad de cero en la topología $@$-ádica existe una vecindad de cero en la topología inducida por $\{B_k\}_{k \in \mathbb{N}}$ que la contiene, y recíprocamente. Claramente $B_k \subset @^k$ porque $a_1^k, a_2^k, \dots, a_n^k \in @^k$ y $@^{kn} \subset B_k$ porque un término $b \in @^{k+1}$ está formado por sumas finitas de elementos de la forma $b_1, b_2 \dots b_{kn}$ donde $b_j \in @$ $(j = 1, \dots, kn)$, es decir, sumas de elementos de la forma

$$\left(\sum_{i=1}^{n} N_{1_i} a_i \cdots\cdots \sum_{i=1}^{n} N_{kn_i} a_i \right) = \sum_{\sigma_1+\sigma_2+\dots+\sigma_n = kn} r\, a_1^{\sigma_1} a_2^{\sigma_2} \dots a_n^{\sigma_n}$$

Por tanto cada uno de los sumandos contiene una potencia mayor que k

para algún a_i , y por tanto $b \in (a_1^k, \dots , a_n^k) = B_k$

Llamemos Ω la topología inducida sobre R por la d-sucesión $\{B_k\}_{k \in \mathbb{N}}$

Como hemos probado que Ω y la topología @-ádica son equivalentes es suficiente probar que R es completo con la topología Ω para obtener que R es completo con la topología @-ádica.

Sea $\{b_n\}_{n \in \mathbb{N}}$ una sucesión Cauchy en Ω, es decir que para todo $k > o$ existe $S_k > o$ tal que $b_n - b_m \in B_{k+1}$ siempre que $n,m \geqslant S_k$

Consideremos, sin pérdida de generalidad, que $S_o \leqslant S_1 \leqslant \dots \leqslant S_k \leqslant \dots$ (con el objeto de que al exigir que $m \geqslant S_k$ sea también $m \geqslant S_i$ para $i = 1, \dots , k$)

Tomemos $i \in \mathbb{N}$, entonces $b_{s_{i+1}} - b_{s_i} \in B_{i+1}$ es decir que $b_{s_{i+1}} - b_{s_i} \in (a_1^{i+1}, \dots , a_n^{i+1})$. Por tanto existen elementos en R , llamémoslos r_{ji} $(j = 1, \dots , n)$ tales que

$b_{s_{i+1}} - b_{s_i} = \sum_{j=1}^{n} r_{ji} a_j^{i+1}$;llamemos $c_i = b_{s_i}$ para $i \geqslant o$ entonces

$$c_o = b_{s_o}$$

$$c_1 = c_o + \sum_{j=1}^{n} r_{j1} a_j$$

$$c_2 = c_1 + \sum_{j=1}^{n} r_{j2} a_j^2 = c_o + \sum_{j=1}^{n} r_{j1} a_j + \sum_{j=1}^{n} r_{j2} a_j^2$$

$$\vdots$$

$$C_{i+1} = c_i + \sum_{j=1}^{n} r_{j\,i+1}\, a_j^{i+1} = c_o + \sum_{j=1}^{n} \sum_{k=1}^{i+1} r_{jk}\, a_j^k$$

Es decir, que dada la sucesión Cauchy $\{b_i\}_{i \in \mathbb{N}}$ hemos construido una subsucesión $\{c_i\}_{i \in \mathbb{N}}$ tal que $c_i = c_o + \sum_{j=1}^{n} \sum_{k=1}^{i} r_{jk}\, a_j^k$, que además satisface que $c_{i+1} - c_i \in B_{i+1}$ para todo $i \geqslant 0$

Consideremos ahora para cada $j \in \{1,\dots, n\}$ la sucesión $\left\{\sum_{k=1}^{i} r_{jk}\, a_j^k\right\}_{i \in \mathbb{N}}$, que es una sucesión Cauchy en (R, a_j) y como esta topología es completa, entonces existe $b_j^* \in R$ tal que $\lim_{i \to \infty} \sum_{k=1}^{i} r_{jk}\, a_j^k = b_j^*$

(Precisamente este valor límite b_j^* es el que acostumbramos notar $\sum_{k=1}^{\infty} r_{jk}\, a_j^k$ cuando el espacio topológico es Hausdorff)

Tenemos entonces que:

$$\lim_{i \to \infty} c_i = \lim_{i \to \infty} \left[c_o + \sum_{j=1}^{n} \sum_{k=1}^{i} r_{jk}\, a_j^k\right] = c_o + \sum_{j=1}^{n} \left(\lim_{i \to \infty} \sum_{k=1}^{i} r_{jk}\, a_j^k\right)$$

$= c_o + \sum_{j=1}^{n} b_j^*$ (Este límite se acostumbra notar como $c_o + \sum_{j=1}^{n} \sum_{k=1}^{\infty} r_{jk}\, a_j^k$ cuando el espacio topológico es Hausdorff).

Asi pues R es un espacio completo con la topología $\mathcal{T}$ y por tanto (R,@) también es completo. ||

Con estos dos resultados que hemos obtenido podemos entonces hacer el siguiente enunciado global:

1.8 PROPOSICION: Sea R un anillo, $@$ un ideal finitamente generado de R y $(R,@)$ un espacio Hausdorff, entonces $(R,@)$ es completo si y solo si (R,a) es completo para todo $a \in @$. Además cada espacio (R,a) es Hausdorff.

Recordemos que el radical de Jacobson de un anillo R, notado frecuentemente por $J(R)$, es la intersección de todos los ideales maximales de R y tiene la siguiente caracterización: $x \in J(R)$ si y solo si $1 - xy$ es unidad de R para todo $y \in R$.

El siguiente lema, que no se refiere a ningún concepto topológico será de gran utilidad para extender el enunciado anterior.

1.9 LEMA: Sea R un anillo conmutativo con unidad y ϕ un R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \sum_{i=0}^{\infty} b_i x^i$. Entonces b_0 pertenece al radical de Jacobson de R.

Sabemos que $1 + rx$ es unidad de $R[[x]]$ para todo $r \in R$, y como ϕ es un R-endomorfismo entonces $\phi(1 + rx) = 1 + r\,\phi(x) = 1 + r \sum_{i=0}^{\infty} b_i x^i = 1 + rb_0 + r \sum_{i=1}^{\infty} b_i x^i$ y como ϕ deja fija la unidad también envía unidades en unidades, por tanto $1 + rb_0 + r \sum_{i=1}^{\infty} b_i x^i$ es unidad de $R[[x]]$, luego el término constante es unidad de R, es decir $1 + rb_0$ es unidad de R para todo $r \in R$. Por tanto b_0 es un elemento del radical de Jacobson de R.

Con la ayuda de este lema podemos enunciar un caso particular de la proposición anterior cuando el anillo R es Noetheriano.

1.10 PROPOSICION: Sea R un anillo Noetheriano y $@$ un ideal de R, entonces $(R,@)$ es un espacio Hausdorff completo si y solo si (R,a) es Hausdorff completo para todo $a \in @$.

Realmente es un caso particular de la proposición anterior porque por estar en un anillo Noetheriano se cumple:

i) Todo ideal $@$ de R es finitamente generado.

ii) Para cualquier ideal $@$ de R, $@ = (a_1, \dots, a_n)$ tenemos que si (R,a_i) es un espacio Hausdorff completo para todo $i = 1,\dots,n$ entonces existen R-endomorfismos ϕ_i de $R[[x]]$ tales que $\phi_i(x) = a_i + x$ (ver (18), prop. 4.3) y por tanto a_i pertenece a $J(R)$, el radical de Jacobson de R, luego $@ \subset J(R)$, y como $\bigcap_{n=1}^{\infty}(J(R))^n = (0)$ por ser R un anillo Noetheriano entonces $\bigcap_{n=1}^{\infty} @^n = (0)$, es decir $(R,@)$ es Hausdorff y efectivamente se cumplen todas las hipótesis de la proposición 1.4.

Otro resultado que se deduce fácilmente de la proposición 1.8 es el siguiente:

1.11 PROPOSICION: Sea $@$ un ideal del anillo R, tal que $(R,@)$ es Hausdorff completo. Entonces para cualquier ideal finitamente generado $B \subset @$, (R,B) es un espacio Hausdorff completo.

Hasta ahora hemos dado resultados que relacionan diversas topologías del mismo anillo R, ahora nos preocuparemos de relacionar topologías de R y de $R[[x]]$.

1.12 PROPOSICION: Sea $@$ un ideal del anillo R. Entonces $(R,@)$ es un espacio completo si y solo si $(R[[x]], @[[x]])$ es un espacio completo.

Supongamos que $(R[[x]], @[[x]])$ es completo, y sea $\{c_n\}_{n \in \mathbb{N}}$ una sucesión Cauchy de $(R,@)$.

Como $@^k \subseteq @^k[[x]]$ para todo $k \in \mathbb{N}$, se cumple que $\{c_n\}_{n \in \mathbb{N}}$ es una sucesión Cauchy en $(R[[x]], @[[x]])$ y como este espacio es completo existe una serie formal $g = \sum_{i=0}^{\infty} g_i x^i$ tal que $\lim_{n \to \infty} \{c_n\} = g$ en $(R[[x]], @[[x]])$.

Es decir que para todo $k > 0$ existe $N_k > 0$ tal que $g - c_n \in @^k[[x]]$ siempre que $n > N_k$.

Por tanto la serie formal $g_0 - c_n + \sum_{i=1}^{\infty} g_i x^i$ tiene coeficientes en $@^k$, luego $g_0 - c_n \in @^k$ siempre que $n > N_k$. Es decir $\lim_{n \to \infty} \{c_n\} = g_0$

en $(R,@)$, entonces este espacio es completo.

Recíprocamente, supongamos que $(R,@)$ es completo. Sea $\{g_i\}_{i \in \mathbb{N}}$ una sucesión Cauchy de $(R[[x]] , @[[x]])$ entonces $g_i = \sum_{j=0}^{\infty} a_{ij} x^j$ para todo $i \in \mathbb{N}$.

Como es una sucesión Cauchy en $(R[[x]] , @[[x]])$ se tiene que para todo $k > 0$ existe $N_k > 0$ tal que si $n,m \geqslant N_k$ entonces

$g_n - g_m = \sum_{j=0}^{\infty} (a_{nj} - a_{mj}) x^j \in @^k[[x]]$ es decir que para todo $j \in \mathbb{N}$ $a_{nj} - a_{mj} \in @^k$ o sea que para cada $j \in \mathbb{N}$ la sucesión $\{a_{ij}\}_{i \in \mathbb{N}}$ es una sucesión Cauchy en $(R,@)$, y por tanto existen $a_j^* \in R$ (para todo $j \in \mathbb{N}$) tales que $\lim_{i \to \infty} a_{ij} = a_j^*$ puesto que $(R,@)$ es completo.

Luego la serie formal $g = \sum_{j=0}^{\infty} a_j^* x^j$ satisface que $\lim_{i \to \infty} g_i = g$ y entonces $(R[[x]] , @[[x]])$ es completo. ∎

1.13 PROPOSICION: Sea $@$ un ideal del anillo R , entonces $(R,@)$ es Hausdorff si y solo si $(R[[x]] , @[[x]])$ es Hausdorff.

Es cierto pues $\bigcap_{k=1}^{\infty} @^k = (0)$ si y solo si $\bigcap_{k=1}^{\infty} @^k [[x]] = (0)$ ∎

1.14 COROLARIO: Si $@$ es un ideal finitamente generado de R se cumple que $(R,@)$ es Hausdorff completo si y solo si $(R[[x]],@[[x]])$ es Hausdorff completo.

Este corolario es cierto debido a que cuando $@$ es finitamente generado se tiene la igualdad $@^n R[[x]] = @^n[[x]]$ (ver 1.1) ||||

1.15 PROPOSICION : Sea R un anillo conmutativo con unidad, $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$, si (R,a_o) es Hausdorff entonces $(R[[x]], f)$ es Hausdorff

Dada la serie formal $f = \sum_{i=0}^{\infty} a_i x^i$ definamos el ideal $@ = \bigcap_{k=0}^{\infty} (a_o)^k$, y veamos que $\bigcap_{k=0}^{\infty} (f)^k \subseteq @[[x]]$. Supongamos que existe una serie formal $g \in \bigcap_{k=0}^{\infty} (f)^k$ tal que $g \notin @[[x]]$

Es decir que $g = \sum_{i=0}^{\infty} c_i x^i$ y tal que $c_n \notin (a_o)^p$ para algún $n \in \mathbb{N}$ y algún $p \in \mathbb{N}$.

Veamos qué significa que $g \in (f)^k$ cuando $n < k$.

$g = h f^k$ donde $h = \sum_{i=0}^{\infty} h_i x^i \in R[[x]]$

Entonces igualando coeficientes

$c_o = h_o a_o^k$

$c_1 = h_o a_o^{k-1} a_1 + h_1 a_o^k$

$$c_2 = h_o\,(a_o^{k-2} + a_1^{k-2}\,a_2\,) + h_1\,(a_o^{k-1}\,a_1\,) + h_2\,a_o^k$$

$$\vdots$$

$$c_n = \sum_{i=0}^{n} h_i \left\{ \begin{array}{l} \displaystyle\sum_{\substack{\alpha_o+\alpha_1+\ldots+\alpha_{n-i}=k \\ \alpha_1.1+\alpha_2.2+\ldots+\alpha_{n-i}(n-i)=n-i}} s_i\, a_o^{\alpha_o}\, a_1^{\alpha_1} \ldots\ldots a_{n-i}^{\alpha_{n-i}} \end{array} \right\} \qquad s_i \in R$$

Es decir que los exponentes α_j se pueden tomar de cualquiera de las formas que satisfagan para cada $i = 0,\ldots,n$

$$\alpha_1+\alpha_2+\ldots+\alpha_{n-i} = k-\alpha_o$$

$$\alpha_1+2\alpha_2+\ldots+(n-i)\alpha_{n-i} = n-i$$

Estamos interesados en saber cuál es el mínimo valor que puede tomar α_o, el coeficiente de a_o, para cada $i = 0,\ldots,n$ y esto se obtiene resolviendo para cada i el problema de

minimizar : $\alpha_o = -\alpha_1-\alpha_2-\ldots-\alpha_{n-i}+k$

sujeto a las restricciones: $\alpha_1+2\alpha_2+\ldots+(n-i)\alpha_{n-i} = n-i$

y $\alpha_j \geqslant 0$ entero , para $j=1,\ldots,n-i$

Que es un problema típico de programación lineal y tiene solución única para $\alpha_1 = n-i$ y $\alpha_j = 0$ para $j = 2,\ldots,n-i$ y el valor mínimo de α_o es $k - n + i$ para cada $i = 0,\ldots,n$. Por tanto el menor valor que puede tomar α_o es cuando $i = 0$, que es precisamente $\alpha_o = k-n$

Es decir $c_n \in (a_o)^{k-n}$ para todo $k > n$.

En particular, para $k = p + n$ tenemos que $c_n \in (a_o)^p$, lo que es absurdo.

Luego $g \in @[[x]]$.

Por tanto si (R,a_o) es Hausdorff tenemos que $@ = \bigcap_{k=1}^{\infty} (a_o)^k = (0)$ y por tanto $\bigcap_{k=1}^{\infty} (f)^k = (0)$, es decir que $(R[[x]], f)$ es un espacio Hausdorff. ∎

La siguiente proposición se sale un poco del esquema en el que veniamos trabajando de relacionar topologías de R con topologías de $R[[x]]$, y tiene como objetivo mostrar un tipo de conjuntos cerrados en la topologia $(R[[x]], @[[x]])$. Estos conjuntos cerrados los emplearemos en el capítulo siguiente.

1.16 PROPOSICION: Sea $@$ un ideal de R, $(R[[x]], @[[x]])$ un espacio Hausdorff, M el R-submódulo de $R[[x]]$ generado por $\{1,x,x^2,\dots,x^n\}$, entonces M es cerrado en $(R[[x]], @[[x]])$.

Necesitamos probar que cualquier sucesión de elementos en M que converja lo hace a un elemento de M.

Sea $\{m_i\}_{i \in \mathbb{N}}$ una sucesión convergente de elementos en M, y sea m el límite de esta sucesión, $m = \lim_{i \to \infty} m_i$.

Como $m_i \in M$ para cada $i \in \mathbb{N}$ entonces existen elementos $m_i^{(j)} \in R$ para $j = 0, \dots, n$ tales que $m_i = m_i^{(0)} + m_i^{(1)} x + \dots + m_i^{(n)} x^n$, por lo tanto podemos construir $n + 1$ sucesiones de elementos en R,

$\left\{ m_i^{(j)} \right\}_{i \in \mathbb{N}}$ con $j = 0, \ldots, n$

Como la sucesión $\left\{ m_i \right\}_{i \in \mathbb{N}}$ converge, entonces cada una de las sucesiones $\left\{ m_i^{(j)} \right\}_{i \in \mathbb{N}}$ también convergen, digamos que $\lim\limits_{i \to \infty} m_i^{(j)} = m^{(j)}$ con $m^{(j)} \in R$

Pero como estamos en un espacio Hausdorff los límites son únicos, entonces $\lim\limits_{i \to \infty} m_i = \lim\limits_{i \to \infty} m_i^{(0)} + \lim\limits_{i \to \infty} m_i^{(1)} x + \ldots + \lim\limits_{i \to \infty} m_i^{(n)} x^n$ o sea que $m = m^{(0)} + m^{(1)} x + \ldots + m^{(n)} x^n$ por tanto $m \in M$ ||||

2. TEOREMA DE PREPARACION

En este capítulo R es un anillo conmutativo con unidad; x una indeterminada sobre R y $R[[x]]$ el anillo de las series formales.

El objetivo central de este capítulo es estudiar tres proposiciones que conforman el llamado Teorema de Preparación de Weierstrass. Estos resultados nos permiten, dada una serie formal f con ciertas características, descomponer cualquiera otra serie formal g como $g = f.h + \eta$ donde h es una serie formal y η un polinomio en x.

Este resultado nos recuerda, por lo menos en la forma, el enunciado de la propiedad Euclidiana que se cumple en el anillo de polinomios $R[x]$ cuando R es un campo; esta propiedad nos permite garantizar que para todo $f, g \in R[x]$ existen polinomios h y η tales que $g = h f + \eta$ con grado $(\eta) \leqslant$ grado (f) y grado $(\eta) \leqslant$ grado (h). Es decir, que el Teorema de Preparación nos proporciona un cierto análogo de la Propiedad Euclidiana para el anillo de las series formales, pero claro está, exigiéndole a la serie formal f algunas condiciones topológicas.

Cuando trabajamos con el anillo de polinomios $R[x]$ es muy útil el concepto de que x sea algebraico sobre $R[f]$, siendo f cualquier

elemento de $R[x]$. En las series formales no existe este concepto; sin embargo una de las consecuencias del Teorema de Preparación nos permite hacer en las series formales un cierto análogo de lo que se hace en los polinomios. Lo que se cumple en las series formales es que si $f = \sum_{i=0}^{\infty} a_i x^i$ es una serie formal, tal que $(a_0, a_1, \dots, a_{n-1})$ genera una topología Hausdorff completa en R y a_n es unidad, entonces $R[[x]]$ puede ser considerado como un $R[[f]]$-módulo generado por el conjunto $\{1, x, \dots, x^{n-1}\}$. Y es esta última forma del Teorema de Preparación la que emplearemos en este trabajo.

Como este Teorema es la herramienta fundamental para el trabajo que desarrollaremos en el capítulo 4, le concedemos un capítulo especial.

El resultado que demostramos aquí es el más general que conocemos. Al final del capítulo enunciamos otros dos teoremas que también se conocen como Teorema de Preparación, y vemos que corresponden a casos particulares del resultado dado.

El resultado que sigue nos muestra que si f es una serie formal con ciertas condiciones, $R[[x]]$ se puede considerar como la suma directa de un módulo finitamente generado y el ideal generado por f.

2.1 TEOREMA: Sea R un anillo conmutativo con unidad, $f \in R[[x]]$, $f = \sum_{i=0}^{\infty} a_i x^i$; supongamos que para algún $n \geqslant 1$, a_n es una unidad de R, y que el ideal $@ = (a_0, a_1, \dots, a_{n-1})$ de R genera una topología Hausdorff completa sobre R. Si M es el R-submódulo de $R[[x]]$ generado por $\{1, x, x^2, \dots, x^{n-1}\}$, entonces $R[[x]] = M \oplus f.R[[x]]$.

Probemos primero que $f\,R[[x]] \cap M = \{0\}$

Sea $g \in f\,R[[x]] \cap M$ entonces $g = \left(\sum_{i=0}^{\infty} b_i x^i\right).\, f$ para $b_i \in R$ $(i \geqslant 0)$ y $g = \sum_{j=0}^{n-1} n_j x^j$ con $n_j \in R$ $(j = 0, \dots, n-1)$

Tenemos que probar que $g = 0$, y para ello basta probar que $b_i \in \bigcap_{k=0}^{\infty} @^k$ $(i \geqslant 0)$, y como $(R,@)$ es Hausdorff tendremos que $b_i = 0$ $(i \geqslant 0)$. (Ver 1.3)

Hagamos la prueba por doble inducción, mostrando que $b_i \in @^k$ para $i \geqslant 0$ y $k \geqslant 0$

- Para $k = 0$ se tiene porque $@^0 = R$ y $b_i \in R$ $(i \geqslant 0)$
- Supongamos que $b_i \in @^{k-1}$ $(i \geqslant 0)$. Probemos que $b_0 \in @^k$ para todo $k \in \mathbb{N}$. Como $b_0 a_n + b_1 a_{n-1} + \dots b_n a_0 = 0$ y como $b_i \in @^{k-1}$ entonces $b_1 a_{n-1} + \dots + b_n a_0 \in @^k$ por tanto $b_0 a_n \in @^k$ y como a_n es unidad entonces $b_0 \in @^k$

Supongamos ahora que $b_i \in @^k$ para $i < j$ y veamos que $b_j \in @^k$.

Como sabemos que

$$\sum_{i=0}^{\infty} b_i x^i \cdot \sum_{i=0}^{\infty} a_i x^i = n_o + n_1 x + \dots + n_{n-1} x^{n-1}$$

comparemos los coeficientes en las dos expresiones. En particular, comparando el coeficiente de x^{n+j} se tiene

$$(b_o a_{n+j} + b_1 a_{n+j-1} + \dots + b_{j-1} a_{n+1}) + b_j a_n + (b_{j+1} a_{n-1} + \dots + b_{j+n} a_o) = 0$$

como por hipótesis de inducción sabemos que $b_i \in @^k$ para $i < j$ tenemos que

$$(b_o a_{n+j} + \dots + b_{j-1} a_{n+1}) \in @^k$$

y como $b_i \in @^{k-1}$ $(i \geqslant 0)$ y $a_o, a_1, \dots, a_{n-1} \in @$, entonces

$$(b_{j+1} a_{n-1} + \dots + b_{j+n} a_o) \in @^k$$

concluimos entonces que $b_j a_n \in @^k$. Pero como a_n es unidad de R, entonces $b_j \in @^k$.

Luego $b_i = 0$ $(i \geqslant 0)$ y por tanto $g = \left(\sum_{i=0}^{\infty} b_i x^i \right) . f = 0$

Veamos ahora que $R[[x]] = M + R[[x]] . f$

Como $f = \sum_{i=0}^{\infty} a_i x^i$, donde a_n es unidad de R, podemos escribir

$f = a_o + a_1 x + \dots + a_{n-1} x^{n-1} + x^n \left(\sum_{i=n}^{\infty} a_i x^{i-n} \right)$ y si llamamos

$g = \sum_{i=n}^{\infty} a_i x^{i-n}$, tenemos que g es una unidad de $R[[x]]$ (por ser a_n unidad de R).

Entonces $f - x^n g = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \in @[[x]]$.

Definamos $h = x^n - f g^{-1} = \sum_{i=0}^{\infty} h_i x^i$. Luego $-h = (f - x^n g) g^{-1}$ y como $f - x^n g \in @[[x]]$ se cumple que $h \in @[[x]]$, pues $@[[x]]$ es un ideal de $R[[x]]$, es decir $h_i \in @$ para todo $i \geqslant 0$.

Sea ahora $P = \sum_{i=0}^{\infty} p_i x^i \in R[[x]]$. Con base en este elemento definamos un conjunto de elementos $\left\{q^{(j)}\right\}_{j=0}^{\infty}$ de $R[[x]]$ de la siguiente manera:

- $q^{(0)} = \sum_{i=0}^{\infty} q_i^{(0)} x^i$, donde $q_i^{(0)} = P_{i+n}$, para $i \geqslant 0$, es decir, que $P - x^n q^{(0)} = P_0 + P_1 x + \dots + P_{n-1} x^{n-1} \in M$ y por tanto $q^{(0)}$ es el único elemento de $R[[x]]$ que satisface la ecuación $P \equiv x^n q^{(0)}$ mod(M). Esta unicidad se cumple por la forma como fue definido $q^{(0)}$.

- Y para $j \geqslant 1$ sea $q^{(j)} = \sum_{i=0}^{\infty} q_i^{(j)} x^i$ donde para $i \geqslant 0$

$$q_i^{(j)} = \sum_{k=0}^{i+n} h_k q_{i+n-k}^{(j-1)}$$

Con esta definición por recurrencia vemos que para $j \geqslant 1$

$$h.q^{(j-1)} = \sum_{l=0}^{\infty} h_l x^l \cdot \sum_{i=0}^{\infty} q_i^{(j-1)} x^i$$

$$= \sum_{l=0}^{\infty} \left(\sum_{k=0}^{l} h_k q_{l-k}^{(j-1)} \right) x^l$$

$$= \sum_{l=0}^{n-1} \left(\sum_{k=0}^{l} h_k \, q_{l-k}^{(j-1)} \right) x^l + \sum_{l=n}^{\infty} \left(\sum_{k=0}^{l} h_k \, q_{l-k}^{(j-1)} \right) x^l$$

pero $S = \sum_{l=0}^{n-1} \left(\sum_{k=0}^{l} h_k \, q_{l-k}^{(j-1)} \right) x^l$ es un polinomio de grado menor que n, por tanto $S \in M$, y

$$\sum_{l=n}^{\infty} \left(\sum_{k=0}^{l} h_k \, q_{l-k}^{(j-1)} \right) x^l = x^n \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i+n} h_k \, q_{i+n-k}^{(j-1)} \right) x^i$$

$$= x^n \sum_{i=0}^{\infty} q_i^{(j)} \, x^i$$

$$= x^n \, q^{(j)}$$

Es decir, si $j \geqslant 1$ se tiene la congruencia

$$h \, q^{(j-1)} \equiv x^n \, q^{(j)} \pmod{M}$$

Veamos por inducción que $q^{(j)} \in @^j[[x]]$.

$q^{(o)} \in R[[x]]$, es decir $q_i^{(o)} \in @^o = R \quad (i \geqslant 0)$

ya que $h \, q^{(o)} \equiv x^n \, q^{(1)} \pmod{M}$ y los coeficientes de $q^{(1)}$ están dados por:

$q_i^{(1)} = \sum_{k=0}^{i+n} h_k \, q_{i+n-k}^{(o)}$ y como $h_k \in @$ entonces $q_i^{(1)} \in @ \quad (i \geqslant 0)$. Y así sucesivamente por inducción como

$q_i^{(j)} = \sum_{k=0}^{i+n} h_k \, q_{i+n-k}^{(j-1)}$ con $h_k \in @$ y $q_{i+n-k}^{(j-1)} \in @^{j-1}$ entonces

$q_i^{(j)} \in @^j$ para $i \geqslant 0$, $j \geqslant 0$

Formemos ahora la sucesión $\left\{ \sum_{j=0}^{t} q^{(j)} \right\}_{t=0}^{\infty}$ y consideremos la topología

$\frown$ inducida sobre $R[[x]]$ por la sucesión de ideales $\left\{ @^k[[x]] \right\}_{k=0}^{\infty}$.

Por ser @ un ideal finitamente generado, ésta es precisamente la topología $@R[[x]]$-ádica, que también hemos notado $(R[[x]], @R[[x]])$

La sucesión $\left\{ \sum_{j=0}^{t} q^{(j)} \right\}_{t=0}^{\infty}$ es Cauchy en $(R[[x]], \frown)$ porque para $m < n$ se tiene

$$\sum_{j=0}^{n} q^{(j)} - \sum_{j=0}^{m} q^{(j)} = \sum_{j=m+1}^{n} q^{(j)} \in @^m[[x]]$$

Es decir que para cualquier $k > 0$ basta tomar $N > k$ y se cumple la condición de que si $m,n > N$ entonces $\sum_{j=0}^{n} q^{(j)} - \sum_{j=0}^{m} q^{(j)} \in @^k[[x]]$

Esto nos permite encontrar un elemento único en $R[[x]]$ que sea el límite de la sucesión, ya que $(R[[x]], \frown)$ es Hausdorff, pues $(R,@)$ lo es. (Ver 1.13).

Sea $q \in R[[x]]$ el elemento tal que $\lim_{t \to \infty} \sum_{j=0}^{t} q^{(j)} = q$

como

$$p \equiv x^n q^{(o)} \quad (\text{Mod } M)$$

$$h\, q^{(o)} \equiv x^n q^{(1)} \quad (\text{Mod } M)$$

$$\vdots$$

$$h\, q^{(j-1)} \equiv x^n q^{(j)} \quad (\text{Mod } M)$$

$$\vdots$$

$$\text{entonces} \quad p + h \sum_{j=0}^{t-1} q^{(j)} \equiv x^n \sum_{j=0}^{t} q^{(j)} \pmod{M}$$

y esta congruencia es cierta para todo $t \geqslant 0$.

Si llamamos $m_t = p + h \sum_{j=0}^{t-1} q^{(j)} - x^n \sum_{j=0}^{t} q^{(j)}$ sabemos que $m_t \in M$ para todo $t \geqslant 0$ y como estamos en un espacio Hausdorff podemos tomar límite a ambos lados de la igualdad, es decir:

$$\lim_{t \to \infty} m_t = \lim_{t \to \infty} \left(p + h \sum_{j=0}^{t-1} q^{(j)} - x^n \sum_{j=0}^{t} q^{(j)} \right)$$

y como el límite de la derecha existe, también existe el límite de la izquierda, por tanto:

$$m = \lim_{t \to \infty} m_t = p + h\, q - x^n q$$

Como M es cerrado en la topología $(R[[x]], \cap)$, (ver 1.16) entonces $m \in M$

Luego $p = (x^n - h)\, q + m$ con $m \in M$. Pero por la definición de h se tiene $x^n - h = f\, g^{-1}$. Por tanto $p = f\, g^{-1} q + m$

$$\text{entonces} \quad R[[x]] = f.R[[x]] + M \quad \text{|||}$$

OBSERVACION: En la demostración usamos que $(R[[x]], \cap)$ es Hausdorff completo y que $(R,@)$ es Hausdorff, pero directamente no utilizamos que $(R,@)$ fuera completo. Esto podría hacernos pensar que esta condición puede suprimirse y exigir en las hipótesis del Teorema que $(R,@)$ sea Hausdorff y $(R[[x]], \cap)$ Hausdorff completo; sin embargo, ésto no tendría ninguna ventaja ya que en este caso, por ser @

finitamente generado, es equivalente que $(R,@)$ sea Hausdorff completo a que $(R[[x]],\frown)$ lo sea. (ver 1.14).

Como consecuencia de esta prueba tenemos también que f es un elemento regular (es decir, no es divisor de cero) en $R[[x]]$. Por eso podemos asegurar que la descomposición que se obtiene para los elementos de $R[[x]]$ es única; pues si para $p \in R[[x]]$ se tiene

$$p = h\,f + \sum_{i=0}^{n-1} v_i\, x^i \quad \text{con} \quad h \in R[[x]] \quad \text{y} \quad v_i \in R \quad (i=1,\ldots n-1)$$

$$p = h_1 f + \sum_{i=0}^{n-1} n_i\, x^i \quad \text{con} \quad h_1 \in R[[x]] \quad \text{y} \quad n_i \in R \quad (i=1,\ldots n-1)$$

entonces $$0 = (h - h_1)\, f + \sum_{i=0}^{n-1} (v_i - n_i)\, x^i$$

es decir $$(h - h_1)\, f = \sum_{i=0}^{n-1} (n_i - v_i)\, x^i \in R[[x]] \cap M$$

luego $$f\,(h - h_1) = 0 \quad \text{y por tanto} \quad h = h_1 \quad \text{y} \quad n_i = v_i \quad (i=1,\ldots\, n-1)$$

NOTACION: Sea $f \in R[[x]]$, si existe un único R-endomorfismo ϕ de $R[[x]]$ tal que $\phi(x) = f$ denotaremos por $R[[f]]$ al rango de ϕ que naturalmente es un subanillo de $R[[x]]$.

OBSERVACION: Podemos trabajar con la idea intuitiva que $R[[f]]$ está compuesto por las series formales evaluadas en la serie f; esta idea, sin embargo, no podemos utilizarla como definición porque faltarían nociones precisas sobre la convergencia que nos permitan explicar las sumas

infinitas que resultan.

En particular si $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ es tal que para algún n, a_n es unidad de R y que $@ = (a_0, a_1, \ldots, a_{n-1})$ genera una topología Hausdorff completa, entonces (por 1.5) R es Hausdorff completo en la topología (a_0)-ádica y por tanto existe un único R-endomorfismo ϕ de $R[[x]]$ tal que $\phi(x) = f$ (ver (9), 4.2 y 4.3); por tanto tiene sentido hablar de $R[[f]]$.

2.2 TEOREMA: Sea R un anillo conmutativo con unidad, $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ con a_n unidad de R para algún $n \geqslant 1$ y supongamos que el ideal $@ = (a_0, a_1, \ldots, a_{n-1})$ de R genera una topología Hausdorff completa sobre R; entonces $\{1, x, \ldots, x^{n-1}\}$ es una base libre para el módulo $R[[x]]$ sobre $R[[f]]$. O sea $R[[x]] = R[[f]] + x.R[[f]] + \ldots + x^{n-1}.R[[f]]$

Utilizamos en esta prueba el resultado anterior y trabajamos con el espacio topológico $(R[[x]], (f))$ que sabemos ya que es Hausdorff (ver 1.15). Como $R[[f]]$ es subanillo de $R[[x]]$ lo que debemos probar es que $R[[x]] \subseteq R[[f]] + R[[f]].x + \ldots + R[[f]]x^{n-1}$.

Seguiremos el siguiente esquema:

Primer paso: Para cada $k \geqslant 1$ construiremos un R-submódulo de $R[[f]]$

llamado T_k tal que $R[[x]] = f^k.R[[x]] + T_k.1 + T_k.x + \dots + T_k.x^{n-1}$

Segundo paso: Probamos que para todo $k \geqslant 1$ se cumple

$$f^k R[[x]] \cap (T_k.1 + T_k.x + \dots + T_k.x^{n-1}) = (0)$$

Es decir, que la suma en el paso uno es, en cierta forma, "directa"; y también se prueba que es "independiente" de k.

Tercer Paso: Probamos $R[[x]] = R[[f]] + R[[f]]\,x + \dots + R[[f]]\,x^{n-1}$

Cuarto Paso: Probamos que $\{1,x,\dots,x^{n-1}\}$ es base libre de $R[[x]]$ como $R[[f]]$ -módulo.

Primer Paso: Para $k \geqslant 1$ sea $T_k = f^{k-1} R + f^{k-2} R + \dots + f R + R$ el R-submódulo de $R[f]$ generado por $\{1,f,\dots,f^{k-1}\}$ es decir, $T_k = \left\{ \sum_{i=0}^{k-1} r_i f^i / r_i \in R \right\}$ En particular $T_1 = R$

Veamos por inducción sobre k que $R[[x]] = f^k R[[x]] + T_k \cdot 1 + \dots + T_k x^{n-1}$

Para $k=1$

Sabemos por el teorema anterior que $R[[x]] = f.R[[x]] + M$ donde M es el R-módulo generado por $\{1,x,\dots,x^{n-1}\}$; entonces como $T_1 = R$ se tiene $M = T_1.1 + T_1.x + \dots + T_1.x^{n-1}$ y por tanto se cumple el resultado para $k=1$

Supongamos ahora que el resultado es cierto para k y veámoslo para $k+1$

Como $T_{k+1} = f^k R + f^{k-1} R + \dots + f R + R$

$$= f^k R + T_k$$

es decir $T_k = T_{k+1} - f^k R$

y sabemos que $R[[x]] = f^k R[[x]] + T_k.1 + \dots + T_k.x^{n-1}$, entonces

$$R[[x]] = f^k R[[x]] + (T_{k+1} - f^k R).1 + (T_{k+1} - f^k R)\, x + \dots + (T_{k+1} - f^k R)x^{n-1}$$

$$= f^k R[[x]] + T_{k+1}.1 + T_{k+1}.x + \dots + T_{k+1}x^{n-1} - f^k R(1 + x + \dots + x^{n-1})$$

$$= f^k(R[[x]] - M) + T_{k+1}.1 + T_{k+1}.x + \dots + T_{k+1}\, X^{n-1}$$

y como $R[[x]] = f.R[[x]] + M$ entonces $R[[x]] - M = f\, R[[x]]$

luego $R[[x]] = f^{k+1} R[[x]] + T_{k+1}.1 + T_{k+1}.x + \dots + T_{k+1}.x^{n-1}$

Segundo Paso: Veamos ahora por inducción sobre k que

$$f\, R[[x]] \cap (T_k.1 + T_k.x + \dots + T_k\, x^{n-1}) = (0)$$

Para $k=1$ se conoce por el teorema anterior

Supongamos que es válido para k y veámoslo para $k+1$

Sea $g \in R[[x]]$ tal que $g\, f^{k+1} \in T_{k+1}.1 + T_{k+1}.x + \dots + T_{k+1}.x^{n-1}$

es decir $g\, f^{k+1} = \sum_{j=0}^{n-1} h_j\, x^j$ con $h_j \in T_{k+1}$

Por tanto $h_j = \sum_{i=0}^{k} n_i^{(j)} f^i$ con $n_i^{(j)} \in R$ para $i,j \geqslant 0$

entonces $g\, f^{k+1} = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k} n_i^{(j)} f^i \right) x^j$

$$= \sum_{j=0}^{n-1} n_k^{(j)} f^k x^j + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} n_i^{(j)} f^i \right) x^j$$

luego $\left(g\ f - \sum_{j=0}^{n-1} n_k^{(j)}\ x^j \right) f^k = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} n_i^{(j)}\ f^i \right) x^j$ es decir, que si

$p = g\ f - \sum_{j=0}^{n-1} n_k^{(j)}\ x^j$ se tiene que

$$p\ f^k \in f^k.R[[x]] \bigcap (T_k.1 + T_k.x + \ldots + T_k x^{n-1})$$

y entonces por hipótesis de inducción $p\ f^k = 0$. Pero como ya probamos que bajo estas condiciones f no es divisor de cero entonces $p = 0$

Luego $g\ f = \sum_{j=0}^{n-1} n_k^{(j)}\ x^j$ y ésto significa que $g\ f \in f\ R[[x]] \bigcap M$, es decir $g = 0$. Entonces $f^k\ R[[x]] \bigcap (T_k.1 + \ldots + T_k\ x^{n-1}) = (0)$ para $k \geqslant 1$

Nota: Veamos que esta propiedad probada para T_k nos permite concluir que hay una cierta "unicidad" en la forma de descomponer los elementos de $R[[x]]$ que no dependen de k.

Elijamos un $k \in \mathbb{N}$ fijo y sea $\alpha \in R[[x]]$; entonces α tiene representación como elemento de $f^k\ R[[x]] + T_k.1 + \ldots + T_k\ x^{n-1}$ dada por

$\alpha = f^k\ s_k + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} n_i^{(j)}\ f^i \right) x^j$, con $s_k \in R[[x]]$ y

$n_i^{(j)} \in R \quad \begin{matrix} i=0,\ldots,k-1 \\ j=0,\ldots,n-1 \end{matrix}$

y como elemento de $f^{k+p}\ R[[x]] + T_{k+p}.1 + \ldots + T_{k+p}\ x^{n-1}$ para $p \geqslant 1$

dada por $\alpha = f^{k+p}\ s_{k+p} + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{p+k-1} t_i^{(j)}\ f^i \right) x^j$ con $s_{k+p} \in R[[x]]$

y $\quad t_i^{(j)} \in R \,, \quad \begin{matrix} i=0,\dots,p+k-1 \\ j=0,\dots,n-1 \end{matrix}$

tenemos entonces

$$0 = f^k\,(f^p s_{k+p} - s_k) + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} (t_i^{(j)} - n_i^{(j)})\, f^i + \sum_{i=k}^{p+k-1} t_i^{(j)} f^i \right) x^j$$

luego

$$f^k\,(s_k - f^p\, s_{k+p} - \sum_{j=0}^{n-1} \sum_{i=k}^{p+k-1} t_i^{(j)}\, f^{i-k}\, x^j) = \sum_{j=0}^{n-1} \sum_{i=0}^{k-1} (t_i^{(j)} - n_i^{(j)}) f^i x^j$$

por tanto este término es igual a cero, es decir

$$\sum_{j=0}^{n-1} \sum_{i=0}^{k-1} (t_i^{(j)} - n_i^{(j)})\, f^i\, x^j = 0$$

o sea que $\quad t_i^{(j)} = n_i^{(j)} \quad$ para $\quad \begin{matrix} i=1,\dots,k-1 \\ j=1,\dots,n-1 \end{matrix}$

Esto significa que en la representación de α como elemento de $f^k\, R[[\,x\,]] + T_k.1 + \dots + T_k\, x^{n-1}$ los elementos $n_i^{(j)}$ para $i < k$ permanecen fijos cuando $k \longrightarrow \infty$

Tercer Paso: Sea $\alpha \in R[[x]]$ y consideremos la siguiente familia de conjuntos $\left\{ f^k\, R[[x]] + T_k.1 + \dots + T_k\, x^{n-1} \right\}_{k \in \mathbb{N}}$

Para cada $k \in \mathbb{N}$ existe una representación de α como elemento del correspondiente conjunto y se crea por tanto la siguiente sucesión

$$\left\{ f^k\, s_k + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} n_i^{(j)}\, f^i \right) x^j \right\}_{k \in \mathbb{N}} \quad \text{con} \quad s_k \in R[[\,x\,]] \text{ y}$$

$n_i^{(j)} \in R \quad , \quad i=1,\dots k-1 \quad , \quad j=1,\dots\, n-1$

Esta sucesión es precisamente $\{\alpha_k\}_{k \in \mathbb{N}}$, donde $\alpha_k = \alpha$ para $k \in \mathbb{N}$

Y como $R[[x]]$ es Hausdorff con la topología (f)-ádica y $\lim_{k \to \infty} \alpha_k = \alpha$

tenemos que el límite de esta sucesión existe y es único; luego

$$\lim_{k \to \infty} \left\{ f^k s_k + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} n_i^{(j)} f^i \right) x^j \right\} = \alpha$$

Veamos ahora que el límite de la izquierda es igual a

$$\sum_{j=0}^{n-1} \sum_{i=0}^{\infty} n_i^{(j)} f^i x^j$$

Sea $(f)^m$ una vecindad de 0 , sea $k \geqslant m$ entonces

$$\sum_{j=0}^{n-1} \sum_{i=0}^{\infty} n_i^{(j)} f^i x^j - \left(f^k s_k + \sum_{j=0}^{n-1} \left[\sum_{i=0}^{k-1} n_i^{(j)} f^i \right] x^j \right) =$$

$$= \sum_{j=0}^{n-1} \left(\sum_{i=k}^{\infty} n_i^{(j)} f^i \right) x^j - f^k s_k$$

$$= f^k \left[\sum_{j=0}^{n-1} \left(\sum_{i=k}^{\infty} n_i^{(j)} f^{i-k} \right) x^j - s_k \right] \in (f^k) \subset (f)^m$$

Luego $\alpha = \sum_{j=0}^{n-1} \sum_{i=0}^{\infty} n_i^{(j)} f^i x^j$

Y como para todo $j=1,\dots,n-1$, $\sum_{i=0}^{\infty} n_i^{(j)} f^i \in R[[f]]$ entonces

$$R[[x]] = R[[f]].1 + R[[f]].x + \dots + R[[f]]\, x^n$$

O sea que el conjunto $\{1, x, \dots x^{n-1}\}$ genera a $R[[x]]$ como módulo sobre $R[[f]]$.

Cuarto Paso: Veamos ahora que $\{1,x,\ldots,x^{n-1}\}$ es una base libre para $R[[x]]$ como $R[[f]]$ -módulo ; es decir, veamos que $\{1,x,\ldots,x^{n-1}\}$ es linealmente independiente.

Supongamos que para $k= 1,\ldots,n-1$, x^k pertenece al $R[[f]]$ -módulo generado por $\{1,x,\ldots,x^{k-1}\}$.

O sea

$$x^k = \sum_{j=0}^{k-1}\left(\sum_{i=0}^{\infty} r_i^{(j)} f^i\right) x^j \qquad \text{con } r_i^{(j)} \in R \quad i=0,\ldots\infty \ , \ j= 1,\ldots k-1$$

emtonces

$$x^k = r_0^{(0)} + r_0^{(1)} x + \ldots + r_0^{(k-1)} x^{k-1} + f\left(\sum_{j=0}^{k-1}\sum_{i=0}^{\infty} r_i^{(j)} f^{i-1} x^j\right)$$

si llamamos $g = \sum_{j=0}^{k-1}\sum_{i=0}^{\infty} r_i^{(j)} f^{i-1} x^j$ se tiene

$$x^k - \sum_{j=0}^{k-1} r_0^{(j)} x^j = f\,g \in f\,R[[x]] \cap M$$

luego $\quad 0 = f\,g = x^k - \sum_{j=0}^{k-1} r_0^{(j)} x^j \quad$ lo que es absurdo.

Por tanto $\{1,x,\ldots x^{n-1}\}$ es una base libre para $R[[x]]$ como $R[[f]]$ -módulo. ∎

2.3 COROLARIO : Sea $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$. Supongamos que para algún $n \geqslant 1$, a_n es una unidad de R y que el ideal $@ = (a_0, a_1, \ldots a_{n-1})$ de R genera una topología Hausdorff completa sobre R. Entonces existe un único par $F \in R[x]$ y $u \in R[[x]]$ tales que $f = u.F$, u unidad de $R[[x]]$ y $F = r_0 + r_1 + \ldots + r_{n-1} x^{n-1} + x^n$ con $r_i \in @$ para $i=1,\ldots,n-1$

Nota: Este corolario aparece con frecuencia citado como lema de preparación. Por ejemplo (2) cap. 7

Ya habiamos visto que bajo estas hipótesis f satisface que $R[[x]] = f.R[[x]] \oplus M$, donde M es el R-submódulo de $R[[x]]$ generado por $\{1, x, \ldots x^{n-1}\}$.

La representación de x^n como elemento de $f\,R[[x]] \oplus M$ es única. Sean $g = \sum_{i=0}^{\infty} g_i x^i \in R[[x]]$ y $r_0, r_1, \ldots r_{n-1} \in R$ los elementos que satisfacen la ecuación:

$$x^n = f\,g + (r_0 + r_1 x + \ldots + r_{n-1} x^{n-1})$$

entonces

$$-f\,g = \left(-\sum_{i=0}^{\infty} a_i x^i\right) . \left(\sum_{i=0}^{\infty} g_i x^i\right) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} - x^n$$

luego $$-\sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k g_{i-k}\right) x^i = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} - x^n$$

igualando los coeficientes tenemos

$$-r_o = a_o\, g_o$$

$$\vdots \qquad\qquad\qquad\qquad \text{si } k < n$$

$$-r_k = \sum_{j=0}^{k} a_j\, g_{k-j}$$

Por tanto $r_k \in (a_o, a_1, \dots a_{n-1}) = @$ para $k = 0,\dots n-1$ y en particular para el coeficiente de x^n tenemos

$$1 = \sum_{j=0}^{n} a_j\, g_{j-k} = a_o\, g_n + a_1\, g_{n-1} + \dots + a_n\, g_o$$

luego $$a_n\, g_o = 1 - (a_o\, g_n + \dots + a_{n-1}\, g_1)$$

Como R es un espacio Hausdorff con la topología @-ádica, @ está contenido en el radical de Jacobson de R (ver 1.9)

Si $h = a_o\, g_n + \dots + a_{n-1}\, g_1$ se cumple que $h \in @$, por tanto h es un elemento del radical de Jacobson de R, luego $1 - h$ es una unidad de R. Pero $1 - h = a_n\, g_o$ y a_n también es unidad de R, luego g_o es unidad en R.

Es así que la serie $g = \sum_{i=0}^{\infty} g_i\, x^i$ es una unidad de $R[[x]]$ por ser su coeficiente independiente, unidad de R. Por tanto existe $g^{-1} \in R[[x]]$, y tenemos que:

$$f = g^{-1}\left[x^n - (r_o + r_1\, x + \dots + r_{n-1}\, x^{n-1})\right]$$

si llamamos $u = g^{-1}$ y $F = x^n - r_o - r_1x - \dots - r_{n-1}x^{n-1}$ obtenemos el resultado deseado.

La unicidad de u y de F proviene de que la suma $f\,R[[x]] \oplus M$ es directa. ∎

OBSERVACION: El siguiente teorema ya no forma parte de los resultados que se conocen como Teorema de Preparación de Weierstrass , pero está muy relacionado y nos permite concluir que bajo nuestras hipótesis los resultados del Teorema 2.1 son equivalentes a los resultados del Teorema 2.2.

2.4 TEOREMA: Sea R un anillo conmutativo con unidad, $g \in R[[x]]$ tal que $(R[[x]], (g))$ es un espacio Hausdorff completo. Sea ϕ el único R-endomorfismo de $R[[x]]$ tal que $\phi(x) = g$, y sea $R[[g]]$ el rango de ϕ. Si T es un subanillo de $R[[x]]$ que contiene a $R[[g]]$, y si M es el R-submódulo de $R[[x]]$ generado por $\{1,x,\dots,x^{n-1}\}$, entonces los siguientes enunciados son equivalentes:

(i) $T = g\,T \oplus M$ y g **es un elemento regular en** T.

(ii) $\{1,x,\dots,x^{n-1}\}$ **es una base libre para** T **como módulo sobre** $R[[g]]$, y ϕ **es un R-endomorfismo uno a uno.**

Supongamos que se cumple (i)

Para probar que $\{1,x,\dots,x^{n-1}\}$ es una base libre para T como

$R[[g]]$ -módulo se sigue el mismo proceso que en la demostración de 2.2 tomando a T en lugar de $R[[x]]$.

Veamos que ϕ es uno a uno.

Sea $h = \sum_{j=0}^{\infty} h_j x^j \in R[[x]]$ tal que $\phi(h) = 0$

Consideremos la sucesión $\left\{ \sum_{j=0}^{k} h_j g^j \right\}_{k=0}^{\infty}$, sabemos (ver (**22**), 2.1) que $\phi(h)$ es el límite de esta sucesión en $(T,(gT))$

Sea $k > 0$. Probemos por inducción que $h_j = 0$ para $0 \leqslant j \leqslant k$ como $\lim_{k \to \infty} \sum_{j=0}^{k} h_j g^j = 0$ para la vecindad de cero $(g^{k+1} T)$ existe un $N \in \mathbb{N}$ y $N > k$ tal que

$$\sum_{j=0}^{s} h_j g^j \in (g^{k+1} T) \quad \text{para} \quad s \geqslant N$$

Sea $\alpha \in T$ tal que $\sum_{j=0}^{s} h_j g^j = g^{k+1} \alpha$

entonces, $h_o = -g\left(\sum_{j=1}^{s} h_j g^{j-1} - g^k \alpha \right)$, es decir, $h_o \in g\,T \cap M$

luego $h_o = 0$.

Supongamos que hemos probado que $h_j = 0$ para $0 \leqslant j < r \leqslant k$, y probemos que $h_r = 0$.

Como sabemos que $\sum_{j=r}^{s} h_j g^j = g^{k+1} \alpha$

entonces $g^r \left(\sum_{j=r}^{s} h_j g^{j-r} - g^{k+1-r} \alpha \right) = 0$

si llamamos $u = \sum_{j=r}^{s} h_j\, g^{j-r} - g^{k+1-r}$, $u \in T$ y $g\,u = 0$, luego $u=0$

Por tanto $h_r = -g\left(\sum_{j=r+1}^{s} h_j\, g^{j-(r+1)} - g^{k-r}\,\alpha \right)$ y por tanto $h_r = 0$

para $0 \leqslant j < r \leqslant k$

Luego $h = 0$ y así ϕ es un R-endomorfismo uno a uno.

Supongamos ahora que $\{1, x, \ldots, x^{n-1}\}$ es una base libre para T como $R[[g]]$-módulo y que ϕ es uno a uno.

Sea $p \in T$, entonces $p = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{\infty} r_i^{(j)}\, g^i \right) x^j$ con $r_i^{(j)} \in R$

$i > 0$

$j = 0, \ldots n-1$

Luego

$$p = \left(r_o^{(o)} + r_o^{(1)}\, x + \ldots + r_o^{(n-1)}\, x^{n-1} \right) - g \left(\sum_{j=0}^{n-1} \left(\sum_{i=1}^{\infty} r_i^{(j)}\, g^{i-1} \right) x^j \right)$$

es decir $p \in g\,T + M$, luego $T = g\,T + M$

Veamos ahora que esta suma es directa.

Sea $p \in T$ tal que $p\,g \in g\,T \cap M$

entonces $p = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{\infty} c_i^{(j)}\, g^i \right) x^j$ con $c_i^{(j)} \in R$

y $p\,g = r_o + r_1\, x + \ldots + r_{n-1}\, x^{n-1}$ con $r_j \in R$

$j = 0, \ldots n-1$

luego

$$0 = p\,g - (r_o + r_1 x + \ldots + r_{n-1}\, x^{n-1})$$

$$= \sum_{j=0}^{n-1} \left(- r_j + \sum_{i=0}^{\infty} c_i^{(j)} g^{i+1} \right) x^j$$

Y como $\{1, x, \ldots, x^{n-1}\}$ es una base libre para T como $R[[g]]$ - módulo, tenemos que todos los coeficientes son cero, es decir

$$- r_j + \sum_{i=0}^{\infty} c_i^{(j)} g^{i+1} = 0 \qquad \text{para } j=0,\ldots,n-1$$

Pero como $\phi \left(-r_j + \sum_{i=0}^{\infty} c_i^{(j)} x^{i+1} \right) = 0$ y ϕ es uno a uno

entonces $r_j = 0 = c_i^{(j)}$ para $j=0,\ldots,n-1$

y para $i \geqslant 0$

Luego $p\, g = 0$ y $g\, T \cap M = (0)$.

Además g es regular, porque de lo anterior concluimos que si $p\, g = 0$ entonces $p = 0$ ||

Veamos ahora los otros dos teoremas que se conocen también como Teorema de Preparación.

En Bourbaki ((2),cap 7, 28) se enuncia el Teorema de la siguiente forma

2.5 TEOREMA: Sea R un anillo conmutativo con unidad, local, $\mathfrak{M}$ su ideal maximal y supongamos que R es Hausdorff completo con la topología $\mathfrak{M}$-ádica. Sea $f \in R[[x]]$ una serie cuyo orden reducido es $n \neq 0$ y sea M el R-submódulo de $R[[x]]$ cuya base es $\{1, x, \ldots, x^{n-1}\}$. Entonces $R[[x]] = M \oplus f\,R[[x]]$ y f no es un divisor de cero en $R[[x]]$.

Este enunciado es un caso particular del 2.1 si R es un anillo local, $\mathfrak{M}$ su ideal maximal y $f = \sum_{i=0}^{\infty} a_i x^i$ es una serie cuyo orden reducido es $n \neq 0$, lo que tenemos es que el primer coeficiente de f que es unidad es a_n, $n \geqslant 1$, y por tanto $\{a_0, a_1, \ldots, a_{n-1}\} \subset \mathfrak{M}$, el único ideal maximal, luego si $\mathfrak{a} = (a_0, a_1, \ldots, a_{n-1})$, $\mathfrak{a} \subset \mathfrak{M}$, y como R es Hausdorff completo con la topología $\mathfrak{M}$-ádica entonces R también es Hausdorff completo con la topología $\mathfrak{a}$-ádica porque $\mathfrak{a}$ es finitamente generado (ver 1.6).

Por tanto se cumplen todas las hipótesis del Teorema 2.1, y se obtiene el resultado deseado.

La prueba de este teorema que hace Bourbaki es practicamente la misma que hemos hecho en el teorema 2.1.

En Zariski se tiene el enunciado siguiente: (ver (26),pág 139)

2.6 TEOREMA: Sea k **un campo y** $k[[x_1,x_2,\ldots,x_n]]$ **el anillo de las series formales en las indeterminadas** $\{x_1,\ldots,x_n\}$ **sobre** k.

Sea $F(x_1,\ldots,x_n) \in k[[x_1,\ldots,x_n]]$ **tal que** $F(x_1,\ldots,x_n)$ **contiene términos de la forma** $a\,x_n^h$, **con** $a \neq 0$, **y notemos por** s $(s \geqslant 1)$ **el menor de los exponentes** h **que tienen esta propiedad. Entonces para cada serie de potencias** $G(x_1,\ldots,x_n)$ **existe una serie de potencias** $U(x_1,\ldots,x_n)$ **y** s **series de potencias** $R_i(x_1,\ldots,x_{n-1})$ **en** $x_1,\ldots,x_{n-1}$ $(i=0,\ldots,s-1)$ **, tales que:**

$$G(x_1,\ldots,x_n) = U(x_1,\ldots,x_n)\,F(x_1,\ldots,x_n) + \sum_{i=0}^{s-1} R_i(x_1,\ldots,x_{n-1})\,x_n^i$$

Las series U **y** R_i **están unívocamente determinadas.**

Consideremos $R = k[[x_1,\ldots,x_{n-1}]]$ el anillo de las series formales en las indeterminadas $\{x_1,\ldots,x_{n-1}\}$; entonces R es un anillo local, pues su único ideal maximal es $\mathcal{M} = (x_1,\ldots,x_{n-1})$, ya que una serie formal es unidad si y solo si su término constante es unidad.

Además R es completo y Hausdorff con la topología $\mathcal{M}$-ádica.

También $k[[x_1,\ldots,x_n]] = k[[x_1,\ldots,x_{n-1}]]\,[[x_n]] = R[[x_n]]$ y la serie formal $F(x_1,\ldots,x_n) = f$ que tiene términos de la forma ax_n^s, con $s \geqslant 1$ y $\underline{a}$ una unidad de R , es una serie en $R[[x_n]]$ tal que su orden reducido es s ; entonces estamos bajo la hipótesis de 2.5 (y por tanto de 2.1)

y se cumple para cualquier serie $g \in R[[x_n]]$ que existe $u \in R[[x_n]]$ y $r \in R[[x_n]]$ tal que:

$$g = u f + r$$

Además u y r son únicos.

Pero como $g \in R[[x_n]]$ entonces $g = G(x_1,\ldots,x_n)$;

$u \in R[[x_n]]$ entonces $u = U(x_1,\ldots,x_n)$

y r es un polinomio de grado s con coeficientes en R , es decir:

$$r = \sum_{i=0}^{s} R_i(x_1,\ldots,x_{n-1})\, x_n^i \quad \text{con} \quad R_i \in k[[x_1,\ldots,x_{n-1}]]$$

o sea

$$G(x_1,\ldots,x_n) = U(x_1,\ldots,x_n)\, F(x_1,\ldots,x_n) + \sum_{i=0}^{s} R_i(x_1,\ldots,x_{n-1})\, x_n^i$$

3. GRUPO FINITO DE R-AUTOMORFISMOS DE $R[x]$

En este capítulo estudiamos el anillo de invariantes de un grupo finito de R-automorfismos de $R[x]$.

En la primera sección obtenemos como resultado que si R es un anillo entero conmutativo con unidad se cumple que $R[x]^G = R[f]$, con

$$f = \prod_{\phi \in G} \phi(x)$$

En la segunda sección consideramos el caso cuando el anillo R es entero, conmutativo sin unidad y logramos como nuevo resultado que

$R[x]^G = k[f] \cap R[x]$, donde k es el campo de fracciones de R. Este es el mejor análogo que podemos encontrar del resultado anterior.

La sección tercera es una recopilación de ejemplos de grupos finitos de R-automorfismos de $R[x,y]$. La única conclusión que podemos sacar de esta sección es que para el anillo de polinomios en varias variables no es posible encontrar ningún análogo del resultado obtenido para el anillo de polinomios en una variable.

Este capítulo es independiente de los dos anteriores, y perfectamente

hubiera podido ser el primero, pues para el trabajo con polinomios no se requiere ningún concepto topológico. Sin embargo adoptamos este orden para que los capítulos que hablan de anillos de invariantes, que son el cuerpo central de la tesis, estén uno a continuación del otro.

3.1 EL CASO DEL ANILLO CON UNIDAD

3.1.1 **PROPOSICION: Sea** R **un anillo conmutativo, entero, con unidad y** G **un grupo finito de** R**-automorfismos de** $R[x]$ **; entonces el anillo** $R[x]^G$ **de invariantes de** G **cumple que:** $R[x]^G = R[f]$ **donde** $f = \prod_{\phi \in G} \phi(x)$

Sea G un grupo de n R-automorfismos de $R[x]$.

Sabemos que para todo $\phi_i \in G$ $(i=1,\dots,n)$, $\phi_i(x) = c_i + b_i x$, con b_i un elemento inversible de R.

Si definimos $f = \prod_{i=1}^{n} \phi_i(x)$ tenemos que f es un polinomio de grado n, y además si $f = a_0 + a_1 x + \dots + a_n x^n$, entonces a_n es un elemento inversible en R (pues $a_n = b_1 b_2 \dots b_n$ y cada b_i es unidad)

Consideremos el anillo $R[f] \subset R[x]$;

como $x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \dots + \frac{a_0}{a_n} - f = 0$ con $\frac{a_{n-i}}{a_n} \in R \subset R[f]$

y $f \in R[f]$

se tiene que x es algebraico sobre $R[f]$. Entonces $R[x]$ es un $R[f]$-módulo con generación finita, y generado precisamente por el conjunto $\{1,x,x^2,\dots,x^{n-1}\}$ (ver (1), pág. 66, prop. 5.1)

Por tanto $R[x] = R[f] + R[f]\,x + \dots + R[f]\,x^{n-1}$ (1). Además, para todo $\phi_i \in G$, $\phi_i(f) = \phi_i(\prod_{j=1}^{n} \phi_j(x)) = \prod_{j=1}^{n} \phi_i.\phi_j(x) = \prod_{k=1}^{n} \phi_k(x) = f$

Es decir, f es invariante por todos los elementos de G, y por tanto $R[f] \subset R[x]^G$

Llamemos $s_i = \phi_i(x)$ para $\phi_i \in G$, $i=1,2,\dots,n$

Sea $g \in R[x]$ tal que $g \in R[x]^G$; entonces por (1) sabemos que $g = d_o + d_1\,x + d_2\,x^2 + \dots + d_{n-1}\,x^{n-1}$ con $d_j \in R[f]$, $j=0,\dots,n-1$

luego para todo $\phi_i \in G$, como $d_j \in R[f]$,

$$\phi_i(g) = \phi_i\left(\sum_{j=0}^{n-1} d_j\,x^j\right) = \sum_{j=0}^{n-1} d_j(\phi_i(x))^j = \sum_{j=0}^{n-1} d_j\,s_i^j = g$$

Tenemos entonces el siguiente sistema de ecuaciones:

$$\begin{aligned}
d_o + d_1\,s_1 + \dots + d_{n-1}\,s_1^{n-1} &= g \\
d_o + d_1\,s_2 + \dots + d_{n-1}\,s_2^{n-1} &= g \\
\vdots \qquad\qquad\qquad & \vdots \\
d_o + d_1\,s_n + \dots + d_{n-1}\,s_n^{n-1} &= g
\end{aligned}$$

o equivalentemente

$$\begin{bmatrix} 1 & s_1 & s_1^2 & \cdots & s_1^{n-1} \\ 1 & s_2 & s_2^2 & \cdots & s_2^{n-1} \\ \vdots & & & & \\ 1 & s_n & s_n^2 & \cdots & s_n^{n-1} \end{bmatrix} \begin{bmatrix} d_o \\ d_1 \\ \vdots \\ d_{n-1} \end{bmatrix} = \begin{bmatrix} g \\ g \\ \vdots \\ g \end{bmatrix}$$

El determinante de esta matriz es diferente de cero, pues es una matriz de Vandermonde y su determinante es $\prod_{i \neq j} (s_i - s_j)$ y todos los valores s_i son diferentes, por lo tanto, por estar trabajando en un anillo entero sabemos que existe una única solución al sistema. Si resolvemos el sistema por eliminación encontramos en el primer paso que:

$$\begin{bmatrix} 1 & s_1 & s_1^2 & \cdots & s_1^{n-1} \\ 0 & s_2-s_1 & s_2^2-s_1^2 & \cdots & s_2^{n-1}-s_1^{n-1} \\ 0 & & & & \vdots \\ \vdots & & & & \\ 0 & s_n-s_1 & s_n^2-s_1^2 & \cdots & s_n^{n-1}-s_1^{n-1} \end{bmatrix} \begin{bmatrix} d_o \\ d_1-d_o \\ d_2-d_o \\ \vdots \\ d_n-d_o \end{bmatrix} = \begin{bmatrix} g \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Por tanto la solución única se obtiene para $d_o=g$, y $d_1=d_2=\ldots=d_n=0$; luego $g=d_o \in R[f]$, y así $R[x]^G = R[f]$ ▥

OBSERVACION: Esta prueba se basa especialmente en que el anillo R es entero, y no es casual, porque esta condición no puede suprimirse. El siguiente ejemplo nos muestra ésto

3.1.3 Ejemplo: Sea $R = \mathbb{Z}/4\mathbb{Z}$

Consideremos el R-automorfismo $\phi : R[x] \longrightarrow R[x]$

$$x \longmapsto \phi(x) = -x$$

Entonces $\phi^2(x) = \phi(-x) = x$, es decir $\phi^2 = I$

Luego el grupo $G = \{I,\phi\}$ es un grupo finito de R-automorfismos de $R[x]$.

Calculemos $R[x]^G$

Sea $g \in R[x]^G$, $g = a_0 + a_1 x + \dots + a_n x^n$ con $a_i \in R$, $i = 1,2,..,n$

entonces $\phi(g) = a_0 - a_1 x + a_2 x^2 + .. + (-1)^n a_n x^n = a_0 + a_1 x + a_2 x^2 + .. + a_n x^n$

es decir $a_i = -a_i$ para todo $i = 2k + 1$

luego $a_i = \overline{0}$ ó $a_i = \overline{2}$ para $i = 2k + 1$

$$g \in R[x^2] + R[\overline{2}x] = R[x^2, \overline{2}x]$$

además cualquier elemento de este anillo es dejado invariante por ϕ , es decir $R[x]^G = R[x^2, \overline{2}x]$ y sin embargo $f = \prod_{\phi \in G} \phi(x) = -x^2$, por tanto no se satisface la conclusión de la proposición anterior ya que

$$R[x^2, \overline{2}x] \neq R[-x^2]$$

Además, tampoco puede hallarse ningún otro polinomio g tal que $R[x^2, \overline{2}x] = R[g]$, es decir, que no podemos pensar en extender el resultado en esta dirección.

3.1.4 **Nota:** Se conoce el siguiente resultado parcial, para anillos no enteros (ver (25) pág. 32 para detalles).

Sea R un anillo conmutativo con unidad, P un ideal primo de R, G un grupo finito de R-automorfismos de $R[x]$. Entonces

$$R[x]^G + P[x] = R[f] + P[x] \text{ , con } f = \prod_{\phi \in G} \phi(x)$$

3.2 EL CASO DEL ANILLO SIN UNIDAD

Consideremos ahora el caso en el que R es un anillo conmutativo, entero y sin unidad, y G un grupo finito de R-automorfismos. Veamos que el resultado ya obtenido acerca del anillo de invariantes de $R[x]$ por G cuando R es un anillo conmutativo entero con unidad es posible extenderlo de una cierta manera al caso de un anillo sin unidad.

Como R es entero, podemos construir su campo de fracciones K, y para un $s \in R$, $s \neq 0$ considerar la inyección canónica

$$\begin{aligned} R &\longrightarrow K \\ a &\longmapsto \frac{as}{s} \end{aligned}$$

Es decir, que todos los elementos de R los consideraremos como elementos de K, pero bajo la forma $\frac{as}{s}$. Obsérvese que la inyección no depende del s de R que hayamos tomado.

Dado un R-automorfismo ϕ de $R[x]$ tal que para $s \in R - \{o\}$

$$\phi(sx) = \sum_{i=0}^{n} a_i x^i \text{ , con } a_i \in R \quad (i=0,\ldots,n)$$

Sabemos que el R-automorfismo ϕ está unívocamente determinado por su acción sobre sx, para cualquier $s \in R - \{0\}$, ya que estamos considerando un anillo entero, pues si ς es otro R-automorfismo de $R[x]$ tal que $\phi(sx) = \varsigma(sx)$ entonces para cualquier $m \in R$ se cumple que: $s\,\phi(mx) = \phi(msx) = m\,\phi(sx) = m\,\varsigma(sx) = s\,\varsigma(mx)$, y como $s \neq 0$ entonces $\phi(mx) = \varsigma(mx)$

Igualmente para cualquier $m \in R$ y $n \in \mathbb{N}$ se tiene que

$$m^{n-1}\,\phi(mx^n) = \phi\left[(mx)^n\right] = \left[\phi(mx)\right]^n = \left[\varsigma(mx)\right]^n = \varsigma(m^n x^n)$$

luego $m^{n-1}\,\phi(mx^n) = m^{n-1}\,\varsigma(mx^n)$, es decir que $\phi(mx^n) = \varsigma(mx^n)$

Por tanto para cualquier polinomio $p \in R[x]$ se cumple que $\phi(p) = \varsigma(p)$ y se tiene que $\phi = \varsigma$.

A partir de ϕ podemos inducir un K-endomorfismo ϕ^* de $K[x]$ definiendo simplemente cuál es la imagen de x. En efecto,

$$\begin{aligned} \phi^* : K[x] &\longrightarrow K[x] \\ x &\longmapsto \phi^*(x) = \frac{\phi(sx)}{s} = \sum_{i=0}^{n} \frac{a_i}{s} x^i \end{aligned}$$

como cada $a_i \in R$, entonces $\frac{a_i}{s} \in K$ y por ello $\phi^*(x)$ es un polinomio de $K[x]$; además $\phi^*(t) = t$ para $t \in K$ por tanto ϕ^* está bien definido.

Con esta forma de definir a ϕ^* tenemos que $\phi^*/R[x] = \phi$ ya que si $q(x) \in R[x]$, $q(x) = \sum_{i=0}^{k} b_i x^i$ entonces

$$\phi^*\left(\sum_{i=0}^{k} b_i\, x^i\right) = \phi^*\left(\sum_{i=0}^{k} \frac{b_i s}{s}\, x^i\right)$$

$$= \sum_{i=0}^{k} \frac{b_i s}{s} \left[\phi^*(x)\right]^i$$

$$= \sum_{i=0}^{k} \frac{b_i s}{s} \left(\frac{\phi(sx)}{s}\right)^i$$

$$= \sum_{i=0}^{k} \frac{b_i s^{k-i}}{s^k} \left(\phi(sx)\right)^i$$

$$= \frac{\sum_{i=0}^{k} b_i s^{k-i} \left(\phi(sx)\right)^i}{s^k}$$

$$= \frac{\phi\left(\sum_{i=0}^{k} b_i s^{k-i}\, s^i x^i\right)}{s^k}$$

$$= \frac{s^k\, \phi\left(\sum_{i=0}^{k} b_i x^i\right)}{s^k}$$

$$= \phi\left(\sum_{i=0}^{k} b_i\, x^i\right)$$

Veamos ahora que ϕ^* es sobreyectivo, y para ello basta probar que x tiene preimagen por ϕ^*.

Como ϕ es sobreyectivo, existe un polinomio $q \in R[x]$ tal que $\phi(q(x)) = sx$ (para el s fijo que habíamos tomado)

entonces $\phi^*\left(\frac{q(x)}{s}\right) = \frac{\phi^*(q(x))}{s} = \frac{\phi(q(x))}{s} = \frac{sx}{s} = x$

Es decir ϕ^* es un K-endomorfismo sobreyectivo, por lo tanto también es inyectivo (ver (**16**), prop 1.3) , es decir ϕ^* es un K-automorfismo.

3.2.1 **OBSERVACION:** Aunque elegimos un elemento fijo $s \in R$ y a través de él hicimos la extensión del R-automorfismo ϕ al K-automorfismo ϕ^* es conveniente caer en la cuenta que ϕ^* es independiente del elemento s elegido; veamos ésto.

Supongamos que $t \in R$, $s \in R$ con $s \neq 0$ y $t \neq 0$, y sean ϕ_s^* y ϕ_t^* los K-automorfismos de $K[x]$ tales que

$\phi_s^*(x) = \frac{\phi(sx)}{s} = \sum_{i=0}^{n} \frac{a_i}{s} x^i$ y $\phi_t^*(x) = \frac{\phi(tx)}{t}$ entonces

$$\phi_s^*(x) = \frac{t}{t}\,\frac{\phi(sx)}{s} = \frac{s\,\phi(tx)}{ts} = \frac{\phi(tx)}{t} = \phi_t^*(x)$$

Y como los K-automorfismos están unívocamente determinados por la acción sobre x, entonces $\phi_s^* = \phi_t^*$

Por tanto, no importa cual sea el elemento s que tomemos siempre obtendremos el mismo K-automorfismo.

Consideremos ahora dos R-automorfismos ϕ , ς , tales que $\phi \neq \varsigma$, entonces $\phi^* \neq \varsigma^*$ porque como los R-automorfismos están unívocamente definidos por su acción sobre sx , por tanto $\phi(sx) \neq \varsigma(sx)$, es decir

$$\phi^*(x) = \frac{\phi(sx)}{s} \neq \frac{\varsigma(sx)}{s} = \varsigma^*(x)$$

Definamos ahora el conjunto $G^* = \{ \phi^* / \phi^*/R[x] = \phi$ para $\phi \in G \}$ Hasta el momento hemos probado que todos los elementos de G^* son K-automorfismos de $K[x]$, que la identidad es un elemento de G^* y que dos R-automorfismos diferentes inducen K-automorfismos diferentes, es decir, que el cardinal de G^* es igual al cardinal de G. Nuestro objetivo ahora es probar que G^* también es grupo, es decir, probar la siguiente proposición:

3.2.2 **PROPOSICION: Sea** R **un anillo conmutativo, entero, sin unidad,** K **el campo de fracciones de** R y G **un grupo de** R-**automorfismos** de $R[x]$, **entonces existe un grupo** G^* **de** K-**automorfismos de** $K[x]$ **tal que si** $\phi^* \in G^*$ **entonces** $\phi^*/R[x] \in G$. **Además el cardinal de** G^* **es igual al cardinal de** G.

Por las consideraciones que hicimos antes de enunciar la proposición falta probar solo que G^* es cerrado bajo el producto y que cada elemento de G^* tiene su inverso en G^*, y ambas cosas se deducen inmediatamente por la forma como fue construido G^*. Veámoslo:

Sean ϕ^* y ς^* dos elementos de G^*, entonces $\phi^*/R[x] = \phi$ y $\varsigma^*/R[x] = \varsigma$ y como $\phi \circ \varsigma \in G$ porque G es grupo, digamos $\phi \circ \varsigma = \psi$ entonces existe $\psi^* \in G^*$ tal que $\psi^*/R[x] = \psi$

Veamos que en efecto $\psi^* = \phi^* \circ \varsigma^*$. Para ello basta probar la igualdad al evaluar en x.

$$\phi^*(x) = \frac{\phi(sx)}{s} = \frac{\phi \circ Ç(sx)}{s} = \frac{\phi\ (\ Ç^*(sx)\ )}{s} = \frac{\phi\ (\ s\ Ç^*(x)\ )}{s} = \frac{\phi^*\ (s\ Ç^*(x)\ )}{s}$$

$$= \frac{s\ (\ \phi^* . Ç^*(x)\ )}{s} = \phi^* \circ Ç^*(x)$$

Igualmente se prueba que dado $\phi^* \in G^*$ existe $(\phi^*)^{-1}$ en G^* tal que $(\phi^*)^{-1} / R[x] = \phi^{-1}$

Es decir, que en efecto G^* es un grupo de K-automorfismos. Y los elementos de G^* están en una correspondencia uno a uno con los elementos de G. ⁞⁞

3.2.3 **Nota:** La propiedad de que $\phi \neq Ç$ si y sólo si $\phi^* \neq Ç^*$ es la que nos asegura que el número de elementos de G y el número de elementos de G^* son el mismo. En el caso que nos ocupa actualmente G es un grupo finito de R-automorfismos y por tanto G^* también es un grupo finito. En el capítulo 4 retomaremos el trabajo anterior, pero en el caso en el que G es un grupo infinito.

Con la herramienta que nos brinda esta proposición podemos enunciar el resultado central de esta sección, que es una generalización del obtenido cuando el anillo tiene unidad.

3.2.4 **TEOREMA: Sea** R **un anillo entero, conmutativo sin unidad,** K **el campo de fracciones de** R, G **un grupo finito de** R**-automorfismos** de $R[x]$, **entonces** $R[x]^G = K[f] \cap R[x]$ **siendo** $f = \prod_{\phi \in G} \phi(sx)$ y $s \in R$ **un elemento fijo,** $s \neq 0$.

Consideremos el grupo G^* de K-automorfismos de $K[x]$ que ya sabemos construir a partir de G.

$q \in R[x]^G$ si y solo si $q \in R[x]$ y $\phi(q) = q$ para todo $\phi \in G$ si y solo si $q \in R[x]$ y $\phi^*(q) = \phi(q) = q$, o sea que $q \in R[x] \cap K[x]^{G^*}$

Como K es un campo, en particular es un dominio entero con unidad y por ello satisface que si $f^* = \prod_{\phi^* \in G^*} \phi^*(x)$ entonces $K[x]^{G^*} = K[f^*]$

Pero como $\phi^*(x) = \dfrac{\phi(sx)}{s}$ entonces $f^* = \prod_{\phi \in G} \dfrac{\phi(sx)}{s}$; $f^* = \dfrac{\prod_{\phi \in G} \phi(sx)}{s^n}$

donde n es el cardinal de G

Si tomamos $f = s^n f^* = \prod_{\phi \in G} \phi(sx)$ tenemos que $f \in R[x]$ y

$(K[x])^{G^*} = K[f^*] = K[s^n f^*] = K[f]$, ya que s^n es invertible en en K ; entonces $(R[x])^G = K[f] \cap R[x]$ con $f = \prod_{\phi \in G} \phi(sx)$

3.2.5 **OBSERVACION:** Aunque $f \in R[x]$ no podemos garantizar que $K[f] \cap R[x] = R[f]$. Veamos un ejemplo en el que no se cumple.

Sea $R = 2\mathbb{Z}$, luego R es un anillo conmutativo, entero sin unidad, sea $\phi : R[x] \longrightarrow R[x]$ tal que $\phi(2x) = -2x$, claramente ϕ es un R-automorfismo, pues es simplemente la restricción a $R[x]$ del $\mathbb{Z}$-automorfismo de $\mathbb{Z}[x]$ que envía x en $-x$; y además $\phi^2(2x) = 2x$

Sea $G = \{I, \phi\}$. El campo de fracciones de R es Q, y $\phi^* : Q[x] \longrightarrow Q[x]$, y sea $G^* = \{I, \phi^*\}$; $f = \prod_{i=1}^{2} \phi_i(2x) = -4x^2$

$x \longmapsto -x$

ent. $(Q[x])^{G^*} = Q[-x^2] = Q[-4x^2]$ y en particular $f = -4x^2$ es invariante por G, sin embargo $f \notin R[-4x^2]$, pues en R no hay unidad.

Nota: El campo de fracciones Q de $2\mathbb{Z}$ es isomorfo al campo de los números racionales $\mathbb{Q}$.

3.3 GRUPOS FINITOS DE R-AUTOMORFISMOS DE $R[x,y]$

Si consideramos un grupo finito de R-automorfismos del anillo de polinomios en varias variables es natural pensar en extender el resultado que se conoce sobre el anillo de invariantes de un grupo finito de R-automorfismos de $R[x]$. Pero nos encontramos con dificultades de tal magnitud como que los R-automorfismos de $R[x_1,\ldots,x_n]$ no están aún clasificados.

Rápidamente encontramos ejemplos que nos permiten ver que el resultado no se cumple, lo que nos queda como interrogante es que si dado un grupo finito de R-automorfismos de $R[x_1,x_2,\ldots,x_n]$ no existirá un conjunto $\{f_1,f_2,\ldots,f_k\}$ de elementos de $R[x_1,x_2,\ldots,x_n]$ tal que $R[x_1,\ldots,x_n]^G = R[f_1,\ldots,f_k]$. El objetivo de nuestro trabajo fue intentar probar esta hipótesis, pero todos nuestros esfuerzos fueron infructuosos. De todo el trabajo realizado deseamos hacer acá un recuento de ejemplos de grupos finitos de R-automorfismos de $R[x,y]$, que puede ser de gran ayuda para alguien que desee investigar este problema. En el apéndice damos algunas explicaciones de la técnica original que diseñamos para construir dichos grupos de R-automorfismos.

Sabemos que los R-automorfismos de $R[x,y]$ están completamente determinados por su acción sobre x y sobre y. Empleamos las clasificaciones parciales de R-automorfismos que se encuentran en **(15)** y **(25)**, y en ninguno de los ejemplos hacemos pruebas.

3.3.1 **EJEMPLO:** El tipo más simple de R-automorfismo de $R[x,y]$ es aquel que restringido a $R[x]$ y a $R[y]$ continúa siendo un R-automorfismo. Este es un ejemplo de un grupo de R-automorfismos de este tipo.

Sean ϕ_1, $\phi_2 : \mathbb{Z}[x,y] \longrightarrow \mathbb{Z}[x,y]$ definidos por $\phi_1(x) = x$ $\quad \phi_1(y) = y$

$\phi_2(x) = -x$ $\quad \phi_2(y) = -$

Como $\phi_2^2 = \phi_1$ y ϕ_1 es la identidad entonces $G = \{\phi_1, \phi_2\}$ es un grupo finito de $\mathbb{Z}$-automorfismos.

Si definimos $f_1 = \prod_{\phi \in G} \phi(x) = -x^2$ y

$$f_2 = \prod_{\phi \in G} \phi(y) = -y^2$$

claramente $\mathbb{Z}[f_1, f_2] \subset \mathbb{Z}[x,y]^G$ pero el polinomio xy cumple que $\phi_2(xy) = \phi_2(x)\,\phi_2(y) = (-x)(-y) = xy$, es decir $xy \in \mathbb{Z}[x,y]^G$ pero $xy \notin \mathbb{Z}[f_1, f_2]$.

Esto prueba que ni aún en este caso tan simple el anillo de invariantes es fácil de estudiar.

3.3.2 Ampliemos el grupo anterior y consideremos los $\mathbb{Z}$-automorfismos de $\mathbb{Z}[x,y]$ dados por

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = -x \qquad \phi_2(y) = -y$$

$$\phi_3(x) = x \qquad \phi_3(y) = -y$$

$$\phi_4(x) = -x \qquad \phi_4(y) = y$$

Sea $G = \{\phi_1, \phi_2, \phi_3, \phi_4\}$, G es un grupo finito de $\mathbb{Z}$-automorfismos (ver apéndice para comprobar que en efecto es grupo).

En este caso las restricciones de los $\mathbb{Z}$-automorfismos a $\mathbb{Z}[x]$ o a $\mathbb{Z}[y]$ continuan siendo $\mathbb{Z}$-automorfismos pero no unívocamente determinados, como $\phi_1 / \mathbb{Z}[x] = \phi_3 / \mathbb{Z}[x]$ y $\phi_2 / \mathbb{Z}[x] = \phi_4 / \mathbb{Z}[x]$

$\phi_1 / \mathbb{Z}[y] = \phi_4 / \mathbb{Z}[y]$ y $\phi_2 / \mathbb{Z}[y] = \phi_3 / \mathbb{Z}[y]$

elijamos $f_1 = \phi_1(x) \cdot \phi_2(x) = -x^2$ y

$f_2 = \phi_1(y) \cdot \phi_2(y) = -y^2$

En este caso si se cumple que $\mathbb{Z}[x,y]^G = \mathbb{Z}[f_1,f_2]$.

3.3.3 **EJEMPLO:** ϕ_1 y ϕ_2 son los $\mathbb{Z}$-automorfismos de $\mathbb{Z}[x,y]$ definidos por $\phi_1(x) = x$ $\phi_1(y) = y$

$\phi_2(x) = y$ $\phi_2(y) = x$

Sea $G = \{\phi_1,\phi_2\}$ que claramente es grupo pues $\phi_2^2 = \phi_1$.

En este ejemplo vemos que si $f_1 = \phi_1(x)\ \phi_2(x) = xy$ y $f_2 = \phi_1(y) \cdot \phi_2(y) = xy$, entonces $f_1 = f_2$. Pero eso no significa que $\mathbb{Z}[x,y]^G = \mathbb{Z}[f_1]$ ya que el polinomio $x + y$ cumple $\phi_2(x+y) = x + y$, y $x+y \notin \mathbb{Z}[x\ y]$.

Observación: Lo que si es cierto es que $x+y = \phi_1(x) + \phi_2(x)$ y

$\mathbb{Z}[x,y]^G = \mathbb{Z}[xy,\ x+y]$.

3.3.4 **EJEMPLO:** Este ejemplo es análogo al anterior, y en este caso $G = \{\phi_1, \phi_2\}$ donde los $\mathbb{Z}$-automorfismos estan dados por:

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = -y \qquad \phi_2(y) = -x$$

Es cierto también que $f_1 = \phi_1(x)\,\phi_2(x) = \phi_1(y)\,\phi_2(y) = -xy = f_2$ y que el polinomio $\phi_1(x) + \phi_2(x) = x-y$ es dejado fijo por G. Además se cumple que $\mathbb{Z}[x,y]^G = \mathbb{Z}[-xy,\ x-y]$.

3.3.5 **EJEMPLO:** En este ejemplo formamos el grupo G obtenido al unir los dos grupos anteriores.

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = -x \qquad \phi_2(y) = -y$$

$$\phi_3(x) = y \qquad \phi_3(y) = x$$

$$\phi_4(x) = -y \qquad \phi_4(y) = -x$$

(ver el apéndice para la prueba de que en efecto es grupo). Se tiene que: $\mathbb{Z}[x,y]^G \subseteq \mathbb{Z}[xy,\ x^2 + y^2]$.

Los últimos ejemplos que consideramos tienen sólo como objeto mostrar grupos de R-automorfismos más complejos.

3.3.6 **EJEMPLO:** Consideremos los $\mathbb{Z}$-automorfismos de $\mathbb{Z}[x,y]$

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = x \qquad \phi_2(y) = 2x - y$$

$$\phi_3(x) = -x \qquad \phi_3(y) = -2x + y$$

$$\phi_4(x) = -x \qquad \phi_4(y) = -y$$

y sea $G = \{\phi_1, \phi_2, \phi_3, \phi_4\}$ (ver apéndice)

En este ejemplo los $\mathbb{Z}$-automorfismos restringidos a $\mathbb{Z}[x]$ continuan siendo $\mathbb{Z}$-automorfismos, por eso, la parte de $\mathbb{Z}[x]$ que es dejada fija por G es $\mathbb{Z}[-x^2]$, pero en general solo sabemos que $\mathbb{Z}[x,y]^G \subset \mathbb{Z}[x^2, f]$ donde $f = \prod_{\phi \in G} \phi(y) = y^2 (2x - y)^2$.

3.3.7 **EJEMPLO:** Sea $R = \mathbb{Z}_3$ y consideremos los siguientes R-automorfismos:

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = x \qquad \phi_2(y) = x+y$$

$$\phi_3(x) = x \qquad \phi_3(y) = -x+y$$

$$\phi_4(x) = -x \qquad \phi_4(y) = y$$

$$\phi_5(x) = -x \qquad \phi_5(y) = x+y$$

$$\phi_6(x) = -x \qquad \phi_6(y) = -x+y$$

El conjunto $G = \{ \phi_1, \phi_2, \ldots, \phi_6 \}$ es en efecto un grupo de R-automorfismos como lo podemos verificar en el apéndice. Acerca del anillo de invariantes $R[x,y]^G$ lo único que sabemos es que $R[x,y]^G \supseteq R[f_1, f_2]$ donde $f_1 = \phi_1(x)\, \phi_4(x) = -x^2$ y $f_2 = \phi_1(y) \cdot \phi_2(y)\, \phi_3(y) = y^3 - x^2 y$

4. GRUPO FINITO DE R-AUTOMORFISMOS DE $R[[x]]$

Sea R un anillo conmutativo, entero con unidad y $R[[x]]$ el anillo de las series formales en una indeterminada sobre R, y sea G un grupo finito de R-automorfismos de $R[[x]]$. El objetivo de este capítulo es probar que se cumple un resultado análogo al ya probado para el caso de estar trabajando con el anillo de polinomios, es decir, que

$R[[x]]^G = R[[f]]$, donde $R[[x]]^G$ es el anillo de invariantes bajo G

y $f = \prod_{\phi \in G} \phi(x)$.

En la segunda sección haremos algunas consideraciones de lo que sucede si trabajamos con un anillo entero, conmutativo sin unidad.

4.1 EL CASO DEL ANILLO CON UNIDAD

En esta sección consideramos el mismo problema que en la sección 3.1, ahora claro para el anillo de las series formales $R[[x]]$, y aunque obtenemos un resultado análogo no podemos emplear los mismos métodos, pues para el estudio de los R-automorfismos de $R[[x]]$ es necesario emplear conceptos topológicos y métodos de trabajo mucho más complejos.

Empezaremos con un lema que nos da información sobre el comportamiento de los R-automorfismos de $R[[x]]$.

4.1.1 LEMA: Sea R un anillo conmutativo con unidad, ϕ_1 y ϕ_2 R-automorfismos de $R[[x]]$ tales que:

$$\phi_1(x) = \alpha = \sum_{j=0}^{\infty} a_j x^j \quad , \quad \phi_2(x) = \sum_{j=0}^{\infty} b_j x^j = \beta$$

entonces se cumplen los siguientes resultados:

a. **Si $(R, (a_0))$ es un espacio Hausdorff, entonces el término constante de $\phi_1 \circ \phi_2(x)$ es un elemento del ideal (a_0, b_0) de R.**

b. **Si α pertenece al ideal (β) entonces $\alpha = h\beta$ donde h es una unidad de $R[[x]]$ y $a_0 = c\, b_0$ donde c es el término constante de h y por tanto una unidad de R.**

a. Como existe un R-automorfismo ϕ_1 tal que $\phi_1(x) = \alpha$ entonces $(R, (a_0))$ es completo y suponemos además que es Hausdorff; podemos entonces decir que

$$\phi_1 \circ \phi_2(x) = \phi_1(\beta) = \phi_1\left(\sum_{j=0}^{\infty} b_j x^j\right) = \lim_{n\to\infty} \sum_{j=0}^{n} b_j \left(\phi_1(x)\right)^j$$

$$= \lim_{n\to\infty} \sum_{j=0}^{n} b_j \left(\sum_{i=0}^{\infty} a_i x^i\right)^j$$

consideremos la sucesión en $R[[x]]$ dada por:

$$\left\{ \sum_{j=0}^{n} b_j \left(\sum_{i=0}^{\infty} a_i x^i \right)^j \right\}_{n\in\mathbb{N}} = \left\{ \sum_{j=0}^{n} b_j \left[a_o^j + \sum_{k=1}^{j} \binom{j}{k} a_o^{j-k} \left(\sum_{i=1}^{\infty} a_i x^i \right)^k \right] \right\}_{n\in\mathbb{N}}$$

$$= \left\{ \sum_{j=0}^{n} b_j a_o^j + x \sum_{j=0}^{n} b_j \left[\sum_{k=1}^{j} \binom{j}{k} a_o^{j-k} \left(\sum_{i=1}^{\infty} a_i x^{i-1} \right)^k \right] \right\}_{n\in\mathbb{N}}$$

Por tanto la sucesión de términos constantes de esta sucesión es la sucesión $\left\{ \sum_{j=0}^{n} b_j a_o^j \right\}_{n\in\mathbb{N}}$ que es una sucesión Cauchy en $(R, (a_o))$ y como este espacio es Hausdorff completo converge a un elemento de R.

Pero además podemos escribir esta sucesión como

$\left\{ b_o \right\}_{n\in\mathbb{N}} + \left\{ a_o \sum_{j=1}^{n} b_j a_o^{j-1} \right\}_{n\in\mathbb{N}}$, y la sucesión $\left\{ \sum_{j=0}^{n} b_j a_o^{j-1} \right\}_{n\in\mathbb{N}}$

también es sucesión Cauchy en $(R, (a_o))$, y por tanto también converge a un elemento de R, digamos $\lim_{n\to\infty} \sum_{j=0}^{n} b_j a_o^{j-1} = r$

entonces $\lim_{n\to\infty} \sum_{j=0}^{n} b_j a_o^j = b_o + a_o \lim_{n\to\infty} \sum_{j=0}^{n} b_j a_o^{j-1}$

$$= b_o + a_o r$$

Es decir, hemos probado que el término constante de $\phi_1 \circ \phi_2(x)$ es de la forma $b_o + a_o r$, o sea que pertenece al ideal (a_o, b_o) de R.

Observación: Como estamos trabajando con un anillo no necesariamente entero hubo que

suponer adicionalmente que $(R, (a_o))$ sea un espacio Hausdorff, pero si R es entero, se sabe que esto siempre es cierto (ver **(18)**, corolario 5.8), y por tanto se cumpliría esta parte a.)

b. Supongamos que $\alpha \in (\beta)$, es decir, que existe $h \in R[[x]]$, $h = \sum_{p=0}^{\infty} h_p x^p$ y tal que $\alpha = h\beta$ tenemos entonces:

$$\sum_{j=0}^{\infty} a_j x^j = \sum_{p=0}^{\infty} h_p x^p \cdot \sum_{i=0}^{\infty} b_i x^i$$

igualando los coeficientes tenemos :

$a_o = h_o b_o$ y $a_1 = h_o b_1 + h_1 b_o$ entonces $h_o b_1 = a_1 - h_1 b_o$

y como $b_o \in J(R)$ el radical de Jacobson de R(ver 1.7) entonces todos los elementos de la forma $1 - x b_o$ son unidades de R, y como b_1 es unidad de R entonces $1 - (a_1^{-1} h_1) b_o$ es unidad de R, luego $a_1 - h_1 b_o$ también es unidad y por tanto h_o es unidad de R.

Luego $h = \sum_{i=0}^{\infty} h_i x^i$ es unidad de $R[[x]]$, y en particular el término constante $a_o = h_o b_o = c\, b_o$, donde c es unidad de R. ⁞⁞

4.1.2 Recordemos que un ideal q de un anillo R es primario si $q \neq R$ y si $xy \in q$ entonces $x \in q$ o $y^n \in q$ para algún $n > 0$. Además si p es el menor primo que contiene a q se dice que q es p-primario.

Apoyándonos en este concepto podemos encontrar una propiedad netamente algebraica para la serie formal α cuando existe un R-automorfismo ϕ tal que $\phi(x) = \alpha$.

4.1.3 **PROPOSICION: Sea R un anillo entero, conmutativo con unidad y ϕ un R-automorfismo de $R[[x]]$ tal que $\phi(x) = \alpha$. Entonces para cada $k \in \mathbb{N}$ el ideal (α^k) es (α)-primario.**

Como R es dominio entero, $R[[x]]$ también es dominio entero, y como $R[[x]]/_{(x)} \simeq R$ entonces (x) es un ideal primo de $R[[x]]$, y para cualquier k el ideal (x^k) es primario, porque si $f\,g \in (x^k)$ y $f \notin (x^k)$ entonces $g = x\,h$ para $h \in R[[x]]$, y entonces $g^k \in (x^k)$.

Esto prueba que (x^k) es (x)-primario para cualquier k , y como ϕ es un R-automorfismo, la imagen de ideales primarios son ideales primarios, y la imagen de ideales primos son ideales primos, así (α^k) es (α)-primario para cada k. ∎

A partir del siguiente enunciado empezamos a considerar grupos finitos de R-automorfismos de $R[[x]]$.

4.1.4 PROPOSICION: **Sea** R **un dominio entero con unidad, y** $G = \{\phi_i\}_{i=1}^{n}$ **un grupo finito de** R**-automorfismos de** $R[[x]]$ **si** $f = \prod_{i=1}^{n} \phi_i(x)$ **, entonces** f **genera una topología Hausdorff completa sobre** $R[[x]]$ **.**

Si $B_i = \phi_i(x)$ para $i = 1,\ldots,n$ basta recordar que como ϕ_i es un R-automorfismo de $R[[x]]$ se tiene que $(R[[x]], (B_i))$ es un espacio Hausdorff completo, y como $f = \prod_{i=1}^{n} \phi_i(x) = \prod_{i=1}^{n} B_i \in (B_i)$ para $i=1,\ldots n$ se cumple que $(R[[x]], (f))$ también es un espacio Hausdorff completo (ver 1.5). ||||

La anterior proposición nos permite hablar de $R[[f]]$ cuando $f = \prod_{\phi \in G} \phi(x)$ pues se garantiza que existe un R-endomorfismo que envía a x en f (ver (**18**), prop. 2.1 y 2.2)

4.1.5 PROPOSICION: **Sea** R **un dominio entero con unidad, y** $G = \{\phi_i\}_{i=1}^{n}$ **un grupo finito de** R**-automorfismos,** $f = \prod_{i=1}^{n} \phi_i(x)$ **, entonces** $R[[f]] \subseteq R[[x]]^G$**. Es decir, los elementos de** G **actuan como la identidad sobre** $R[[f]]$ **.**

Claramente por la forma como está construido f se tiene que $\phi_i(f) = f$ para $i=1,\ldots,n$, ya que $\phi_i(f) = \phi_i\left(\prod_{j=1}^{n} \phi_j(x)\right) = \prod_{j=1}^{n} \phi_i \circ \phi_j(x) = \prod_{j=1}^{n} \phi_j(x) = f$

Sea $h \in R[[f]]$, entonces h es el límite de una sucesión de la forma $\left\{ \sum_{j=0}^{k} h_j f^j \right\}_{k \in \mathbb{N}}$ con $h_j \in R$, en la topología f-ádica, es decir $h = \lim_{k \to \infty} \sum_{j=0}^{k} h_j f^j$ luego, para cada $i=1,\ldots,n$ se tiene:

$$\phi_i(h) = \phi_i \lim_{k \to \infty} \sum_{j=0}^{k} h_j f^j = \lim_{k \to \infty} \phi_i \sum_{j=0}^{k} h_j f^j = \lim_{k \to \infty} \sum_{j=0}^{k} h_j f^j = h$$

4.1.6 **OBSERVACION:** Pudimos hacer esta prueba porque cada ϕ_i es continua en la topología f-ádica, ya que $\phi_i(f)=f$ (ver (**18**), lema 4.9)

Hasta el momento tenemos que $R[[f]] \subset R[[x]]^G$, de ahora en adelante nuestro objetivo será probar que $R[[x]]^G \subset R[[f]]$.

4.1.7 **PROPOSICION:** **Sea** R **un dominio entero con unidad, y** $G = \left\{ \phi_i \right\}_{i=1}^{n}$ **un grupo finito de** R**-automorfismos y supongamos que** T **es un subanillo de** $R[[x]]$ **tal que** $\phi_i(t) = t$ **para cada** i **y** t **en** T**. Si** $R[[x]]^G \subseteq T.1 + T.x + \ldots + T.x^{n-1}$ **entonces** $R[[x]]^G = T$

Nota: La demostración de esta proposición es básicamente igual a la demostración que habíamos hecho de la proposición 3.1.1. Por ello omitimos algunos detalles.

Supongamos que T es un subanillo de $R[[x]]$ tal que $\phi_i(t) = t$, para $i=1,\dots,n$ y para todo $t \in T$ y además $R[[x]]^G \subset T.1 + T.x + \dots + T.x^{n-1}$

Sea $g \in R[[x]]^G$, entonces $g = \sum_{i=0}^{n-1} t_i x^i$ con $t_i \in T$, $i=0,\dots,n-1$

y $\phi_j(g) = g = \sum_{i=0}^{n-1} \phi_j(t_i x^i) = \sum_{i=0}^{n-1} t_i \phi_j(x)^i = \sum_{i=0}^{n-1} t_i \beta_j^i$

Tenemos entonces el siguiente sistema de ecuaciones:

$$t_o + t_1 \beta_1 + t_2 \beta_1^2 + \dots + t_{n-1} \beta_1^{n-1} = g$$

$$t_o + t_1 \beta_2 + t_2 \beta_2^2 + \dots + t_{n-1} \beta_2^{n-1} = g$$

$$\vdots$$

$$t_o + t_1 \beta_n + \dots \qquad + t_{n-1} \beta_n^{n-1} = g$$

y como R es un dominio entero, también lo es $R[[x]]$, y por ello el sistema tiene solución única para $t_o = g$ y $t_i = 0$, $i=1,\dots,n-1$, es decir $g \in T$. Luego $R[[x]]^G = T$ ∎

4.1.8 OBSERVACION: Si $T = R[[f]]$ en la proposición anterior obtenemos que $R[[x]]^G = R[[f]]$, es decir que para llegar al resultado que buscamos debemos encontrar primero que se cumple la condición

$$R[[x]]^G \subset R[[f]] + R[[f]].x + \dots + R[[f]]\, x^{n-1}$$

4.1.9 PROPOSICION: Sea R un dominio entero con unidad y $G = \{\phi_i\}_{i=1}^{n}$ un grupo finito de R-automorfismos de $R[[x]]$, con $\phi_i(x) = R_i = \sum_{j=0}^{\infty} b_j^{(i)} x^j$ para $i=1,\dots,n$, $e = (b_o^{(1)}, b_o^{(2)}, \dots, b_o^{(n)})$ y si $\bigcap_{k\in\mathbb{N}} e^k = \{o\}$ entonces $R[[x]]^G = R[[f]]$, con $f = \prod_{i=1}^{n} \phi_i(x)$

Sea $f = \prod_{i=1}^{n} R_i = \sum_{j=0}^{\infty} a_j x^j$, veamos que bajo estas condiciones f satisface las hipótesis del Teorema de Preparación, es decir, que a_n es unidad y $@ = (a_o, a_1, \dots, a_{n-1})$ genera una topología Hausdorff completa sobre R.

Sabemos que para cada i, $b_o^{(i)}$ es un elemento de $J(R)$ el radical de Jacobson de R, y que $(R, b_o^{(i)})$ es un espacio Hausdorff completo, y además que $b_1^{(i)}$ es unidad. Igualando coeficientes tenemos:

$a_o = b_o^{(1)} b_o^{(2)} \dots b_o^{(n)} = 0$ es decir $a_o \in e \subset J(R)$

$a_1 = \sum_{\substack{r_1+r_2+\dots+r_n=1 \\ r_i \geqslant 0}} b_{r_1}^{(1)} b_{r_2}^{(2)} \dots b_{r_n}^{(n)}$, por tanto $n-1$ de los r_i debe ser cero, y se tiene que $a_1 \in (b_o^{(1)}, b_o^{(2)}, \dots, b_o^{(n)}) = e$

Así mismo para cada $i < n$ se cumple

$$a_i = \sum_{\substack{r_1+r_2+\dots+r_n=i \\ r_i \geqslant 0}} b_{r_1}^{(i)} \, b_{r_2}^{(i)} \dots b_{r_n}^{(i)}$$, y como $i < n$, alguno de los $r_i = 0$, y por tanto $a_i \in e$

es decir que $@ = (a_o, a_1, \dots, a_{n-1}) \subset e$ y como $\bigcap_{k \in \mathbb{N}} e^k = \{0\}$ se tiene también que $\bigcap_{k \in \mathbb{N}} @^k = \{0\}$. Por tanto $@$ genera una topología Hausdorff sobre R. Además como la topología $(R, b_o^{(i)})$ es completa para cada $i=1,\dots,n-1$, también (R,e) es completa (por ser e finitamente generado) . Y por tanto $(R,@)$ es completo. (ver 1.7 y 1.8)

Tenemos en definitiva que $(R,@)$ es Hausdorff completo. Consideremos ahora a a_n.

$$a_n = \sum_{r_1+r_2+\dots+r_n=n} b_{r_1}^{(1)} \, b_{r_2}^{(2)} \dots b_{r_n}^{(n)} = b_1^{(1)} \, b_1^{(2)} \dots b_1^{(n)} + \sum_{\substack{r_1+r_2+\dots+r_n=n \\ \text{con } r_j = 0 \text{ para algún } j}} b_{r_1}^{(1)} \dots b_{r_n}^{(n)}$$

si $p = \sum_{\substack{r_1+r_2+\dots+r_n=n \\ \text{con } r_j=0 \text{ para algún } j}} b_{r_1}^{(1)} \, b_{r_2}^{(2)} \dots b_{r_n}^{(n)}$ tenemos que $p \in e$ y como $e \subset J(R)$ entonces p es un elemento del radical de Jacobson de R, y por ello todos los elementos de la forma $1 - sp$, con $s \in R$, son unidades de R.

Si tomamos $s = b_1^{(1)} \, b_1^{(2)} \dots b_1^{(n)}$, s es una unidad de R porque cada $b_1^{(i)}$ lo es , luego $1 + s^{-1}p$ es unidad de R, por tanto s+p es

unidad, es decir, $a_n = s + p$ es unidad de R.

Y es así como estamos bajo las hipótesis del Teorema de Preparación de Weierstrass, y por tanto $R[[x]]^G$ es un módulo libre sobre $R[[f]]$ generado por $\{1, x, \ldots, x^{n-1}\}$, es decir,

$R[[x]]^G = R[[f]].1 + R[[f]]\,x + \ldots + R[[f]]\,x^{n-1}$ y entonces por los teoremas 4.1.5 y 4.1.7 tenemos que $R[[x]]^G = R[[f]]$. ∎

4.1.10 Nota: Este Teorema está bastante cerca del resultado que queremos, y si pudiéramos probar que bajo estas circunstancias el ideal $@ = (a_0, a_1, \ldots a_{n-1})$ satisface que $\bigcap_{k=0}^{\infty} @^k = \{0\}$ tendríamos ya la prueba. Debido a la imposibilidad de realizar la prueba en esta dirección tendremos que hacer otro trabajo. Sin embargo en algunos casos particulares si podemos obtener el resultado inmediatamente.

En particular si $e = (b_0^{(i)})$ se tiene el resultado, porque sabemos ya que $(R, b_0^{(i)})$ es Hausdorff completo.

Este caso particular lo usaremos para probar el resultado general.

4.1.11 COROLARIO: Si R es un dominio entero y $G = \{\phi_i\}_{i=1}^{n}$ es un grupo finito de R-automorfismos de $R[[x]]$, $f = \prod_{i=1}^{n} \phi_i(x)$ y si $\bigcap_{k\in\mathbb{N}} J(R)^k = \{0\}$ entonces $R[[x]]^G = R[[f]]$.

Como vimos en el 1.9 cada $b_o^{(i)}$ es un elemento de $J(R)$, el radical de Jacobson de R, por tanto el ideal $e = (b_o^{(1)}, b_o^{(2)}, \dots, b_o^{(n)})$ cumple que $e \subset J(R)$, entonces si $\bigcap_{k\in\mathbb{N}} J(R)^k = \{0\}$ también se cumple que $\bigcap_{k\in\mathbb{N}} e^k = \{0\}$, luego por el teorema 4.19 podemos concluir que $R[[x]]^G = R[[f]]$. ∎

4.1.12 Notas

a. En el caso de estar trabajando con un dominio entero Noetheriano sabemos por el Teorema de Krull (ver (1) cor 10.18) $\bigcap_{k\in\mathbb{N}} J(R)^k = \{0\}$ o sea que se cumple el teorema y $R[[x]]^G = R[[f]]$.

b. Existen demostraciones particulares de este resultado cuando R es un dominio entero, Noetheriano local y completo en Samuel (24), y cuando R es un anillo entero, Noetheriano y tal que su clausura íntegra sea un R-módulo finito en O'Malley (19)

4.1.13 **PROPOSICION: Sea R un dominio entero con unidad,**

$G = \{\phi_i\}_{i=1}^{n}$ **un grupo finito de R-automorfismos de** $R[[x]]$,

$f = \prod_{i=1}^{n} \phi_i(x)$ **,entonces** $R[[x]]^G = f.R[[x]]^G \oplus R$.

Como $f \in R[[x]]^G$ y $R \subset R[[x]]^G$ entonces

$(f.R[[x]]^G + R) \subset R[[x]]^G$.

Sea $\phi_i(x) = \beta_i = \sum_{j=0}^{\infty} b_j^{(i)} x^j$ y $f = \prod_{i=1}^{n} \phi_i(x) = \sum_{j=0}^{\infty} a_j x^j$; el término constante de f, $a_o = b_o^{(1)} b_o^{(2)} \dots b_o^{(n)} = 0$ ya que $b_o^{(i)} = 0$ para algún i, pues la identidad debe ser uno de los elementos de G; es decir $o(f) \geqslant 1$ entonces $f \notin R$ y por tanto $R \cap f\, R[[x]]^G = \{0\}$.

Además si $g \in R[[x]]^G$, $g = \sum_{j=0}^{\infty} g_j x^j$ entonces $g - g_o \in R[[x]]^G$ ya que éste es un subanillo, y los elementos de R son siempre dejados fijos por G. Por tanto, nos falta por probar que si $g \in R[[x]]^G$ y $o(g) \geqslant 1$ entonces $g \in f.R[[x]]^G$.

Sea $T = \{\phi_i(x)\}_{i=1}^{n} = \{\beta_i\}_{i=1}^{n}$ donde $\beta_i = \sum_{j=0}^{\infty} b_j^{(i)} x^j$

Definamos sobre T una relación de equivalencia "$\sim$" de la siguiente forma:

$\beta_i \sim \beta_j$ si y solo si $\beta_i = u_{ij}\, \beta_j$ donde u_{ij} es unidad de $R[[x]]$.

Obsérvese que por estar trabajando con un anillo R entero ésto se cumple si y solo si $(\beta_i) = (\beta_j)$. (ver proposición 4.1.1 parte b.)

Veamos que "$\sim$" es relación de equivalencia. Efectivamente

i) $\beta_i = 1.\beta_i$ donde 1 es unidad de $R[[x]]$

Nota: Es imprescindible entonces en esta prueba que el anillo sea unitario.

ii) Si $\beta_i = u_{ij}\,\beta_j$ entonces $\beta_j = u_{ij}^{-1}\,\beta_i$. Luego es simétrica.

iii) Si $\beta_i = u_{ij}\,\beta_j$ y $\beta_j = u_{jk}\,\beta_k$ entonces $\beta_i = u_{ik}\,\beta_k$ donde $u_{ik} = u_{ij}\circ u_{jk}$ que es unidad de $R[[x]]$.

Con esta relación de equivalencia se efectúa una partición del conjunto T en clases de equivalencia disjuntas $E_1, E_2, \ldots, E_k$ con $1 \leqslant k \leqslant n$

Haciendo una renumeración adecuada podemos decir que $\beta_1, \beta_2, \ldots, \beta_k$ son los representantes de las clases $E_1, \ldots, E_k$ respectivamente.

O sea que $E_j = \left\{ \beta \in T \,/\, (\beta) = (\beta_j) \right\}$ para $j=1,\ldots k$ y $T = \bigcup_{j=1}^{k} E_j$.

Consideremos además que $\beta_1 = x$ y por tanto E_1 es la clase de equivalencia de (x), entonces si $o(\beta_i) = 1$ para algún $i = 1,\ldots,n$ se cumple que $\beta_i = \sum_{j=1}^{\infty} b_j^{(i)} x^j = \left(\sum_{j=0}^{\infty} b_{j+1}^{(i)} x^j \right) x$ donde $b_1^{(i)}$ es unidad de R , luego $\sum_{j=0}^{\infty} b_{j+1}^{(i)} x^j$ es unidad de $R[[x]]$, y por tanto $\beta_i \in E_1$.

Nuestro objetivo ahora será partir el grupo G en subgrupos donde sea más fácil probar el resultado, y para ello necesitamos modificar los conjuntos E_j para que contengan el "cero". Por ello definimos los siguientes conjuntos para $j=1,\ldots,k$.

$$U_j = \left\{ \beta_r \in T \,/\, b_o^{(r)} \in \left(b_o^{(j)} \right) \right\}$$

Tenemos así por consiguiente que $\mathcal{U}_j$ es un subconjunto de T tal que $E_j \subset \mathcal{U}_j$, pues si $\beta_i \in E_j$ entonces $\beta_i \in (\beta_j)$ y entonces por el lema 3.2.1 se cumple que $b_o^{(i)} \in b_o^{(j)}$, es decir $\beta_i \in \mathcal{U}_j$.

Pero además E_1, la clase de equivalencia de (x) satisface que $E_1 \subset \mathcal{U}_j$ para todo $j=1,\ldots,k$, porque el coeficiente independiente de todos los elementos de E_1 es 0.

A partir de estos conjuntos $\mathcal{U}_j$, que satisfacen también que $T = \bigcup_{j=1}^{n} \mathcal{U}_j$ definamos:

$$H_j = \left\{ \phi_r \in G \ / \ \phi_r(x) = \beta_r \in \mathcal{U}_j \right\} \qquad \text{para} \quad j=1,\ldots,k$$

Veamos que cada H_j es un subgrupo de G.

i) Sean $\phi_r \in H_j$ y $\phi_p \in H_j$ entonces $\phi_r(x) = \beta_r \in \mathcal{U}_j$ y $\phi_p(x) = \beta_p \in \mathcal{U}_j$, por tanto $b_o^{(r)} \in \left(b_o^{(j)} \right)$ y $b_o^{(p)} \in \left(b_o^{(j)} \right)$, sabemos que $\left(R, \left(b_o^{(p)} \right) \right)$ es un espacio Hausdorff por ser R un anillo entero, y por tanto el término constante de $\phi_r \circ \phi_p$ es un elemento del ideal $\left(b_o^{(r)}, b_o^{(p)} \right)$ (lema 3.2.1 parte a.). Pero como $b_o^{(r)} \in \left(b_o^{(j)} \right)$ y $b_o^{(p)} \in \left(b_o^{(j)} \right)$ entonces $\left(b_o^{(r)}, b_o^{(p)} \right) \subset \left(b_o^{(j)} \right)$. Es decir, el término independiente de $\phi_r \circ \phi_p$ es un elemento de $b_o^{(j)}$, luego $\phi_r \circ \phi_p \in H_j$

ii) ϕ_1, que es la identidad, pertenece a H_j para $j=1,\ldots,k$ porque el término constante de $\phi_1(x) = x$ es un

elemento de cualquier ideal.

iii) Veamos que todo elemento de H_j tiene inverso en H_j.

Sea $\phi_r \in H_j$ y tal que ϕ_r no es la identidad. Como $\phi_r \in G$ y G es de orden finito, entonces ϕ_r también es de orden finito, digamos q, es decir $\phi_r^q = \phi_1$ y por ello $\phi_r^{q-1} = \phi_r^{-1}$, y como $\phi_r \in H_j$ y H_j es cerrado bajo la composición, tenemos que $\phi_r^{-1} = \phi_r^{q-1} \in H_j$.

Tenemos entonces que efectivamente H_j es un subgrupo de G para $j=1,\ldots,k$ y se cumple que $G = \bigcup_{j=1}^{k} H_j$; entonces $R[[x]]^G = \bigcap_{j=1}^{k} R[[x]]^{H_j}$

Veamos que para cada $j=1,\ldots,k$ se tienen las condiciones necesarias para calcular $R[[x]]^{H_j}$.

Enumeremos los elementos de $\mathcal{U}_j$ como $\underset{\sim}{B}^{(j_1)}, \underset{\sim}{B}^{(j_2)},\ldots,\underset{\sim}{B}^{(j_s)}$ y definamos

$f_j = \prod_{\phi \in H_j} \phi(x) = \prod_{i=1}^{s} \underset{\sim}{B}^{(j_i)}$ y $e = \left(b_o^{(j_1)}, b_o^{(j_2)},\ldots,b_o^{(j_s)} \right)$, el ideal de R generado por los coeficientes independientes de $\underset{\sim}{B}^{(j_i)}$ $(i=1,\ldots,s)$ satisface que $e \subset \left(b_o^{(j)}\right)$ y como $\bigcap_{k=0}^{\infty} \left(b_o^{(j)}\right)^k = \{0\}$ entonces se cumplen las condiciones del Teorema 4.1.9 . Por tanto $R[[x]]^{H_j} = R[[f_j]]$ y ésto se cumple para cualquier $j=1,\ldots,k$

Entonces $R[[x]]^G = \bigcap_{j=1}^{k} R[[f_j]]$ con $f_j = \prod_{\phi \in H_j} \phi(x)$

Sea $g \in R[[x]]^G$ con $o(g) \geqslant 1$, recordemos que deseamos probar que $g \in f.R[[x]]^G$

Como $g \in R[[x]]^G = \bigcap_{j=1}^{k} R[[f_j]]$ entonces $g \in R[[f_j]]$ para $j=1,\ldots,k$

y como $o(g) \geqslant 1$ entonces $g = t_j f_j$ para $t_j \in R[[x]]$ pero como

$E_j \subseteq U_j$ entonces $\left(\prod_{\underset{\sim}{P} \in U_j} \underset{\sim}{P}\right) \subset \left(\prod_{\underset{\sim}{P} \in E_j} \underset{\sim}{P}\right)$. Por tanto $f_j \in \left(\prod_{\underset{\sim}{P} \in E_j} \underset{\sim}{P}\right)$, es decir $f_j = h_j . \prod_{\underset{\sim}{P} \in E_j} \underset{\sim}{P}$ con $h_j \in R[[x]]$.

Sea c_j el cardinal de E_j y consideremos $E_j = \left\{ \underset{\sim}{P}^{(1)},\ldots,\underset{\sim}{P}^{(c_j)} \right\}$

si $\underset{\sim}{P} \in E_j$ entonces $(\underset{\sim}{P}) = (\underset{\sim}{P}_j)$ y por tanto por lema 4.1.1 (b) existen unidades $u_j^{(i)}$ de $R[[x]]$, $(i=1,\ldots,c_j)$ tal que $\underset{\sim}{P}^{(i)} = u_j^{(i)} \underset{\sim}{P}_j$ luego

$$\prod_{\underset{\sim}{P} \in E_j} \underset{\sim}{P} = u_j^{(1)} u_j^{(2)} \ldots u_j^{(c_j)} \underbrace{\underset{\sim}{P}_j \ldots \underset{\sim}{P}_j}_{c_j} = u_j \underset{\sim}{P}_j^{(c_j)} \text{ con } u_j \text{ unidad de } R[[x.]]$$

Es decir que $f_j = h_j u_j \underset{\sim}{P}_j^{c_j}$ y por tanto $g = t_j h_j u_j \underset{\sim}{P}_j^{c_j}$ para cada $j=1,\ldots,k$, o sea que $g = w_j \underset{\sim}{P}_j^{c_j}$ para $j=1,\ldots,k$ y $w_j \in R[[x]]$.

En particular para $j=1$ y $j=2$ se tiene que

$g = w_1 \underset{\sim}{P}_1^{c_1} = w_2 \underset{\sim}{P}_2^{c_2} \in \left(\underset{\sim}{P}_2^{c_2} \right)$, y como $\left(\underset{\sim}{P}_2^{c_2} \right)$ es $\left(\underset{\sim}{P}_2 \right)$-primario

(ver 3.2.2) se cumple que $\left(\mathfrak{P}_1^{c_1}\right)^m \in \left(\mathfrak{P}_2^{c_2}\right)$ para algún $m \in \mathbb{N}$ o que $w_2 \in \left(\mathfrak{P}_2^{c_2}\right)$. Como $\left(\mathfrak{P}_2^{c_2}\right) \subset (\mathfrak{P}_2)$ y $(\mathfrak{P}_2)$ es primo se sabe que si $\left(\mathfrak{P}_1^{c_1}\right)^m \in \left(\mathfrak{P}_2^{c_2}\right) \subset (\mathfrak{P}_2)$ entonces $\mathfrak{P}_1 \in (\mathfrak{P}_2)$, lo que no es posible por la escogencia que hicimos de $\mathfrak{P}_1$ y $\mathfrak{P}_2$. Por tanto $w_1 \in \left(\mathfrak{P}_2^{c_2}\right)$, es decir, existe $V_2 \in R[[x]]$ tal que $w_1 = V_2\, \mathfrak{P}_2^{c_2}$ luego $g = w_1\, \mathfrak{P}_1^{c_1} = V_2\, \mathfrak{P}_2^{c_2}\, \mathfrak{P}_1^{c_1}$.

De la misma forma se prueba que $V_2 \in \left(\mathfrak{P}_3^{c_3}\right)$ y así sucesivamente, para concluir finalmente que $g = w \prod_{j=1}^{k} \mathfrak{P}_j^{c_j}$, donde $w \in R[[x]]$.

Pero como para cada $\mathfrak{P}_i \in T$ se tiene $\mathfrak{P}_i \in E_j$ para algún $j=1,\ldots,k$ se cumple que existen unidades u_{ij} de $R[[x]]$ tales que si $\mathfrak{P}_i \in (\mathfrak{P}_j)$ entonces $\mathfrak{P}_i = u_{ij}\, \mathfrak{P}_j$ y por tanto

$$g = w \prod_{j=1}^{k} \mathfrak{P}_j^{c_j} = w \prod_{j=1}^{k} \left(\prod_{i=1}^{c_j} u_{ij}^{-1}\, \mathfrak{P}_i \right) = w\, u \prod_{j=1}^{n} \mathfrak{P}_j = t\, f$$

con $t \in R[[x]]$.

Pero como $g \in R[[x]]^G$ entonces $\phi_i(g) = g$ para $i=1,\ldots,n$ es decir $t\, f = \phi_i(t\, f) = \phi_i(t).\phi_i(f) = \phi_i(t).f$ para $i=1,\ldots,n$ y como $R[[x]]$ es dominio entero tenemos que $\phi_i(t) = t$ para todo $i=1,\ldots,n$ luego $t \in R[[x]]^G$.

Hemos probado entonces que $g = f.t \in f\, R[[x]]^G$, y por tanto que $R[[x]]^G = f\, R[[x]]^G \oplus R$. ▒

Con este teorema hemos hecho ya el trabajo principal para demostrar el resultado que nos interesa.

4.1.14 TEOREMA: **Sea** R **un anillo entero, conmutativo con unidad,** $G = \{\phi_i\}_{i=1}^{n}$ **un grupo finito de R-automorfismos de** $R[[x]]$, $f = \prod_{i=1}^{n} \phi_i(x)$ **entonces** $R[[x]]^G = R[[f]]$.

Si $f = \prod_{i=1}^{n} \phi_i(x)$ sabemos que $(R[[x]], (f))$ es un espacio Hausdorff completo (4.1.4), entonces estamos bajo las condiciones del Teorema 2.4. Además se cumple que $R[[x]]^G = f.R[[x]]^G \oplus R$, donde R es un R-módulo libre generado por $\{1\}$ y f es un elemento regular de $R[[x]]$ (porque $R[[x]]$ es dominio entero), por tanto, según la equivalencia del Teorema 2.4 se tiene que $\{1\}$ es una base libre para $R[[x]]^G$ como $R[[f]]$ -módulo, es decir $R[[x]]^G = R[[f]]$. ▒

4.2 ANILLOS SIN UNIDAD

Cuando R es un anillo entero conmutativo sin unidad y ϕ un R-automorfismo nos hacemos la pregunta de si será posible construir un K-automorfismo de $K[[x]]$, K el campo de fracciones de R, de igual manera que cuando ϕ era un R-automorfismo de $R[x]$.

Lamentablemente la respuesta es negativa, simplemente porque al hablar de R-automorfismos de $R[[x]]$ tenemos que considerar condiciones topológicas sobre el anillo R que no pueden extenderse fácilmente al campo de fracciones K de R.

El siguiente ejemplo justifica plenamente lo dicho.

4.2.1 **EJEMPLO:** Sea $R = 2\,\mathbb{Z}[[x]]$ el anillo de las series formales en la indeterminada x y con coeficientes en el anillo $2\,\mathbb{Z}$. De esta forma R es un anillo entero, conmutativo, sin unidad y Hausdorff completo con la topología $(2x)$-ádica (pues $\mathbb{Z}[[x]]$ es Hausdorff completo con la topología (x)-ádica.)

Consideremos el anillo de las series formales $R[[y]]$, siendo y una indeterminada sobre R.

Sea $\phi : R[[y]] \longrightarrow R[[y]]$ tal que $\phi(r) = r$ si $r \in R$ y $\phi(2y) = 2x + 2y$

ϕ es un R-automorfismo de $R[[x]]$ pues es simplemente la restricción del $\mathbb{Z}[[x]]$-automorfismo $\varsigma : \mathbb{Z}[[x]][[y]] \longrightarrow \mathbb{Z}[[x]][[y]]$ tal que $\varsigma(y) = x + y$, y de ς sabemos que es $\mathbb{Z}[[x]]$-automorfismo porque el coeficiente de y es unidad y el término constante x genera una topología Hausdorff completa en $\mathbb{Z}[[x]]$. (ver (**16**), prop. 5.20 y 6.1.5)

Sea K el campo de fracciones de R, y consideremos el anillo de las series formales $K[[x]]$.

Deseamos extender el R-automorfismo ϕ a un K-automorfismo ϕ^* de $K[[x]]$ de la misma forma como lo hacíamos en la sección 3.2.

Consideremos el elemento $2 \in R$, $2 \neq 0$, y definamos

$\phi^*(y) = \dfrac{\phi(2y)}{2} = \dfrac{2x + 2y}{2}$ es decir que $\phi^*(y) = x + y$ y $\phi^*(k) = k$

para todo $k \in K$.

Pero resulta que como K es campo y $x \neq 0$, entonces K no es un espacio Hausdorff completo con la topología (x)-ádica, por tanto ϕ^* no está bien definido como K-endomorfismo (ver (9), prop. 4.12).

Este ejemplo muestra lo diferente que es el trabajo con el anillo de polinomios al trabajo con el anillo de las series formales.

Con el objeto de evitar el tipo de problemas que se nos presentaron en el ejemplo anterior, podemos exigir condiciones sobre los R-automorfismos de $R[[x]]$ de tal forma que podamos aplicar los mismos argumentos que en la sección 3.2. Podemos por tanto hacer una proposición análoga a la proposición 3.2.2.

4.2.2 PROPOSICION: Sea R un anillo conmutativo, entero sin unidad, K el campo de fracciones de R, $s \in R$ con $s \neq 0$ y G un grupo de R-automorfismos de $R[[x]]$ tales que para todo $\phi \in G$ $\phi(sx) = \sum_{i=1}^{\infty} a_i x^i$, entonces existe un grupo G^* de K-automorfismos de $K[[x]]$ tales que si $\phi^* \in G^*$ entonces $\phi^* / R[[x]] \in G$. Además el cardinal de G es igual al cardinal de G^*.

Nota: Exigir la condición de que el término constante de $\phi(sx)$ sea cero para algún $s \in R$, $s \neq 0$, equivale a que el término constante de $\phi(rx)$ sea cero para cualquier $r \in R$.

Con esta condición que exigimos al grupo de R-automorfismos el método de la demostración de la proposición 3.2.2 puede calcarse, por tanto lo omitimos.

5. GRUPO INFINITO DE R-AUTOMORFISMOS

En este capítulo estudiaremos el anillo de invariantes bajo un grupo infinito de R-automorfismos de $R[x]$; haremos también algunas consideraciones cuando se trata de un grupo infinito de R-automorfismos de las series formales $R[[x]]$.

Daremos además algunos contraejemplos que nos muestran que no podemos extender el resultado obtenido para el anillo de polinomios en varias variables, ni para las series formales en varias variables.

5.1 TEOREMA: **Sea** R **un anillo conmutativo, entero y con unidad, y** G **un grupo infinito de** R-**automorfismos de** $R[x]$ **, entonces** $R[x]^G = R$

Sea K el cuerpo de fracciones de R. El anillo $R[x]$ también es un anillo entero, por tanto posee también un cuerpo de fracciones, llamémoslo T . Consideremos también el anillo $K[x]$ y su correspondiente cuerpo de fracciones, que se acostumbra notar por $K(x)$. Vemos que T y $K(x)$ son el mismo cuerpo, pues $x \in T$ y $K \subset T$ y como $K(x)$ es el menor cuerpo que contiene a x y a K entonces $K(x) \subset T$. Pero se sabe siempre que como $R[x] \subset K[x]$ entonces $T \subset K(x)$. Luego $R[x]$ y $K[x]$ tienen el mismo cuerpo de fracciones.

Sea $\phi \in G$ un R-automorfismo de $R[x]$. Podemos construir los siguientes automorfismos que hacen conmutar el siguiente diagrama:

$$\begin{tikzcd}
R[x] \arrow[r, "\phi"] \arrow[d] & R[x] \arrow[d] \\
K[x] \arrow[r, "\phi^*"] \arrow[d] & K[x] \arrow[d] \\
K(x) \arrow[r, "\phi^{**}"] & K(x)
\end{tikzcd}$$

donde $\phi^* / R[x] = \phi$ y $\phi^*(k) = k$ para todo $k \in K$ y $\phi^{**}\left(\frac{p}{q}\right) = \frac{\phi^*(p)}{\phi^*(q)}$ para todo $p/q \in K(x)$ y por tanto para todo $k \in K$, $\phi^{**}(k) = k$.

Es decir, a partir de ϕ inducimos un K-automorfismo ϕ^* de $K[x]$ y otro K-automorfismo ϕ^{**} de $K(x)$.

Además si $\phi^{**}(x) = \varsigma^{**}(x)$ entonces $\phi^*(x) = \varsigma^*(x)$ y también $\phi(x) = \varsigma(x)$.

Luego G genera un grupo infinito de K-automorfismos de $K[x]$, que notaremos G^*, y otro grupo infinito G^{**} de K-automorfismos de $K(x)$

Supongamos ahora que $f \in R[x]^G$, por tanto $\phi(f) = f$ y entonces $\phi^*(f) = f$ para todo $\phi^* \in G^*$ o sea que $f \in K[x]^{G^*}$.

Supongamos además que el grado de f es mayor o igual a 1, y que

$f = \phi(f) = a_0 + a_1 x + \dots + a_n x^n$ con $n \geqslant 1$ entonces x es algebraico sobre $K[f]$, y por tanto sobre $K(f)$, luego $K(x)$ es una extensión finita de $K(f)$ y como $\phi^{**}(f) = f$ para todo $\phi^{**} \in G^{**}$ entonces tenemos infinitos automorfismos que dejan a $K(f)$ fijo.

Pero por el teorema fundamental de la teoría de Galois (ver (13), teo. 5.5.6) sabemos que solo puede existir un grupo finito de estos automorfismos, lo que es absurdo; luego f tiene grado 0, es decir $f \in R$, y por ello $R[x]^G = R$ ||||

Veamos ahora que la condición de que R sea unitario puede ser suprimida, es decir, que el resultado acerca del anillo de invariantes bajo un grupo infinito de R-automorfismos de $R[x]$ es igual a R, cuando R es entero y conmutativo, independientemente de que tenga o no unidad. Este resultado no se conocía antes.

5.2 PROPOSICION: **Sea R un anillo entero, conmutativo sin unidad, y G un grupo infinito de R-automorfismos de $R[x]$, entonces $R[x]^G = R$**

Sea K el cuerpo de fracciones de R, como ya habíamos visto en 3.1.3 podemos extender cada R-automorfismo ϕ de $R[x]$ a un K-automorfismo ϕ^* de $K[x]$, con la característica de que si $\phi \neq Ç$ entonces $\phi^* \neq Ç^*$; por tanto el grupo infinito G induce un grupo infinito G^* de K-automorfismos.

Por el resultado anterior sabemos que $K[x]^{G^*} = K$ y

$R[x]^G = K[x]^{G^*} \cap R[x]$ pues si $f \in K[x]^{G^*} \cap R[x]$ entonces $f \in R[x]$ y $\phi^*(f) = \phi(f) = f$ para todo $\phi \in G$; es decir que $K[x]^{G^*} \cap R[x] \subset R[x]^G$.

Recíprocamente, si $f \in R[x]^G$ entonces $\phi(f) = f$ $\forall \phi \in G$, Por tanto $\phi^*(f) = \phi(f) = f$ para todo $\phi^* \in G^*$, es decir $R[x]^G \subset K[x]^{G^*} \cap R[x]$.

Luego $R[x]^G = K[x]^{G^*} \cap R[x] = K \cap R[x] = R$. ⁞⁞

Análogamente a lo que sucedía cuando considerábamos en el capítulo 3 un grupo finito de R-automorfismos de $R[x]$, la condición de que R sea entero no puede ser debilitada, es decir, que si R no es entero no podemos garantizar que el anillo de invariantes bajo un grupo infinito de R-automorfismos de $R[x]$ sea solamente R. Veamos un ejemplo:

5.3 EJEMPLO: Sean x,y indeterminadas sobre $\mathbb{Z}$ tales que $xy = yx = 0$

Sea $R = \mathbb{Z}[x,y]$, es decir que $R = \left\{ \sum_{i,j} a_{ij}\, x^i\, y^j \;/\; a_{ij} \in \mathbb{Z} \right\}$.

(Nótese que R no es el anillo de polinomios en las variables x y y con coeficientes en $\mathbb{Z}$). En R los elementos x y y son divisores de cero.

Este anillo R es conmutativo con unidad, pero no entero.

Sea z una variable independiente sobre R, y consideremos el anillo $R[z]$, y consideremos el R-automorfismo ϕ de $R[z]$ definido por $\phi(z) = x + z$. (En efecto es R-automorfismo porque el coeficiente de z es unidad de R). Ahora $\phi^n(z) = n\,x + z$ para todo $n \in \mathbb{Z}$, es decir, que si G es el grupo cíclico generado por ϕ, entonces G es un grupo infinito de R-automorfismos.

Consideremos el polinomio yz.

$\phi(yz) = y\,\phi(z) = y(x + z) = y\,x + y\,z = y\,z$.

Es decir que yz es dejado fijo por ϕ, y por tanto es dejado fijo por todo G. Luego $yz \in R[z]^G$, y ésto significa que $R[z]^G \neq R$.

Veamos ahora que el teorema tampoco se cumple para un grupo infinito de R-automorfismos del anillo de polinomios en varias variables. El siguiente ejemplo nos muestra ésto en el caso de un anillo de polinomios en 2 variables, aunque el anillo de coeficientes sea entero, conmutativo con unidad.

5.4 EJEMPLO: Sea $R = \mathbb{Z}$, y sea $\phi : R[x,y] \longrightarrow R[x,y]$ definido por $\phi(x) = x + (x + y)^2$ y $\phi(y) = y - (x + y)^2$

como $\phi(x - (x + y)^2) = x + (x + y)^2 - (x + (x + y)^2 + y - (x + y)^2)^2 = x$

y $\phi(y + (x + y)^2) = y - (x + y)^2 + (x + (x + y)^2 + y - (x + y)^2)^2 = y$

se tiene que ϕ es un R-endomorfismo sobreyectivo, y por tanto es inyectivo (ver (25), prop. 4.14)

Se cumple también que $\phi^n(x) = x + n(x + y)^2$ y $\phi^n(y) = y - n(x + y)^2$ para todo $n \in \mathbb{Z}$ (en particular ϕ^{-1} es el R-automorfismo definido por $\phi^{-1}(x) = x - (x + y)^2$ y $\phi^{-1}(y) = y + (x + y)^2$). Por tanto el grupo cíclico generado por ϕ es un grupo infinito de R-automorfismos.

Consideremos el polinomio $x + y$.

Como $\phi(x + y) = x + (x + y)^2 + y - (x + y)^2 = x + y$, es decir que $x + y$ es dejado fijo por ϕ , por tanto es dejado fijo por todo G. Luego $x + y \in R[x,y]^G$ y se concluye que $R[x,y]^G \neq R$.

A partir de los dos resultados anteriores acerca del anillo de invariantes bajo un grupo infinito de R-automorfismos de $R[x]$ podemos obtener el siguiente resultado que clasifica los R-automorfismos de $R[x]$ cuando R es entero y conmutativo.

Recordemos que un elemento ϕ de un grupo G se llama nilpotente si existe un entero K tal que $\phi^K = I$, donde I es la identidad de G. La siguiente proposición utilizará este concepto.

5.5 PROPOSICION: Sea R un anillo entero y conmutativo y ϕ un R-automorfismo de $R[x]$, entonces ó ϕ es nilpotente o los únicos invariantes de ϕ son los elementos de R.

Basta considerar el grupo cíclico G generado por ϕ , es decir

$$G = \{\phi^i / i \in \mathbb{Z}\}$$

Si ϕ no es nilpotente, entonces este grupo G es infinito, y por tanto $R[x]^G = R$ según los resultados anteriores, ahora, si $p \in R[x]$ es tal que $\phi(p) = p$ entonces $\phi^n(p) = \phi^{n-1}(\phi(p)) = \phi^{n-1}(p) = \dots = p$, es decir que $p \in R[x]^G$, luego $p \in R$.

Por tanto los únicos elementos que son dejados fijos por ϕ son los elementos de R ⁞⁞

Nota: Es importante recalcar que en la proposición anterior no se requiere que el anilo R tenga unidad.

La proposición anterior tiene una buena aplicación en el estudio de los grupos finitos de $\mathbb{Z}$-automorfismos del anillo $\mathbb{Z}[x]$.

5.6 APLICACION: Grupos finitos de $\mathbb{Z}$-automorfismos de $\mathbb{Z}[x]$.

Para que un $\mathbb{Z}$-automorfismo de $\mathbb{Z}[x]$ pertenezca a un grupo finito tiene que ser nilpotente, es decir que $\phi^k(x) = x$ para algún $k \geqslant 1$.

En $\mathbb{Z}[x]$ existen dos tipos de $\mathbb{Z}$-automorfismos; dependiendo de su acción sobre x. El primer tipo es aquel en el que $\phi(x) = m + x$ para algún $m \in \mathbb{Z}$. Y el segundo tipo de $\mathbb{Z}$-automorfismo es aquel en el que $\phi(x) = m - x$ para $m \in \mathbb{Z}$.

Si un $\mathbb{Z}$-automorfismo del primer tipo fuera nilpotente tendríamos que para algún $k \geqslant 1$ $\phi^k(x) = x$, pero $\phi^k(x) = x + k\,m$, es decir que

$k\,m = 0$, luego $m = 0$.

Por tanto el único $\mathbb{Z}$-automorfismo de este tipo que puede pertenecer a un grupo finito es la identidad.

Ahora, si consideramos cualquier $\mathbb{Z}$-automorfismo del segundo tipo tenemos que $\phi^2(x) = \phi(m - x) = m - (m - x) = x$, es decir, que todos los $\mathbb{Z}$-automorfismos de este segundo tipo son de orden 2.

Si llamamos ϕ_m al $\mathbb{Z}$-automorfismo tal que $\phi_m(x) = m - x$ podemos formar grupos finitos de $\mathbb{Z}$-automorfismos de la forma $\{ I, \phi_m \}$ para cada $m \in \mathbb{Z}$.

Estos son los únicos grupos finitos de $\mathbb{Z}$-automorfismos que podemos formar, pues $\phi_m \circ \phi_n(x) = \phi_m(n - x) = n - (m - x) = (n - m) + x$, es decir, que la composición de dos $\mathbb{Z}$-automorfismos del segundo tipo siempre dará uno del primer tipo. Por tanto ningún grupo finito puede tener más de 2 elementos.

5.7 OBSERVACION: Nótese que la aplicación anterior es la caracterización de todos los grupos finitos de R-automorfismos, donde R es isomorfo a $\mathbb{Z}$.

Deseamos ahora estudiar el anillo de invariantes bajo un grupo infinito de R-automorfismos de $R[[x]]$.

El artículo de J. Castillon "Réciproque à un Théorème de P. Samuel"

afirma que si R es un anillo conmutativo, entero y unitario, G es un grupo infinito de R-automorfismos de $R[[x]]$ entonces $R[[x]]^G = R$; y para la demostración utiliza el mismo razonamiento que cuando se trabaja en el anillo de polinomios. Pero esta prueba no puede efectuarse de esa forma, pues se usa el hecho de que si K es el campo de fracciones de R entonces el campo de fracciones del anillo $R[x]$ y el campo de fracciones de $K[x]$ son iguales; sin embargo en general no es cierto que el campo de fracciones de $R[[x]]$ sea igual al campo de fracciones de $K[[x]]$. Veamos un caso en el que esta igualdad no es cierta.

5.8 EJEMPLO: Sea R un anillo entero, conmutativo y K su cuerpo de fracciones, recordemos que R es un dominio de valoración discreta v , si existe una aplicación $v : K^* \longrightarrow \mathbb{Z}$, donde $K^* = K - \{o\}$ tal que :

i) $v(xy) = v(x) + v(y)$, es decir, v es un homomorfismo

ii) $v(x + y) \geqslant \min \{ v(x), v(y) \}$

iii) $R = \{o\} \cup \{ x \in K^* \ / \ v(x) \geqslant o \}$

Consideremos para nuestro ejemplo un anillo R de valoración discreta v, K es su cuerpo de fracciones, L es campo de fracciones de $R[[x]]$ y T el campo de fracciones de $K[[x]]$.

Como $L = \{ p/_q \ / \ p,q \in R[[x]] \}$, entonces $K \subset L$ y $K[x] \subset L$, el problema radica en que no necesariamente $K[[x]]$ es subconjunto de L. Supongamos que la serie $\sum_{i=0}^{\infty} z_i \, x^i \in K[[x]]$ también es elemento de L,

es decir, existen $\sum_{i=0}^{\infty} b_i x^i \in R[[x]]$ y $\sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ tal que

$$\sum_{i=0}^{\infty} z_i x^i = \frac{\sum_{i=0}^{\infty} b_i x^i}{\sum_{i=0}^{\infty} a_i x^i} \qquad a_i , b_i \in R$$

luego $$\sum_{i=0}^{\infty} z_i x^i \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} b_i x^i$$

Supongamos que $a_o \neq 0$ (esta suposición no resta generalidad, pues de lo contrario dividimos por la potencia adecuada de x)

Tenemos entonces que para todo $n \in \mathbb{N}$, $z_n a_o + z_{n-1} a_1 + \ldots + z_o a_n = b_n$

Veamos por inducción que $v(z_n) \geqslant -(n + 1) v(a_o)$

Para $n = 0$, se tiene que $z_o a_o = b_o$, entonces por las propiedades de v tenemos $v(z_o) + v(a_o) = v(b_o) \geqslant 0$ por ser $b_o \in R$ luego $v(z_o) \geqslant -(1) v(a_o)$

Supongamos que el resultado es válido para $K < n$, y veámoslo para n.

$$z_n a_o = b_n - z_{n-1} a_1 - \ldots - z_o a_n$$

luego $$v(z_n) + v(a_o) \geqslant \min \left\{ v(b_n), v(-z_{n-1} a_1), \ldots , v(-z_o a_n) \right\}$$

Si $v(b_n)$ es el mínimo entonces $v(z_n) + v(a_o) \geqslant v(b_n) \geqslant 0$

Por tanto se cumple naturalmente que $v(z_n) \geqslant - (n +1) v(a_o)$

Si $v(b_n)$ no es mínimo tenemos que

$v(z_n) + v(a_o) \geqslant \min \left\{ v(z_{n-1}) + v(-a_1) , \ldots , v(z_o) + v(-a_n) \right\}$ y como $v(-a_1) \geqslant 0 , \ldots , v(-a_n) \geqslant 0$ entonces

$$v(z_n) + v(a_o) \geqslant \min \left\{ v(z_{n-1}) , v(z_{n-2}) , \dots , v(z_o) \right\}$$

$$\geqslant \min \left\{ -n\ v(a_o) , -(n-1)\ v(a_o) , \dots , -(1)\ v(a_o) \right\}$$

$$\geqslant -(n)\ v(a_o)$$

es decir $\qquad v(z_n) \geqslant -(n+1)\ v(a_o)$

Consideremos un elemento $a \in K$ tal que $v(a) > 0$, y la serie $\sum_{n=0}^{\infty} a^{-n^2} x^2 \in K[[x]]$; si esta serie perteneciera a L tendríamos que: $v(a^{-n^2}) \geqslant -(n+1)\ v(a_o)$ para $a_o \in R$ es decir $n^2\ v\left(\frac{1}{a}\right) \geqslant -(n+1)\ v(a_o)$, y como $v\left(\frac{1}{a}\right) = -\ v(a)$ entonces $-\ n^2\ v(a) \geqslant -(n+1)\ v(a_o)$, luego $\forall\ n \in \mathbb{N}$, $n^2 \leqslant (n+1)\dfrac{v(a_o)}{v(a)}$

¡Absurdo! $\qquad$ entonces $\sum_{n=0}^{\infty} a^{-n^2} x^n \notin L.$

Luego el campo de fracciones L de $R[[x]]$ es diferente al campo de fracciones de $K[[x]]$.

5.9 COMENTARIO: Como lo prueba el ejemplo anterior, al hacer el campo de fracciones L de $R[[x]]$ no podemos garantizar que $K[[x]]$ sea un subconjunto de L , entonces al tratar de imitar la prueba del teorema 5.1 nos encontramos con el problema de no poder, en general, inducir un K-automorfismo de $K[[x]]$ a partir de un R-automorfismo de $R[[x]]$, que era el mismo problema con el que nos

enfrentabamos en el capítulo 4 , (ver ejemplo 4.2.1).

Sin embargo, la siguiente proposición nos permite decir cuál es el anillo de invariantes bajo un grupo infinito de R-automorfismos de $R[[x]]$, cuando R es entero, conmutativo, con unidad, pero imponiendole restricciones al grupo G.

5.10 PROPOSICION: Sea R un anillo entero, conmutativo, unitario, G un grupo infinito de R-automorfismos de $R[[x]]$ tal que para todo $\phi \in G$ el término constante de $\phi(x)$ sea cero, entonces $R[[x]]^G = R$

Sea K el campo de fracciones de R , y $\phi \in G$, entonces

$$\phi(x) = \sum_{i=1}^{\infty} b_i x^i \quad \text{con } b_1 \text{ unidad de } R$$

Podemos construir un K-automorfismo ϕ^* de $K[[x]]$ dado por

$$\phi^*(x) = \sum_{j=1}^{\infty} \frac{b_j}{1} x^j = \sum_{j=1}^{\infty} b_j x^j$$

ϕ^* es un K-automorfismo porque b_1 es unidad de K y $b_0 = 0$ genera una topología Hausdorff completa en K. Además, si $f \in R[[x]]$ entonces $\phi^*(f) = \phi(f)$ es decir que $\phi^* / R[[x]] = \phi$.

Sea $K((x))$ el campo de fracciones de $K[[x]]$, a partir de ϕ^* podemos inducir un K-automorfismo de $K((x))$, simplemente definiendo

UNIVERSIDAD NACIONAL
BIBLIOTECA CENTRAL

$\phi^{**}\left(p/_q\right) = \dfrac{\phi^*(p)}{\phi^*(q)}$ naturalmente $\phi^{**}/R[[x]] = \phi$.

Además, si $\phi \neq Ç$ entonces $\phi^{**} \neq Ç^{**}$ y recíprocamente, por tanto el grupo G induce un grupo infinito G^* de K-automorfismos de $K[[x]]$, y un grupo infinito G^{**} de K-automorfismos de $K((x))$.

Sea $f \in R[[x]]^G$, veamos que f tiene que ser un elemento de R.

Supongamos que $f = \sum_{i=n}^{\infty} a_i x^i$ (es decir que f no tiene elemento constante) con $a_n \neq 0$ y veamos que hay una contradicción. Como $\phi(f) = f$ para todo $\phi \in G$ también se cumple que $\phi^*(f) = f$ para $\phi^* \in G^*$ y $\phi^{**}(f) = f$ para $\phi^{**} \in G^{**}$. Consideremos f como elemento de $K[[x]]$, como el primer coeficiente $a_n \neq 0$ es unidad de K tenemos que f satisface las hipótesis del Teorema de Preparación de Weierstrass , (ver 2.1) y por tanto $K[[x]]$ es un $K[[f]]$ -módulo generado por $\{1,x,\ldots,x^{n-1}\}$, luego $K((x))$ es una extensión finita de $K((f))$, entonces por el Teorema Fundamental de la teoría Galois (ver (13) teor. 5.6.6) cualquier grupo de automorfismos que deje fijo a $K((f))$ debe ser finito. ¡Absurdo! , pues sabemos que G^{**} es infinito. Luego f tiene que ser un elemento de R , y por tanto $R[[x]]^G = R$ ∎

5.11 OBSERVACIONES:

a) En el teorema anterior podemos debilitar un poco la condición sobre el grupo G , exigiendo solo que el subgrupo de G formado por los

R-automorfismos que no tienen elemento constante sea infinito, y el resultado se sigue cumpliendo.

b) Análogamente a lo que habíamos hecho cuando trabajábamos con el anillo de polinomios también podemos suprimir en la proposición anterior la hipótesis de que el anillo R tenga unidad, y el resultado sigue siendo válido. No hacemos la prueba pues es completamente análoga a la prueba de 5.10.

c) La hipótesis de que el anillo R sea entero no puede ser suprimida tampoco cuando consideramos R-automorfismos de $R[[x]]$. Un ejemplo similar al que dábamos para los polinomios se aplica en este caso.

5.12 PROBLEMA: Probablemente sea cierto el resultado de que $R[[x]]^G = R$ siempre que R es un anillo entero, conmutativo con unidad, pero no pudimos encontrar una prueba. Este es el interrogante que continúa sin respuesta.

APENDICE

En este apéndice queremos dar un breve recuento de un método que diseñamos para formar grupos finitos de R-automorfismos del anillo de polinomios en varias variables, aunque solo lo emplearemos con el anillo de polinomios en dos variables.

Como sabemos, un R-automorfismo de $R[x,y]$ está determinado por su acción sobre x y sobre y. Esto hace que al considerar la composición de R-automorfismos de $R[x,y]$ para comprobar que en efecto un conjunto dado es un grupo es preciso elaborar dos tablas diferentes, una que refleje como se comporta la acción de la composición sobre x y otra para la acción sobre y; y solo al cruzar la información de ambas tablas puede comprobarse que realmente se trata de un grupo finito de R-automorfismos, y además obtenemos la tabla de multiplicación del grupo.

Para dar un ejemplo de la forma como se pueden utilizar estas tablas consideremos el anillo de polinomios $\mathbb{Z}[x,y]$ y los $\mathbb{Z}$-automorfismos así definidos:

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = -x \qquad \phi_2(y) = -y$$

$$\phi_3(x) = x \qquad \phi_3(y) = -y$$

y consideremos el conjunto $G = \{\phi_1, \phi_2, \phi_3\}$

Necesitamos comprobar si en efecto G es grupo. Hagamos una tabla que represente la acción de la composición sobre x .

x	ϕ_1	ϕ_2	ϕ_3
ϕ_1	ϕ_1, ϕ_3	ϕ_2	ϕ_3, ϕ_1
ϕ_2	ϕ_2	ϕ_1, ϕ_3	ϕ_2
ϕ_3	ϕ_3, ϕ_1	ϕ_2	ϕ_1, ϕ_3

Obsérvese que esta tabla no está unívocamente determinada, y es natural pues sucede que hay diferentes $\mathbb{Z}$-automorfismos que actuan igual sobre x. Por eso es imprescindible conocer la acción sobre y. Construyamos entonces una segunda tabla.

y	ϕ_1	ϕ_2	ϕ_3
ϕ_1	ϕ_1	ϕ_2, ϕ_3	ϕ_3, ϕ_2
ϕ_2	ϕ_2, ϕ_3	ϕ_1	ϕ_1
ϕ_3	ϕ_2, ϕ_3	ϕ_1	ϕ_1

Aunque ambas tablas por separado parecen dar a entender que en efecto se trata de un grupo vemos que $\phi_2 \circ \phi_3(x) = \phi_2(x)$ pero que $\phi_2 \circ \phi_3(y) = \phi_1(y)$. Es decir que G no es grupo, pues no es cerrado bajo el producto.

Para remediar el problema definamos un cuarto $\mathbb{Z}$-automorfismo así:

$\phi_4(x) = -x$ y $\phi_4(y) = y$, y consideremos el conjunto $G = \{\phi_1, \phi_2, \phi_3, \phi_4\}$. Ahora construyamos las tablas para x y y .

x	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1, ϕ_3	ϕ_2, ϕ_4	ϕ_1, ϕ_3	ϕ_2, ϕ_4
ϕ_2	ϕ_2, ϕ_3	ϕ_1, ϕ_3	ϕ_2, ϕ_4	ϕ_1, ϕ_3
ϕ_3	ϕ_3, ϕ_1	ϕ_2, ϕ_4	ϕ_3, ϕ_1	ϕ_2, ϕ_4
ϕ_4	ϕ_4, ϕ_2	ϕ_1, ϕ_3	ϕ_2, ϕ_4	ϕ_1, ϕ_3

y	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1, ϕ_4	ϕ_2, ϕ_3	ϕ_3, ϕ_2	ϕ_4, ϕ_1
ϕ_2	ϕ_2, ϕ_3	ϕ_1, ϕ_4	ϕ_1, ϕ_4	ϕ_2, ϕ_3
ϕ_3	ϕ_3, ϕ_4	ϕ_1, ϕ_4	ϕ_1, ϕ_4	ϕ_2, ϕ_3
ϕ_4	ϕ_4, ϕ_3	ϕ_2, ϕ_3	ϕ_2, ϕ_3	ϕ_1, ϕ_4

Al comparar la información dada por ambas tablas tenemos que

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	ϕ_1	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

Y por tanto G es un grupo. Este es precisamente el ejemplo 3.3.2

El siguiente ejemplo, que es el que habíamos presentado como 3.3.5 , nos muestra que a veces las tablas para x y y pueden ser unívocas.

Consideremos los $\mathbb{Z}$-automorfismos de $\mathbb{Z}[x,y]$ dados por:

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = -x \qquad \phi_2(y) = -y$$

$$\phi_3(x) = y \qquad \phi_3(y) = x$$

$$\phi_4(x) = -y \qquad \phi_4(y) = -x$$

las correspondientes tablas para x y y son

x	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	ϕ_1	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

y	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	ϕ_1	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

Como ambas tablas son iguales, G es un grupo y su tabla de multiplicación es igual a cualquiera de ellas.

Utilicemos ahora este método para comprobar que en efecto los conjuntos dados en los ejemplos 3.3.6 y 3.3.7 son grupos.

En el ejemplo 3.3.6 considerábamos los $\mathbb{Z}$-automorfismos de $\mathbb{Z}[x,y]$ definidos por:

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = x \qquad \phi_2(y) = 2x - y$$

$$\phi_3(x) = -x \qquad \phi_3(y) = -2x + y$$

$$\phi_4(x) = -x \qquad \phi_4(y) = -y$$

Sus tablas de multiplicación para x y y son

x	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1,ϕ_2	ϕ_2,ϕ_1	ϕ_3,ϕ_4	ϕ_4,ϕ_3
ϕ_2	ϕ_2,ϕ_1	ϕ_1,ϕ_2	ϕ_3,ϕ_4	ϕ_3,ϕ_4
ϕ_3	ϕ_3,ϕ_4	ϕ_3,ϕ_4	ϕ_1,ϕ_2	ϕ_1,ϕ_2
ϕ_4	ϕ_4,ϕ_3	ϕ_3,ϕ_4	ϕ_1,ϕ_2	ϕ_1,ϕ_2

y	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	ϕ_1	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

La primera tabla no nos da ninguna información en este ejemplo, pero solo al cruzar los datos de ambas tablas vemos que en efecto G si es cerrado bajo la composición y por tanto es grupo.

En el ejemplo 3.3.7 considerábamos el anillo $R = \mathbb{Z}_3$ y los R-automorfismos de $R[x,y]$:

$$\phi_1(x) = x \qquad \phi_1(y) = y$$

$$\phi_2(x) = x \qquad \phi_2(y) = x + y$$

$$\phi_3(x) = x \qquad \phi_3(y) = -x + y$$

$$\phi_4(x) = -x \qquad \phi_4(y) = y$$

$$\phi_5(x) = -x \qquad \phi_5(y) = x + y$$

$$\phi_6(x) = -x \qquad \phi_6(y) = -x + y$$

En este caso si que se vuelve imprescindible el uso de las tablas, pues aunque el anillo $\mathbb{Z}_3$ es muy simple, el número de R-automorfismos complica el problema. Las tablas son las siguientes :

x	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
ϕ_1	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6
ϕ_2	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6
ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6
ϕ_4	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3
ϕ_5	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3
ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_4,ϕ_5,ϕ_6	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3	ϕ_1,ϕ_2,ϕ_3

La tabla para y es la siguiente

y	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
ϕ_1	ϕ_1,ϕ_4	ϕ_2,ϕ_5	ϕ_3,ϕ_6	ϕ_1,ϕ_4	ϕ_2,ϕ_5	ϕ_3,ϕ_6
ϕ_2	ϕ_2,ϕ_5	ϕ_3,ϕ_6	ϕ_1,ϕ_4	ϕ_2,ϕ_5	ϕ_3,ϕ_5	ϕ_3,ϕ_6
ϕ_3	ϕ_3,ϕ_6	ϕ_1,ϕ_4	ϕ_2,ϕ_5	ϕ_3,ϕ_6	ϕ_1,ϕ_4	ϕ_2,ϕ_5
ϕ_4	ϕ_1,ϕ_4	ϕ_2,ϕ_5	ϕ_2,ϕ_5	ϕ_1,ϕ_4	ϕ_3,ϕ_6	ϕ_2,ϕ_5
ϕ_5	ϕ_2,ϕ_5	ϕ_1,ϕ_4	ϕ_3,ϕ_6	ϕ_2,ϕ_5	ϕ_1,ϕ_4	ϕ_3,ϕ_6
ϕ_6	ϕ_3,ϕ_6	ϕ_1,ϕ_4	ϕ_1,ϕ_4	ϕ_3,ϕ_6	ϕ_2,ϕ_5	ϕ_1,ϕ_4

Y en definitiva la tabla de multiplicación se vuelve

	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
ϕ_2	ϕ_2	ϕ_3	ϕ_1	ϕ_5	ϕ_5	ϕ_6
ϕ_3	ϕ_3	ϕ_1	ϕ_2	ϕ_6	ϕ_4	ϕ_5
ϕ_4	ϕ_4	ϕ_5	ϕ_5	ϕ_1	ϕ_3	ϕ_2
ϕ_5	ϕ_5	ϕ_4	ϕ_6	ϕ_2	ϕ_1	ϕ_3
ϕ_6	ϕ_6	ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

Luego G es grupo.

Nota: Obsérvese que este grupo no es conmutativo, en cambio los ejemplos anteriores eran todos de grupos conmutativos. Esto prueba que esta técnica para construir grupos, permite la aparición tanto de grupos conmutativos como no conmutativos.

REFERENCIAS BIBLIOGRAFICAS

1 ATIYAH, M.F., MACDONALD, I.G. "Introducción al álgebra conmutativa. Ed. Reverté S.A. Barcelona, 1.975

2 BOURBAKI, N. "Algèbre Conmutative". Paris, Hermann, 1.965

3 --------. "Topologie Génerale". Paris, Hermann, 1.965

4 CASTILLON, J.B. "Groupe fini d'automorphismes des anneaux de polynômes et de séries formelles". Bull. Sc. Math. 95 (1971). 237 a 240

5 --------. "Réciproque à un Théorème de P. Samuel". C.R. Acad. Sc. Paris, t. 283 (13 septembre 1976)

6 DUGUNDJI, J. "Topology". Allyn and Bacon, Inc., Boston, 1.976

7 EAKIN, P. and SATHAYE, A. "R-endomorphisms of $R[[x]]$ are essentially continuous". Pacific J.Math. 66(1976) 83,87

8 GILMER, R. "R-automorphisms of $R[x]$ ". Proc. London math. soc. (3), 18 (1968), 328-336.

9 --------. "R-automorphisms of $R[[x]]$ ". Michigan Math. J. 17 (1970), 15-21

10 --------. "On ideal-adic topologies for a conmutative ring". L'enseignement mathém, t. XVIII, fasc. 3, (1972), 14-17

11 GILMER, R., O'MALLEY, M. "R-endomorphisms of $R[[x_1,x_2,\ldots,x_n]]$ ". J. Algebra vol. 48, Nº 1, (1977), 30-44

12 GRECO, S., SALMON, P. "Topics in m-adic topologies". Springer-Verlag, 1971

13 HERSTEIN, I.N. "Topics in Algebra". Xerox College Publishing. Lexington, Massachusetts. 2nd Edition. 1975

14 KIM, Joong-Ho. "R-automorphisms of $R[t][[x]]$ ". Pacific J. Math 42 (1972) 81,88

15 MALLOL, C "Sur les f-morphismes. Sur la structure des groupes finis d'automorphismes". Thèse de 3ème cycle. Université de Montpellier II. Montpellier. Juin 1979.

16 MEJIA, C. "Automorfismos de anillos de series formales". Trabajo de Tesis en preparación. Universidad Nacional. Seccional Medellín.

17 NAGATA, M. "Local Rings". Interscience, 1962.

18 O'MALLEY, M. "R-automorphisms of $R[[x]]$ ". Proc. London Math. Soc. (3) 20 (1970), 60-72.

19 --------. "Some remarks on the formal power series rings". Bull. soc. math. France, 99,(1971), 247-258.

20 --------. "On the Weierstrass preparation theorem". Rocky Mountain, Journal of Mathematics, vol 2, Nº 2, springer 1972, 265-273.

21 --------. "Finite groups of R-automorphisms of $R[[x]]$ ". Michigan Math. J., 20 (1973) 272-284.

22 O'MALLEY M., WOOD, C. "R-endomorphisms of $R[[x]]$". J. Algebra 15 (1970), 314-327.

23 SAMUEL, P. "Méchants anneaux de séries formelles". Journée d'algèbre du 8 Juin 63. Université de Clermont. Faculté des Sciences.

24 --------. "Groupes finis d'automorphismes des anneaux de séries formelles". Bull. Sci. Math. (2) 90 (1966), 97-101.

25 TEJADA, D. "Automorphismes d'anneaux de Polynômes". Thèse de 3ème cycle. Université de Montpellier II. Montpellier. Mars 1981.

26 ZARISKI, O., SAMUEL, P. "Conmutative algebra". I. Univ. series in Higher Math, van Nostrand, 1958.

27 --------. "Conmutative algebra". II Univ. series in Higher Math, van Nostrand, 1960.