Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Matemática

Caracterización de los R-automorfismos de series de potencias formales con coeficientes en un anillo R

TESIS

Para optar el Título Profesional de Licenciado en Matemática

AUTOR

Anderson Policarpo CÁRDENAS FALCÓN

ASESOR

Mg. Soledad RAMÍREZ CARRASCO

Lima, Perú

2024

Referencia bibliográfica

Cárdenas, A. (2024). *Caracterización de los R-automorfismos de series de potencias formales con coeficientes en un anillo R*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Matemática]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Anderson Policarpo Cárdenas Falcón
Tipo de documento de identidad	DNI
Número de documento de identidad	46210884
URL de ORCID	https://orcid.org/0000-0002-6313-4474
Datos de asesor	
Nombres y apellidos	Soledad Ramírez Carrasco
Tipo de documento de identidad	DNI
Número de documento de identidad	25795247
URL de ORCID	https://orcid.org/0000-0002-9974-0943
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Jorge Luis Crisóstomo Parejas
Tipo de documento	DNI
Número de documento de identidad	43688114
Miembro del jurado 1	
Nombres y apellidos	Jorge Alberto Coripaco Huarcaya
Tipo de documento	DNI
Número de documento de identidad	41075852
Datos de investigación	
Línea de investigación	Algebra y Topología

Grupo de investigación	Ecuaciones Diferenciales Análisis y Aplicaciones
Agencia de financiamiento	Ninguno
Ubicación geográfica de la investigación	Lima, Metropolitana
Año o rango de años en que se realizó la investigación	2021-2024
URL de disciplinas OCDE	MATEMATICA PURA https://purl.org/pe-repo/ocde/ford#1.01.00

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE CIENCIAS MATEMATICAS
Ciudad Universitaria - Av. Venezuela S/N cuadra 34
Teléfono: 619-7000, Anexo 1610
Correo Postal: 05-0021, E-mail: eapmat@unmsm.edu.pe
Lima - Perú

Escuela Profesional de Matemática

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN MATEMÁTICA
(Modalidad Presencial)

En la UNMSM - Ciudad Universitaria - Facultad de Ciencias Matemáticas, siendo las 16:05 *horas del viernes 19 de abril del 2024, se reunieron los docentes designados como Miembros del Jurado Evaluador de Tesis: Dr. Jorge Luis Crisóstomo Parejas (PRESIDENTE), Dr. Jorge Alberto Coripaco Huarcaya (MIEMBRO) y la Dra. Soledad Ramírez Carrasco (MIEMBRO ASESOR), para la sustentación de la tesis titulada:* ***"CARACTERIZACIÓN DE LOS R-AUTOMORFISMOS DE SERIES DE POTENCIAS FORMALES CON COEFICIENTES EN UN ANILLO R"*** *presentado por el señor Bachiller Anderson Policarpo Cárdenas Falcón, para optar el Título Profesional de Licenciado en Matemática.*

Luego de la exposición de la tesis, el Presidente invitó al expositor a dar respuesta a las preguntas formuladas.

Realizada la evaluación correspondiente por los miembros del Jurado Evaluador, el expositor mereció la aprobación ……… SOBRESALIENTE ……… *con un calificativo promedio de* DIECISIETE ……(17).

A continuación, el Presidente del Jurado, Dr. Jorge Luis Crisóstomo Parejas, manifestó que el señor Bachiller Anderson Policarpo Cárdenas Falcón, en vista de haber aprobado la sustentación de su tesis, será propuesto para que se le otorgue el Título Profesional de Licenciado en Matemática.

Siendo las 17:10 *horas se levantó la sesión firmando para constancia la presente Acta en tres (3) copias originales.*

Dr. Jorge Luis Crisóstomo Parejas *PRESIDENTE*	*Dr. Jorge Alberto Coripaco Huarcaya* *MIEMBRO*

S. Ramírez C.

Dra. Soledad Ramírez Carrasco
MIEMBRO ASESOR

CERTIFICADO DE SIMILITUD

Yo Dra. Soledad Ramirez Carrasco en mi condición de asesor acreditado con la Resolución Decanal N°000334-2023-D-FCM/UNMSM de la tesis/monografía/informe de investigación/trabajo académico, cuyo título es **"CARACTERIZACIÓN DE LOS R-AUTOMORFISMOS DE SERIES DE POTENCIAS FORMALES CON COEFICIENTES EN UN ANILLO R",** presentado por el bachiller Anderson Policarpo Cárdenas Falcón, para optar el título Profesional de Licenciado en Matemática CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y deSimilitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 20% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorioinstitucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado/ título/ especialidad correspondiente.

Firma S. Ramirez C.

DNI: 25795247

SOLEDAD RAMIREZ CARRASCO

A mis padres y hermano Jhonny.

Agradecimientos

Resumen

En la tesis, utilizando anillos conmutativos con identidad R, estudiamos y caracterizamos los automorfismos en el anillo de polinomios en una indeterminada y con coeficientes en R, también los automorfismos en el anillo de las series de potencias formales en una indeterminada y con coeficientes en R. Finalmente, en el último capítulo realizamos el estudio del anillo de las series de potencias formales en varias indeterminadas y con coeficientes en un cuerpo, y caracterizamos los automorfismos en estos anillos.

Palabras claves: Serie de potencias formal. R-endomorfismos. Automorfismos. Topología I-ádica. Homomorfismos. Isomorfismos.

Abstract

In the thesis, using commutative rings with identity R, we study and characterize the automorphisms in the ring of polynomials in an indeterminate and with coefficients in R, also the automorphisms in the ring of formal power series in an indeterminate and with coefficients in R. Finally, in the last chapter we carry out the study of the ring of formal power series in several indeterminates and with coefficients in a field, and we characterize the automorphisms in these rings.

Keywords: Formal power series. R-endomorphisms. Automorphisms. I-addic topologies. Homomorphisms. Isomorphisms.

Índice general

Introducción

Nuestra motivación para este trabajo, fue estudiar las series de potencias formales con coeficientes en un anillo conmutativo con identidad. Esta necesidad nos condujo a revisar los R-endomorfismos, R-automorfismos de polinomios y de series formales. También, revisamos los automorfismos de las series de potencias en varias indeterminadas y con coeficientes en un cuerpo.

En el primer capítulo, abordamos algunos conceptos previos y definiciones fundamentales, las cuales establecerán una base sólida para nuestra investigación. Este enfoque nos proporcionará un contexto necesario para los resultados que se presentarán en los capítulos siguientes. Describimos la bibliografía utilizada en este capítulo: (Adamson, 1995), (Atiyah, 1989), (Ayres, 1992), (Beachy, 2019), (Dugundji, 1978), (Gentile, 1967), (Herstein, 1970), (Hungerford, 2012), (Lima, 2014), (Lang, 2012), (Lezama, 2014), (Munkres, 2002), (Wawrzynczyk, 1993), (Zaldıvar, 2011).

En el segundo capítulo, utilizamos la bibliografía siguiente:(Churchill, 1992), (Lang, 2013), (Narasimhan, 2012). Veremos algunos resultados de la convergencia de series de potencias y el radio de convergencia. Además, estudiamos el comportamiento de las series de potencias formales, pero consideraremos dichas series con coeficientes complejos. Es natural y frecuente encontrar series de potencias formales con coeficientes en números complejos pero nos interesamos en las series de potencias formales con coeficientes en un anillo en general.

En el tercer capítulo, utilizamos las siguientes bibliografías: (Alvarado, 2015), (Gilmer, 1968), (O'Malley Wood, 1970), (Mejía, 1985). Estudiamos los polinomios con coeficientes en un anillo, y de esta forma exploraramos el comportamiento de los automorfismos en el anillo de estos polinomios. Este análisis, nos proporcionará una base para poder extender los automorfismos a las series de potencias formales, esta vez con coeficientes en un anillo. Sin embargo, nos encontramos con dificultades en este proceso, es por eso que, incorporamos algunos conceptos de topología. Esto nos permitió examinar estas series, desde una nueva perspectiva y extender propiedades para los automorfismos de dichas series de potencias formales.

Finalmente, en el cuarto capítulo usando (Chenciner, 2008) y (Hefez, 2003) extendemos los automorfismos a las series de potencias formales en varias indeterminadas y con coeficientes en un cuerpo K. Para esto, examinamos las series de potencias formales con varias indeterminadas, las cuales tienen propiedades similares a las series en una determinada vista en el tercer capítulo. Esto nos llevó a estudiar los homomorfismos de K-álgebras y sus propiedades, así como los isomorfismos de K-álgebras. Este estudio, nos permitió establecer una conexión con los automorfismos de series de potencias formales en varias indeterminadas, lo que nos llevó a una propiedad vinculada con la determinante de una matriz formada con los coeficientes de las formas lineales de establecidas series formales.

Capítulo 1

CONCEPTOS PREVIOS

En este capítulo, presentaremos algunos conceptos y propiedades principales que serán de gran utilidad para las propiedades de los capítulos posteriores.

Definición 1.1 (**Espacios Topológicos**). Una topología sobre un conjunto X es una colección τ de subconjuntos de X con las siguientes propiedades:

(1) $\emptyset$, $X \in \tau$.

(2) Si $A, B \in \tau$, entonces $A \cap B \in \tau$.

(3) La unión de los elementos de cualquier subcolección de τ está en τ.

Un conjunto X para el que se ha definido una topología τ se llama "Espacio Topológico".

Hablando con propiedad, un espacio topológico es un par ordenado (X, τ) que esta formado por un conjunto X y una topología τ sobre X, omitiremos hacer esta mención específica de τ si no existe confusión.

Si X es un espacio topológico con su topología τ, diremos que $U \subset X$ es un conjunto abierto si $U \in \tau$.

Definición 1.2. Sean los espacios topológicos (X, τ_0) y (X, τ_1), diremos que τ_0 es más pequeño que τ_1 si $\tau_0 \subset \tau_1$.

Definición 1.3 (**Base de una topología**). Sea (X, τ) un espacio topológico. Una familia $\beta \subset \tau$ es llamado base de τ si cada conjunto abierto de X es la unión arbitraria de elementos de β.

Es decir, para todo $U \in \tau$, existe una subfamilia $\{B_j\}_{j \in J} \subset \beta$ tal que $U = \bigcup_{j \in J} B_j$.

Los elementos de la base β lo llamaremos "Elementos básicos de la topología τ".

Teorema 1.1. Sea (X, τ) un espacio topológico y $\beta \subset \tau$ entonces β es base de τ si y solo si para cada $U \in \tau$ y $x \in U$, existe un $B \in \beta$ tal que $x \in B \subset U$.

Prueba. La demostración se puede ver en (Munkres, 2002; p.91). $\square$

Teorema 1.2. Sea β una familia de subconjuntos de X. β es base de alguna topología $\tau(\beta)$ sobre X si y solo si

(1) $X = \bigcup\limits_{B\in\beta} B.$

(2) Para cada $B_1, B_2 \in \beta$ y cada $x \in B_1 \cap B_2$, existe $B_3 \in \beta$ tal que $x \in B_3 \subset B_1 \cap B_2$.

En tal caso $\tau(\beta)$ es la familia de uniones arbitrarias de elementos básicos de β.

Prueba. Si β es base de alguna topología $\tau(\beta)$ sobre X, puede probar de forma inmediata las condiciones (1) y (2) usando el teorema 1.1.

La demostración del recíproco se puede ver en (Adamson, 1995; p.80). □

Observación 1.1.

(i) Si $\beta = \{B_i\}_{i\in I} \subset P(X)$ cumple las condiciones (1) y (2) del Teorema, entonces

$$\tau(\beta) = \left\{ \bigcup_{j\in J} B_j \;/\; \{B_j\}_{j\in J} \subset \beta, J \subset I \right\}$$

es una topología sobre X donde $\beta \subset \tau(\beta)$ es su base.

(ii) $\tau(\beta)$ se llama "Topología generada por β".

(iii) $\tau(\beta)$ es la topología más pequeña de todas las topologías sobre X que contienen a β y es única. El lector puede consultar (Adamson, 1995; p.10).

Definición 1.4 (Topología producto). Sean los espacios topológicos (X, τ_X) y (Y, τ_Y). La topología producto sobre $X \times Y$ (denotada $\tau_{X\times Y}$) es la topología que tiene como base a la familia

$$\beta = \{\ U \times V \ /\ U \in \tau_X, V \in \tau_Y\ \}.$$

Observación 1.2 (Topologías de subespacios).

- Sea el espacio topológico (X, τ), $Y \subset X$, entonces

  $$\tau_{|_Y} := \{\ Y \cap U \ /\ U \in \tau\ \}$$

  es una topología sobre Y.

  Demostraremos esta afirmación:

  (i) Como $X, \emptyset \in \tau$ entonces $Y \cap \emptyset = \emptyset, Y \cap X = Y \in \tau_{|_Y}$.

  (ii) Dados $Y \cap U_1, Y \cap U_2 \in \tau_{|_Y}$.

  $$(Y \cap U_1) \cap (Y \cap U_2) = Y \cap (U_1 \cap U_2) \in \tau_Y, \text{ pues } U_1 \cap U_2 \in \tau.$$

  (iii) Dado la subcolección $\{Y \cap U_j\}_{j\in J}$ de $\tau_{|_Y}$.

  $$\bigcup_{j\in J}(Y \cap U_j) = Y \cap \left(\bigcup_{j\in J} U_j \right) \in \tau_{|_Y}, \text{ pues } \bigcup_{j\in J} U_j \in \tau.$$

- $\tau_{|_Y}$ se denomina topología inducida sobre Y por τ .
- Decimos que $(Y, \tau_{|_Y})$ es un subespacio topológico de (X, τ).

Proposición 1.1. Si β es una base para el espacio topológico (X, τ), entonces la colección

$$\beta_{|_Y} = \{\, Y \cap B \,/\, B \in \beta \,\}$$

es una base de $\tau_{|_Y}$.

Prueba. Esta prueba se puede encontrar en (Munkres, 2002; p.101). □

Definición 1.5 (Entornos). Sea el espacio topológico (X, τ), $V \subset X$ y $x \in X$. Llamaremos entorno de x a cualquier conjunto abierto V (es decir, $V \in \tau$) que contiene a x. De esta manera podemos definir el conjunto de entornos y lo denotaremos

$$\mathcal{N}_{(x)} = \{\ V \subset X \ /\ V \text{ es entorno de } x\ \}.$$

Proposición 1.2. Sea el espacio topológico (X, τ). $U \in \tau$ si y sólo si $U \in \mathcal{N}_{(x)}$, para todo $x \in U$.

Prueba. La demostración puede ser vista en (Adamson, 1995; p.82) □

Proposición 1.3. Sea el espacio topológico (X, τ) y $x \in X$, entonces:

(i) $\mathcal{N}_{(x)} \neq \emptyset$.

(ii) Si $V \in \mathcal{N}_{(x)}$ entonces $x \in V$.

(iii) Si $V \in \mathcal{N}_{(x)}$ y $V \subset W$, entonces $W \in \mathcal{N}_{(x)}$.

(iv) Si $V, W \in \mathcal{N}_{(x)}$ entonces $V \cap W \in \mathcal{N}_{(x)}$.

(v) Para cada $V \in \mathcal{N}_{(x)}$, existe $W \in \mathcal{N}_{(x)}$ tal que $V \in \mathcal{N}_{(y)}$, para todo $y \in W$.

Prueba. La prueba de los ítem del (i) al (iv) son de forma inmediata.
El ítem (v) se puede consultar en (Adamson, 1995; p.83). □

Definición 1.6 (Conjuntos cerrados). Un subconjunto U de de un espacio topológico X se dice que es cerrado si el conjunto $X - U$ es abierto.

Definición 1.7 (Clausura de un conjunto). Dado un subconjunto A de un espacio topológico X. La clausura de A se define como la intersección de todos los conjunto cerrados que contienen a A (también llamado cerradura o adherencia) y se denota mediante $\overline{A}$.

Proposición 1.4. Sea A un subconjunto del espacio topológico X.

(i) $A \subset \overline{A}$.

(ii) A es cerrado si y solo si $A = \overline{A}$.

(iii) $x \in \overline{A}$ si y solo si para todo $U \in \mathcal{N}_{(x)}$, $U \cap A \neq \emptyset$.

Prueba. Esta demostración se puede consultar en (Munkres, 2002; p.105). □

Definición 1.8 (**Espacios de Hausdorff**). Un espacio topológico X se denomina espacio de Hausdorff si para cada par x, y de puntos distintos de X, existen los entornos $U \in \mathcal{N}_{(x)}$, $V \in \mathcal{N}_{(y)}$ tales que $U \cap V = \emptyset$.

Definición 1.9. Sean los espacios topológicos (X, τ_X), (Y, τ_Y). la aplicación $f : X \longrightarrow Y$ se dice que es continua si para todo $V \in \tau_Y$, $f^{-1}(V) = \{\, x \in X \,/\, f(x) \in V \,\} \in \tau_X$.

Definición 1.10 (**Homeomorfismos**). Sean los espacios topológicos (X, τ_X), (Y, τ_Y) y $f : X \longrightarrow Y$ una aplicación biyectiva. Si f y su aplicación inversa $f^{-1} : Y \longrightarrow X$ son continuas, entonces diremos que f es un **homeomorfismo**.

Proposición 1.5. Sean los espacios topológicos (X, τ_X), (Y, τ_Y) y $f : X \longrightarrow Y$ una aplicación. Entonces f es continua si y solo si para cada $x \in X$ y cada $V \in \mathcal{N}_{(f(x))}$, existe $U \in \mathcal{N}_{(x)}$ tal que $f(U) \subset V$.

Prueba. Esta demostración se puede ver en (Munkres, 2002; p.118). □

Observación 1.3.

(i) Cuando se cumple esta condición para el punto $x \in X$ diremos que f es continua en el punto x.

(ii) Esta propiedad sigue siendo válida si se reemplazan los entornos por entornos básicos (es decir, que $V \in \mathcal{N}_{f(x)}$ y V esté en una base de τ_Y).

Teorema 1.3 (**Reglas para construir funciones continuas**).

(i) Sean X_1, X_2 espacios topológicos y $X_1 \times X_2$ con la topología producto, entonces la aplicación proyección

$$\begin{array}{rccc} \phi_i : & X_1 \times X_2 & \longrightarrow & X_i \\ & (x_1, x_2) & \longmapsto & x_i \end{array}$$

para cada $i = 1, 2,$ es continua.

(ii) Sean X, Y espacios topológicos, $y_0 \in Y$ (fijo), entonces la aplicación constante

$$\begin{array}{rccc} C_{y_0}: & X & \longrightarrow & Y \\ & x & \longmapsto & y_0 \end{array}$$

es continua.

(iii) Sea X un espacio topológico, entonces la aplicación identidad

$$\begin{array}{rccc} Id: & X & \longrightarrow & X \\ & x & \longmapsto & x \end{array}$$

es continua.

(iv) Sean X, Y y Z espacios topológicos. Si $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ son aplicaciones continuas, entonces la aplicación composición $g\,o\,f : X \longrightarrow Z$ es continua.

(v) Sean X, X_1, X_2 espacios topológicos y $X_1 \times X_2$ con la topología producto, $f_i : X \longrightarrow X_i$ $(i = 1, 2)$ aplicaciones, entonces la aplicación

$$\begin{array}{rccc} f: & X & \longrightarrow & X_1 \times X_2 \\ & x & \longmapsto & (f_1(x), f_2(x)) \end{array}$$

es continua si y solo si f_i es continua, para todo $i = 1, 2$.

(vi) Sea X un espacio topológico, $a \in X$ fijo, entonces la aplicación

$$\begin{array}{rccc} i_a: & X & \longrightarrow & X \times X \\ & x & \longmapsto & (a, x) \end{array}$$

es continua.

***Prueba**.*

(i) Si $U_i \in \tau_{X_i}$, $(i = 1, 2)$, entonces:

$$\phi_i^{-1}(U_1) = \{\, (x_1, x_2) \in X_1 \times X_2 \,/\, x_1 \in U_1 \,\} = U_1 \times X_2 \in \tau_{X_1 \times X_2}.$$

$$\phi_i^{-1}(U_2) = \{\, (x_1, x_2) \in X_1 \times X_2 \,/\, x_2 \in U_1 \,\} = X_1 \times U_2 \in \tau_{X_1 \times X_2}.$$

Por lo tanto ϕ_i es continua.

(ii) Esta prueba puede ser vista en (Munkres, 2002; p.122).

(iii) Esta prueba puede ser vista en (Munkres, 2002; p.122).

(iv) Esta prueba puede ser vista en (Munkres, 2002; p.122).

(v) Esta orueba puede ser vista en (Munkres, 2002; p.124).

(vi) Sea $x \in X$ (arbitrario) y $a \in X$ (fijo), tenemos:

$$i_a(x) = (a, x) = (C_a(x), Id(x)).$$

Se sabe de los ítems **(i)** y **(ii)** que C_a y Id son continuas.
Por lo tanto del ítem **(v)**, i_a es continua.

□

Definición 1.11 (**Sucesión**). Sea X un conjunto no vacío. Una sucesión en X es una aplicación

$$\begin{array}{rccl} f: & \mathbb{N} & \longrightarrow & X \\ & n & \longmapsto & f(n) := x_n \end{array}$$

y lo denotaremos $(x_n)_{n\in\mathbb{N}} \subset X$ y si no hay confusión sera denotado por $(x_n)_{n\in\mathbb{N}}$.

Definición 1.12 (**Subsucesión**). Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión en X. Llamaremos subsucesión $(y_n)_{n\in\mathbb{N}}$ de $(x_n)_{n\in\mathbb{N}}$ a la sucesión definida por $y_n = x_{\varphi(n)}$ donde $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ es una aplicación estrictamente creciente, es decir que elegimos elementos de la sucesión original sin alterar el orden.

Lema 1.1. Si una aplicación $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ es estrictamente creciente, entonces $\varphi(n) \geq n$, para todo $n \in \mathbb{N}$.

Prueba. En efecto, evidentemente se cumple para $n = 1$.
Si se cumple $\varphi(n) \geq n$, para todo $n \in \mathbb{N}$ (Hipótesis Inductiva).
Supongamos que $\varphi(n+1) < n+1$.
$n \leq \varphi(n) < \varphi(n+1) < n+1$, luego $n < \varphi(n+1) < n+1$ lo cual es una contradicción, por lo tanto $\varphi(n+1) \geq n+1$. □

Ejemplo 1.1. Sea la sucesión $(x_n)_{n\in\mathbb{N}}$ en $\mathbb{R}$ definida por $x_n = \frac{1}{n}$, para todo $n \in \mathbb{N}$.

Una subsucesión de $(x_n)_{n\in\mathbb{N}}$ es la sucesión definida por $y_n = \frac{1}{2n}$, para todo $n \in \mathbb{N}$, pues $\varphi(n) = 2n$ es una aplicación estrictamente creciente y $y_n = \frac{1}{2n} = \frac{1}{\varphi(n)} = x_{2n}$.

Definición 1.13. Sea X un espacio topológico. Decimos que una sucesión $(x_n)_{n\in\mathbb{N}}$ en X converge a un punto $x \in X$ si y solo si para todo $V \in \mathcal{N}_{(x)}$, existe $n_0 \in \mathbb{N}$ tal que para cada $n \geq n_0$, $x_n \in V$ y lo denotaremos por:

$$x_n \longrightarrow x, \quad \lim x_n = x \quad \text{o} \quad \lim_{n\to\infty} x_n = x.$$

- La siguiente proposición nos dice que en esta definición se puede reemplazar los entornos $V \in \mathcal{N}_{(x)}$ por entornos básicos.

Proposición 1.6. Sea (X,τ) un espacio topológico, β una base de τ, $(x_n)_{n\in\mathbb{N}}$ una sucesión de X y $x \in X$, entonces $x_n \longrightarrow x$ si y solo si para todo V entorno básico de x, existe $n_0 \in \mathbb{N}$ tal que para cada $n > n_0$, $x_n \in V$.

Prueba. Sea $x_n \longrightarrow x$ y V un entorno básico de x, entonces $V \in \mathcal{N}_{(x)}$. Luego de la hipótesis, existe $n_0 \in \mathbb{N}$ tal que para cada $n > n_0$, $x_n \in V$.

Recíprocamente, si $V \in \mathcal{N}_{(x)}$, entonces $V \in \tau$ y $x \in V$.

Luego por el teorema 1.1, existe un $B \in \beta$ tal que $x \in B \subset V$. Así B es un entorno básico de x.

De hipótesis tenemos que existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$, $x_n \in B \subset V$.

Por lo tanto $x_n \longrightarrow x$. □

Teorema 1.4. Sea X un espacio topológico de Hausdorff, entonces una sucesión $(x_n)_{n\in\mathbb{N}}$ en X converge únicamente en un punto de X.

Prueba. Supongamos que la sucesión $(x_n)_{n\in\mathbb{N}}$ en X converge en dos puntos diferentes $x, y \in X$.

Luego $x_n \longrightarrow x$, $x_n \longrightarrow y$ donde $x \neq y$.

Tenemos que existen los entornos $U \in \mathcal{N}_{(x)}$, $V \in \mathcal{N}_{(y)}$ tal que $U \cap V = \emptyset$.

Por definición de límite:

$$\begin{array}{l} \text{Existe } n_1 \in \mathbb{N} \text{ tal que para todo } n \geq n_1,\ x_n \in U. \\ \text{Existe } n_2 \in \mathbb{N} \text{ tal que para todo } n \geq n_2,\ x_n \in V. \end{array}$$

Tomamos $n_0 = max\{n_1, n_2\}$, entonces $x_{n_0} \in U \cap V$ lo cual es una contradicción pues U y V son disjuntos.

Por lo tanto su límite en un espacio de Hausdorff es único.

□

Definición 1.14 (Espacios métricos). La métrica o distancia en un conjunto no vacío X es una aplicación

$$d: \ X \times X \ \longrightarrow \ \mathbb{R}$$

que satisface las siguientes propiedades:

(1) $d(x,y) \geq 0$, para todo $x, y \in X$ (No negatividad).

(2) $d(x,y) = 0$ si y solo si $x = y$, para todo $x, y \in X$.

(3) $d(x,y) = d(y,x)$, para todo $x, y \in X$ (Simetría).

(4) $d(x,z) \leq d(x,y) + d(y,z)$, para todo $x, y, z \in X$ (Desigualdad triangular).

Si d es una métrica de X, al par (X, d) se le denomina espacio métrico.

Observación 1.4.

(i) La aplicación mencionada d se llamará pseudométrica si solo cumple las propiedades de simetría, desigualdad triangular y si $d(x,x)=0,$ para todo $x\in X$.

(ii) De estas condiciones se deduce que $d(x,y)\geq 0,$ pues

$$d(x,y)=\frac{1}{2}(d(x,y)+d(y,x))\geq\frac{1}{2}d(x,x)=0.$$

(iii) En una pseudométrica si $d(x,y)=0,$ no necesariamente $x=y$.

(iv) Todo espacio métrico es un espacio pseudométrico.

Definición 1.15. Dado un espacio métrico (X,d). Se denomina bola abierta (de la métrica d) de centro $a\in X$ y radio $r>0$ al conjunto

$$B_d(a,r)=\{\ x\in X\ /\ d(x,a)<r\ \}.$$

Nota: Normalmente, se omite el subíndice d de las bolas abiertas si no da lugar a confusión.

Definición 1.16 (Topología inducida por una métrica). Dado un espacio métrico (X,d), la colección de todas las bolas abiertas

$$\beta_d=\{\ B_d(a,r)\ /\ a\in X,\ r>0\ \}.$$

es una base de alguna topología sobre X.

Efectivamente:

(i) $X=\bigcup\limits_{x\in X}B_d(x,1)$.

(ii) Sea $B_d(x_1,r_1),B_d(x_2,r_2)\in\beta_d$ tal que $x\in B_d(x_1,r_1)\cap B_d(x_2,r_2)$,
entonces existe $B_d(x,r)\in\beta_d$ tal que $x\in B_d(x,r)\subset B_d(x_1,r_1)\cap B_d(x_2,r_2)$
donde $r=min\{r_1-d(x,x_1),r_2-d(x,x_2)\}$.

Dicha topología se denomina topología inducida por la métrica d y se denota τ_d.

Diremos que un espacio topológico (X,τ) es metrizable si existe un espacio métrico (X,d) tal que $\tau=\tau_d$.

Observación 1.5. Una topología puede tener bases diferentes que generan la misma topología. Por ejemplo las familias de conjuntos

$$\beta_1=\left\{\ B_d(a,\tfrac{1}{n})\ /\ a\in X,\ n\in\mathbb{N}\ \right\}.$$
$$\beta_2=\{\ B_d(a,e^{-n})\ /\ a\in X,n\in\mathbb{N}_0\ \}.$$

son bases que generan la topología métrica τ_d.

En efecto, si $U \in \tau_d$ y $x \in U$, entonces por el teorema 1.1, existe $B_d(a, r) \in \beta_d$ tal que $x \in B_d(a, r) \subset U$.

Si escogemos $s = min\{\, d(x, a), r - d(x, a)\,\}$, entonces por la propiedad Arquimediana, existe un $n \in \mathbb{N}$ tal que $\frac{1}{n} < s < r$.

Luego $x \in B_d(x, \frac{1}{n}) \subset B_d(x, s) \subset B_d(a, r) \subset U$.

Es decir que existe $B = B_d(x, \frac{1}{n}) \in \beta_1$ tal que $x \in B \subset U$.

Por lo tanto β_1 es base de τ_d.

De forma análoga se prueba que β_2 es base de τ_d.

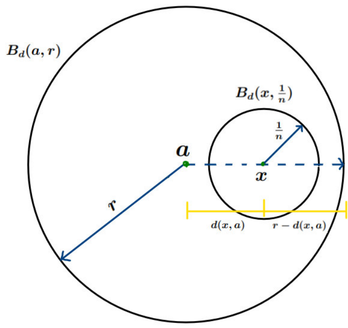

Figura 1.1: **Inclusión de bolas abiertas**

Definición 1.17. Dado el espacio métrico $(X, d\,)$. Se dice que la sucesión $(x_n)_{n\in\mathbb{N}}$ de X converge en un punto $x \in X$ si y solo si para todo $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que para cada $n \geq n_0$, $d(x, x_n) < \varepsilon$.

Decimos también que x es el límite de $(x_n)_{n\in\mathbb{N}}$ y lo representaremos por:

$$x_n \longrightarrow x, \quad \lim x_n = x \quad \text{o} \quad \lim_{n\to\infty} x_n = x.$$

Observación 1.6. Si (X, τ) es un espacio topológico metrizable, la definición de convergencia de un espacio topológico y un espacio métrico son equivalentes.

En efecto:

Supongamos que en el espacio topológico (X, τ), $x_n \longrightarrow x \in X$.

Dado $\varepsilon > 0$, $B_d(x, \varepsilon)$ es un entorno básico de x en $\tau_d = \tau$.

Luego existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$, $x_n \in B_d(x, \varepsilon)$, esto es, $d(x, x_n) < \varepsilon$.

Recíprocamente, Supongamos que en el espacio métrico (X, d), $x_n \longrightarrow x \in X$.

Dado V un entorno básico de x en $\tau_d = \tau$, $V = B_d(x, r)$, para algún $r > 0$.

Luego existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$, $d(x, x_n) < r$, esto es, $x_n \in B_d(x, r) = V$.

Teorema 1.5. Una sucesión convergente en un espacio métrico (X, d) lo hace únicamente en un punto.

Prueba. Supongamos que una sucesión $(x_n)_{n\in\mathbb{N}}$ en X converge a x e y donde $x \neq y$. Como $x \neq y$ y d es una métrica entonces $d(x, y) = \varepsilon > 0$.

Por definición de convergencia

$$\text{existe } n_1 \in \mathbb{N} \text{ tal que para todo } n \geq n_1, \; d(x, x_n) < \tfrac{\varepsilon}{2}$$
$$\text{existe } n_2 \in \mathbb{N} \text{ tal que para todo } n \geq n_2, \; d(x, x_n) < \tfrac{\varepsilon}{2}$$

Luego existe $n_0 = max\{n_1, n_2\}$ tal que $x_{n_0} \in B(x, \frac{\varepsilon}{2}) \cap B(y, \frac{\varepsilon}{2}) = \emptyset$, lo cual es una contradicción.

□

Teorema 1.6. Dado un espacio métrico (X, d), $(x_n)_{n\in\mathbb{N}}$ una sucesión en X.
Si $(x_n)_{n\in\mathbb{N}}$ converge a $x \in X$ entonces cualquier subsucesión $(y_n)_{n\in\mathbb{N}}$ de $(x_n)_{n\in\mathbb{N}}$ converge a x.

Prueba. De hipótesis, $y_n = x_{\varphi(n)}$ donde $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ es una aplicación estrictamente creciente.

Dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$, $d(x, x_n) < \varepsilon$.

Si $n \geq n_0$, entonces $\varphi(n) \geq n \geq n_0$, luego $d(x, x_{\varphi(n)}) < \varepsilon$.

Por lo tanto para todo $n \geq n_0$, $d(x, y_n) < \varepsilon$.

□

Proposición 1.7. Sea X un espacio topológico, $A \subset X$ y $x \in X$. Si existe una sucesión $(x_n)_{n\in\mathbb{N}}$ en A que converge a x, entonces $x \in \overline{A}$. El recíproco se cumple si X es metrizable.

Prueba. Sea $V \in \mathcal{N}_{(x)}$, entonces por definición de convergencia, existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$, $x_n \in V$.

En particular $x_{n_0} \in V \cap A$, luego $x \in \overline{A}$.

Recíprocamente, sea d una métrica para la topología de X.

Si $x \in \overline{A}$, entonces para todo $n \in \mathbb{N}$

$$B_d\left(x, \frac{1}{n}\right) \cap A \neq \emptyset \tag{1.0.1}$$

Dado $\varepsilon > 0$, entonces existe $n_0 \in \mathbb{N}$ tal que $\frac{1}{n_0} < \varepsilon$.

Sea $n \geq n_0$, de (1.0.1) tenemos $d(x, x_n) < \frac{1}{n} \leq \frac{1}{n_0} < \varepsilon$.

Por lo tanto $x_n \in A$ donde $x_n \longrightarrow x$.

□

Definición 1.18 (Espacios métricos completos). Sea (X, d) un espacio métrico. Una sucesión $(x_n)_{n\in\mathbb{N}}$ de X se dice que es una sucesión de Cauchy si y solo si para todo $\varepsilon > 0$, existe un $n_0 \in \mathbb{N}$ tal que $d(x_n, x_m) < \varepsilon$, para cada $n, m \geq n_0$.

El espacio métrico (X, d) se dice que es completo si toda sucesión de Cauchy en X es convergente en un elemento de X.

Observación 1.7. De forma análoga a la observación 1.6, podemos definir una sucesión de Cauchy en un espacio topológico metrizable.

Si (X, τ) es un espacio topológico metrizable, una sucesión $(x_n)_{n\in\mathbb{N}}$ en X es de Cauchy si y solo si para todo $V \in \mathcal{N}_{(x)}$, existe $n_0 \in \mathbb{N}$ tal que para todo $n, m \geq n_0$, $x_n - x_m \in V$.

También análogamente, de la proposición 1.6, en esta definición de sucesiones de Cauchy podemos reemplazar los entornos $V \in \mathcal{N}_{(x)}$ por entornos básicos de x.

Proposición 1.8. Toda sucesión convergente de un espacio métrico (X, d) es sucesión de Cauchy en (X, d).

Prueba. La demostración puede ser vista en (Lima, 2014; p.168). □

Proposición 1.9. Sea $(x_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy de un espacio métrico X. Si $(y_n)_{n\in\mathbb{N}}$ es una subsucesión de $(x_n)_{n\in\mathbb{N}}$ tal que $(y_n)_{n\in\mathbb{N}}$ converge a un punto $x \in X$, entonces $(x_n)_{n\in\mathbb{N}}$ converge a x.

Prueba. Tenemos $y_n = x_{\varphi(n)}$ donde $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ es una aplicación estrictamente creciente.

Dado $\varepsilon > 0$, entonces

$$\text{existe } n_1 \in \mathbb{N} \text{ tal que para todo } n, m \geq n_1,\ d(x_n, x_m) < \tfrac{\varepsilon}{2}.$$
$$\text{existe } n_2 \in \mathbb{N} \text{ tal que para todo } n \geq n_2,\ d(x, y_n) < \tfrac{\varepsilon}{2}.$$

Si $n \geq n_0 = max\{n_1, n_2\}$, entonces $\varphi(n) \geq n \geq n_1$ y $n \geq n_2$.

Luego $d(x_{\varphi(n)}, x_n) = d(y_n, x_n) < \frac{\varepsilon}{2}$ y $d(x, y_n) < \frac{\varepsilon}{2}$.

Finalmente por la desigualdad triangular

$$d(x, x_n) \leq d(x, y_n) + d(y_n, x_n) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Por lo tanto $x_n \longrightarrow x$.

□

Definición 1.19 (**Grupos**). Dado un conjunto $G \neq \emptyset$ y $* : G \times G \longrightarrow G$ una operación binaria, $(G, *)$ es llamado grupo si se cumplen las siguientes propiedades

(1) $a * (b * c) = (a * b) * c$, para todo $a, b, c \in G$. (Asociatividad).

(2) Existe un $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$.
(Existencia del elemento neutro).

(3) Para todo $a \in G$, existe $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$.
(Existencia del elemento inverso).

Si no hay confusión simplemente denotaremos al grupo $(G, *)$ por G.

Se puede probar que el elemento neutro y los elementos inversos son únicos.

Definición 1.20. Un grupo $(G, *)$ es llamado grupo Abeliano si cumple la propiedad de conmutatividad, es decir $a * b = b * a$, para todo $a, b \in G$.

Definición 1.21 (**Subgrupos**). Sea $(G, *)$ un grupo y $H \subset G$. Decimos que H es subgrupo de G si $(H, *)$ es un grupo.

Proposición 1.10. Sea $(G, *)$ un grupo y $H \neq \emptyset$ un subconjunto de G es subgrupo de G si y solo si

(1) Si $a, b \in H$ entonces $a * b \in H$.

(2) Si $a \in H$ entonces $a^{-1} \in H$.

Prueba. La demostración puede verse en (Herstein, 1970; p.46). □

Proposición 1.11. Sea $(G, *)$ un grupo y $H \neq \emptyset$ un subconjunto de G.

H es subgrupo de G si y solo si $a * b^{-1} \in H$, para todo $a, b \in H$.

Prueba. Si $a, b \in H$ entonces por proposición 1.10, $a, b^{-1} \in H$ y luego $a * b^{-1} \in H$.

Reciprocamente, si $a, b \in H$ entonces $b^{-1} = e * b^{-1} \in H$ cumpliendo así la parte **(2)** de la proposición 1.10 y luego $a * (b^{-1})^{-1} = a * b \in H$ cumpliendo la parte **(1)** de la proposición 1.10.

Por lo tanto H es subgrupo de G.

□

Definición 1.22 (**Anillos**). Dado un conjunto $R \neq \emptyset$, $+, \cdot : R \times R \longrightarrow R$ son operaciones binarias. Diremos que $(R, +, \cdot)$ es un anillo si se cumple

(1) $(R, +)$ es grupo Abeliano (0_R es su elemento neutro).

(2) $a.(b.c) = (a.b).c$, para todo $a, b, c \in R$. (" $\cdot$ " es asociativa).

(3) $a.(b+c) = a.b + a.c$ y $(a+b).c = a.c + b.c$. (Distributividad).

Además diremos que: $(R, +, \cdot)$ es un anillo con identidad si se cumple (1),(2),(3) y

(4) Existe $1_R \in R$ tal que $1_R.a = a, 1_R = a$, para todo $a \in R$.

$(R, +, \cdot)$ es un anillo con identidad y división si se cumple (1),(2),(3),(4) y

(5) Para todo $a \in R \setminus \{0_R\}$, existe $b \in R$ tal que $a.b = b.a = 1_R$. $(b = a^{-1})$.

$(R, +, \cdot)$ es un cuerpo si se cumple (1),(2),(3),(4),(5) y

(6) $a.b = b.a$, para todo $a, b \in R$. (" $\cdot$ " es conmutativo).

$(R, +, \cdot)$ es un anillo conmutativo con identidad (a.c.c.i) si se cumple (1),(2),(3),(4) y (6).

Observación 1.8.

(i) Si no hay confusión simplemente denotaremos al anillo $(R, +, \cdot)$ por R.

(ii) Al inverso de $a \in R$ respecto a la suma lo denotaremos por $-a$ y $a.b$ se denotará ab.

(iii) Si $n \in \mathbb{N}$ y $a \in R$, entonces denotaremos por a^n al proceso $aaa...a$ donde se repite n veces.

(iv) Si R es un anillo con identidad, diremos que un elemento $a \in R$ es unidad (o inversible) en R si existe $b := a^{-1} \in R - \{0_R\}$ tal que $ab = 1_R$.

(v) $R = \{0\}$ es un anillo y se llamará anillo trivial.

Definición 1.23. Sea R un anillo conmutativo. Un elemento $a \in R \setminus \{0\}$ es divisor de 0 si existe un $b \in R \setminus \{0\}$ tal que $ab = 0$.

Caso contrario, si un elemento $a \in R$ no es divisor de cero en R diremos que este elemento es regular en R.

Es decir, si a es regular en R si para todo $r \in R$ tal que $ra = 0$ entonces $r = 0$.

Proposición 1.12. Sea R un anillo conmutativo, si a es regular en R entonces a^n es regular en R, para todo $n \in \mathbb{N}$.

Prueba. Probaremos por inducción. Para $n = 1$ es de inmediato por la hipótesis.

Supongamos que a^n es regular en R. (Hipótesis Inductiva)

Sea $r \in R$ tal que $raa^n = ra^{n+1} = 0$ entonces $ra = 0$ y como a es regular en R, $r = 0$.

Por lo tanto a^{n+1} es regular en R.

$\square$

Definición 1.24 (Dominio de Integridad). Un anillo conmutativo no trivial sin divisores de cero es llamado un dominio de integridad (DI), es decir:

R es DI si para todo $a, b \in R$ tal que $ab = 0$ entonces $a = 0$ o $b = 0$.

Proposición 1.13. Todo cuerpo es domino de integridad.

Prueba. Dado un cuerpo R. Sean $a, b \in R$ tal que $ab = 0$.

Supongamos que $a \neq 0$ y $b \neq 0$, entonces $1 = (a^{-1}b^{-1})ab = (a^{-1}b^{-1})0 = 0$, lo cual es una contradicción. Así concluimos que $a = 0$ o $b = 0$.

Por lo tanto R es dominio de integridad.

$\square$

Definición 1.25 (Subanillos). Sea $(R, +, \cdot)$ un anillo y $S \subset R$ un subconjunto no vacío. Diremos que S es un subanillo de R si $(S, +, \cdot)$ es un anillo.

Proposición 1.14. Sea $(R, +, \cdot)$ un anillo y $S \subset R$ un subconjunto no vacío. Entonces S es un subanillo de R si y solo si

(i) Para todo $a, b \in S$, $a - b \in S$.

(ii) Para todo $a, b \in S$, $ab \in S$.

Prueba. Sea S subanillo de R.

(i) Como $S \subset R$, tenemos que $(S, +)$ es subgrupo abeliano de $(R, +)$. De esta manera por la proposición 1.11, $a - b \in S$, para todo $a, b \in S$.

(ii) Es de inmediato debido que S es un anillo.

Recíprocamente, si se cumple los ítems **(i)** y **(ii)**, de la proposición 1.11, $(S, +)$ es un grupo abeliano.

Como $S \subset R$, la propiedad asociativa y distributiva en S se cumplen de inmediato.

Por lo tanto S es subanillo de R. $\square$

Definición 1.26 (Homomorfismos). Sean los anillos $(R, +_R, \cdot_R)$ y $(S, +_S, \cdot_S)$.
Un homomorfismo de anillos (o simplemente morfismo de anillos) es una aplicación $f : R \longrightarrow S$ tal que para todo $a, b \in R$, $f(a +_R b) = f(a) +_S f(b)$ y $f(a \cdot_R b) = f(a) \cdot_S f(b)$.

Además, si R y S tienen elementos identidad, se cumple que $f(1_R) = 1_S$.

Al homomorfismo $f : R \longrightarrow R$ lo llamaremos endomorfismo de R.

Definición 1.27. Sea $f : R \longrightarrow S$ un homomorfismo de anillos. Diremos que f es isomorfismo si f es biyectiva.

Si el endomorfismo $f : R \longrightarrow R$ es un isomorfismo diremos que f es un automorfismo de R.

Proposición 1.15.

(i) Si $f : R \longrightarrow S$ es un homomorfismo de anillos, entonces $f(0_R) = 0_S$ y $f(-a) = -f(a)$, para todo $a \in R$.

(ii) Si $f : R \longrightarrow S$ es un isomorfismo de anillos, entonces su aplicación inversa $f^{-1} : S \longrightarrow R$ también lo es.

(iii) La composición de dos isomorfismos de anillos es isomorfismo.

Prueba. La demostración de **(i)** puede ser vista en (Herstein, 1970; p.113). Las demostraciones de **(ii)** y **(iii)** se encuentran en (Beachy, 2019; p.239). □

Definición 1.28. Sea $f : R \longrightarrow S$ un homomorfismo de anillos. Los conjuntos

$$Nu(f) = \{ \ r \in R \ / \ f(r) = 0_S \ \}$$
$$Im(f) = \{ \ s \in S \ / \ \exists \ r \in R, f(r) = s \ \}$$

son llamados núcleo e imagen de f respectivamente.

Proposición 1.16. Sea $f : R \longrightarrow S$ un homomorfismo de anillos.

(i) $Nu(f)$ y $Im(f)$ son subanillos en sus anillos respectivos.

(ii) f es inyectiva si y solo si $Nu(f) = \{0_R\}$.

Prueba.

(i) Esta demostración puede verse en (Beachy, 2019; p.241).

(ii) Si $x \in Nu(f)$ entonces $f(x) = 0 = f(0)$, luego por la inyectividad de f, $x = 0$. Por lo tanto $Nu(f) = \{0_R\}$.
Recíprocamente, sean $x, y \in R$ tal que $f(x) = f(y)$, entonces $f(x - y) = 0$, así $x - y \in Nu(f) = \{0_R\}$, es decir, $x = y$. Por lo tanto f es inyectiva. □

Definición 1.29 (Ideales). Sea R un anillo, $I \subset R$ un subconjunto no vacío. Diremos que I es un ideal de R si se cumple:

(1) Para todo $a, b \in I$, $a - b \in I$ (esto quiere decir que $(I, +)$ es subgrupo de R).

(2) Para todo $a \in I$ y para todo $r \in R$, $ra, ar \in I$.

Proposición 1.17 (Ideales especiales). Sea I, J ideales del anillo R. Definimos los conjuntos:

$$I + J = \{ \ a + b \ / \ a \in I, b \in J \ \}$$
$$IJ = \{ \ a_1b_1 + a_2b_2 + ... + a_nb_n \ / \ a_i \in I, b_i \in J, n \in \mathbb{N} \ \}$$

y sea $\{I_\lambda\}_{\lambda \in \Lambda}$ una colección de ideales de R, entonces $I + J$, IJ y $\displaystyle\bigcap_{\lambda \in \Lambda} I_\lambda$ son ideales de R.

Prueba. La demostración que $I+J$ y IJ son ideales de R puede verse en (Hungerford, 2012; p.124), mientras que la demostración que $\bigcap_{\lambda\in\Lambda} I_\lambda$ es un ideal de R sale de forma inmediata aplicando la definición de ideales en I_λ. □

Observación 1.9.

(i) Los ideales $I+J$, y IJ se llaman ideal suma e ideal producto respectivamente.

(ii) La unión de dos ideales de R no necesariamente es un ideal de R.

(iii) Sea $n \in \mathbb{N}$, I ideal de R, luego denotaremos al producto de n ideales como

$$I^n = \underbrace{III...I}_{n-veces}.$$

Definición 1.30. Sea S un subconjunto del anillo R, representaremos a $\langle S\rangle$ como el mínimo ideal de todos los ideales que contienen a S.

Proposición 1.18. Sea R un anillo conmutativo y S un subconjunto no vacío de R, entonces

$$\langle S\rangle = \{\ r_1s_1 + r_2s_2 + ... + r_ns_n\ /\ r_i \in R, s_i \in S, n \in \mathbb{N}\ \}.$$

Prueba. La demostración puede ser vista en (Lezama, 2014; p.16). □

Proposición 1.19. Sea S un subconjunto del anillo conmutativo R, $\{I_\lambda\}_{\lambda\in\Lambda}$ una colección de todos los ideales de R tal que $S \subset I_\lambda$, entonces

$$\langle S\rangle = \bigcap_{\lambda\in\Lambda} I_\lambda.$$

Prueba. La demostración puede ser vista en (Lezama, 2014; p.16).

□

Observación 1.10. Sea R un anillo conmutativo y S un subconjunto de R.

(i) Si $S = \{a_1, a_2, ..., a_n\}$ entonces

$$\langle S\rangle := \langle a_1, a_2, ..., a_n\rangle R = \{\ r_1a_1 + r_2a_2 + ... + r_na_n\ /\ r_i \in R\ \}$$

es llamado ideal finitamente generado. (si no hay confusión $\langle a_1, a_2, ..., a_n\rangle R$ simplemente lo denotaremos por $\langle a_1, a_2, ..., a_n\rangle$).

(ii) Si $S := \{a\}$ entonces

$$\langle S\rangle = \langle a\rangle = \{\ ra\ /\ r \in R\ \} = aR$$

es llamado ideal principal de R.

(iii) Sea $a \in R$, se puede probar que $\langle a^n \rangle = \langle a \rangle^n$, para todo $n \in \mathbb{N}$.

Definición 1.31 (**Anillo Cociente**). Sea R un anillo con $I \subset R$ ideal. Definimos una relación en R. Para todo $a, b \in R$

$$a \sim b \quad \text{si y solo si} \quad a - b \in I.$$

Afirmación: " $\sim$ " es una relación de equivalencia.

Reflexividad. Para todo $a \in R$, $a - a = 0 \in I$, entonces $a \sim a$.

Simetría. Sean $a, b \in R$ tal que $a \sim b$, entonces $a - b \in I$. Como I es ideal, $-(a - b) = b - a \in I$, así $b \sim a$.

Transitividad. Sean $a, b, c \in R$ tal que $a \sim b$ y $b \sim a$.
Tenemos $(a - b), (b - c) \in I$, luego $a - c = (a - b) + (b - c) \in I$ y por ende $a \sim c$.

Por lo tanto " $\sim$ " es una relación de equivalencia.

Si $a \in R$, llamaremos al conjunto $\overline{a} = \{ \, b \in R \ / \ a \sim b \, \}$ como **"clase de equivalencia de $\boldsymbol{a}$"**.

Observamos que $\overline{a} = a + I$.

Estas clases de equivalencia conforman una partición de R denominada anillo cociente R/I, es decir,

$$\frac{R}{I} = \{ \, a + I \ / \ a \in R \, \}.$$

Vamos a dotar a R/I con las operaciones de suma y producto.

- Suma: $(a + I) + (b + I) := (a + b) + I$.
- Producto: $(a + I).(b + I) := (ab) + I$.

Estas operaciones están bien definidas. En efecto:

• Suma: Sean $a' \in a + I$ y $b' \in b + I$, entonces $(a' - a), (b' - b) \in I$, luego
$(a' + b') - (a + b) = (a' - a) + (b' - b) \in I$, así $(a' + b') \sim (a + b)$.
Por lo tanto $(a' + b') + I = (a + b) + I$.

• Producto: Sean $a' \in a + I$ y $b' \in b + I$, entonces $h = (a' - a)$, $k = (b' - b) \in I$.
Luego $a' = a + h$, $b' = b + k$, con $h, k \in I$, por consiguiente $a'b' = ab + ak + hb + hk$, donde $ak, hb, hk \in I$, es decir, $a'b' = ab + g$, donde $g = ak + hb + hk \in I$, así $g = a'b' - ab \in I$, $(a'b') \sim (ab)$. Por lo tanto $(a'b') + I = (ab) + I$.

Con estas operaciones definidas proporcionan que R/I sea un anillo denominada **anillo cociente**.

Si R es a.c.c.i, entonces R/I es a.c.c.i donde el elemento el elemento aditivo es $\overline{0} = 0 + I = I$ y el elemento identidad es $\overline{1} = 1 + I$.

La aplicación

$$\begin{aligned} \pi : \quad R &\longrightarrow \tfrac{R}{I} \\ a &\longmapsto \pi(a) = a + I \end{aligned}$$

es un homomorfismo sobreyectivo llamado **"proyección natural al cociente"**.

Definición 1.32 (**Ideal primo**)**.** Sea R un anillo, P un ideal de R con $P \neq R$ (o también se dice que P es ideal propio de R). Diremos que P es in ideal primo si se cumple la siguiente condición:

Si $I, J \subset R$ son ideales tal que $IJ \subset P$, entonces $I \subset P$ o $J \subset P$.

En el caso de que R sea conmutativo tenemos la siguiente equivalencia:

P es ideal primo si y solo si para todo $a, b \in R$ tal que $ab \in P$, se tiene que $a \in P$ o $b \in P$.

Definición 1.33 (**Ideal maximal**)**.** Sea R un a.c.c.i, M un ideal de R con $M \neq R$. El ideal M se llama maximal si no existe otro ideal I tal que $M \subset I \subset R$ con $M \neq I$ y $I \neq R$.

Es decir, M es ideal maximal de R si para todo I ideal de R tal que $M \subset I$, entonces $M = I$ o $I = R$.

Proposición 1.20. Sea R un anillo, M y P los ideales propios de R, entonces

(i) P es ideal primo si y solo si $\dfrac{R}{P}$ es Dominio de Integridad.

(ii) M es ideal maximal si y solo si $\dfrac{R}{M}$ es un cuerpo.

Prueba.

(i) Esta demostración puede verse en (Hungerford, 2012; p.127).

(ii) Esta demostración puede verse en (Hungerford, 2012; p.129).

$\square$

Proposición 1.21. Todo ideal maximal es ideal primo.

Prueba. Usando la proposición 1.20 tenemos que si M es un ideal maximal de un anillo R entonces de $\dfrac{R}{M}$ es un cuerpo, luego de 1.13, $\dfrac{R}{M}$ es DI y de la misma proposición 1.20, M es un ideal primo.

$\square$

Definición 1.34 (Ideales Nilpotentes). Sea R a.c.c.i. Diremos que $a \in R$ es un elemento nilpotente si existe un $n \in \mathbb{N}$ tal que $a^n = 0$.

El conjunto de todos los elementos nilpotentes de R,
$Rad(R) = \{ \ a \in R \ / \ a$ es nilpotente $\}$ se llamará nilradical o radical de R.

Un ideal I de R se llamará nilpotente si existe un $n \in \mathbb{N}$ tal que $I^n = 0$.

Proposición 1.22. Si R es un anillo conmutativo, entonces

(i) $Rad(R)$ es un ideal de R.

(ii) $Rad(R)$ es la intersección de todos los ideales primos de R.

Prueba. Las demostraciones de **(i)** y **(ii)** se pueden encotrar en (Atiyah, 1989; p.5). □

Proposición 1.23. Sea R a.c.c.i. Si $a_1, a_2, ..., a_n \in R$ son nilpotentes entonces $\langle a_1, a_2, ..., a_n \rangle$ es un ideal nilpotente.

Prueba. Probaremos por inducción.

(i) Si $k = 1$.
Tenemos que si a_1 es nilpotente entonces existe un $r \in \mathbb{N}$ tal que $a_1^r = 0$, luego $\langle a_1 \rangle^r = 0$.

(ii) Supongamos que la proposición es verdad para $k = n$ (Hipótesis Inductiva).

(iii) Veamos si se cumple para $k = n + 1$.

Sean $a_1, a_2, ..., a_n, a_{n+1} \in R$ nilpotentes. Denotemos $I = \langle a_1, a_2, ..., a_n \rangle$.

Tenemos del ítem **(i)** y la Hipótesis Inductiva tenemos que existen $r, m \in \mathbb{N}$ tal que $\langle a_{n+1} \rangle^r = 0$ y $I^m = 0$.

Luego:

$$\langle a_1, a_2, ..., a_n, a_{n+1} \rangle^{m+r} = (\ I + \langle a_{n+1} \rangle \ )^{m+r} = \sum_{i=0}^{m+r} I^{m+r-i} \langle a_{n+1} \rangle^i$$

$$\langle a_1, a_2, ..., a_n, a_{n+1} \rangle^{m+r} = I^{m+r} \ + \ \sum_{i=1}^{r-1} I^{m+r-i} \langle a_{n+1} \rangle^i \ + \ I^m \langle a_{n+1} \rangle^r$$
$$+ \sum_{i=r+1}^{m+r-1} I^{m+r-i} \langle a_{n+1} \rangle^i \ + \ \langle a_{n+1} \rangle^{m+r}$$

$$\langle a_1, a_2, ..., a_n, a_{n+1} \rangle^{m+r} = I^m \sum_{i=1}^{r-1} I^{r-i} \langle a_{n+1} \rangle^i \ + \ \sum_{i=r+1}^{m+r-1} I^{m+r-i} \langle a_{n+1} \rangle^i$$

$$\langle a_1, a_2, ..., a_n, a_{n+1} \rangle^{m+r} = \sum_{i=r+1}^{m+r-1} I^{m+r-i} \langle a_{n+1} \rangle^i$$

$$\langle a_1, a_2, ..., a_n, a_{n+1} \rangle^{m+r} = I^{m-1} \langle a_{n+1} \rangle^{r+1} + I^{m-2} \langle a_{n+1} \rangle^{r+2} + \cdots + I \langle a_{n+1} \rangle^{m+r-1}$$

$$\langle a_1, a_2, ..., a_n, a_{n+1} \rangle^{m+r} = 0.$$

Por lo tanto $\langle a_1, a_2, ..., a_n, a_{n+1}\rangle$ es un ideal nilpotente.

$\square$

Proposición 1.24. Sea R un anillo. Si a no es unidad de R, entonces existe un ideal maximal M de R tal que $a \in M$.

Prueba. La demostración puede ser vista en (Martinez, 1997; p.19). $\square$

Observación 1.11.

(i) Ya que todo ideal maximal es un ideal primo entonces podemos decir que si a no es unidad de un anillo R entonces existe un ideal primo P de R tal que $a \in P$.

(ii) También se puede decir que, si $a \notin P$, para cualquier P ideal primo de R, entonces a es unidad de R.

Definición 1.35 (Estructuras de módulos sobre un anillo). Sea R un anillo conmutativo con identidad (a.c.c.i), A un grupo abeliano y la aplicación

$$\begin{array}{rccc} \lambda: & R\times A & \longrightarrow & A \\ & (r,a) & \longmapsto & r\cdot a \end{array}$$

A junto con λ lo llamaremos R-módulo A (o A es un R-módulo) si satisfacen las siguientes propiedades:

(m1) $r\cdot(a_1+a_2) = r\cdot a_1 + r\cdot a_2$.

(m2) $(r_1+r_2)\cdot a = r_1\cdot a + r_2\cdot a$.

(m3) $(r_1\cdot r_2)\cdot a = r_1\cdot(r_2\cdot a)$.

(m4) $1_R\cdot a = a$.

cualesquiera que sean $a, a_1, a_2 \in A$ y $r, r_1, r_2 \in R$.

Definición 1.36 (Homomorfismos de módulos). Sean M, N R-módulos. La aplicación $f: M \longrightarrow N$ es un homomorfismo de R-módulos si para cada $x, y \in M$, $r \in R$ se cumple:

$$f(x+y) = f(x) + f(y) \;\text{ y }\; f(rx) = rf(x).$$

Definición 1.37 (Filtraciones). Sea R un anillo conmutativo. Una filtración en R es una familia de ideales, $\{I_n\}_{n\in\mathbb{N}_0}$ de R tales que

$$I = I_0 \supset I_1 \supset I_2 \supset ... \supset I_n \supset ... \;\text{ y }\; I_nI_m \subset I_{n+m}.$$

Si $\{I_n\}_{n\in\mathbb{N}_0}$ es una filtración de R, diremos que R es un anillo filtrado.

Ejemplo 1.2. Sea R un anillo conmutativo, I un ideal de R, entonces $\{I^n\}_{n\in\mathbb{N}_0}$ forma una filtración en R.

En efecto, denotamos $R = I^0$. Evidentemente $I^nI^m = I^{n+m}$.

Afirmación: $I^{n+1} \subset I^n$, para todo $n \in \mathbb{N}$.

(i) Si $n = 1$.
Sea $x \in I^2$, entonces $x = x_1y_1 + x_2y_2 + ... + x_ny_n$ donde $x_i, y_i \in I$.
Como $x_iy_i \in I$, $x \in I$. Luego $I^2 \subset I$.

(ii) Supongamos que se cumple para $n \in \mathbb{N}$, $I^{n+1} \subset I^n$ (Hipótesis Inductiva)
Luego $I^{n+2} = I^{n+1}I \subset I^nI = I^{n+1}$.

Esto quiere decir que se cumple para $n + 1$ probando así la afirmación.

Como I^n es un ideal y por la afirmación, $I^n \subset I$, para todo $n \in \mathbb{N}$,
entonces I^n cumple las condiciones (i) y (ii) de submódulos.

Por lo tanto

$$I \supset I^2 \supset I^3 \supset ... \supset I^n \supset ...$$

es una filtración de R.

• Estos tipos de filtraciones son llamadas **"Filtración *I*-ádica de *R*"**.

Capítulo 2

CONVERGENCIA DE SERIES

En este capítulo inicialmente estudiamos las series complejas, principales propiedades y teoremas relacionados. También estudiamos las series de potencias con coeficientes complejos, su relación con las funciones holomorfas y en la sección 2.1 describimos el radio de convergencia para las funciones complejas holomorfas.

Definición 2.1. Llamaremos sucesión de números complejos a una aplicación $z : \mathbb{N} \longrightarrow \mathbb{C}$ que asocia a cada número natural n un número complejo z_n llamado n-ésimo término de la sucesión la cual denotaremos $(z_n)_{n\in\mathbb{N}} \subset \mathbb{C}$ o simplemente $(z_n) \subset \mathbb{C}$.

Definición 2.2. Sea $(z_n) \subset \mathbb{C}$, diremos que esta sucesión converge a $z \in \mathbb{C}$ si

$\lim\limits_{n\to\infty} z_n = z$. Además de la definicion de sucesión convergente se puede deducir que:

$\lim\limits_{n\to\infty} z_n = z$ si y solo si para todo $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $|z_n - z| < \varepsilon$, para todo $n > n_0$.

Observación 2.1.

- Si existe este límite, este límite debe ser único.
- Si no existe este límite se dice que la sucesión diverge.

Teorema 2.1. Sea $(z_n)\subset\mathbb{C}$ con $z_n = x_n + iy_n$ $(n \in \mathbb{N})$, además si $z = x + iy$ entonces $\lim\limits_{n\to\infty} z_n = z$ si y solo si $\lim\limits_{n\to\infty} x_n = x$ y $\lim\limits_{n\to\infty} y_n = y$.

Prueba. Para cada $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que para cada $n > n_0$ tenemos $|z_n - z| < \varepsilon$, utlizando las siguientes desigualdades:

$$\begin{aligned} |x_n - x| + |y_n - y| &\leq |z_n - z| < \varepsilon \\ |x_n - x| &\leq |z_n - z| < \varepsilon \\ |y_n - x| &\leq |z_n - z| < \varepsilon \end{aligned}$$

Obtenemos que $\lim_{n\to\infty} x_n = x$ y $\lim_{n\to\infty} y_n = y$.

Recíprocamente, dado $\varepsilon > 0$, entonces tenemos que existe $n_1 \in \mathbb{N}$ tal que para todo $n > n_1$, $|x_n - x| < \frac{\varepsilon}{2}$ y existe $n_2 \in \mathbb{N}$ tal que para todo $n > n_2$, $|x_n - x| < \frac{\varepsilon}{2}$.

Tomamos un $n_0 = max\{n_1, n_2\}$, luego si $n > n_0$ tenemos que
$|x_n - x| < \frac{\varepsilon}{2}$ y $|x_n - x| < \frac{\varepsilon}{2}$.

En consecuencia $|z_n - z| \leq |x_n - x| + |y_n - y| < \varepsilon$.

$\square$

A continuación daremos la definición de series de números complejos.

Definición 2.3. Dada la sucesión $(z_n) \subset \mathbb{C}$, una serie infinita de números complejos denotada por $\sum_{n=0}^{\infty} z_n$ se dice que converge a un número complejo S si la sucesión de sumas parciales $S_N = \sum_{n=0}^{N} z_n$ converge a S, escribimos en tal caso $\sum_{n=0}^{\infty} z_n = S$.

Teorema 2.2. Sea $(z_n) \subset \mathbb{C}$ con $z_n = x_n + iy_n$ $(n \in \mathbb{N})$ y $S = X + iY \in \mathbb{C}$, entonces $\sum_{n=0}^{\infty} z_n = S$ si y solo si $\sum_{n=0}^{\infty} x_n = X$ y $\sum_{n=0}^{\infty} y_n = Y$.

Prueba. Sea $S_N = \sum_{n=0}^{N} z_n = X_N + iY_N$, para todo $N \in \mathbb{N}$ donde
$\sum_{n=0}^{N} x_n = X_N$ y $\sum_{n=0}^{N} y_n = Y_N$.

Luego tenemos
$\sum_{n=0}^{\infty} z_n = S$ si $\lim_{n\to\infty} S_n = S$

$\lim_{n\to\infty} X_n = X$ y $\lim_{n\to\infty} Y_n = Y$ (por teorema 2.1)

es decir, $\sum_{n=0}^{\infty} X_n = X$ y $\sum_{n=0}^{\infty} Y_n = Y$.

$\square$

Proposición 2.1.

(i) Si la serie de números complejos $\sum_{n=0}^{\infty} z_n$ converge entonces $\lim_{n\to\infty} z_n = 0$.

(ii) Los términos de una serie convergente son acotados. (Es decir, existe $M > 0$ tal que $|z_n| \leq M$, para todo $n \in \mathbb{N}$).

Prueba.

(i) Sea $z_n = x_n + iy_n$ con $\sum_{n=0}^{\infty} z_n = X + iY \in \mathbb{C}$.

Luego por el teorema 2.1 tenemos $\sum_{n=0}^{\infty} X_n = X$ y $\sum_{n=0}^{\infty} Y_n = Y$, entonces $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n = 0$. Por lo tanto $\lim_{n\to\infty} z_n = 0$.

(ii) Es inmediato, pues de la parte (i) de la proposición tenemos que $\lim_{n\to\infty} z_n = 0$, luego $(z_n) \subset \mathbb{C}$ es acotado.

□

Teorema 2.3. La convergencia absoluta de una serie de números complejos implica la convergencia de la serie.

Prueba. Como la serie $\sum_{n=0}^{\infty} |z_n|$ es convergente y además $|x_n| \leq |z_n|$ y $|y_n| \leq |z_n|$.

Por el criterio de comparación de los números reales tenemos que $\sum_{n=0}^{\infty} |x_n|$ y $\sum_{n=0}^{\infty} |y_n|$ son series convergentes.

Ya que la convergencia absoluta de una serie de números reales implica la convergencia de la propia serie tenemos que:

Existen $X, Y \in \mathbb{R}$ tales que $\sum_{n=0}^{\infty} X_n = X$ y $\sum_{n=0}^{\infty} Y_n = Y$.

Finalmente por el teorema 2.2, $\sum_{n=0}^{\infty} z_n = X + iY$.

□

Observación 2.2.

(i) Si $S = \sum_{n=0}^{\infty} z_n$ y $S_N = \sum_{n=0}^{N} z_n$, ρ_N representara la sucesión de restos de la serie la cual es definida como $\rho_N = S - S_N$.

(ii) Si $S_N = \sum_{n=0}^{N} z_n$ y $\lim_{n\to\infty} S_N = S$, además $S = S_N + \rho_N$ lo que implica que "una serie converge a un número S si y solo si la sucesión de restos tiende a cero".

2.1. Radio de convergencia

Antes de estudiar la serie de potencias convergentes, vamos a recordar la definición de función holomorfa. Es claro que, al tener una función holomorfa , existe una estrecha relación con una serie de potencias convergentes en una región de convergenvia y por ello es imprescindible definir el concepto de radio de convergencia.

Definición 2.4. Sea f una función con valores complejos definidas en un conjunto abierto $\Omega \subset \mathbb{C}$. Decimos que f es holomorfa en Ω si, para cada $a \in \Omega$, existe un entorno $U \in \mathcal{N}_{(a)}$ $(U \subset \Omega)$ y una sucesión $(c_n) \subset \mathbb{C}$ tal que para cada $z \in U$, la serie

$$\sum_{n=0}^{\infty} c_n (z-a)^n$$

converge a $f(z)$.

A continuación, mostramos una propiedad fundamental relacionada a radio de convergencia relacionada a las funciones holomorfas.

Lema 2.1 (**Lema de Abel**). Sea una sucesión $(c_n) \subset \mathbb{C}$, entonces existe un $R \geq 0$ (R puede ser igual a ∞) tal que la serie

$$\sum_{n=0}^{\infty} c_n z^n$$

converge (absolutamente) para $|z| < R$ y diverge (absolutamente)para $|z| > R$.
Ademas la serie converge uniformemente en todo subconjunto compacto del disco $D_{(0,R)} = \{ z \in \mathbb{C} \,/\, |z| < R \}$.

Prueba. Dado el conjunto $A = \{ r \geq 0 \,/\, (\, |c_n| r^n \,)_{n \in \mathbb{N}}$ es una sucesión acotada $\}$.
Es claro que $A \neq \emptyset$, puesto que $0 \in A$.

Caso 1: Si A es acotado.

Sea $R = sup\, A$ y supongamos que $|z| > R$.

Afirmamos que $(\, |c_n||z|^n \,)_{n \in \mathbb{N}}$ no esta acotado, pues de lo contrario $|z| \in A$ y luego por definición de supremo $|z| \leq R$ lo cual es una contradicción.

Así concluimos que $\displaystyle\sum_{n=0}^{\infty} c_n z^n$ diverge (absolutamente) cuando $|z| > R$.

Ahora, si tenemos un subconjunto compacto K del disco $D_{(0,R)}$, entonces existe un $\rho > 0$ tal que $K \subset \overline{D_{(0,\rho)}} \subsetneq D_{(0,R)}$.

Como $\rho < R$ (lo suficientemente cercano a R), entonces existe $r \in A$ tal que $\rho < r \leq R$.

Sea $z \in K$ arbitrario, entonces $|z| \leq \rho < r$. Así tenemos la siguiente desigualdad

$$\text{existe } M > 0 \text{ tal que } |c_n||z|^n \leq |c_n|\rho^n \leq |c_n| r^n \leq M.$$

Luego $|c_n z^n| \leq |c_n|\rho^n \leq M(\frac{\rho}{r})^n$. Como $\frac{\rho}{r} < 1$ entonces $\displaystyle M \sum_{n=0}^{\infty} (\frac{\rho}{r})^n < \infty$.

Aplicando el criterio de comparación tenemos que $\sum_{n=0}^{\infty} c_n z^n$ converge (absolutamente).

Por lo tanto $\sum_{n=0}^{\infty} c_n z^n$ converge uniformemente en K.

Análogamente a la demostración anterior podemos obtener que $\sum_{n=0}^{\infty} c_n z^n$ converge (absolutamente) para $|z| < R$.

Caso 2: Si A no es acotado.

Sea $t > 0$. Como A no es acotado entonces existe una sucesión acotada $(\,|c_n|r^n\,)_{n\in\mathbb{N}}$ tal que $r > t$, esto implica que existe $M > 0$ tal que $|c_n|t^n \leq |c_n|r^n \leq M$, luego $t \in A$.

Además como $0 \in A$ entonces $\mathbb{R}^+ \cup \{0\} \subset A$, es decir, $\mathbb{R}^+ \cup \{0\} = A$.

Luego R se puede interpretar como infinito $(R = sup\,A = \infty)$.

Esto quiere decir que $\sum_{n=0}^{\infty} c_n z^n$ converge (absolutamente), para todo $z \in \mathbb{C}$.

$\square$

Observación 2.3.

- R es llamado **Radio de convergencia** de la serie $\sum_{n=0}^{\infty} c_n z^n$, es decir, $\sum_{n=0}^{\infty} c_n z^n$ es convergente en $D_{(0,R)}$.

- Si $\sum_{n=0}^{\infty} c_n z^n$ converge (absolutamente), para todo $z \in \mathbb{C}$, entonces $R = \infty$.

- Si $R = 0$ entonces $\sum_{n=0}^{\infty} c_n z^n$ converge para $z = 0$.

- Si $\sum_{n=0}^{\infty} c_n z^n$ es una serie de potencia con radio de convergencia $R \neq 0$, la serie se denomina "Serie de potencia convergente".

- Si D es un disco de centro 0 tal que $D \subset D_{(0,R)}$, tenemos que $\sum_{n=0}^{\infty} c_n z^n$ converge en D.

El radio de convergencia se puede determinar con la información que proporciona los coeficientes de la serie de potencias. Veamos:

Sea $(t_n)_{n\in\mathbb{N}}$ una sucesión de números reales no negativos $(t_n \geq 0)$.
Recordemos que un número $t \in \mathbb{R}$ es un punto de acumulación de $(t_n)_{n\in\mathbb{N}}$ si para cada $\varepsilon > 0$ existen infinitos índices n tal que $|t_n - t| < \varepsilon$.

Una propiedad principal de los números reales **(Teorema Bolzano-Weiertrass)** nos afirma que cada sucesión acotada tiene al menos un punto de acumulación. (observar la figura)

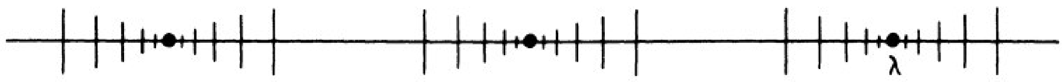

Figura 2.1: **Puntos de acumulación**

Supongamos ahora que $(t_n)_{n\in\mathbb{N}}$ es una sucesión acotada de números reales no negativos y S el conjunto de los puntos de acumulación de la figura 2.1. Es decir:

$$S = \{\ p \in \mathbb{R}\ /\ p \text{ es punto de acumulación de } (t_n)_{n\in\mathbb{N}}\ \}.$$

Definimos el límite superior de $(t_n)_{n\in\mathbb{N}}$ como $\lambda = \text{lím}\, sup(t_n) = Sup\, S$.

Algunas propiedades que tenemos de este limite superior son:

Proposición 2.2. $\lambda = \text{lím}\, sup(t_n)$ es un punto de acumulación de (t_n).

Prueba. Sea $\varepsilon > 0$, entonces existe $p \in S$ tal que $\lambda - \varepsilon < p$, esto implica que existen infinitos índices n tal que $p - t_n \leq |t_n - p| < p + \varepsilon - \lambda$, así

$$\lambda - \varepsilon < t_n \tag{2.1.1}$$

Como $p \in S$ y $\lambda = sup\, S$, entonces $p \leq \lambda < \lambda + \varepsilon$, luego existen infinitos índices n tal que $t_n - p \leq |t_n - p| < \lambda + \varepsilon - p$, lo que implica que

$$t_n < \varepsilon + \lambda \tag{2.1.2}$$

Por lo tanto de (2.1.1) y de (2.1.2) tenemos que existen infinitos índices n tales que $(\lambda - \varepsilon) < t_n < (\varepsilon + \lambda)$, es decir que λ es un punto de acumulación de $(t_n)_{n\in\mathbb{N}}$.

□

Esta propiedad nos dice que $\lambda \in S$, lo que nos garantiza que

$$\lambda = \text{lím}\, sup(t_n) = Max\, S.$$

Proposición 2.3. λ es igual al $\text{lím}\, sup(t_n)$ si y solo si para cada $\varepsilon > 0$ existen infinitos índices n tales que $\lambda - \varepsilon \leq t_n$ y ademas existen finitos índices n tales que $\varepsilon + \lambda \leq t_n$.

Prueba. Sea $\varepsilon > 0$. Como $\lambda \in S$, entonces existen infinitos índices n tales que $\lambda - \varepsilon < t_n < \varepsilon + \lambda$.

Ahora supongamos que existen infinitos índices n tales que $\varepsilon + \lambda \leq t_n$, entonces existe un conjunto infinito y acotado $\{t_{n_1}, t_{n_2}, ...\}$ tal que

$$\varepsilon + \lambda \leq t_{n_j} \tag{2.1.3}$$

Luego existe un punto de acumulación p donde t_{n_j} converge a p, aplicando el limite a la desigualdad (2.1.3) tenemos que $\lambda < \varepsilon + \lambda \leq p$ y esto es una contradicción, pues $p \in S$.

Recíprocamente, Sea $p \in S$ y supongamos que $p > \lambda$.
Ahora tomemos un $\varepsilon = (p-\lambda)/2 > 0$, entonces por la hipótesis existen finitos índices n tales que $(\lambda + p)/2 = \lambda + \varepsilon \leq t_n$.

Así existen finitos índices n tales que $(\lambda + p)/2 = p - \varepsilon \leq t_n \leq p + \varepsilon$ lo que implica que $p \notin S$ lo cual es una contradicción.

Por lo tanto para todo $p \in S$, $p \leq \lambda$, es decir, $\lambda = Max\, S$.

□

Proposición 2.4. Sea $(t_n)_{n\in\mathbb{N}}$ una sucesión acotada de números no negativos, entonces

$$lím\, sup(t_n) = \lim_{n\to\infty}\left(\sup_{k\geq n}(t_k)\right).$$

Prueba. Sea $p \in S$ arbitrario (p es punto de acumulación de $(t_n)_{n\in\mathbb{N}}$).

Luego la sucesión $(t_n)_{n\in\mathbb{N}}$ tiene una subsucesión $(t_{k_{(n)}})$ tal que $\lim\limits_{n\to\infty} t_{k_{(n)}} = p$

Como k es una aplicación estrictamente creciente entonces $k_{(n)} \geq n$, para todo $n \in \mathbb{N}$.

Por la definición de supremo tenemos $t_{k_{(n)}} \leq \sup\limits_{k\geq n}(t_k)$.

Tomando el límite a la desigualdad obtenemos $p \leq \lim\limits_{n\to\infty}(\sup\limits_{k\geq n}(t_k))$.

Como esto se cumple para cualquier $p \in S$ entonces

$$lím\, sup(t_n) := Max\, S = \lim_{n\to\infty}\left(\sup_{k\geq n}(t_k)\right).$$

□

Proposición 2.5. Sea $(t_n)_{n\in\mathbb{N}}$ una sucesión acotada de números no negativos, entonces

$$lím\, sup(t_n) = \inf_{n\in\mathbb{N}}\left(\sup_{k\geq n}(t_k)\right).$$

Prueba. Sea $A_n = \{t_n, t_{n+1}, t_{n+2}, ...\}$, para todo $n \in \mathbb{N}$.

Evidentemente A_n es acotado.

Ahora definimos la sucesión $(S_n)_{n\in\mathbb{N}}$ definida por $S_n = \sup\limits_{n\in\mathbb{N}} A_n = \sup\limits_{k\geq n}(t_k)$, para todo $n \in \mathbb{N}$.

Como $A_{n+1} \subset A_n$, para todo $n \in \mathbb{N}$, entonces $S_{n+1} \leq S_n$, para todo $n \in \mathbb{N}$. Lo que significa que la sucesión $(S_n)_{n\in\mathbb{N}}$ es monótona decreciente y además esta acotada.

Esto quiere decir que $\lim\limits_{n\to\infty} S_n = \inf\limits_{n\in\mathbb{N}}(S_n)$.

Por lo tanto $\lim\limits_{n\to\infty}\left(\sup\limits_{k\geq n}(t_k)\right) = \inf\limits_{n\in\mathbb{N}}\left(\sup\limits_{k\geq n}(t_k)\right)$.

□

Con estas dos propiedades anteriores el límite superior de una sucesión acotada $(t_n)_{n\in\mathbb{N}}$ se puede expresar de tres maneras

$$lím\, sup(t_n) := Max\, S = \lim_{n\to\infty}\left(\sup_{k\geq n}(t_k)\right) = \inf_{n\in\mathbb{N}}\left(\sup_{k\geq n}(t_k)\right).$$

Donde S es el conjunto de todos los puntos de acumulación de $(t_n)_{n\in\mathbb{N}}$.

Por conveniencia, si la sucesión $(t_n)_{n\in\mathbb{N}}$ con $t_n \geq 0$ no esta acotada superiormente definimos su limite superior como infinito $(lím\, sup(t_n) = \infty)$.

Proposición 2.6. Sean las sucesiones de números reales $(t_n)_{n\in\mathbb{N}}$, $(s_n)_{n\in\mathbb{N}}$ con $t_n, s_n \geq 0$. Si $t = lím\ sup(t_n)$ y $s = lím\ sup(s_n)$ entonces:

(i) $lím\, sup(t_n + s_n) = t + s$.

(ii) Si $t \neq 0$, entonces $lím\, sup(t_n s_n) = ts$.

(iii) Si existe un $n_0 \in \mathbb{N}$ tal que $t_n \leq s_n$, para todo $n \geq n_0$, entonces $t \leq s$.

(iv) Si existe $\lim\limits_{n\to\infty} t_n$, entonces $t = \lim\limits_{n\to\infty} t_n$.

Prueba.
Las partes **(i)**,**(ii)** y **(iii)** salen inmediatamente si reemplazamos a t y s con

$$t = \lim_{n\to\infty}\left(\sup_{k\geq n}(t_k)\right) \quad \text{y} \quad s = \lim_{n\to\infty}\left(\sup_{k\geq n}(s_k)\right).$$

Luego aplicamos las propiedades de supremo y los límites clásicos de sucesiones.

(iv) Sea $\lim\limits_{n\to\infty} t_n = a$, afirmamos que $(t_n)_{n\in\mathbb{N}}$ tiene un único punto de acumulación.

En efecto :
Sean α y β puntos de acumulación de $(t_n)_{n\in\mathbb{N}}$, entonces existen t_{n_1},$t_{n_2}, ...$ infinitos tales que $t_{n_j} \longrightarrow \alpha$ y existen $t_{m_1}, t_{m_2}, ...$ infinitos tales que $t_{m_j} \longrightarrow \beta$.

Luego por el teorema de Bolzano Weierstrass tenemos que $a = \alpha = \beta$.

Como $(t_n)_{n\in\mathbb{N}}$ tiene un solo punto de acumulación entonces $S = \{a\}$, esto quiere decir que $t = lím\, sup(t_n) = sup\, S = a = \lim\limits_{n\to\infty} t_n$.

□

La hipótesis de **(ii)** que dice que $t \neq 0$ esta hecho para permitir la posibilidad de que $s = \infty$ en cuyo caso ts es ∞.

Si $s \neq \infty$ y $t \neq \infty$ entonces $lím\, sup(t_n s_n) = ts$ sin restricciones.

Teorema 2.4. Sea $\sum\limits_{n=0}^{\infty} c_n z^n$ una serie de potencia con radio de convergencia $R > 0$, entonces

$$lím\, sup|c_n|^{1/n} = \frac{1}{R}.$$

Si $R = 0$ entonces $\left(|c_n|^{1/n}\right)_{n\in\mathbb{N}}$ es una sucesión no acotada .

Si $R = \infty$ entonces $\textit{lím sup}|c_n|^{1/n} = 0$.

Prueba. Sea $A = \left\{ r \geq 0 \ / \ (|c_n|r^n)_{n\in\mathbb{N}} \text{ es una sucesión acotada} \right\}$ donde el radio de convergencia de la serie de potencia es $R = sup\, A$.

Caso 1. Supongamos que $0 < R < \infty$.

Sea un s arbitrario tal que $0 < s < R$.

Esto quiere decir que la serie $\sum\limits_{n=0}^{\infty} |c_n|s^n$ converge, entonces

existe $c > 0$ tal que $|c_n|s^n \leq c$, para todo $n \in \mathbb{N}$, luego $|c_n|^{1/n} \leq \dfrac{c^{1/n}}{s}$ y como $\lim\limits_{n\to\infty} c^{1/n} = 1$ puesto que $c > 0$.

Luego tenemos que

$$\textit{lím sup}|\, c_n|^{1/n} \leq \textit{lím sup}\left(\frac{c^{1/n}}{s}\right) = \frac{1}{s}.$$

Entonces $\textit{lím sup}|\, c_n|^{1/n} \leq \dfrac{1}{s}$ para cualquier $s < R$.

Esto implica que

$$\textit{lím sup}|\, c_n|^{1/n} \leq \frac{1}{R}. \tag{2.1.4}$$

Ahora si $s > R$ (s arbitrario)

tenemos que $\sum\limits_{n=0}^{\infty} |c_n|s^n$ es divergente, luego por el criterio de la raíz

existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$, $(|c_n|s^n)^{1/n} \geq 1$, es decir, $|c_n|^{1/n} \geq \frac{1}{s}$, para todo $n > n_0$.

Entonces $\textit{lím sup}|c_n|^{1/n} \geq \frac{1}{s}$, para cualquier $s > R$ el cual implica que

$$\textit{lím sup}|c_n|^{1/n} \geq \frac{1}{R}. \tag{2.1.5}$$

Por lo tanto de (2.1.4) y (2.1.5) tenemos $\textit{lím sup}|c_n|^{1/n} = \frac{1}{R}$.

Caso 2. Si $R = 0$.

Tenemos que para todo $r > 0$, $(|c_n|r^n)_{n\in\mathbb{N}}$ es una sucesión no acotada.

Esto quiere decir que si tomamos un $M > 0$ arbitrario entonces $\left(|c_n|\dfrac{1}{M^n}\right)_{n\in\mathbb{N}}$ no esta acotada, es decir, existe $n \in \mathbb{N}$ tal que $|c_n|\frac{1}{M^n} > 1$, lo que implica que $|c_n|^{1/n} > M$

Por lo tanto $\left(|c_n|^{1/n}\right)_{n\in\mathbb{N}}$ no esta acotado .

Caso 3. Si $R = \infty$.

Se sabe que A no esta acotado. Dado un $\varepsilon > 0$ arbitrario, entonces existe un $s \in A$ tal que $s > \frac{1}{\varepsilon}$, luego existe $M > 0$ tal que $|c_n|s^n \leq M$, para todo $n \in \mathbb{N}$, lo que implica que $\lim\limits_{n\to\infty} |c_n|^{1/n} < \frac{1}{s} < \varepsilon$, entonces existe $n_0 \in \mathbb{N}$ tal que para todo $n > n_0$, $|c_n|^{1/n} < \varepsilon$, es decir, $\lim\limits_{n\to\infty} |c_n|^{1/n} = 0$ y por proposición 2.6-(iv), $\textit{lím}\, sup|c_n|^{1/n} = 0$.

□

2.2. Cociente de series de potencias formales con coeficientes complejos

Definición 2.5. Una serie de potencias formal de T con coeficientes complejos es una expresión de la forma:

$$\sum_{n=0}^{\infty} a_n T^n = a_0 + a_1 T + a_2 T^2 + \ldots$$

La cual esta definida pricipalmente en aplicación de sus coeficientes

$$\{a_0, a_1, a_2, \ldots\} \subset \mathbb{C}.$$

También podemos identificar las series formales como una función $A : \mathbb{N} \longrightarrow \mathbb{C}$, donde $A(n) = a_n$ que podremos denotar como $f(T) = a_0 + a_1T + a_2T^2 + \ldots$, cabe notar que aquí f no es una aplicación, sino una expresión formal.

Ejemplo 2.1. También podemos usar expresiones para las series formales como $2 + 3T + 7T^3$, que no entenderemos como un polinomio de grado 3, sino como una representación de la serie $2 + 3T + 0T^2 + 7T^3 + 0T^4 + \ldots$ donde $a_n = 0$ para todo $n > 3$.

Denominaremos término constante de una serie compleja formal de potencias al coeficiente a_0.

2.2.1. Operaciones de series de potencias formales con coeficientes complejos

Dadas las series

$$f = \sum_{n=0}^{\infty} a_n T^n \quad \text{y} \quad g = \sum_{n=0}^{\infty} b_n T^n$$

Definimos:

- $f + g = \sum\limits_{n=0}^{\infty} c_n T^n$ donde $c_n = a_n + b_n$ y
- $fg = \sum\limits_{n=0}^{\infty} d_n T^n$ donde $d_n = \sum\limits_{i=0}^{n} a_i b_{n-i}$.

Si α es un número complejo, definimos

$$\alpha f = \sum_{n=0}^{\infty}(\alpha a_n)T^n.$$

Al igual que para los polinomios, con estas dos operaciones (suma y producto) se verifica que las series complejas formales de potencias son conmutativas, asociativas y distributivas.

Definición 2.6. Dada una serie de potencias formal con coeficientes complejos

$$f = \sum_{n=0}^{\infty} a_n T^n$$

llamaremos orden de f, al menor número natural r tal que a_r sea diferente de cero y lo denotaremos $r = Ord(f)$.

Por tanto si tenemos, $f = a_r T^r + ...$ y $g = b_s T^s + ...$ con $a_r, b_s \neq 0$ se verifica que $fg = a_r b_s T^{r+s} + t.o.s.$

De donde se deduce que

$$Ord(fg) = Ord(f) + Ord(g).$$

Observación 2.4.

(i) El orden de una serie de potencias será 0 si y solo si su término constante a_0 es no nulo.

(ii) Diremos que el orden de una serie de potencia nula, donde todos los coeficientes son cero, es infinito (∞).

(iii) Dada una serie formal f diremos que la serie formal g es inversa de f si

$$fg = 1.$$

Denotaremos $g = f^{-1}$.

Notemos por la observación anterior que si f tiene inversa entonces su término constante es diferente de cero, es decir, $Ord(f) = 0$.

La recíproca, también es verdadera, lo cual veremos a continuación.

Teorema 2.5. Sea una serie formal f, si $Ord(f) = 0$ entonces existe una serie formal g que es inversa de f.

Prueba. Sea $f = \sum_{n=0}^{\infty} a_n T^n$, considerando $a_0^{-1} f$ en lugar de f, reducimos el problema al caso con término constante igual a 1.

Antes de proceder observemos que

$$1 = (1 - T)(1 + T + T^2 + T^3 + ...)$$

Entonces consideremos

$$f = 1 - h, \text{ donde } h = -(a_1 T + a_2 T^2 + ...) \text{ y } Ord\, h \geq 1.$$

Para definir la inversa de $(1 - h)$ intuitivamente podemos afirmar que

$$\phi = (1 - h)^{-1} = 1 + h + h^2 + h^3 + ...$$

De este modo se nos plantea la interrogante, **¿ Es $\boldsymbol{\phi}$ una serie de potencia formal de $\boldsymbol{T}$?**, para responder a esto consideremos la suma finita

$$1 + h + h^2 + h^3 + ... + h^m$$

que al ser un producto y suma finita de series de potencias formales con coeficientes complejos es a su vez una serie de potencias formal y como el $Ord(h) \geq 1$, al añadir un sumando de la forma h^{m+1}, cuyo orden es estrictamente mayor que m, los m primeros coeficientes no varían, característica que se repite al añadir h^{m+2}, y en general, al añadir cualquier h^p con $p > m$.

Así al ir aumentando la cantidad de sumandos, notamos que el i-ésimo coeficiente queda establecido una vez que pasemos por el sumando h^i, por lo tanto podemos definir

$$\phi = \sum_{n=0}^{\infty} e_n T^n$$

donde e_n es el n-ésimo término de $\sum_{n=0}^{\infty} h^i$.

De todo lo anterior tenemos que

$$(1 - h)(1 + h + h^2 + h^3 + ...) = (1 - h)\, \phi = f\, \phi = 1.$$

$\square$

2.3. Campo de fracciones de series de potencias formales con coeficientes complejos

Consideremos ahora, el conjunto de todas las series complejas formales junto a las operaciones de suma y producto que definimos, otorgándole así una estructura de anillo. Ahora podemos afirmar que dicho anillo es un Dominio de Integridad, es decir, no posee divisores de cero, por lo cual es posible definir un campo que contenga a dicho anillo. Para definir este campo es necesario primero dar la noción de cociente entre dos series complejas formales cualesquiera.

Definición 2.7. Dadas las series de potencias formales $f = \sum_{n=0}^{\infty} a_n T^n$ y $g = \sum_{n=0}^{\infty} b_n T^n$. Al igual que los números racionales m/n son formadas por enteros m, n con $n \neq 0$ podemos definir cocientes de series formales como:

$$f/g = \frac{f(T)}{g(T)}$$

donde $g(T) \neq 0$. Dos cocientes f/g y f_1/g_1 se consideran iguales si $fg_1 = f_1 g$ exactamente con la misma condición que se da en el caso de números racionales.

Definición 2.8. Definiremos la suma y el producto de cocientes de series formales de la siguientes manera:

- $f/g \; + \; p/q = (fq + gp)/(gq)$
- $f/g \; . \; p/q = (fp)/(gq)$

Con estas definiciones se verifican de forma inmediata las siguientes propiedades:

(i) Sea f una serie de potencias formal, entonces

$$f/1 = f.$$

(ii) Si f es una serie de potencias formal invertible, entonces

$$1/f = f^{-1}.$$

(iii) Sean f, g y h series de potencias formal, donde $g \neq 0$ y $h \neq 0$ entonces

$$(hf)/(hg) = f/g.$$

Observación 2.5. Sea la serie compleja formal de potencias

$$f = a_m T^m + a_{m+1} T^{m+1} + \cdots = \sum_{n=m}^{\infty} a_n T^n$$

donde $a_m \neq 0$. Podemos reescribir f de la forma

$$f = (a_m T^m) g$$

donde g es una serie de potencias formal con coeficientes complejos de orden igual a cero, en consecuencia $1/f$ tiene la forma

$$1/f = \frac{1}{a_m T^m} . \frac{1}{g}$$

Ya sabemos que $\dfrac{1}{g}$ es una serie de potencias formal de orden igual a cero, podemos escribir entonces De esta manera $1/f$ se expresa como

$$1/f = a_m^{-1}\frac{1}{T^m} + a_m^{-1}\frac{b_1}{T^{m-1}} + a_m^{-1}\frac{b_2}{T^{m-2}} + \cdots$$

la cual es una serie de potencias formal con coeficientes complejos con una cantidad finita de términos con potencias negativas de T, de esta manera se ve que un cociente de series formales arbitrarias se puede ver como una serie de la forma

$$f/g = \frac{c_{-m}}{T^m} + \frac{c_{-m+1}}{T^{m-1}} + \cdots + \frac{c_1}{T} + c_0 + c_1T + c_2T^2 + \cdots = \sum_{n\geqslant -m} c_nT^n.$$

Es fácil notar que f/g no es necesariamente una serie de potencias formal; para solventar esto es conveniente ampliar la definición de series de potencias formales con coeficientes complejos de la siguiente manera:

$$f/g = \phi = \sum_{n\in\mathbb{Z}} a_nT^n = \sum_{-\infty}^{\infty} a_nT^n.$$

Donde existe un $m \in \mathbb{Z}$, tal que $a_n = 0$ para todo $n < m$. Así tenemos la siguiente representación alternativa

$$\phi = \sum_{n=m}^{\infty} a_nT^n.$$

Ejemplo 2.2. Considerando $\phi = 5T^{-2}+6iT^{-1}+1+6T+iT^2+\cdots = \sum_{n=-2}^{\infty} a_nT^n$, notemos que ϕ puede escribirse también de la forma:
$\phi = 0T^{-3} + 5T^{-2} + 6iT^{-1} + 1 + 6T + iT^2 + \cdots = \sum_{n=-3}^{\infty} a_nT^n$, pero es imposible darle a ϕ una representación de la forma $\sum_{n=-1}^{\infty} a_nT^n$.

Del ejemplo anterior deducimos que cualquier serie de potencias formal tiene una cantidad infinita de representaciones simplemente añadiendo términos a la izquierda con coeficiente nulo, y en caso de que ϕ fuese diferente de cero, existe un máximo número k tal que $\phi = \sum_{n=k}^{\infty} a_nT^n$.

Diremos entonces que el orden de ϕ es k, y análogamente a las series de potencias formales inicialmente consideradas, se verifica también

$$Ord(\phi\,\phi_1) = Ord(\phi) + Ord(\phi_1).$$

Diremos que el orden de $\phi = 0$ es ∞.

2.4. Operaciones en el campo de fracciones de series formales con coeficientes complejos

Dado que hemos redefinido el concepto de serie formal con coeficientes complejos, es necesario hacer pequeños ajustes a la definición de sus operaciones para eliminar cualquier ambiguedad posible.

Sean las series complejas formales

$$\phi_1 = \sum_{n=i}^{\infty} a_n T^n \quad \text{y} \quad \phi_2 = \sum_{n=j}^{\infty} b_n T^n.$$

donde $i \leq j$. Añadiendo los términos a la izquierda que fuesen necesarios podemos escribir $\phi_2 = \sum_{n=i}^{\infty} a_n T^n$ teniendo así

- $\phi_1 + \phi_2 = \sum_{n=i}^{\infty} c_n T^n$ donde $c_n = a_n + b_n$.

Notemos que podemos escribir

$$\phi_1 = T^i \sum_{n=0}^{\infty} a_{i+n} T^n = T^i f \quad \text{y} \quad \phi_2 = T^j \sum_{n=0}^{\infty} b_{j+n} T^n = T^j g$$

donde f y g son series formales clásicas, definimos entonces

- $\phi_1 \, \phi_2 = T^{i+j} f g$ donde fg es producto usual de series formales.
- Si $\phi_2 \neq 0$, $\phi_1/\phi_2 = T^{i-j} f/g$ donde f/g es cociente usual de series formales.

2.5. Composición de Series de Potencias Formales

Sean las series de potencias formales $f(T) = \sum_{n=0}^{\infty} a_n T^n$ y $h(T) = \sum_{n=0}^{\infty} c_n T^n$ con término constante nulo ($c_0 = 0$) entonces la composición $(f \, o \, h)$ está definida como

$(f \, o \, h)(T) := f(h(T)) := f \, o \, h := a_0 + a_1 h + a_2 h^2 + ...$ donde $h = h(T)$.

Esta serie formal está bien definida, veamos :

Como $c_0 = 0$ entonces $Ord(h^m) \geq m$, para todo $m \in \mathbb{N}$, puesto que $Ord(h) \geq 1$.

Tenemos:

$$\begin{array}{rcccccccl}
a_1h & = & v_1^{(1)}T & + & v_2^{(1)}T^2 & + & v_3^{(1)}T^3 & + & ... \\
a_2h^2 & = & v_2^{(2)}T^2 & + & v_3^{(2)}T^3 & + & v_4^{(2)}T^4 & + & ... \\
a_3h^3 & = & v_3^{(3)}T^3 & + & v_4^{(3)}T^4 & + & v_5^{(3)}T^5 & + & ... \\
\vdots & & \vdots & & \vdots & & \vdots & & \\
a_mh^m & = & v_m^{(m)}T^m & + & v_{m+1}^{(m)}T^{m+1} & + & v_{m+2}^{(m)}T^{m+2} & + & ...
\end{array}$$

Ahora si le sumamos a_0 a estas expresiones tenemos:

$a_0 + a_1h + a_2h^2 + a_3h^3 + ...a_mh^m = a_0 + v_1^{(1)}T + (v_2^{(1)} + v_2^{(2)})T^2 + (v_3^{(1)} + v_3^{(2)} +$

$v_3^{(3)})T^3 + ... + (v_m^{(1)} + v_m^{(2)} ... + v_m^{(m)})T^m + ...$

Como vemos todos los coeficientes existen ya que son sumatorias finitas, es decir que se pueden escribir de la siguiente manera:

$a_0 + a_1h + a_2h^2 + a_3h^3 + ...a_mh^m = e_0 + e_1T + e_2t^2 + e_3T^3 + ... + e_mT^m + ...$

esta característica no variará al sumarle a una expresión de la forma

$$a_{m+1}h^{m+1}, a_{m+2}h^{m+2}, a_{m+3}h^{m+3}, ...$$

Entonces $(f\,o\,h)(T)$ se puede expresar como una serie de potencia formal

$$(f\,o\,h)(T) = a_0 + a_1h + a_2h^2 + a_3h^3 + ...a_mh^m + ...$$

$$= e_0 + e_1T + e_2t^2 + e_3T^3 + ... + e_mT^m + ...$$

Lo que quiere decir que $(f\,o\,h)$ esta bien definido.

¿ Qué sucede si el término constante c_0 es diferente de cero ?

Veamos el siguiente ejemplo:

Sea la serie de potencia formal $f(T) = 1 + T + T^2 + T^3 + ...$
Como observamos su término constante no es nulo y el $Ord(f) = 0$ *luego* $Ord(f^m) = 0$.

Formando la composición $(f\,o\,f)(T) = 1 + f + f^2 + f^3 + ...$ *tenemos:*

$$\begin{array}{rcccccccc} f = & 1 & + & T & + & T^2 & + & T^3 & +... \\ f^2 = & 1 & + & v_1^{(2)}T & + & v_2^{(2)}T^2 & + & v_3^{(2)}T^3 & +... \\ f^3 = & 1 & + & v_1^{(3)}T & + & v_2^{(3)}T^2 & + & v_3^{(3)}T^3 & +... \\ & & & & \vdots & & & & \\ f^m = & 1 & + & v_1^{(m)}T & + & v_2^{(m)}T^2 & + & v_3^{(m)}T^3 & +... \end{array}$$

Luego,

$1 + f + f^2 + f^3 + ... + f^m = 1 + m + (1 + v_1^{(2)} + v_1^{(3)} + ... + v_1^{(m)})T + (1 + v_2^{(2)} +$

$v_2^{(3)} + ... + v_2^{(m)})T^2 + ... + (1 + v_m^{(2)} + v_m^{(3)} + ... + v_m^{(m)})T^m + ...$

Si sumamos las series de potencias formales $f^{m+1}, f^{m+2}, f^{m+3}, ...$ *los coeficientes de la nueva suma no se podrían controlar (es decir divergen ya que sería una suma infinita de coeficientes).*

Podemos calcular la composición, suma y producto de series de potencias formales a través de la aproximación de estas series de potencias formales con polinomios. Para ello daremos la siguiente definición:

Definición 2.9. Sean $f(T) = \displaystyle\sum_{n=0}^{\infty} a_n T^n$ y $g(T) = \displaystyle\sum_{n=0}^{\infty} b_n T^n$ dos series de potencias formales. Diremos que f y g son $mod\,T^N$ $(N \geq 1)$ congruentes y lo denotaremos $f \equiv g(mod\,T^N)$ si $a_n = b_n,$ para todo $n = 0, 1, 2, ..., N-1.$

Proposición 2.7. Sea $f(T) = \displaystyle\sum_{n=0}^{\infty} a_n T^n$ una serie de potencias formal, entonces existe un único polinomio $P(T)$ de grado $\leq N-1$ tal que $f \equiv P(mod\,T^N)$.

Prueba. En efecto:

Si $P(T) = a_0 + a_1 T + a_2 T^2 + ... + a_{N-1} T^{N-1}$ entonces P es un polinomio de grado $\leq N-1$ donde evidentemente $f \equiv P(mod\,T^N)$.

Supongamos que existe otro polinomio de grado $\leq N-1,$ digamos Q.

Sea $Q(T) = b_0 + b_1 T + b_2 T^2 + ... + b_{N-1} T^{N-1}$ tal que $f \equiv Q(mod\,T^N),$ esto quiere decir que $a_n = b_n,$ para todo $n = 0, 1, 2, ..., N-1.$

Luego $Q(T) = a_0 + a_1 T + a_2 T^2 + ... + a_{N-1} T^{N-1} = P(T).$

$\square$

Proposición 2.8. Sean $f_1 \equiv f_2(mod\, T^N)$ y $g_1 \equiv g_2(mod\, T^N)$, entonces

(i) $(f_1 + g_1) \equiv (f_2 + g_2)(mod\, T^N)$.

(ii) $(f_1 g_1) \equiv (f_2 g_2)(mod\, T^N)$.

Prueba. Sean

$$f_1(T) = \sum_{n=0}^{\infty} a_n T^n, \quad f_2(T) = \sum_{n=0}^{\infty} a_n^* T^n, \quad g_1(T) = \sum_{n=0}^{\infty} b_n T^n \quad \text{y} \quad g_2(T) = \sum_{n=0}^{\infty} b_n^* T^n.$$

Donde la suma y producto de estas series tienen las siguientes representaciones:

$$f_1 + g_1 = \sum_{n=0}^{\infty} (a_n + b_n) T^n,$$
$$f_2 + g_2 = \sum_{n=0}^{\infty} (a_n^* + b_n^*) T^n$$
$$f_1 g_1 = \sum_{n=0}^{\infty} d_n T^n \quad \text{donde} \quad d_n = \sum_{k=0}^{n} a_k b_{n-k} \ ,$$
$$f_2 g_2 = \sum_{n=0}^{\infty} d_n^* T^n \quad \text{donde} \quad d_n^* = \sum_{k=0}^{n} a_k^* b_{n-k}^* \ .$$

De la hipótesis por definición tenemos que para cada $n = 0, 1, ..., N-1$, se cumple que $a_n = a_n^*$ y $b_n = b_n^*$, lo cual implica que

$$a_n + b_n = a_n^* + b_n^* \quad \text{y} \quad d_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} a_k^* b_{n-k}^* = d_n^* \ .$$

Como esto se cumple para todo $n = 0, 1, ..., N-1$, tenemos:
$(f_1 + g_1) \equiv (f_2 + g_2)(mod\, T^N)$ y $(f_1 g_1) \equiv (f_2 g_2)(mod\, T^N)$.

□

Proposición 2.9. "$\equiv (\ )(mod\, T^N)$" es una relación de equivalencia.

Prueba. Dados $f(T) = \sum_{n=0}^{\infty} a_n T^n$, $g(T) = \sum_{n=0}^{\infty} b_n T^n$ y $h(T) = \sum_{n=0}^{\infty} c_n T^n$.

(i) Reflexividad:

Evidentemente, $a_n = a_n$, para todo $n = 0, 1, 2, ..., N-1$. Es decir, $f \equiv f(mod\, T^N)$.

(ii) Simetría:

Si $f \equiv g(mod\, T^N)$, entonces $a_n = b_n$, para todo $n = 0, 1, 2, ..., N-1$.

Luego $b_n = a_n$, para todo $n = 0, 1, 2, ..., N-1$.

Por lo tanto $g \equiv f(mod\, T^N)$.

(iii) Transitividad:

Sean $f \equiv g(mod\, T^N)$ y $g \equiv f(mod\, T^N)$.

Tenemos $a_n = b_n = c_n$, para todo $n = 0, 1, 2, ..., N-1$.

Por lo tanto $f \equiv h(mod\, T^N)$.

□

Proposición 2.10. Sean f_1, f_2, h_1, h_2 series de potencias formales tales que h_1 y h_2 tienen término constante igual a cero.

Si $f_1 \equiv f_2(mod\, T^N)$ y $h_1 \equiv h_2(mod\, T^N)$ entonces $f_1 o\, h_1 \equiv f_2 o\, h_2(mod\, T^N)$.

Prueba. De la proposición 2.7 sabemos que existen dos polinomios P_1 y P_2 de grado $\leq N-1$ tales que $f_1 \equiv P_1(mod\, T^N)$ y $f_2 \equiv P_2(mod\, T^N)$.

Para evitar el abuso de notación de los módulos congruentes en la prueba, lo denotaremos de la siguiente manera: $f_1 \equiv P_1$ y $f_2 \equiv P_2$.

Como $f_1 \equiv f_2$ y por ser " $\equiv$ " una relación de equivalencia tenemos por transitividad $P_1 \equiv P_2$.

Esto quiere decir que $P_1(T) = P_2(T) = P(T) = a_0 + a_1 T + ... + a_{N-1} T^{N-1}$.

Además, como $h_1(T)$ es una sfp con término constante nulo, entonces tenemos:

$$f_1\, o\, h_1(T) = a_0 + v_1 T + ... + v_{N-1} T^{N-1} + v_N T^N + v_{N+1} T^{N+1} + ...$$

$$P_1\, o\, h_1(T) = a_0 + v_1 T + ... + v_{N-1} T^{N-1} + v_N^* T^N + v_{N+1}^* T^{N+1} + ...$$

Luego $f_1\, o\, h_1 \equiv P_1\, o\, h_1 = P\, o\, h_1$.
De manera análoga obtenemos $f_2\, o\, h_2 \equiv P_2\, o\, h_2 = P\, o\, h_2$.

Como $h_1 \equiv h_2$, entonces existe un polinomio Q de grado $\leq N-1$ tal que $h_1 \equiv h_2 \equiv Q$.

Luego de proposición 2.8:

$$P\, o\, h_1 = a_0 + a_1 h_1 + ... + a_{N-1} h_1^{N-1} \equiv \; a_0 + a_1 Q + ... + a_{N-1} Q^{N-1}$$
$$P\, o\, h_2 = a_0 + a_1 h_2 + ... + a_{N-1} h_2^{N-1} \equiv \; a_0 + a_1 Q + ... + a_{N-1} Q^{N-1}$$

Es decir, $P\, o\, h_1 \equiv P\, o\, h_2$

Finalmente $f_1 o\, h_1 \equiv P\, o\, h_1 \equiv P\, o\, h_2 \equiv f_2\, o\, h_2$.

□

Con estas propiedades podemos calcular los coeficientes de operaciones fundamentales entre series de potencias formales reduciendo los cálculos a operaciones polinómicas.

Definición 2.10. Sean f y g series de potencias formales, diremos que $f = g$ si para cada $N \in \mathbb{Z}^+$, $f_1 \equiv f_2(mod\, T^N)$.

Proposición 2.11. Si f_1,f_2 y h son series de potencias formales tales que h tiene su término constante igual a cero, entonces

(i) $(f_1 + f_2)\, o\, h = f_1\, o\, h + f_2\, o\, h$.

(ii) $(f_1 f_2)\, o\, h = (f_1\, o\, h)(f_2\, o\, h)$.

(iii) Si $Ord\, f_2 = 0$, $(f_1/f_2)\, o\, h = (f_1\, o\, h)/(f_2\, o\, h)$.

Prueba. Sea un $N \in \mathbb{Z}^+$ arbitrario, entonces existen los polinomios P, Q, R de grados $\leq N-1$ tales que $f_1 \equiv P(mod\, T^N)$, $f_2 \equiv Q(mod\, T^N)$, $h \equiv R(mod\, T^N)$.

Luego aplicando las propiedades anteriores y las propiedades polinómicas tenemos:

(i) $(f_1 + f_2)\, o\, h \equiv (P + Q)\, o\, R \equiv (P\, o\, R) + (Q\, o\, R) \equiv (f_1\, o\, h) + (f_2\, o\, h)$ para cada N entonces por definición $(f_1 + f_2)\, o\, h = (f_1\, o\, h) + (f_2\, o\, h)$.

(ii) $(f_1 f_2)\, o\, h \equiv (PQ)\, o\, R \equiv (P\, o\, R)(Q\, o\, R) \equiv (f_1\, o\, h)(f_2\, o\, h)$ para cada N entonces por definición $(f_1 f_2)\, o\, h = (f_1\, o\, h)(f_2\, o\, h)$.

(iii) Si $Ord\, f_2 = 0$ entonces f_2 tiene inversa la cual es $f_2^{-1} = 1/f_2$.

Luego por la parte (ii) tenemos

$(f_1/f_2)\, o\, h = (f_1 f_2^{-1})\, o\, h = (f_1\, o\, h)(f_2^{-1}\, o\, h)$
$(f_1/f_2)\, o\, h = (f_1\, o\, h)(1/f_2\, o\, h) = (f_1\, o\, h)/(f_2\, o\, h)$

□

Proposición 2.12. Sean f, g, h series de potencias formales donde g y h tienen términos constantes igual a cero entonces $f\, o\, (g\, o\, h)$=$(f\, o\, g)\, o\, h$.

Prueba. Sea un $N \in \mathbb{Z}^+$ arbitrario.

Entonces existen los polinomios P, Q, R de grados $\leq N-1$ tales que
$f \equiv P(mod\, T^N)$, $g \equiv Q(mod\, T^N)$, $h \equiv R(mod\, T^N)$.

Luego por la proposición 2.9 y las propiedades polinómicas tenemos
$f\, o\, (g\, o\, h) \equiv P\, o\, (Q\, o\, R) \equiv (P\, o\, Q)\, o\, R \equiv (f\, o\, g)\, o\, h$ entonces $f\, o\, (g\, o\, h) \equiv (f\, o\, g)\, o\, h$ para todo $N \in \mathbb{Z}^+$. Por lo tanto $f\, o\, (g\, o\, h) = (f\, o\, g)\, o\, h$.

□

Capítulo 3

AUTOMORFISMOS DE POLINOMIOS Y SERIES FORMALES

En este capítulo, que constituye la parte central nuestro trabajo, buscaremos una caracterización en los automorfismos de polinomios y, posteriormente, en series de potencias formales.

3.1. Anillo de polinomios con coeficientes en un anillo

Sea R a.c.c.i, denotaremos $R[x]$ al conjunto de polinomios con indeterminada x y coeficientes en R.

Recordemos que en la sección 2.2 definimos las series de potencias formales sobre números complejos, de esta manera definimos de forma más general las series de potencias formales si reemplazamos el conjunto de los números complejos con sus operaciones de suma y producto por R a.c.c.i, es decir,

$$f = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + ...$$

es una serie de potencias formal (s.p.f) con indeterminada x y coeficientes en R.

Dos series de potencias formales $f = \sum_{n=0}^{\infty} a_n x^n$ y $g = \sum_{n=0}^{\infty} b_n x^n$ son iguales si $a_i = b_i$, para todo $i \in \mathbb{N}_0$.

También representaremos $R[[x]]$ al conjunto de series de potencias formales con indeterminada x y coeficientes en R.

Con las operaciones de suma y producto se verifican que $R[x]$ y $R[[x]]$ son a.c.c.i.

Definición 3.1. Sea R un anillo conmutativo con identidad (a.c.c.i). Diremos que:

(i) ϕ es R-endomorfismo de $R[x]$ si ϕ es endomorfismo de $R[x]$ y para todo $r \in R,\ \phi(r) = r$.

(ii) ϕ es R-automorfismo de $R[x]$ si ϕ es automorfismo de $R[x]$ y para todo $r \in R,\ \phi(r) = r$.

• Estas definiciones son análogas para $R[[x]]$ y $R[[x_1, x_2, ..., x_n]]$.

Nota: $\{1, x, x^2, ..., x^n, ...\}$ es Linealmente Independiente en R.

Proposición 3.1 (**Propiedad universal de anillos polinomios**). Sea S un a.c.c.i., $\phi : R \longrightarrow S$ un homomorfismo y sea $t \in S$ entonces existe un único $f : R[x] \longrightarrow S$ homomorfismo tal que para todo $r \in R$ se cumple $f(r) = \phi(r),\ f(x) = t$.

Prueba. Fijamos $t \in S$ y definimos:

$$\begin{array}{rcl} f : R[x] & \longrightarrow & S \\ P = \sum_{i=0}^{n} r_i x^i & \longmapsto & f(P) = \sum_{i=0}^{n} \phi_{(r_i)} t^i \end{array}$$

Esta aplicación se verifica inmediatamente que es un homomorfismo y además es único.

Supongamos que existe otro homomorfismo $\varphi : R[x] \longrightarrow S$ tal que para todo $r \in R$, $\varphi(r) = \phi(r)$ y $\varphi(x) = t$.

Entonces $\varphi(P) = \sum_{i=0}^{n} \varphi(r_i)\varphi(x)^i = \sum_{i=0}^{n} \phi(r_i) t^i = f(P)$.

□

Observación 3.1. Si $S = R[x]$ y $\phi = Id_R : R \hookrightarrow R[x]$ la aplicación identidad, entonces para cada $t \in S$ existe un único $f : R[x] \longrightarrow R[x]$ endomorfismo tal que para todo $r \in R$ se cumple $f(r) = r$ y $f(x) = t$.

Es decir, f es un R-endomorfismo de $R[x]$ tal que $f(x) = t$.

Luego denotaremos: $f := f_t$, esto es,
para cada $t \in R[x]$ existe un único endomorfismo

$$f_t : R[x] \to R[x]$$

tal que para todo $r \in R,\ f_t(r) = r$ y $f_t(x) = t$.

Lema 3.1. Sea $t \in R[x],\ r \in R$ y u unidad de R, entonces

(a) f_t es sobreyectiva si y solo si f_{r+t} es sobreyectiva si y solo si f_{ut} es sobreyectiva.

(b) f_t es inyectiva si y solo si f_{r+t} es inyectiva si y solo si f_{ut} es inyectiva.

Prueba. Como $t \in R[x]$, $r \in R$ y u unidad de R, entonces

$$\begin{aligned} f_t(x) &= f_{r+t}(x-r) = f_{ut}(u^{-1}x) = t \\ f_{r+t}(x) &= f_t(x+r) = r+t \\ f_{ut}(x) &= f_t(ux) = ut \end{aligned}$$

Estas propiedades las aplicaremos para demostrar las partes **(a)** y **(b)**.

(a) Primero probaremos que para cualquier $t \in R[x]$, $r \in R$ y u unidad de R,

$$\text{si } f_t \text{ es sobreyectiva entonces } f_{r+t} \text{ y } f_{ut} \text{ son sobreyectivas.} \tag{3.1.1}$$

Para todo $w \in R[x]$, existe $v = \sum_{i=0}^{n} v_i x^i \in R[x]$ tal que

$$w = f_t\left(\sum_{i=0}^{n} v_i x^i\right) = f_{r+t}\left(\sum_{i=0}^{n} v_i (x-r)^i\right) = f_{ut}\left(\sum_{i=0}^{n} v_i (u^{-1}x)^i\right).$$

Ahora supongamos que f_{r+t} es sobreyectiva.

De (3.1.1) tomando a $r+t \in R[x]$ y $(-r) \in R$ tenemos que, $f_{(r+t)-r} = f_t$ es sobreyectiva.

Por lo tanto f_t es sobreyectiva si y solo si f_{r+t} es sobreyectiva.

Por otro lado, supongamos que f_{ut} es sobreyectiva.

De (3.1.1) tomando a $ut \in R[x]$ y u^{-1} unidad de R tenemos que $f_{u^{-1}(ut)} = f_t$ es sobreyectiva.

Por lo tanto f_t es sobreyectiva si y sólo si f_{ut} es sobreyectiva.

(b) Probaremos que para cualquier $t \in R[x]$, $r \in R$ y u unidad de R,

$$\text{si } f_t \text{ es inyectiva entonces } f_{r+t} \text{ y } f_{ut} \text{ son inyectivas.} \tag{3.1.2}$$

En efecto, afirmamos que $Nu(f_{r+t}) = \{0\}$.

Veamos, si $v = \sum_{i=0}^{n} v_i x^i \in Nu(f_{r+t})$, entonces

$$f_t\left(\sum_{i=0}^{n} v_i (x+r)^i\right) = f_{r+t}\left(\sum_{i=0}^{n} v_i x^i\right) = 0.$$

Luego,

$$v_0 + v_1(x+r) + v_2(x+r)^2 + ... + v_n(x+r)^n = 0.$$

$$v_0 + v_1(x+r) + (\text{ términos de grado inferior a } n\,) + v_n x^n = 0.$$

Así, $v_n = 0$.

Luego nos queda

$$v_0 + v_1(x+r) + v_2(x+r)^2 + ... + v_{n-1}(x+r)^{n-1} = 0.$$

$$v_0 + v_1(x+r) + (\text{ términos de grado inferior a } n-1) + v_{n-1}x^{n-1} = 0.$$

por ende, $v_n = v_{n-1} = 0$.

Haciendo este proceso de forma iterativa obtenemos

$$v_n = v_{n-1} = v_{n-2} = ... = v_1 = v_0 = 0.$$

Por lo tanto f_{r+t} es inyectiva.

Ahora afirmamos que $Nu(f_{ut}) = \{0\}$.

Sea $v = \sum_{i=0}^{n} v_i x^i \in Nu(f_{ut})$, entonces

$$f_t\left(\sum_{i=0}^{n} v_i(ux)^i\right) = f_{ut}\left(\sum_{i=0}^{n} v_i x^i\right) = 0.$$

Luego

$$v_0 + (v_1u)x + (v_2u^2)x^2 + ... + (v_nu^n)x^n = 0.$$

$$v_0 = v_1u = v_2u^2 = ... = v_nu^n = 0.$$

Como u es unidad de R, $v_0 = v_1 = v_2 = ... = v_n = 0$, probamos así la afirmación.

Luego, se prueba de forma análoga a la parte **(a)**, que si f_{r+t} y f_{ut} son inyectivas, de (3.1.2) se tiene que f_t es inyectiva en ambos casos.

Por lo tanto, f_t es inyectiva si y solo si f_{r+t} es inyectiva y f_t es inyectiva si y solo si f_{ut} es inyectiva.

□

Observación 3.2. Sea $t = \sum_{i=0}^{n} a_i x^i \in R[x]$, el lema 3.1 nos dice que estudiar a f_t es lo mismo que estudiar a f_{t-a_0}. Es decir, sin pérdida de generalidad se puede trabajar con $a_0 = 0$.

Sea $t' = t - a_0$ y a_1 unidad de R entonces es lo mismo trabajar con $f_{t'}$ que con $f_{a_1^{-1}t'}$.

Observación 3.3. Sean R a.c.c.i. y P, Q polinomios en $R[x]$ de grados n y m respectivamente. (Denotaremos $grad(P) = n$ y $grad(Q) = m$).

Si R es un Dominio de Integridad entonces $grad(PQ) = n + m$.

Sean

$$\begin{array}{l} P = a_0 + a_1x + a_2x^2 + ... + a_nx^n \quad \text{con } a_n \neq 0 \\ Q = b_0 + b_1x + b_2x^2 + ... + b_mx^m \quad \text{con } b_m \neq 0 \end{array}$$

Luego $PQ = a_0b_0 + (a_0b_1 + a_1b_0)x + ... + (a_nb_m)x^{n+m}$.

Como R es Dominio de Integridad, $a_n \neq 0$ y $b_m \neq 0$, entonces $a_nb_m \neq 0$
lo que nos garantiza que $grad(PQ) = n + m$.

• Si R no es un Dominio de Integridad a_nb_m se podría anular y luego el grado de PQ puede ser menor que $m + n$.

3.2. Automorfismos en anillos de polinomios

Teorema 3.1. Sea R un Dominio de Integridad, ϕ un R-endomorfismo de $R[x]$.

(i) Si ϕ es sobreyectiva entonces $\phi(x) = a + bx$ donde $a, b \in R$ con b invertible en R.

(ii) Si ϕ es sobreyectiva entonces ϕ es inyectiva.

(iii) Si $\phi(x) = a + bx$ donde $a, b \in R$ con b invertible en R entonces ϕ es sobreyectiva.

Prueba.

(i) Probaremos que $grad(\phi(x)) = 1$.

Caso 1: Si $grad(\phi(x)) = 0$ o $grad(\phi(x)) = -\infty$.

Tenemos $\phi(x) = a \in R$ (a es una constante), como ϕ es sobreyectiva entonces existe $t = \sum_{i=0}^{n} t_ix^i \in R[x]$ tal que

$$x = \phi(t) = t_0 + t_1a + t_2a^2 + ... + t_na^n.$$

Luego $grad(x) \leq 0$, lo cual es una contradicción.

Caso 2: Si $grad(\phi(x)) = n \geq 2$.

Como R es un Dominio de Integridad,

$$grad(a_i\phi^i(x)) = in \geq 2, \quad \text{donde } a_i \neq 0, \text{ para todo } i \in \mathbb{N} \tag{3.2.1}$$

Dado $P \in R[x]$ arbitrario.

Si $P = 0$, $grad(P) = -\infty$.
Si $P \neq 0$, existe $m \in \mathbb{N}_0$ tal que $grad(P) = m$.

Luego,

$$\begin{array}{rcccccccccl} P = & a_0 & + & a_1x & + & a_2x^2 & + & ... & + & a_mx^m & \text{con } a_m \neq 0 \\ \phi(P) = & a_0 & + & a_1\phi(x) & + & a_2\phi^2(x) & + & ... & + & a_m\phi^m(x) & \end{array}$$

Por (3.2.1) $grad(\phi(P)) = grad(a_m\phi^m(x)) \neq 1$.

Esto quiere decir que

$$grad(\phi(P)) \neq 1, \quad \text{para cualquier } P \in R[x]. \tag{3.2.2}$$

Ya que ϕ es sobreyectiva, $x = \phi(Q)$, para algún $Q \in R[x]$.

Luego por (3.2.2): $grad(x) = grad(\phi(Q)) \neq 1$, lo cual es una contradicción.

Por lo tanto $grad(\phi(x)) = 1$, es decir, $\phi(x) = a + bx$ donde $a, b \in R$ con $b \neq 0$.

Como $x \in R[x]$ y ϕ es sobreyectiva, existen $t_0, t_1, t_2, ..., t_n \in R$ tal que

$$\begin{aligned} x &= t_0 + t_1\phi(x) + t_2\phi(x)^2 + ... + t_n\phi(x)^n \\ x &= t_0 + t_1(a + bx) + t_2(a + bx)^2 + ... + t_n(a + bx)^n \\ x &= (\text{ términos de grado inferior a } n\ ) + t_n b^n x^n \end{aligned}$$

Luego $t_n b^n = 0$ con $b \neq 0$ y como R es Dominio de Integridad, $t_n = 0$.

De forma análoga se puede deducir que $t_2 = t_3 = ... = t_n = 0$, así tenemos que $x = t_0 + t_1 a + t_1 bx$. Esto implica que $t_1 \in R$ tal que $t_1 b = 1$, es decir que b es invertible en R.

(ii) Afirmación. Para todo $n \in \mathbb{N}$, si $\displaystyle\sum_{i=0}^{n} t_i(a + bx)^i = 0$ donde $t_i, a, b \in R$ con $b \neq 0$, entonces $t_i = 0$.

En efecto, probaremos por Inducción Matemática.

Para $n = 1$:

Sea $t_0 + t_1(a + bx) = 0$, entonces $t_0 + t_1 a = 0$ y $t_1 b = 0$.

Como R es Dominio de Integridad y $b \neq 0$ tenemos $t_1 = 0$.

Por lo tanto $t_0 = t_1 = 0$.

Supongamos que la afirmación se cumple para $n \in \mathbb{N}$ (Hipótesis Inductiva).

Veamos que se cumple para $n + 1$.

Sea $\displaystyle\sum_{i=0}^{n+1} t_i(a + bx)^i = 0$. Luego,

$$\sum_{i=0}^{n} t_i(a + bx)^i \quad + \quad t_{n+1}(a + bx)^{n+1} = 0$$

$$\sum_{i=0}^{n} t_i(a + bx)^i \quad + \quad (\text{términos de grado inferior a } n + 1\,) \quad + \quad t_{n+1} b^{n+1} x^{n+1} = 0.$$

Entonces $t_{n+1} b^{n+1} = 0$ donde $b^{n+1} \neq 0$ y como R es Dominio de Integridad tenemos $t_{n+1} = 0$.

Por otro lado por la hipótesis inductiva tenemos $t_0 = t_1 = ... = t_n = 0$.

Por lo tanto $t_0 = t_1 = ... = t_n = t_{n+1} = 0$ probando así la afirmación.

Ahora, si ϕ es inyectiva basta probar que $Nu(\phi) = \{0\}$.

En efecto, sea $t = \displaystyle\sum_{i=0}^{n} t_i x^i \in Nu(\phi)$, entonces $\phi(t) = \displaystyle\sum_{i=0}^{n} t_i \phi^i(x) = 0$.

Como ϕ es sobreyectiva, de (i) tenemos que $\sum_{i=0}^{n} t_i(a+bx)^i = 0$.

Luego por la afirmación $t_0 = t_1 = ... = t_n = 0$, lo que implica que $t = 0$.

Por lo tanto ϕ es inyectiva.

(iii) De hipótesis tenemos que $\phi(x) = a + bx$ donde $a, b \in R$ con b invertible en R. Como b es invertible podremos despejar x quedando así, $x = \phi(b^{-1}(x-a))$.

Sea $t = \sum_{i=0}^{n} t_i x^i \in R[x]$, entonces

$$t = \sum_{i=0}^{n} t_i \left[\phi\left(b^{-1}(x-a)\right)\right]^i = \phi\left(\sum_{i=0}^{n} t_i \left[b^{-1}(x-a)\right]^i\right).$$

Luego existe $r = \sum_{i=0}^{n} t_i \left[b^{-1}(x-a)\right]^i \in R[x]$ tal que $\phi(r) = t$, esto es, $t \in Im(\phi)$.

Por lo tanto ϕ es sobreyectiva.

□

Corolario 3.1.1. Sea R un $D.I$, ϕ un R-endomorfismo de $R[x]$, entonces ϕ es R-automorfismo de $R[x]$ si y solo si $\phi(x) = a + bx$ donde $a, b \in R$ con b invertible en R.

Prueba. Si ϕ es R-automorfismo de $R[x]$, por el Teorema 3.1-(i) sale de inmediato.

Recíprocamente, si $\phi(x) = a + bx$ donde $a, b \in R$ con b invertible en R.

Por el Teorema 3.1-(iii) tenemos que ϕ es sobreyectiva.

Luego, por el Teorema 3.1-(ii) ϕ es inyectiva.

Por lo tanto ϕ es un R-automorfismo.

□

Lema 3.2. Sea R un a.c.c.i y dados $h_2, h_3, ..., h_v \in R$ arbitrarios, si $\langle h_2, h_3, ..., h_v\rangle^k = 0$, para algún $k \in \mathbb{N}$, entonces $f_{(x+h_2x^2+...+h_vx^v)}$ es sobreyectiva.

Prueba. Consideremos $h = x + h_2x^2 + ... + h_vx^v \in R[x]$

Probaremos por inducción sobre k.

(i) Si $k = 1$.

Tenemos $h_2, h_3, ..., h_v \in \langle h_2, h_3, ..., h_v\rangle = 0$, entonces $h = x$, luego f_h es sobreyectiva, pues $f_h(x) = h$.

(ii) Supongamos que el lema es verdad para $k = n \geq 2$ (Hipótesis Inductiva).

(iii) Veamos si se cumple para $k = n + 1$.

Tenemos que $\langle h_2, h_3, ..., h_v\rangle^{n+1} = 0$.

Para cada $i = 2, 3, ..., v$.

$$h^i = x^i + \sum_{j=i+1}^{n_i} u_{ij} x^j \quad \text{donde} \quad u_{ij} \in \langle h_2, h_3, ..., h_v\rangle.$$

$$h_i h^i = h_i x^i + \sum_{j=i+1}^{n_i} r_{ij} x^j \quad \text{donde} \quad r_{ij} \in \langle h_2, h_3, ..., h_v\rangle^2.$$

Sea $g = f_h(x - h_2x^2 - ... - h_vx^v) = h - h_2h^2 - ... - h_vh^v$

$$g = x - \sum_{j=3}^{n_2} r_{2j}x^j - \sum_{j=4}^{n_3} r_{3j}x^j - ... - \sum_{j=v+1}^{n_v} r_{vj}x^j$$

Luego $g = x + g_2x^2 + ... + g_mx^m$ donde $g_i \in \langle h_2, h_3, ..., h_v\rangle^2$.

Esto implica que $\langle g_2, g_3, ..., g_m\rangle \subset \langle h_2, h_3, ..., h_v\rangle^2$. Por consiguiente

$$\langle g_2, g_3, ..., g_m\rangle^n \subset \langle h_2, h_3, ..., h_v\rangle^{2n} = \langle h_2, h_3, ..., h_v\rangle^{n+1}\langle h_2, h_3, ..., h_v\rangle^{n-1} = 0,$$

así tenemos $\langle g_2, g_3, ..., g_m\rangle^n = 0$.

Aplicando la Hipótesis Inductiva para $k = n$ tenemos que f_g es sobreyectiva.

Esto quiere decir que existen $a_0, a_1, ..., a_\alpha \in R$ tal que

$$x = f_g(a_0 + a_1x + a_2x^2 + ... + a_\alpha x^\alpha) = a_0 + a_1g + a_2g^2 + ... + a_\alpha g^\alpha$$
$$x = a_0 + a_1f_h(w) + a_2f_h(w)^2 + ... + a_\alpha f_h(w)^\alpha \quad \text{donde} \quad w = x - h_2x^2 - ... - h_vx^v$$
$$x = f_h(a_0 + a_1w + a_2w^2 + ... + a_\alpha w^\alpha).$$

Por lo tanto f_h es sobreyectiva.

$\square$

Teorema 3.2. Sea R un a.c.c.i. y $t = \sum_{i=0}^{n} t_ix^i \in R[x]$, entonces f_t es sobreyectiva si y solo si t_1 es una unidad en R y t_i es nilpotente, para todo $i \geq 2$.

Prueba. Si f_t es sobreyectiva, entonces existe $a = \sum_{i=0}^{k} a_ix^i \in R[x]$ tal que $x = f_t(a)$,

$$x = a_0 + a_1t + a_2t^2 + ... + a_kt^k.$$

Sea un ideal primo P de R, arbitrario.

Tenemos que $\overline{R} := \frac{R}{P} = \{\ \overline{r} = r + P\ /\ r \in R\ \}$ es un $D.I$ con identidad.

Ya que

$$\begin{array}{rcl} \pi : R & \longrightarrow & \overline{R} \\ r & \longmapsto & \pi(r) = \overline{r} \end{array}$$

es un homomorfismo, si tomamos la indeterminada $y = \overline{1}y \in \overline{R}[y]$, tenemos por la propiedad universal de anillos de polinomios que existe un único homomorfismo $\varphi : R[x] \longrightarrow \overline{R}[y]$ tal que $\varphi(r) = \overline{r}$ y $\varphi(x) = y$.

Luego

$$\begin{array}{rcl} \varphi : R[x] & \longrightarrow & \overline{R}[y] \\ \displaystyle\sum_{i=0}^{n} r_i x^i & \longmapsto & \displaystyle\sum_{i=0}^{n} \overline{r_i} y^i \end{array}$$

es un homomorfismo.

Así, $\varphi(t) = \overline{t_0} + \overline{t_1}y + \overline{t_2}y^2 + ... + \overline{t_n}y^n$, entonces existe un único $f_{\varphi(t)}$ que es $\overline{R}$-endomorfismo de $\overline{R}[y]$ tal que $f_{\varphi(t)}(y) = \varphi(t)$.

Además,

$$y = \varphi(x) = \overline{a_0} + \overline{a_1}\varphi(t) + \overline{a_2}\varphi(t)^2 + ... + \overline{a_k}\varphi(t)^k = f_{\varphi(t)}\left(\sum_{i=0}^{k} \overline{a_i} y^i\right).$$

Por ende, $f_{\varphi(t)}$ es sobreyectiva.

Como $f_{\varphi(t)}(y) = \overline{t_0} + \overline{t_1}y + \overline{t_2}y^2 + ... + \overline{t_n}y^n$, por el Teorema 3.1-(i) tenemos que $\overline{t_1}$ es una unidad en $\overline{R}$ y $\overline{t_2} = \overline{t_3} = ... = \overline{t_n} = \overline{0} = P$.

Por otro lado tenemos que existe $\overline{r} \in \overline{R}$ tal que $\overline{rt_1} = \overline{1}$.

Entonces $1 - rt_1 \in P$, esto quiere decir que $t_1 \notin P$, pues si $t_1 \in P$, $1 = rt_1 + (1 - rt_1) \in P$, por consiguiente $P = R$ lo cual es una contradicción.

Así t_1 es una unidad en R (Observación 1.11-(ii)).

Por otro lado, tenemos $t_2, t_3, ..., t_n \in P$, para cualquier P ideal primo en R.

Luego $t_2, t_3, ..., t_n \in \bigcap\limits_{P \subset R \text{ ideal primo}} P = Rad(R)$, debido a la Proposición 1.22-(ii).

Por lo tanto $t_2, t_3, ..., t_n$ son nilpotentes.

Recíprocamente, sea $t = t_0 + t_1x + t_2x^2 + ... + t_nx^n \in R[x]$ con t_1 unidad de R y $t_2, t_3, ..., t_n$ nilpotentes.

Consideremos $h = (t - t_0)t_1^{-1} = x + h_2x^2 + ... + h_nx^n$ donde $h_i = t_1^{-1}t_i$ es nilpotente, para todo $i = 2, 3, ..., n$.

Luego $\langle h_2, h_3, ..., h_n \rangle$ es un ideal nilpotente debido a la Proposición 1.23, es decir que existe $k \in \mathbb{N}$ tal que $\langle h_2, h_3, ..., h_n \rangle^k = 0$.

Del lema 3.2, tenemos que $f_h = f_{(t-t_0)t_1^{-1}}$ es sobreyectiva.

Por lo tanto del lema 3.1, f_t es sobreyectiva.

$\square$

Teorema 3.3. Sea R un a.c.c.i. y $t = \sum_{i=0}^{n} t_i x^i \in R[x]$.

(i) Si f_t es sobreyectiva entonces f_t es inyectiva.

(ii) Si f_t es automorfismo si y solo si t_1 es una unidad en R y t_i es nilpotente, para todo $i \geq 2$.

Prueba.

(i) Si f_t es sobreyectiva entonces por el Teorema 3.2, t_1 es una unidad en R.
Luego $f_h(x) = x + h_2x^2 + ... + h_nx^n$ donde $h = (t - t_0)t_1^{-1}$ y $h_i = t_1^{-1}t_i$.

Afirmación: $Nu(f_h) = \{0\}$.

En efecto, sea $v = \sum_{i=0}^{m} v_i x^i \in Nu(f_h)$, entonces

$$f_h(v) = v_0 + v_1h + ... + v_mh^m = 0.$$

$$v_0 + v_1(x + h_2x^2 + ... + h_nx^n) + ... + v_m(x + h_2x^2 + ... + h_nx^n)^m = 0$$

$$v_0 + v_1x + \text{ términos de grado superior} = 0. \text{ Así, } v_0 = v_1 = 0.$$

Luego nos queda

$$v_2(x + h_2x^2 + ... + h_nx^n)^2 + ... + v_m(x + h_2x^2 + ... + h_nx^n)^m = 0$$

$$v_2x^2 + \text{ términos de grado superior} = 0. \text{ Así, } v_0 = v_1 = v_2 = 0.$$

Quedando así

$$v_3(x + h_2x^2 + ... + h_nx^n)^3 + ... + v_m(x + h_2x^2 + ... + h_nx^n)^m = 0$$

De forma iterativa obtenemos $v_0 = v_1 = v_2 = ... = v_m = 0$, es decir, $v = 0$, probando así la afirmación.

De esta afirmación $f_h = f_{(t-t_0)t_1^{-1}}$ es inyectiva.

Por lo tanto del lema 3.1, f_t es inyectiva.

(ii) Si f_t es automorfismo, f_t es sobreyectiva y por el Teorema 3.2 t_1 es una unidad en R y t_i es nilpotente, para todo $i \geq 2$.

Recíprocamente, si t_1 es una unidad en R y t_i es nilpotente, para todo $i \geq 2$, por el Teorema 3.2, f_t es sobreyectiva y por la parte **(i)**, f_t es inyectiva.

Por lo tanto f_t es automorfismo.

$\square$

Observación 3.4. Si h es un R-automorfismo de $R[x]$ entonces existe un $t \in R[x]$ tal que $h = f_t$.

En efecto, ya que h^{-1} es sobreyectiva entonces $x = h^{-1}(t)$, para algún $t \in R[x]$, así $h(x) = t = f_t(x)$.

Luego para cualquier $w = \sum_{i=0}^{n} w_i x^i \in R[x]$, $h(w) = \sum_{i=0}^{n} w_i t^i = f_t(w)$.

Por lo tanto $h = f_t$.

Teorema 3.4. Sean R, S anillos conmutativos con identidad, $\phi : R[x] \longrightarrow S[x]$ un homomorfismo tal que $\phi_{|_R} : R \longrightarrow S$ es isomorfismo entonces existe únicamente un $\psi : R[x] \longrightarrow S[x]$ isomorfismo tal que para todo $r \in R$, $\psi(r) = \phi(r)$ y $\psi(x) = x$.

Prueba. Denotaremos $\mathcal{C} = \phi_{|_R}$. Por hipótesis $\mathcal{C} : R \longrightarrow S$ es un isomorfismo definido por $\mathcal{C}(r) = \phi(r)$, para todo $r \in R$.

Además existe un isomorfismo $\mathcal{C}^{-1} : S \longrightarrow R$.

Tenemos $\phi : R[x] \longrightarrow S[x]$ homomorfismo, entonces $\mathcal{C} : R \longrightarrow S[x]$ es homomorfismo.

Como $x \in S[x]$, por la Propiedad Universal de Anillos de Polinomios tenemos que:

Existe un único $\psi : R[x] \longrightarrow S[x]$ homomorfismo tal que para todo $r \in R$,

$$\psi(r) = \mathcal{C}(r) \quad \text{y} \quad \psi(x) = x. \tag{3.2.3}$$

Por otro lado como $\mathcal{C}^{-1} : S \longrightarrow R$ es isomorfismo, entonces $\mathbf{C} : S \longrightarrow R[x]$ es homomorfismo definido por $\mathbf{C}(b) = \mathcal{C}^{-1}(b)$, para todo $b \in S$.

Una vez más como $x \in S[x]$, por la Propiedad Universal de Anillos de Polinomios tenemos que:

Existe un único $\rho : S[x] \longrightarrow R[x]$ homomorfismo tal que para todo $b \in S$, $\rho(b) = \mathbf{C}(b) = \mathcal{C}^{-1}(b)$ y $\rho(x) = x$.

Luego, afirmamos que:

$$\rho\, o\, \psi = Id_{R[x]} \quad \text{y} \quad \psi\, o\, \rho = Id_{S[x]} \tag{3.2.4}$$

En efecto, dado $P = \sum_{i=0}^{n} a_i x^i \in R[x]$.

$$\rho(\psi(P)) = \rho\left(\sum_{i=0}^{n} \psi(a_i)\psi^i(x)\right) = \rho\left(\sum_{i=0}^{n} \mathcal{C}(a_i)x^i\right) = \sum_{i=0}^{n} \rho(\mathcal{C}(a_i))\rho^i(x)$$

$$\rho(\psi(P)) = \sum_{i=0}^{n} \mathcal{C}^{-1}(\mathcal{C}(a_i))x^i = \sum_{i=0}^{n} a_i x^i = P.$$

Es decir, $(\rho\, o\, \psi)(P) = P \in R[x]$.

De forma análoga obtenemos $(\psi\, o\, \rho)(Q) = Q \in S[x]$, probando así la afirmación.

Por lo tanto de (3.2.3) y (3.2.4):

Existe únicamente un $\psi : R[x] \longrightarrow S[x]$ isomorfismo tal que para todo $r \in R$, $\psi(r) = \phi(r)$ y $\psi(x) = x$.

$\square$

Teorema 3.5. Sean R, S anillos conmutativos con identidad, $\phi : R[x] \longrightarrow S[x]$ un homomorfismo tal que $\phi_{|_R} : R \longrightarrow S$ es isomorfismo entonces existe un único S-endomorfismo ϕ' de $S[x]$ tal que

$$\begin{tikzcd} R[x] \arrow[r, "\phi"] \arrow[d, "\psi"'] & S[x] \\ S[x] \arrow[ur, "\phi'"'] & \end{tikzcd}$$

Es un diagrama conmutativo (es decir, $\phi = \phi' \, o \, \psi$). Además, ϕ es sobreyectivo (inyectivo) si y solo si ϕ' es sobreyectivo (inyectivo).

Prueba. De la hipótesis y por el teorema 3.4 tenemos que:

Existe un único isomorfismo $\psi : R[x] \longrightarrow S[x]$ tal que para todo $r \in R$,

$$\psi(r) = \phi(r) \quad \text{y} \quad \psi(x) = x. \tag{3.2.5}$$

Además, existe un único isomorfismo $\psi^{-1} : S[x] \longrightarrow R[x]$.

Luego existe un homomorfismo $\phi^{'} = \phi \; o \; \psi^{-1} : S[x] \longrightarrow S[x]$, es decir,

$$\phi^{'} \text{ es un endomorfismo de } S[x]. \tag{3.2.6}$$

La unicidad de $\phi^{'}$ se debe a la unicidad de ψ^{-1}.

Ahora, probaremos que

$$\phi'(b) = b, \text{ para todo } b \in S. \tag{3.2.7}$$

En efecto, sea $b \in S$, como $\phi_{|_R} : R \longrightarrow S$ es isomorfismo entonces existe $r \in R$ tal que $\phi(r) = b$.

Luego de (3.2.5): $\psi(r) = b$, $r = \psi^{-1}(b) \in R$, $\psi(\psi^{-1}(b)) = \phi(\psi^{-1}(b))$.
Entonces $b = (\phi \; o \; \psi^{-1})(b)$, $\phi'(b) = b$.

Luego de (3.2.6) y (3.2.7) ϕ' es un R-endomorfismo de $S[x]$.

También como $\phi' = \phi \; o \; \psi^{-1}$, entonces $\phi = \phi' \; o \; \psi$, es decir, el diagrama es conmutativo.

Además como ψ es biyectiva se prueba inmediatamente que:
$\phi = \phi' \; o \; \psi$ es sobreyectiva (inyectiva) si y solo si $\phi' = \phi \; o \; \psi^{-1}$ es sobreyectiva (inyectiva).

$\square$

Teorema 3.6. Sean R, S anillos conmutativos con identidad, $t = \sum_{i=0}^{n} t_i x^i \in S[x]$ y $\phi : R[x] \longrightarrow S[x]$ un homomorfismo tal que $\phi_{|_R} : R \longrightarrow S$ es isomorfismo y $\phi(x) = t$, entonces se cumple:

(i) ϕ es sobreyectiva si y solo si t_1 es una unidad de S y t_i es nilpotente, para todo $i \geq 2$.

(ii) Si ϕ es sobreyectiva entonces ϕ es inyectiva.

Prueba. Debido a que $t \in S[x]$, por la observación 3.1, existe un único φ_t S-endomorfismo de $S[x]$ tal que $\varphi_t(x) = t$.

Por otro lado, por el teorema 3.5 tenemos que existe un único ϕ' S-endomorfismo de $S[x]$ tal que $\phi = \phi' \, o \, \psi$, donde $\psi : R[x] \longrightarrow S[x]$ es isomorfismo con $\psi(x) = x$, o también $\psi^{-1}(x) = x$.

Afirmación: $\varphi_t = \phi'$.

Sea $r \in S$ entonces

$\phi'(r) = r = \varphi_t(r)$ y $\phi'(x) = \phi(\psi^{-1}(x)) = \phi(x) = t = \varphi_t(x)$.

Luego, sea $P = \sum_{i=0}^{n} b_i x^i \in S[x]$, $\phi'(P) = \sum_{i=0}^{n} b_i t^i = \sum_{i=0}^{n} \varphi_t(b_i)\varphi_t^i(x) = \varphi_t(P)$.

Demostramos así la afirmación.

Luego por los teoremas 3.2, 3.3 y 3.5, tenemos:

(i) ϕ es sobreyectiva si y solo si $\phi' = \varphi_t$ es sobreyectiva si y solo si t_1 es una unidad de S y t_i es nilpotente, para todo $i \geq 2$.

(ii) ϕ es sobreyectiva si y solo si $\phi' = \varphi_t$ es sobreyectiva, entonces $\phi' = \varphi_t$ es inyectiva, luego ϕ es inyectiva.

$\square$

3.3. Anillo de series de potencias formales con coeficientes en un anillo

3.3.1. Nociones topológicas para series formales

Sea R un a.c.c.i, suponiendo que podemos aplicar de manera análoga para $R[[x]]$ la Propiedad Universal del anillo de polinomios y obtener que los automorfismos ϕ sean de la forma f_t tal que $\phi(x) = \mathcal{T}$.

Nos preguntamos si es posible caracterizar dichos automorfismos ϕ, donde se exija al coeficiente de x en $\mathcal{T}$, que sea una unidad de R (como en $R[x]$).

Suponiendo que existe un ψ R-endomorfismo de $R[[x]]$ tal que $\psi(x) = b + x$, para algún $b \in R$.

Esperamos que ψ sea un automorfismo de $R[[x]]$.

Dado $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$,

$$\psi(f) = \psi\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} a_i (b+x)^i = (a_0 + a_1 b + a_2 b^2 + ...) + x(a_1 + 2a_2 b + 3a_3 b^2 + ...)$$
$$+x^2(a_2 + 3a_3 b + 6a_4 b^2 + ...) + ... = \sum_{i=0}^{\infty} r_i x^i, \text{ con } r_i \in R[[b]]$$

Para que los r_i sean elementos en R tendremos que agregar la introducción de alguna topología en R o en $R[[b]]$.

Las nociones topológicas en estos anillos son necesarias para trabajar con los R-endomorfismos en anillos de series formales.

Analizaremos lo necesario sobre las estructuras topológicas en $R, R[[x]], R[[x_1, x_2, ..., x_n]]$ que se elegirán en cada ocasión respectiva.

Definición 3.2 (**Grupos topológicos**). Sea $G = (G, +)$ un grupo abeliano con alguna topología. Diremos que G es un grupo topológico (con respecto a su topología dada) si

$$\begin{array}{rccc} g: & G \times G & \longrightarrow & G \\ & (x,y) & \longmapsto & x+y \end{array} \qquad \text{y} \qquad \begin{array}{rccc} h: & G & \longrightarrow & G \\ & x & \longmapsto & -x \end{array}$$

son aplicaciones continuas (donde a $G \times G$ se le da la topología producto).

Definición 3.3 (**Anillos topológicos**). Sea $R = (R, +, .)$ un anillo con alguna topología. Diremos que R es un anillo topológico si

$$\begin{array}{rccc} g: & R \times R & \longrightarrow & R \\ & (x,y) & \longmapsto & x-y \end{array} \qquad \text{y} \qquad \begin{array}{rccc} h: & R \times R & \longrightarrow & R \\ & (x,y) & \longmapsto & xy \end{array}$$

son aplicaciones continuas.

Proposición 3.2. Sea G un grupo topológico, $a \in G$, entonces la aplicación traslación

$$\begin{array}{rccc} T_a: & G & \longrightarrow & G \\ & x & \longmapsto & a+x \end{array}$$

es un homeomorfismo.

Prueba.

(i) La aplicación traslación T_{-a} es la aplicación inversa de T_a.

Sea $x \in G$, $(T_a \, o \, T_{-a})(x) = T_a(-a+x) = a - a + x = x$ y de forma análoga se verifica que $(T_{-a} \, o \, T_a)(x) = x$.

Así concluimos que T_a es biyectiva.

(ii) Como G es un grupo topológico, entonces la aplicación

$$\begin{array}{rccc} g: & G \times G & \longrightarrow & G \\ & (x,y) & \longmapsto & x+y \end{array}$$

es continua.

Se sabe del Teorema 1.3-(vi) que la aplicación

$$\begin{array}{rccc} I_a: & G & \longrightarrow & G \times G \\ & x & \longmapsto & I_a(x) = (a,x) \end{array}$$

es continua. Así mismo por el Teorema 1.3-(iv) concluimos que $T_a = g \, o \, I_a$ es continua.

De forma análoga la función inversa $T_{-a} = g \, o \, I_{-a}$ es continua.

Por lo tanto T_a es un homeomorfismo.

$\square$

Nota:

(i) $(T_a)^{-1} = T_{-a}$.

(ii) Sea V un subconjunto de G, entonces $T_a(V) = a + V = V + a$.

(iii) Como T_a es homeomorfismo, si $B \in \tau$, por la continuidad de T_a, $T_a(B) = B + a \in \tau$.

Proposición 3.3. Sea G un grupo topológico, $x \in G$, entonces $V \in \mathcal{N}_{(x)}$ si y solo si existe $U \in \mathcal{N}_{(0)}$ tal que $V = U + x$.

Prueba. Si $V \in \mathcal{N}_{(x)}$, entonces $V \in \mathcal{N}_{(x)}$ y $V \in \tau$.

Luego $x \in V$, $0 = T_{-x}(x) \in T_{-x}(V) \in \tau$, $0 \in (V - x) \in \tau$.

Esto es $U = (V - x) \in \mathcal{N}_{(0)}$, así $V = U + x$, donde $U \in \mathcal{N}_{(0)}$.

Recíprocamente, sea $V = U + x$, donde $U \in \mathcal{N}_{(0)}$, entonces $0 \in (V - x) \in \tau$,

$x = T_x(0) \in T_x(V - x) \in \tau$. Luego $x \in (V - x) + x = V \in \tau$.

Por lo tanto $V \in \mathcal{N}_{(x)}$.

$\square$

Proposición 3.4. Sea G un grupo topológico, entonces el conjunto

$$B = \{ \ \delta + a \ / \ a \in G, \ \delta \in \mathcal{N}_{(0)} \ \}$$

es base para la topología más pequeña sobre G que contiene a B.

Prueba.

(i) Como G es un abierto, entonces para cualquier $x \in G$, $G \in \mathcal{N}_{(x)}$.

Luego usando la Proposición 3.3 tenemos que si $x \in G$, entonces existe un $\delta_x \in \mathcal{N}_{(0)}$ tal que $G = \delta_x + x$, es decir, existe $B_x = \delta_x + x \in B$ tal que $x \in B_x = G$.

Por lo tanto $G = \bigcup_{x \in G} B_x$.

(ii) Sean $V_1 = \delta_1 + a_1 \in B$, $V_2 = \delta_2 + a_2 \in B$ y $x \in V_1 \cap V_2$.

Como V_1 y V_2 son abiertos entonces $V_1 \cap V_2$ es abierto.

Ya que $x \in V_1 \cap V_2$, $V_1 \cap V_2 \in \mathcal{N}_{(x)}$, luego $V_1 \cap V_2 = \delta + x$, donde $\delta \in \mathcal{N}_{(0)}$.

Por lo tanto $V_1 \cap V_2 \in B$ tal que $x \in V_1 \cap V_2$.

- Como observamos, B cumple las condiciones (i) y (ii) del teorema 1.2 lo que quiere decir que B es una base de una topología sobre G. Esta topología es la generada por la base B (denotada por $\tau(B)$) que la determinan únicamente los entornos de 0 en G, siendo además la topología más pequeña de todas la topologías que contienen a B.

$\square$

Proposición 3.5. Sea G un grupo topológico con sus operaciones

$$\begin{array}{rccc} g: & G \times G & \longrightarrow & G \\ & (x,y) & \longmapsto & x+y \end{array} \qquad \text{y} \qquad \begin{array}{rccc} h: & G & \longrightarrow & G \\ & x & \longmapsto & -x \end{array}$$

Si $U \in \mathcal{N}_{(0)}$ entonces existe $V \in \mathcal{N}_{(0)}$ tal que $V = h(V)$ y $g(V \times V) \subset U$.

Prueba. De la hipótesis tenemos que U es un abierto tal que $0 \in U$.

Por la continuidad de g, $g^{-1}(U) = \{ \ (x,y) \in G \times G \ / \ x+y \in U \ \}$ es un abierto y además $(0,0) \in g^{-1}(U)$.

Como $g^{-1}(U)$ es un entorno de $(0,0)$, en la topología producto existen abiertos V_1 y V_2 tales que $(0,0) \in V_1 \times V_2 \subset g^{-1}(U)$.

Entonces $0 = h(0) \in h(V_i)$, es decir que $h(V_i)$ es un entorno abierto de 0, para cada $i = 1, 2$. Además, $g(V_1 \times V_2) \subset U$.

Ahora si tomamos el conjunto $V = V_1 \cap V_2 \cap h(V_1) \cap h(V_2)$, V es un abierto y también se cumple:

$0 \in V$ y $h(V) = V$. Como $V \subset V_i$ $(i = 1, 2)$ entonces

$$g(V \times V) \subset g(V_1 \times V_2) \subset U \quad .$$

Por lo tanto $V \in \mathcal{N}_{(0)}$ tal que $V = h(V)$ y $g(V \times V) \subset U$.

$\square$

Observación 3.5.

(i) Todo anillo topológico es un grupo topológico.

(ii) No todo grupo topológico es un espacio de Hausdorff.

(iii) Un grupo G con mas de un elemento, dotado con la topología indiscreta es un grupo topológico que no es de Hausdorff.

El lema siguiente aclara esta Observación.

Lema 3.3. Sea G un grupo topológico y H la intersección de todos los entornos de 0 en G, entonces:

(i) H es subgrupo de G.

(ii) H es la clausura de $\{0\}$.

(iii) G es de Hausdorff si y solo si $H = \{0\}$.

Prueba.

(i) Evidentemente $0 \in H$, entonces $H \neq \emptyset$.

Sea $x, y \in H$. Dado $V \in \mathcal{N}_{(0)}$, entonces por la Propiedad 3.5 existe $W \in \mathcal{N}_{(0)}$ tal que $g(W \times h(W)) \subset V$.

Como W es un entorno de 0, entonces $x, y \in W$.

Luego $x - y = g(x, h(y)) \in g(W \times h(W)) \subset V$.

Así tenemos que para todo $V \in \mathcal{N}_{(0)}$, $x - y \in V$, esto quiere decir que $x - y \in H$.

Por lo tanto H es subgrupo de G.

(ii) Sea $x \in \overline{\{0\}}$, entonces

$$0 \in V, \quad \text{para todo} \quad V \in \mathcal{N}_{(x)} \tag{3.3.1}$$

Dado $U \in \mathcal{N}_{(0)}$, $U + x \in \mathcal{N}_{(x)}$. De (3.3.1) tenemos $0 \in U + x$, $-x \in U$.

Luego $-x \in H$, como H es un subgrupo de G, entonces $x \in H$. Así $\overline{\{0\}} \subset H$.

Sea $x \in H$, entonces $-x \in H$, esto quiere decir que:

$$\text{Para todo } U \in \mathcal{N}_{(0)}, \ -x \in U \ \ (\ 0 \in U + x \ ). \tag{3.3.2}$$

Dado $V \in \mathcal{N}_{(x)}$. entonces existe $U_0 \in \mathcal{N}_{(0)}$ tal que $V = U_0 + x$.

Luego por (3.3.2), $0 \in U_0 + x = V$, así para todo $V \in \mathcal{N}_{(x)}$, $0 \in V$, entonces $x \in \overline{\{0\}}$, y concluimos que $H \subset \overline{\{0\}}$.

Por lo tanto $H = \overline{\{0\}}$.

(iii) Sea G un espacio de Hausdorff y si $x \in \overline{\{0\}}$, entonces:

$$\text{Para todo } V \in \mathcal{N}_{(x)},\ 0 \in V \tag{3.3.3}$$

Supongamos que $x \neq 0$. Como G es Hausdorff, entonces existen los entornos $V \in \mathcal{N}_{(x)}$ y $U \in \mathcal{N}_{(0)}$ tal que $U \cap V = \emptyset$.

Luego de (3.3.3), $0 \in U \cap V$, lo cual es una contradicción, pues U y V son disjuntos. Esto quiere decir que $x = 0$.

Por lo tanto $H = \overline{\{0\}} = \{0\}$.

Recíprocamente, sean $x, y \in G$ donde $x \neq y$. Tenemos, $x - y \notin \{0\} = H$, entonces:

$$\text{Existe } U \in \mathcal{N}_{(0)} \text{ tal que } x - y \notin U. \tag{3.3.4}$$

Como $U \in \mathcal{N}_{(0)}$, por la Proposición 3.5, existe $W \in \mathcal{N}_{(0)}$ tal que $g(W \times h(W)) \subset U$.

Luego $W + x \in \mathcal{N}_{(x)}$, $W + y \in \mathcal{N}_{(y)}$.

Afirmación: $(W + x) \cap (W + y) = \emptyset$.

Supongamos que existe un $w \in (W + x) \cap (W + y)$.

Entonces $w = w_1 + x = w_2 + y$, donde $w_1, w_2 \in W$.

$x - y = w_2 - w_1 = g(w_2, h(w_1)) \in g(W \times h(W)) \subset U$.

Luego $x - y \in U$, lo cual contradice (3.3.4), probando así la afirmación.

Así concluimos que para cada $x \neq y$, existen los entornos
$V_1 = W + x \in \mathcal{N}_{(x)}$ y $V_2 = W + y \in \mathcal{N}_{(y)}$ tales que $V_1 \cap V_2 = \emptyset$.

Por lo tanto G es un espacio de Hausdorff.

□

Proposición 3.6. Sea R un a.c.c.i, $\mathcal{M}$ un ideal de R, entonces el conjunto $B = \{\, \mathcal{M}^n + a \ / \ a \in R, n \in \mathbb{N}_0 \,\}$ forma una base de alguna topología de R.

Prueba. Veamos que B forma una base de alguna topología:

(i) Sea $x \in R$, entonces $\mathcal{M}^{n_0} + x \in B$, para algún $n_0 \in \mathbb{N}_0$.

Como $0 \in \mathcal{M}^{n_0}$, $x \in \mathcal{M}^{n_0} + x$.

Luego existe $V = \mathcal{M}^{n_0} + x \in B$ tal que $x \in V$, es decir, $x \in \bigcup_{V \in B} V$.

Por lo tanto $R = \bigcup_{V \in B} V$.

(ii) Sean $\mathcal{M}^n + a \in B$, $\mathcal{M}^m + b \in B$ y $x \in (\mathcal{M}^n + a) \cap (\mathcal{M}^m + b)$.

Sin pérdida de generalidad, supongamos $m \leq n$, entonces $\mathcal{M}^n \subset \mathcal{M}^m$, $\mathcal{M}^n + a \subset \mathcal{M}^m + a$.

Por otro lado, $x = y_1 + a = y_2 + b$, donde $y_1 \in \mathcal{M}^n$, $y_2 \in \mathcal{M}^m$.

Por consiguiente, $a - b = y_2 - y_1 \in \mathcal{M}^m$.

Luego $\mathcal{M}^m = \mathcal{M}^m + (a - b)$, $\mathcal{M}^m + a = \mathcal{M}^m + b$, $\mathcal{M}^n + a \subset \mathcal{M}^m + a = \mathcal{M}^m + b$.

Por lo tanto $x \in (\mathcal{M}^n + a) \cap (\mathcal{M}^m + b) = \mathcal{M}^n + a \in B$.

Del Teorema 1.2 se sabe que, efectivamente B es una base alguna topología $\tau(B)$ sobre R. □

- Recordemos que $\{\mathcal{M}^n\}_{n\in\mathbb{N}_0}$ forma una filtración $\mathcal{M}$-ádica (ver el Ejemplo 1.2)
- Esta topología que tiene a B como base (la topología $\tau(B)$) se denomina topología $\mathcal{M}$-ádica o $\mathcal{M}$-Topología.
- Denotaremos $(R, \mathcal{M})$ para indicar que estamos considerando a R un anillo topológico con su topología $\mathcal{M}$-ádica en R.

Proposición 3.7. Sea R un a.c.c.i. con su ideal $\mathcal{M}$ y $B=\{\ \mathcal{M}^n + a\ /\ a \in R,\ n \in \mathbb{N}_0\ \}$, entonces R con su topología $\mathcal{M}$-ádica es un anillo topológico.

Prueba.

(i) Sea la aplicación:

$$\begin{array}{rccl} g: & R\times R & \longrightarrow & R \\ & (x,y) & \longmapsto & g(x,y) = x - y \end{array}$$

Dado $(a,b) \in R\times R$ arbitrario y V un entorno básico (arbitrario) de $g(a,b) = a - b$.

Entonces $V = \mathcal{M}^n + (a-b)$, para algún $n \in \mathbb{N}_0$.

Tomamos el conjunto $U = (\mathcal{M}^n + a) \times (\mathcal{M}^n + b)$.

Luego U es un abierto en $R\times R$ y $(a,b) \in U$, en consecuencia $U \in \mathcal{N}_{(,)}$.

Sea $z \in g(U)$, entonces existe un $(x_0, y_0) \in U$ tal que $z = g(x_0, y_0)$.

Por consiguiente $x_0 \in \mathcal{M}^n + a$, $y_0 \in \mathcal{M}^n + b$ tal que $z = x_0 - y_0$.

Tenemos $x_0 = m_1 + a$, $y_0 = m_2 + b$, con $m_1, m_2 \in \mathcal{M}^n$,
$z = x_0 - y_0 = (m_1 - m_2) + (a - b)$ con $m_1 - m_2 \in \mathcal{M}^n$.

Por ende $z \in \mathcal{M}^n + (a-b) = V$.

Luego existe $U \in \mathcal{N}_{(a,b)}$ tal que $g(U) \subset V$.

Así, por la Observación 1.3-(ii) concluimos que g es continua.

(ii) Sea la aplicación

$$\begin{array}{rccl} h: & R\times R & \longrightarrow & R \\ & (x,y) & \longmapsto & h(x,y) = xy \end{array}$$

Dado $(a,b) \in R\times R$ arbitrario y W un entorno básico de $h(a,b) = ab$.

Entonces $W = \mathcal{M}^n + ab$, para algún $n \in \mathbb{N}_0$.

Tomamos el conjunto $U' = (\mathcal{M}^n + a) \times (\mathcal{M}^n + b)$. Como en (i), $U' \in \mathcal{N}_{(a,b)}$.

Sea $z \in h(U')$, entonces existe un $x_0, y_0 \in U'$ tal que $z = h(x_0, y_0)$.

Por consiguiente $x_0 \in \mathcal{M}^n + a$, $y_0 \in \mathcal{M}^n + b$ tal que $z = x_0 y_0$.

Tenemos $x_0 = m_1 + a$, $y_0 = m_2 + b$, con $m_1, m_2 \in \mathcal{M}^n$,

$z = x_0\, y_0 = m_1 m_2 + m_1 b + a m_2 + ab$ donde $m_1 m_2, m_1 b, a m_2 \in \mathcal{M}^n$.

Por ende $z \in \mathcal{M}^n + ab = W$.

Luego existe $U' \in \mathcal{N}_{(a,b)}$ tal que $h(U') \subset W$.

Así, por la Observación 1.3-(ii) concluimos que h es continua.

Por lo tanto, R con su topología $\mathcal{M}$-ádica es un anillo topológico.

□

• Nos proponemos a encontrar una condición necesaria y suficiente para que $(R, \mathcal{M})$ sea un espacio métrico.

Definición 3.4. Sea R el anillo topológico con su topología $\mathcal{M}$-ádica.
Definimos la aplicación

$$\begin{array}{rccc} v: & R & \longrightarrow & \mathbb{N}_0 \cup \{\infty\} \\ & x & \longmapsto & v(x) \end{array}$$

donde:

$$v(x) = \begin{cases} \infty & , \text{si} \quad x \in \bigcap\limits_{n \in \mathbb{N}_0} \mathcal{M}^n \quad (\mathcal{M}^0 := R) \\ \\ Sup\{n \in \mathbb{N}_0 \,/ x \in \mathcal{M}^n\} & , \text{si} \quad x \notin \bigcap\limits_{n \in \mathbb{N}_0} \mathcal{M}^n \end{cases}$$

La aplicación v es llamada “ **Aplicación de orden en el anillo** R ”.

Nota: Ya que $\mathcal{M}^0 := R$, entonces $\bigcap\limits_{n \in \mathbb{N}_0} \mathcal{M}^n = \bigcap\limits_{n \in \mathbb{N}} \mathcal{M}^n$.

Proposición 3.8. Sea R el anillo topológico con su topología $\mathcal{M}$-ádica y H la intersección de todos los entornos de 0 en R, entonces $H = \bigcap\limits_{n \in \mathbb{N}} \mathcal{M}^n$.

Prueba. Sea $x \in H$, entonces tenemos:

$$\text{Para todo } U \in \mathcal{N}_{(0)},\ x \in U. \tag{3.3.5}$$

Si $n \in \mathbb{N}$, entonces $0 \in \mathcal{M}^n$ y además $\mathcal{M}^n$ pertenece a la base de la topología $\mathcal{M}$-ádica sobre R, así $\mathcal{M}^n \in \mathcal{N}_{(0)}$. Luego de 3.3.5, $x \in \mathcal{M}^n$, es decir, $x \in \bigcap\limits_{n \in \mathbb{N}} \mathcal{M}^n$.

Recíprocamente, sea $x \in \bigcap\limits_{n \in \mathbb{N}} \mathcal{M}^n$, entonces:

$$\text{Para todo } n \in \mathbb{N},\ x \in \mathcal{M}^n. \tag{3.3.6}$$

Dado $U \in \mathcal{N}_{(0)}$, entonces $0 \in U$, donde U esta en la topología $\mathcal{M}$-ádica sobre R, es decir, $0 \in U = \bigcup_{i \in I} U_i$, con $U_i = \mathcal{M}^{n_i} + a_i$. Luego $-a_i \in \mathcal{M}^{n_i}$, para algún $i \in I$.

Como $n_i \in \mathbb{N}$, de 3.3.6 tenemos que $x \in \mathcal{M}^{n_i}$, así $x - a_i \in \mathcal{M}^{n_i}$, $x \in \mathcal{M}^{n_i} + a_i = U_i$, para algún $i \in I$, esto es, $x \in \bigcup_{i \in I} U_i = U$. Luego x esta cualquier U entorno de $0 \in R$.

Por lo tanto $x \in H$.

$\square$

Observación 3.6.

- Si $v(x) = \infty$ entonces $x \in \bigcap_{n \in \mathbb{N}} \mathcal{M}^n$ y por el lema 3.3, $x \in \overline{\{0\}}$.
- Si $v(x)$ es finito, esto es, $v(x) = Sup\{\, n \in \mathbb{N}_0 \,/\, x \in \mathcal{M}^n \,\} = n'$, entonces $x \in \mathcal{M}^{n'}$ y como $n' < n' + 1$ tenemos que $x \notin \mathcal{M}^{n'+1}$.

Lema 3.4. Dado $(R, \mathcal{M})$, sean $x, y \in R$, entonces:

(i) $v(x + y) \geq min\{v(x), v(y)\}$.

(ii) $v(xy) \geq v(x) + v(y)$.

Prueba.

Caso 1: $v(x) = v(y) = \infty$.

Tenemos $x, y \in \bigcap_{n \in \mathbb{N}} \mathcal{M}^n$ luego $x + y,\, xy \in \bigcap_{n \in \mathbb{N}} \mathcal{M}^n$.

Por lo tanto $v(x + y) = v(xy) = \infty$.

Caso 2: $v(x) = \infty$, $v(y) = j \in \mathbb{N}_0$.

$x \in \bigcap_{n \in \mathbb{N}} \mathcal{M}^n$, $y \in \mathcal{M}^j$ para algún $j \in \mathbb{N}_0$. Tenemos $x + y \in \mathcal{M}^j$, $xy \in \bigcap_{n \in \mathbb{N}} \mathcal{M}^n$.

Luego $v(x + y) \geq j$ y $v(xy) = \infty$.

Caso 3: $v(x) = n \geq j = v(y)$, donde $n, j \in \mathbb{N}_0$.

Tenemos $x \in \mathcal{M}^n$, $y \in \mathcal{M}^j$. Luego $x + y \in \mathcal{M}^j$, $xy \in \mathcal{M}^{n+j}$.

Por lo tanto $v(x + y) \geq j = min\{n, j\}$ y $v(xy) \geq n + j$.

$\square$

Observación 3.7.

(i) El anillo de los polinomios $R[x]$, donde R es un anillo conmutativo con identidad con su ideal $\langle x\rangle = xR[x]$ es un anillo topológico, es decir, $(R[x], \langle x\rangle)$ es un anillo topológico con su topología $\langle x\rangle$-ádica.

(ii) El anillo de series formales $R[[x]]$, donde R es un anillo conmutativo con identidad con su ideal $\langle x\rangle = xR[[x]]$ es también un anillo topológico, es decir, $(R[[x]], \langle x\rangle)$ es anillo topológico con su topología $\langle x\rangle$-ádica.

(iii) En los anillos topológicos $R[x]$ y $R[[x]]$ los entornos básicos de 0 de sus topologías $\langle x\rangle$-ádicas son los ideales

$$\langle x\rangle^n = x^n R[x] = \{x^n f \ / \ f \in R[x]\} = \left\{ \sum_{i=n}^{m} f_i x^i \in R[x] \ / \ m \in \mathbb{N} \right\}, \ \text{y}$$

$$\langle x\rangle^n = x^n R[[x]] = \{x^n f \ / \ f \in R[[x]]\} = \left\{ \sum_{i=0}^{\infty} f_i x^i \in R[[x]] \ / \ f_0 = f_1 = ... = f_{n-1} = 0 \right\}$$

respectivamente.

Proposición 3.9. $(R[[x]], \langle x\rangle)$ y $(R[x], \langle x\rangle)$ son espacios de Hausdorff.

Prueba. Sea $f = \sum_{i=0}^{\infty} f_i x^i \in \bigcap_{n \in \mathbb{N}} \langle x\rangle^n$, entonces $f \in \langle x\rangle^n$, para todo $n \in \mathbb{N}$.

Luego para todo $n \in \mathbb{N}$, $f_0 = f_1 = ... = f_{n-1} = 0$.

Esto quiere decir que $f_i = 0$, para todo $i \in \mathbb{N}_0$, entonces $f = 0$.

Por lo tanto

$$\bigcap_{n \in \mathbb{N}} \langle x\rangle^n = \{0\}$$

y por la parte (iii) del lema 3.3 tenemos que $(R[[x]], \langle x\rangle)$ es de Hausdorff.

De forma análoga se prueba que $(R[x], \langle x\rangle)$ es espacio de Hausdorff.

□

- Además podemos ver que $f = 0$ si y solo si $v(f) = \infty$.
- Si $f \neq 0$ entonces $v(f) = Sup\{\, n \in \mathbb{N}_0 \,/\, f \in \langle x\rangle^n \,\}$ la cual llamaremos " **Orden de f** " y la denotaremos:

$$v(f) := Ord(f).$$

Esta aplicación de orden es una generalización del concepto de orden de una serie de potencia formal vista anteriormente en el capítulo 2, definición 2.6.

Definición 3.5. Dado la definición de orden v en el anillo R, definimos:

$$\begin{array}{rccl} d: & R\times R & \longrightarrow & \mathbb{R} \\ & (x,y) & \longmapsto & d(x,y)=e^{-v(x-y)} \end{array}$$

Denotaremos $e^{-\infty}:=0$

Proposición 3.10. d es una pseudométrica.

Prueba. Evidentemente $d(x,x)=0$ y $d(x,y)\geq 0$, para todo $x,y\in R$.

$v(x)=v(-x)$, para todo $x\in R$.

Luego $d(x,y)=e^{-v(x-y)}=e^{-v(y-x)}=d(y,x)$, para todo $x,y\in R$.

Afirmación: Para todo $x,y,z\in R$, $d(x,z)\leq Max\{d(x,y),d(y,z)\}$.

Veamos, $x-z=(x-y)+(y-z)$, luego de 3.4:

$v(x-z)\geq min\{v(x-y),v(y-z)\}$

$-v(x-z)\leq -min\{v(x-y),v(y-z)\}=Max\{-v(x-y),-v(y-z)\}$,

Por lo tanto $e^{-v(x-z)}\leq Max\{e^{-v(x-y)},e^{-v(y-z)}\}$.

Así, queda probada esta afirmación.

Sin pérdida de generalidad supongamos que $d(x,y)\leq d(y,z)$, luego por la afirmación $d(x,z)\leq d(y,z)$.

Luego, $d(x,z)\leq d(x,z)+d(x,y)\leq d(x,y)+d(y,z)$.

Por lo tanto $d(x,y)=e^{-v(x-y)}$ es una pseudométrica.

□

Proposición 3.11. Sea R un a.c.c.i. y $\mathcal{M}$ ideal de R, entonces

a) $(R,\mathcal{M})$ es de Hausdorff si y solo si d es una métrica.

b) Si $(R,\mathcal{M})$ es de Hausdorff entonces su $\mathcal{M}$-Topología se puede definir con la métrica d.

Prueba.

a) Supongamos que R es un espacio de Hausdorff entonces $\bigcap\limits_{n\in\mathbb{N}}\mathcal{M}^n=\{0\}$.

Dados $x,y\in R$, si $d(x,y)=0$ entonces $e^{-v(x-y)}=0$.
$v(x-y)=\infty$, esto quiere decir que $(x-y)\in\bigcap\limits_{n\in\mathbb{N}}\mathcal{M}^n=\{0\}$ entonces $x=y$.

Recíprocamente, si $x\in\bigcap\limits_{n\in\mathbb{N}}\mathcal{M}^n$ entonces $v(x)=v(x-0)=\infty$.

Como d es una métrica, $d(x,0)=e^{-\infty}=0$, luego $x=0$.

Por lo tanto $\bigcap\limits_{n\in\mathbb{N}}\mathcal{M}^n=\{0\}$, así del lema 3.3 concluimos que $(R,\mathcal{M})$ es un espacio de Hausdorff.

b) Al ser $(R, \mathcal{M})$ un espacio de Hausdorff nos garantiza que d es una métrica. Ahora veremos que la topología inducida por d es igual a la topología de $(R, \mathcal{M})$.

Definimos para cada $a \in R$ y $n \in \mathbb{N}_0$,

$$S_n(a) := B_d(a, e^{-n}) = \{\ x \in R \ / \ d(x, a) < e^{-n}\ \}.$$

Estos conjuntos de bolas abiertas determinan una base de la topología inducida por la métrica d, esta base la representaremos como β_d. (ver la Observación 1.5)

Afirmación: Para todo $n \in \mathbb{N}_0$, $\mathcal{M}^n = S_{n-1}(0)$.

En efecto, si $x \in \mathcal{M}^n$, entonces de la Observación 3.6, $n \leq v(x)$ y $-v(x) < -(n-1)$.

$d(x, 0) = e^{-v(x)} < e^{-(n-1)}$, luego $x \in S_{n-1}(0)$. Así concluimos que $\mathcal{M}^n \subset S_{n-1}(0)$.

Si $x \in S_{n-1}(0)$, entonces $d(x, 0) = e^{-v(x)} < e^{-(n-1)}$, luego $n - 1 < v(x)$, $n \leq v(x)$ (fijamos n).

Ahora supongamos que:

$$x \notin \mathcal{M}^n \tag{3.3.7}$$

Entonces $v(x) = Sup\{\ n \in \mathbb{N}_0 \ / \, x \in \mathcal{M}^n\ \}$.

Por la observación 3.6, $x \in \mathcal{M}^{v(x)}$.

Por otro lado, de (3.3.7), $x \notin \mathcal{M}^m$, para todo $m \geq n$.

Luego como $n \leq v(x)$, $x \notin \mathcal{M}^{v(x)}$ lo cual es una contradicción.

Esto quiere decir que $x \in \mathcal{M}^n$, así $S_{n-1}(0) \subset \mathcal{M}^n$, probando de esta manera la afirmación.

De la afirmación, para cada $a \in R$ y $n \in \mathbb{N}_0$ tenemos:

$$\begin{aligned}
\mathcal{M}^n + a &= S_{n-1}(0) + a \\
\mathcal{M}^n + a &= \{x + a \in R / \ x \in S_{n-1}(0)\} = \{x + a \in R / \ d(x, 0) < e^{-(n-1)}\} \\
\mathcal{M}^n + a &= \{x + a \in R / \ e^{-v(x)} < e^{-(n-1)}\} = \{y \in R / \ e^{-v(y-a)} < e^{-(n-1)}\} \\
\mathcal{M}^n + a &= \{y \in R / \ d(y, a) < e^{-(n-1)}\} = S_{n-1}(a).
\end{aligned}$$

Luego $\beta_d = \{\ \mathcal{M}^n + a \, / \, a \in R,\ n \in \mathbb{N}_0\ \}$ la cual es una base de la topología $\mathcal{M}$-ádica.

Por lo tanto la topología $(R, \mathcal{M})$ se puede generar a partir de la base de la topología inducida por d.

□

Observación 3.8.

(i) En $(R, \mathcal{M})$ sus entornos básicos de $x \in R$ en su topología $\mathcal{M}$-ádica son de la forma $\mathcal{M}^n + x$. De la proposición 1.6, una sucesión $(x_n)_{n \in \mathbb{N}}$ en R converge a x si y solo si para todo $k \in \mathbb{N}_0$, existe $s_k \in \mathbb{N}$ tal que $x_n - x \in \mathcal{M}^k$, para todo $n \geq s_k$.

(ii) Si en $(R, \mathcal{M})$ su topología $\mathcal{M}$-ádica es metrizable entonces de la observación 1.7 una sucesión $(x_n)_{n\in\mathbb{N}}$ en R es de Cauchy si y solo si:

para todo $k \in \mathbb{N}_0$, existe $s_k \in \mathbb{N}$ tal que $x_n - x_m \in \mathcal{M}^k$, para todo $n, m \geq s_k$.

Lema 3.5. Sea S un a.c.c.i, $b \in S$ y $(S, \langle b\rangle)$ el anillo topológico con la topología $\langle b\rangle$-ádica. Si $(a_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy de $(S, \langle b\rangle)$ entonces existe una subsucesión $(c_n)_{n\in\mathbb{N}}$ de $(a_n)_{n\in\mathbb{N}}$ tal que $c_n = \sum_{i=0}^{n} r_i b^i$, para todo $n \in \mathbb{N}$ donde $r_i \in S$.

Prueba. Sea $(a_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en $(S, \langle b\rangle)$.

Para todo $k \in \mathbb{N}_0$, existe $s_k \in \mathbb{N}_0$ tal que $a_n - a_m \in \langle b\rangle^{k+1}$, para todo $n, m \geq s_k$.

Sin pérdida de generalidad ordenamos $s_0 \leq s_1 \leq s_2 \leq ...$

Luego para cada $i \in \mathbb{N}_0$, existe $s_i \in \mathbb{N}_0$ tal que $a_{s_{i+1}} - a_{s_i} \in \langle b\rangle^{i+1}$ ya que $s_{i+1} \geq s_i$.

Entonces existe $r_{i+1} \in S$ tal que $a_{s_{i+1}} - a_{s_i} = r_{i+1} b^{i+1}$, para todo $i \in \mathbb{N}_0$.

Para $i \in \mathbb{N}$, sea $c_i = a_{s_i}$ y $r_0 = a_{s_0}$.

$$\begin{array}{ccccccc}
c_1 & = & a_{s_1} & = & a_{s_0} + r_1 b & = & r_0 + r_1 b \\
c_2 & = & a_{s_2} & = & a_{s_1} + r_2 b^2 & = & r_0 + r_1 b + r_2 b^2 \\
 & & & & & \vdots & \\
c_n & = & a_{s_n} & = & a_{s_{n-1}} + r_n b^n & = & r_0 + r_1 b + ... + r_{n-1} b^{n-1} + r_n b^n
\end{array}$$

Por lo tanto $(c_n)_{n\in\mathbb{N}} = (a_{s_n})_{n\in\mathbb{N}}$ es la subsucesión buscada tal que $c_n = \sum_{i=0}^{n} r_i b^i$, para todo $n \in \mathbb{N}$.

$\square$

Observación 3.9. Si el anillo topológico $(S, \langle b\rangle)$ es un espacio de Hausdorff, entonces de la proposición 3.11 este espacio topológico es metrizable.

Si esta subsucesión $(c_n)_{n\in\mathbb{N}}$ es convergente entonces $(a_n)_{n\in\mathbb{N}}$ converge al mismo límite. (Ver proposición 1.9)

La notación de este límite es

$$\lim_{n\to\infty} \sum_{i=0}^{n} r_i b^i := \sum_{i=0}^{\infty} r_i b^i.$$

Por lo tanto el límite de cualquier sucesión convergente de $(S, \langle b\rangle)$ es una serie de potencias de b.

Observación 3.10. Si $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ entonces

$$f = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + x^n(a_n + a_{n+1}x + a_{n+2}x^2 + ...)$$

Es decir que para cualquier $f \in R[[x]]$, $f = h + tx^n$, para todo $n \in \mathbb{N}$, donde $h \in R[x]$ y $t \in R[[x]]$.

Lema 3.6. Si $f = h + tx^n$, donde $h \in R[x]$ y $t \in R[[x]]$, entonces

$$h + x^nR[x] = (f + x^nR[[x]]) \cap R[x]\,.$$

Prueba. Sea $g \in (h + x^nR[x])$, $g = h + ux^n = (f - tx^n) + ux^n$, donde $u \in R[x]$.
Luego $g = f + (u - t)x^n \in f + x^nR[[x]]$ y además $g \in R[x]$.
Así $g \in (f + x^nR[[x]]) \cap R[x]$.
Recíprocamente, si $p \in (f + x^nR[[x]]) \cap R[x]$, $p = (h + tx^n) + sx^n$, donde $s \in R[[x]]$ y $p \in R[x]$, entonces $p - h = (t + s)x^n \in (x^nR[[x]]) \cap R[x] = x^nR[x]$.
Por lo tanto $p \in h + x^nR[x]$.

$\square$

• La siguiente definición que presentamos a continuación es suficiente para explicar las completaciones de anillos topológicos.

Definición 3.6. Sea $(R, \mathcal{M})$ un anillo topológico de de Hausdorff, R^* a.c.c.i con su ideal $\mathcal{M}^*$. Decimos que $(R^*, \mathcal{M}^*)$ es una completación de $(R, \mathcal{M})$ si se cumple:

(i) $(R^*, \mathcal{M}^*)$ es espacio de Hausdorff.

(ii) R es subanillo de R^*.

(iii) La topología inducida sobre R por la $\mathcal{M}^*$- topología en R^* es equivalente a la $\mathcal{M}$ - topología en R.

(iv) Cada elemento de R^* es el límite de una sucesión de Cauchy en R (o también se dice que R es denso en R^*).

(v) $(R^*, \mathcal{M}^*)$ es completo.

Si se cumple estas 5 propiedades escribiremos $\widehat{(R, \mathcal{M})} = (R^*, \mathcal{M}^*)$.

Ejemplo 3.1. Si R un a.c.c.i., entonces $\widehat{(R[x], \langle x \rangle)} = (R[[x]], \langle x \rangle)$.

Veamos:

Recordar que en $(R[x], \langle x \rangle)$, $\langle x \rangle = xR[x]$ y en $(R[[x]], \langle x \rangle)$, $\langle x \rangle = xR[[x]]$.

(i) Por la proposición 3.9 $(R[x], \langle x\rangle)$ y $(R[[x]], \langle x\rangle)$ son espacios de Hausdorff.

(ii) De manera trivial $R[x]$ es subanillo de $R[[x]]$.

(iii) **Afirmación:** Dadas las bases

$$\beta_1 = \{\, x^n R[x] + f \,/\, f \in R[x],\, n \in \mathbb{N}_0 \,\}$$
$$\beta_2 = \{\, x^n R[[x]] + f \,/\, f \in R[[x]],\, n \in \mathbb{N}_0 \,\}$$

de $(R[x], \langle x\rangle)$ y $(R[[x]], \langle x\rangle)$ respectivamente, entonces

$$R[x] \cap \bigcup_{\substack{i\in I\\ V_i\in\beta_2}} V_i = \bigcup_{\substack{i\in J\\ B_i\in\beta_1}} B_i \,.$$

En efecto:

Si $g \in R[x] \cap \bigcup_{\substack{i\in I\\ V_i\in\beta_2}} V_i$, entonces $g \in R[x]$ y se cumple que

$g \in (x^n R[x] + g)$, para cualquier $n \in \mathbb{N}_0$.

Sea $B_{i_0} = x^{n_0} R[x] + g$, para algún $n_0 \in \mathbb{N}_0$ (arbitrario fijo).

Luego $g \in B_{i_0} \subset \bigcup_{\substack{i\in J\\ B_i\in\beta_1}} B_i$.

Recíprocamente, si $h \in \bigcup_{\substack{i\in I\\ B_i\in\beta_1}} B_i$, entonces $h \in (x^{n_i} R[x] + f_i)$ donde $f_i \in R[x]$, para algún $i \in I$.

Luego $h \in (x^{n_i} R[[x]] + f_i) \in \beta_2$ y además $h \in R[x]$.

Por lo tanto $h \in R[x] \cap \bigcup_{\substack{i\in I\\ V_i\in\beta_2}} V_i$, probando así la afirmación.

Esta afirmación quiere decir que los elementos de la topología inducida sobre $R[x]$ por la $\langle x\rangle$-topología en $R[[x]]$ son los mismos elementos de la $\langle x\rangle$-topología en $R[x]$.

Por lo tanto esto implicará que sus respectivas topologías sean equivalentes.

Afirmación: Dadas las bases

$$\beta_1 = \{\, x^n R[x] + f \,/\, f \in R[x],\, n \in \mathbb{N}_0 \,\}$$
$$\beta_2 = \{\, x^n R[[x]] + f \,/\, f \in R[[x]],\, n \in \mathbb{N}_0 \,\}$$

de $(R[x], \langle x\rangle)$ y $(R[[x]], \langle x\rangle)$ respectivamente, entonces $\beta_1 = (\beta_2)_{|_{R[x]}}$.

En efecto:

Si $(x^n R[x] + h) \in \beta_1$, entonces $h = h + 0.x^n \in R[x]$.

Luego del lema 3.6, $(h + x^n R[x]) = (h + x^n R[[x]]) \cap R[x] \in (\beta_2)_{|_{R[x]}}$.

Recíprocamente, si $(f + x^n R[[x]]) \cap R[x] \in (\beta_2)_{|_{R[x]}}$, entonces

$f = h + tx^n \in R[[x]]$, donde $h \in R[x]$ y $t \in R[[x]]$.

Luego del lema 3.6, $(f + x^n R[[x]]) \cap R[x] = (h + x^n R[x]) \in \beta_1$, probando así la afirmación.

Esta afirmación quiere decir que los elementos de la base de la topología inducida sobre $R[x]$ por la $\langle x \rangle$-topología en $R[[x]]$ son los mismos elementos de la base de la $\langle x \rangle$-topología en $R[x]$.

Por lo tanto esto implicará que sus respectivas topologías sean equivalentes.

(iv) Veamos si cada elemento de $R[[x]]$ es el límite de una sucesión de Cauchy en $R[x]$.

Dado $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ arbitrario.

Definimos para todo $n \in \mathbb{N}$, $f_n = \sum_{i=0}^{n} a_i x^i \in R[x]$.

Afirmación: $(f_n)_{n\in\mathbb{N}}$ es una sucesión de $(R[x], \langle x \rangle)$ tal que $f_n \longrightarrow f$.

Sea $k \in \mathbb{N}_0$ arbitrario, si $n \geq k = s_k$, entonces

$$f - f_n = x^{n+1}(a_{n+1} + a_{n+2}x + a_{n+3}x^2 + ...) \in \langle x \rangle^{n+1} \subset \langle x \rangle^n \subset \langle x \rangle^k.$$

Luego $f - f_n \in \langle x \rangle^k$, así $f_n \longrightarrow f$.

De esta afirmación $(f_n)_{n\in\mathbb{N}}$ converge en $(R[[x]], \langle x \rangle)$, entonces $(f_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $(R[[x]], \langle x \rangle)$, esto es:

Para cada $k \in \mathbb{N}_0$, existe $s_k \in \mathbb{N}_0$ tal que $f_n - f_m \in x^k R[[x]]$, para todo $n, m \geq s_k$.

y como $f_n - f_m \in R[x]$, $f_n - f_m \in \left(x^k R[[x]]\right) \bigcap R[x] = x^k R[x]$.

Luego $(f_n)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $(R[x], \langle x \rangle)$.

Por lo tanto, para todo $f \in R[[x]]$, existe una sucesión $(f_n)_{n\in\mathbb{N}}$ de Cauchy en $R[x]$ tal que $f_n \longrightarrow f$.

(v) $(R[[x]], \langle x \rangle)$ es Completo.

Sea $(F_n)_{n\in\mathbb{N}_0}$ una sucesión de Cauchy en $R[[x]]$, entonces por el lema 3.5 tenemos que existe una subsucesión $(G_n)_{n\in\mathbb{N}_0}$ de $(F_n)_{n\in\mathbb{N}_0}$ tal que

$G_n = \sum_{i=0}^{n} H_i x^i$, para todo $n \in \mathbb{N}_0$ donde $H_i = \sum_{j=0}^{\infty} h_{i,j} x^j \in R[[x]]$.

Luego:

$$G_n = H_0 + H_1 x + H_2 x^2 + ... + H_n x^n$$

$$G_n = \sum_{j=0}^{\infty} h_{0,j} x^j + \sum_{j=0}^{\infty} h_{1,j} x^{j+1} + \sum_{j=0}^{\infty} h_{2,j} x^{j+2} + ... + \sum_{j=0}^{\infty} h_{n,j} x^{j+n}$$

Tenemos:

$$G_n = h_{0,0}x^0 + (h_{0,1} + h_{1,0})x^1 + (h_{0,2} + h_{1,1} + h_{2,0})x^2 + \cdots$$

$$+(h_{0,n} + h_{1,n-1} + \cdots + h_{n,0})x^n + (h_{0,n+1} + h_{1,n} + \cdots + h_{n,1})x^{n+1} + \cdots$$

Esta sumatoria se puede escribir de la siguiente manera:

$$G_n = \sum_{j=0}^{n-1} T_j x^j + \sum_{j=0}^{\infty} P_{n,j} x^{n+j} \quad \text{donde} \quad T_j = \sum_{i=0}^{j} h_{i,j-i} \quad \text{y} \quad P_{n,j} = \sum_{i=0}^{n} h_{i,n+j-i}.$$

Ahora definimos $T = \sum_{j=0}^{\infty} T_j x^j \in R[[x]]$.

Afirmación: $\lim_{n\to\infty} G_n = T$.

En efecto, para cada $k \in \mathbb{N}$, si $n \geq k$ entonces

$$T - G_n = \sum_{j=n}^{\infty} T_j x^j - \sum_{j=0}^{\infty} P_{n,j} x^{n+j}$$

$$T - G_n = x^n(T_n + T_{n+1}x + T_{n+2}x^2 + ...) + x^n(P_{n,0} + P_{n,1}x + P_{n,2}x^2 + ...)$$

$$T - G_n \in \langle x\rangle^n \subset \langle x\rangle^k.$$

Como la afirmación nos dice que la subsucesión $(G_n)_{n\in\mathbb{N}_0}$ tiende a T y se sabe que $(R[[x]], \langle x\rangle)$ es de Hausdorff, entonces

$$\lim_{n\to\infty} F_n = T$$

Es decir que cada sucesión de Cauchy $(F_n)_{n\in\mathbb{N}_0}$ en $R[[x]]$ es convergente, luego el espacio $(R[[x]], \langle x\rangle)$ es Completo.

Por lo tanto como cumple las cinco propiedades $(R[[x]], \langle x\rangle)$ es una completación de $(R[x], \langle x\rangle)$.

3.4. Automorfismos en anillos de series formales

En esta sección, estudiamos las propiedades que existen en los R-endomorfismos de $R[[x]]$ y mostramos las condiciones necesarias y suficientes para los R-automorfismos en $R[[x]]$.

El Teorema a continuación, describe un resultado análogo a la Propiedad Universal de Anillos de polinomios para las series formales.

Teorema 3.7. Sea R un a.c.c.i, $\mathcal{T} = \sum_{i=k}^{\infty} b_i x^i \in R[[x]]$ con $k \geq 1$, entonces existe un único $\phi_{\mathcal{T}}$ R-endomorfismo de $R[[x]]$ tal que $\phi_{\mathcal{T}}\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} a_i \mathcal{T}^i$ y $\phi_{\mathcal{T}}(x) = \mathcal{T}$.

Prueba. Dado $g = \sum_{q=0}^{\infty} a_q x^q \in R[[x]]$, denotemos $g_q(x) = a_q x^q$ y $g_q(\mathfrak{T}) = a_q \mathfrak{T}^q$.

Como $Ord(\mathfrak{T}) \geq 1$ entonces $Ord(\mathfrak{T}^q) \geq q$, luego $Ord(g_q(\mathfrak{T})) \geq q$ ó $g_q(\mathfrak{T}) = 0$.

Así, definimos la sucesión $(h_n)_{n\in\mathbb{N}_0}$ de modo que $h_n = \sum_{q=0}^{n} g_q(\mathfrak{T})$, para todo $n \in \mathbb{N}_0$.

Afirmación: $(h_n)_{n\in\mathbb{N}_0}$ es una sucesión de Cauchy en $(R[[x]], \langle x\rangle)$.

En efecto, para cada $k \in \mathbb{N}_0$ existirá un $s_k = k$ tal que si $n, m \geq s_k$ $(n > m)$ entonces:

$$h_n - h_m = \sum_{q=0}^{n} g_q(\mathfrak{T}) - \sum_{q=0}^{m} g_q(\mathfrak{T}) = g_{m+1}(\mathfrak{T}) + g_{m+2}(\mathfrak{T}) + ... + g_{m+p}(\mathfrak{T}) \in \langle x^{m+1}\rangle,$$

para algún $p \in \mathbb{N}$, tal que $n = m + p$.

Luego $h_n - h_m \in \langle x\rangle^{m+1} \subset \langle x\rangle^{s_k} = \langle x\rangle^k$, probando de esta manera la afirmación.

Como $(h_n)_{n\in\mathbb{N}_0}$ es una sucesión de Cauchy en $(R[[x]], \langle x\rangle)$, luego por el ejemplo 3.1-(v), $(h_n)_{n\in\mathbb{N}_0}$ es convergente en $R[[x]]$.

Si definimos $\phi_{\mathfrak{T}}(g) = \lim_{n\to\infty} h_n = \lim_{n\to\infty}\left(\sum_{q=0}^{n} a_q \mathfrak{T}^q\right)$

Recordemos que de la proposición 3.9 $(R[[x]], \langle x\rangle)$ es un espacio de Hausdorff y el teorema 1.4 verifica la unicidad de este límite en $(R[[x]], \langle x\rangle)$ que nos garantiza la buena definición y la unicidad de $\phi_{\mathfrak{T}}$.

Además se verifica que $\phi_{\mathfrak{T}}(r) = r$, para todo $r \in R$ y $\phi_{\mathfrak{T}}(x) = \mathfrak{T}$.

Ahora probaremos que $\phi_{\mathfrak{T}}$ es un endomorfismo de $R[[x]]$.

En efecto, sean $f = \sum_{i=0}^{\infty} f_i x^i$, $g = \sum_{i=0}^{\infty} g_i x^i \in R[[x]]$.

Denotemos $f_n(x) = \sum_{i=0}^{n} f_i x^i$ y $g_n(x) = \sum_{i=0}^{n} g_i x^i$.

Luego,

$$f + g = \sum_{i=0}^{\infty}(f_i + g_i)x^i \quad \text{y} \quad fg = \sum_{i=0}^{\infty} h_i x^i \quad \text{con} \quad h_i = \sum_{k+j=i} f_k g_j.$$

Además,

$$(f + g)_n(x) = \sum_{i=0}^{n}(f_i + g_i)x^i = f_n(x) + g_n(x) \quad \text{y} \quad (fg)_n(x) = \sum_{i=0}^{n} h_i x^i.$$

$$\begin{aligned}\phi_{\mathfrak{T}}(f)+\phi_{\mathfrak{T}}(g) &= \lim_{n\to\infty} f_n(\mathfrak{T}) + \lim_{n\to\infty} g_n(\mathfrak{T}) &&= \lim_{n\to\infty}[f_n(\mathfrak{T})+g_n(\mathfrak{T})]\\ \phi_{\mathfrak{T}}(f)+\phi_{\mathfrak{T}}(g) &= \lim_{n\to\infty}(f+g)_n(\mathfrak{T}) &&= \phi_{\mathfrak{T}}(f+g).\end{aligned}$$

Por otro lado,

$$f_n(x)\,g_n(x) = \left(\sum_{i=0}^{n} f_i x^i\right)\left(\sum_{i=0}^{n} g_i x^i\right) = \sum_{i=0}^{2n} h_i x^i \ \text{ con } \ h_i = \sum_{k+j=i} f_k g_j,$$

para todo $0 \le i \le 2n$.

Como $\displaystyle\sum_{i=0}^{2n} h_i\mathfrak{T}^i = \sum_{i=0}^{n} h_i\mathfrak{T}^i + \sum_{i=n+1}^{2n} h_i\mathfrak{T}^i$.

Tenemos $\displaystyle f_n(\mathfrak{T})\,g_n(\mathfrak{T}) - (fg)_n(\mathfrak{T}) = \sum_{i=n+1}^{2n} h_i\mathfrak{T}^i.$

Afirmación: $\displaystyle\lim_{n\to\infty}\left(\sum_{i=n+1}^{2n} h_i\mathfrak{T}^i\right) = 0.$

En efecto, dado un $k \in \mathbb{N}_0$, si $n \ge k$ entonces $n+p \ge k$, para todo $p \in \mathbb{N}_0$.

Luego $\mathfrak{T}^{n+p} \in \langle x\rangle^{n+p} \subset \langle x\rangle^k$, para todo $p \in \mathbb{N}_0$.

$$\sum_{i=n+1}^{2n} h_i\mathfrak{T}^i = h_{n+1}\mathfrak{T}^{n+1} + h_{n+2}\mathfrak{T}^{n+2} + \ldots + h_{2n}\mathfrak{T}^{2n} \in \langle x\rangle^k,$$

probando así esta afirmación.

De esta afirmación tenemos:

$$\lim_{n\to\infty}\left(\sum_{i=n+1}^{2n} h_i\mathfrak{T}^i\right) = \lim_{n\to\infty}[f_n(\mathfrak{T})g_n(\mathfrak{T})] - \lim_{n\to\infty}[(fg)_n(\mathfrak{T})] = 0.$$

Así concluimos que $\phi_{\mathfrak{T}}(fg) = \phi_{\mathfrak{T}}(f)\,\phi_{\mathfrak{T}}(g)$.

Por lo tanto $\phi_{\mathfrak{T}}$ es un R-endomorfismo de $R[[x]]$.

□

Teorema 3.8. Sea R un a.c.c.i, $\mathfrak{T} = \displaystyle\sum_{i=k}^{\infty} b_i x^i \in R[[x]]$ con $k \ge 1$, entonces $\phi_{\mathfrak{T}}$ es sobreyectiva si y solo si $k = 1$ y b_1 es unidad de R.

Prueba. Supongamos que $\phi_{\mathfrak{T}}$ es sobreyectiva.

Como $x \in R[[x]]$, entonces existe un $f = \displaystyle\sum_{i=0}^{\infty} r_i x^i \in R[[x]]$ tal que $x = \phi_{\mathfrak{T}}(f)$.

Esto quiere decir que $\phi_{\mathfrak{T}}(f) = \sum_{i=0}^{\infty} r_i \mathfrak{T}^i = \lim_{n\to\infty}\left(\sum_{i=0}^{n} r_i \mathfrak{T}^i\right) = x.$

Para $2 \in \mathbb{N}$, existe $n_0 \in \mathbb{N}$ tal que para cada $n \geq n_0$, $\sum_{i=0}^{n} r_i \mathfrak{T}^i - x \in \langle x \rangle^2$.

$r_0 + r_1\mathfrak{T} - x + \sum_{i=2}^{n} r_i \mathfrak{T}^i = r_0 + \sum_{i=k}^{\infty} r_1 b_i x^i - x + \sum_{i=2}^{n} r_i \mathfrak{T}^i \in \langle x \rangle^2$

$$r_0 - x + (r_1 b_k x^k + r_1 b_{k+1} x^{k+1} + ...) + (\text{términos de orden } \geq 2) = \sum_{i=0}^{\infty} g_i x^{i+2}. \qquad (3.4.1)$$

Luego, si fuera $k > 1$, en la igualdad de (3.4.1), el coeficiente de "x" en ambos miembros no coincidirían.

Por lo tanto $k = 1$.

Esto implica que $r_0 = 0$ y $r_1 b_1 = 1$, es decir que b_1 es una unidad de R.

Recíprocamente supongamos que $k = 1$ y b_1 es unidad de R.

Entonces $\mathfrak{T} = \sum_{i=1}^{\infty} b_i x^i$.

Ahora dado un $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$, tenemos que demostrar la existencia de una serie de potencia $g = \sum_{i=0}^{\infty} r_i x^i \in R[[x]]$ de modo que $\lim_{n\to\infty}\left(\sum_{i=0}^{n} r_i \mathfrak{T}^i\right) = f$.

Para cada $j \in \mathbb{N}_0$, debe de existir un $s_j \in \mathbb{N}$ tal que para cada $n \geq s_j$ se cumpla que

$$\sum_{i=0}^{n} r_i \mathfrak{T}^i - \sum_{i=0}^{\infty} a_i x^i \in \langle x \rangle^j.$$

$$(r_0 + r_1\mathfrak{T} + r_2\mathfrak{T}^2 + ...) - (a_0 + a_1 x + a_2 x^2 + ...) \in \langle x \rangle^j.$$

De esta manera, si igualamos a 0 esta expresión (pues $0 \in \langle x \rangle^j$, para todo $j \in \mathbb{N}_0$), podemos encontrar los coeficientes de g los cuales son:

$r_0 = a_0$

$r_1 = a_1 b_1^{-1}$

$r_2 = (a_2 - r_1 b_2)(b_1^2)^{-1}$

$r_3 = (a_3 - r_1 b_3 - r_2(2b_1 b_2))(b_1^3)^{-1}$

$\vdots$

$r_i = [a_i - r_1 b_i - r_2(\text{coeficientes de } x^i \text{ en } \mathfrak{T}^2) - r_3(\text{coeficientes de } x^i \text{ en } \mathfrak{T}^3) - ... - r_{i-1}(\text{coeficientes de } x^i \text{ en } \mathfrak{T}^{i-1})](b_1^i)^{-1}.$

Así, encontramos la existencia de la serie de potencias formal g que garantiza que $\phi_{\mathfrak{T}}$ sea sobreyectiva.

□

Lema 3.7. Sea R un a.c.c.i, $\mathfrak{T} = \sum_{i=k}^{\infty} b_i x^i \in R[[x]]$ donde $k \geq 1$ y $b_k \neq 0$, $\phi_{\mathfrak{T}}$ un endomorfismo de $R[[x]]$ tal que $\phi_{\mathfrak{T}}(r) = r$, para todo $r \in R$ y $\phi_{\mathfrak{T}}(x) = \mathfrak{T}$.
Si $\phi_{\mathfrak{T}}$ no es inyectiva entonces b_k es un divisor de 0 en R.

Prueba. Supongamos que $\phi_{\mathfrak{T}}$ no es inyectiva.
Esto quiere decir que existe una serie formal $f = \sum_{i=0}^{\infty} c_i x^i \in Nu(\phi_{\mathfrak{T}})$ tal que $f \neq 0$.
Luego $\phi_{\mathfrak{T}}(f) = \sum_{i=0}^{\infty} c_i \mathfrak{T}^i = c_0 + \sum_{i=1}^{\infty} c_i \mathfrak{T}^i = 0$. Esto implica que $c_0 = 0$.
Como $\sum_{i=1}^{\infty} c_i x^i \neq 0$, entonces existe un $c_m \neq 0$ tal que

$$f = c_m x^m + c_{m+1} x^{m+1} + ... = \sum_{i=m}^{\infty} c_i x^i.$$

Luego,

$$\phi_{\mathfrak{T}}(f) = c_m \mathfrak{T}^m + c_{m+1} \mathfrak{T}^{m+1} + ... = 0.$$

$$c_m(b_k^m x^{mk} + \text{t.o.s}) + c_{m+1}(b_k^{m+1} x^{(m+1)k} + \text{t.o.s}) + ... = 0.$$

$$c_m b_k^m x^{mk} + \text{t.o.s} = 0, \text{ esto es } c_m b_k^m = 0.$$

Como $c_m \neq 0$ y $b_k \neq 0$ tenemos que b_k es un divisor de 0 en R.

□

Corolario 3.11.1. Sea R un a.c.c.i con $D.I$, $\mathfrak{T} = \sum_{i=k}^{\infty} b_i x^i \in R[[x]]$ donde $k \geq 1$ y $b_k \neq 0$, $\phi_{\mathfrak{T}}$ un endomorfismo de $R[[x]]$ tal que $\phi_{\mathfrak{T}}(x) = \mathfrak{T}$, entonces $\phi_{\mathfrak{T}}$ es inyectiva.

Prueba. Por hipótesis tenemos que $b_k \neq 0$, como R es un Dominio Integridad entonces b_k no es divisor de 0 en R y por el lema 3.7 $\phi_{\mathfrak{T}}$ es inyectiva.

□

Teorema 3.9. Dado $\mathcal{T} = \sum_{i=k}^{\infty} b_i x^i \in R[[x]]$ con $k \geq 1$, $\phi_{\mathcal{T}}$ un R-endomorfismo de $R[[x]]$ tal que $\phi_{\mathcal{T}}(x) = \mathcal{T}$, entonces

$\phi_{\mathcal{T}}$ es R- automorfismo de $R[[x]]$ si y solo si $k = 1$ y b_1 es unidad de R.

Prueba. Si $\phi_{\mathcal{T}}$ es R-automorfismo de $R[[x]]$ entonces por el Teorema 3.8, $k = 1$ y b_1 es unidad de R.

Recíprocamente, supongamos que $k = 1$ y b_1 es unidad de R. Por el mismo teorema 3.8, $\phi_{\mathcal{T}}$ es sobreyectiva.

También tenemos que $b_1 \neq 0$, entonces b_1 no es divisor de 0 en R y por el lema 3.7, $\phi_{\mathcal{T}}$ es inyectiva.

Por lo tanto $\phi_{\mathcal{T}}$ es R-automorfismo de $R[[x]]$.

□

Observación 3.11.

- Sean R a.c.c.i y $\mathcal{T} \in R[[x]]$. El conjunto $R[\mathcal{T}] = \left\{ \sum_{i=0}^{n} r_i \mathcal{T}^i \ / \ r_i \in R, \ n \in \mathbb{N}_0 \right\}$ es un subanillo de $R[[x]]$ generado por R y $\mathcal{T}$.
- Si $\mathcal{T} \in R[[x]]$ y S es subanillo de $R[[x]]$ tal que $R[\mathcal{T}] \subset S$, entonces $\mathcal{T}^n S$ es un ideal de S generado por $\mathcal{T}^n$. Además $(S, \mathcal{T}S)$ es el anillo topológico S con su topología $\mathcal{T}S$ - ádica.
- Si $\mathcal{T} \in R[[x]]$ y $\bigcap_{n \in \mathbb{N}} (\mathcal{T}^n R[\mathcal{T}]) = \{0\}$, entonces $(R[\mathcal{T}], \mathcal{T}R[\mathcal{T}])$ es un espacio de Hausdorff.

Proposición 3.12. Sean R a.c.c.i, $\mathcal{T} \in R[[x]]$ y ϕ un R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathcal{T}$. Si S es un subanillo de $R[[x]]$ tal que $\phi(R[[x]]) \subset S$, entonces

(i) La aplicación $\phi : (R[[x]], \langle x \rangle) \longrightarrow (S, \mathcal{T}S)$ es continua.

(ii) Si $f = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$, entonces existe $\lim_{n \to \infty} \left(\sum_{i=0}^{\infty} f_i \mathcal{T}^i \right)$ en $(S, \mathcal{T}S)$ y converge a $\phi(f)$.

Prueba.

(i) Necesitaremos de la siguiente afirmación.

Afirmación: $\phi\left(\langle x \rangle^k\right) = \mathcal{T}^k \phi\left(R[[x]]\right)$.

En efecto, si $f \in \phi(\langle x \rangle^k)$, entonces existe $h \in R[[x]]$ tal que

$f = \phi(hx^k) = \phi(h)\phi(x)^k = \mathcal{T}^k \phi(h) \in \mathcal{T}^k \, \phi(R[[x]])$.

Si $f \in \mathcal{T}^k \phi(R[[x]])$, entonces para algún $h \in R[[x]]$, $f = \mathcal{T}^k \phi(h) = \phi(x)^k \phi(h)$, luego $f = \phi(x^k h) \in \phi(\langle x \rangle^k)$, probamos así la afirmación.

Veamos la continuidad de ϕ. Dado $g \in R[[x]]$ arbitrario.

Para cada $\phi(g) + \mathcal{T}^k S$ entorno de $\phi(g)$ en $(S, \mathcal{T}S)$ escogemos $g + \langle x \rangle^k$ que es entorno de g en $(R[[x]], \langle x \rangle)$.

Luego de la afirmación y como $\phi(R[[x]]) \subset S$,

$\phi\left(g + \langle x \rangle^k\right) = \phi(g) + \phi(\langle x \rangle^k) = \phi(g) + \mathcal{T}^k \phi(R[[x]]) \subset \phi(g) + \mathcal{T}^k S.$

Por lo tanto ϕ es continua.

(ii) Para cada $k \in \mathbb{N}$ escogemos el mismo $s_k = k$ tal que si $n \geq s_k$

$$f - \sum_{i=0}^{n} f_i x^i = \sum_{i=n+1}^{\infty} f_i x^i = x^{n+1}(f_{n+1} + f_{n+2}x + f_{n+3}x^2 + ...) \in \langle x \rangle^{n+1} \subset \langle x \rangle^k.$$

Luego, $\lim\limits_{n \to \infty} \left(\sum_{i=0}^{n} f_i x^i \right) = f$ en $(R[[x]], \langle x \rangle)$.

Además, $\phi\left(\sum_{i=0}^{n} f_i \phi(x)^i \right) = \sum_{i=0}^{n} f_i \phi(x)^i = \sum_{i=0}^{n} f_i \mathcal{T}^i$ y como ϕ es continua de $(R[[x]], \langle x \rangle)$ en $(S, \mathcal{T}S)$, entonces

$$\phi(f) = \lim_{n \to \infty} \phi\left(\sum_{i=0}^{n} f_i x^i \right) = \lim_{n \to \infty} \left(\sum_{i=0}^{n} f_i \mathcal{T}^i \right) \text{ en } (S, \mathcal{T}S).$$

$\square$

Observación 3.12.

(i) En la Proposición anterior, si le agregamos a la hipótesis la condición $\bigcap_{n \in \mathbb{N}} (\mathcal{T}^n S) = \{0\}$, es decir que $(S, \mathcal{T}S)$ es un espacio de Hausdorff, entonces para cualquier $f \in R[[x]]$, $\phi(f) = \lim\limits_{n \to \infty} \left(\sum_{i=0}^{n} f_i \mathcal{T}^i \right) \in S$ es único.

(ii) En particular, dado $\mathcal{T} \in R[[x]]$ y ϕ un R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathcal{T}$ con $\bigcap_{n \in \mathbb{N}} (\mathcal{T}^n R[[x]]) = \{0\}$, entonces ϕ es único.

En efecto, supongamos que existe otro ψ R-endomorfismo de $R[[x]]$ tal que $\psi(x) = \mathcal{T}$ y $\psi(R[[x]]) \subset S$.

Dado $f \in R[[x]]$ arbitrario, por la proposición 3.12 ψ es continua, así

$$\psi(f) = \lim_{n \to \infty} \left(\sum_{i=0}^{n} f_i \mathcal{T}^i \right) \text{ en } (S, \mathcal{T}S).$$

Ya que $\phi(f) = \lim\limits_{n \to \infty} \left(\sum_{i=0}^{n} f_i \mathcal{T}^i \right) \in S$ y este límite es único, por ser $(S, \mathcal{T}S)$ un espacio de Hausdorff, tenemos que $\psi(f) = \phi(f)$. Por lo tanto $\psi = \phi = \phi_{\mathfrak{T}}$ y lo llamaremos **"Aplicación sustitución"**.

Teorema 3.10. Sean R a.c.c.i, $\mathfrak{T} \in R[[x]]$, S subanillo de $R[[x]]$ tal que $R[\mathfrak{T}] \subset S$. Si la topología S-ádica $(S, \mathfrak{T}S)$ es un espacio de Hausdorff completo, entonces existe únicamente un ϕ R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$ y $\phi(R[[x]]) \subset S$.

Prueba. Dado $f = \sum_{i=0}^{\infty} f_i x^i \in R[[x]]$ arbitrario. Definimos para esta serie de potencias formal la sucesión en $R[[x]]$, $f_n(\mathfrak{T}) = \sum_{i=0}^{n} f_i \mathfrak{T}^i$, para todo $n \in \mathbb{N}$.

Afirmación 1: $(f_n(\mathfrak{T}))_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $(S, \mathfrak{T}S)$.
En efecto, para cada $k \in \mathbb{N}_0$ escogemos el mismo $s_k = k$ tal que si $n, m \geq s_k$, (elegimos sin pérdida de generalidad $n \geq m \geq s_k$), tenemos

$$f_n(\mathfrak{T}) - f_m(\mathfrak{T}) = \sum_{i=m+1}^{n} f_i \mathfrak{T}^i = \mathfrak{T}^{m+1}\left(f_{m+1} + f_{m+2}\mathfrak{T} + ... + f_n \mathfrak{T}^{n-(m+1)}\right)$$

$f_n(\mathfrak{T}) - f_m(\mathfrak{T}) \in \mathfrak{T}^{m+1}R[\mathfrak{T}] \subset \mathfrak{T}^k R[\mathfrak{T}] \subset \mathfrak{T}^k S$, probando así la afirmación.

Ya que $(S, \mathfrak{T}S)$ es un espacio de Hausdorff y completo, entonces $(f_n(\mathfrak{T}))_{n\in\mathbb{N}}$ converge en $(S, \mathfrak{T}S)$ y su límite es único.

Esto nos garantiza la definición de la aplicación

$$\begin{aligned} \phi : R[[x]] &\longrightarrow S \subset R[[x]] \\ f = \sum_{i=0}^{\infty} f_i x^i &\longmapsto \phi(f) = \lim_{n\to\infty} f_n(\mathfrak{T}) \end{aligned}$$

Además, si $f \in \phi(R[[x]])$, entonces existe algún $g \in R[[x]]$ tal que $f = \phi(g) = \lim_{n\to\infty} g_n(\mathfrak{T}) \in S$. Así, $\phi(R[[x]]) \subset S$.

Ahora veamos si ϕ es un R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$.

(i) Si $f = r \in R$, $f_n(\mathfrak{T}) = r$, así $\phi(r) = \lim_{n\to\infty} f_n(\mathfrak{T}) = r$.

(ii) Si $f = x \in R[[x]]$, $f_n(\mathfrak{T}) = \mathfrak{T}$, así $\phi(x) = \lim_{n\to\infty} f_n(\mathfrak{T}) = \mathfrak{T}$.

(iii) Sean $f = \sum_{i=0}^{\infty} f_i x^i$, $g = \sum_{i=0}^{\infty} g_i x^i \in R[[x]]$, entonces

$$\phi(f+g) = \lim_{n\to\infty}(f+g)_n(\mathfrak{T}) = \lim_{n\to\infty}\sum_{i=0}^{n}(f_i+g_i)\mathfrak{T}^i = \lim_{n\to\infty}\left[\sum_{i=0}^{n} f_i\mathfrak{T}^i + \sum_{i=0}^{n} g_i\mathfrak{T}^i\right]$$

$$\phi(f+g) = \lim_{n\to\infty}[\,f_n(\mathfrak{T}) + g_n(\mathfrak{T})\,] = \lim_{n\to\infty} f_n(\mathfrak{T}) + \lim_{n\to\infty} g_n(\mathfrak{T}) = \phi(f) + \phi(g).$$

(iv) Por otro lado, como $f_n(\mathfrak{T})=\sum_{i=0}^{n} f_i\mathfrak{T}^i$ y $g_n(\mathfrak{T})=\sum_{i=0}^{n} g_i\mathfrak{T}^i$, entonces

$(fg)_n(\mathfrak{T}) = \sum_{i=0}^{n} h_i\mathfrak{T}^i$, donde $h_i = \sum_{r+s=i} f_r g_s \ \ (0 \leq r, s \leq n)$.

Además, $f_n(\mathfrak{T})g_n(\mathfrak{T}) = \sum_{i=0}^{2n} h_i\mathfrak{T}^i = \sum_{i=0}^{n} h_i\mathfrak{T}^i + \sum_{i=n+1}^{2n} h_i\mathfrak{T}^i = (fg)_n(\mathfrak{T}) + \sum_{i=n+1}^{2n} h_i\mathfrak{T}^i$.

Afirmación 2: $\lim_{n\to\infty}\left(\sum_{i=n+1}^{2n} h_i\mathfrak{T}^i\right) = 0$ en $(S, \mathfrak{T}S)$.

En efecto, para cada $k \in \mathbb{N}_0$ escogemos el mismo $s_k = k$ tal que si $n \geq s_k$

$$\sum_{i=n+1}^{2n} h_i\mathfrak{T}^i = \mathfrak{T}^{n+1}\left(h_{n+1} + h_{n+2}\mathfrak{T} + ... + h_{2n}\mathfrak{T}^{n-1}\right) \in \mathfrak{T}^{n+1}R[\mathfrak{T}] \subset \mathfrak{T}^k R[\mathfrak{T}] \subset \mathfrak{T}^k S,$$

probando así la afirmación.

Luego, $\lim_{n\to\infty} [f_n(\mathfrak{T})g_n(\mathfrak{T}) - (fg)_n(\mathfrak{T})] = 0$. Así,

$$\phi(fg) = \lim_{n\to\infty} (fg)_n(\mathfrak{T}) = \lim_{n\to\infty} [f_n(\mathfrak{T})g_n(\mathfrak{T})] = \lim_{n\to\infty} f_n(\mathfrak{T}) \lim_{n\to\infty} g_n(\mathfrak{T}) = \phi(f)\,\phi(g).$$

Para finalizar, ya que $(S, \mathfrak{T}S)$ es un espacio de Hausdorff, por la observación 3.12 obtenemos la unicidad de ϕ.

□

Teorema 3.11. Sea R a.c.c.i, $\mathfrak{T} \in R[[x]]$ y S subanillo de $R[[x]]$ tal que $R[\mathfrak{T}] \subset S$. Si se cumple:

(i) $(S, \mathfrak{T}S)$ es Hausdorff completo.

(ii) Cada elemento de S es el límite de una sucesión de Cauchy en $(R[\mathfrak{T}], \mathfrak{T}R[\mathfrak{T}])$.

Entonces existe únicamente un ϕ R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$ y $S = \phi(R[[x]])$.

Recíprocamente si ϕ es un R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$, $S = \phi(R[[x]])$ y $\bigcap_{n\in\mathbb{N}}(\mathfrak{T}^n S) = \{0\}$, entonces S es subanillo de $R[[x]]$ tal que $R[\mathfrak{T}] \subset S$ cumpliendo **(i)** y **(ii)**.

Prueba. Sea S subanillo de $R[[x]]$ tal que $R[\mathfrak{T}] \subset S$ que cumple **(i)** y **(i)**.

Aplicando en **(i)** del teorema 3.10 tenemos que existe únicamente ϕ R-endomorfismo tal que $\phi(x) = \mathfrak{T}$ y $\phi(R[[x]]) \subset S$.

También por la proposición 3.12 tenemos que ϕ es continua de $(R[[x]], \langle x\rangle)$ en $(S, \mathfrak{T}S)$.

Solo faltaría probar que $S \subset \phi(R[[x]])$.

En efecto, sea $g \in S$, entonces existe $(f_n)_{n\in\mathbb{N}}$ sucesión de Cauchy en $(R[\mathfrak{T}], \mathfrak{T}R[\mathfrak{T}])$ tal que $\lim\limits_{n\to\infty} f_n = g$.

Del lema 3.5, existe $(d_n)_{n\in\mathbb{N}}$ subsucesión de $(f_n)_{n\in\mathbb{N}}$ tal que $d_n=\sum\limits_{i=0}^{n} g_i\mathcal{T}^i$ donde $g_i \in R[\mathcal{T}] = \phi(R[x])$, es decir, que para cada $i \in \mathbb{N}_0$, existe $h_i \in R[x]$ tal que $\phi(h_i)=g_i$.

Luego $d_n=\sum\limits_{i=0}^{n} \phi(h_i)\phi(x)^i = \phi\left(\sum\limits_{i=0}^{n} h_ix^i\right)$, para todo $n \in \mathbb{N}_0$.

Del ejemplo 3.1-(iv),(v) se sabe que $\left(\sum\limits_{i=0}^{n} h_ix^i\right)_{n\in\mathbb{N}}$ es una sucesión de Cauchy en $(R[[x]], \langle x\rangle)$ que además es completo.

Entonces existe $h\in R[[x]]$ tal que $\lim\limits_{n\to\infty}\left(\sum\limits_{i=0}^{n} h_ix^i\right) = h$.

Luego por la continuidad de ϕ, $\lim\limits_{n\to\infty} d_n = \lim\limits_{n\to\infty} \phi\left(\sum\limits_{i=0}^{n} h_ix^i\right) = \phi(h) \in S$.

Ya que $(S, \mathcal{T}S)$ es un espacio de Hausdorff y la subsucesión $(d_n)_{n\in\mathbb{N}}$ de $(f_n)_{n\in\mathbb{N}}$ converge a $\phi(h) \in S$, entonces por la observación 3.9, $(f_n)_{n\in\mathbb{N}}$ converge a $\phi(h) \in S$, es decir, $g = \phi(h) \in \phi(R[[x]])$, probando así que $S \subset \phi(R[[x]])$.

Por lo tanto $S = \phi(R[[x]])$.

Recíprocamente, si ϕ es R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathcal{T}$, $S=\phi(R[[x]])$ y $(S, \mathcal{T}S)$ es de Hausdorff, pues $\bigcap\limits_{n\in\mathbb{N}}(\mathcal{T}^nS) = \{0\}$.

Además, por la proposición 3.12, ϕ es continua de $(R[[x]], \langle x\rangle)$ en $(S, \mathcal{T}S)$.

Evidentemente S es subanillo de $R[[x]]$ y $R[\mathcal{T}]=\phi(R[x]) \subset \phi(R[[x]])=S$.

(i) Sea $(f_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en $(S, \mathcal{T}S)$.

Luego por el lema 3.5 existe $(d_n)_{n\in\mathbb{N}}$ subsucesión de $(f_n)_{n\in\mathbb{N}}$ tal que

$$d_n=\sum_{i=0}^{n} \phi(h_i)\mathcal{T}^i =\sum_{i=0}^{n} \phi(h_i)\phi(x)^i = \phi\left(\sum_{i=0}^{n} h_ix^i\right), \text{ donde } \phi(h_i)\in S = \phi(R[[x]]).$$

Como vimos anteriormente, la sucesión $\left(\sum\limits_{i=0}^{n} h_ix^i\right)_{n\in\mathbb{N}}$ es de Cauchy en $(R[[x]], \langle x\rangle)$ y que además es completo, entonces existe $h\in R[[x]]$ tal que $\lim\limits_{n\to\infty}\left(\sum\limits_{i=0}^{n} h_ix^i\right) = h$ y por la continuidad de ϕ tenemos que

$$\lim_{n\to\infty} d_n= \lim_{n\to\infty}\phi\left(\sum_{i=0}^{n} h_ix^i\right) = \phi(h) \in S.$$

Finalmente, al ser $(f_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en el espacio de Hausdorff $(S, \mathcal{T}S)$ y su subsucesión $(d_n)_{n\in\mathbb{N}}$ que converge en $\phi(h)\in S$, entonces por la observación 3.9 tenemos que $\lim\limits_{n\to\infty} f_n = \phi(h) \in S$, es decir, $(f_n)_{n\in\mathbb{N}}$ es convergente en $(S, \mathcal{T}S)$.

Por lo tanto $(S, \mathfrak{T}S)$ es completo.

(ii) Sea $g \in S$ arbitrario, entonces existe $h = \sum_{i=0}^{\infty} h_i x^i \in R[[x]]$ tal que $\phi(h) = g$.

Del ejemplo 3.1, $\left(\sum_{i=0}^{n} h_i x^i\right)_{n \in \mathbb{N}}$ es una sucesión de Cauchy en $(R[[x]], \langle x \rangle)$,

además $\lim\limits_{n\to\infty}\left(\sum_{i=0}^{n} h_i x^i\right) = h$ y por continuidad de ϕ tenemos que

$$\lim_{n\to\infty}\left(\sum_{i=0}^{n} h_i \mathfrak{T}^i\right) = \lim_{n\to\infty} \phi\left(\sum_{i=0}^{n} h_i x^i\right) = \phi(h) = g.$$

Para concluir, $\left(\sum_{i=0}^{n} h_i \mathfrak{T}^i\right)_{n \in \mathbb{N}}$ es una sucesión de Cauchy en $(R[\mathfrak{T}], \mathfrak{T}R[\mathfrak{T}])$,

pues para todo $k \in \mathbb{N}_0$, existe $s_k = k \in \mathbb{N}_0$ tal que si $n \geq m \geq s_k$,

$$\sum_{i=0}^{n} h_i \mathfrak{T}^i - \sum_{i=0}^{m} h_i \mathfrak{T}^i = \sum_{i=m+1}^{n} h_i \mathfrak{T}^i = \mathfrak{T}^{m+1} \sum_{i=m+1}^{n} h_i \mathfrak{T}^{i-m-1} \in \mathfrak{T}^{m+1} R[\mathfrak{T}] \subset \mathfrak{T}^k R[\mathfrak{T}].$$

□

Observación 3.13. Del teorema 3.11, si $S = R[[x]]$ y cumple **(i)** y **(ii)**, entonces existe únicamente un ϕ R-endomorfismo sobreyectivo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$

Lema 3.8. Sea R a.c.c.i, $\mathfrak{T} = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ y ψ un R-homomorfismo de $R[x]$ en $R[[x]]$ tal que $\psi(x) = \mathfrak{T}$.

Luego ψ es inyectiva si y solo si $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$.

Prueba. Sea $\left(\sum_{i=0}^{n} r_i \mathfrak{T}^i\right)(\mathfrak{T} - a_0) = 0$, entonces $\psi\left(\left(\sum_{i=0}^{n} r_i x^i\right)(x - a_0)\right) = \psi(0)$.

Por la inyectividad de ψ tenemos $\left(\sum_{i=0}^{n} r_i x^i\right)(x - a_0) = 0$.

Afirmación. $(x - a_0)$ es regular en $R[x]$.

En efecto, supongamos que $(x - a_0)$ es divisor de 0 en $R[x]$.

Por el Teorema de McCoy's existe $c \in R$ diferente de 0 tal que $c(x - a_0) = 0$ y esto implica que $c = 0$ siendo una contradicción, probando así la afirmación.

Luego $\sum_{i=0}^{n} r_i x^i = 0$, $\sum_{i=0}^{n} r_i \mathfrak{T}^i = \psi\left(\sum_{i=0}^{n} r_i x^i\right) = \psi(0) = 0$.

Por lo tanto $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$.

Reciprocamente, supongamos que $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$.

Sea $f = \sum_{i=0}^{n} r_i x^i \in Nu(\psi)$, tenemos:

$0 = \psi(f) = \sum_{i=0}^{n} r_i \mathfrak{T}^i = \sum_{i=0}^{n} r_i[a_0 + (\mathfrak{T} - a_0)]^i = \sum_{i=0}^{n} p_i(\mathfrak{T} - a_0)^i,$

donde $p_i = \sum_{j=i}^{n} r_j \binom{j}{i} a_0^{j-i} \in R$, para $i = 0, 1, ..., n$.

Afirmación 1. $p_i = 0$, para $i = 0, 1, ..., n$.

En efecto, para $i = 0$:

Ya que $\sum_{i=0}^{n} p_i(\mathfrak{T} - a_0)^i = 0$, $p_0 = -\sum_{i=1}^{n} p_i(\mathfrak{T} - a_0)^i = -(\mathfrak{T} - a_0)\sum_{i=1}^{n} p_i(\mathfrak{T} - a_0)^{i-1}$.

Además $Ord(\mathfrak{T} - a_0) \geq 1$, así $Ord(p_0) \geq 1$ y como $p_0 \in R$ deducimos que $p_0 = 0$.

Ahora supongamos que $p_i = 0$, para $i = 0, 1, ..., l$. (Hipótesis Inductiva).

Luego, tenemos:

$0 = \sum_{i=0}^{n} p_i(\mathfrak{T} - a_0)^i = p_0 + p_1(\mathfrak{T} - a_0) + ... + p_l(\mathfrak{T} - a_0)^l + \sum_{i=l+1}^{n} p_i(\mathfrak{T} - a_0)^i$

$0 = (\mathfrak{T} - a_0)^{l+1} \sum_{i=l+1}^{n} p_i(\mathfrak{T} - a_0)^{i-l-1}$ con $(\mathfrak{T} - a_0)^{l+1}$ regular en $R[\mathfrak{T}]$, pues $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$ (ver proposición 1.12).

Entonces $0 = \sum_{i=l+1}^{n} p_i(\mathfrak{T} - a_0)^{i-l-1} = p_{l+1} + (\mathfrak{T} - a_0) \sum_{i=l+2}^{n} p_i(\mathfrak{T} - a_0)^{i-l-2}$

$p_{l+1} = -(\mathfrak{T} - a_0) \sum_{i=l+2}^{n} p_i(\mathfrak{T} - a_0)^{i-l-2}$. Así $Ord(p_{l+1}) \geq 1$ donde $p_{l+1} \in R$.

De esta manera se concluye que $p_{l+1} = 0$, así probamos la afirmación.

Afirmación 2. $r_{n-i} = 0$, para $i = 0, 1, ..., n$.

En efecto, para $i = 0$ es de inmediato pues de la Afirmación 1:

$0 = p_n = \sum_{j=n}^{n} r_j \binom{j}{n} a_0^{j-n} = r_n = r_{n-0}$.

Ahora supongamos que $r_{n-i} = 0$, para $i = 0, 1, ..., m$. (Hipótesis Inductiva).

Es decir, $r_n = r_{n-1} = ... = r_{n-(m-1)} = r_{n-m} = 0$.

Luego, la Afirmación 1 nos dice que $0 = p_{n-(m+1)} = \sum_{j=n-m-1}^{n} r_j \binom{j}{n-m-1} a_0^{j-(n-m-1)}$

$0 = r_{n-m-1} + r_{n-m}\binom{n-m}{n-m-1} a_0 + r_{n-m+1}\binom{n-m+1}{n-m-1} a_0^2 + ... + r_n \binom{n}{n-m-1} a_0^{m+1} = r_{n-(m+1)}$,

así hemos probado la afirmación.

De la afirmación 2, concluimos que $f = \sum_{i=0}^{n} r_i x^i = 0$. Por lo tanto, ψ es inyectiva. $\square$

Observación 3.14. Sea ϕ un R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$.

Podemos generalizar la observación 3.10 y el lema 3.6 si reemplazamos los anillos $R[x]$ y $R[[x]]$ por los anillos $R[\mathfrak{T}]$ y $S = \phi\,(R[[x]])$.

Si $f \in S = \phi(R[[x]])$, entonces $f = \phi\left(\sum_{i=0}^{\infty} a_i x^i\right)$, donde $a_i \in R$.

Luego:

$$f = \phi\,((a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1}) + x^n(a_n + a_{n+1}x + a_{n+2}x^2 + ...))$$

$$f = (a_0 + a_1\mathfrak{T} + a_2\mathfrak{T}^2 + ... + a_{n-1}\mathfrak{T}^{n-1}) + \phi\,(x^n(a_n + a_{n+1}x + a_{n+2}x^2 + ...))$$

$$f = (a_0 + a_1\mathfrak{T} + a_2\mathfrak{T}^2 + ... + a_{n-1}\mathfrak{T}^{n-1}) + \mathfrak{T}^n\phi\,(a_n + a_{n+1}x + a_{n+2}x^2 + ...)$$

Es decir que para cualquier $f \in S = \phi(R[[x]])$, $f = h + t\mathfrak{T}^n$, para todo $n \in \mathbb{N}$, donde $h \in R[\mathfrak{T}]$ y $t \in S$.

Lema 3.9. Sea ϕ un R-endomorfismo inyectivo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$.
Si $f = h + t\mathfrak{T}^n$, donde $h \in R[\mathfrak{T}]$ y $t \in S = \phi(R[[x]])$, entonces

(i) $(\mathfrak{T}^n S) \cap R[\mathfrak{T}] = \mathfrak{T}^n R[\mathfrak{T}]$

(ii) $h + \mathfrak{T}^n R[\mathfrak{T}] = (f + \mathfrak{T}^n S) \cap R[\mathfrak{T}]$.

Prueba.

(i) $(\mathfrak{T}^n S) \cap R[\mathfrak{T}] = [\phi(x)^n \phi\,(R[[x]])] \cap \phi\,(R[x]) = \phi\,(x^n R[[x]]) \cap \phi\,(R[x])$.

Ya que ϕ es inyectiva tenemos:

$(\mathfrak{T}^n S) \cap R[\mathfrak{T}] = \phi\,((x^n R[[x]]) \cap R[x]) = \phi\,(x^n R[x]) = \mathfrak{T}^n \phi\,(R[x]) = \mathfrak{T}^n R[\mathfrak{T}]$.

(ii) Sea $g \in (h + \mathfrak{T}^n R[\mathfrak{T}])$, $g = h + u\mathfrak{T}^n = (f - t\mathfrak{T}^n) + u\mathfrak{T}^n$, donde $u \in R[\mathfrak{T}]$.

Luego $g = f + (u - t)\mathfrak{T}^n \in f + \mathfrak{T}^n S$ y además $g \in R[\mathfrak{T}]$.

Así $g \in (f + \mathfrak{T}^n S) \cap R[\mathfrak{T}]$.

Recíprocamente, si $p \in (f + \mathfrak{T}^n S) \cap R[\mathfrak{T}]$, $p = (h + t\mathfrak{T}^n) + s\mathfrak{T}^n$, donde $s \in S$ y $p \in R[\mathfrak{T}]$, entonces $p - h = (t + s)\mathfrak{T}^n \in (\mathfrak{T}^n S) \cap R[\mathfrak{T}] = \mathfrak{T}^n R[\mathfrak{T}]$.

Por lo tanto $p \in h + \mathfrak{T}^n R[\mathfrak{T}]$.

$\square$

Teorema 3.12. Sea R a.c.c.i y $\mathfrak{T} = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$, entonces
existe un ϕ R-endomorfismo inyectivo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$ si y solo si

(i) $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$.

(ii) Existe S subanillo de $R[[x]]$ tal que $(\widehat{R[\mathfrak{T}], \mathfrak{T}R[\mathfrak{T}]}) = (S, \mathfrak{T}S)$.

Prueba.

(i) Ya que $\phi_{|_{R[x]}}$ es R-homomorfismo de $R[x]$ en $R[[x]]$ tal que $\phi(x) = \mathcal{T}$, entonces por el lema 3.8, $(\mathcal{T} - a_0)$ es regular en $R[\mathcal{T}]$.

(ii) Ya que ϕ es inyectiva tenemos:

$$\bigcap_{n\in\mathbb{N}} (\mathcal{T}^n R[\mathcal{T}]) = \bigcap_{n\in\mathbb{N}} (\phi(x)^n \phi\,(R[x])) = \bigcap_{n\in\mathbb{N}} \phi\,(x^n R[x]) = \phi\left(\bigcap_{n\in\mathbb{N}} x^n R[x]\right)$$

$$\bigcap_{n\in\mathbb{N}} (\mathcal{T}^n R[\mathcal{T}]) = \phi(\{0\}) = \{0\}.$$

Sea $S = \phi(R[[x]])$, entonces S es subanillo de $R[[x]]$ y además $R[\mathcal{T}] = \phi(R[x]) \subset S$. Usando la propiedad dada en la afirmación de la proposición 3.12 y por la inyectividad de ϕ tenemos:

$$\bigcap_{n\in\mathbb{N}} (\mathcal{T}^n S) = \bigcap_{n\in\mathbb{N}} (\mathcal{T}^n \phi\,(R[[x]])) = \bigcap_{n\in\mathbb{N}} \phi\,(x^n R[[x]]) = \phi\left(\bigcap_{n\in\mathbb{N}} x^n R[[x]]\right)$$

$$\bigcap_{n\in\mathbb{N}} (\mathcal{T}^n S) = \phi(\{0\}) = \{0\}.$$

Luego del teorema 3.11 tenemos:

(1) $(S, \mathcal{T}S)$ es un espacio de Hausdorff completo.

(2) Cada elemento de S es el límite de una sucesión de Cauchy en $(R[\mathcal{T}], \mathcal{T}R[\mathcal{T}])$.

Afirmación. Dadas las bases

$$\beta_1 = \{\, \mathcal{T}^n R[\mathcal{T}] + f \,/\, f \in R[\mathcal{T}], n \in \mathbb{N}_0 \,\}$$
$$\beta_2 = \{\, \mathcal{T}^n S + f \,/\, f \in S, n \in \mathbb{N}_0 \,\}$$

de $(R[\mathcal{T}], \mathcal{T}R[\mathcal{T}])$ y $(S, \mathcal{T}S)$ respectivamente, entonces

$$R[\mathcal{T}] \cap \bigcup_{\substack{i\in J\\ V_i\in\beta_2}} V_i = \bigcup_{\substack{i\in I\\ B_i\in\beta_1}} B_i\ .$$

En efecto:

Evidentemente, si $g \in R[\mathcal{T}] \cap \bigcup_{\substack{i\in J\\ V_i\in\beta_2}} V_i$, $g \in R[\mathcal{T}]$ y $g \in \mathcal{T}^n R[\mathcal{T}] + g \in \beta_1$, para cualquier $n \in \mathbb{N}_0$. Luego $g \in \bigcup_{\substack{i\in I\\ B_i\in\beta_1}} B_i$.

Si $h \in \bigcup_{\substack{i\in I\\ B_i\in\beta_1}} B_i$, entonces $h \in (\mathcal{T}^{n_i} R[\mathcal{T}] + f_i)$ donde $f_i \in R[\mathcal{T}]$, para algún $i \in I$.

Luego $h \in (\mathcal{T}^{n_i} S + f_i) \in \beta_2$ y además $h \in R[\mathcal{T}]$.

Por lo tanto $h \in R[\mathfrak{T}] \cap \bigcup_{\substack{i\in J \\ V_i \in \beta_2}} V_i$, probando así la afirmación.

Esta afirmación quiere decir que los elementos de la topología inducida sobre $R[\mathfrak{T}]$ por la $\mathfrak{T}S$ - topología en S son los mismos elementos de la $\mathfrak{T}R[\mathfrak{T}]$ - topología en $R[\mathfrak{T}]$.

Esto implicará que sus respectivas topologías sean equivalentes.

Afirmación: Dadas las bases

$$\beta_1 = \{\, \mathfrak{T}^n R[\mathfrak{T}] + f \,/\, f \in R[\mathfrak{T}],\, n \in \mathbb{N}_0 \,\}$$
$$\beta_2 = \{\, \mathfrak{T}^n S + f \,/\, f \in S,\, n \in \mathbb{N}_0 \,\}$$

de $(R[\mathfrak{T}], \mathfrak{T}R[\mathfrak{T}])$ y $(S, \mathfrak{T}S)$ respectivamente, entonces $\beta_1 = (\beta_2)_{|R[\mathfrak{T}]}$.

En efecto:

Si $(\mathfrak{T}^n R[\mathfrak{T}] + h) \in \beta_1$, entonces $h = h + 0.\mathfrak{T}^n \in R[\mathfrak{T}]$.

Luego del lema 3.9, $(h + \mathfrak{T}^n R[\mathfrak{T}]) = (h + \mathfrak{T}^n S) \cap R[\mathfrak{T}] \in (\beta_2)_{|R[\mathfrak{T}]}$.

Recíprocamente, si $(f + \mathfrak{T}^n S) \cap R[\mathfrak{T}] \in (\beta_2)_{|R[\mathfrak{T}]}$, entonces $f = h + t\mathfrak{T}^n \in S$, donde $h \in R[\mathfrak{T}]$ y $t \in S$.

Luego del lema 3.9, $(f + \mathfrak{T}^n S) \cap R[\mathfrak{T}] = (h + \mathfrak{T}^n R[\mathfrak{T}]) \in \beta_1$, probando así la afirmación.

Esta afirmación quiere decir que los elementos de la base de la topología inducida sobre $R[\mathfrak{T}]$ por la $(\mathfrak{T}S)$-topología en S son los mismos elementos de la base de la $(\mathfrak{T}R[\mathfrak{T}])$-topología en $R[\mathfrak{T}]$.

Esto implicará que sus respectivas topologías sean equivalentes.

Por lo tanto, concluimos que $(\widehat{R[\mathfrak{T}], \mathfrak{T}R}[\mathfrak{T}]) = (S, \mathfrak{T}S)$.

Recíprocamente, si existe S subanillo de $R[[x]]$ tal que $(\widehat{R[\mathfrak{T}], \mathfrak{T}R}[\mathfrak{T}]) = (S, \mathfrak{T}S)$ entonces $R[\mathfrak{T}] \subset S$ y $(S, \mathfrak{T}S)$ es Hausdorff completo.

Luego del teorema 3.10 existe únicamente un ϕ R-endomorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$ y $\phi(R[[x]]) \subset S$.

Ahora vamos a demostrar que ϕ es inyectiva.

Sea $f = \sum_{i=0}^{\infty} r_i x^i \in Nu(\phi)$, es decir, $\phi(f) = \lim_{n\to\infty} \left(\sum_{i=0}^{n} r_i \mathfrak{T}^i \right) = 0 \in S$.

De la hipótesis se sabe que la topología inducida sobre S por la $\mathfrak{T}R[\mathfrak{T}]$-Topología en $R[\mathfrak{T}]$ es equivalente a la $\mathfrak{T}S$-Topología en S.

Luego para $k \in \mathbb{N}_0$, $\mathfrak{T}^{k+1} R[\mathfrak{T}] \in \tau(\beta_1) = \tau(\beta_2)_{|R[\mathfrak{T}]}$, entonces

$$R[\mathfrak{T}] \cap (\mathfrak{T}^m S) \subset R[\mathfrak{T}] \cap \bigcup_{\substack{i\in I \\ V_i \in \beta_2}} V_i = \mathfrak{T}^{k+1} R[\mathfrak{T}], \text{ para algún } m \in \mathbb{N}_0. \tag{3.4.2}$$

Ya que $m \in \mathbb{N}_0$, entonces existe $s_m \in \mathbb{N}_0$ tal que $\sum_{i=0}^{n} r_i \mathfrak{T}^i \in \mathfrak{T}^m S$, para todo $n \geq s_m$.

Además $\sum_{i=0}^{n} r_i \mathfrak{T}^i \in R[\mathfrak{T}]$, luego de 3.4.2, $\sum_{i=0}^{n} r_i \mathfrak{T}^i \in \mathfrak{T}^{k+1} R[\mathfrak{T}]$, para todo $n \geq s_m$.

$\phi\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=0}^{n} r_i \mathfrak{T}^i = \mathfrak{T}^{k+1} \sum_{i=0}^{l} r'_i \mathfrak{T}^i = \phi\left(x^{k+1} \sum_{i=0}^{l} r'_i x^i\right)$, para todo $n \geq s_m$.

Como $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$, por el lema 3.8 $\phi_{|_{R[x]}}$ es inyectivo, así $\sum_{i=0}^{n} r_i x^i = x^{k+1} \sum_{i=0}^{l} r'_i x^i$, para todo $n \geq s_m$. Luego $r_0 = r_1 = ...r_k = 0$.

Esto implica que para todo $k \in \mathbb{N}_0$, $r_k = 0$ y consecuentemente $f = 0$.

Por lo tanto ϕ es un R-endomorfismo inyectivo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$.

□

Teorema 3.13. Sea R a.c.c.i y $\mathfrak{T} = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$.
Existe un ϕ R-automorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$ si y solo si $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$ y $(\widehat{R[\mathfrak{T}], \mathfrak{T}R}[\mathfrak{T}]) = (R[[x]], \mathfrak{T}R[[x]])$.

Prueba. Supongamos que existe un ϕ R-automorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$.

Luego por el teorema 3.12 tenemos que $(\mathfrak{T} - a_0)$ es regular en $R[\mathfrak{T}]$ y existe $S = \phi(R[[x]])$ subanillo de $R[[x]]$ tal que $(\widehat{R[\mathfrak{T}], \mathfrak{T}R}[\mathfrak{T}]) = (S, \mathfrak{T}S)$.

Además, por ser ϕ sobreyectiva, $S = \phi(R[[x]]) = R[[x]]$.

Por lo tanto $(\widehat{R[\mathfrak{T}], \mathfrak{T}R}[\mathfrak{T}]) = (R[[x]], \mathfrak{T}R[[x]])$.

Recíprocamente, si $(\widehat{R[\mathfrak{T}], \mathfrak{T}R}[\mathfrak{T}]) = (R[[x]], \mathfrak{T}R[[x]])$ entonces

- **(i)** $(R[[x]], \mathfrak{T}R[[x]])$ es Hausdorff completo.
- **(ii)** Cada elemento de $R[[x]]$ es el límite de una sucesión de Cauchy en $(R[\mathfrak{T}], \mathfrak{T}R[\mathfrak{T}])$.

Luego, aplicando la observación 3.13, existe únicamente un ϕ R-endomorfismo sobreyectivo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$.

También en la hipótesis aplicamos el teorema 3.12, así existe un ϕ' R-endomorfismo inyectivo de $R[[x]]$ tal que $\phi'(x) = \mathfrak{T}$.

Ya que ϕ es único entonces $\phi = \phi'$ es inyectivo.

Por lo tanto ϕ es un R-automorfismo de $R[[x]]$ tal que $\phi(x) = \mathfrak{T}$.

□

Capítulo 4

SERIES FORMALES EN VARIAS INDETERMINADAS

En este capítulo estudiamos las series de potencias formales en varias indeterminadas con coeficientes en un cuerpo. Mostramos también, las principales propiedades en estas series de potencias con coeficientes en un anillo conmutativo con identidad general.

4.1. Anillos de Series de Potencias Formales en varias indeterminadas

Sea R un a.c.c.i. Denotaremos

$$R^{((n))} = R[[x_1, x_2, ..., x_n]]$$

al conjunto de las series de potencias formales ($s.p.f$) en las indeterminadas $x_1, x_2, ..., x_n$ con coeficientes en R.

Cada elemento $f \in R^{((n))}$ se puede expresar como una suma de polinomios homogéneos, es decir,

$$f = \sum_{i=0}^{\infty} P_i = P_0 + P_1 + P_2 + ...$$

donde P_i es un polinomio homogéneo de grado i en las indeterminadas $x_1, x_2, ..., x_n$ con coeficientes en R. Consideramos al polinomio cero como un polinomio de grado $-\infty$.

Definición 4.1. Sean las series formales $f = \sum_{i=0}^{\infty} P_i, \;\; g = \sum_{i=0}^{\infty} Q_i \in R^{((n))}$.

(i) Diremos que $f = g$ sí y solo si $P_i = Q_i$, para todo $i \in \mathbb{N}_0$.

(ii) Definiremos $f + g = \sum_{i=0}^{\infty}(P_i + Q_i)$ como la suma de dos $s.p.f.$

(iii) Definiremos $fg = \sum_{i=0}^{\infty}\left(\sum_{j=0}^{i} P_j Q_{i-j}\right) = \sum_{i=0}^{\infty}\left(\sum_{j+k=i} P_j Q_k\right)$ como el producto de dos $s.p.f.$

Con estas operaciones podemos probar que $\left(R^{((n))},+,\cdot\right)$ es un anillo conmutativo con unidad a la cual llamaremos **“El anillo de las series de potencias formales en indeterminadas $\boldsymbol{x_1, x_2, ..., x_n}$ con coeficientes en $\boldsymbol{R}$”**.

Como R es un a.c.c.i, podemos observar que R y $R[x_1, x_2, ..., x_n]$ son subanillos de $R^{((n))}$.

Una $s.f.p$ $f \in R^{((n))}$ también se puede representar de forma:

$$f = \sum_{i=0}^{\infty}\left(\sum_{i_1+i_2+...+i_n=i} a_{i_1,i_2,...,i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}\right)$$

donde $a_{i_1,i_2,...,i_n} \in R$.

• Recordemos que un elemento $f \in R^{((n))}$ es unidad (o invertible) en $R^{((n))}$ si existe otro elemento $g \in R^{((n))}$ tal que $f.g = g.f = 1$.

Proposición 4.1. Sea R a.c.c.i, $f = \sum_{i=0}^{\infty} P_i \in R^{((n))}$ es unidad en $R^{((n))}$ si y solo si $P_0 \neq 0$.

Prueba. Sea $g = \sum_{i=0}^{\infty} Q_i \in R^{((n))}$ el elemento inverso de f.

Luego $1 = f.g = P_0Q_0 + (P_1Q_0 + P_0Q_1) + ...,$ entonces $1 = P_0Q_0$.

Por lo tanto $P_0 \neq 0$.

Recíprocamente encontraremos un elemento $g = \sum_{i=0}^{\infty} Q_i \in K\left[[x_1, x_2, ..., x_n]\right]$ que verifique $f.g = P_0Q_0 + (P_1Q_0 + P_0Q_1) + ... = 1$.

Igualando término por término:

$$\begin{aligned}
&P_0Q_0 = 1\\
&P_1Q_0 + P_0Q_1 = 0\\
&\vdots\\
&P_nQ_0 + P_{n-1}Q_1 + ... + P_1Q_{n-1} + P_0Q_n = 0
\end{aligned}$$

Como $P_0 \neq 0$ podemos encontrar los polinomios homogéneos de g de forma iterativa los cuales serian:

$$\begin{aligned}
&Q_0 = P_0^{-1}\\
&Q_1 = -P_0^{-1}P_1Q_0\\
&\vdots\\
&Q_n = -P_0^{-1}(P_nQ_0 + P_{n-1}Q_1 + ... + P_1Q_{n-1})
\end{aligned}$$

Por lo tanto f es unidad.

□

Observación 4.1. Sea R a.c.c.i, se puede deducir:

(i) $\mathcal{M} = \left\{ f = \sum_{i=0}^{\infty} P_i \in R^{((n))} \,/\, P_0 = 0 \right\}$ es un ideal de $R^{((n))}$.

(ii) $\mathcal{M}$ es el ideal generado por las indeterminadas $x_1, x_2, ..., x_n$, es decir,

$$\mathcal{M} = \langle x_1, x_2, ..., x_n \rangle R^{((n))} := \langle x_1, x_2, ..., x_n \rangle.$$

(iii) Para cada $k \in \mathbb{N}$,

$$\mathcal{M}^k = \left\{ f = \sum_{i=0}^{\infty} P_i \in R^{((n))} \,/\, P_0 = P_1 = P_2 = ... = P_{k-1} = 0 \right\}$$

es la k-ésima potencia de $\mathcal{M}$. Por convención denotaremos $\mathcal{M}^0 := R^{((n))}$.

Proposición 4.2. Sea R a.c.c.i, $\langle x_1, x_2, ..., x_n \rangle$ es el único ideal maximal de $R^{((n))}$ y además se cumple $\bigcap_{k \in \mathbb{N}} \langle x_1, x_2, ..., x_n \rangle^k = 0$.

Prueba. Evidentemente se puede ver que $\langle x_1, x_2, ..., x_n \rangle \neq R^{((n))}$, pues $1 \notin \langle x_1, x_2, ..., x_n \rangle$.

Sea I un ideal de $R^{((n))}$ tal que $\langle x_1, x_2, ..., x_n \rangle \subseteq I \subseteq R^{((n))}$.

Supongamos $\langle x_1, x_2, ..., x_n \rangle \neq I$, entonces existe un $f \in I$ tal que $f \notin \langle x_1, x_2, ..., x_n \rangle$.

Esto quiere decir que $f(0) \neq 0$, lo que implica que f es unidad de $R^{((n))}$.

Así existe $g \in R^{((n))}$ tal que $g.f = 1 \in I$. Luego para todo $g \in R^{((n))}$, $g = 1.g \in I$, por lo tanto $I = R^{((n))}$, es decir que $\langle x_1, x_2, ..., x_n \rangle$ es un ideal maximal.

Ahora probemos la unicidad de $\langle x_1, x_2, ..., x_n \rangle$.

Supongamos que existe otro ideal maximal $\mathcal{M}'$ de $R^{((n))}$.

Afirmamos que $\mathcal{M}' \subseteq \langle x_1, x_2, ..., x_n \rangle$, en efecto :

Si no fuera así existiría un $f \in \mathcal{M}'$ tal que $f \notin \langle x_1, x_2, ..., x_n \rangle$, entonces tenemos que $1 \in \mathcal{M}'$.

Luego para todo $g \in R^{((n))}$, $g = 1.g \in \mathcal{M}'$, por lo tanto $\mathcal{M}'_{\mathcal{R}} = R^{((n))}$, lo que es un absurdo.

Como $\mathcal{M}'$ es un ideal maximal y $\mathcal{M}' \subseteq \langle x_1, x_2, ..., x_n \rangle$, por definición tenemos que $\mathcal{M}' = \langle x_1, x_2, ..., x_n \rangle$.

Finalmente probaremos que $\bigcap_{k \in \mathbb{N}} \langle x_1, x_2, ..., x_n \rangle^k = 0$.

Dado $f = \sum_{i=0}^{\infty} P_i \in \bigcap_{k\in\mathbb{N}} \langle x_1, x_2, ..., x_n\rangle^k$, entonces para todo $k \in \mathbb{N}_0$,
$P_0 = P_1 = ... = P_{k-1} = 0$.

Luego para todo $k \in \mathbb{N}_0$, $P_k = 0$, es decir $f = 0$.
Por lo tanto $\bigcap_{k\in\mathbb{N}} \langle x_1, x_2, ..., x_n\rangle^k = 0$.

$\square$

Observación 4.2.

(i) Como $R^{((n))}$ es a.c.c.i y $\langle x_1, x_2, ..., x_n\rangle$ es su ideal respectivo, entonces $\left(R^{((n))}, \langle x_1, x_2, ..., x_n\rangle\right)$ representa el anillo topológico $R^{((n))}$ con su topología $\langle x_1, x_2, ..., x_n\rangle$-ádica (ver la proposición 3.7).

(ii) Ya que $\bigcap_{k\in\mathbb{N}} \langle x_1, x_2, ..., x_n\rangle^k = 0$, entonces por el lema 3.3, $\left(R^{((n))}, \langle x_1, x_2, ..., x_n\rangle\right)$ es un espacio de Hausdorff. Además, por la proposición 3.11, se puede definir una métrica en este espacio.

Proposición 4.3. $\left(R^{((n))}, \langle x_1, x_2, ..., x_n\rangle\right)$ es un espacio métrico completo.

Prueba. Sea $(f_i)_{i\in\mathbb{N}}$ una sucesión de Cauchy en $\left(R^{((n))}, \langle x_1, x_2, ..., x_n\rangle\right)$.
Dado $i \in \mathbb{N}$, entonces existen $k_i, k_{i+1} \in \mathbb{N}$ tales que para todo $l, m, \geq k_i$ ($l, m \geq k_{i+1}$ respectivamente), $f_l - f_m \in \langle x_1, x_2, ..., x_n\rangle^i$.
Sin pérdida de generalidad escogemos $k_i \leq k_{i+1}$, así, $f_{k_{i+1}} - f_{k_i} \in \langle x_1, x_2, ..., x_n\rangle^i$.
Para cada $i \in \mathbb{N}$, sean

$$\begin{aligned} f_{k_i} &= P_{i0} + P_{i1} + P_{i2} + ... \in R^{((n))} \\ f_{k_{i+1}} &= P_{i+1,0} + P_{i+1,1} + P_{i+1,2} + ... \in R^{((n))} \end{aligned}$$

Luego, $f_{k_{i+1}} - f_{k_i} = \sum_{j=0}^{\infty} (P_{i+1,j} - P_{ij}) \in \langle x_1, x_2, ..., x_n\rangle^i$.
Por consiguiente, $P_{i,j} = P_{i+1,j}$, para todo $j = 0, 1, ..., i-1$; $i \in \mathbb{N}$.

Definimos la serie formal

$$f = P_{1,0} + P_{2,1} + ... + P_{i,i-1} + P_{i+1,i} ... = (P_{i,0} + P_{i,1} + ... + P_{i,i-1}) + P_{i+1,i} ... \in R^{((n))}$$

Así, $f - f_{k_i} = (P_{i+1,i} - P_{ii}) + (P_{i+2,i+1} - P_{i,i+1}) + ... \in \langle x_1, x_2, ..., x_n\rangle^i$.

Es decir que existe $f \in R^{((n))}$ tal que $f - f_{k_i} \in \langle x_1, x_2, ..., x_n\rangle^i$, para todo $i \in \mathbb{N}$.

Luego $\lim\limits_{i \to \infty} f_{k_i} = f$, por ende, la sucesión de Cauchy $(f_i)_{i\in\mathbb{N}}$ tiene una subsucesión $(f_{k_i})_{i\in\mathbb{N}}$ convergente en $\left(R^{((n))}, \langle x_1, x_2, ..., x_n\rangle\right)$ que es un espacio de Hausdorff metrizable.

Por lo tanto $(f_i)_{i\in\mathbb{N}}$ converge en $\left(R^{((n))}, \langle x_1, x_2, ..., x_n\rangle\right)$.

$\square$

Observación 4.3.

- De la definición 3.4, tenemos la aplicación orden

$$\begin{array}{rccc} v: & R^{((n))} & \longrightarrow & \mathbb{N}_0 \cup \{\infty\} \\ & f & \longmapsto & v(f) \end{array}$$

  Donde:

$$v(f) = \begin{cases} \infty & ,\text{si} \quad f = 0 \\ \\ Max\{m \in \mathbb{N}_0 \,/\, f \in \mathcal{M}^m\} & ,\text{si} \quad f \neq 0 \end{cases}$$

  Si $f \neq 0$, entonces existe algún $r \in \mathbb{N}$ tal que $f = P_r + P_{r+1} + P_{r+2} + ...$, donde $P_r \neq 0$.

  Luego, dado un $f \in \langle x_1, x_2, ..., x_n\rangle^m$ arbitrario. Supongamos que $m > r$, tenemos

$$f = P_r + P_{r+1} + ... + P_m + ... \in \langle x_1, x_2, ..., x_n\rangle^m.$$

  Esto quiere decir que $P_r = 0$, lo cual es una contradicción.

  Así, $m \leq r$, para todo $f \in \langle x_1, x_2, ..., x_n\rangle^m$.

  Por lo tanto, $v(f) = Max\{\, m \in \mathbb{N}_0 \,/\, f \in \mathcal{M}^m\} = r$.

- En conclusión:
  Si $f = 0$, entonces $Ord(f) = \infty$.
  Si $f \neq 0$, entonces $Ord(f) = r$, donde $f = P_r + P_{r+1} + ...$, con $P_r \neq 0$.

- Llamaremos a P_r “ **Forma inicial de *f*** ”.

- $f \in R^{((n))}$ es unidad en $R^{((n))}$ si y solo si $Ord(f) = 0$.

- $f \in \langle x_1, x_2, ..., x_n\rangle^m$ si y solo si $Ord(f) \geq m$.

Proposición 4.4. Sea R un Dominio de Integridad. Dados $f, g \in R^{((n))}$, entonces se cumple:

(i) $Ord(f.g) = Ord(f) + Ord(g)$.

(ii) $Ord(f \pm g) \geq min\{Ord(f), Ord(g)\}$.
Además, si $Ord(f) \neq Ord(g)$ entonces $Ord(f \pm g) = min\{Ord(f), Ord(g)\}$.

Prueba.

(i) Dados $f=\sum_{i=r}^{\infty} P_i,\ g=\sum_{i=m}^{\infty} Q_i$ con $P_r \neq 0$ y $Q_m \neq 0$.

Luego $f.g = P_rQ_m + (P_{r+1}Q_m + P_rQ_{m+1}) + ...,$ donde $P_rQ_m \neq 0$ por ser R un $D.I$ y además el grado de P_rQ_m es $r+m$.

Por lo tanto, $Ord(f.g) = r+m = Ord(f) + Ord(g)$.

(ii) Por el lema 3.4 se sabe que $Ord(f \pm g) \geq min\{Ord(f), Ord(g)\}$.

Teniendo a f y g establecidos como en la parte (i) tenemos que $Ord(f) = r$ y $Ord(g) = m$.

Si $m > r$, entonces $f \pm g = P_r + P_{r+1} + ... + (P_m \pm Q_m) + (P_{m+1} \pm Q_{m+1}) + ...$ y como $P_r \neq 0$ tenemos que $Ord(f \pm g) = r = min\{Ord(f), Ord(g)\}$.

□

Proposición 4.5. Si R es DI, entonces $R^{((n))}$ es un DI.

Prueba. Dados $f, g \in R^{((n))} \setminus \{0\}$.
Esto quiere decir que existen $r, m \in \mathbb{N}_0$ tales que $Ord(f) = r$ y $Ord(g) = m$.
Luego como R es DI, $Ord(f.g) = r+m$, por lo tanto $f.g \neq 0$.

□

Observación 4.4.

- Dados $\alpha_1, \alpha_2, ..., \alpha_n \in R^{((n))}$, escribiremos para cada $i \in \mathbb{N}_0$,

$$P_i(\alpha_1, \alpha_2, ..., \alpha_n) = \sum_{i_1+...+i_n=i} r_{i_1,...,i_n} \alpha_1^{i_1} \alpha_2^{i_2} ... \alpha_n^{i_n} \in R^{((n))}$$

  donde $r_{i_1,...,i_n} \in R$.

- Luego el conjunto $R[\alpha_1, \alpha_2, ..., \alpha_n] = \left\{ \sum_{i=0}^{q} P_i(\alpha_1, \alpha_2, ..., \alpha_n) \,/\, q \in \mathbb{N}_0 \right\}$ es un subanillo de $R^{((n))}$ generado por R y $\alpha_1, \alpha_2, ..., \alpha_n$.

- El ideal de $R[\alpha_1, \alpha_2, ..., \alpha_n]$ generado por $\alpha_1, \alpha_2, ..., \alpha_n$ se pueden escribir de la forma

$$\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle R[\alpha_1, \alpha_2, ..., \alpha_n] = \left\{ \sum_{i=1}^{q} P_i(\alpha_1, \alpha_2, ..., \alpha_n) \,/\, q \in \mathbb{N} \right\}.$$

- Luego para cada $k \in \mathbb{N}$,

$$\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle^k R[\alpha_1, \alpha_2, ..., \alpha_n] = \left\{ \sum_{i=k}^{k+q} P_i(\alpha_1, \alpha_2, ..., \alpha_n) \,/\, q \in \mathbb{N}_0 \right\}$$

  es la k-ésima potencia del ideal $\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle$.

4.2. Homomorfismos de K-álgebras

Recordemos que si K es un cuerpo, un álgebra sobre K o también llamado K-álgebra con unidad es un anillo con unidad $(A,+,\cdot)$ cumpliendo que

(i) A es un espacio vectorial sobre K.
(ii) Para todo $\lambda \in K$ y $a,b \in A$, $\lambda(ab) = (\lambda a)b = a(\lambda b)$.

Un homomorfismo de K-álgebras es una aplicación entre dos K-álgebras $\psi : A \longrightarrow B$ de manera que para todo $a,b \in A$ y $\lambda \in K$ se cumple

$$\begin{array}{l} \psi(a+b) = \psi(a) + \psi(b) \\ \psi(ab) = \psi(a)\psi(b) \\ \psi(1_A) = 1_B \\ \psi(\lambda a) = \lambda\psi(a). \end{array}$$

Por ejemplo, si K es un cuerpo, el anillo de series formales en varias indeterminadas $K[[x_1,x_2,...,x_n]]$ es un K-álgebra.

Además, si la aplicación ψ es un K-endomorfismo (unitario) de $K[[x_1,x_2,...,x_n]]$, tenemos que para todo $f,g \in K[[x_1,x_2,...,x_n]]$ y $\lambda \in K$ se cumple

$$\begin{array}{l} \psi(f+g) = \psi(f) + \psi(g) \\ \psi(fg) = \psi(f)\psi(g) \\ \psi(\lambda f) = \psi(\lambda)\psi(f) = \lambda\psi(f). \\ \psi(1) = 1 \end{array}$$

Esto quiere decir que cuando K es un cuerpo, un K-endomorfismo de $K[[x_1,x_2,...,x_n]]$ se puede ver también como un homomorfismo de K-álgebras.

• De ahora en adelante, si tenemos un cuerpo K, denotaremos los conjuntos de las series formales de la siguiente manera

$$\begin{array}{l} K_x^{((n))} := K[[x_1,x_2,...,x_n]] \\ K_y^{((m))} := K[[y_1,y_2,...,y_m]] \end{array}$$

con sus respectivos ideales maximales

$$\begin{array}{l} \langle x_1,x_2,...,x_n\rangle K_x^{((n))} := \langle x_1,x_2,...,x_n\rangle \\ \langle y_1,y_2,...,y_m\rangle K_y^{((m))} := \langle y_1,y_2,...,y_m\rangle. \end{array}$$

• Dados $\alpha_1,\alpha_2,...,\alpha_n \in K_y^{((m))}$. Sabemos que para cada $i \in \mathbb{N}$

$P_i(x_1,...,x_n) = \sum\limits_{i_1+...+i_n=i} k_{i_1,...,i_n} x_1^{i_1}x_2^{i_2}...x_n^{i_n}$ es un polinomio homogéneo de grado i en $K[x_1,x_2,...,x_n]$. También, $\sum\limits_{i=0}^{r} P_i(x_1,...,x_n) \in K[x_1,x_2,...,x_n]$.

Luego, si $\alpha_1, \alpha_2, ..., \alpha_n \in K_y^{((m))}$ sustituimos en $P_i(x_1, ..., x_n)$, tenemos

$$P_i(\alpha_1, ..., \alpha_n) = \sum_{i_1+...+i_n=i} k_{i_1,...,i_n} \alpha_1^{i_1} \alpha_2^{i_2} ... \alpha_n^{i_n} \in K_y^{((m))} \quad \text{y} \quad \sum_{i=0}^{r} P_i(\alpha_1, ..., \alpha_n) \in K_y^{((m))},$$

es decir que en $K[x_1, x_2, ..., x_n]$ podemos sustituir las series formales $\alpha_1, ..., \alpha_n$.

- Ahora veamos el siguiente caso, si $f(x_1, ..., x_n) = \sum_{i=0}^{\infty} P_i(x_1, ..., x_n) \in K_x^{((n))}$,

¿ Será posible sustituir en una serie formal arbitraria las indeterminadas $\boldsymbol{x_1, ..., x_n}$ por las series formales $\boldsymbol{\alpha_1, \alpha_2, ..., \alpha_n \in K_y^{((m))}}$?

¿ $\boldsymbol{f(\alpha_1, ..., \alpha_n) = \sum_{i=0}^{\infty} P_i(\alpha_1, ..., \alpha_n) \in K_x^{((n))}}$ estará bien definido ?

Supongamos que esté bien definido, veamos el siguiente ejemplo:

Sean $\alpha_1, \alpha_2, ..., \alpha_n \in K_y^{((m))}$ tal que $\alpha_i = c + \sum_{i=1}^{\infty} P_i(y_1, ..., y_m)$ con $c \in K \setminus \{0\}$, para algún $i \in \{1, ..., n\}$.

Si $f(x_1, ..., x_n) = 1 + c^{-1} y_i + c^{-2} y_i^2 + c^{-3} y_i^3 + ... \in K_y^{((m))}$, entonces,

$$f(\alpha_1, ..., \alpha_n) = 1 + c^{-1}\alpha_i + c^{-2}\alpha_i^2 + c^{-3}\alpha_i^3 + ...$$

$$f(\alpha_1, ..., \alpha_n) = 1 + c^{-1}\left[c + \sum_{i=1}^{\infty} P_i(y_1, ..., y_m)\right] + c^{-2}\left[c + \sum_{i=1}^{\infty} P_i(y_1, ..., y_m)\right]^2 + ...$$

$$f(\alpha_1, ..., \alpha_n) = (1 + 1 + 1 + ...) + g, \quad \text{donde} \quad Ord(g) \geq 1.$$

Así, $1 + 1 + 1 + ... \in K$, lo cual es una contradicción.

En general no siempre es posible efectuar esa sustitución, pues el resultado no siempre esta definido en $K_x^{((n))}$.

- Antes de resolver esta pregunta, veamos la siguiente proposición que será de gran ayuda:

Proposición 4.6. Dado el homomorfismo de K-álgebras, entonces $\psi : \left(K_x^{((n))}, \langle x_1, ..., x_n \rangle\right) \longrightarrow \left(K_y^{((m))}, \langle y_1, ..., y_m \rangle\right)$ es continua.

Prueba.

Afirmación: $\psi(\langle x_1, ..., x_n \rangle) \subset \langle y_1, ..., y_m \rangle$.

En efecto, sea $h \in \psi(\langle x_1, ..., x_n \rangle)$, tenemos que existe un $f \in \langle x_1, ..., x_n \rangle$ tal que $\psi(f) = h$.

Ahora supongamos que $\psi(f) \notin \langle y_1, ..., y_m \rangle$, esto quiere decir que

$$\psi(f) = P_0 + P_1 + ... \in K_y^{((m))} \text{ con } P_0 \neq 0,$$

entonces $\psi(f) = c + g$, donde $c \in K \setminus \{0\}$ y $g \in \langle y_1, ..., y_m \rangle$.

Luego $\psi(f - c) = g$, donde g no es unidad en $K_y^{((m))}$.

Pero como $c \neq 0$ y $f \in \langle x_1, ..., x_n \rangle$, $f - c$ es unidad en $K_x^{((n))}$, por ende, $\psi(f - c)$ es unidad en $K_y^{((m))}$, lo cual es una contradicción.

Por lo tanto $h = \psi(f) \in \langle y_1, ..., y_m \rangle$, probando así la afirmación.

Veamos si ψ es continua. Dado $a \in K_x^{((n))}$ arbitrario.

Para cada $\psi(a) + \langle y_1, ..., y_m \rangle^l$ entorno de $\psi(a)$ escogemos un $a + \langle x_1, ..., x_n \rangle^l$ entorno de $a \in K_x^{((n))}$.

Para que ψ sea continua bastará con probar que

$$\psi(a + \langle x_1, ..., x_n \rangle^l) \subset \psi(a) + \langle y_1, ..., y_m \rangle^l.$$

Si $h \in \psi\big(a + \langle x_1, ..., x_n \rangle^l\big)$, entonces existe $f \in \langle x_1, ..., x_n \rangle^l$ tal que $h = \psi(a + f)$.

Luego por la afirmación, $\psi(f) \in \psi\left(\langle x_1, ..., x_n \rangle^l\right) \subset \langle y_1, ..., y_m \rangle^l$.

Por lo tanto $h = \psi(a) + \psi(f) \in \psi(a) + \langle y_1, ..., y_m \rangle^l$.

□

Proposición 4.7. Sean $\alpha_1, \alpha_2, ..., \alpha_n \in \langle y_1, ..., y_m \rangle$, entonces existe únicamente un homomorfismo de K-álgebras $\phi : K_x^{((n))} \longrightarrow K_y^{((m))}$ tal que $\phi(x_i) = \alpha_i$.

Prueba. Sea $f = \displaystyle\sum_{i=0}^{\infty} P_i \in K_x^{((n))}$. Definimos $f_q(\alpha_1, \alpha_2, ..., \alpha_n) = \displaystyle\sum_{i=0}^{q} P_i(\alpha_1, \alpha_2, ..., \alpha_n)$, para todo $q \in \mathbb{N}_0$.

Afirmación 1: $(f_q(\alpha_1, \alpha_2, ..., \alpha_n))_{q \in \mathbb{N}_0}$ es una sucesión de Cauchy en $\left(K_y^{((m))}, \langle y_1, ..., y_m \rangle\right)$.

En efecto, para cada $l \in \mathbb{N}_0$ escogemos el mismo $n_0 = l$.

Sea $r, q \geq n_0$, sin pérdida de generalidad ponemos $p \geq q \geq n_0$ $(q + 1 > l)$.

Luego $f_r(\alpha_1, \alpha_2, ..., \alpha_n) - f_q(\alpha_1, \alpha_2, ..., \alpha_n) = \displaystyle\sum_{i=q+1}^{r} P_i(\alpha_1, \alpha_2, ..., \alpha_n)$.

Como $Ord(\alpha_i) \geq 1$, entonces $Ord\left(P_i(\alpha_1, \alpha_2, ..., \alpha_n)\right) \geq i$, así,

$$Ord\left(\sum_{i=q+1}^{r} P_i(\alpha_1, \alpha_2, ..., \alpha_n)\right) \geq q + 1 > l.$$

Esto quiere decir que $f_r(\alpha_1, \alpha_2, ..., \alpha_n) - f_q(\alpha_1, \alpha_2, ..., \alpha_n) \in \langle y_1, ..., y_m \rangle^l$, probando de esta manera la afirmación.

Ya que $\left(K_y^{((m))}, \langle y_1, ..., y_m\rangle\right)$ es un espacio de Hausdorff completo (Ver la proposición 4.2 y 4.3), entonces la sucesión $(f_q(\alpha_1, \alpha_2, ..., \alpha_n))_{q\in\mathbb{N}_0}$ converge a un único elemento de $K_y^{((m))}$ que denotaremos

$$f(\alpha_1, \alpha_2, ..., \alpha_n) := \lim_{n\to\infty} f_q(\alpha_1, \alpha_2, ..., \alpha_n) = \lim_{q\to\infty} \sum_{i=0}^{q} P_i(\alpha_1, \alpha_2, ..., \alpha_n) \in K_y^{((m))}$$

Esto nos garantiza la definición de la aplicación

$$\begin{array}{rcl} \phi : K_x^{((n))} & \longrightarrow & K_y^{((m))} \\ f & \longmapsto & \phi(f) = f(\alpha_1, \alpha_2, ..., \alpha_n) \end{array}$$

Veamos si ϕ es un homomorfismo de K-álgebras con $\phi(x_i) = \alpha_i$.

(i) Si $f = k \in K$, $f_q(\alpha_1, \alpha_2, ..., \alpha_n) = k$, entonces

$$\phi(k) = \lim_{q\to\infty} f_q(\alpha_1, \alpha_2, ..., \alpha_n) = k.$$

(ii) Si $f = x_i \in K_x^{((n))}$, para todo $i = 1, ..., n$, entonces $\displaystyle\sum_{i=0}^{q} P_i = P_1 = x_i$.

Luego $f_q(\alpha_1, \alpha_2, ..., \alpha_n) = P_1(\alpha_1, \alpha_2, ..., \alpha_n) = \alpha_i$, así,

$$\phi(x_i) = \lim_{q\to\infty} f_q(\alpha_1, \alpha_2, ..., \alpha_n) = \alpha_i.$$

(iii) Sean $f = \displaystyle\sum_{i=0}^{\infty} P_i$, $g = \displaystyle\sum_{i=0}^{\infty} Q_i \in K_x^{((n))}$, entonces

$$\phi(f+g) = \lim_{q\to\infty} \sum_{i=0}^{q} (P_i + Q_i)(\alpha_1, \alpha_2, ..., \alpha_n)$$

$$\phi(f+g) = \lim_{q\to\infty} \left[\sum_{i=0}^{q} P_i(\alpha_1, \alpha_2, ..., \alpha_n) + \sum_{i=0}^{q} Q_i(\alpha_1, \alpha_2, ..., \alpha_n)\right]$$

$$\phi(f+g) = \lim_{q\to\infty} \sum_{i=0}^{q} P_i(\alpha_1, \alpha_2, ..., \alpha_n) + \lim_{q\to\infty} \sum_{i=0}^{q} Q_i(\alpha_1, \alpha_2, ..., \alpha_n)$$

$$\phi(f+g) = \phi(f) + \phi(g).$$

(iv) Por otro lado, como $fg = \displaystyle\sum_{i=0}^{\infty} h_i$, donde $h_i = \displaystyle\sum_{r+s=i} P_r q_s$, entonces,

$$(fg)_q(\alpha_1, \alpha_2, ..., \alpha_n) = \sum_{i=0}^{q} h_i(\alpha_1, \alpha_2, ..., \alpha_n).$$

Luego,

$$[f_q(\alpha_1, \alpha_2, ..., \alpha_n)][g_q(\alpha_1, \alpha_2, ..., \alpha_n)] = \left[\sum_{i=0}^{q} P_i(\alpha_1, \alpha_2, ..., \alpha_n)\right]\left[\sum_{i=0}^{q} Q_i(\alpha_1, \alpha_2, ..., \alpha_n)\right]$$

$$[f_q(\alpha_1,\alpha_2,...,\alpha_n)][g_q(\alpha_1,\alpha_2,...,\alpha_n)] = \sum_{i=0}^{2q} h_i(\alpha_1,\alpha_2,...,\alpha_n)$$
$$[f_q(\alpha_1,\alpha_2,...,\alpha_n)][g_q(\alpha_1,\alpha_2,...,\alpha_n)] = \sum_{i=0}^{q} h_i(\alpha_1,\alpha_2,...,\alpha_n) + \sum_{i=q+1}^{2q} h_i(\alpha_1,\alpha_2,...,\alpha_n)$$
$$[f_q(\alpha_1,\alpha_2,...,\alpha_n)][g_q(\alpha_1,\alpha_2,...,\alpha_n)] = (fg)_q(\alpha_1,\alpha_2,...,\alpha_n) + \sum_{i=q+1}^{2q} h_i(\alpha_1,\alpha_2,...,\alpha_n).$$

Afirmación 2: $\lim\limits_{q\to\infty} \sum\limits_{i=q+1}^{2q} h_i(\alpha_1,\alpha_2,...,\alpha_n) = 0$ en $\left(K_y^{((m))}, \langle y_1,...,y_m\rangle\right)$.

En efecto, para cada $l \in \mathbb{N}$ escogemos el mismo $n_0 = l$.

Sea $q \geq n_0$ ($q+1 > l$).

Ya que $Ord(\alpha_i) \geq i$, para todo $i = 1,...,n$, entonces $Ord(h_i(\alpha_1,\alpha_2,...,\alpha_n)) \geq i$, así,

$$Ord\left(\sum_{i=q+1}^{2q} h_i(\alpha_1,\alpha_2,...,\alpha_n)\right) \geq q+1 > l.$$

Luego $\sum\limits_{i=q+1}^{2q} h_i(\alpha_1,\alpha_2,...,\alpha_n) \in \langle y_1,...,y_m\rangle^l$, probando así la afirmación.

De esta afirmación concluimos:

$\phi(fg) = \lim\limits_{q\to\infty} (fg)_q(\alpha_1,\alpha_2,...,\alpha_n) = \left[\lim\limits_{q\to\infty} f_q(\alpha_1,\alpha_2,...,\alpha_n)\right]\left[\lim\limits_{q\to\infty} g_q(\alpha_1,\alpha_2,...,\alpha_n)\right]$

$\phi(fg) = \phi(f)\phi(g)$.

(iv) ϕ es único:

Supongamos que existe otro homomorfismo de K-álgebras ψ tal que $\psi(x_i) = \alpha_i$, para todo $i = 1,...,n$.

Dado $f = \sum\limits_{i=0}^{\infty} P_i \in K_x^{((n))}$. Para cada $l \in \mathbb{N}$, si $q \geq l$,

$Ord\left(f - \sum\limits_{i=0}^{q} P_i\right) = Ord\left(\sum\limits_{i=q+1}^{\infty} P_i\right) \geq q+1 > l$, entonces $f = \lim\limits_{q\to\infty} \sum\limits_{i=0}^{q} P_i$.

Sabemos de la proposición 4.6 que ψ es continua, luego

$\psi(f) = \lim\limits_{q\to\infty} \psi\left(\sum\limits_{i=0}^{q} P_i\right) = \lim\limits_{q\to\infty} \sum\limits_{i=0}^{q} P_i(\alpha_1,\alpha_2,...,\alpha_n) = \lim\limits_{q\to\infty} f_q(\alpha_1,\alpha_2,...,\alpha_n)$.

Como $\phi(f) = \lim\limits_{q\to\infty} f_q(\alpha_1,\alpha_2,...,\alpha_n) \in K_y^{((m))}$ y este limite es único por ser $\left(K_y^{((m))}, \langle y_1,...,y_m\rangle\right)$ de Hausdorff, tenemos $\psi(f) = \phi(f)$.

Por lo tanto $\psi = \phi$.

$\square$

Observación 4.5.

(i) Cuando este tipo de homomorfismo de K-álgebras ϕ es único lo denotaremos de la forma $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$.

(ii) La proposición 4.7 nos responde a la pregunta de inicio que para poder sustituir en una serie formal arbitraria

$$f(x_1,...,x_n) = \sum_{i=0}^{\infty} P_i(x_1,...,x_n) \in K_x^{((n))}$$

las indeterminadas $x_1,...,x_n$ por las series formales $\alpha_1,\alpha_2,...,\alpha_n \in K_y^{((m))}$ deberán de cumplir la condición que estas estén en el ideal de maximal $K_y^{((m))}$.

- La siguiente Proposición nos dice que todo homomorfismo de K-álgebras de $K_x^{((n))}$ en $K_y^{((m))}$ son del tipo $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$, para algunos $\alpha_1,\alpha_2,...,\alpha_n \in \langle y_1,...,y_m\rangle$.

Proposición 4.8. Si $\psi : K_x^{((n))} \longrightarrow K_y^{((m))}$ es un homomorfismo de K-álgebras, entonces existen $\alpha_1,\alpha_2,...,\alpha_n \in \langle y_1,...,y_m\rangle$ tal que $\psi = \phi_{\alpha_1,\alpha_2,...,\alpha_n}$.

Prueba. Ya que $x_i \in \langle x_1,...,x_n\rangle$, para todo $i = 1,...,n$, elegimos $\alpha_i = \psi(x_i)$.
Luego por la afirmación de la proposición 4.6, $\alpha_i \in \psi(\langle x_1,...,x_n\rangle) \subset \langle y_1,...,y_m\rangle$.

Ahora bastará probar que para cada $f \in K_x^{((n))}$, $\psi(f) = \phi_{\alpha_1,\alpha_2,...,\alpha_n}(f)$.

Sea $f = \sum_{i=0}^{\infty} P_i = \lim_{q\to\infty} \sum_{i=0}^{q} P_i$. Luego por la continuidad de ψ tenemos

$$\psi(f) = \lim_{q\to\infty} \psi\left(\sum_{i=0}^{q} P_i\right) = \lim_{q\to\infty} \sum_{i=0}^{q} \psi(P_i) = \lim_{q\to\infty} \sum_{i=0}^{q} P_i(\alpha_1,\alpha_2,...,\alpha_n)$$

Como $\left(K_y^{((m))}, \langle y_1,...,y_m\rangle\right)$ es un espacio de Hausdorff, este límite es único.
Por lo tanto $\psi(f) = \phi_{\alpha_1,\alpha_2,...,\alpha_n}(f)$.

□

Proposición 4.9. Sea $f \in K_x^{((n))}$ y $\alpha_1,\alpha_2,...,\alpha_n \in \langle y_1,...,y_m\rangle$, entonces

$$Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f)) \geq Ord(f). \min_{1\leq i\leq n}\{Ord(\alpha_i)\}.$$

Prueba. Sea $Ord(f) = v$, entonces $f = P_v + P_{v+1} + ...$, donde $P_v \neq 0$ y

$$P_i = \sum_{i_1+...+i_n=i} a_{i_1,...,i_n} x_1^{i_1} ... x_n^{i_n}, \text{ para todo } i = v, v+1, ...$$

Luego,

$Ord(P_i(\alpha_1, \alpha_2, ..., \alpha_n)) \geq min\{ Ord(\alpha_1^{i_1} ... \alpha_n^{i_n}) \,/\, i_1 + ... + i_n = i \}$

$Ord(P_i(\alpha_1, \alpha_2, ..., \alpha_n)) \geq min\left\{ \sum_{j=1}^{n} i_j Ord(\alpha_j) \,/\, i_1 + ... + i_n = i \right\}$

Como $\sum_{j=1}^{n} i_j Ord(\alpha_j) \geq (i_1 + ... + i_n) \min_{1\leq j\leq n} \{Ord(\alpha_j)\}$, entonces

$min\left\{ \sum_{j=1}^{n} i_j Ord(\alpha_j) \,/\, i_1 + ... + i_n = i \right\} \geq i. \min_{1\leq j\leq n} \{Ord(\alpha_j)\}$

$Ord(P_i(\alpha_1, \alpha_2, ..., \alpha_n)) \geq v. \min_{1\leq j\leq n} \{Ord(\alpha_j)\}$, para todo $i = v, v+1, ...$

Así, $Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f)) \geq \min_{i\geq v} \{Ord(P_i(\alpha_1, \alpha_2, ..., \alpha_n))\} \geq v. \min_{1\leq j\leq n} \{Ord(\alpha_j)\}$.

□

- De esta proposición deducimos:

$$Ord(f) \leq Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f))$$

4.3. Isomorfismos de K-álgebras

Proposición 4.10. Si $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es un K-isomorfismo de $K_x^{((n))}$ en $K_y^{((m))}$, entonces $Ord(f) = Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f))$, para todo $f \in K_x^{((n))}$.

Prueba. Ya que $T = \phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es K-isomorfismo, entonces existe un homomorfismo de K-álgebras $T^{-1} : K_y^{((m))} \longrightarrow K_x^{((n))}$ tal que $T \, o \, T^{-1} = Id$.

Además, $T(f) \in K_y^{((m))}$, luego por la proposición 4.9,

$$Ord(T(f)) \leq Ord(T^{-1}(T(f))) = Ord(f) \leq Ord(T(f)).$$

□

- Recordemos que si V es un espacio vectorial sobre K y $v_1, v_2, ..., v_n \in V$ son K-linealmente independiente sobre V, escribiremos abreviadamente que $v_1, v_2, ..., v_n$ son K-$L.I$ sobre V o simplemente K-$L.I$ si no hay confusión.

Proposición 4.11. Sean $\alpha_1, \alpha_2, ..., \alpha_n \in \langle y_1, ..., y_m \rangle$, $\phi_{\alpha_1,\alpha_2,...,\alpha_n} : K_x^{((n))} \longrightarrow K_y^{((m))}$ el homomorfismo de K-álgebras y $L_1, L_2, ..., L_n$ las formas lineales de $\alpha_1, \alpha_2, ..., \alpha_n$ respectivamente.
Si $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es un K-isomorfismo, entonces $L_1, L_2, ..., L_n$ son K-$L.I$ sobre $K_y^{((m))}$.

Prueba. Ya que $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es K-isomorfismo entonces

$$Ord(\alpha_i) = Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n(x_i)}) = Ord(x_i) = 1, \text{ para todo } i = 1, ..., n.$$

Luego $\alpha_i = L_i + \beta_i$, donde $L_i \neq 0$ y $Ord(\beta_i) \geq 2$, para todo $i = 1, ..., n$.

Supongamos que $L_1, L_2, ..., L_n$ son K linealmente dependiente (No trivial).

Tenemos que existe algún $a_{i_0} \neq 0$ tal que

$$a_1L_1 + a_2L_2 + ... + a_nL_n = 0, \quad \text{donde } a_i \in K \tag{4.3.1}$$

Si escogemos la serie formal $f = a_1x_1 + a_2x_2 + ... + a_nx_n \in K_x^{((n))}$ y como $a_{i_0} \neq 0$, entonces $Ord(f) = 1$.

Además, $\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f) = a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n$

$\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f) = a_1(L_1 + \beta_1) + a_2(L_2 + \beta_2) + ... + a_n(L_n + \beta_n)$, con $Ord(\beta_i) \geq 2$

$\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f) = a_1L_1 + a_2L_2 + ... + a_nL_n + g$, donde $Ord(g) \geq 2$.

Luego de (4.3.1), $\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f) = g$. Así, $Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f)) \geq 2 > 1 = Ord(f)$.

De la proposición 4.10 tenemos que $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ no es un K-isomorfismo, lo cual es una contradicción.

Por lo tanto, $L_1, L_2, ..., L_n$ son K-L.I sobre $K_y^{((m))}$.

□

- Recordemos que si V es un K-$e.v$, con $S = \{v_1, v_2, ..., v_m\} \subset V$ y $S' = \{u_1, u_2, ..., u_n\} \subset \mathcal{L}(S)$, donde $\mathcal{L}(S)$ representa el subespacio vectorial de V generado por S. Si S' es K-$L.I$, entonces, $n \leq m$.

- Por ejemplo, si tenemos a $K_y^{((m))}$ como un K-$e.v$, el ideal $\langle y_1, ..., y_m \rangle$ se puede ver como un subespacio vectorial de $K_y^{((m))}$ generado por $S = \{y_1, ..., y_m\}$, pues, para todo $\lambda \in K, f, g \in K_y^{((m))}$, $\lambda f, f + g \in K_y^{((m))}$.

Luego si $u_1, u_2, ..., u_n \in \langle y_1, ..., y_m \rangle$ son vectores K-$L.I$, entonces $n \leq m$.

- Este ejemplo nos servirá de apoyo para poder probar la siguiente proposición:

Proposición 4.12. Si $\phi_{\alpha_1,\alpha_2,...,\alpha_n} : K_x^{((n))} \longrightarrow K_y^{((m))}$ es un K-isomorfismo, entonces $n = m$.

Prueba. Tenemos que $Ord(\alpha_i) = Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n}(x_i)) = Ord(x_i) = 1,$ para todo $i = 1, ..., n$.

Luego las formas iniciales de α_i son

$L_i = a_{i1}y_1 + a_{i2}y_2 + ... + a_{im}y_m \in \langle y_1, ..., y_m\rangle,$ para todo $i = 1, ..., n$.

Ya que $L_1, L_2, ..., L_n$ son K-$L.I$ sobre $K_y^{((m))}$, entonces $m \leq n$.

Como $\phi^{-1}_{\alpha_1,\alpha_2,...,\alpha_n} : K_y^{((m))} \longrightarrow K_x^{((n))}$ es también un K-isomorfismo, obtenemos de forma análoga que $n \leq m$.

Por lo tanto $n = m$.

□

Proposición 4.13. Dado un homomorfismo de K-álgebras $T : K_x^{((n))} \longrightarrow K_y^{((m))}$.
Si existe un homomorfismo de de K-álgebras $\psi : K_y^{((m))} \longrightarrow K_x^{((n))}$ tal que

$$\psi o T(x_i) = x_i, \text{ para todo } i = 1, ..., n.$$
$$T o \psi(y_j) = y_j, \text{ para todo } j = 1, ..., m.$$

Entonces T es K-isomorfismo.

Prueba. Dados $f = \sum_{i=0}^{\infty} P_i(x_1, ..., x_n) = \lim_{q\to\infty} \sum_{i=0}^{q} P_i(x_1, ..., x_n) \in K_x^{((n))}$ y
$g = \sum_{i=0}^{\infty} Q_i(y_1, ..., y_m) = \lim_{q\to\infty} \sum_{i=0}^{q} Q_i(y_1, ..., y_m) \in K_y^{((m))}$.

Por la proposición 4.6 tenemos que ψ y T son continuas, luego por las propiedades de continuidad, $\psi\, o\, T$ y $T\, o\, \psi$ son continuas, entonces

$$(\psi\, o\, T)(f) = \lim_{q\to\infty} (\psi\, o\, T)\left(\sum_{i=0}^{q} P_i(x_1, ..., x_n)\right) = \lim_{q\to\infty} \sum_{i=0}^{q} P_i(\psi\, o\, T(x_1), ..., \psi\, o\, T(x_n))$$
$$(\psi\, o\, T)(f) = \sum_{i=0}^{\infty} P_i(x_1, ..., x_n) = f.$$

Por otro lado,
$$(T\, o\, \psi)(g) = \lim_{q\to\infty} (T\, o\, \psi)\left(\sum_{i=0}^{q} Q_i(y_1, ..., y_m)\right) = \lim_{q\to\infty} \sum_{i=0}^{q} Q_i(T\, o\, \psi(y_1), ..., T\, o\, \psi(y_m))$$
$$(\psi\, o\, T)(g) = \sum_{i=0}^{\infty} Q_i(y_1, ..., y_m) = g.$$

Por lo tanto, T es un K-isomorfimo.

$\square$

- En las siguientes proposiciones asumiremos que $m = n$.

Proposición 4.14. Sea $L_i = a_{i1}y_1 + a_{i2}y_1 + ... + a_{in}y_n \in K_y^{((n))}$, para todo $i = 1, ..., n$, entonces $L_1, L_2, ..., L_n$ son K-$L.I$ sobre $K_y^{((n))}$ si y solo si $Det(a_{ij})_{n\times n} \neq 0$.

Prueba. De la hipótesis tenemos

$$\begin{array}{rcl} L_1 = & a_{11}y_1 \ + \ a_{12}y_2 \ + \ ... \ + \ a_{1n}y_n \\ L_2 = & a_{21}y_1 \ + \ a_{22}y_2 \ + \ ... + \ a_{2n}y_n \\ & \vdots \\ L_n = & a_{n1}y_1 \ + \ a_{n2}y_2 \ + \ ... \ + \ a_{nn}y_n \end{array}$$

Luego

$$\begin{bmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{bmatrix} = A. \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}, \text{ donde } A = (a_{ij}) \in K^{n\times n}$$

Primero supondremos que $L_1, L_2, ..., L_n$ son K-$L.I.$ en $K_y^{((n))}$.

Dado el sistema de ecuaciones con incógnitas $\lambda_1, \lambda_2, ..., \lambda_n \in K$

$$(\sigma) \begin{cases} a_{11}\lambda_1 \ + \ a_{21}\lambda_2 \ + \ ... \ + \ a_{n1}\lambda_n = 0 \\ a_{12}\lambda_1 \ + \ a_{22}\lambda_2 \ + \ ... \ + \ a_{n2}\lambda_n = 0 \\ \vdots \\ a_{1n}\lambda_1 \ + \ a_{2n}\lambda_2 \ + \ ... \ + \ a_{nn}\lambda_n = 0 \end{cases}$$

Este sistema (σ) lo podemos escribir de la siguiente forma

$$A^t. \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \text{ entonces } \left[A^t. \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix} \right]^t = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}^t$$

$$\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix}^t .A = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}^t, \text{ entonces } \begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{bmatrix} .A = \begin{bmatrix} 0 & 0 & \cdots & 0 \end{bmatrix}$$

Luego,

$$\begin{bmatrix} \lambda_1 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{bmatrix} = \begin{bmatrix} \lambda_1 & \cdots & \lambda_n \end{bmatrix} A \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = 0$$

Así tenemos, $\lambda_1 L_1 + \lambda_2 L_2 + ... + \lambda_n L_n = 0$ y como $L_1, L_2, ..., L_n$ son K-$L.I.$ en $K_y^{((n))}$ entonces $\lambda_i = 0$, para todo $i = 1, ..., n$, que es la única solución del sistema (σ).

Por lo tanto $Det(A) = Det(A^t) \neq 0$.

Recíprocamente, ahora supongamos que $Det(A) \neq 0$ y si se cumple:

$$\begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{bmatrix} = 0, \text{ donde } \lambda_1, \lambda_2, ..., \lambda_n \in K.$$

Probaremos que $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$. Tenemos

$$\begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{bmatrix} A \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = 0, \quad \text{entonces} \quad \begin{bmatrix} b_1 & b_2 & \cdots & b_n \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = 0,$$

donde $\begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{bmatrix} A = \begin{bmatrix} b_1 & b_2 & \cdots & b_n \end{bmatrix}$. $(b_i \in K)$

Luego $b_1 y_1 + b_2 y_2 + ... + b_n y_n = 0$, entonces $b_1 = b_2 = ... = b_n = 0$.

Por consiguiente, $\begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{bmatrix} A = \begin{bmatrix} 0 & 0 & \cdots & 0 \end{bmatrix}$.

De esta manera nos queda el siguiente sistema de ecuaciones:

$$(\beta) \begin{cases} a_{11}\lambda_1 + a_{21}\lambda_2 + ... + a_{n1}\lambda_n = 0 \\ a_{12}\lambda_1 + a_{22}\lambda_2 + ... + a_{n2}\lambda_n = 0 \\ \vdots \\ a_{1n}\lambda_1 + a_{2n}\lambda_2 + ... + a_{nn}\lambda_n = 0 \end{cases}$$

que también lo podemos representar de forma matricial como

$$A^t \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \text{ y además, de hipótesis, } Det(A^t) = Det(A) \neq 0.$$

Entonces (β) tiene solución única y es $\lambda_i = 0$, para todo $i = 1, ..., n$.

Por lo tanto $L_1, L_2, ..., L_n$ son K-L.I. sobre $K_y^{((n))}$.

□

Observación 4.6. Si $Det(A) \neq 0$, entonces A tiene en sus matrices filas y columnas elementos no nulos. Esto quiere decir que si las formas lineales $L_1, L_2, ..., L_n$ son K-$L.I$ sobre $K_y^{((n))}$, entonces $L_i \neq 0$, para todo $i = 1, ..., n$ y por lo tanto $Ord(L_i) = 1$.

Proposición 4.15. Sean $L_1, L_2, ..., L_n$ formas lineales en $K_y^{((n))}$ que son K-$L.I$, entonces $\phi_{L_1, L_2, ..., L_n} : K_x^{((n))} \longrightarrow K_y^{((n))}$ es un K-isomorfismo.

Prueba. Como las formas lineales $L_1, L_2, ..., L_n$ son K-$L.I$ sobre $K_y^{((n))}$, tenemos que

$$Ord(\phi_{L_1, L_2, ..., L_n}(x_i)) = Ord(L_i) = 1, \text{ para todo } i = 1, ..., n.$$

Es decir, cada forma lineal L_i se puede representar de la siguiente manera

$$\begin{aligned} L_1 &= a_{11}y_1 + a_{12}y_2 + ... + a_{1n}y_n \\ L_2 &= a_{21}y_1 + a_{22}y_2 + ... + a_{2n}y_n \\ &\vdots \\ L_n &= a_{n1}y_1 + a_{n2}y_2 + ... + a_{nn}y_n \end{aligned}$$

donde en cada L_i existe al menos un $a_{ij} \neq 0$.

De estas formas lineales, tenemos la siguiente matriz de sus coeficientes $M = (a_{ij}) \in K^{n \times n}$ que además por ser $L_1, L_2, ..., L_n$ K-$L.I$, la proposición 4.14 nos dice que $Det(M) \neq 0$.

Luego existe una matriz no nula $M^{-1} = (b_{ij}) \in K^{n \times n}$ tal que $M^{-1}.M = M.M^{-1} = I$ (M es invertible).

Además, $Det(M^{-1}) = \frac{1}{Det(M)} \neq 0$, entonces la matriz M^{-1} tiene en sus matrices filas y columnas elementos no nulos.

Esto garantiza la existencia de las formas lineales

$$\begin{aligned} L'_1 &= b_{11}x_1 + b_{12}x_2 + ... + b_{1n}x_n \\ L'_2 &= b_{21}x_1 + b_{22}x_2 + ... + b_{2n}x_n \\ &\vdots \\ L'_n &= b_{n1}x_1 + b_{n2}x_2 + ... + b_{nn}x_n \end{aligned}$$

donde en cada L'_i existe al menos un $b_{ij} \neq 0$, es decir que $Ord(L'_i) = 1$, para todo $i = 1, ..., n$.

Como $L'_1, L'_2, ..., L'_n \in \langle x_1, ..., x_n \rangle$, entonces existe un homomorfismo de K-álgebras $\psi_{L'_1, L'_2, ..., L'_n} : K_y^{((n))} \longrightarrow K_x^{((n))}$ tal que $\psi_{L'_1, L'_2, ..., L'_n}(y_i) = L'_i$, para todo $i = 1, ..., n$.

Denotaremos $T = \phi_{L_1,L_2,...,L_n}$ y $T' = \psi_{L'_1,L'_2,...,L'_n}$. Por la proposición 4.13 para que T sea un K-isomorfismo bastará con probar que $(T' \, o \, T)(x_i) = x_i$ y $(T \, o \, T')(y_i) = y_i$, para todo $i = 1, ..., n$.

Dado $1 \leq i \leq n$.

$T'(T(x_i)) = T'(L_i) = T'(a_{i1}y_1 + a_{i2}y_2 + ... + a_{in}y_n) = a_{i1}L'_1 + a_{i2}L'_2 + ... + a_{in}L'_n$

$T'(T(x_i)) = a_{i1}(b_{11}x_1 + ... + b_{1n}x_n) + a_{i2}(b_{21}x_1 + ... + b_{2n}x_n) + ... + a_{in}(b_{n1}x_1 + ... + b_{nn}x_n)$

$$T'(T(x_i))=\left(\sum_{k=1}^{n} a_{ik}b_{k1}\right)x_1+...+\left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)x_j+...+\left(\sum_{k=1}^{n} a_{ik}b_{ki}\right)x_i+...+\left(\sum_{k=1}^{n} a_{ik}b_{kn}\right)x_n.$$

Como $M.M^{-1} = I$, entonces tenemos

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Luego $T'(T(x_i)) = 0.x_1 + ... + 0.x_j + ... + 1.x_i + ... + 0.x_n = x_i$.

Análogamente usando $M^{-1}.M = I$ obtenemos $T(T'(y_i)) = y_i$.

Por lo tanto $T = \phi_{L_1,L_2,...,L_n}$ es K-isomorfismo.

$\square$

Lema 4.1. Sea A un subanillo de $K_x^{((n))}$. A es denso en $K_x^{((n))}$ si y solo si para cada polinomio $P \in K[x_1, x_2, ..., x_n]$ homogéneo, existe una serie de potencias formal $f \in A$ tal que P es forma inicial de f.

Prueba. Dado un polinomio homogéneo arbitrario $P \in K[x_1, x_2, ..., x_n]$ de grado d.

Ya que A es denso en $K_x^{((n))}$, entonces $P \in K_x^{((n))} = \overline{A}$, es decir que existe una sucesión $(f_q)_{q \in \mathbb{N}}$ de A tal que $\lim_{q \to \infty} f_q = P$.

Tomando $d + 1 > 0$, tenemos que existe $q_0 \in \mathbb{N}$ tal que para todo $q \geq q_0$,
$f_q - P \in \langle x_1, ..., x_n \rangle^{d+1}$.

En particular $f_{q_0} \in A$ tal que $Ord(f_{q_0} - P) \geq d + 1$.

Si $f_{q_0} - P = 0$, el resultado es inmediato.

Si $f_{q_0} - P \neq 0$, existe $m \geq d + 1$ tal que $f_{q_0} - P = Q_m + Q_{m+1} + ...$, donde Q_i son polinomios homogéneos de grado i y $Q_m \neq 0$.

$f_{q_0} = P + Q_m + Q_{m+1} + ...$ y como $grad(P) = d < d + 1 \leq m$,
P es la forma inicial de f.

Por lo tanto existe un $f = f_{q_0} \in A$ donde P es su forma inicial.

RecÍprocamente, dado $f \in K_x^{((n))}$, para que A sea denso en $K_x^{((n))}$, bastará con demostrar que $f \in \overline{A}$.

Si $f = 0$, el resultado es inmediato. Supongamos ahora que $f \neq 0$.

Afirmación: Para todo $q \in \mathbb{N}$, existe $f_q \in A$ tal que $Ord(f - f_q) \geq q$.

En efecto, probaremos esta afirmación por inducción.

Si $q=1$, existe un $m \in \mathbb{N}_0$ tal que $f = P_m + P_{m+1} + ...$, donde P_i son polinomios homogéneos de grado i y $P_m \neq 0$.

Como P_m es un polinomio homogéneo, de la hipótesis tenemos que existe un $f_1 \in A$ tal que P_m es su forma inicial.

Luego $f - f_1 = Q_{m+1} + Q_{m+2} + ...$, donde $Q_i = 0$ ó Q_i es polinomio homogéneo de grado i. Así $Ord(f - f_1) \geq m + 1 \geq 1$.

Supongamos que la afirmación se cumple para $q \in \mathbb{N}$, es decir que existe un $f_q \in A$ tal que $Ord(f - f_q) \geq q$. (Hipótesis Inductiva).

Veamos si se cumple para $q + 1$.

Si $f - f_q = 0$, la prueba de la afirmación es inmediata.

Si $f - f_q \neq 0$, existe $m \geq q$ tal que $f - f_q = G_m + G_{m+1} + ...$, donde G_i son polinomios homogéneos de grado i y $G_m \neq 0$.

Luego de la hipótesis tenemos que existe un $h_q \in A$ tal que G_m es su forma inicial.

Escogiendo un $f_{q+1} = f_q + h_q \in A$ tenemos:

$f - f_{q+1} = (f - f_q) - h_q = H_{m+1} + H_{m+2} + ...$, donde $H_i = 0$ ó H_i es polinomio homogéneo de grado i.

AsÍ $Ord(f - f_{q+1}) \geq m + 1 \geq q + 1$, probando de esta manera la afirmación.

Esta afirmación quiere decir que existe una sucesión $(f_q)_{q \in \mathbb{N}}$ de A tal que para todo $q \in \mathbb{N}$, $f - f_q \in \langle x_1, ..., x_n \rangle^q$, es decir, $\lim\limits_{q \to \infty} f_q = f$.

Por lo tanto $f \in \overline{A}$.

$\square$

- En particular $K[x_1, x_2, ..., x_n]$ es denso en $K_x^{((n))}$

Teorema 4.1. Sean $\alpha_1, \alpha_2, ..., \alpha_n \in \langle y_1, y_2, ..., y_n \rangle$ con sus formas lineales respectivas $L_1, L_2, ..., L_n$ K-$L.I$ sobre $K_y^{((n))}$, entonces $\phi_{\alpha_1, \alpha_2, ..., \alpha_n} \colon K_x^{((n))} \longrightarrow K_y^{((n))}$ es un K-isomorfismo.

Prueba. De la hipótesis tenemos, $Ord(\alpha_i) \geq 1$, para todo $i = 1, ..., n$, entonces

$$\alpha_i = L_i + \beta_i, \text{ con } Ord(\beta_i) \geq 2, \text{ para todo } i = 1, ..., n.$$

Ya que $L_1, L_2, ..., L_n$ son K-$L.I$, por la observación 4.6 se cumple
$Ord(L_i) = grad(L_i) = 1$. ($L_i \neq 0$)

Luego $Ord(\alpha_i) = 1$ para todo $i = 1, ..., n$. Además por la proposición 4.15,
$\phi_{L_1,L_2,...,L_n} : K_x^{((n))} \longrightarrow K_y^{((n))}$ es un K-isomorfismo.

(i) Probaremos que $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es inyectiva, para esto es suficiente con probar que $Nu(\phi_{\alpha_1,\alpha_2,...,\alpha_n}) \subset \{0\}$.

Dado $f \in K_x^{((n))} \setminus \{0\}$, debemos probar que $\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f) \neq 0$.

Como $f \neq 0$, $f = P_r + P_{r+1} + P_{r+2} + ...$, donde $P_r \neq 0$.

Esta serie formal lo escribiremos de la forma $f = P_r + h$, donde $P_r \neq 0$ y $Ord(h) \geq r + 1$.

Luego:
$\phi_{\alpha_1,...,\alpha_n}(f) = \phi_{\alpha_1,...,\alpha_n}(P_r) + \phi_{\alpha_1,...,\alpha_n}(h)$, con $Ord(\phi_{\alpha_1,...,\alpha_n}(h)) \geq Ord(h) \geq r + 1$

Ahora analicemos el orden de $\phi_{\alpha_1,...,\alpha_n}(P_r)$, veamos

$$\phi_{\alpha_1,...,\alpha_n}(P_r) = P_r(\alpha_1, \alpha_2, ..., \alpha_n) = \sum_{i_1+...+i_n=r} a_{i_1,...,i_n} \alpha_1^{i_1} ... \alpha_n^{i_n}$$

$$\phi_{\alpha_1,...,\alpha_n}(P_r) = \sum_{i_1+...+i_n=r} a_{i_1,...,i_n} (L_1 + \beta_1)^{i_1} ... (L_n + \beta_n)^{i_n}, \text{ con } Ord(\beta_i) \geq 2$$

$$\phi_{\alpha_1,...,\alpha_n}(P_r) = \sum_{i_1+...+i_n=r} a_{i_1,...,i_n} (L_1^{i_1} + \theta_1) ... (L_n^{i_n} + \theta_n), \text{ con } Ord(\theta_i) \geq i_j$$

$$\phi_{\alpha_1,...,\alpha_n}(P_r) = \sum_{i_1+...+i_n=r} a_{i_1,...,i_n} (L_1^{i_1} ... L_n^{i_n} + z_{i_1,...,i_n}), \text{ con } Ord(z_{i_1,...,i_n}) > r$$

$$\phi_{\alpha_1,...,\alpha_n}(P_r) = \phi_{L_1,...,L_n}(P_r) + Z, \text{ con } Ord(Z) > r.$$

Por consiguiente,

$$\phi_{\alpha_1,...,\alpha_n}(f) = \phi_{L_1,...,L_n}(P_r) + Z + \phi_{\alpha_1,...,\alpha_n}(h) = \phi_{L_1,...,L_n}(P_r) + W, \text{ con } Ord(W) > r.$$

Como $\phi^{-1}_{L_1,...,L_n}(\phi_{L_1,...,L_n}(P_r)) = P_r \neq 0$, entonces $\phi_{L_1,...,L_n}(P_r) \neq 0$.

También, al ser $L_1, ..., L_n$ polinomios lineales homogéneos, $\phi_{L_1,...,L_n}(P_r)$ es un polinomio homogéneo. Luego,

$$grad(\phi_{L_1,...,L_n}(P_r)) = Max \left\{ grad(L_1^{i_1} ... L_n^{i_n}) \,/\, i_1 + ... + i_n = r \right\}$$

$$grad(\phi_{L_1,...,L_n}(P_r)) = Max \left\{ \sum_{j=1}^{n} i_j \, grad(L_j) \,/\, i_1 + ... + i_n = r \right\} = r.$$

AsÍ, $Ord(\phi_{L_1,...,L_n}(P_r)) = r < Ord(W)$, entonces

$$Ord(\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f)) = min\{ Ord(\phi_{L_1,...,L_n}(P_r)), Ord(W) \} = r.$$

Esto quiere decir que $\phi_{\alpha_1,\alpha_2,...,\alpha_n}(f) \neq 0$. Por lo tanto $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es inyectiva.

De esta prueba de inyectividad tenemos que para cualquier $f \in K_x^{((n))}$,

$$Ord\left(\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f)\right) = Ord(f) \tag{4.3.2}$$

la cual nos servirá para probar la sobreyectividad de $\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}$.

(ii) Denotaremos, $A = \phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}\Big(K_x^{((n))}\Big)$.

Dado $f \in K[y_1, y_2, \ldots, y_n]$ un polinomio homogéneo arbitrario.

De forma análoga como en la prueba de inyectividad obtenemos que $Q = \phi^{-1}_{L_1,L_2,\ldots,L_n}(P)$ es un polinomio homogéneo en $K[x_1, x_2, \ldots, x_n]$ y también

$$\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(Q) = \phi_{L_1,L_2,\ldots,L_n}(Q) + F = P + F, \text{ con } Ord(P) < Ord(F) \text{ y } P \neq 0.$$

AsÍ tenemos que $\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(Q) \in A$ donde $P = \phi_{L_1,L_2,\ldots,L_n}(Q)$ es su forma inicial.

Luego por el lema 4.1, A es denso en $K_y^{((n))}$, es decir, $\overline{A} = K_y^{((n))}$.

Afirmación: A es cerrado en $K_y^{((n))}$.

En efecto, dado $h \in \overline{A}$, entonces existe una sucesión en A, $(\,\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f_i)\,)_{i\,\in\,\mathbb{N}_0}$ tal que $\lim\limits_{i\to\,\infty} \phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f_i) = h \in K_y^{((n))}$.

Por consiguiente $(\,\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f_i)\,)_{i\,\in\,\mathbb{N}}$ es una sucesión de Cauchy en $\Big(K_y^{((n))}, \langle y_1, \ldots, y_n\rangle\Big)$.

Esto quiere decir que para cada $q \in \mathbb{N}$, existe un $n_0 \in \mathbb{N}$ tal que si $i, j > n_0$,

$$\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f_i - f_j) = \phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f_i) - \phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f_j) \in \langle y_1, \ldots, y_n\rangle^q.$$

Luego por (4.3.2), $Ord(f_i - f_j) = Ord(\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}(f_i - f_j)) \geq q$, asÍ $f_i - f_j \in \langle x_1, \ldots, x_n\rangle^q$.

Entonces $(f_i)_{i\in\mathbb{N}}$ es una sucesión de Cauchy en $\Big(K_x^{((n))}, \langle x_1, \ldots, x_n\rangle\Big)$ y como este espacio es de Hausdorff y completo, existe unicamente una serie formal $f \in K_x^{((n))}$ tal que $\lim\limits_{i\to\,\infty} f_i = f$.

Por la continuidad de $\phi_{\alpha_1,\ldots,\alpha_n}$ tenemos $\lim\limits_{i\to\,\infty} \phi_{\alpha_1,\ldots,\alpha_n}(f_i) = \phi_{\alpha_1,\ldots,\alpha_n}(f) \in A$.

Pero $\lim\limits_{i\to\,\infty} \phi_{\alpha_1,\ldots,\alpha_n}(f_i) = h$. Así por la unicidad del límite, $h = \phi_{\alpha_1,\ldots,\alpha_n}(f) \in A$.

Por ende, $\overline{A} \subset A$, probando de esta manera la afirmación.

Usando esta afirmación y por la densidad de A probada tenemos $A = \overline{A} = K_y^{((n))}$, es decir, $\phi_{\alpha_1,\ldots,\alpha_n}(K_x^{((n))}) = K_y^{((n))}$ probando así la sobreyectividad de $\phi_{\alpha_1,\ldots,\alpha_n}$.

Por lo tanto de la parte **(i)** y **(ii)** $\phi_{\alpha_1,\ldots,\alpha_n}(K_x^{((n))})$ es K-isomorfismo.

$\square$

Definición 4.2. Sean $\alpha_1, \alpha_2, ..., \alpha_n \in \langle y_1, y_2, ..., y_n\rangle$ y $\phi_{\alpha_1,\alpha_2,...,\alpha_n} : K_x^{((n))} \longrightarrow K_y^{((n))}$ el homomorfismo de K-álgebras.

Tenemos, $\alpha_i = (a_{i1}y_1 + ... + a_{ij}y_j + ... + a_{in}y_n) + \sum_{i=2}^{\infty} P_i(y_1, y_2, ..., y_n),$

para todo $i = 1, ..., n$.

Luego representaremos $\frac{\partial \alpha_i}{\partial y_j}(0, ..., 0) = a_{ij}$, para todo $i, j = 1, 2, ..., n$.

Así denotaremos $J_0(\alpha_1, \alpha_2, ..., \alpha_n) := Det\left[\left(\frac{\partial \alpha_i}{\partial y_j}(0, ..., 0)\right)_{n\times n}\right] = Det[(a_{ij})_{n\times n}]$

Es decir:

$$J_0(\alpha_1, \alpha_2, ..., \alpha_n) = Det\begin{bmatrix} \frac{\partial \alpha_1}{\partial y_1}(0, ..., 0) & \frac{\partial \alpha_1}{\partial y_2}(0, ..., 0) & \cdots & \frac{\partial \alpha_1}{\partial y_n}(0, ..., 0) \\ \frac{\partial \alpha_2}{\partial y_1}(0, ..., 0) & \frac{\partial \alpha_2}{\partial y_2}(0, ..., 0) & \cdots & \frac{\partial \alpha_2}{\partial y_n}(0, ..., 0) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \alpha_n}{\partial y_1}(0, ..., 0) & \frac{\partial \alpha_n}{\partial y_2}(0, ..., 0) & \cdots & \frac{\partial \alpha_n}{\partial y_n}(0, ..., 0) \end{bmatrix}$$

Teorema 4.2. Sean $\alpha_1, \alpha_2, ..., \alpha_n \in \langle y_1, y_2, ..., y_n\rangle$ y $\phi_{\alpha_1,\alpha_2,...,\alpha_n} : K_x^{((n))} \longrightarrow K_y^{((n))}$ el homomorfismo de K álgebras.
$\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es K-isomorfismo si y solo si $J_0(\alpha_1, \alpha_2, ..., \alpha_n) \neq 0$.

Prueba. Tenemos, $\alpha_i = (a_{i1}y_1 + ... + a_{in}y_n) + \beta_i$, donde $Ord(\beta_i) \geq 2$, para todo $i = 1, ..., n$.

Luego denotamos $L_i = a_{i1}y_1 + ... + a_{in}y_n$, para todo $i = 1, ..., n$, que son formas lineales de α_i y además $J_0(\alpha_1, \alpha_2, ..., \alpha_n) = Det[(a_{ij})_{n\times n}]$.

Ya que $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es K-isomorfismo, entonces por la proposición 4.8 tenemos que $L_1, L_2, ..., L_n$ son K-$L.I$ y por la proposición 4.14,

$$J_0(\alpha_1, \alpha_2, ..., \alpha_n) = Det[(a_{ij})_{n\times n}] \neq 0.$$

Recíprocamente, por la misma proposición 4.14, si $J_0(\alpha_1, \alpha_2, ..., \alpha_n) \neq 0$, entonces, $L_1, L_2, ..., L_n$ son K-$L.I$, y finalmente por el teorema 4.1, $\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es K-isomorfismo. □

Del teorema 4.2, obtenemos un resultado descrito en el Corolario siguiente, el cual caracteriza los automorfsmos de series de potencias formales en varias indeterminadas y con coeficientes en un cuerpo.

Corolario 4.15.1. Sea K un cuerpo y $\alpha_1, \alpha_2, ..., \alpha_n \in \langle x_1, x_2, ..., x_n\rangle$.
$\phi_{\alpha_1,\alpha_2,...,\alpha_n}$ es K-automorfismo de $K_x^{((n))}$ si y solo si $J_0(\alpha_1, \alpha_2, ..., \alpha_n) \neq 0$.

Prueba. Como K es un cuerpo, $\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n}$ que es el automorfismo de $K_x^{((n))}$, se puede ver como un isomorfismo de K-álgebras $\phi_{\alpha_1,\alpha_2,\ldots,\alpha_n} : K_x^{((n))} \longrightarrow K_x^{((n))}$.

Así, usando el teorema 4.2 la prueba es inmediata.

$\square$

Este resultado es muy importante, pues nos brinda información valiosa para los K-automorfismos de las series de potencias formales con coeficientes en un cuerpo en varias indeterminadas, cuando usemos los cuerpos K, conocidos como son los números reales, los números complejos, los racionales, etc.

Conclusiones

Nuestro trabajo de tesis, estudió a los anillos conmutativos con identidad y nos preocupamos en los automorfismos que se puedan construir ya sea en anillo de polinomios y en anillo de series de potencias formales en una indeterminada con coeficientes en un anillo.

Precisamos que estudiamos a los anillos conmutativos con identidad, pues si consideramos anillos sin identidad la caracterización de los automorfismos cambia, esto no fue de nuestro interés en la tesis.

En el caso de los automorfismos antes descrito, también utilizamos los anillos sin divisores de cero, esto es, los dominios de integridad.

También, nos planteamos la interrogante siguiente: si consideramos el anillo que sea un cuerpo como serían los automorfismos en las series de potencias formales con coeficientes en un cuerpo, pero esta vez en varias indeterminadas. La respuesta a esta pregunta, se encuentra en el capítulo 4.

Bibliografía

[1] Adamson, I. T. (1995). *A General Topology Workbook.* Springer Science & Business Media.

[2] Alvarado, C. D. (2015). Grupos Topológicos.

[3] Atiyah, M. F., & Macdonald, I. G. (1989). *Introducción al álgebra conmutativa.* Reverté.

[4] Ayres, F., Jr. (1992). *Algebra Moderna*. McGraw-Hill Companies

[5] Beachy, J. A., & Blair, W. D. (2019). *Abstract algebra.* Waveland Press.

[6] Chenciner, A. (2008). *Courbes algébriques planes.* Springer.

[7] Churchill, R. V., & Brown, J. W. (1992). *Variable compleja y aplicaciones.*

[8] Dugundji, J. (1978). Topología. Reimpresión del original de 1966.

[9] Gentile, E. R. (1967). *Estructuras algebraicas I.* [Monografía, Universidad de Buenos Aires].

[10] Gilmer Jr, R. W. (1968). R-automorphisms of $R[X]$. In *Proc. London Math. Soc.(3)* (Vol. 18, pp. 328-336).

[11] Hefez, A. (2003). *In Real and complex singularities* (pp. 1-120). CRC Press.

[12] Herstein, I. N., & Lluis, E. (1970). *Algebra moderna: grupos, anillos, campos, teoría de Galois.* Trillas.

[13] Hungerford, T. W. (2012). *Algebra* (Vol. 73). Springer Science & Business Media.

[14] Martinez, P. J. (1997).*NOTAS DE TRABAJO, 6 ÁLGEBRA CONMUTATIVA.*

[15] Lima, E. L. (2014). *Espaços métricos.* (1.a ed.). IMPA.

[16] Lang, S. (2013). *Complex analysis* (Vol. 103). Springer Science & Business Media.

[17] Lang, S. (2012). *Algebra* (Vol. 211). Springer Science & Business Media.

[18] Lezama Serrano, J. O. (2014, 30 junio). *CUADERNOS DE ÁLGEBRA No. 2 Anillos.*

[19] Mejía Salazar, C. E. (1985). *Automorfismos de anillos de series formales* (Doctoral dissertation).

[20] Munkres, J. R. (2002). *Topología* (2.a ed.). Prentice Hall.

[21] Narasimhan, R., & Nievergelt, Y. (2012). *Complex analysis in one variable.* Springer Science & Business Media.

[22] O'Malley, M. J. (1970). R-automorphisms of R [[x]]. *Proceedings of the London Mathematical Society*, 3(1), 60-78.

[23] O'Malley, M., & Wood, C. (1970). r-Endomorphisms of R [[X]]. *Journal of Algebra, 15*(3), 314-327.

[24] Wawrzynczyk, A. (1993). *Introducción al análisis funcional.* UAM, Unidad Iztapalapa.

[25] Zaldıvar, F. (2011). *Introducción al álgebra conmutativa.* México DF.