UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

ESCUELA PROFESIONAL DE MATEMÁTICA

‘’TEOREMA DE NEWTON-PUISEUX EN LAS CURVAS PLANAS’’

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE

LICENCIADO EN MATEMÁTICA

MARISOL PAOLA DELGADO BALTAZAR

Callao, Enero, 2019

PERÚ

HOJA DE REFERENCIA DEL JURADO Y APROBACIÓN

"Teorema de Newton-Puiseux en las Curvas Planas"

MARISOL PAOLA DELGADO BALTAZAR

TESIS PRESENTADA A CONSIDERACIÓN DEL CUERPO DOCENTE DE LA FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA DE LA UNIVERSIDAD NACIONAL DEL CALLAO, COMO PARTE DE LOS REQUISITOS PARA OBTENER EL TÍTULO PROFESIONAL DE LICENCIADO EN MATEMÁTICA. APROBADA POR:

....

PRESIDENTE

....

VOCAL

....

SECRETARIO

....

SUPLENTE

....

ASESOR

UNIVERSIDAD NACIONAL DEL CALLAO
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA PROFESIONAL DE MATEMÁTICA
TITULACIÓN PROFESIONAL POR LA MODALIDAD DE TESIS CON CICLO DE TESIS
II CICLO DE TESIS

JURADO EVALUADOR PARA LA TITULACIÓN PROFESIONAL EN EL SEGUNDO CICLO DE TESIS

RESOLUCIÓN DECANAL N°147-2018-D-FCNM

ACTA DE SUSTENTACIÓN DE TESIS

En el auditorio de la Facultad de Ciencias Naturales y Matemática, sito Av. Juan Pablo II N° 306, Bellavista – Callao, siendo las 16:50 hrs. del día viernes 25 de enero de 2019, se reunieron los miembros del Jurado Evaluador del II Ciclo de Tesis para la Titulación Profesional por la modalidad de Tesis con Ciclo de Tesis de la Facultad de Ciencias Naturales y Matemática de la Universidad Nacional del Callao:

- Dr. Walter Flores Vega : Presidente
- Lic. Herminia Bertha Tello Bedriñana : Vocal
- Lic. Elmer Alberto León Zárate : Secretario

Designados por Resolución N° 147-2018-D-FCNM de fecha 28 de diciembre de 2018 a fin de proceder al acto de evaluación de la Tesis titulada: ***"TEOREMA DE NEWTON-PUISEUX EN LAS CURVAS PLANAS"***, presentada por la señorita Bachiller ***DELGADO BALTAZAR MARISOL PAOLA***.

Contando con la presencia del Supervisor General, Decano de la Facultad de Ciencias Económicas Dr. Pablo Mario Coronado Arrilucea, Supervisor de la FCNM, Mg. Roel Mario Vidal Guzmán, el representante de la Comisión de Grados y Títulos Dr. Richard Saúl Toribio Saavedra y el Coordinador del II Ciclo de Tesis Lic. Absalón Castillo Valdivieso.

A continuación, se dio inicio a la sustentación de la Tesis de acuerdo a lo normado en los numerales del 10.1 al 10.4 del capítulo X de la Directiva para la Titulación Profesional por la modalidad de Tesis con Ciclo de Tesis en la Universidad Nacional del Callao, aprobada por Resolución Rectoral N° 754-2013-R del 21 de agosto de 2013, modificada por la Resolución Rectoral N° 777-2013-R de fecha 29 de agosto de 2013 y la Resolución Rectoral N° 281-2014-R del 14 de abril de 2014 con la que se modifica el Art. 4.5 del capítulo IV de la organización del Ciclo de Tesis, así como lo normado en el Reglamento de Grados y Títulos de Pregrado, aprobado por Resolución de Consejo Universitario N° 135-2017-CU de fecha 22 de junio de 2017 y también lo establecido en el Reglamento de Grados y Títulos de la UNAC aprobado por Resolución N° 309-2017-CU de fecha 24 de octubre de 2017.

Culminado el acto de sustentación, los señores miembros del Jurado Evaluador procedieron a formular las preguntas a la indicada bachiller, las mismas que fueron absueltas satisfactoriamente.

Luego de un cuarto intermedio, para la deliberación en privado del Jurado respecto a la evaluación de la Tesis, se acordó calificar la Tesis sustentada por la señorita bachiller ***DELGADO BALTAZAR MARISOL PAOLA***, para optar el Título Profesional de Licenciada en Matemática por la modalidad de Tesis con Ciclo de Tesis, según la puntuación cuantitativa y cualitativa que a continuación se indica:

CALIFICACIÓN CUANTITATIVA	CALIFICACIÓN CUALITATIVA
14 (CATORCE)	BUENO

Finalmente, se procedió a leer en público el acta de la sustentación realizada.

Siendo las 17:20 hrs. del día viernes veinticinco de enero del dos mil diecinueve, el señor Presidente del Jurado Evaluador dio por concluido el acto de sustentación de Tesis.

En señal de conformidad con lo actuado, se levanta la presente acta.

Dr. Walter Flores Vega
Presidente

Lic. Herminia Bertha Tello Bedriñana
Vocal

Lic. Elmer Alberto León Zárate
Secretario

AGRADECIMIENTO

A mi madre Zenobia Baltazar Leyva y a mi padre Emilio Delgado Condorccahua: Por haberme apoyado en todo momento, por sus consejos y valores que me han inculcado para ser una persona de bien y por los ejemplos de perseverancia que me han infundido siempre.

A mi asesora:
Mg. Sofía Irena Durán Quiñones.
Por su gran ayuda para la redacción del anteproyecto y de la tesis. Además, por el tiempo que me ha brindado para aconsejarme y hacer de mí, una mejor profesional.

“TEOREMA DE NEWTON-PUISEUX EN LAS CURVAS PLANAS’’

INDICE

RESUMEN

“TEOREMA DE NEWTON-PUISEUX EN LAS CURVAS PLANAS”

MARISOL PAOLA DELGADO BALTAZAR

Enero - 2019

Asesor: Mg. Sofía Irena Durán Quiñones

Titulo obtenido: Licenciado en Matemática

En el presente trabajo haremos el estudio del Anillo de las Series de potencias formales, para después definir la Curva Plana, demostrando luego el Teorema de Newton-Puiseux que da como resultado la parametrización de una Curva Plana.

Palabras Claves

- Anillo de Series de Potencias.
- Índice de intersección de Curvas Planas.

ABSTRACT

"NEWTON-PUISEUX THEOREM IN THE FLAT CURVES"

MARISOL PAOLA DELGADO BALTAZAR

JANUARY, 2019

Advisor : Sofía Irena Durán Quiñones

Degree obtained: Bachelor of Mathematics

In the present work we will study the Ring of the Series of formal powers, to then define the Flat Curve, then demonstrating the Newton-Puiseux Theorem that results in the parameterization of a Flat Curve.

Keywords

- Ring of Power Series.

- Index of intersection of Curves Planas.

INTRODUCCIÓN

En matemáticas, las series de Puiseux son una generalización de las series de potencias que permiten exponentes positivos y fraccionarios del parámetro T indeterminado. Primero fueron introducidos por Isaac Newton en 1676 y redescubiertos por Víctor Puiseux en 1850.

El Teorema de Puiseux, afirma que dada una ecuación polinómica $P(x, y) = 0$, sus soluciones en y, vistas como funciones de x, pueden expandirse como series de Puiseux que son convergentes en alguna vecindad del origen. En otras palabras, cada rama de una curva algebraica puede ser localmente descrita por una serie de Puiseux.

El conjunto de series de Puiseux sobre un campo algebraicamente cerrado de característica 0 es en sí mismo un campo algebraicamente cerrado, llamado campo de la Serie de Puiseux, es el cierre algebraico del campo de la serie de Laurent.

Esta declaración también se conoce como el Teorema de Puiseux, siendo una expresión del Teorema de Puiseux original en el lenguaje moderno abstracto.

CAPÍTULO I

PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. Determinación del problema

En México, Guanajuato, Wágner Badilla Céspedes, en su tesis **"Estudio geométrico de las singularidades de Curvas planas: el método de newton, pares de Puiseux y grafo de resolución"** concluye que Los generadores del semigrupo de valores y los exponentes característicos se obtienen uno del otro, luego con los exponentes característico se obtienen los pares de Puiseux, estos me permiten definir los carruseles, de acuerdo a sus movimientos nos brindan comportamientos de la curva plana con la que se trabaja. Incluso se tienen los pares de Puiseux a partir la expansión de Puiseux, para obtener finalmente los exponentes característicos y los generadores del semigrupo.

Mientras que en Argentina, Buenos Aires, María Solange Scelzaen,en su tesis **"Una generalización del Teorema de Puiseux"** analiza un método clásico para la determinación de soluciones de una ecuación del tipo f(x, y) = 0, con f un polinomio en dos variables con coeficientes en un cuerpo algebraicamente cerrado K, y una generalización de este método para la determinación de soluciones de una ecuación polinomial en varias variables con coeficientes complejos. Más precisamente, dada una ecuación del tipo, $F(x_1, x_2, x_3, \dots, x_N, x_{N+1}) = 0$ con F un polinomio con coeficientes complejos, el objetivo es hallar una solución, considerando como incógnita a la variable x_{N+1}, que esté representada en función de $x_1, x_2, x_3, \dots, x_N$ .En el caso $N = 1$, un procedimiento para calcular soluciones de $f(x, y) = 0$ ya era conocido por Newton y fue posteriormente formalizado por V. Puiseux. Estas soluciones pertenecen al cuerpo de series de potencias en una variable con coeficientes en K y exponentes fraccionarios llamadas series de Puiseux, que resulta ser un cuerpo algebraicamente cerrado. El primer capítulo de esta tesis está dedicado a la presentación de este resultado, conocido como Teorema de Puiseux.

Así mismo en Lima, Edison Marcavillaca Niño de Guzmán, en su tesis **"Moduli analítico de curvas analíticas irreductibles planas"** introduce el concepto de curva algebraica irreducible plana o rama plana y estudia su parametrización dada por el Teorema de Newton-Puiseux. Como también Frank Collantes, docente de la UNMSM, en su tesis **"Curvas Planas"** se puede apreciar un estudio del anillo de las series de potencias formales, para luego definir las curva algebroide plana, demuestra el teorema de Newton-Puiseux que da como resultados la parametrización de una curva plana. Finalmente analizó la resolución de singularidades de una curva plana, usando las transformaciones cuadráticas u explosiones.

El problema en sí, considerando previamente a $\mathbb{C}[\![x]\!]$ como el conjunto de las series de potencias formales en una indeterminada y dada una curva algebraica (f) de multiplicidad "n".Se tiene además por el teorema de Preparación de Weierstrass; lo cual es equivalente a una curva algebraica definida por un polinomio de Weierstrass.

$$P = P(x,y) = y^n + a_1(x)y^{n-1} + a_2(x)y^{n-2} + \cdots + a_n(x)y$$

Donde $a_i(x) \in \mathbb{C}[\![x]\!]$ y $mult\big(a_i(x)\big) \geq i$. Si denotamos por $\mathbb{C}((x))$ al cuerpo de fracciones de $\mathbb{C}[\![x]\!]$. Por lo tanto para estudiar las propiedades de la curva f es de gran utilidad conocer las raíces del polinomio P en el cierre algebraico de $\mathbb{C}((x))$; esto es, $\overline{\mathbb{C}((x))}$, donde debe contener las raíces de la ecuación: $y^n - x = 0,\ \forall n \in \mathbb{Z}^+$.

Luego de ello estudiaremos el Teorema de Newton-Puiseux que afirma que: $\overline{\mathbb{C}((x))} = \mathbb{C}((x))^*$ dónde:

$$\mathbb{C}((x))^* = \bigcup_{n=1}^{\infty} \mathbb{C}((x^{1/n}))\,;$$

1.2. Formulación del problema

Dada la curva algebraica definida por el polinomio de Weierstrass.

$P = P(x,y) = y^n + a_1(x)y^{n-1} + a_2(x)y^{n-2} + \cdots + a_n y \ \in \ \mathbb{C}[\![x,y]\!]$;

$a_i(x) \in \mathbb{C}((x))$ y $mult\big(a_i(x)\big) \geq i,\ i = 1; 2; \dots; n$.

¿Será posible conocer la raíces de P en el cierre algebraico de $\mathbb{C}((x))$?

Si eso es posible ¿Cómo podríamos explicitar $P(x,y) = \prod_{i=1}^{n}(y - \alpha_i)$ donde $\alpha_i = \varphi\left(\xi^i x^{1/n}\right) \in \ \mathbb{C}((x))$?

1.3. Objetivos de la investigación

1.3.1 Objetivo General

Estudiaremos el teorema de Newton-Puiseux que afirma que:

$$\overline{\mathbb{C}((\mathrm{x}))} = \mathbb{C}((\mathrm{x}))^*$$

Y como consecuencia de ello mostraremos que: Dado $f(x,y) \in \mathbb{C}[\![x,y]\!]$ un pseudo polinomio de grado "n"; existe una extensión $\mathbb{C}\big((\mathrm{x})\big)[\alpha]$ donde ella es resuelta; es decir, existe una función:

$$\varphi\left(x^{1/n}\right) = \sum_{i\geq 1} b_i\, x^{1/n} \ \in \ \mathbb{C}((x))^*$$

tal que $\mathrm{f}\left(x, \varphi\left(x^{1/n}\right)\right) = 0$ donde podemos tomar una parametrización:

$$\mathrm{f} = \mathrm{f}(x,y) = \begin{cases} \mathrm{x} = T^n \\ \mathrm{y} = \displaystyle\sum_{i\geq 1} b_i T^i \end{cases}$$

de $\mathrm{f}(x,y)$.

1.3.2 Objetivos Específicos

-Estudiar las Series de potencias formales $\mathbb{C}[\![x]\!]$ como un anillo con unidad.

-Estudiar el Teorema de Preparación de Weierstrass, que permite transformar una serie de potencias en un polinomio.

-Estudiar las curvas algebraicas planas.

-Demostrar el Teorema de Newton-Puiseux.

1.4. Justificación

La importancia de este trabajo radica en probar la existencia de la parametrización de una curva algebraica representada por un pseudo polinomio.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANILLOS.

Definición 2.1.1.

Un anillo $(R, +, \cdot)$ es un conjunto R junto con dos operaciones binarias $+$ y $\cdot$, llamados adición y multiplicación, respectivamente, tales que:

(a) $(\mathrm{a}+\mathrm{b})+\mathrm{c}=\mathrm{a}+(\mathrm{b}+\mathrm{c})$ para todo $a, \mathrm{b}, \mathrm{c} \in R$.

(b) $a+\mathrm{b}=\mathrm{b}+\mathrm{a}$ para todo $a, \mathrm{b} \in R$.

(c) Existe un elemento $0 \in R$ tal que

$$a+0=a \text{ para todo } a \in R.$$

El elemento $0 \in R$ será llamado elemento cero.

(d) Dado $a \in R$, existe $b \in R$ tal que $a+b=0$.

El elemento b es único y denotaremos $-a$.

(e) $a \cdot (b \cdot c)=(a \cdot b) \cdot c$ para todo $a, \mathrm{b}, \mathrm{c} \in R$.

(f) Se cumple que

$$a \cdot (b+c)=(a \cdot b)+(a \cdot c)$$

y

$$(a+b) \cdot c=(a \cdot c)+(b \cdot c)$$

para todo $a, b, c \in R$.

Los ítems (a)-(d), dicen que $(R, +)$ es un grupo abeliano.

El ítem (f) es llamado propiedad asociativa.

Las operaciones $+$ y $\cdot$ serán sobreentendidas.

Omitiremos el símbolo $\cdot$, escribiendo ab en vez de $a \cdot b$.

Definición 2.1.2.

Un anillo R en el cual la multiplicación cumple la propiedad conmutativa, esto es,

$$ab=ba \text{ para todo } a, \mathrm{b} \in R,$$

es llamado anillo conmutativo.

Definición 2.1.3.

Un anillo R en el cual la multiplicación tiene elemento neutro, esto es, existe un elemento $1 \in R$ tal que

$$a1 = 1a \text{ para todo } a \in R,$$

es un anillo con unidad.

El elemento $1 \in R$ será llamado elemento uno o unidad.

Definición 2.1.4.

Un anillo con unidad R es llamado anillo de división si para todo $a \neq 0$ existe un elemento $b \in R$ tal que implica que $ab = 1$.

El elemento b es único y denotaremos b^{-1}.

Diremos que R es un cuerpo si R es un anillo de división conmutativo en el cual $1 \neq 0$.

Definición 2.1.5.

Sean a un elemento no cero en un anillo R.

Diremos que a es un divisor de cero si existe b no cero en R tal que $ab = 0$.

Diremos que R es un dominio de integridad si R es un anillo conmutativo con unidad $1 \neq 0$ y que no contiene divisores de cero.

Ejemplo.

Consideraremos las operaciones usuales.

1. $\mathbb{Z}$ es un dominio de integridad con unidad que no es cuerpo.
2. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.
3. $\mathbb{Z} \times \mathbb{Z}$ es un anillo conmutativo con unidad $(1,1)$, que no es un dominio de integridad debido a que $(1,0)(0,1) = (0,0)$.
4. $\mathbb{N}$ no es un anillo.
5. El conjunto de los números irracionales no es un anillo.
6. Dado $n \in \mathbb{N}$ con $n \geq 2$, el conjunto de matrices de orden $n \times n$ con entradas en $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, es un anillo no conmutativo con unidad.

Definición 2.1.6.

Un subanillo de un anillo R es un subconjunto S de R el cual es un anillo con las operaciones restrictas de R.

Definición 2.1.7.

Una función $f: R \to S$ de un anillo R en un anillo S es llamado homomorfismo de anillos si para todo $a, b \in R$,

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

$$f(ab) = f(a)f(b).$$

Si R y S son anillos con unidad, se debe cumplir que $f(1_R) = 1_S$.

Definición 2.1.8.

Sea $f: R \to S$ un homomorfismo de un anillo R en un anillo S.

Diremos que f es monomorfismo si f es inyectivo.

Diremos que f es epimorfismo si f es sobreyectivo.

Diremos que f es isomorfismo si f es biyectivo.

Diremos que f es automorfismo si $R = S$ y f es isomorfismo.

Ejemplo.

1. Las inclusiones $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Q} \to \mathbb{R}$, $\mathbb{R} \to \mathbb{C}$ y composiciones de estos, son monomorfismo de anillos.
2. Las proyecciones $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ sobre la primera o segunda coordenada son epimorfismos de anillos.
3. El único automorfismo $\mathbb{Z} \to \mathbb{Z}$ es la identidad.

Definición 2.1.9.

Sea $f: R \to S$ un homomorfismo de anillos, denotaremos el núcleo de f y la imagen de f como

$$ker(f) = \{x \in R: f(x) = 0\},$$

$$im(f) = \{f(x) : x \in R\},$$

respectivamente.

Definición 2.1.10.

Sea R un anillo. Un subconjunto no vacío I de R es llamado un ideal si:

(a) I es un subgrupo aditivo de R.
(b) Dados $r \in R$, $a \in I$, se cumple que $ar, ra \in I$.

Ejemplo.

Consideraremos las operaciones usuales.

1. Todo anillo R tiene como ideales a $\{0\}$ y R.
2. Todo ideal $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con n entero no negativo.
3. El anillo (no conmutativo) de todas las matrices triangulares superiores de orden $n \times n$, con $n \geq 2$ y entradas en $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, tiene como ideal el conjunto de matrices estrictamente triangulares.

Lema 2.1.11.

Si $f: R \to S$ es un homomorfismo de anillos, entonces:

1. $ker(f)$ es un ideal de R.
2. $im(f)$ es un subanillo de S.
3. $im(f)$ podría no ser ideal de S.
4. $f^{-1}(I)$ es un ideal de R para todo ideal de S.

Lema 2.1.12.

Sea $f: R \to S$ es un homomorfismo de anillos. Se cumple que f es un monomorfismo si y solo si $ker(f) = 0$.

Teorema 2.1.13.

Sea R un anillo conmutativo con unidad. Se cumple que R es un cuerpo si y solo los únicos ideales de R son $\{0\}$ y R.

Teorema 2.1.14.

Un homomorfismo $f: R \to S$ de un cuerpo R en un anillo S. Se cumple que $f = 0$ o f es monomorfismo.

Demostración.

Como $ker(f)$ es ideal del cuerpo R, entonces $ker(f) = 0$ o $ker(f) = R$.

Si $ker(f) = 0$, entonces f es un monomorfismo.

Si $ker(f) = R$, entonces $f = 0$. □

Definición 2.1.15.

Sea T un subconjunto de un anillo conmutativo R. Llamaremos ideal de R generado por T al conjunto

$$\{r_1t_1 + \ldots + r_1t_1 : n \in \mathbb{N}, t_1, \ldots, t_n \in T, r_1, \ldots, r_n \in R\},$$

que es en efecto un ideal de R.

Definición 2.1.16.

Sean $I, J, I_1, \ldots, I_n$ ideal de un anillo conmutativo R.

Denotaremos IJ, llamado ideal producto de los ideales I y J, como el ideal generado por el conjunto

$$\{rs : r \in I, s \in J\}.$$

Definiremos inductivamente

$$I_1 \ldots I_n = (I_1 \ldots I_{n-1})I_n.$$

El producto n veces de I, será denotado como I^n.

Definición 2.1.17.

Sea I un ideal en un anillo R. Diremos que I es un ideal maximal de R si dado J ideal de R tal que $I \subseteq J$, entonces $J = I$ o $J = R$.

2.2. ANILLO DE POLINOMIOS.

Sea K un cuerpo y X una indeterminada sobre K. Denotaremos por $K[X]$, el conjunto de las sumas formales de la forma

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, n \geq 0,$$

donde los $a_i's$ son llamados los coeficientes del polinomio $p(X)$. Emplearemos, también, la notación alternativa

$$p(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n, n \geq 0.$$

Diremos que a_i está definido para todo $i \geq 0$, haciendo $a_i = 0$ para todo $i > n$.

Definiremos en $K[X]$, la igualdad, suma y multiplicación de dos polinomios para hacer de $K[X]$ un dominio de integridad, como sigue:

Sean dos polinomios

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, n \geq 0,$$
$$q(X) = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m, m \geq 0,$$

tenemos:

1. **Igualdad.**

   Diremos que son iguales si y solo si $a_i = b_i$ para todo $i \geq 0$.
2. **Suma.**

   Definiremos

   $$p(X) + q(X) = c_0 + c_1X + c_2X^2 + \cdots + c_rX^r, r \geq 0$$

   donde

   $$c_i = a_i + b_i \text{ para todo } i \geq 0.$$
3. **Multiplicación.**

   Definiremos

   $$p(X)q(X) = c_0 + c_1X + c_2X^2 + \cdots + c_rX^r, r \geq 0$$

   donde, para todo $i \geq 0$,

   $$c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_1.$$

Ejemplo.

Ilustraremos estas operaciones.

Sean

$$\begin{aligned} p(X) &= 1 + 0X + 3X^2 + 0X^3, \\ q(X) &= 4 + (-5)X + 7X^2 + (-1)X^3. \end{aligned}$$

Podemos escribir en forma más simple como,

$$\begin{aligned} p(X) &= 1 + 3X^2, \\ q(X) &= 4 - 5X + 7X^2 - X^3. \end{aligned}$$

Así,

$$\begin{aligned} p(X) + q(X) &= (1 + 3X^2) + (4 - 5X + 7X^2 - X^3) \\ &= (1 + 4) - 5X + 3X^2 + (3 + 7)X^2 - X^3 \\ &= 5 - 5X + 3X^2 + 10X^2 - X^3. \end{aligned}$$

y

$$\begin{aligned} p(X)q(X) &= (1 + 3X^2)(4 - 5X + 7X^2 - X^3) \\ &= (1)(4 - 5X + 7X^2 - X^3) + (3X^2)(4 - 5X + 7X^2 - X^3) \\ &= (4 - 5X + 7X^2 - X^3) + (12X^2 - 15X^3 + 21X^4 - 3X^5) \\ &= 4 - 5X + 19X^2 - 16X^3 + 21X^4 - 3X^5. \end{aligned}$$

Definición 2.2.1.

El conjunto $K[X]$ con las operaciones de adición y de producto será el anillo de los polinomios en la indeterminada X y con coeficientes en K.

Teorema 2.2.2.

$K[X]$ es un dominio de integridad con unidad.

Definición 2.2.3.

Si

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X], a_n \neq 0.$$

Definiremos el grado de $p(X)$, que denotaremos $deg(p)$, como el entero no negativo n. Que es el mayor entero no negativo i tal que a_i es no nulo.

Ejemplo.

Sean

$$\begin{array}{rcl} p(X) & = & 1+3X^2, \\ q(X) & = & 4-5X+7X^2-X^3. \end{array}$$

Entonces,

$$deg(p)=2, deg(p)=3.$$

Teorema 2.2.4 (Algoritmo de división).

Dados dos polinomios $f, g \in K[X]$ donde $g \neq 0$, existen $q, r \in K[X]$ únicos tal que

$$f = qg + r$$

y, $r = 0$ o $\deg(r) < \deg(g)$.

Definición 2.2.5.

Un dominio de integridad R es llamado es llamado dominio de ideales principales (DIP) si todo ideal I de R es de la forma

$$I = \{ax : x \in R\}$$

para algún $a \in I$.

Teorema 2.2.6.

El anillo $K[X]$ es un dominio de ideales principales.

Definición 2.2.7.

Un polinomio $f(X) \in K[X]$ es llamado polinomio mónico si el coeficiente de si término de mayor potencia es 1, esto es, $f(X)$ es de la forma

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + X^n, n \geq 0,$$

Definición 2.2.8.

Sean $f(X), g(X) \in K[X]$. Diremos que:

$$g(X) \text{ divide a } f(X),$$

y escribiremos que

$$g(X)|f(X),$$

si

$$f(X) = g(X)h(X) \text{ para algún } h(X) \in K[X].$$

Definición 2.2.9.

Sean $f(X), g(X) \in K[X]$ ambos no nulos, el polinomio $d(X) \in K[X]$ es llamado el máximo común divisor de $f(X)$ y $g(X)$, $d(X)$ es un polinomio mónico tal que:

(a) $d(X)|f(X)$ y $d(X)|g(X)$.
(b) Si $h(X) \in K[X]$ es tal que $h(X)|f(X)$ y $h(X)|g(X)$, entonces $h(X)|d(X)$.

Teorema 2.2.10.

Sean $f(X), g(X) \in K[X]$ ambos no nulos, el máximo común divisor $\mathrm{d}(X) \in K[X]$ de $f(X)$ y $g(X)$ existe; y, además, existen $a(X), b(X) \in K[X]$ tal que

$$d(X) = a(X)f(X) + b(X)g(X).$$

Definición 2.2.11.

Dos polinomios $f(X), g(X) \in K[X]$ son llamados primos relativos o primos entre sí el máximo común divisor de $f(X)$ y $g(X)$ exactamente 1.

Teorema 2.2.12.

Sean $f(X), g(X) \in K[X]$ ambos no nulos. Se cumple que $f(X), g(X)$ son primos relativos si y solo si

$$1 = a(X)f(X) + b(X)g(X)$$

para algunos $a(X), b(X) \in K[X]$.

Definición 2.2.13.

El anillo de polinomio en r indeterminadas y con coeficientes en K,

$$K[X_1, X_2, \dots, X_r],$$

será el anillo definido inductivamente como

$$K[X_1, X_2, \ldots, X_r] = K[X_1, X_2, \ldots, X_{r-1}][X_r].$$

2.3. CUERPO DE COCIENTES.

Sea D un dominio de integridad se puede construir un cuerpo con la propiedad de ser el menor cuerpo F que contiene D. Este cuerpo es el cuerpo de cocientes de D.

Consideremos el conjunto

$$S = \{(a,b): a,b \in D, b \neq 0\}$$

Pensemos en (a,b) como a/b.

Dos elementos a/b y c/d son iguales si $ab = bc$. Definamos entonces la relación $\sim$ en S, como

$$(a,b)\sim(c,d) \text{ si } ab = bc.$$

Lema 2.3.1.

La relación $\sim$ en S es una relación de equivalencia.

Definamos F como el conjunto de todas las clases de equivalencia $[a,b]$ de los elementos $(a,b) \in S$. Inspirados en las reglas de las operaciones del cuerpo $\mathbb{Q}$, se define las operaciones en F como

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

definiremos en F las operaciones,

$$[a,b] + [c,d] = [ad + bc, bd],$$

$$[a,b] \cdot [c,d] = [ac, bd],$$

Teorema 2.3.2.

La terna $(F,+,\cdot)$ forma un cuerpo con elementos

$$0_F = [0,1], \quad 1_F = [1,1].$$

El cuerpo F es llamado cuerpo de cocientes de D y es el menor campo conteniendo a D como subanillo.

Ejemplo.

1. El cuerpo de cocientes de $\mathbb{Z}$ es $\mathbb{Q}$.
2. El cuerpo de cocientes de un cuerpo es el mismo cuerpo.
3. El cuerpo de cocientes del anillo de polinomios
$$K[X],$$
es denotado como
$$K(X)$$
y es llamado, el cuerpo de las funciones racionales en la indeterminada X con coeficientes en K.
4. El cuerpo de cocientes del anillo de polinomios
$$K[X_1, X_2, \dots, X_r],$$
es denotado como
$$K(X_1, X_2, \dots, X_r),$$
y es llamado el cuerpo de las funciones racionales en r indeterminadas con coeficientes en K.

2.4. EXTENSIONES DE CUERPOS.

Definición 2.4.1.

Un cuerpo K ese dice de característica p si p es el menor entero positivo tal que

$$px = 0 \text{ para todo } x \in K.$$

Si no existe tal p, se dice que K tiene característica 0.

Teorema 2.4.2.

La característica de un cuerpo es 0 o un número primo.

Ejemplo.

1. Los cuerpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son de característica cero.
2. El cuerpo $\mathbb{Z}_p$, con p primo positivo, es de característica p.
3. El cuerpo $K(X)$ tiene la misma característica que el cuerpo K.
4. Generalizando, el cuerpo $K(X_1, X_2, \dots, X_r)$ tiene la misma característica que el cuerpo K.

Definición 2.4.3.

Sean K y F dos cuerpos tal que $F \subseteq K$. En este caso diremos que F es un subcuerpo de K y que K es una extensión de F. Denotaremos esto como $F\backslash K$.

Ejemplo.

1. $\mathbb{R}\backslash\mathbb{Q}$.
2. $\mathbb{C}\backslash\mathbb{R}$.
3. $\mathbb{C}\backslash\mathbb{Q}$.
4. Ni $\mathbb{Q}$, ni $\mathbb{R}$, ni $\mathbb{C}$ son extensiones de $\mathbb{Z}_p$ para ningún p primo positivo.
5. Sea K un cuerpo y $X_1, X_2, \dots, X_r$ indeterminadas sobre K. Entonces, $K(X_1, X_2, \dots, X_r)\backslash K$.

Definición 2.4.4.

Sea K un cuerpo. Sea $a \in K$ y

$$p(x) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$$

Denotaremos

$$p(a) = a_0 + a_1(a) + a_2(a^2) + \cdots + a_n(a^n)$$

que es llamado evaluación de $p(x)$ en a.

Diremos que a es raíz de $p(x)$ si $p(a) = 0$.

Definición 2.4.5.

Sean $F\backslash K$ dos cuerpos. Diremos que $a \in K$ es algebraico sobre F si existe un polinomio no nulo $p(x) \in F[X]$ tal que $p(a) = 0$.

La extensión $F\backslash K$ es llamada algebraica si todo elemento de F es algebraico sobre K.

Definición 2.4.6.

Sean K un cuerpo. Diremos que K es algebraicamente cerrado si todo polinomio no constante $p(x) \in F[X]$ tiene una raíz en K.

Teorema 2.4.7.

Todo cuerpo tiene un cuerpo de extensión algebraicamente cerrado.

Ejemplo.

1. $\mathbb{R}$ no es algebraicamente cerrado, por ejemplo $x^2 + 1$ no tiene raíz en $\mathbb{R}$.
2. $\mathbb{C}$ es algebraicamente cerrado.

Definición 2.4.8.

Sea K un cuerpo. Un automorfismo de K es un homomorfismo de $\sigma: K \to K$ que es monomorfismo y epimorfismo.

El conjunto de todos los automorfismos de K será denotado como $Aut(K)$.

Definición 2.4.9.

Sea $F\backslash K$ una extensión de cuerpos.

Denotemos

$$G(F\backslash K) = \{\sigma \in Aut(F): \sigma(x) = x \ \forall x \in K\}$$

Si

$$G(F\backslash K) \text{ es finito}$$

y

$$\{a \in F: \sigma(a) = a \ \forall \sigma \in G(F\backslash K)\} = K,$$

diremos que $F\backslash K$ es extensión galoisiana y $G(F\backslash K)$ es llamado grupo de Galois de $F\backslash K$.

2.5. ESPACIOS MÉTRICOS

Definición 2.5.1.

Una métrica en un conjunto M es una función $d: M \times M \to \mathbb{R}$ tal que para cualesquiera $x, y, z \in M$:

1. $d(x, y) \geq 0$.
2. $d(x, y) > 0 \Leftrightarrow x \neq y$.
3. $d(x, y) = d(y, x)$.
4. $d(x, z) \leq d(x, y) + d(y, z)$.

El par (M, d) es llamado espacio métrico.

Ejemplo.

1. La función $d: M \times M \to \mathbb{R}$, definida como $d(x, x) = 0$ y $d(x, y) = 1$ si $x \neq y$, es una métrica.
2. La función $d: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, definida como $d(x, y) = |x - y|$, es una métrica.

Definición 2.5.2.

Una sucesión en un conjunto M es una función $f: \mathbb{N} \to M$. Se acostumbra a escribir $(x_i)_{i \in \mathbb{N}}$ donde $x_i = f(i)$.

Una subsucesión de $(x_i)_{i \in \mathbb{N}}$ es una sucesión $\left(x_{n_i}\right)_{i \in \mathbb{N}}$ donde $\{n_1 < n_2 < \cdots < n_i < \cdots\}$.

Definición 2.5.3.

Sea (M, d) un espacio métrico. Una sucesión $(x_i)_{i \in \mathbb{N}}$ en M converge a $x \in M$, o x es límite de $(x_i)_{i \in \mathbb{N}}$, si para todo $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $d(x_n, x) < \varepsilon$ si $n \geq N$. Denotaremos esto como

$$\lim_{i \to +\infty} x_i = x.$$

Diremos que una sucesión en M es convergente si converge a algún $x \in M$. Caso contrario, diremos que la sucesión es divergente.

Proposición 2.5.4.

Una sucesión no puede tener dos límites diferentes.

Proposición 2.5.5.

Si $(x_i)_{i\in\mathbb{N}}$ es una sucesión que converge a x, entonces toda subsucesión de $(x_i)_{i\in\mathbb{N}}$ converge, también, a x.

Definición 2.5.6.

Sea (M,d) un espacio métrico. Una sucesión $(x_i)_{i\in\mathbb{N}}$ en M es llamado sucesión de Cauchy si para todo $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que $d(x_n, x_m) < \varepsilon$ si $n, m \geq N$.

Proposición 2.5.7.

Toda sucesión convergente es sucesión de Cauchy.

Proposición 2.5.8.

Si $(x_i)_{i\in\mathbb{N}}$ es una sucesión de Cauchy que tiene una subsucesión convergente, entonces $(x_i)_{i\in\mathbb{N}}$ es convergente.

Definición 2.5.9.

Diremos que un espacio métrico es completo si toda sucesión de Cauchy es convergente.

Definición 2.5.10.

Sean M, N espacios métricos. Diremos que una función $f: M \to N$ es continua si para todo $x \in M$, $\varepsilon > 0$ existe $\delta > 0$ tal que $d(x,y) < \varepsilon$ si $d(x,y) < \delta$.

Proposición 2.5.11.

Sean M, N espacios métricos. Una función $f: M \to N$ es continua si y solo si para toda sucesión $(x_i)_{i\in\mathbb{N}}$ en M que converge a $x \in M$, la sucesión $\left(f(x_i)\right)_{i\in\mathbb{N}}$ converge a $f(x)$.

Definición 2.5.12.

Sea M un espacio métrico y $A \subseteq M$. Diremos que A es denso en M si para todo $x \in M$ y $\varepsilon > 0$ existe $y \in A$ tal que $d(x,y) < \varepsilon$.

Proposición 2.5.13.

Sea M un espacio métrico y $A \subseteq M$. Se cumple que A es denso en M si y solo si para todo $x \in M$ existe $(x_i)_{i\in\mathbb{N}}$ en A que converge a x.

2.6. ANILLO DE SERIES DE POTENCIAS

Sea K un cuerpo y $X_1, X_2, \dots, X_r$ indeterminadas sobre K. Denotamos por

$$K\big[[X_1, X_2, \dots, X_r]\big]$$

el conjunto de las sumas formales de la forma

$$f = \sum_{i=0}^{\infty} P_i = P_0 + P_1 + P_2 + \cdots$$

Donde cada P_i es un polinomio homogéneo de grado i, en las indeterminadas

$$X_1, X_2, \dots, X_r$$

con coeficientes en K.

Sean

$$f = \sum_{i=0}^{\infty} P_i \,, g = \sum_{i=0}^{\infty} Q_i \in K\big[[X_1, X_2, \dots, X_r]\big],$$

por definición se cumple

$$f = g \Leftrightarrow P_i = Q_i \ \forall i \geq 0$$

Se define en $K\big[[X_1, X_2, \dots, X_r]\big]$ la suma y multiplicación como:

$$\begin{aligned} f + g &= \sum_{i=0}^{\infty} P_i + Q_i \\ fg &= \sum_{i=0}^{\infty} \sum_{j=0}^{i} P_i Q_{i-j} \end{aligned}$$

Definición 2.6.1.

El conjunto $K\big[[X_1, X_2, \dots, X_r]\big]$ con las operaciones de adición y de producto será el anillo de las series de potencias formales en r indeterminadas y con coeficientes en K.

El anillo $K\big[[X_1, X_2, \dots, X_r]\big]$ es conmutativo con elemento neutro $\sum_{i=0}^{\infty} 0$ y elemento unidad $1 + \sum_{i=1}^{\infty} 0$.

El anillo $K[[X_1, X_2, \dots, X_r]]$ contiene al cuerpo K mediante el monomorfismo

$$\begin{array}{ccc} K & \to & K[[X_1, X_2, \dots, X_r]] \\ x & \mapsto & x + \sum_{i=1}^{\infty} 0 \end{array}$$

Y contiene al anillo

$$K[X_1, X_2, \dots, X_r],$$

ya que todo elemento de $K[X_1, X_2, \dots, X_r]$ puede ser escrito como suma finita de elementos homogéneos.

Lema 2.6.2.

Un elemento $f = \sum_{i=0}^{\infty} a_i X^i \in K[[X]]$ es invertible si y solo si $a_0 \neq 0$.

Denotemos $K((X))$ el cuerpo de cocientes de $K[[X]]$.

Demostración.

Necesitamos determinar una serie

$$g = \sum_{i=0}^{\infty} b_i X^i \in K[[X]]$$

tal que

$$fg = 1.$$

Expandiendo este producto tenemos

$$\begin{aligned} fg &= \left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{i=0}^{\infty} b_i X^i\right) \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k \end{aligned}$$

Comparando los coeficientes de X^k en ambos lados de $fg = 1$, obtenemos

$$a_0 b_0 = 1 \text{ y } \sum_{i=0}^{k} a_i b_{k-i} = 0 \text{ para } k \geq 1.$$

Notemos que si f es invertible, entonces a_0 es invertible.

Recíprocamente, si a_0 es invertible, entonces podemos definir g como $b_0 = a_0^{-1}$ y, por $\sum_{i=0}^{k} a_i b_{k-i} = 0$, para $k \geq 1$, inductivamente,

$$b_k = -a_0^{-1} \sum_{i=1}^{k} a_i b_{k-i}$$

Tal que $fg = 1$. □

Teorema 2.6.3.

Todo ideal de $K\big[[X]\big]$ es generado por X^k para algún $k \geq 0$.

En consecuencia, $K\big[[X]\big]$ es un dominio de ideales principales y el ideal generado por X es el único ideal maximal de $K\big[[X]\big]$.

Demostración.

Sea I un ideal propio de $K\big[[X]\big]$. Tomemos

$$k = min\left\{r : f = \sum_{i=r}^{\infty} a_i X^i \in I, a_r \neq 0\right\}.$$

Sea $g = \sum_{i=k}^{\infty} b_i X^i \in I$ con $b_k \neq 0$. Luego, podemos factorizar

$$g = X^k \sum_{i=0}^{\infty} b_{i+k} X^i.$$

Por el lema anterior

$$X^k = \left(\sum_{i=0}^{\infty} b_{i+k} X^i\right)^{-1} g \in I.$$

Por definición de k, todo elemento no nulo de I se puede factorizar por X^k. Luego I es generado por X^k. □

Corolario 2.6.4.

El ideal maximal de $K\big[[X_1, X_2, \ldots, X_r]\big]$ es el ideal generado por $X_1, X_2, \ldots, X_r$.

Demostración.

Por la proposición anterior e inducción sobre r aplicado a

$$K[[X_1, X_2, \dots, X_r]] = K[[X_1, X_2, \dots, X_{r-1}]][[X_r]].$$

Corolario 2.6.5.

El cuerpo de cocientes de $K[[X]]$, que se denota como $K((X))$, cumple que

$$K((X)) = \left\{ \frac{\sum_{i=0}^{\infty} a_{i-k} X^i}{X^k} : para\ algún\ k \in \mathbb{Z}^+ \cup \{0\}, \sum_{i=0}^{\infty} a_{i-k} X^i \in K[[X]] \right\}$$

Denotaremos

$$\sum_{i=-k}^{\infty} a_i X^i := \frac{\sum_{i=0}^{\infty} a_{i-k} X^i}{X^k}$$

Demostración.

Sean f y $g \neq 0$ en $K[[X]]$. Podemos factorizar

$$g = X^k h \text{ con } h \text{ invertible en } K[[X]].$$

Luego,

$$\frac{f}{g} = \frac{f}{X^k h} = \frac{f h^{-1}}{X^k}$$

Definición 2.6.6.

Dado $f \in K((X))$ no nulo, podemos escribir de manera única

$$f = \sum_{i=i_0}^{\infty} b_i X^{\mathrm{i}}, b_i \in K, b_{i_0} \neq 0.$$

Definimos la multiplicidad de f, como

$$mult(f) = i_0.$$

Por comodidad se define

$$mult(0) = \infty.$$

Lema 2.6.7.

Dado $f, g \in K\big((X)\big)$ tenemos que:

1. Si $f \neq 0$, entonces $mult(f^{-1}) = -mult(f)$.
2. $mult(fg) = mult(f) + mult(g)$.
3. $mult(f \pm g) = min\{mult(f), mult(g)\}$.
4. $mult(f) \geq 0$ si y solo si $f \in K\big[[X]\big]$.

Demostración.

Podemos escribir, para algún n,

$$f = \sum_{i=i_0}^{\infty} b_i X^{\mathrm{i}}, g = \sum_{i=j_0}^{\infty} c_i X^{\mathrm{i}}, b_i, c_i \in K, b_{i_0} \neq 0, c_{j_0} \neq 0.$$

Esto significa que

$$mult(f) = i_0, mult(g) = j_0.$$

1. Tenemos que

$$\begin{aligned} f^{-1} &= \left(b_{i_0} X^{i_0} + b_{i_0+1} X^{i_0+1} + \ldots\right)^{-1} \\ &= \Big(X^{i_0}\big(b_{i_0} + b_{i_0+1} X + \ldots\big)\Big)^{-1} \\ &= X^{-i_0}\big(b_{i_0} + b_{i_0+1} X + \ldots\big)^{-1} \\ &= X^{-i_0}\big(b_{I_0}^{-1} + cX + \ldots\big) \end{aligned}$$

   De donde,

$$mult(f^{-1}) = -i_0 = -mult(f).$$

2. Ahora,

$$\begin{aligned} fg &= \left(\sum_{i=i_0}^{\infty} b_i X^i\right)\left(\sum_{i=j_0}^{\infty} c_i X^i\right) \\ &= b_{i_0} c_{j_0} X^{i_0+j_0} + dX^{i_0+j_0+1} + \cdots \end{aligned}$$

   Como $b_{i_0} c_{j_0} \neq 0$,

$$mult(fg) = i_0 + j_0 = mult(f) + mult(g).$$

3. Tenemos tres casos,

   Caso 1. Si $i_0 < j_0$.

$$f \pm g = b_{i_0}X^{i_0} + dX^{i_0+1} + \cdots$$

$$\begin{array}{rcl} ord(f \pm g) & = & i_0 \\ & = & min\{i_0, j_0\} \\ & = & mín\{mult(f), mult(g)\} \end{array}$$

   Caso 2. Si $i_0 = j_0$.

$$f \pm g = (b_{i_0} \pm c_{i_0})X^{i_0} + (b_{i_0+1} \pm c_{i_0+1})X^{i_0+1} + \cdots$$

$$\begin{array}{rcl} mult(f \pm g) & \geq & i_0 \\ & = & mín\{mult(f), mult(g)\} \end{array}$$

   Caso 3. Si $i_0 > j_0$.

$$f \pm g = \pm c_{j_0}X^{i_0} + dX^{i_0+1} + \cdots$$

$$\begin{array}{rcl} mult(f \pm g) & = & j_0 \\ & = & mín\{i_0, j_0\} \\ & = & mín\{mult(f), mult(g)\} \end{array}$$

   En cualquier caso

$$mult(f \pm g) \geq mín\{mult(f), mult(g)\}.$$

4. Finalmente,

$$mult(f) \geq 0 \Leftrightarrow i_0 \geq 0 \Leftrightarrow f \in K\big[[X]\big].$$

2.7. SUSTITUCIÓN EN $\boldsymbol{K}[[\boldsymbol{X_1}, \dots, \boldsymbol{X_r}]]$

Denotaremos S al anillo $K[[X_1, \dots, X_r]]$ y R al anillo $K[[Y_1, \dots, Y_s]]$. Denotaremos M_S y M_R los ideales maximales de S y R, respectivamente.

Sea $\Phi: R \to S$ un homomorfismo. Luego, la restricción de Φ al anillo de polinomios $K[Y_1, \dots, Y_s]$ es, también, un homomorfismo. Tenemos, así, que Φ es determinado por los valores

$$g_i = \Phi(Y_i), i = 1, \dots, s.$$

Esto es, si $p(Y_1, \dots, Y_s) \in K[Y_1, \dots, Y_s]$ entonces

$$\Phi(p(Y_1, \dots, Y_s)) = p(g_1, \dots, g_s)$$

Para estudiar los homomorfismos de R en S estudiaremos el problema de sustituir en una serie arbitraria $f \in R$ las indeterminadas $Y_1, \dots, Y_s$ por series $g_1, \dots, g_s \in S$.

Por ejemplo, podemos sustituir $Y_1, \dots, Y_s$ por 0 en f y obtenemos el término independiente de f. Pero, en general, no siempre es posible efectuar una sustitución, pues el resultado no siempre puede estar definido en S. Por ejemplo, si

$$f(X) = \sum_{k=0}^{\infty} X^k = 1 + X + X^2 + \cdots \in K[[X]]$$

Veremos en adelante que es siempre posible sustituir las indeterminadas $Y_1, \dots, Y_s$ por series de potencias $g_1, \dots, g_s \in M_S$ en cualquier $f \in R$, obteniendo de esta manera una serie de potencias

$$f(g_1, \dots, g_s) \in S.$$

Definición 2.7.1.

Dado $i \in \mathbb{N}$ y $f, h \in R$, se define f es congruente a h módulo M_R^i como

$$f \approx h \, mod \, M_R^i \Leftrightarrow f - h \in M_R^i.$$

Proposición 2.7.2.

Sean $f, h, h_1, h_2, f_1, f_2, \dots \in R$ y sea $g_1, \dots, g_s \in M_S$. Se cumple:

1. $f \approx h \; mod \; M_R^i \Leftrightarrow mult(f-h) \geq i$
2. Si $f_1 \approx f_2 \; mod \; M_R^i$ y $h_1 \approx h_2 \; mod \; M_R^i$, entonces

$$f_1 \pm h_1 \approx f_2 \pm h_2 \; mod \; M_R^i,$$

$$f_1 h_1 \approx f_2 h_2 \; mod \; M_R^i,$$

3. Si para todo $i \in \mathbb{N}$ se tiene que $f \approx h \; mod \; M_R^i$, entonces $f = h$.
4. Si f_1, f_2 son polinomios y $f_1 \approx f_2 \; mod \; M_R^i$, entonces

$$f_1(g_1, \dots, g_s) \approx f_2(g_1, \dots, g_s) \; mod \; M_S^i.$$

5. Si para todo $i \in \mathbb{N}$ se tiene que $f_{i+1} \approx f_i \; mod \; M_R^i$, entonces existe único $f \in R$ tal que

$$f \approx f_i \; mod \; M_R^i, i = 1,2, \dots$$

Demostración.

1. Como los elementos de M_R^i no tienen componente homogénea de grado $< i$, tenemos

$$\begin{aligned} f \approx h \; mod \; M_R^i \quad &\Leftrightarrow \quad f - h \in M_R^i \\ &\Leftrightarrow \quad mult(f-h) \geq i. \end{aligned}$$

2. Como $f_1 \approx f_2 \; mod \; M_R^i$ y $h_1 \approx h_2 \; mod \; M_R^i$, tenemos $f_1 - f_2, h_1 - h_2 \in M_R^i$. Luego,

$$(f_1 \pm h_1) - (f_2 \pm h_2) = (f_1 - f_2) \pm (h_1 - h_2) \in M_R^i,$$

de donde

$$f_1 \pm h_1 \approx f_2 \pm h_2 \; mod \; M_R^i.$$

Por otro lado, también

$$h_1(f_1 - f_2), f_2(h_1 - h_2) \in M_R^i,$$

se sigue que

$$f_1 h_1 - f_2 h_2 = h_1(f_1 - f_2) - f_2(h_1 - h_2) \in M_R^i,$$

de donde

$$f_1 h_1 \approx f_2 h_2 \; mod \; M_R^i,$$

3. Como $f \approx h \; mod \; M_R^i$ para todo $i \in \mathbb{N}$, esto es,

$$mult(f - h) \geq i \text{ para todo } i \in \mathbb{N}.$$

De donde, $f - h = 0$, esto es, $f = h$.

4. Como $f_1 \approx f_2 \ mod\ M_R^i$, tenemos $f_1 - f_2 \in M_R^i$. Esto implica que,
$$f_1 - f_2 = P_i + P_{i+1} + P_{i+2} + \cdots + P_d$$
donde cada P_j es un polinomio homogéneo de grado j. Se sigue que,
$$f_1(g_1, \dots, g_s) - f_2(g_1, \dots, g_s) = P_i(g_1, \dots, g_s) + \cdots + P_d(g_1, \dots, g_s).$$
Como $g_1, \dots, g_s \in M_S$, tenemos
$$mult(g_i) \geq 1 \ para\ todo\ i = 1, \dots, s.$$
Luego,
$$mult\left(P_j(g_1, \dots, g_s)\right) \geq j \geq i \ para\ todo\ j = i, i+1, \dots, d.$$
De donde, sumando los términos anteriores, tenemos
$$mult\big(f_1(g_1, \dots, g_s)\big) - mult\big(f_2(g_1, \dots, g_s)\big) \geq i.$$

5. Si para todo $i \in \mathbb{N}$ podemos escribir
$$f_i = \sum_{k=0}^{\infty} P_{i,k} = P_{i,0} + P_{i,1} + \cdots$$
donde cada $P_{i,j}$ es un polinomio homogéneo de grado j. Como
$$f_{i+1} \approx f_i \ mod\ M_R^i,$$

se sigue,

$$f_i - f_{i+1} = \left(P_{i,0} - P_{i+1,0}\right) + \cdots + \left(P_{i,i-1} - P_{i+1,i-1}\right) + \left(P_{i,i} - P_{i+1,i}\right) + \cdots \in M_R^i.$$

De aquí,

$$P_{i,0} = P_{i+1,0}, P_{i,1} = P_{i+1,1}, \dots, P_{i,i-1} = P_{i+1,i-1}$$

ya que todas las componentes homogéneas de grado menor que i de elementos de M_R^i deben de ser cero.

De donde, se sigue que

$$P_{i,j} = P_{k,j} \ para\ todo\ j \geq 0, k \geq j+1, i \geq j+1.$$

Definimos

$$f = \sum_{k=0}^{\infty} P_{k+1,k} = P_{1,0} + P_{2,1} + \cdots + P_{i+1,i} + \cdots$$

Tenemos, así,

$$\begin{aligned} f - f_i &= \sum_{k=0}^{\infty} P_{k+1,k} - P_{i,k} \\ &= \left(\sum_{k=0}^{i-1} P_{k+1,k} - P_{i,k}\right) + \left(P_{i+1,i} - P_{i,i}\right) + \cdots \\ &= 0 + \left(P_{i+1,i} - P_{i,i}\right) + \cdots \\ &= \left(P_{i+1,i} - P_{i,i}\right) + \cdots \in M_R^i. \end{aligned}$$

De donde,

$$f \approx f_i \; mod \; M_R^i \; para \; todo \; i \in \mathbb{N}.$$

Verifique que f es único. Sea $g \in R$ tal que

$$g \approx f_i \; mod \; M_R^i \; para \; todo \; i \in \mathbb{N}.$$

De esto,

$$f \approx g \; mod \; M_R^i \; para \; todo \; i \in \mathbb{N}.$$

Por el ítem 2, $f = g$. Termina la prueba. □

Definición 2.7.3.

Dado $r > 1$ definimos la función $d: S \times S \to [0, +\infty >$ definida como

$$d(f,h) = r^{-mult(f-h)}$$

Es una métrica en S.

Demostración.

Sean $f, h, g \in S$.

1. $d(f,h) \geq 0$.

   En efecto, debido a que $d(f,h)$ es potencia de base positiva.
2. $d(f,h) = 0$ si y solo si $f = h$.

   En efecto,

$$\begin{aligned} d(f,h)=0 &\Leftrightarrow r^{-mult(f-h)}=0 \\ &\Leftrightarrow mult(f-h)=+\infty \\ &\Leftrightarrow f-h=0 \\ &\Leftrightarrow f=h. \end{aligned}$$

3. $d(f,h)=d(h,f)$.

   En efecto,

$$\begin{aligned} d(f,h) &= r^{-mult(f-h)} \\ &= r^{-mult\left(-(f-h)\right)} \\ &= r^{-mult(h-f)} \\ &= d(h,f). \end{aligned}$$

4. $d(f,h)\leq d(h,g)+d(g,f)$.

   En efecto,

$$\begin{aligned} d(f,h) &= r^{-mult(f-h)} \\ &= r^{-mult\left(f-g+(g-h)\right)} \\ &\leq r^{-mín\{mult(f-g),mult(g-h)\}} \\ &= r^{máx\{-mult(f-g),-mult(g-h)\}} \\ &= máx\left\{r^{-mult(f-g)},r^{-mult(g-h)}\right\} \\ &\leq r^{-mult(f-g)}+r^{-mult(g-h)} \\ &= d(f,g)+d(g,h). \end{aligned}$$

Definición 2.7.4.

Dado $f\in S$ definiremos para $i\in\mathbb{N}$ el conjunto

$$V_i(f):=B\left(f,r^{-(i-1)}\right)=\left\{h\in S: d(f,h)<r^{-(i-1)}\right\}.$$

Proposición 2.7.5.

$V_i(f)=\left\{h\in S: f\approx h \; mod \; M_S^i\right\}$ para todo $i\in\mathbb{N}$.

Demostración.

$$\begin{aligned} h\in V_i(f) &\Leftrightarrow d(f,h)<r^{-(i-1)} \\ &\Leftrightarrow r^{-mult(f-h)}<r^{-(i-1)} \\ &\Leftrightarrow mult(f-h)>i-1 \\ &\Leftrightarrow mult(f-h)\geq i \\ &\Leftrightarrow f-h\in M_S^i \\ &\Leftrightarrow f\approx h \; mod \; M_S^i. \end{aligned}$$

Lema 2.7.6

Si $(g_i)_{i\in\mathbb{N}}$ sucesión de S tal que $g_{i+1} \approx g_i \; mod \; M_S^i$, entonces existe $g \in S$ tal que $\lim_{i\to+\infty} g_i = g$.

Demostración.

Por la proposición anterior, existe $g \in S$ tal que $g \approx g_i \; mod \; M_S^i$. Probemos que $\lim_{i\to+\infty} g_i = g$. Dado $i \in \mathbb{N}$, la relación $g \approx g_i \; mod \; M_S^i$ implica, $d(g_i, g) < r^{-(i-1)}$. Haciendo $i \to +\infty$, tenemos que $\lim_{i\to+\infty} g_i = g$. □

Proposición 2.7.7.

El espacio métrico (S, d) es completo.

Demostración.

Sea $(f_n)_{n\in\mathbb{N}}$ sucesión de Cauchy. Dado $i \in \mathbb{N}$ existe $N_i \in \mathbb{N}$ tal que $d(f_j, f_k) < r^{-(i-1)}$ para todo $j, k \geq N_i$. Podemos considerar $N_i < N_{i+1}$ para todo $i \in \mathbb{N}$. Consideremos $g_i = f_{N_i}$. Haciendo $j = N_{i+1}, k = N_i$, tenemos $d(g_{i+1}, g_i) = d\left(f_{N_{i+1}}, f_{N_i}\right) < r^{-(i-1)}$ para todo $i \in \mathbb{N}$. Luego,

$$d(g_{i+1}, g_i) < r^{-(i-1)} \quad \Leftrightarrow \quad g_{i+1} - g_i \in M_S^i.$$

Por el lema anterior, $(g_i)_{i\in\mathbb{N}}$ es convergente. Luego, la sucesión $(f_n)_{n\in\mathbb{N}}$ tiene una subsucesión convergente. Entonces, $(f_n)_{n\in\mathbb{N}}$ es una sucesión convergente. Por tanto, (S, d) es espacio métrico completo. □

Lema 2.7.8

Dados $g_1, \dots, g_s \in M_S$, $f \in R$, es siempre posible sustituir $Y_1 = g_1, \dots, Y_s = g_s$ en f.

Demostración.

Sea

$$f = F_0 + F_1 + \cdots$$

con F_m polinomio homogéneo de grado m. Para cada $i \in \mathbb{N}$, haciendo

$$f_i := F_0 + F_1 + \cdots + F_{i-1}$$

tenemos

$$f - f_i = F_i + F_{i+1} + \cdots \in M_R^i,$$

$$f_{i+1} - f_i = F_i \in M_R^i,$$

de donde,

$$f \approx f_i \; mod \; M_R^i,$$

$$f_{i+1} \approx f_i \; mod \; M_R^i.$$

Haciendo,

$$h_i := f_i(g_1, \dots, g_s),$$

Tenemos,

$$h_{i+1} \approx h_i \; mod \; M_S^i.$$

Existe único $h \in S$ tal que

$$h \approx h_i \; mod \; M_S^i.$$

Veamos, ahora, que h no depende la elección de los polinomios f_i. Sean f_i' otros polinomios tal que

$$f \approx f_i' \; mod \; M_R^i.$$

Sea $h' \in S$ construido a partir de f_i' de igual manera que h. Como $f \approx f_i \; mod \; M_R^i$, tenemos

$$f_i \approx f_i' \; mod \; M_R^i.$$

Po,

$$f_i(g_1, \dots, g_s) \approx f_i'(g_1, \dots, g_s) \; mod \; M_R^i.$$

De donde resulta que $h = h'$. Este único elemento $h \in S$ será denotada por $f_i(g_1, \dots, g_s)$.

□

Proposición 2.7.9

Dados $g_1, \dots, g_s \in M_S$ la función

$$\begin{array}{cccccc} S_{g_1,\dots,g_s} & : & R = K[[Y_1, \dots, Y_s]] & \to & S = K[[X_1, \dots, X_s]] \\ & & f & \to & f(g_1, \dots, g_s) \end{array}$$

es un homomorfismo.

Demostración.

Sean $f, h \in R$. Consideremos para cada $i \in \mathbb{N}$, como en el lema anterior, $f_i, h_i \in R$ tal que $f \approx f_i \; mod \; M_R^i, f_{i+1} \approx f_i \; mod \; M_R^i, h \approx h_i \; mod \; M_R^i, h_{i+1} \approx h_i \; mod \; M_R^i$. Tenemos,

$$f + h \approx f_i + h_i \; mod \; M_R^i, \quad f_{i+1} + h_{i+1} \approx f_i + h_i \; mod \; M_R^i, \qquad (*)$$

$$fh \approx f_i h_i \; mod \; M_R^i, \quad f_{i+1} h_{i+i} \approx f_i h_i \; mod \; M_R^i, \qquad (**)$$

Sustituyendo $Y_1 = g_1, \dots, Y_s = g_s$ en $f + g, fg$ tenemos

$$(f + h)(g_1, \dots, g_s), f(g_1, \dots, g_s) + h(g_1, \dots, g_s)$$

resuelven $(*)$; y

$$(fh)(g_1, \dots, g_s), f(g_1, \dots, g_s)h(g_1, \dots, g_s)$$

Resuelven $(**)$.

$$(f + h)(g_1, \dots, g_s) = f(g_1, \dots, g_s) + h(g_1, \dots, g_s)$$

$$(fh)(g_1, \dots, g_s), f(g_1, \dots, g_s)h(g_1, \dots, g_s)$$

Por tanto,

$$\begin{array}{rcl} S_{g_1,\dots,g_s}(f + h) & = & (f + h)(g_1, \dots, g_s) \\ & = & f(g_1, \dots, g_s) + h(g_1, \dots, g_s) \\ & = & S_{g_1,\dots,g_s}(f) + S_{g_1,\dots,g_s}(h) \\ S_{g_1,\dots,g_s}(fh) & = & (fh)(g_1, \dots, g_s) \\ & = & f(g_1, \dots, g_s)h(g_1, \dots, g_s) \\ & = & S_{g_1,\dots,g_s}(f)S_{g_1,\dots,g_s}(h) \end{array}$$

Como se quería. □

Proposición 2.7.11

El homomorfismo $S_{g_1,\dots,g_s}$ es continuo.

Demostración.

Dados $\varepsilon = r^{i-1}$ con $i \in \mathbb{N}$ y $f \in R$ tomaremos $\delta = \varepsilon = r^{i-1} > 0$. Dado $h \in R$ tal que $d(f,h) < \delta = r^{i-1}$. Esto significa que $f - h \in M_R^i$. De donde,

$$f(g_1, \dots, g_s) - h(g_1, \dots, g_s) \in M_S^i.$$

De donde:

$$d\big(f(g_1, \dots, g_s), h(g_1, \dots, g_s)\big) < \varepsilon = r^{i-1}.$$

Como se quería. □

Lema 2.7.12

Un subanillo A de S es denso en S si y solo si para todo polinomio homogéneo $P \in K[X_1, \dots, X_r]$ existe un elemento en $f \in A$ tal que P es la componente homogénea de grado $mult(f)$ de f.

Proposición 2.7.13

Sean $g_1, \dots, g_r \in S$ con componentes homogéneas lineales $L_1, \dots, L_r$ linealmente independiente sobre K. Entonces $S_{g_1,\dots,g_r}: S \to S$ es un automorfismo.

2.8. El cuerpo $\boldsymbol{K}\big((\boldsymbol{X})\big)^*$

Denotaremos

$$\overline{K((X))}$$

el cuerpo clausura algebraica de $K((X))$.

Dado n entero positivo, el polinomio

$$Y^n - X \in K((X))[Y]$$

debe contener soluciones en $\overline{K((X))}$.

Luego debe contener elementos de la forma

$$X^{1/n},$$

sujetos a las relaciones

1. $X^{1/1} = X$,
2. $(X^{1/rn})^r = X^{1/n}$ para todo $n, r \in \mathbb{Z}$ con $r > 0$.
3. $(X^{1/n})^s = X^{s/n}$ para todo $n, s \in \mathbb{Z}$.

De esta manera obtenemos extensiones

$$K\left(\left(X^{1/n}\right)\right)/K\big((X)\big).$$

Teorema 2.8.1.

La extensión

$$K\left(\left(X^{1/n}\right)\right)/K\big((X)\big)$$

es galoisiana con grupo de Galois isomorfo al grupo aditivo $\mathbb{Z}^n$.

Demostración.

Denotemos

$$G = G\left(K\left(\left(X^{1/n}\right)\right)/K\big((X)\big)\right).$$

Sea $\sigma \in G$,

$$\left(\sigma\big(X^{1/n}\big)\right)^n = \sigma\Big(\big(X^{1/n}\big)^n\Big) = \sigma(X) = X$$

De donde,

$$\sigma\left(X^{1/n}\right) \in K\left(\left(X^{1/n}\right)\right).$$

Luego, podemos escribir

$$\sigma\left(X^{1/n}\right) = \sum_{i=i_0}^{\infty} b_i X^{i/n}$$

Donde $b_i \in K$ para todo $i \geq i_0$ con $b_{i_0} \neq 0$. Luego,

$$\begin{array}{rcl} X & = & \left(\sigma\left(X^{1/n}\right)\right)^n \\ & = & \left(\sum_{i=i_0}^{\infty} b_i X^{i/n}\right)^n \\ & = & \left(b_{i_0} X^{i_0/n} + b_{i_0+1} X^{(i_0+1)/n} + \cdots \right)^n \end{array}$$

Igualando, obtenemos

$$i_0 = 1,\ b_{i_0}^n = b_1^n = 1 \text{ y } b_i = 0 \text{ para todo } i > i_0 = 1.$$

Denotando b_1 por b_σ, tenemos

$$\sigma\left(X^{1/n}\right) = b_\sigma X^{1/n}$$

donde b_σ es raíz n-ésima de la unidad.

Denotemos μ_n el conjunto de las raíces n-ésimas de la unidad. Definamos, entonces, la función

$$\begin{array}{rcccl} h & : & G & \rightarrow & \mu_n \\ & & \sigma & \mapsto & b_\sigma \end{array}$$

Se cumple que h es un homomorfismo.

En efecto,

$$\begin{array}{rcl} h(\rho \circ \sigma) X^{1/n} & = & (\rho \circ \sigma)\left(X^{1/n}\right) \\ & = & \rho\left(\sigma\left(X^{1/n}\right)\right) \\ & = & \rho\left(b_\sigma X^{1/n}\right) \\ & = & b_\sigma \rho\left(X^{1/n}\right) \\ & = & b_\sigma b_\rho X^{1/n} \end{array}$$

De donde,

$$h(\rho \circ \sigma) = b_\sigma b_\rho = b_\rho b_\sigma = h(\rho) h(\sigma).$$

Se cumple h es un monomorfismo.

En efecto, sea $\sigma \in G$ tal que $h(\sigma) = 1$. De donde, $b_\sigma = 1$. Luego,

$$\sigma\left(X^{1/n}\right) = b_\sigma X^{1/n} = X^{1/n}.$$

Esto es, σ es el isomorfismo identidad $K\left(\left(X^{\frac{1}{n}}\right)\right)$.

Esto comprueba que h es monomorfismo.

Se cumple h es un epimorfismo.

En efecto, sea $b \in \mu_n$. Definamos $\sigma_b \in G$ como

$$\sigma_b\left(X^{\frac{1}{n}}\right) = bX^{\frac{1}{n}}.$$

Claramente $h(\sigma_b) = b$.

Esto comprueba que h es epimorfismo.

Así, h es un isomorfismo.

Con esto, G es un grupo finito. Para probar que

$$K\left(\left(X^{\frac{1}{n}}\right)\right)/K\big((X)\big)$$

es extensión galoisiana debemos probar q ue

$$\left\{f \in K\left(\left(X^{\frac{1}{n}}\right)\right) : \sigma(f) = f \ \forall \sigma \in G\right\} = K\big((X)\big)$$

Sea

$$f = \sum_{i=i_0}^{\infty} b_i X^{i/n} \in K\left(\left(X^{1/n}\right)\right)$$

no nulo tal que

$$\sigma(f) = f \text{ para todo } \sigma \in G.$$

Dado $\sigma \in G$, existe $b \in \mu_n$ tal que $\sigma = \sigma_b$.

Luego,

$$\begin{aligned}
\sum_{i=i_0}^{\infty} b_i X^{i/n} &= \sigma_b\left(\sum_{i=i_0}^{\infty} b_i X^{i/n}\right) \\
&= \sigma_b\left(\sum_{i=i_0}^{\infty} b_i \left(X^{1/n}\right)^i\right) \\
&= \sum_{i=i_0}^{\infty} b_i \left(bX^{1/n}\right)^i \\
&= \sum_{i=i_0}^{\infty} b_i b^i X^{i/n}
\end{aligned}$$

Luego,

$$b_i = b_i b^i \text{ para todo } i \geq i_0.$$

Para todo i que no es divisible por n, escogiendo cómo b es raíz n-ésima primitiva de la unidad, tenemos $b^i \neq 1$.

Para todo i que no es divisible por n, tenemos entonces $b_i = 0$.

Luego,

$$\begin{aligned}
f &= \sum_{i=i_0}^{\infty} b_i X^{i/n} \\
&= \sum_{i \geq i_0} b_i X^{i/n} \\
&= \sum_{kn \geq i_0} b_{kn} X^{kn/n} \\
&= \sum_{kn \geq i_0} b_{kn} X^{k}
\end{aligned}$$

Esto es, $f \in K\big((X)\big)$.

El grupo de Galois G es isomorfo al grupo de las raíces n-ésimas de la unidad, que a su vez es isomorfo al grupo aditivo $\mathbb{Z}^n$.

Podemos definir entonces

$$K((X))^* = \bigcup_{n=1}^{\infty} K\left(\left(X^{\frac{1}{n}}\right)\right) \subseteq \overline{K((X))},$$

el cual es un cuerpo, ya que para todo n, m enteros positivos

$$K\left(\left(X^{\frac{1}{n}}\right)\right) \subseteq K\left(\left(X^{\frac{1}{nm}}\right)\right),$$

$$K\left(\left(X^{\frac{1}{m}}\right)\right) \subseteq K\left(\left(X^{\frac{1}{nm}}\right)\right).$$

También, definimos

$$K[[X]]^* = \bigcup_{n=1}^{\infty} K\left[\left[X^{\frac{1}{n}}\right]\right] \subseteq K((X))^*,$$

el cual es un anillo, ya que para todo n, m enteros positivos

$$K\left[\left[X^{\frac{1}{n}}\right]\right] \subseteq K\left[\left[X^{\frac{1}{nm}}\right]\right],$$

$$K\left[\left[X^{\frac{1}{m}}\right]\right] \subseteq K\left[\left[X^{\frac{1}{nm}}\right]\right].$$

Definición 2.8.2.

Dado $f \in K((X))^*$, existe n entero positivo tal que

$$f \in K\left(\left(X^{\frac{1}{n}}\right)\right)$$

Podemos escribir de manera única

$$f = \sum_{i=i_0}^{\infty} b_i X^{i/n}, b_i \in K, b_{i_0} \neq 0.$$

Definimos el orden de f, como

$$ord(f) = \frac{i_0}{n}.$$

Por comodidad se define

$$ord(0) = \infty.$$

Lema 2.8.3.

Dado $f, g \in K\big((X)\big)^*$ tenemos que:

1. Si $f(X) = p\big(X^{1/n}\big)$ para algún $p \in K\big((X)\big)$, entonces
$$ord(f) = \frac{mult(p)}{n}.$$
2. $ord(fg) = ord(f) + ord(g)$.
3. $ord(f \pm g) = min\{ord(f), ord(g)\}$.
4. $ord(f) \geq 0$ si y solo si $f \in K\big[[X]\big]^*$.

Demostración. Podemos escribir, para algún n entero positivo,

$$f(X) = p\big(X^{1/n}\big), g(X) = q\big(X^{1/n}\big)$$

con $p, q \in K\big((X)\big)$.

1. Si

$$p = \sum_{i=i_0}^{\infty} b_i X^{\mathrm{i}}, b_i \in K, b_{i_0} \neq 0,$$

entonces

$$f = \sum_{i=i_0}^{\infty} b_i X^{i/n}.$$

Luego,

$$ord(f) = \frac{i_0}{n} = \frac{mult(p)}{n}.$$

2. Ahora,

$$\begin{aligned} ord(fg) &= ord\left(p\left(X^{1/n}\right)q\left(X^{1/n}\right)\right) \\ &= \frac{mult(pq)}{n} \\ &= \frac{mult(p)}{n} + \frac{mult(q)}{n} \\ &= ord(f) + ord(g) \end{aligned}$$

3. Luego,

$$\begin{aligned} ord(f \pm g) &= ord\left(p\left(X^{1/n}\right) \pm q\left(X^{1/n}\right)\right) \\ &= \frac{mult(p \pm q)}{n} \\ &\geq \frac{mín\{mult(p), mult(q)\}}{n} \\ &= mín\left\{\frac{mult(p)}{n}, \frac{mult(q)}{n}\right\} \\ &= mín\{f, g\} \end{aligned}$$

4. Finalmente,

$$\begin{aligned} ord(f) \geq 0 &\Leftrightarrow \frac{mult(p)}{n} \geq 0 \\ &\Leftrightarrow mult(p) \geq 0 \\ &\Leftrightarrow p \in K\big[[X]\big] \\ &\Leftrightarrow f(X) = p\left(X^{1/n}\right) \in K\big[[X]\big]^* \end{aligned}$$

2.9. EL TEOREMA DE NEWTON-PIUSEUX

Lema 2.9.1.

Sean K un cuerpo y $p, q \in K[X]$ no constantes primos relativos tal que

$$\mathrm{gr}(p) = r, \mathrm{gr}(q) = s.$$

Dado $F \in K[X]$ tal que

$$\mathrm{gr}(f) \leq r + s,$$

existen únicos polinomios $g, h \in K[X]$ tales que

$$\mathrm{gr}(h) < r, \mathrm{gr}(g) < s$$

y

$$F = gp + hq.$$

Demostración.

Como $p, q \in K[X]$ son no constantes primos relativos, existen $m, n \in K[X]$ tales que

$$mp + nq = 1.$$

Multiplicando por F,

$$Fmp + Fnq = F.$$

Aplicando el algoritmo de la división a Fn y p, existen $a, h \in K[X]$ tales que

$$Fn = ap + h$$

Con $\deg(h) < \deg(p) = r$.

Reemplazando Fn en la igualdad anterior,

$$\begin{aligned} F &= Fmp + Fnq \\ &= Fmp + (ap + h)q \\ &= (Fm + aq)p + hq \end{aligned}$$

Denotemos $g = Fm + aq$.

Luego $F = gp + hq$, $\deg(h) < r$ y

$$\begin{array}{rcl} deg(g) & = & deg(F-hq)-deg(p) \\ & \leq & max\{deg(F), deg(h)+deg(q)\}-r \\ & < & max\{deg(F), r+deg(q)\}-r \\ & = & max\{r+s, r+s\}-r \\ & = & s. \end{array}$$

Falta probar la unicidad de h y g.

Supongamos otros h' y g' tal que

$$F = gp + hq = g'p + h'q$$

con $\deg(h') < r, \deg(g') < s$.

Luego,

$$(g-g')p = (h'-h)q$$

Como p y q son primos relativos, p divide a $h'-h$; de donde

$$\begin{array}{rcl} r & = & gr(p) \\ & \leq & gr(h'-h) \\ & \leq & max\{gr(h'), gr(h)\} \\ & < & max\{r, r\} \\ & = & r \end{array}$$

Esta contradicción, obliga que $h'-h=0$, esto es, $h=h'$.

De igual manera, $g=g'$. □

Lema 2.9.2 (Lema de Hensel).

Sea K un cuerpo y $f \in K[[X]][Y]$ mónico tal que

$$f(0,Y) = p(Y)q(Y)$$

donde $p(Y)$ y $q(Y)$ son coprimos en $K[Y]$ de grados r y s, respectivamente.

Entonces existen dos únicos $g, h \in K[[X]][Y]$ de grados r y s, respectivamente, tal que

$$f = gh$$

con

$$g(0,Y) = p(Y), \quad h(0,Y) = q(Y).$$

Demostración.

Sea $n = deg_Y(f)$.

Como $f \in K\big[[X]\big][Y]$ es mónico

$$f(X,Y) = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$$

luego

$$f(0,Y) = Y^n + a_1(0)Y^{n-1} + \cdots + a_n(0)$$

tiene grado n.

Escribimos

$$f(X,Y) = \sum_{i=0}^{\infty} f_i(Y)X^i = f_0(Y) + Xf_1(Y) + X^2 f_2(Y) + \cdots$$

Donde $f_i(Y) \in K[Y]$ para cada $i \geq 0$, con grado menor o igual a n, ya que $n = deg_Y(f)$. Haciendo X=0, tenemos

$$f_0(Y) = f(0,Y) \text{ tiene grado } n.$$

Debemos hallar

$$g(X,Y) = g_0(Y) + Xg_1(Y) + X^2 g_2(Y) + \cdots$$

$$h(X,Y) = h_0(Y) + Xh_1(Y) + X^2 h_2(Y) + \cdots$$

Cumpliendo lo pedido.

Como $f = gh$, deberíamos tener para cada $i \geq 1$

$$f_i(Y) = p(Y)h_i(Y) + g_1(Y)h_{i-1}(Y) + \cdots + g_i(Y)q(Y).$$

De donde

$$q(Y)g_i(Y) + p(Y)h_i(Y) = f_i(Y) - g_1(Y)h_{i-1}(Y) - \cdots - g_{i-1}(Y)h_1(Y).$$

Por inducción, conociendo

$$g_1(Y), \ldots, g_{i-1}(Y)$$

de grados menores e iguales a r y

$$h_1(Y), \ldots, h_{i-1}(Y)$$

de grados menores e iguales a r, por el lema anterior, podemos encontrar $g_i(Y), h_i(Y)$ de grados menores o iguales que r y s, respectivamente. $\square$

Finalmente, llegamos al resultado principal de este trabajo.

Teorema 2.9.3. (de Newton-Puiseux).

Si K es un cuerpo algebraicamente cerrado de característica 0, entonces

$$K\big((X)\big)^*$$

es algebraicamente cerrado**.**

Demostración.

Debemos probar que todo polinomio mónico de $K\big((X)\big)^*$ con grado mayor o igual a dos es reducible.

Tomemos

$$p(X,Y) = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X) \in K\big((X)\big)^*[Y]$$

con $n \geq 2$.

Consideremos el K-isomorfismo

$$\begin{array}{ccccc} \Phi & : & K\big[[X,Y]\big] & \to & K\big[[X,Z]\big] \\ & & p(X,Y) & \mapsto & p\big(X, Z - n^{-1}a_1(X)\big) \end{array}$$

y aplicando a $p(X,Y)$, tenemos el polinomio en $K\big((X)\big)^*[Z]$.

$$\begin{aligned} q(X,Z) &= \Phi\big(p(X,Y)\big) \\ &= p\big(X, Z - n^{-1}a_1(X)\big) \\ &= \big(Z - n^{-1}a_1(X)\big)^n + a_1(X)\big(Z - n^{-1}a_1(X)\big)^{n-1} + \cdots + a_n(X) \\ &= Z^n + \big(-n(n^{-1})a_1(X) + a_1(X)\big)Z^{n-1} + b_2(X)Z^{n-2} + \cdots + b_n(X) \\ &= Z^n + b_2(X)Z^{n-2} + \cdots + b_n(X) \end{aligned}$$

Ahora, tenemos dos casos:

Caso 1:

Si $b_i(X) = 0$ para todo $i = 2, \dots, n$.

Se sigue que $\Phi\big(p(X,Y)\big) = Z^n$ es reducible en $K\big((X)\big)^*[Z]$, y por tanto $p(X,Y)$ es reducible en $K\big((X)\big)^*[Y]$.

Caso 2:

Si $b_i(X) \neq 0$ para algún $i = 2, \dots, n$.

Denotemos por u_i el orden de $b_i(X)$ para cada $i = 2, \dots, n$ y sea

$$u = mín\left\{\frac{u_i}{i} : i = 2, \dots, n\right\}$$

Sea $i = 2, \dots, n$ tal que $u = \frac{u_r}{r}$.

Consideremos el isomorfismo

$$\begin{array}{cccc} \Psi & : & K\big((X)\big)^*[Z] & \to & K\big((W)\big)^*[Z] \\ & & f(X,Z) & \mapsto & f(W^r, ZW^{u_r}) \end{array}$$

que preserva los grados en Z, ya que $\Psi(Z) = ZW^{u_r}$.

Ψ tiene inverso

$$\begin{array}{cccc} \Psi^{-1} & : & K\big((W)\big)^*[Z] & \to & K\big((X)\big)^*[Z] \\ & & f(W,Z) & \mapsto & f\big(X^{1/r}, ZW^{-\mathrm{u}}\big) \end{array}$$

Sea

$$h(W,Z) \quad = \quad W^{-nu_r}\Psi(q(X,Z)).$$

Luego:

$$\begin{aligned} h(W,Z) &= W^{-nu_r}\Psi\big(q(X,Z)\big) \\ &= W^{-nu_r} q(W^r, ZW^{u_r}) \\ &= W^{-nu_r}\big((ZW^{u_r})^n + \textstyle\sum_{i=2}^n b_i(W^r)(ZW^{u_r})^{n-i}\big) \\ &= W^{-nu_r}W^{nu_r}Z^n + \textstyle\sum_{i=2}^n b_i(W^r) Z^{n-i} W^{(n-i)u_r} W^{-nu_r} \\ &= Z^n + \textstyle\sum_{i=2}^n b_i(W^r) W^{-iu_r} Z^{n-i} \end{aligned}$$

Denotando

$$c_i(W) = b_i(W^r)W^{-iu_r} \in K\big((X)\big)^*,$$

tenemos

$$h(W,Z) = Z^n + \sum_{i=2}^{n} c_i(W)Z^{n-i}.$$

Tenemos que, para todo $i = 2, \dots, n$,

$$\begin{array}{rcl} ord(c_i(W)) & = & ord\big(b_i(W^r)W^{-iu_r}\big) \\ & = & ord\big(b_i(W^r)\big) + ord\big(W^{-iu_r}\big) \\ & = & ru_i - iu_r \\ & \geq & 0 \end{array}$$

ya que

$$\frac{u_i}{i} \geq \frac{u_r}{r},$$

y también,

$$ord(c_r(W)) = 0.$$

En consecuencia,

$$c_r(0) = 0$$

y

$$c_i(W) \in K\big[[W]\big]^* \text{ para todo } i = 2, \dots, n.$$

Ahora, tomemos, M entero positivo tal que

$$h(W^M,Z) = Z^n + \sum_{i=2}^{n} c_i(W^M)Z^{n-i} \in K\big[[W]\big][Z].$$

Como $c_r(0) = 0$ y evaluando $h(W^M,Z)$ en $W = 0$, tenemos

$$h(0,Z) = Z^n + \sum_{i=2}^{n} c_i(0)Z^{n-i}$$

y podemos factorizar

$$h(0,Z) = \overline{h_1}(Z)\overline{h_2}(Z)$$

Por el lema de Hensel, existen

$$h(W^M, Z) = h_1(W,Z)h_2(W,Z).$$

De donde,

$$h(W,Z) = h_1\left(W^{1/M}, Z\right)h_2\left(W^{1/M}, Z\right).$$

Luego,

$$\begin{aligned}
q(X,Z) &= \Psi^{-1}\left(W^{nu_r}h(W,Z)\right) \\
&= \Psi^{-1}\left(W^{nu_r}h_1\left(W^{1/M},Z\right)h_2\left(W^{1/M},Z\right)\right) \\
&= \Psi^{-1}(W^{nu_r})\Psi^{-1}\left(h_1\left(W^{1/M},Z\right)\right)\Psi^{-1}\left(h_2\left(W^{1/M},Z\right)\right) \\
&= W^{nu_r/r}\Psi^{-1}\left(h_1\left(W^{1/M},Z\right)\right)\Psi^{-1}\left(h_2\left(W^{1/M},Z\right)\right)
\end{aligned}$$

En consecuencia, $q(X,Z)$ es reducible en $K\big((X)\big)^*[Z]$, esto es, existen

$$q_1(X,Z), q_2(X,Z) \in K\big((X)\big)^*[Z]$$

no invertibles tal que

$$q_1(X,Z) = q_1(X,Z)q_2(X,Z).$$

Luego,

$$\begin{aligned}
p(X,Y) &= \Phi^{-1}\big(q(X,Z)\big) \\
&= \Phi^{-1}\big(q_1(X,Z)q_2(X,Z)\big) \\
&= \Phi^{-1}\big(q_1(X,Z)\big)\Phi^{-1}\big(q_2(X,Z)\big)
\end{aligned}$$

Y por tanto $p(X,Y)$ es reducible en $K\big((X)\big)^*[Y]$.

CAPÍTULO III

VARIABLES E HIPÓTESIS

3.1 Variables de la investigación

La variable de investigación es el anillo de series de potencias formales $\mathbb{C}[\![x,y]\!] = A$

3.2 Operacionalización de variables

Usaremos el teorema de preparación de Weierstrass que consiste en preparar una serie de potencias:

$$f(x,y) = F_n(x,y) + F_{n+1}(x,y) + \cdots + F_j(x,y) \in \mathbb{C}[\![x,y]\!]$$

con multiplicidad n y $F_j(x,y)$ polinomios homogéneos de grado j, en una serie polinómica de la forma

$$f(x,y) = Y^n + a_1\,(x)\,Y^{n-1} + \cdots + a_j\,(x)\,Y^{n-j} + \cdots + a_n\,(x)$$

donde; $a_j\,(x) \in \mathbb{C}[\![x]\!]$

3.3 Hipótesis General

Es factible parametrizar una curva algebraica plana representada en un polinomio de Weierstrass, como consecuencia al teorema de Newton-Puiseux.

3.4 Hipótesis Específica

Dado una serie de potencias formales f ∈ $\mathbb{C}[\![x,y]\!]$, es posible tener su equivalente en un polinomio de Weierstrass f ∈ $\mathbb{C}((x))[y]$.

CAPÍTULO IV

METODOLOGÍA

4.1 Tipo de la investigación:

El presente trabajo se encuentra inmerso en un nivel de investigación descriptiva, tanto en los resultados obtenidos como en su aplicación, teniendo como el universo, el álgebra.

El método a utilizar es de tipo deductivo y analítico, el que permitirá establecer el teorema de Newton-Puiseux.

4.2 Diseño de la investigación

Primero presentamos un soporte teórico del anillo de las series de potencias formales, segundo presentamos el teorema de preparación de Weierstrass que permite escribir una serie de potencias en un polinomio.

Tercero, probamos el teorema de Newton Puiseux cuya consecuencia permite ver un polinomio de Weierstrass en su forma parametrizada.

4.3 Población y muestra

Por ser nuestro trabajo de carácter abstracto, no existe población ni muestra que tomar. Sin embargo el tema a tratar está inmerso dentro de las Series de Potencias formales en los polinomios de Weierstrass.

4.4 Técnicas e instrumentos de recolección de datos

Para la realización de nuestro trabajo se revisará bibliografía especializada así como también tesis de licenciatura y de maestría de universidades de la capital.

4.5 Plan de análisis estadístico de datos

La presente investigación no requerirá de análisis estadísticos de datos por ser un tema netamente abstracto.

CAPÍTULO V

RESULTADOS

1. Todo ideal de $K[[X]]$ es generado por un X^k para algún $k \geq 0$.
2. El anillo $K[[X]]$ es un dominio de ideales principales.
3. La extensión $K\left(\left(X^{\frac{1}{n}}\right)\right) \backslash K((X))$ es galoisiana con grupo de Galois isomorfo al grupo aditivo $\mathbb{Z}^n$.
4. Si K es un cuerpo algebraicamente cerrado de característica 0, entonces $K((X))^*$.

CAPÍTULO VI

DISCUSIÓN DE RESULTADOS

1. El anillo $K[[X]]$ es dominio de ideales principales al igual que $K[X]$.
2. Es falso que $K((X))^*$ sea un cuerpo algebraicamente cerrado para K, un cuerpo algebraicamente cerrado de característica $p > 0$.

CAPÍTULO VII

CONCLUSIONES

1. En este trabajo se usó muchas de las definiciones principales del álgebra abstracta, como son anillos, cuerpos, polinomios, series de potencias, clausura algebraica, etc.
2. En este trabajo se usó nociones del análisis, como son funciones continuas y convergencia de sucesiones.
3. En este trabajo se usaron conjuntamente herramientas del álgebra y análisis.

REFERENCIAS BIBLIOGRÁFICAS

[1]. I.N. HERSTEIN, **Álgebra Moderna, Editorial Trillas**, Sexta impresión, 1983.

[2]. PAUL J. MC CARTHY, **Algebraic Extensions of Fields**, Editorial Springer, Cuarta Edición , 2000.

[3]. M.F. ATIYAH – L.G. MACDONALD, **Introducción al Algebra Conmutativa**, Editorial Reverté S.A., Tercera edición, 1998.

[4]. A. HEFEZ **– Irreducible Plane Curve Singularities. Real and Complex Singularities**,1 – 120. Lectures Notes in Pure and Appl, Math. 232 Dekker, New York (2003)

[5]. EDISON NIÑO DE GUZMÁN, **Moduli Analítico de Curvas Analíticas Irreducibles Planas**, publicación Tesis de Maestría. PUCP, 2011.

[6]. HEFEZ, M.E HERNANDEZ. –**The Analytic Classification of Plane Branches**, Bull. London Math. Soc. 43 (2013) 289-298.

[7]. E. LIMA, **Espacios Métricos**, Quinta edición, IMPA, Río de Janeiro, 2017.

ANEXO

MATRIZ DE CONSISTENCIA

TITULO: ''TEOREMA DE NEWTON-PUISEUX EN LAS CURVAS PLANAS''

PROBLEMA	OBJETIVOS	VARIABLES E HIPÓTESIS	METODOLOGÍA	POBLACIÓN
PROBLEMA GENERAL En la presente investigación pretendemos demostrar el teorema Newton-Puiseux en las curvas planas para así poder aplicarla. **FORMULACIÓN DEL PROBLEMA** Se quieren resolver las siguientes interrogantes. ¿Será posible conocer las raíces de un polinomio de Weierstrass P, en el cierre algebraico de $\mathbb{C}((x))$? De ser así ¿Cómo podríamos explicitar $P(x,y)=\prod_{i=1}^{n}(y-\alpha_i)$ donde $\alpha_i=\varphi\left(\xi^i x^{1/n}\right)\in\mathbb{C}((x))$?	**OBJETIVO GENERAL** Demostraremos el teorema de Newton-Puiseux que afirma que la cerradura del cuerpo de fracciones de $\mathbb{C}[\![x]\!]$ es $\bigcup_{n=1}^{\infty}\mathbb{C}(x^{\frac{1}{n}})$) Y como consecuencia de ello mostrar que existe una parametrización: $\begin{cases} \mathrm{x}=T^n \\ \mathrm{y}=\sum_{i\geq 1} b_i T^i \end{cases}$ de $f(x,y)$. **OBJETIVO ESPECÍFICO** - Estudiar el Teorema de Preparación de Weierstrass. - Estudiar las curvas algebraicas planas para la demostración del teorema Newton-Puiseux	**VARIABLES DE LA INVESTIGACIÓN** La variable de investigación es el anillo de series de potencias formales $\mathbb{C}[\![x,y]\!]=A$ **HIPÓTESIS GENERAL** Es factible parametrizar una curva algebraica plana representada en un polinomio de Weierstrass, como consecuencia al teorema de Newton-Puiseux.	**TIPO DE INVESTIGACIÓN** El presente trabajo se encuentra inmerso en un nivel de investigación básica, tanto en los resultados obtenidos y como en su aplicación, teniendo como el universo, el álgebra. **DISEÑO DE INVESTIGACIÓN** Presentamos un soporte teórico del anillo de las series de potencias formales, luego presentamos el teorema de preparación de Weierstrass que permite escribir una serie de potencias en un polinomio y probamos el teorema de Newton Puiseux cuya consecuencia permite ver un polinomio de Weierstrass en su forma parametrizada.	Tenemos como población, las series de potencias formales, luego los polinomios de Weierstrass y como consecuencia la parametrización.