Universidad de Valladolid

Facultad de ciencias

Trabajo fin de grado

Grado en matemáticas

Cálculos con series de potencias. Anillos completos

Autora: Marina Alonso García
Tutor: Santiago Encinas Carrión

Julio 2025

Agradecimientos

A Santiago, mi tutor, por toda su ayuda y atención,
que sin él no habría llegado hasta aquí.

A Chus, la profesora que me acercó a este mundo,
y me mostró que las matemáticas eran más que solo números.

A mis padres, por toda la paciencia durante estos cuatro años,
gracias por vuestro apoyo incondicional.

A mis amigos, por sacarme una sonrisa incluso viendo las notas.
En especial a Claudia, por estar siempre ahí,
incluso desde Oviedo.

A Gonzalo, por aguantar todos mis llantos y dramas.
Gracias por guiarme en este camino.

Índice general

Resumen

Este trabajo tiene como objetivo el estudio de los anillos de series de potencias formales, explorando en qué medida se puede trasladar parte de la teoría de los anillos de polinomios. Se abordan conceptos fundamentales de álgebra conmutativa, como la localización, los anillos noetherianos, los módulos y las extensiones de anillos. Posteriormente, se estudian las propiedades algebraicas y topológicas de los anillos de series de potencias, centrándose en los teoremas de División y Preparación de Weierstrass, que generalizan el algoritmo de la división euclídea en este contexto. Finalmente, se introduce el concepto de base estándar y su importancia en el cálculo computacional dentro de la geometría analítica local.

Palabras clave: series de potencias formales, bases estándar, teorema de División de Weierstrass, localización.

Abstract

This thesis focuses on the study of formal power series rings, examining to what extent part of the theory of polynomial rings can be extended to this context. Key notions from commutative algebra are revisited, such as localization, Noetherian rings, modules, and ring extensions. The algebraic and topological structure of formal power series rings is then explored, emphasizing the Weierstrass Division and Preparation Theorems, which generalize the Euclidean division algorithm. This work concludes with the introduction of standard bases and their relevance for computational purposes in local analytic geometry.

Key words: formal power series, standard basis, Weierstrass Division theorem, localization.

Introducción

Las series de potencias formales son una generalización natural de los polinomios, en las que se permite un número infinito de términos, constituyendo así una herramienta fundamental en varias áreas de las matemáticas, especialmente en álgebra conmutativa y geometría analítica. A diferencia de las series convergentes que aparecen en análisis, las series de potencias formales se estudian desde un punto de vista puramente algebraico, lo que proporciona mayor flexibilidad en ciertos desarrollos teóricos. Por ejemplo, permite trabajar con resultados análogos a los teoremas de la función implícita y la función inversa sin necesidad de recurrir a nociones como la continuidad o la diferenciabilidad, como veremos en el Capítulo 3.

El objetivo de este trabajo es estudiar cómo se puede trasladar parte de la teoría de los anillos de polinomios a los anillos de series de potencias formales, teniendo en cuenta que con esta transición se introducen nuevas restricciones y problemas que requieren un tratamiento más cuidadoso. Para poder visualizar alguna de las ideas desarrolladas y aplicaciones de los teoremas, usaremos el programa SINGULAR, especializado en álgebra computacional. El Capítulo 6 del libro [4] de Greuel y Pfister ha servido como guía principal para el desarrollo de una parte del contenido, especialmente en lo referente a los algoritmos y técnicas aplicadas al anillo de series de potencias formales.

En el Capítulo 1 se revisarán algunos conceptos fundamentales del curso de Álgebra Conmutativa, centrados principalmente en el estudio del anillo de polinomios, que servirán de base para los desarrollos posteriores del trabajo. Entre ellos se encuentran la localización, los anillos noetherianos, los módulos y la normalización de Noether. Para facilitar su comprensión, se han consultado varios manuales de Álgebra Conmutativa, entre los que destacan el de Bosch [5], el Stacks Project [8], y especialmente las notas de Gathmann [6]. Además, se introducirán nociones nuevas para mí, como los órdenes monomiales y las bases estándar, que no formaban parte del temario del curso pero son esenciales desde el punto de vista computacional.

En el Capítulo 2 comenzaremos a trabajar con el anillo de series de potencias formales. Presentaremos sus propiedades básicas y algunas definiciones fundamentales que nos permitirán comprender mejor su estructura algebraica. En particular, introduciremos una topología sobre este anillo, con la que podremos demostrar que $K[[x]]$ es un anillo local y completo.

En el Capítulo 3, estudiaremos los Teoremas de División y Preparación de Weierstrass, que permiten generalizar el algoritmo de la división euclídea al contexto de series de potencias formales. A partir de estos resultados, demostraremos que $K[[x]]$ es un anillo noetheriano, e introduciremos algunas herramientas que nos permitirán determinar cuando un módulo está finitamente generado. Finalmente, enunciaremos la Normalización de Noether en el caso de series de potencias formales.

En el último capítulo, nos centraremos en el estudio de las bases estándar en el anillo de series de potencias formales. Estudiaremos una generalización del Teorema de División, es decir, el Teorema de División de Grauert, que extiende el algoritmo clásico a este nuevo entorno. Asimismo, veremos cómo se pueden calcular las bases estándar a partir de ideales generados únicamente por polinomios, lo que permite aprovechar herramientas desarrolladas previamente. Estos resultados constituyen una base fundamental para la parte computacional de la geometría analítica local.

Capítulo 1

Preliminares

1.1. Localización

La localización es una herramienta fundamental que permite estudiar las propiedades de un anillo o módulo en un contexto más accesible, al hacer invertibles ciertos elementos. En esta sección se introducen las definiciones básicas y algunos resultados que se utilizarán más adelante en el trabajo.

Definición 1.1.1. Sea A un anillo.

1) Se dice que es **local** si solo tiene un idea maximal $\mathfrak{m}$. $A/\mathfrak{m} = \kappa$ se llama **cuerpo residual** de A.

2) Si tiene un número finito de ideales maximales se denomina **semi-local**.

Definición 1.1.2. Sean $(A_1, \mathfrak{m}_1, \kappa_1)$, $(A_2, \mathfrak{m}_2, \kappa_2)$ dos anillos locales. Un **homomorfismo de anillos locales** es un morfismo de anillos $\varphi : A_1 \to A_2$ tal que $\varphi(\mathfrak{m}_1) \subset \mathfrak{m}_2$.

La localización permite introducir las fracciones en un anillo donde no todos los elementos no nulos son unidades, esto es, que no es un cuerpo. Es decir, consiste en generalizar la construcción del cuerpo de fracciones, $\{Q(A), +, \cdot\}$, donde A es un dominio,

$$\mathrm{Quot}(A) := Q(A) := \left\{ \frac{a}{b} \;\middle|\; a, b \in A, b \neq 0 \right\}$$

y las operaciones vienen dadas por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Asimismo, por $\frac{a}{b}$ nos referimos a la clase de equivalencia (a,b) dada por la relación

$$(a, b) \sim (c, d) \Longleftrightarrow ad = cb.$$

Nuestro objetivo consiste en la generalización de este proceso. Para ello, es necesario introducir las siguientes nociones.

Definición 1.1.3. Sea A un anillo.

1) Un subconjunto $S \subset A$ se dice que es **multiplicativamente cerrado** si se cumple:

   a) $1 \in S$

   b) $a \in S,\ b \in S \Rightarrow ab \in S$

2) Sea $S \subset A$ multiplicativamente cerrado. La **localización** o el **anillo de fracciones** $S^{-1}A$ de A respecto a S es:

$$S^{-1}A := \left\{ \frac{a}{b} \;\middle|\; a, b \in A, b \in S \right\},$$

   donde a/b denota la clase de equivalencia $(a, b) \in A \times S$ con

$$(a, b) \sim (c, d) \Longleftrightarrow \exists\ s \in S \text{ tal que } s(ad - cb) = 0.$$

   Además, se definen la suma y la multiplicación de la misma manera que para el cuerpo de fracciones.

Veamos que $\sim$ es una relación de equivalencia:

1) **Reflexiva**: tomando $s = 1$, se tiene que

$$(a, b) \sim (a, b) \Longleftrightarrow 1 \cdot (ab - ab) = 0.$$

2) **Simétrica**: $(a, b) \sim (c, d) \Longleftrightarrow \exists\ s \in S$ con $s(ad - cb) = 0$.
   Si se multiplica por -1 en la igualdad anterior, que es equivalente a tomar $s' = -s$, se tiene que $-s(ad-cb) = 0 = s'(cb-ad)$. Por lo tanto, se cumple $(c, d) \sim (a, b)$.

3) **Transitiva**: $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$, entonces $\exists\ s, t \in S$ tales que:

$$(ad - cb)s = 0, \quad (cf - ed)t = 0$$

   Multiplicando las dos ecuaciones anteriores por ft y bs, respectivamente, y sumándolas se tiene:

$$0 = (ad - cb)s \cdot ft + (cf - ed)t \cdot bs = (af - eb)std,$$

   donde $std \in S$, por ser S multiplicativamente cerrado. Por consiguiente, $(a, b) \sim (e, f)$.

Proposición 1.1.4. *1) Las operaciones $+$ y $\cdot$ en $S^{-1}A$ están bien definidas, es decir, son independientes de los representantes elegidos. Además, $(S^{-1}A, +, \cdot)$ es un anillo conmutativo con unidad $1/1 = 1$.*

2) La inclusión canónica $\varphi : A \to S^{-1}A$ dada por $\varphi(a) = \frac{a}{1}$ es un homomorfismo de anillos.

Demostración. 1) En primer lugar, veamos que las operaciones están bien definidas. Sean $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$, entonces

$$\exists\, s, t \in S \text{ tales que } s(ab' - a'b) = 0, \quad t(cd' - c'd) = 0. \tag{1.1}$$

Queremos ver que $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ pertenece a la misma clase que $\frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd'+c'b'}{b'd'}$. Es decir, queremos probar que

$$\exists\, r \in S \,:\, r\,[(ad + cb)b'd' + (a'd' + b'c')bd] = 0.$$

Expandiendo el producto y reagrupando se tiene que:

$$b'd'ad + b'd'cb - bda'd' - bdb'c' = dd'(ab' - a'b) + bb'(cd' - c'd).$$

Si multiplicamos ahora por st, por ser A conmutativo, y usando las relaciones en (1.1), los dos términos se anulan, por lo que podemos elegir $r = st$, concluyendo que la suma está bien definida.
Ahora veamos qué sucede con el producto. Elegimos los mismos elementos que antes, y queremos ver que $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ y $\frac{a'}{b'} \cdot \frac{c'}{d'} = \frac{a'c'}{b'd'}$ pertenecen a la misma clase, es decir, queremos probar que:

$$\exists\, r \in S : r(acb'd' - a'c'bd) = 0.$$

Por (1.1), se tiene que $sab' - sa'b = 0 \Rightarrow sab' = sa'b$ y $tcd' - tc'd = 0 \Rightarrow tcd' = tc'd$. Podemos multiplicar ambas igualdades y se obtiene:

$$(sab')(tcd') = (sa'b)(tc'd).$$

Como A es conmutativo, podemos reagrupar los términos, y eligiendo de nuevo $r = st$, se tiene que el producto también está bien definido.
El resto de las propiedades de $S^{-1}A$ se heredan de A, con $0 := \frac{0}{1}$ el elemento neutro para la suma y $1 := \frac{1}{1}$ el elemento neutro para el producto.
2) Veamos ahora que la inclusión canónica φ es un morfismo de anillos. En primer lugar, $\varphi(1) = \frac{1}{1} = 1$. Por como se han definido las operaciones, se tiene que

$$\varphi(a) + \varphi(b) = \frac{a}{1} + \frac{b}{1} = \varphi(a + b), \quad \varphi(a) \cdot \varphi(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} = \varphi(ab).$$

□

Ejemplo 1.1.5. Un caso especial es la localización de $K[x] = K[x_1, ..., x_n]$ con respecto al ideal maximal $\langle x \rangle = \langle x_1, ..., x_n \rangle$, que viene dada por:

$$K[x]_{\langle x \rangle} = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[x],\ g(0) \neq 0 \right\}.$$

Profundizaremos más en ella en el Capítulo 2.

1.2. Anillos noetherianos e ideales

En esta sección vamos a introducir alguna caracterización de los anillos noetherianos, que será de gran importancia para el estudio de los anillos de polinomios, gracias al Teorema de la base de Hilbert (1.2.2). Además, repasaremos ciertas operaciones con ideales, que nos serán de utilidad para la demostración de algún teorema de los siguientes capítulos.

1.2.1. Anillos noetherianos

Definición 1.2.1. A es un **anillo noetheriano** si satisface las siguientes condiciones equivalentes:

1) Todo conjunto no vacío de ideales en A tiene un elemento maximal.

2) Toda cadena ascendente de ideales en A

$$I_1 \subset I_2 \subset ... \subset I_j \subset ...$$

se estabiliza, es decir, existe un k_0 tal que $I_k = I_{k_0}$ para todo $k \geq k_0$.

3) Todo ideal en A está finitamente generado.

La demostración de esta equivalencia se encuentra en el Capítulo 7 de [6], aplicando el Lema 7.4 considerando A como un A-módulo.
Para demostrar la Proposición 3.2.6, en la que se establece que $K[[x_1, ..., x_n]]$ es un anillo noetheriano si K es un cuerpo, utilizaremos un resultado fundamental: el Teorema de la base de Hilbert.

Teorema 1.2.2 (Teorema de la base de Hilbert)**.** *Si A es un anillo noetheriano, entonces el anillo de polinomios $A[x_1, ..., x_n]$ es noetheriano.*

La demostración se puede encontrar en el Capítulo 7 de [6].

1.2.2. Ideales

Definición 1.2.3. Sean A un anillo, $I, J \subset A$ ideales. El **cociente de ideales** de I por J se define como:

$$I : J := \{a \in A \mid aJ \subset I\}.$$

Un caso particular es el **anulador** de J, que es:

$$\langle 0 \rangle : J := \mathrm{Ann}_A(J) = \{a \in A \mid aJ \subset 0\}.$$

Si no hay confusión sobre el ideal donde se está trabajando, se denotará simplemente por $\mathrm{Ann}(J)$.

1.3. Módulos

Una de las estructuras más importantes en álgebra conmutativa son los módulos, que pueden considerarse como una generalización de los espacios vectoriales, pero donde el producto escalar se define sobre un anillo conmutativo en lugar de un cuerpo.

Definición 1.3.1. Sea A un anillo. Un conjunto M, junto con las dos operaciones:

$$+ : M \times M \to M \text{ (suma)} \qquad \cdot : R \times M \to M \text{ (producto escalar)},$$

se llama A**-módulo** si para todo $a, b \in A$, $m, n \in M$ se cumple:

1) $(M, +)$ es un grupo abeliano.

2) $(a + b) \cdot m = a \cdot m + b \cdot m$ y $a \cdot (m + n) = a \cdot m + a \cdot n$, la suma y el producto escalar satisfacen la propiedad distributiva.

3) $(a \cdot b) \cdot m = a \cdot (b \cdot m)$, el producto escalar es asociativo.

4) $1 \cdot m = m$, con $1 \in A$. Si el contexto es claro, se dirá que M es un módulo sobre R, o que es simplemente un módulo.

Observación 1.3.2. Un semimódulo sobre un semianillo tiene una estructura análoga a la de un módulo, salvo que $(M, +)$ es un monoide conmutativo en vez de un grupo abeliano, por lo que no está garantizada la existencia de elementos inversos.
Este concepto será necesario para la demostración del Teorema 4.0.4

Definición 1.3.3. Sea M un A-módulo. Un conjunto no vacío $N \subset M$ es un **submódulo** de M, si para todo $m, n \in N$, $a \in A$, se cumple $m + n \in N$ y $a \cdot m \in N$.
N es un A-módulo con la misma suma y producto escalar que en M.

Definición 1.3.4. Sean M, N A-módulos. Un homomorfismo $\varphi : M \to N$ se llama **homomorfismo de A-módulos** si para todo $a \in A$ y $m, n \in M$ se tiene:

1) $\varphi(am) = a\varphi(m)$,

2) $\varphi(m + n) = \varphi(m) + \varphi(n)$.

Si $N = M$, entonces φ es un **endomorfismo**.
El conjunto de todos los homomorfismos de A-módulos de M a N se denota por $\mathrm{Hom}_A(M, N)$.

Vamos a introducir algunos conceptos, que se pueden considerar como una generalización de aquellos mencionados en la sección 1.2.2 sobre ideales.

Definición 1.3.5. Sean N, P dos submódulos de M, el **cociente de módulos** de N por P es:

$$N : P := N :_A P := \{a \in A \mid aP \subset N\}.$$

Un caso particular, es de nuevo el **anulador** de P, que es:

$$\mathrm{Ann}(P) := \mathrm{Ann}_A(P) := \langle 0 \rangle : P = \{a \in A \mid aP = 0\}.$$

Definición 1.3.6. Sea I un ideal de A, se define

$$IM := \left\{ \sum_{j \in J} a_j m_j \,\middle|\, J \text{ finito},\ a_j \in I,\ m_j \in M \right\}$$

Definición 1.3.7. Sea M un A-módulo, y sea S un subconjunto de elementos de M. Entonces, el conjunto

$$\langle S \rangle := \{a_1 m_1 + ... + a_n m_n \mid n \in \mathbb{N}, a_1, ..., a_n \in A, m_1, ..., m_n \in S\}$$

de todas las combinaciones lineares de elementos de S con coeficientes en A es el submódulo más pequeño de M que contiene a S. También se llama el submódulo **generado** por S.
Si $S = \{m_1, ..., m_n\}$ es finito, se puede escribir $\langle S \rangle = \langle \{m_1, ..., m_n\} \rangle$ como $\langle m_1, ..., m_n \rangle$. Se dice que M está **finitamente generado** si $M = \langle S \rangle$ para S un subconjunto finito de M.

Definición 1.3.8. Sea $M_i, i \in I$ A-módulos. La **suma directa** es

$$\bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i, m_i \neq 0 \text{ para solo un número finito de índices}\}.$$

El **producto directo** es

$$\prod_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i\}.$$

Observación 1.3.9. Para un conjunto finito de índices $I = \{1, ..., n\}$, la suma directa y el producto directo coinciden y se denota por

$$M_1 \oplus ... \oplus M_n.$$

Definición 1.3.10. Sea M un A-módulo, se dice que es **libre** si $M \cong \bigoplus_{i\in I} A$. El cardinal del conjunto de índices I se llama **rango** de M.
Un subconjunto $S \subset M$ es una **base** de M si todo $m \in M$ se puede escribir de manera única como una combinación lineal $m = a_1m_1 + ... + a_nm_n$ con $m_i \in S$, $a_i \in A$, para un n que depende de m.

Teorema 1.3.11 (Cayley-Hamilton)**.** *Sea A un anillo, $I \subset A$ un ideal , M un A-módulo finitamente generado y sea $\varphi : M \to M$ un endomorfismo entre A-módulos con $\varphi(M) \subset IM$.*
Entonces existe un polinomio mónico

$$p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \quad \in A[x]$$

con $a_o, ..., a_{n-1} \in I$ y

$$p(\varphi) := \varphi^n + a_{n-1}\varphi^{n-1} + ... + a_0 id = 0 \quad \in Hom_A(M, M),$$

donde φ^i denota la i-ésima composición de φ consigo misma.

La demostración se puede encontrar en la Sección 4.1 de [2].

1.4. Extensiones de anillos

1.4.1. Extensiones Enteras y Finitas

Definición 1.4.1. Sea A un anillo. Una **A-álgebra** es un anillo B junto con un morfismo de anillos $\varphi : A \to B$.

Definición 1.4.2. Sean $A \subset B$ dos anillos.

1) $b \in B$ es **entero** sobre A si existe un polinomio mónico $f \in A[x]$ tal que $f(b) = 0$, es decir, existen $n \in \mathbb{N}_{>0}$ y $c_0, ..., c_{n-1} \in A$ tales que

$$b^n + c_{n-1}b^{n-1} + ... + c_1 b + c_0 = 0.$$

B es **entero** sobre A, o B es una **extensión entera** de A si todo elemento de B es entero sobre A.

2) B es una **extensión finita** de A si B está finitamente generado como un A-módulo.

3) Sea $\varphi : A \to B$ es un homomorfismo de anillos. Si B es **entero**, respectivamente **finito**, sobre el subanillo $\varphi(A)$, entonces φ es un homomorfismo **entero**, respectivamente **finito**.

Observación 1.4.3. Si el contexto es claro, se tiende a omitir φ en la notación, es decir, se dice que B es entero, respectivamente finito, sobre A.

Proposición 1.4.4. *Sean $A \subset B \subset C$ anillos.*

1) Si $A \subset B$ y $B \subset C$ son extensiones finitas, entonces $A \subset C$ también es finita.

2) Si $A \subset B$ y $B \subset C$ son extensiones enteras, entonces $A \subset C$ también es entera.

La demostración se puede encontrar en el Capítulo 9 de [6].

1.4.2. Dimensión

Para poder hablar de dimensión de un anillo conmutativo, es necesario introducir la noción de dimensión de Krull, que se basa en la longitud de las cadenas estrictamente crecientes de ideales primos.

Definición 1.4.5. Sea A un anillo. La **dimensión de Krull**, o simplemente **dimensión**, es el máximo $n \in \mathbb{N}$ tal que existe una cadena de ideales primos

$$P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_n$$

de longitud n en A.

1.4.3. Normalización de Noether

Sea K un cuerpo, y sea $A = K[x_1, ..., x_n]$ el anillo de polinomios en n variables. Dado un ideal $I \subset A$, una de las herramientas más importantes en la teoría de K-álgebras afines es la Normalización de Noether, que permite encontrar un subanillo de polinomios $K[x_{s+1}, ..., x_n] \subset A/I$ tal que la extensión es finita.
La clave de este resultado radica en el uso de un cambio de coordenadas adecuado que nos permita trabajar con polinomios mónicos, facilitando así el estudio de A/I.
Aunque el teorema también es válido si K es finito, nos centraremos en el caso en que K es infinito, ya que se simplifican notablemente tanto las demostraciones como los cálculos en este contexto.
Un resultado fundamental para la demostración es el Lema 3.1.4, adaptado al caso de polinomios, que también nos servirá para estudiar la Normalización de Noether para series de potencias formales.

Teorema 1.4.6 (Normalización de Noether)**.** *Sea K un cuerpo, y sea $I \subset K[x_1, ..., x_n]$ un ideal. Entonces existe un número entero $s \leq n$ y un isomorfismo*

$$\varphi : K[x_1, ..., x_n] \to A := K[y_1, ..., y_n]$$

tal que la inclusión canónica $K[y_{s+1}, ..., y_n] \to A/\varphi(I)$, $y_i \mapsto y_i \bmod \varphi(I)$ es inyectiva y finita.

La demostración de este teorema puede consultarse tanto en [3] como en [9]. Esta última ofrece un análisis más detallado a partir de las indicaciones del ejercicio 16 del Capítulo 6 del libro [1].

1.5. Órdenes monomiales

Debido a la conmutatividad de la suma en $K[x]$, con K cuerpo, la representación de un polinomio como suma de monomios solo puede ser única hasta un orden de los sumandos. Esta ambigüedad puede generar ciertos problemas al implementar algoritmos que trabajan con polinomios de forma sistemática. Para evitar estas dificultades, es fundamental establecer un orden total sobre el conjunto de monomios. Este tipo de orden nos permite, por ejemplo, definir de forma coherente el término líder de un polinomio o introducir las bases estándar. En el Capítulo 2 del libro [7], se presentan diversas aplicaciones algorítmicas que recalcan la importancia de los órdenes monomiales.

Definición 1.5.1. Un **orden total** u **orden lineal** en un conjunto X es una relación binaria sobre X tal que si denotamos la relación por $\leq$, para cualquier $a, b, c \in X$ se satisfacen las siguientes propiedades:

1) $a \leq a$ (reflexiva).

2) Si $a \leq b$ y $b \leq a$, entonces $a = b$ (antisimétrica).

3) Si $a \leq b$ y $b \leq c$, entonces $a \leq c$ (transitiva).

4) $a \leq b$ o $b \leq a$ (totalidad o completitud). Un conjunto dotado con un orden total se denomina **conjunto totalmente ordenado** o **linealmente ordenado**.

La propiedad 4 es equivalente a decir que todo par de elementos del conjunto es comparable bajo la relación.

Definición 1.5.2. Un **orden monomial** es un orden total $>$ sobre el conjunto de monomios $\text{Mon}_n = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ en n variables tal que

$$x^\alpha > x^\beta \Rightarrow x^\gamma x^\alpha > x^\gamma x^\beta$$

para todo $\alpha, \beta, \gamma \in \mathbb{N}^n$. Sea A un anillo, también definimos el orden monomial $>$ en $A[x_1, ..., x_n]$, cuando lo es sobre el conjunto de monomios Mon_n.

Definición 1.5.3. Sea $>$ un orden monomial, y $f \in K[x]$ no nulo representado de forma única como la suma de términos no nulos

$$f = a_\alpha x^\alpha + a_\beta x^\beta + ... + a_\gamma x^\gamma, \quad x^\alpha > x^\beta > ... > x^\gamma,$$

con $a_\alpha, a_\beta, ..., a_\gamma \in K$. Definimos los siguientes términos:

1) $\text{LM}(f) := x^\alpha$, el monomio líder de f.

2) $\text{LE}(f) := \alpha$, el exponente líder de f.

3) $\text{LT}(f) := a_\alpha x^\alpha$, el término líder de f.

4) $\text{LC}(f) := a_\alpha$, el coeficiente líder de f.

5) $\text{tail}(f) := f - \text{LT}(f) = a_\beta x^\beta + ... + a_\gamma x^\gamma$, la cola de f.

Definición 1.5.4. Sea $>$ un orden monomial en $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$.

1) $>$ es un **orden global** si $x^\alpha > 1$ para todo $\alpha \neq (0, ..., 0)$.

2) $>$ es un **orden local** si $x^\alpha < 1$ para todo $\alpha \neq (0, ..,0)$.

3) $>$ es un **orden mixto** si no es global ni local.

Observación 1.5.5. Sea $w = (w_1, ..., w_n)$ un vector de pesos. El **grado con pesos** de x^α viene dado por: w-deg$(x^\alpha) := \langle w, \alpha \rangle = w_1\alpha_1 + ... + w_n\alpha_n$, es decir, por el producto escalar de w y α.

Ejemplo 1.5.6 (**Órdenes monomiales**)**.** Antes de introducir un par de ejemplos de órdenes globales y locales, fijamos una enumeración de variables $x_1, ..., x_n$, ya que dicha elección influye en la definición de los órdenes: con una enumeración distinta, los órdenes resultantes también cambian.

1) **Órdenes globales:** En SINGULAR, todos los órdenes globales se indican con una `p` al final, que se refiere a *polynomial ring* en inglés.

   a) *Orden lexicográfico*: lo denotamos por $>_{lp}$, y se define de la siguiente manera:

   $$x^\alpha >_{lp} x^\beta :\Longleftrightarrow \exists\, 1 \leq i \leq n : \alpha_1 = \beta_1, ..., \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

   b) *Orden lexicográfico con peso*: en este caso lo denotamos con Wp y viene dado por:

   $$x^\alpha >_{Wp} x^\beta \iff \begin{array}{c} \text{w-deg}(x^\alpha) > \text{w-deg}(x^\beta) \quad \text{o} \\ \text{w-deg}(x^\alpha) = \text{w-deg}(x^\beta) \ \text{ y } \ \exists\, 1 \leq i \leq n : \\ \alpha_1 = \beta_1,\ \ldots,\ \alpha_{i-1} = \beta_{i-1},\ \alpha_i > \beta_i. \end{array}$$

   c) *Orden lexicográfico inverso con grado*: lo denotamos por $>_{dp}$, y se define de la siguiente manera:

   $$x^\alpha >_{dp} x^\beta \iff \begin{array}{c} \deg(x^\alpha) > \deg(x^\beta) \quad \text{o} \\ \deg(x^\alpha) = \deg(x^\beta) \ \text{ y } \ \exists\, 1 \leq i \leq n : \\ \alpha_n = \beta_n,\ \ldots,\ \alpha_{i+1} = \beta_{i+1},\ \alpha_i < \beta_i. \end{array}$$

   Ahora, apliquemos estos órdenes a algún monomio y polinomio:
   Consideramos dos monomios en tres variables: $x_1x_2^2x_3^4$, $x_1x_2^3x_3^2$, y el vector de pesos $w = (1, 2, 2)$. Se tiene que $x_1x_2^3x_3^2 >_{lp} x_1x_2^2x_3^4$, mientras que $x_1x_2^2x_3^4 >_{Wp} x_1x_2^3x_3^2$, ya que w-deg$(x_1x_2^2x_3^4) >$ w-deg$(x_1x_2^3x_3^2)$. El orden lexicográfico inverso con grado coincide con este último, $x_1x_2^2x_3^4 >_{dp} x_1x_2^3x_3^2$, debido a que $\deg(x_1x_2^2x_3^4) > \deg(x_1x_2^3x_3^2)$.
   Consideremos $f = x_1x_2^2x_3^4 + x_1x_2^3x_3^2 + x_1^2x_2x_3^2 + x_1^3$, podemos ordenar sus monomios con los diferentes órdenes definidos previamente como hemos establecido en la Definición 1.5.3:

- Con el orden lexicográfico: $f = x_1^3 + x_1^2x_2x_3^2 + x_1x_2^3x_3^2 + x_1x_2^2x_3^4$.
- Con el orden lexicográfico con peso w: $f = x_1x_2^2x_3^4 + x_1x_2^3x_3^2 + x_1^2x_2x_3^2 + x_1^3$.
- Con el orden lexicográfico inverso con grado: $f = x_1x_2^2x_3^4 + x_1x_2^3x_3^2 + x_1^2x_2x_3^2 + x_1^3$.

2) **Órdenes locales:** En SINGULAR, todos los órdenes locales se indican con una `s` al final, que se refiere *series ring* en inglés.

   a) *Orden lexicográfico negativo*: lo denotamos por $>_{ls}$, y viene dado por:

$$x^\alpha >_{ls} x^\beta :\Longleftrightarrow \exists\, 1 \leq i \leq n : \alpha_1 = \beta_1, ..., \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i.$$

   b) *Orden lexicográfico negativo con peso*: en este caso lo denotamos con Ws y viene dado por:

$$x^\alpha >_{Ws} x^\beta \iff \begin{array}{c} \text{w-deg}(x^\alpha) < \text{w-deg}(x^\beta) \quad \text{o} \\ \text{w-deg}(x^\alpha) = \text{w-deg}(x^\beta) \ \text{ y } \ \exists\, 1 \leq i \leq n : \\ \alpha_1 = \beta_1,\ \ldots,\ \alpha_{i-1} = \beta_{i-1},\ \alpha_i < \beta_i. \end{array}$$

   c) *Orden lexicográfico negativo inverso con grado*: lo denotamos por $>_{ds}$, y se define de manera similar al anterior, pero con peso $w = 1$:

$$x^\alpha >_{ds} x^\beta \iff \begin{array}{c} \deg(x^\alpha) < \deg(x^\beta) \quad \text{o} \\ \deg(x^\alpha) = \deg(x^\beta) \ \text{ y } \ \exists\, 1 \leq i \leq n : \\ \alpha_n = \beta_n,\ \ldots,\ \alpha_{i+1} = \beta_{i+1},\ \alpha_i < \beta_i. \end{array}$$

   Si consideramos de nuevo los mismos monomios que antes, pero con el vector de pesos $w = (-1, -4, -1)$, se tiene que $x_1x_2^2x_3^4 >_{ls} x_1x_2^3x_3^2$, mientras que $x_1x_2^3x_3^2 >_{Ws} x_1x_2^2x_3^4$. Además, $x_1x_2^3x_3^2 >_{ds} x_1x_2^2x_3^4$.
   Si ahora ordenamos los monomios del polinomio f con estos nuevos órdenes, se tiene:

   - *Orden lexicográfico negativo*: $f = x_1x_2^2x_3^4 + x_1x_2^3x_3^2 + x_1^2x_2x_3^2 + x_1^3$.
   - *Orden lexicográfico negativo con peso w:* $f = x_1x_2^3x_3^2 + x_1x_2^2x_3^4 + x_1^2x_2x_3^2 + x_1^3$.
   - *Orden lexicográfico negativo inverso con grado*: $f = x_1^3 + x_1^2x_2x_3^2 + x_1x_2^3x_3^2 + x_1x_2^2x_3^4$.

Ejemplo 1.5.7. Sea $\mathbb{Q}[x, y, z]$, veamos cómo podemos usar SINGULAR para calcular los diferentes datos líder de un polinomio. Indicamos el anillo con `0` a la hora de definirlo. Consideramos el orden lexicográfico definido en el ejemplo anterior.

```
ring Q = 0, (x,y,z),lp;
poly f = 6 + 5x2yz +xy3z5 + 2xy6z4 + 3x2yz8;
f;                  // muestra f ordenado con lp
//-> 3x2yz8 + 5x2yz + 2xy6z4 + xy3z5 + 6
leadmonom(f);       //monomio lider
//-> x2yz8
leadexp(f);         //exponente lider
//-> 2,1,8
lead(f);            //termino lider
//-> 3x2yz8
leadcoef(f);        //coeficiente lider
//-> 3
f - lead(f);        //cola
//-> 5x2yz + 2xy6z4 + xy3z5 + 6
```

Sea ahora K un cuerpo, y $K[x] = K[x_1, ..., x_n]$ su anillo de polinomios en n variables. Sea también $>$ un orden monomial en el conjunto de monomios $\text{Mon}(x_1, ..., x_n) = \{x^\alpha \,|\, \alpha \in \mathbb{N}^n\}$. La función monomio líder LM tiene las siguientes propiedades:

1) $\text{LM}(gf) = \text{LM}(g)\text{LM}(f)$,

2) $\text{LM}(g + f) \leq \max\{\text{LM}(g), \text{LM}(f)\}$, dándose la igualdad si, y solo si los términos líder de f y g no se cancelan,

con $f, g \in K[x] \setminus \{0\}$.

Demostración. 1) Sean $f = a_\alpha x^\alpha + ... + a_\gamma x^\gamma$, $a_\alpha \neq 0$, $g = b_\nu x^\nu + ... + b_\mu x^\mu$, $b_\nu \neq 0$, con las notaciones de la Definición 1.5.3. Se tiene que

$$\text{LM}(f) = x^\alpha,\ \text{LM}(g) = x^\nu \Rightarrow \text{LM}(fg) = x^{\alpha+\nu}.$$

Por otro lado, $fg = x^{\alpha+\nu} +$ monomios estrictamente menores que $x^{\alpha+\nu}$ respecto al orden monomial. Entonces, $\text{LM}(fg) = x^{\alpha+\nu}$, lo que prueba la igualdad.

2) Usemos la misma notación que en el apartado anterior. Distinguimos dos casos.

   - Suponemos que $x^\alpha > x^\nu$, en caso de que la desigualdad estuviese invertida, se procede de manera análoga. Entonces, al sumar f y g, x^α no puede cancelarse con ningún término de g. Por tanto, $\mathrm{LM}(f+g) = \max\{\mathrm{LM}(g), \mathrm{LM}(f)\}$.
   - Supongamos ahora que $x^\alpha = x^\nu$, entonces, $f + g = (a_\alpha + b_\alpha)x^\alpha +$ monomios estrictamente menores que x^α respecto al orden monomial. Aquí se distinguen otros dos casos:
     - $a_\alpha + b_\alpha \neq 0$, luego, $\mathrm{LM}(f+g) = x^\alpha = \max\{\mathrm{LM}(g), \mathrm{LM}(f)\}$.
     - $a_\alpha + b_\alpha = 0$, entonces el término x^α se cancela y por tanto $\mathrm{LM}(f+g) < x^\alpha = \max\{\mathrm{LM}(g), \mathrm{LM}(f)\}$.

   Por ende, en todos los casos se tiene $\mathrm{LM}(g+f) \leq \max\{\mathrm{LM}(g), \mathrm{LM}(f)\}$. □

De aquí se obtiene que

$$S_> := \{u \in K[x] \setminus \{0\} \mid \mathrm{LM}(u) = 1\}$$

es un conjunto multiplicativamente cerrado.

Definición 1.5.8. Sea $>$ un orden monomial sobre $\mathrm{Mon}(x_1, ..., x_n)$, entonces definimos

$$K[x]_> := S_>^{-1} K[x] = \left\{ \frac{f}{u} \;\middle|\; f, u \in K[x], \mathrm{LM}(u) = 1 \right\},$$

la localización de $K[x]$ con respecto a $S_>$ y $K[x]_>$ es el anillo asociado a $K[x]$ y $>$.

Definición 1.5.9. Sea $>$ un orden monomial, entonces:

1) Para $f \in K[x]_>$, se elige $u \in K[x]$ tal que $\mathrm{LT}(u) = 1$ y $uf \in K[x]$. Se definen

$$\begin{aligned} \mathrm{LM}(f) &:= \mathrm{LM}(uf), \\ \mathrm{LC}(f) &:= \mathrm{LC}(uf), \\ \mathrm{LT}(f) &:= \mathrm{LT}(uf), \\ \mathrm{LE}(f) &:= \mathrm{LE}(uf), \end{aligned}$$

   y $\mathrm{tail}(f) = f - \mathrm{LT}(f)$.

2) Para cualquier subconjunto $G \subset K[x]_>$, se define el ideal

$$L_>(G) := L(G) := \langle \mathrm{LM}(g) \mid g \in G \setminus \{0\} \rangle_{K[x]}.$$

   $L(G) \subset K[x]$ es el **ideal líder** de G.

1.6. Bases estándar para polinomios

En esta sección se introduce el concepto de base estándar, una herramienta fundamental en el álgebra computacional. Se estudian sus propiedades básicas, así como distintos tipos de formas normales asociadas.
Sea $>$ un orden monomial, para simplificar la notación, tomamos $R = K[x_1, ..., x_n]_>$ la localización de $K[x]$ respecto a $>$, como en 1.5.8.

Definición 1.6.1. Sea $I \subset R$ un ideal. Un conjunto finito $G \subset R$ es una **base estándar** de I si

$$G \subset I, \text{ y } L(I) = L(G).$$

Por lo tanto, G es una base estándar, si los monomios líder de los elementos de G generan el ideal líder de I, es decir, si para cualquier $f \in I \setminus \{0\}$ existe un $g \in G$ tal que $\mathrm{LM}(g)|\mathrm{LM}(f)$.

Definición 1.6.2. Sea $G \subset R$ un subconjunto.

1) G se dice **interreducido** si $0 \notin G$ y si $\mathrm{LM}(g) \nmid \mathrm{LM}(f)$ para todo $f, g \in G$ tales que $f \neq g$. Una base estándar interreducida también se dice **mínima**.

2) $f \in R$ se dice que está **(completamente) reducido** respecto a G si ningún monomio de la expansión en series de potencias formales de f está contenido en $L(G)$.

3) G está **(completamente) reducido** si G es interreducido y si, para cualquier $g \in G$, $\mathrm{LC}(g) = 1$ y $\mathrm{tail}(g)$ está totalmente reducida respecto a G.

Definición 1.6.3. Sea $\mathcal{G}$ el conjunto de todas las listas finitas $G \subset R$.

$$\mathrm{NF} : R \times \mathcal{G} \to R, (f, G) \mapsto \mathrm{NF}(f \mid G),$$

es una **forma normal** en R, si para todo $G \in \mathcal{G}$ y $f \in R$, se satisfacen las siguientes propiedades:

1) $\mathrm{NF}(0 \mid G) = 0$,

2) $\mathrm{NF}(f \mid G) \neq 0 \Rightarrow \mathrm{LM}(\mathrm{NF}(f \mid G)) \notin L(G)$,

3) Si $G = \{g_1, ..., g_s\}$, entonces $f - \mathrm{NF}(f \mid G)$, (o, abusando de notación, f), tiene una **representación estándar** respecto a $\mathrm{NF}(- \mid G)$, es decir,

$$f - \mathrm{NF}(f \mid G) = \sum_{i=1}^{s} a_i g_i, \ a_i \in R, \ s \geq 0,$$

de manera que $\mathrm{LM}(\sum_{i=1}^{s} a_i g_i) \geq \mathrm{LM}(a_i g_i)$ para todo i con $a_i g_i \neq 0$.
NF se llama **forma normal reducida** si $\mathrm{NF}(f \mid G)$ está además reducida respecto a G.

NF es una **forma normal débil** si en vez de satisfacer 3), vale:

3') para todo $f \in R$ y $G \in \mathcal{G}$ existe una unidad $u \in R^*$ tal que uf tiene una representación estándar respecto a $\mathrm{NF}(- \mid G)$.

Lema 1.6.4. *Sea $I \subset R$ un ideal, $G \subset I$ una base estándar de I y $\mathrm{NF}(- \mid G)$ una forma normal débil en R.*

1) Para todo $f \in R$, se tiene $f \in I$ si y solo si $\mathrm{NF}(f \mid G) = 0$.

2) Si $J \subset R$ es un ideal tal que $I \subset J$, entonces $L(I) = L(J)$ implica $I = J$.

3) $I = \langle G \rangle_R$, es decir, la base estándar G genera I como un ideal de R.

4) Si $\mathrm{NF}(- \mid G)$ es una forma normal reducida, entonces es única.

Demostración. 1) Supongamos que $\mathrm{NF}(f \mid G) = 0$. Por definición, existe $u \in R^*$ unidad tal que uf tiene una representación normal, es decir, $uf - \mathrm{NF}(f \mid G) \in \langle G \rangle_R$, pero $\mathrm{NF}(f \mid G) = 0$, por lo que $uf \in \langle G \rangle_R$. Y como $\langle G \rangle_R \subset I$ y por tanto $uf \in I$, Podemos escribir $f = u^{-1}(uf)$, y de ahí $f \in I$, por ser I un ideal.
Veamos ahora la implicación inversa. Razonamos por reducción al absurdo, suponiendo que $\mathrm{NF}(f \mid G) \neq 0$. Entonces, $\mathrm{LM}(\mathrm{NF}(f \mid G)) \notin L(G) = L(I)$. Por tanto, $\mathrm{NF}(f \mid G) \notin I$. Esto implica que $f \notin I$, ya que $\langle G \rangle_R \subset I$, llegando a un absurdo.
2) Sea $f \in J$. Razonamos de nuevo por reducción al absurdo, suponiendo que $\mathrm{NF}(f \mid G) \neq 0$. Por ello, $\mathrm{LM}(\mathrm{NF}(f \mid G)) \notin L(G) = L(I) = L(J)$, pero esto contradice que $\mathrm{NF}(f \mid G) \in J$. Por tanto, por el punto 1), $f \in I$.
3) Como $L(I) = L(G) \subset L(\langle G \rangle_R) \subset L(I)$, y en particular, G también es una base estándar de $\langle G \rangle_R$, por el punto 2), se tiene la igualdad $\langle G \rangle_R = I$.
4) Sea $f \in R$, y sean h, h' dos formas reducidas normales de f respecto a G. Entonces, ningún monomio de la expansión en serie de potencias de h o h' es divisible por algún monomio de $L(G)$. Asimismo, $h - h' = (f - h') - (f - h) \in \langle G \rangle_R = I$. Si $h - h' \neq 0$, entonces $\mathrm{LM}(h - h') \in L(I) = L(G)$, lo cual es absurdo ya que $LM(h - h')$ es un monomio de h o h'. □

Ejemplo 1.6.5 (**Monomio líder**). Queremos analizar cómo varía el monomio líder de un polinomio en función del orden monomial elegido. Para

facilitar las cuentas, usaremos SINGULAR.
Sea $f = 7xy^2z^5 - xy^2z^4 + x^2y^2z^3 - 6x^2y^3z^2 + 9xy^3z \in \mathbb{Q}[x, y, z]$. Vamos a calcular $\mathrm{LM}(f)$ con respecto a distintos órdenes monomiales definidos en el Ejemplo 1.5.6. Para cambiar de orden monomial sin redefinir el polinomio, usamos `imap(Q1, f)`, que aplica el morfismo canónico inducido por la identidad sobre las variables, trasladando `f` desde el anillo `Q1` al nuevo anillo con el orden deseado.

```
ring Q1 = 0,(x,y,z),lp;          //Ordenes globales
poly f = 7xy2z5 - xy2z4 + x2y2z3 - 6x2y3z2 + 9xy3z;
leadmonom(f);
//-> x2y3z2

ring Q2 = 0,(x,y,z),dp;
poly f = imap(Q1,f), leadmonom(f);
//-> xy2z5

ring Q3 = 0,(x,y,z),ls;          //Ordenes locales
poly f = imap(Q1,f), leadmonom(f);
//-> xy2z4

ring Q4 = 0,(x,y,z),ds;
poly f = imap(Q1,f), leadmonom(f);
//-> xy3z

ring Q5 = 0,(x,y,z),Ws(-10,-1,-3);
poly f = imap(Q1,f), leadmonom(f);
//-> x2y2z3
```

Se puede observar que, para cada orden, se obtiene un monomio líder distinto. Por ello, la elección de un orden monomial adecuado es de gran importancia a la hora de calcular bases estándar, ya que dependen del orden utilizado. En el Ejemplo 4.0.7, veremos cómo varían las bases estándar según el orden monomial en el caso de series, de forma similar al caso de polinomios.

Capítulo 2

Anillos de Series de Potencias Formales

En este capítulo se van a tratar propiedades básicas de los anillos de series de potencias formales y su estructura algebraica. Se profundizará en la propiedad local de este tipo de anillos, y, se les dotará, además, de una estructura topológica.
Sea K un cuerpo, $x = (x_1, ..., x_n)$ variables, y $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$. Entonces, se escribe $x^\alpha = x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$ y su grado se denota por $\deg(x^\alpha) = |\alpha| = \sum_{i=1}^n \alpha_i$. Sea $w = (w_1, ..., w_n)$, con $w_i \in \mathbb{Z}, w_i > 0$, un **vector de pesos**. El **grado con peso** o **peso total** es $\text{w-deg}(x^\alpha) = |\alpha|_w = \sum_{i=1}^n w_i \alpha_i$. En particular, si se tiene $w = (1, .., 1)$, entonces se cumple $\text{w-deg}(x^\alpha) = \deg(x^\alpha)$.

Definición 2.0.1. Teniendo lo anterior en cuenta, se pueden definir los siguientes conceptos:

1) Una **serie de potencias formal** es una expresión $\sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$, con $a_\alpha \in K$. También se puede escribir como $\sum_{|\alpha|=0}^\infty a_\alpha x^\alpha$ o $\sum a_\alpha x^\alpha$.

2) Sea $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$ una serie de potencias formal, entonces se definen el **orden** y **orden con peso** de f como:

$$\text{ord}(f) := \min\{|\alpha| \mid a_\alpha \neq 0\} \text{ y } \text{w-ord}(f) := \min\{|\alpha|_w \mid a_\alpha \neq 0\}$$

3) El **anillo de series de potencias formales** es

$$K[[x]] := \{ \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha \mid a_\alpha \in K, \alpha \in \mathbb{N}^n \}$$

con la suma y multiplicación:

$$\sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha + \sum_{\alpha\in\mathbb{N}^n} b_\alpha x^\alpha := \sum_{\alpha\in\mathbb{N}^n} (a_\alpha + b_\alpha)\, x^\alpha$$

$$\sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha \cdot \sum_{\beta\in\mathbb{N}^n} b_\beta x^\beta := \sum_{\gamma\in\mathbb{N}^n} \left(\sum_{\alpha+\beta=\gamma} a_\alpha \cdot b_\beta \right) x^\gamma.$$

4) Además, $f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha \in K\left[[x]\right]$ se puede escribir recursivamente de la siguiente manera: $f = \sum_{\nu=0}^{\infty} b_\nu\left(x_1, ..., x_{n-1}\right) x_n^\nu = \sum_{\nu=0}^{\infty} b_\nu x_n^\nu$, con

$$b_\nu = \sum_{\substack{\alpha\in\mathbb{N}^n \\ \alpha_n=\nu}} a_\alpha x_1^{\alpha_1} \cdot ... \cdot x_{n-1}^{\alpha_{n-1}} \in K\left[[x_1, ..., x_{n-1}]\right].$$

5) Sea $f = \sum a_\alpha x^\alpha \in K\left[[x]\right]$, y $k \in \mathbb{N}$, entonces un ***k*-jet** o **truncación de orden *k* de *f*** es la suma de todos los términos de orden $\leq k$, y se denota por $j_k\left(f\right) := \sum_{|\alpha|\leq k} a_\alpha x^\alpha$.

Ejemplo 2.0.2. Para familiarizarnos con las series de potencias formales, veamos algún ejemplo con coeficientes en un cuerpo K:
Bien definidos para cualquier cuerpo:

- La serie geométrica: $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$, para el caso de una variable, que se deduce de $(1-x)\cdot\sum_{n=0}^{\infty} x^n = 1$.
- Para el caso de varias variables se tiene $\frac{1}{1-x_1...x_n} = \sum_{n=0}^{\infty}(x_1....x_n)^n$.
- También se tienen las series del tipo $\frac{1}{1+x} = \sum_{n=0}^{\infty}(-1)^n x^n$, que es un caso particular de la serie geométrica.

Válidas solo para K con característica 0, como por ejemplo $\mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$:

- La función exponencial: $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.
- Las funciones seno y coseno:

$$\operatorname{sen}(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n}, \;\; \cos(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1}.$$

- Si por ejemplo en la serie geométrica $\frac{1}{1-r}$ tomásemos $r = x + y$, podríamos reescribir su expresión usando el binomio de Newton:

$$\frac{1}{1-x-y} = \sum_{n=0}^{\infty}(x+y)^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

2.1. Localización del Anillo de Series de Potencias Formales

A continuación, profundizaremos en la estructura de $K[[x]]$ y en su propiedad local.

Lema 2.1.1. *$K[[x]]$ con las operaciones definidas en 2.0.1, es un anillo conmutativo.*

Demostración. Sean $f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha$, $g = \sum_{\beta\in\mathbb{N}^n} b_\beta x^\beta$ y $h = \sum_{\gamma\in\mathbb{N}^n} c_\gamma x^\gamma$ en $K[[x]]$.
En primer lugar, veamos que tanto la suma como el producto son conmutativos:

$$f+g = \sum_{\alpha\in\mathbb{N}^n} (a_\alpha + b_\alpha)\, x^\alpha = \sum_{\alpha\in\mathbb{N}^n} (b_\alpha + a_\alpha)\, x^\alpha = g+f$$

$$f\cdot g = \sum_{\gamma\in\mathbb{N}^n} \left(\sum_{\alpha+\beta=\gamma} a_\alpha \cdot b_\beta \right) x^\gamma = \sum_{\gamma\in\mathbb{N}^n} \left(\sum_{\alpha+\beta=\gamma} b_\beta \cdot a_\alpha \right) x^\gamma = g\cdot f,$$

para todo $f, g \in K[[x]]$, por ser K un cuerpo.
$(K[[x]], +)$ es un grupo abeliano, ya que:

1) La suma es asociativa:

$$f+(g+h) = f + \left(\sum_{\alpha\in\mathbb{N}^n} (b_\alpha + c_\alpha)x^\alpha \right) = \sum_{\alpha\in\mathbb{N}^n} (a_\alpha + b_\alpha + c_\alpha)x^\alpha =$$
$$\left(\sum_{\alpha\in\mathbb{N}^n} (a_\alpha + b_\alpha)x^\alpha \right) + h = (f+g)+h, \quad \forall f,g,h \in K[[x]].$$

2) Existe elemento neutro: $0 := \sum_{\alpha\in\mathbb{N}^n} 0\cdot x^\alpha \in K[[x]]$, $0+f=f$, para todo $f \in K[[x]]$.

3) Existe elemento opuesto:

$$\exists -f \in K[[x]] \ / \ f+(-f) = \sum_{\alpha\in\mathbb{N}^n} (a_\alpha + (-a_\alpha))\, x^\alpha = 0, \quad \forall f \in K[[x]].$$

También se tiene que el producto es asociativo:

$$f(g\cdot h) = f\cdot \left(\sum_{\theta\in\mathbb{N}^n} \left(\sum_{\beta+\gamma=\theta} b_\beta \cdot c_\gamma \right) x^\theta \right) = \sum_{\delta\in\mathbb{N}^n} \left(\sum_{\alpha+\beta+\gamma=\delta} a_\alpha \cdot b_\beta \cdot c_\gamma \right) x^\delta$$

$$(f\cdot g)h = \left(\sum_{\omega\in\mathbb{N}^n} \left(\sum_{\alpha+\beta=\omega} a_\alpha \cdot b_\beta \right) x^\omega \right) \cdot h = \sum_{\delta\in\mathbb{N}^n} \left(\sum_{\alpha+\beta+\gamma=\delta} a_\alpha \cdot b_\beta \cdot c_\gamma \right) x^\delta,$$

para todo $f, g, h \in K[[x]]$.
Se da la propiedad distributiva:

$$\forall f, g, h \in K[[x]]: \quad f \cdot (g+h) = \sum_{\gamma \in \mathbb{N}^n} \left(\sum_{\alpha+\beta=\gamma} a_\alpha \cdot (b_\beta + c_\beta) \right) x^\gamma =$$

$$\sum_{\gamma \in \mathbb{N}^n} \left(\sum_{\alpha+\beta=\gamma} a_\alpha \cdot b_\beta \right) x^\gamma + \sum_{\gamma \in \mathbb{N}^n} \left(\sum_{\alpha+\beta=\gamma} a_\alpha \cdot c_\beta \right) x^\gamma = f \cdot g + f \cdot h,$$

para todo $f, g, h \in K[[x]]$.
Hay elemento neutro para el producto: $1 := 1_K \in K[[x]], 1 \cdot f = f$, para todo $f \in K[[x]]$. □

Lema 2.1.2. *El anillo $K[[x]]$ es local, la inclusión canónica $K[x]_{\langle x \rangle} \to K[[x]]$ es un homomorfismo de anillos locales e induce los isomorfismos*

$$K[x]/\langle x \rangle^\nu \cong K[x]_{\langle x \rangle}/\langle x \rangle^\nu \cong K[[x]]/\langle x \rangle^\nu.$$

Demostración. Primero veamos que $K[[x]]$ es un anillo local, es decir, que tiene un único ideal maximal, $\langle x \rangle$. Para ello, empezamos viendo que $K[[x]]/\langle x \rangle$ es un cuerpo, que es equivalente a probar que $\langle x \rangle$ es maximal.
Los únicos elementos no invertibles de $K[[x]]/\langle x \rangle$ son los pertenecientes a $\langle x \rangle$, es decir, aquellos con término independiente nulo. Sea $f = \sum_\alpha a_\alpha x^\alpha$en $K[[x]]$, con $a_0 \neq 0$, basta con probar que tiene inverso en $K[[x]]$.
Lo demostraremos por inducción. Para $n = 0$ es trivial.
Supongamos que es cierto para $n-1$. Definimos f recursivamente, $f = \sum_{\nu=0}^\infty b_\nu x_n^\nu$ en $K[[x_1, ..., x_{n-1}]]$ y sea b_0 una unidad en $K[[x_1, ..., x_{n-1}]]$, entonces existe $c_0 \in K[[x_1, ..., x_{n-1}]]$ tal que $b_0 c_0 = 1$.
Buscamos c_ν en $K[[x_1, ..., x_{n-1}]]$, con $\nu \geq 1$ tal que $g := \sum_{\nu=0}^\infty c_\nu x_n^\nu$ sea el inverso de f, es decir, $fg = 1$.
Ya tenemos c_0, ahora hay que encontrar c_ν que satisfagan $\sum_{i=0}^\nu b_i c_{\nu-i} = 0$ para todo $\nu > 0$ para que al multiplicar $f \cdot g$ se cancelen todos los términos salvo el término independiente, que es 1 por construcción. Por la hipótesis de inducción, ya hemos encontrado $c_0, ..., c_{\nu-1}$ con esta propiedad. Si definimos $c_\nu := -c_0 \sum_{i=1}^\nu b_i c_{\nu-i}$, ya habríamos encontrado el inverso g.
Veamos que $\langle x \rangle$ es el único ideal maximal. Sea $\mathfrak{m} \subset K[[x]]$ otro ideal maximal propio.
Si $\mathfrak{m} \subset \langle x \rangle$ como $\mathfrak{m}$ es maximal y está contenido en un ideal propio, se tiene $\mathfrak{m} = \langle x \rangle$. En cambio, si $\mathfrak{m} \not\subset \langle x \rangle$, existe $f \in \mathfrak{m} \setminus \langle x \rangle$, con $f(0) \neq 0$, por lo que f es una unidad ya que su término independiente es no nulo. Luego $f^{-1} \in K[[x]]$, y como $\mathfrak{m}$ es un ideal, el producto $f^{-1} \cdot f = 1 \in \mathfrak{m}$. Por tanto $\mathfrak{m}$ contiene al 1, y así $K[[x]] = \mathfrak{m}$, lo cual contradice que sea un ideal propio.

Por consiguiente, no puede existir otro ideal maximal distinto de $\langle x \rangle$.
Vamos a construir ahora el morfismo de anillos locales. Sea φ, la inclusión canónica, tal que:

$$\begin{aligned} K\left[x\right]_{\langle x \rangle} &\xrightarrow{\varphi} K\left[\left[x\right]\right] \\ \frac{p(x)}{q(x)} &\longmapsto \frac{p(x)}{q(x)} \end{aligned}$$

Se tiene que $f(x) = \frac{p(x)}{q(x)} \in K\left[\left[x\right]\right]$ ya que se puede escribir como el producto de dos series de potencias, puesto que $q(0) \neq 0$ y por tanto es una unidad de $K\left[\left[x\right]\right]$, por lo que es invertible.
Obviamente, $\varphi(\frac{1}{1}) = \frac{1}{1} = 1$.
Sean ahora $f(x) = \frac{p(x)}{q(x)}$, $g(x) = \frac{r(x)}{s(x)} \in K\left[x\right]_{\langle x \rangle}$. Se tiene que:

$$\varphi\left(f(x) + g(x)\right) = \varphi\left(\frac{p(x)s(x) + r(x)q(x)}{q(x)s(x)}\right) = \frac{p(x)s(x) + r(x)q(x)}{q(x)s(x)} =$$
$$\frac{p(x)}{q(x)} + \frac{r(x)}{s(x)} = \varphi\left(f(x)\right) + \varphi\left(g(x)\right)$$
$$\varphi\left(f(x) \cdot g(x)\right) = \varphi\left(\frac{p(x)r(x)}{q(x)s(x)}\right) = \frac{p(x)r(x)}{q(x)s(x)} =$$
$$\frac{p(x)}{q(x)} \cdot \frac{r(x)}{s(x)} = \varphi\left(f(x)\right) \cdot \varphi\left(g(x)\right)$$

Queda probado que es un homomorfismo, ahora hay que comprobar que manda la imagen del ideal maximal de $K\left[x\right]_{\langle x \rangle}$ en el de $K\left[\left[x\right]\right]$, que denotaremos por $\mathfrak{m}_1$ y $\mathfrak{m}_2$, respectivamente. Es decir, que $\varphi(\mathfrak{m}_1) \subset \mathfrak{m}_2$.
El ideal maximal de $K\left[x\right]_{\langle x \rangle}$ es

$$\mathfrak{m}_1 := \langle x \rangle_{K[x]_{\langle x \rangle}} = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p(x) \in \langle x \rangle,\ q(x) \notin \langle x \rangle \right\}.$$

Sea $\frac{p(x)}{q(x)} \in \mathfrak{m}_1$, $\varphi(\frac{p(x)}{q(x)}) = \frac{p(x)}{q(x)}$. Considerándolo como una serie, se tiene que $\mathrm{ord}(p(x)) \geq 1$, ya que $p(x) \in \langle x \rangle$. En cuanto a $q(x)$, tiene un término independiente no nulo, por ello, su inversa $\frac{1}{q(x)}$ es una serie de potencias bien definida. Al multiplicar $p(x) \cdot \frac{1}{q(x)}$, sigue sin tener término independiente y por tanto, $\mathrm{ord}\left(\frac{p(x)}{q(x)}\right) \geq 1$. Por ende, se tiene $\varphi(\mathfrak{m}_1) \subseteq \mathfrak{m}_2$.
Finalmente, estudiemos los isomorfismos inducidos. Empecemos por el segundo:
Sabemos ya que la inclusión canónica es un homomorfismo de anillos locales.

Se tiene que $\varphi(\langle x\rangle^\nu) \subseteq \langle x\rangle^\nu$, y por ello, se obtiene el homomorfismo inducido

$$\bar{\varphi} : K[x]_{\langle x\rangle} / \langle x\rangle^\nu \to K[[x]] / \langle x\rangle^\nu$$
$$\frac{p(x)}{q(x)} + \langle x\rangle^\nu \mapsto \frac{p(x)}{q(x)} + \langle x\rangle^\nu$$

Para ver que es un isomorfismo, hay que probar es inyectiva y sobreyectiva, es decir, $\ker(\bar{\varphi}) = \{0\}$ e $\mathrm{im}(\bar{\varphi}) = K[[x]] / \langle x\rangle^\nu$. Obviamente es sobreyectiva, veamos la otra condición.
Sea $\frac{p(x)}{q(x)} + \langle x\rangle^\nu \in \ker(\bar{\varphi})$, entonces $\bar{\varphi}\left(\frac{p(x)}{q(x)} + \langle x\rangle^\nu\right) = 0$. Se tiene que $\frac{p(x)}{q(x)}$ pertenece a $\langle x\rangle^\nu$ en $K[[x]]$. Sin embargo, como $\frac{p(x)}{q(x)}$ es un elemento de $K[x]_{\langle x\rangle}$, y no una serie infinita, si en $K[[x]]$ pertenece a $\langle x\rangle^\nu$, entonces en $K[x]_{\langle x\rangle}$ también pertenece a $\langle x\rangle^\nu$. Por ello, su clase en $K[x]_{\langle x\rangle} / \langle x\rangle^\nu$ es 0, lo que implica la inyectividad de $\bar{\varphi}$.
Finalmente, veamos que $K[x] / \langle x\rangle^\nu \cong K[x]_{\langle x\rangle} / \langle x\rangle^\nu$ de manera similar. Sea $\psi : K[x] \to K[x]_{\langle x\rangle}$ la inclusión canónica, dada por $\psi(p(x)) = \frac{p(x)}{1}$, que es un homomorfismo de anillos. Obviamente, $\psi(\langle x\rangle^\nu) \subseteq \langle x\rangle^\nu_{K[x]_{\langle x\rangle}}$ ya que $\langle x\rangle^\nu$ es un ideal tanto en $K[x]$ como en $K[x]_{\langle x\rangle^\nu}$. Por tanto, se obtiene el homomorfismo inducido $\bar{\psi} : K[x] / \langle x\rangle^\nu \to K[x]_{\langle x\rangle} / \langle x\rangle^\nu$, dado por $\bar{\psi}(p(x) + \langle x\rangle^\nu) = \frac{p(x)}{1} + \langle x\rangle^\nu$.
Veamos que es un isomorfismo. Empecemos probando la inyectividad.
Sea $p(x) \in \ker(\bar{\psi})$, entonces $\bar{\psi}(p(x) + \langle x\rangle^\nu) = 0$ en $K[x]_{\langle x\rangle} / \langle x\rangle^\nu$, es decir, $\frac{p(x)}{1} \in \langle x\rangle^\nu_{K[x]_{\langle x\rangle}}$. Como $\langle x\rangle^\nu_{K[x]_{\langle x\rangle}}$ es un ideal en este anillo, se tiene que $p(x) \in \langle x\rangle^\nu$ en $K[x]$. Así pues, su clase en $K[x] / \langle x\rangle^\nu$ es 0, es decir, $\ker(\bar{\psi}) = \{0\}$.
Ahora veamos la sobreyectividad, queremos probar que para todo $\frac{p(x)}{q(x)} + \langle x\rangle^\nu$ en $K[x]_{\langle x\rangle} / \langle x\rangle^\nu$ existe un $r(x) + \langle x\rangle^\nu \in K[x] / \langle x\rangle^\nu$ tal que $\bar{\psi}(r(x) + \langle x\rangle^\nu) = \frac{p(x)}{q(x)} + \langle x\rangle^\nu$. Esto se cumple si $\frac{r(x)}{1} \equiv \frac{p(x)}{q(x)} \mod(\langle x\rangle^\nu_{K[x]_{\langle x\rangle}})$. Como los denominadores $q(x)$ son unidades en $K[x]_{\langle x\rangle}$, podemos elegir $r(x)$ tal que $r(x) \equiv p(x)q^{-1}(x) \mod\langle x\rangle^\nu$, lo que concluye que $\bar{\psi}$ es un isomorfismo. □

Ejemplo 2.1.3 (**Inverso de un polinomio**)**.** Vamos a introducir un procedimiento en SINGULAR para calcular el inverso de un polinomio en n variables como una serie de potencias hasta orden k. Para ello, consideramos un polinomio p con término independiente no nulo, para que sea invertible. Buscamos una serie de potencias q tal que

$$p \cdot q \equiv 1 \mod(\langle x_1, ..., x_n\rangle^k).$$

El procedimiento en SINGULAR es el siguiente:

```
proc invers(poly p, int k)
{
  poly q=1/p[1];
  poly re=q;
  p=q*(p[1]-jet(p,k));
  poly s=p;
  while (p!=0)
  {
    re=re+q*p;
    p=jet(p*s,k);
  }
  return(re);
}
```

Vamos a justificar y explicar el procedimiento. En primer lugar se empieza calculando el inverso de $p[1]$, es decir, $q = \frac{1}{p[1]}$. Definimos $re = q$, donde `re` será una variable de tipo polinomio donde guardamos el inverso de p.
Ahora nos interesa calcular el error de la aproximación. Para ello, redefinimos p como

$$p := q \cdot (p[1] - \text{jet}(p, k)),$$

donde `jet(p,k)` indica la truncación de p de orden k. Guardamos el error en s, que es una variable auxiliar, y mientras que p no sea nulo se reiteran los pasos $re = re + p \cdot q$ y $p = jet(p \cdot s, k)$, que es equivalente a calcular los nuevos términos del producto $p \cdot re$ que no se cancelan. Una vez que $p = 0$, los términos de orden menor que k no se pueden aproximar mejor, es decir, que $p \cdot re \equiv 1 \mod(\langle x_1, ..., x_n \rangle^k)$, con re el inverso de p.
Veamos un ejemplo numérico de este procedimiento. Para ello, vamos a trabajar en el anillo $\mathbb{Q}[x, y, z]$. Queremos calcular el desarrollo en series de potencias de $p = 1+x^2+y^2+z^2$ hasta orden 4. Asimismo, también tenemos que indicar que orden monomial vamos a usar, en este caso el orden lexicográfico negativo inverso con grado, $>_{ds}$, definido en el Ejemplo 1.5.6. El siguiente código nos permite calcularlo:

```
ring Q=0,(x,y,z),ds;
poly p=1+x2+y2+z2;
poly q=invers(p,4);
```

Esto nos devuelve el desarrollo $q = 1-x^2-y^2-z^2+x^4+2x^2y^2+y^4+2x^2z^2+2y^2z^2+z^4$. Podemos comprobar si es correcto calculando la truncación de orden 4 del producto pq con `jet(p*q,4);`, que devuelve 1. Esto confirma que hemos encontrado el inverso de p hasta orden 4.

2.1.1. Propiedades del orden

Lema 2.1.4. *Sean* $f, g \in K[[x]]$. *Entonces* $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$ *y* $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
De manera similar, $\text{w-ord}(f+g) \geq \min\{\text{w-ord}(f), \text{w-ord}(g)\}$ *y* $\text{w-ord}(fg) = \text{w-ord}(f) + \text{w-ord}(g)$.

Demostración. Sean $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$, $g = \sum_{\alpha \in \mathbb{N}^n} b_\alpha x^\alpha$ en $K[[x]]$, con orden $\operatorname{ord}(f) = \min\{|\alpha| \mid a_\alpha \neq 0\}$, $\operatorname{ord}(g) = \min\{|\alpha| \mid b_\alpha \neq 0\}$, entonces $f + g = \sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha) x^\alpha$ y

$$\operatorname{ord}(f+g) = \min\{|\alpha| \mid a_\alpha + b_\alpha \neq 0\}$$

Si $a_\alpha + b_\alpha \neq 0$, entonces al menos uno de los términos debe ser distinto de cero. Por tanto, si $a_\alpha \neq 0$, entonces $|\alpha| \geq \operatorname{ord}(f)$, por la definición de orden. Análogamente con el orden de g si $b_\alpha \neq 0$.
Como $\operatorname{ord}(f+g)$ es el mínimo $|\alpha|$ tal que $a_\alpha + b_\alpha \neq 0$, se deduce que

$$\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}.$$

Ahora veamos que $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
Consideremos $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$, $g = \sum_{\beta \in \mathbb{N}^n} b_\beta x^\beta$ en $K[[x]]$, con $\operatorname{ord}(f) = \min\{|\alpha| \mid a_\alpha \neq 0\}$,$\operatorname{ord}(g) = \min\{|\beta| \mid b_\beta \neq 0\}$. Denotaremos estos valores como $|\alpha_0|$ y $|\beta_0|$ respectivamente. Se tiene $fg = \sum_{\gamma \in \mathbb{N}^n} \left(\sum_{\gamma = \alpha + \beta} a_\alpha b_\beta \right) x^\gamma$ y

$$\operatorname{ord}(fg) = \min\{|\gamma| \mid \sum_{\gamma = \alpha + \beta} a_\alpha b_\beta \neq 0\}.$$

Como $a_{\alpha_0} \cdot b_{\beta_0} \neq 0$ y $|\alpha_0 + \beta_0| = |\alpha_0| + |\beta_0| = \operatorname{ord}(f) + \operatorname{ord}(g)$, existe al menos un término de grado $\operatorname{ord}(f) + \operatorname{ord}(g)$ en el producto fg. Por tanto, $\operatorname{ord}(fg) \leq \operatorname{ord}(f) + \operatorname{ord}(g)$.
Veamos ahora la otra desigualdad. Si

$$a_\alpha b_\beta \neq 0 \Rightarrow a_\alpha \neq 0,\ b_\beta \neq 0 \Rightarrow |\alpha| \geq \operatorname{ord}(f),\ |\beta| \geq \operatorname{ord}(g).$$

Entonces, todos los exponentes $\gamma = \alpha + \beta$ en el producto fg satisfacen $|\gamma| \geq \operatorname{ord}(f) + \operatorname{ord}(g)$. Por tanto, se da la desigualdad, de donde se deduce,

$$\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g).$$

Para los órdenes con peso, la demostración es similar, la diferencia es que hay que reemplazar $|\alpha|$ por $|\alpha|_w$, es decir, por el producto escalar $\alpha \cdot w$.

□

Lema 2.1.5. *Se cumple* $\bigcap_{\nu=1}^{\infty}\langle x\rangle^{\nu} = \langle 0\rangle$.

Demostración. Sea $f \in \langle x\rangle^{\nu}$, entonces $\operatorname{ord}(f) \geq \nu$. Si $f = \sum_{\alpha} a_{\alpha}x^{\alpha}$, entonces $a_{\alpha} = 0$ si $|\alpha| < \nu$ debido a la definición de orden.
Por tanto, si $f \in \langle x\rangle^{\nu}$ para todo ν, se tiene que $a_{\alpha} = 0$ para todo α, ya que siempre se puede tomar $\nu > |\alpha|$. Por ello $f = 0$, lo que implica que la intersección de todos los ideales de la forma $\langle x\rangle^{\nu}$ está contenida en $\langle 0\rangle$. La otra contención es trivial, ya que $0 \in \langle x\rangle^{\nu}$ para todo ν, de donde se deduce la igualdad. □

2.2. Topología

Para poder estudiar propiedades en $K[[x]]$, como la convergencia, es necesario dotar al anillo de una estructura topológica. Esto nos permitirá analizar la completitud de $K[[x]]$. Por ello, definiremos la topología $\langle x\rangle$-ádica, que será la base del estudio de las sucesiones de Cauchy y la convergencia en este contexto.

Definición 2.2.1. Consideremos $K[[x]]$ como un espacio topológico, con $F := \{\langle x\rangle^{\nu} \mid \nu \in \mathbb{N}\}$ un sistema fundamental de entornos de 0. Esta topología se denomina **topología $\langle x\rangle$ - ádica**.
Para una serie $f \neq 0$, en $K[[x]]$ sus entornos son los trasladados $f + F$.

2.2.1. Convergencia y completitud

Definición 2.2.2. 1) Una sucesión $\{f_{\nu}\} = \{f_{\nu}\}_{\nu\in\mathbb{N}}, f_{\nu} \in K[[x]]$, se llama **sucesión de Cauchy** si, para todo $k \in \mathbb{N}$ existe $l \in \mathbb{N}$ tal que

$$f_{\nu} - f_{m} \in \langle x\rangle^{k},\ \forall \nu, m \geq l.$$

2) Una sucesión $\{f_{\nu}\}_{\nu\in\mathbb{N}}$, $f_{\nu} \in K[[x]]$, se dice que es **convergente** si existe una serie de potencias $f \in K[[x]]$ tal que para todo $k \in \mathbb{N}$ existe un $l \in \mathbb{N}$ tal que $f - f_{\nu} \in \langle x\rangle^{k}$ para todo $\nu \geq l$. Entonces f está unívocamente determinada, y se escribe $f := \lim_{\nu\to\infty} f_{\nu}$.

Teorema 2.2.3. *$K[[x]]$ es completo, es decir, toda sucesión de Cauchy en $K[[x]]$ es convergente, y Hausdorff.*

Demostración. Veamos que $K[[x]]$ es Hausdorff, es decir, dados dos elementos f, g distintos, queremos probar que existen dos entornos $U = f + \langle x\rangle^{\nu}$, $V = g + \langle x\rangle^{\mu}$ tal que $U \cap V = \emptyset$ para $\nu, \mu \in \mathbb{N}$ adecuados.
Se tiene que $f \neq g$ elementos de $K[[x]]$, es decir $f - g \neq 0$. Por el lema 2.1.5

$f-g$ no puede pertenecer a todos los ideales $\langle x\rangle^\nu$, ya que $f-g \notin \langle 0\rangle$. Por lo tanto, existe $v \in \mathbb{N}$ tal que $f-g \notin \langle x\rangle^v$.
Si consideramos los entornos $U = f + \langle x\rangle^v$, $V = g + \langle x\rangle^v$, habríamos terminado ya que son disjuntos. Si no lo fuesen, existiría $h \in U \cap V$ tal que $h - f \in \langle x\rangle^v$ y $h - g \in \langle x\rangle^v$, lo que implicaría $f - g \in \langle x\rangle^v$, contradiciendo la elección de v.
Sea $\{f_\nu\}$ una sucesión de Cauchy en $K[[x]]$. Queremos ver que es convergente, es decir que existe $f \in K[[x]]$ tal que $\lim_{\nu\to\infty} f_\nu = f$.
Sea $f_\nu = \sum a_\alpha^{(\nu)} x^\alpha$, donde $\alpha \in \mathbb{N}^n$ con $|\alpha| = s$. Como es de Cauchy, existe $l \in \mathbb{N}$ tal que $f_\nu - f_\mu \in \langle x\rangle^{s+1}$, $\forall \nu, \mu \geq l$. Esto quiere decir que $a_\alpha^{(\nu)} = a_\alpha^{(\mu)}$ para todo $\nu, \mu \geq l$. Definimos $f = \sum b_\alpha x^\alpha$, donde $\alpha \in \mathbb{N}^n$ con $|\alpha| = s$ y $b_\alpha := a_\alpha^{(l)} = a_\alpha^{(\nu)}$, $\forall \nu \geq l$. Veamos que f es el límite de $\{f_\nu\}$.
Tomamos $k = s+1$, se tiene que para $|\alpha| < k$, $b_\alpha = a_\alpha^{(\nu)}$, $\forall \nu \geq l$, por tanto, $f - f_\nu$ no tiene términos de orden menor que k, es decir, $f - f_\nu \in \langle x\rangle^\nu$, $\forall \nu \geq l$, lo que concluye la demostración. □

Observación 2.2.4. Si una sucesión $\{f_\nu\}$ es convergente en $K[[x]]$, entonces es de Cauchy.
Esto es cierto ya que $f_m - f_n = (f_m - f) - (f_n - f) \in \langle x\rangle^k$ $\forall m, n \geq l$ debido a que para todo $k \in \mathbb{N}$, existe $l \in \mathbb{N}$ tal que $f - f_\nu \in \langle x\rangle^\nu$, $\forall \nu \geq l$.

Proposición 2.2.5. *Si $\{f_\nu\}_{\nu\in\mathbb{N}}$, $f_\nu \in K[[x]]$ es una sucesión convergente tal que $\lim_{\nu\to\infty} f_\nu = 0$, entonces la sucesión de sumas parciales $\{\sum_{\nu=0}^m f_\nu\}_{m\in\mathbb{N}}$ converge, y se define*

$$\sum_{\nu=0}^{\infty} f_\nu := \lim_{m\to\infty} \left(\sum_{\nu=0}^{m} f_\nu \right).$$

Demostración. Sea $\{S_m\}_{m\in\mathbb{N}} = \{\sum_{\nu=0}^m f_\nu\}_{m\in\mathbb{N}}$ la sucesión de sumas parciales. Como $\lim_{\nu\to\infty} f_\nu = 0$, por definición de convergencia en la topología $\langle x\rangle$-ádica, para todo $k \in \mathbb{N}$ existe $l \in \mathbb{N}$ tal que $f_\nu \in \langle x\rangle^k$ con $\nu \geq l$.
Por otra parte, $\forall k \in \mathbb{N}$, se tiene $S_m - S_{m-1} = f_m \in \langle x\rangle^k$ con $m \geq l$, es decir, $\{S_m\}_{m\in\mathbb{N}}$ es de Cauchy, y por ello, convergente. □

Observación 2.2.6. De la forma habitual, dadas dos sucesiones convergentes $\{f_\nu\}, \{g_\nu\}$, se tiene

$$\lim_{\nu\to\infty}(f_\nu + g_\nu) = \lim_{\nu\to\infty} f_\nu + \lim_{\nu\to\infty} g_\nu, \quad \lim_{\nu\to\infty}(f_\nu \cdot g_\nu) = \lim_{\nu\to\infty} f_\nu \cdot \lim_{\nu\to\infty} g_\nu,$$

y si $\lim_{\nu\to\infty} f_\nu = \lim_{\nu\to\infty} g_\nu = 0$ entonces

$$\sum_{\nu=0}^{\infty} f_\nu + \sum_{\nu=0}^{\infty} g_\nu = \sum_{\nu=0}^{\infty}(f_\nu + g_\nu),$$
$$\sum_{\nu=0}^{\infty} f_\nu \cdot \sum_{\nu=0}^{\infty} g_\nu = \sum_{\nu=0}^{\infty}\sum_{i=0}^{\nu} f_{\nu-i} g_i.$$

Demostración. Como $\{f_\nu\}$ y $\{g_\nu\}$ son convergentes, existen $f, g \in K[[x]]$ tales que para todo $k \in \mathbb{N}$, existen $l_1, l_2 \in \mathbb{N}$ tales que si $\nu \geq \max\{l_1, l_2\}$, entonces

$$f_\nu - f \in \langle x \rangle^k, \quad g_\nu - g \in \langle x \rangle^k.$$

Tomamos $l := \max\{l_1, l_2\}$, entonces

$$(f_\nu + g_\nu) - (f + g) = (f_\nu - f) + (g_\nu - g) \in \langle x \rangle^k \quad \forall \nu \geq l,$$

debido a que $\langle x \rangle^k$ es un ideal, es cerrado para la suma. De aquí se deduce que

$$\lim_{\nu \to \infty} (f_\nu + g_\nu) = f + g = \lim_{\nu \to \infty} f_\nu + \lim_{\nu \to \infty} g_\nu.$$

Para el producto, razonamos de manera similar, y volvemos a tomar $l := \max\{l_1, l_2\}$. Entonces,

$$f_\nu g_\nu - fg = (f_\nu - f)(g_\nu - g) + f(g_\nu - g) + (f_\nu - f)g.$$

Cada uno de los términos pertenece a $\langle x \rangle^k$ para todo $\nu \geq l$ debido a la definición de ideal y que $f, g \in K[[x]]$. Por ende,

$$\lim_{\nu \to \infty} (f_\nu \cdot g_\nu) = fg = \lim_{\nu \to \infty} f_\nu \cdot \lim_{\nu \to \infty} g_\nu.$$

Ahora supongamos $f = g = 0$.
Reescribiendo la condición de convergencia, con $l := \max\{l_1, l_2\}$,

$$f_\nu \in \langle x \rangle^k, \quad g_\nu \in \langle x \rangle^k \quad \forall \nu \geq l.$$

Consideramos las sumas parciales $W_n = \sum_{\nu=0}^{n} (f_\nu + g_\nu) = \sum_{\nu=0}^{n} f_\nu + \sum_{\nu=0}^{n} g_\nu = S_n + T_n$. Se tiene que $\lim_{\nu \to \infty} (f_\nu + g_\nu) = 0$, entonces, aplicando la Proposición 2.2.5, las tres sumas parciales convergen,

$$\sum_{\nu=0}^{\infty} (f_\nu + g_\nu) = \sum_{\nu=0}^{\infty} f_\nu + \sum_{\nu=0}^{\infty} g_\nu.$$

Para el producto, usamos la notación precedente. Multiplicando las sumas parciales se obtiene

$$S_n \cdot T_n = \left(\sum_{\nu=0}^{n} f_\nu \right) \cdot \left(\sum_{\nu=0}^{n} g_\nu \right) = \sum_{\nu=0}^{2n} \left(\sum_{i=0}^{\nu} f_{\nu-i} g_i \right),$$

ya que estamos haciendo el producto de dos sumas finitas. Por la Proposición 2.2.5, las sumas parciales son convergentes, entonces

$$\left(\sum_{\nu=0}^{\infty} f_\nu \right) \cdot \left(\sum_{\nu=0}^{\infty} g_\nu \right) = \lim_{n \to \infty} S_n \cdot T_n = \lim_{n = \to \infty} \sum_{\nu=0}^{2n} \left(\sum_{i=0}^{\nu} f_{\nu-i} g_i \right).$$

Dado que f_ν y g_ν convergen a 0, entonces, tomando $\nu \geq 2l$, se tiene que $\sum_{i=0}^{\nu} f_{\nu-i}g_i \in \langle x \rangle^k$ para todo $k \in \mathbb{N}$ debido a que $\langle x \rangle^k$ es un ideal y $f_{\nu-i}g_i \in \langle x \rangle^k$. Es decir, $\sum_{i=0}^{\nu} f_{\nu-i}g_i$ converge a 0, luego el doble sumatorio converge de nuevo por la proposición precedente. Por tanto, tomando límites se concluye

$$\left(\sum_{\nu=0}^{\infty} f_\nu\right) \cdot \left(\sum_{\nu=0}^{\infty} g_\nu\right) = \sum_{\nu=0}^{\infty} \left(\sum_{i=0}^{\nu} f_{\nu-i}g_i\right).$$

□

2.2.2. Sustitución

Definición 2.2.7. Sean $f, g_1, ..., g_n \in K[[x]]$ y supongamos que $\text{ord}(g_i) \geq 1$ para todo i, entonces se define la **sustitución**

$$f(g_1, ..., g_n) = \lim_{m\to\infty} j_m(f)(g_1, ..., g_n),$$

donde $\{j_m(f)\}_{m\in\mathbb{N}}$ es la sucesión de los polinomios truncados de f en $K[x]$.

Proposición 2.2.8. *La sucesión de polinomios $\{j_m(f)\}_{m\in\mathbb{N}}$ de la anterior definición es de Cauchy.*

Demostración. Sean $f = \sum_\nu a_\nu x^\nu$ y $j_m(f) = \sum_{|\nu|\leq m} a_\nu x^\nu$ la truncación de orden m de f. Se tiene que $f_{m+1}(f) - f_m(f) = \sum_{|\nu|=m+1} a_\nu x^\nu \in \langle x \rangle^{m+1}$. Sabemos que $\langle x \rangle^{m+1} \subseteq \langle x \rangle^k$ si $k \leq m+1$. Por tanto, para todo $k \in \mathbb{N}$, tomando $l = k$, se tiene que $f_{m+1}(f) - f_m(f) \in \langle x \rangle^k$, para todo $m \geq l$, lo que prueba que la sucesión es de Cauchy. □

Corolario 2.2.9. *Sea $y = (y_1, ..., y_m)$, y sea $\varphi : K[[x]] \to K[[y]]$ un homomorfismo de K-álgebras continuo con $f_i := \varphi(x_i)$, $i = 1, ..., n$. Entonces, se tiene $\varphi(g) = g(f_1, ..., f_n)$ para todo $g \in K[[x]]$.*

Demostración. Para todo m, se tiene $\varphi(j_m(g)) = j_m(g)(f_1, ..., f_n)$ ya que φ es un homomorfismo entre K-álgebras y como $j_m(g)$ es un polinomio, podemos aplicarlo directamente sobre las imágenes f_i , donde $\{j_m(g)\}_{m\in\mathbb{N}}$ es la sucesión de Cauchy de la definición 2.2.7.
Como φ es continuo, eso implica

$$\varphi(g) = \lim_{m\to\infty} \varphi(j_m(g)) = \lim_{m\to\infty} j_m(g)(f_1, ..., f_n)$$

Y de nuevo, por la definición de sustitución, $\varphi(g) = g(f_1, ..., f_n)$. □

Observación 2.2.10. 1) Sea

$$\varphi : K\left[[x]\right] \to K\left[[y]\right]$$

un homomorfismo entre K-álgebras, se puede ver que es local, es decir, $\varphi(\langle x\rangle) \subset \langle y\rangle$. Para ello, sea $f \in \langle x\rangle$ y $\varphi(f) = g + c$ con $g \in \langle y\rangle$, con $c \in K \setminus \{0\}$. $f - c$ es una unidad en $K\left[[x]\right]$, debido a que f no tiene término independiente y por hipótesis, c es no nula. Entonces, $\varphi(f - c) = g$ es también una unidad, llegando a una contradicción.

2) En particular, si

$$\varphi : K\left[[x]\right] \to K\left[[y]\right]$$

es un homomorfismo entre K-álgebras, también es continuo. Además, por el Corolario 2.2.9, φ está unívocamente determinado por las imágenes $f_i := \varphi(x_i), i = 1, ..., n$, donde f_i son series de potencias formales con $f_1, ..., f_n \in \langle x\rangle$.
Recíprocamente, a partir de una colección de series de potencias formales $f_1, ..., f_n \in \langle x\rangle$ se puede definir un único homomorfismo continuo tomando

$$\varphi(g) := \varphi\left(\sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha\right) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha f_1^{\alpha_1} \cdot ... \cdot f_n^{\alpha_n} = g(f_1, ..., f_n).$$

Capítulo 3

Teorema de Preparación de Weierstrass

Este capítulo está dedicado al estudio del Teorema de Preparación de Weierstrass y alguna de sus consecuencias en los anillos de la forma $K[[x]]$, tales como la Normalización de Noether, el Teorema de la Función Implícita y el Teorema de la Función Inversa.

3.1. Teorema de División de Weierstrass

Definición 3.1.1. Sea $f \in K[[x]]$, se dice que f es x_n**- general de orden** m o x_n**- regular de orden** m si

$$f(0,...,0,x_n) = x_n^m \cdot g(x_n), \text{ con } g(x_n) \in K[[x_n]],\ g(0) \neq 0.$$

Ejemplo 3.1.2. Sea $f(x,y) = y^3 + \frac{y^2}{1-2x+x^2} + yx \in K[[x,y]]$, está bien definida por ser $1-2x+x^2$ invertible.
Si tomamos $x = 0$, $f(0,y) = y^3 + y^2 = y^2 \cdot g(y)$, con $g(y) = y + 1 \in K[[y]]$, $g(0) = 1$. Por tanto, f es y-general de orden 2.
Sin embargo, si tomamos $y = 0$, $f(x,0) = 0$, por lo que f no puede ser x-general.

Lema 3.1.3. *Sea $f \in K[[x]]$. Sea $\mathfrak{m} = \langle x_1,...,x_{n-1}\rangle$. Entonces f es x_n-general de orden m, si, y solo si, existen u unidad en $K[[x]]$ y $w \in \mathfrak{m}[x_n]$ tales que $f = ux_n^m - w$.*

Demostración. Supongamos que f es x_n-general de orden m, es decir, existe $g \in K[[x_n]]$ tal que $f(0,...,0,x_n) = x_n^m \cdot g(x_n)$.
Podemos descomponer f en dos sumatorios de manera que

$$f = \sum_{i<m} a_i(x_1,...,x_{n-1})x_n^i + \sum_{i\geq m} a_i(x_1,...,x_{n-1})x_n^i,$$

donde $a_i \in K\left[\left[x_1, ..., x_{n-1}\right]\right]$.
Por hipótesis, $f(0, ..., 0, x_n) = x_n^m \cdot g(x_n) \Rightarrow \sum_{i<m} a_i(0, ..., 0)x_n^i = 0 \Rightarrow a_i(x_1, ..., x_{n-1}) \in \mathfrak{m}$.
Además, $\sum_{i\geq m} a_i(x_1, ..., x_{n-1})x_n^i = x_n^m \cdot g(x_n) \Rightarrow a_m(a_1, ..., a_{n-1}) \notin \mathfrak{m}$.
Entonces, basta tomar $u = \sum_{i\geq m} a_i(x_1, ..., x_{n-1})x_n^{i-m} \in K\left[\left[x\right]\right]^*$, ya que su término independiente es no nulo, y $w = \sum_{i<m} a_i(x_1, ..., x_{n-1})x_n^i \in \mathfrak{m}\left[x_n\right]$.
Consideremos ahora $f = ux_n^m - w$. Se tiene que $w(0, ..., 0, x_n) = 0$ porque $w \in \mathfrak{m}\langle x_n\rangle$. Entonces, $f(0, ..,0, x_n) = u(0, ..,0, x_n) \cdot x_n^m = g(x_n) \cdot x_n^m$, y como u es una unidad, $g(0) = u(0) \neq 0$. □

Lema 3.1.4. *Sea $f \in K\left[\left[x\right]\right]$ y $f = \sum_{\nu\geq m} f_\nu$ con f_ν un polinomio homogéneo de grado ν, f_m no nulo. Sea $(a_1, ..., a_{n-1}) \in K^{n-1}$, tal que*

$$f_m(a_1, ..., a_{n-1}, 1) \neq 0.$$

Entonces $f(x_1 + a_1x_n, ..., x_{n-1} + a_{n-1}x_n, x_n)$ es x_n-general de orden m.

Demostración. Como f_ν es un polinomio homogéneo de orden ν, se tiene que $f_\nu(x_1 + a_1x_n, ..., x_{n-1} + a_{n-1}x_n, x_n)$ también es homogéneo de orden ν. Por ello, al evaluar $f_m(x_1 + a_1x_n, ..., x_{n-1} + a_{n-1}x_n, x_n)$ en $x_1 = ... = x_{n-1} = 0$, se obtiene $f_m(a_1x_n, ..., a_{n-1}x_n, x_n) = x_n^m \cdot f(a_1, ..., a_{n-1}, 1)$.
Entonces,

$$f(a_1x_n, ..., a_{n-1}x_n, x_n) = x_n^m f_m(a_1, ...a_{n-1}, 1) + \sum_{\nu\geq m+1} x_n^\nu f_\nu(a_1, ..., a_{n-1}, 1).$$

Tomando $g(x_n) = f_m(a_1, ...a_{n-1}, 1) + \sum_{\nu\geq m+1} x_n^{\nu-m} f_\nu(a_1, ..., a_{n-1}, 1)$, que está bien definido por ser $\nu > m$, se tiene $g(0) = f_m(a_1, ..., a_{n-1}, 1) \neq 0$ y $f(a_1x_n, ..., a_{n-1}x_n, x_n) = x_n^m \cdot g(x_n)$. □

Lema 3.1.5. *Sea K un cuerpo infinito y $f \in K\left[x\right]$ un polinomio homogéneo de grado $m > 0$, entonces existe $(a_1, ..., a_{n-1}) \in K^{n-1}$ tal que*

$$f(a_1, ..., a_{n-1}, 1) \neq 0$$

, es decir, f es x_n-general de algún orden.

Demostración. Vamos a demostrar este resultado por inducción.
El caso $n = 1$ es trivial, ya que un polinomio homogéneo en una variable es solo un múltiplo constante de un monomio, es decir, es de la forma $c \cdot x^m$ para algún $c \in K$.
Para $n \geq 2$, se tiene $K\left[x_1, ..., x_n\right] = \left(K\left[x_2, ..., x_n\right]\right)\left[x_1\right]$ y se puede escribir $f = \sum_{i=0}^d f_i x_1^i$, con $f_i \in K\left[x_2, ..., x_n\right]$ homogéneo de grado $d-i$. Entonces, como f no es nulo, existe al menos un f_i no nulo. Aplicando la hipótesis de inducción

a ese f_i, se puede elegir $a_2, ..., a_{n-1} \in K$ tales que $f_i(a_2, ..., a_{n-1}, 1) \neq 0$.
Por tanto, $f(x_1, a_2, ..., a_{n-1}, 1) \in K[x_1]$ es un polinomio no nulo, entonces solo tiene un número finito de ceros $\alpha_1, ..., \alpha_m \in K$. Por consiguiente, como K es infinito, podemos encontrar $a_1 \in K$ tal que $f(a_1, ..., a_{n-1}, 1) \neq 0$. De hecho, esto es cierto para todo $a_1 \in K \setminus \{\alpha_1, ..., \alpha_m\}$.
En particular, por el Lema 3.1.4, esto implica que es x_n-general de algún orden.

□

Observación 3.1.6. Con las notaciones del Lema 3.1.4, sea K un cuerpo finito. Si se cumple que $f_m(a_1, ..., a_{n-1}, 1) = 0$ para todo $(a_1, ..., a_{n-1})$ en K^{n-1} entonces, mediante la transformación $x_i \mapsto x_i + x_n^{\beta_i}, x_n \mapsto x_n$ con $\beta_1, ..., \beta_{n-1}$ adecuados, se obtiene una serie de potencias x_n-general de la forma $f(x_1 + x_n^{\beta_1}, ..., x_{n-1} + x_n^{\beta_{n-1}}, x_n)$.
La demostración se puede encontrar en [3], en la sección 4.7. Está demostrado para polinomios, pero se puede adaptar al caso de series haciendo un razonamiento similar al del Lema 3.1.4.

La demostración del siguiente teorema está basada en [10].

Teorema 3.1.7 (Teorema de la División de Weierstrass)**.** *Sea $f \in K[[x]]$ x_n-general de orden m, $g \in K[[x]]$, entonces existen $q \in K[[x]]$ y $r_0, ..., r_{m-1} \in K[[x_1, ..., x_{n-1}]]$ únicos tales que*

$$g = qf + r, \quad con\ r = \sum_{\nu=0}^{m-1} r_\nu x_n^\nu.$$

Demostración. Sea $p \in K[[x]]$, entonces se puede escribir $p = \sum_{\nu=0}^{\infty} a_\nu x_n^\nu$, donde $a_\nu \in K[[x_1, ..., x_{n-1}]]$. Definimos dos funciones K-lineales en $K[[x]]$,

$$r(p) = \sum_{\nu=0}^{m-1} a_\nu x_n^\nu \ \text{ y } \ h(p) = (p - r(p))/x_n^m.$$

Reescribiendo la última expresión, se obtiene $p = h(p)x_n^m + r(p)$. Sea $\mathfrak{m}$ el ideal maximal de $K[[x_1, ..., x_{n-1}]]$.
Por hipótesis, al ser f x_n-general de orden m, existen $u \in K[[x]]$ una unidad y $w \in \mathfrak{m}[x_n]$ tales que $f = ux_n^m - w$. Por tanto, tiene sentido considerar u^{-1}. Consideremos $T : K[[x]] \to K[[x]]$, dada por $T(g) = h(g)u^{-1}f + r(g)$. Obviamente, T es una función K-lineal. Veamos que T es un isomorfismo, para ello, vamos a construir su inverso. El objetivo es usar la siguiente identidad

$$T^{-1} = (id - (id - T))^{-1} = \sum_{i=0}^{\infty} (id - T)^i, \tag{3.1}$$

donde id es el morfismo identidad.
Se tiene que

$$g - T(g) = h(g)x_n^m + r(g) - h(g)u^{-1}f - r(g) = h(g)(x_n^m - u^{-1}f) = h(g)u^{-1}w.$$

Si $g \in \mathfrak{m}^k [[x_n]]$ para algún $k \geq 0$, entonces

$$h(g) \in \mathfrak{m}^k [[x_n]] \Rightarrow h(g)u^{-1} \in \mathfrak{m}^k [[x_n]] \Rightarrow h(g)u^{-1}w \in \mathfrak{m}^{k+1} [[x_n]],$$

debido a que w tiene coeficientes en $\mathfrak{m}$, es decir, $g - T(g) \in \mathfrak{m}^{k+1} [[x_n]]$.
Definimos $S(g) = g - T(g) = (id - T)(g)$. Se tiene que $S^j(g) \in \mathfrak{m}^j [[x_n]]$ para todo $j \geq 0$. Asimismo, para cualquier sucesión de elementos $\{h_i\}_{i=0}^{\infty} \in K [[x]]$ tal que $h_i \in \mathfrak{m}^i [[x_n]]$, la suma $\sum_{i=0}^{\infty} h_i$ está bien definida y pertenece a $K [[x]]$, debido a que solo aparecen en h_i los monomios en $x_1, ..., x_n$ de grado mayor o igual que i. Por tanto, para cualquier $g \in K [[x]]$, la serie $\sum_{i=0}^{\infty} S^i(g)$ es un elemento bien definido de $K [[x]]$. Entonces, por la identidad 3.1, se tiene que $T^{-1} = \sum_{i=0}^{\infty}(id - T)^i = \sum_{i=0}^{\infty} S^i$.
Además, se cumple que $g = qf + r$ como se afirma en el enunciado si y solo si, $g = T(qux_n^m + r)$. Como qux_n^m tiene grado estrictamente mayor que $m - 1$, $r(qux_n^m) = 0$. Por ello, $r(qux_n^m + r) = r$, por ser una función K-lineal y por cómo está definida r en el enunciado.
Por otro lado,

$$h(qux_n^m + r) = \frac{qux_n^m + r - r(qux_n^m + r)}{x_n^m} = qu.$$

Entonces, $T(qux_n^m + r) = qu \cdot u^{-1}f + r = qf + r$, lo que prueba la equivalencia.
Nos falta por demostrar la existencia y unicidad de q y r.
Se cumple que

$$T^{-1}(g) = T^{-1}(T(qux_n^m + r)) = qux_n^m + r. \tag{3.2}$$

Además, se puede escribir $T^{-1}(g) = h(T^{-1}(g))x_n^m + r(T^{-1}(g))$. Basta tomar $q := h(T^{-1}(g))u^{-1}$ y $r := r(T^{-1}(g))$, ya que la existencia de $T^{-1}(g)$ viene garantizada por ser T un isomorfismo.
Para la unicidad, supongamos que existen q, q' y r, r' satisfaciendo las hipótesis del enunciado, tales que

$$g = qf + r = q'f + r'.$$

Por la expresión 3.2, se tiene que

$$T^{-1}(g) = qux_n^m + r = q'ux_n^m + r' \Rightarrow (q - q')ux_n^m + (r - r') = 0.$$

Como $(q-q')ux_n^m$ tiene los términos de grado mayor o igual que m en x_n, mientras que $r-r'$ tiene grado menor estrictamente que m en x_n, ambos sumandos se deben anular. Por ello, como x_n^m no se anula y u es una unidad, por lo que se puede multiplicar por su inverso, se llega a $q-q'=0$, $r-r'=0$, concluyendo la demostración. □

Ejemplo 3.1.8. Vamos a trabajar en $\mathbb{Q}[[x,y]]$. Sea $f=y^2-x$, la cual es y - general de orden 2. Consideramos $g=y^3+\frac{y}{1-x}=y^3+\sum_{n=0}^{\infty}x^ny$. El Teorema de División de Weierstrass nos garantiza que existen $q\in\mathbb{Q}[[x,y]]$ y $r_0,r_1\in\mathbb{Q}[[x]]$ únicos tales que

$$g=qf+r,\quad r=\sum_{k=0}^{1}r_ky^k.$$

Se tiene que

$$y^3=y\cdot y^2=y(y^2-x+x)=y(y^2-x)+xy=yf+xy.$$

Por tanto, sustituyendo en g:

$$g=yf+xy+\frac{y}{1-x}=yf+y\frac{1+x-x^2}{1-x}.$$

Tomando $q=y$, $r_0=0$, y $r_1=y\left(\frac{1+x-x^2}{1-x}\right)$, se tiene la descomposición que estábamos buscando.

3.2. Consecuencias del Teorema de División de Weierstrass

El Teorema de División de Weierstrass 3.1.7 no solo es fundamental por sí mismo, sino que también permite enunciar el Teorema de Preparación de Weierstrass y deducir otros resultados de gran importancia, que estudiaremos en esta sección.

3.2.1. Teorema de Preparación de Weierstrass

Definición 3.2.1. Sea $p=x_n^m+\sum_{\nu=0}^{m-1}a_\nu x_n^\nu\in K[[x_1,...,x_{n-1}]][x_n]$ un polinomio en x_n con coeficientes a_ν en $K[[x_1,...,x_{n-1}]]$. Se dice que es un **polinomio de Weierstrass** respecto a x_n si $a_\nu\in\langle x_1,...,x_{n-1}\rangle$ para todo ν.

Ejemplo 3.2.2. Veamos algún ejemplo sencillo de polinomios de Weierstrass en dos variables, es decir, en el anillo de polinomios $K[[x]][y]$.

Consideramos el polinomio $p = y^3 + \frac{x}{1-x}y^2 + x^2y + x^5$. Es de Weierstrass respecto a y debido a que es mónico en y y $\frac{x}{1-x} = \sum_{n=1}^{\infty} x^n \in \langle x \rangle$ y tanto x^2 como x^5 pertenecen a $\langle x \rangle$.
Sin embargo, el polinomio $q = y^3 + \frac{1}{1-x}y^2 + x^2y + x^5$ no es de Weierstrass respecto a y ya que $\frac{1}{1-x} = 1 + x + x^2... = \sum_{n=0}^{\infty} x^n \notin \langle x \rangle$.

Corolario 3.2.3 (Teorema de Preparación de Weierstrass)**.** *Sea $f \in K[[x]]$ x_n-general de orden m, entonces existe una unidad $u \in K[[x]]$ y un polinomio de Weierstrass p de grado m respecto a x_n tales que $f = u \cdot p$, con p y u únicos.*

Demostración. Vamos a aplicar el Teorema de División de Weierstrass (3.1.7) a $g = x_n^m$. Entonces, se tiene $g = qf + r$, es decir, $x_n^m = qf + r$, con q, r con la notación del enunciado.
Haciendo $x_1 = ... = x_{n-1} = 0$, se obtiene

$$x_n^m = q(0, ..., 0, x_n)f(0, ..., 0, x_n) + r(0, ..., 0, x_n).$$

Por ser f x_n- general , existe $h \in K[[x_n]]$ tal que $f(0, ..., 0, x_n) = x_n^m \cdot h(x_n)$, con $h(0) \neq 0$. Sustituyendo en la expresión anterior,

$$x_n^m = x_n^m \cdot q(0, ..., 0, x_n) \cdot h(x_n). \tag{3.3}$$

Como $r = \sum_{\nu=0}^{m-1} r_\nu x_n^\nu$, con $r_\nu \in K[[x_1, ..., x_{n-1}]]$, sus términos son todos de grado menor estrictamente que m respecto a x_n. Por ello, en (3.3), se tiene $r(0, .,0, x_n) = 0$, que implica $r_\nu \in \langle x_1, ..., x_{n-1} \rangle$, para todo $\nu = 0, ..., m-1$.
Por otro lado, $x_n^m = x_n^m \cdot q(0, ..., 0, x_n) \cdot h(x_n)$. Igualando los coeficientes de x_n^m, $1 = q(0, ..., 0, x_n)h(x_n)$. Necesariamente, al evaluar en $x_n = 0$, $q(0, ..., 0) \neq 0$ debido a que $h(0) \neq 0$. Entonces, q es una unidad en $K[[x]]$, y tiene sentido considerar q^{-1}, que también es una unidad.
Definimos $p := x_n^m - r$ y $u := q^{-1}$. p es un polinomio de Weierstrass de grado m respecto a x_n, debido a que $r = \sum_{\nu=0}^{m-1} r_\nu x_n^\nu$, con $r_\nu \in \langle x_1, ..., x_{n-1} \rangle$ para todo ν. Por tanto,

$$x_n^m = qf + r \Rightarrow (x_n^m - r) \cdot q^{-1} = f \Rightarrow f = u \cdot p.$$

Además, p y u son únicos debido a la unicidad de q y r. □

Ejemplo 3.2.4. Trabajamos de nuevo en $K[[x, y]]$. Sea $f(x, y) = y^3 + x^2y^3 + x^2 + x^4 \in K[[x, y]]$ la cual es y-general de orden 3. Estamos buscando u unidad y p polinomio de Weierstrass de grado 3 tales que $f = u \cdot p$. Por el Teorema de Preparación de Weierstrass, su existencia está garantizada y de hecho, reescribiendo f se tiene

$$f = y^3 + x^2y^3 + x^2 + x^4 = (1 + x^2)(y^3 + x^2).$$

Por tanto, tomando $u = 1 + x^2$, que es una unidad por tener término independiente no nulo, y $p = y^3 + x^2$, polinomio de Weierstrass de grado 3, ya habríamos acabado.

Corolario 3.2.5. *Sea $f \in K[[x]]$ x_n-general de orden m, entonces $K[[x]]/\langle f \rangle$ es un $K[[x_1, ..., x_{n-1}]]$-módulo libre de rango m.*

Demostración. El Teorema de la División de Weierstrass (3.1.7) establece que cualquier elemento de $K[[x]]$ se puede expresar de la forma $qf + r$, con q, r únicos. Esto nos garantiza que cualquier elemento de $K[[x]]/\langle f \rangle$ se puede expresar como combinación lineal de $1, x_n, ...x_n^{m-1}$, es decir, que $K[[x]]/\langle f \rangle$ es un $K[[x_1, ..., x_{n-1}]]$-módulo finitamente generado por $\{1, x_n, ...x_n^{m-1}\}$. Por la unicidad de la división, $\{1, x_n, ..., x_n^{m-1}\}$ es linealmente independiente, por lo que constituye una base y por tanto $K[[x]]/\langle f \rangle$ es un $K[[x_1, ..., x_{n-1}]]$-módulo libre de rango m. □

3.2.2. Noetherianidad en los Anillos de Series de Potencias Formales

Proposición 3.2.6. *Sea K un cuerpo, entonces $K[[x_1, ..., x_n]]$ es noetheriano.*

Demostración. Vamos a demostrarlo por inducción sobre n, probando que todo ideal en $K[[x_1, ..., x_n]]$ está finitamente generado.
Sea $n = 1$. Sea $I \subset K[[x_1]]$ un ideal no nulo, tomamos $f \in I, f \neq 0$ tal que $m = \text{ord}(f)$ sea mínimo. Entonces, se puede escribir $f = x_1^m \cdot u$, con u unidad. Por tanto, se tiene $I = \langle x_1^m \rangle$.
Supongámoslo cierto para $n - 1$, veamos que es cierto para n. Es decir, supongamos que $K[[x_1, ..., x_{n-1}]]$ es noetheriano.
Sea $I \subset K[[x_1, ..., x_n]]$ un ideal no nulo, y $f \in I, f \neq 0$. Por el Lema 3.1.4, podemos asumir que f es x_n-general de orden m. Por el Teorema de la base de Hilbert (1.2.2), como $K[[x_1, ..., x_{n-1}]]$ es un anillo noetheriano por la hipótesis de inducción, también $K[[x_1, ..., x_{n-1}]][x_n]$ es un anillo noetheriano. Entonces, $I \cap K[[x_1, ..., x_{n-1}]][x_n]$ está finitamente generado por ser un ideal en un anillo noetheriano. Supongamos que está generado por $f_1, ..., f_m$. Veamos que $I = \langle f, f_1, ..., f_m \rangle$. Sea $g \in I$, por el Teorema de División de Weierstrass, se puede escribir $g = qf + r$, con $r \in I \cap K[[x_1, ..., x_{n-1}]][x_n]$, por ende, para adecuados $\alpha_i \in K[[x_1, ..., x_{n-1}]][x_n]$, se tiene $r = \sum_{i=1}^m \alpha_i f_i$, concluyendo la demostración. □

Proposición 3.2.7. *Sea $y = (y_1, ..., y_m)$, y sea M un $K[[x, y]]$-módulo finitamente generado. Si $\dim_K(M/\langle x \rangle M) < \infty$, entonces M es un $K[[x]]$-módulo finitamente generado.*

Demostración. Vamos a demostrarlo por inducción sobre m.
Sea $m = 1$. Definimos el morfismo $\varphi : M/\langle x\rangle M \to M/\langle x\rangle M$ dado por $\varphi(m + \langle x\rangle M) = y_1 \cdot (m + \langle x\rangle M)$. Como $M/\langle x\rangle M$ es un K- espacio vectorial de dimensión finita, aplicando el teorema de Cayley - Hamilton, existe un polinomio

$$f := z^q + c_{q-1}z^{q-1} + ... + c_1 z + c_0 \in K\left[[x, y_1]\right][z],$$

con $c_0, ..., c_{q-1} \in K$ tal que al evaluarlo en φ se tiene

$$f(\varphi) = \varphi^q + c_{q-1}\varphi^{q-1} + ... + c_0 id \equiv 0,$$

donde id es la identidad.
Se tiene que $\mathrm{Ann}(M/\langle x\rangle M) = \{h \in K\left[[x, y_1]\right] \mid h \cdot M/\langle x\rangle M = 0\}$. Como $(\varphi^q + c_{q-1}\varphi^{q-1} + ... + c_0 id)(m + \langle x\rangle M) = 0$, entonces

$$f \cdot (m + \langle x\rangle M) = (y_1^q + c_{q-1}y_1^{q-1} + ... + c_0)(m + \langle x\rangle M) = 0,$$

para todo $m + \langle x\rangle M \in M/\langle x\rangle M$ y por tanto, $f \in \mathrm{Ann}(M/\langle x\rangle M)$. De aquí se obtiene que $fM \subset \langle x\rangle M$.
Tomemos $I = \langle x\rangle$ y definimos el morfismo $K\left[[x, y_1]\right]$-lineal $\psi : M \to M$ dado por $\psi(m) = f \cdot m$. Se tiene que $\psi(M) \subset IM$ y por hipótesis M es un $K\left[[x, y_1]\right]$-módulo finitamente generado. Por tanto, podemos volver a aplicar Cayley - Hamilton y entonces existe un polinomio

$$g := z^r + d_{r-1}z^{r-1} + ... + d_1 z + d_0 \in K\left[[x, y_1]\right][z],$$

con $d_{r-1}, ..., d_0 \in \langle x\rangle \subset \langle x, y_1\rangle$ tal que evaluando en ψ se obtiene

$$g(\psi) = \psi^r + d_{r-1}\psi^{r-1} + ... + d_0 id \equiv 0 \in Hom_{K[[x,y_1]]}(M, M).$$

Razonando de manera análoga al caso anterior, se tiene que

$$g = f^r + d_{r-1}f^{r-1} + ... + d_0 \in \mathrm{Ann}(M).$$

Como por hipótesis M es un $K\left[[x, y_1]\right]$-módulo finitamente generado, también es un $K\left[[x, y_1]\right]/\langle g\rangle$-módulo si lo dotamos de la siguiente estructura: $(p(x, y_1) + \langle g\rangle) \cdot m = p(x, y_1) \cdot m$, que está bien definida ya que $g \cdot m = 0$ para todo $m \in M$. Por ello, M es un $K\left[[x, y_1]\right]/\langle g\rangle$-módulo finitamente generado. Por construcción, g es y_1-general. Por el Corolario 3.2.5, $K\left[[x, y_1]\right]/\langle g\rangle$ es un $K\left[[x]\right]$-módulo finitamente generado. Esto implica que M es un $K\left[[x]\right]$-módulo finitamente generado.
Ahora supongamos que es cierto para $m - 1$, y lo probamos para m.
Tomamos M un $K\left[[x, y_1, ..., y_m]\right]$-módulo finitamente generado de manera

que $\dim_K(M/\langle x\rangle M) < \infty$.
Para simplificar la notación, definimos $A := K[[x, y_1, ..., y_{m-1}]]$. Se tiene que M es un $A[[y_m]]$-módulo.
Como $M/\langle x, y_1, ..., y_{m-1}\rangle M \subset M/\langle x\rangle M$, y este último tiene dimensión finita, entonces $\dim_K(M/\langle x, y_1, ..., y_{m-1}\rangle M) < \infty$. Razonando de manera análoga al caso $m = 1$, se obtiene que M es un A-módulo finitamente generado. Aplicando la hipótesis de inducción a M como A-módulo finitamente generado, se tiene que M es un $K[[x]]$-módulo finitamente generado. □

3.2.3. Álgebras Analíticas

Definición 3.2.8. Una K-álgebra analítica A es un anillo cociente de un anillo de series de potencias formales, $A = K[[x_1, ..., x_n]]/I$.

Corolario 3.2.9. *Sean A, B dos K-álgebras analíticas y sea $\varphi : A \to B$ un homomorfismo de anillos locales. Entonces φ es un homomorfismo finito si, y solo si $\dim_K(B/\varphi(\mathfrak{m}_A)B) < \infty$, donde $\mathfrak{m}_A$ denota el ideal maximal de A.*

Demostración. Supongamos que φ es finito, entonces B está finitamente generado como un $\varphi(A)$-módulo. Como $\mathfrak{m}_A$ es el ideal maximal de A, $A/\mathfrak{m}_A$ es un cuerpo. Denotando por $\varphi(\mathfrak{m}_A)B$ el ideal generado por $\varphi(\mathfrak{m}_A)$ en B, se tiene que $B/\varphi(\mathfrak{m}_A)B$ es un $A/\mathfrak{m}_A$-espacio vectorial finitamente generado. Por tanto, $\dim_K(B/\varphi(\mathfrak{m}_A)B) < \infty$.
Recíprocamente, supongamos que $\dim_K(B/\varphi(\mathfrak{m}_A)B) < \infty$. Como A, B son K-álgebras analíticas, podemos suponer $A = K[[x]]/I$ y $B = K[[y]]/J$, con $y = (y_1, ..., y_m)$. Entonces, B es un $K[[x, y]]$-módulo finitamente generado, donde la estructura del módulo viene dada por:
Sea $b \in B$, $x_i b = \varphi(x_i \bmod I) \cdot b, \quad y_i b = (y_i \bmod J) \cdot b$.
Además, $B/\langle x\rangle B = B/\varphi(A)B$. Por la Proposición 3.2.7, B es un $\varphi(A)$-módulo finitamente generado, y por tanto, φ es un homomorfismo finito. □

3.3. Teoremas Fundamentales de la Geometría Analítica

En esta sección se introducirá la Normalización de Noether para el caso de series de potencias normales, una herramienta fundamental para comprender mejor la estructura de los anillos cociente. Asimismo, se introducen dos teoremas clásicos de análisis desde un punto de vista algebraico.

Teorema 3.3.1 (Normalización de Noether)**.** *Sea K un cuerpo infinito, sean $A = K[[x_1, ..., x_n]]$ y $I \subset A$ un ideal. Entonces existe un número entero $s \leq n$*

y una matriz $M \in GL(n, K)$*, tal que si definimos las variables* $y_1, ..., y_n$ *mediante*

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = M^{-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

se tiene que la inclusión canónica $K[[y_{s+1}, ..., y_n]] \to A/I$*, definida por* $y_i \mapsto y_i \bmod I$*, es inyectiva y finita.*

Demostración. Vamos a demostrarlo por inducción sobre n. Sea $n = 0$, se tiene que $A = K$, por tanto, tomando $s = 0$ se tendría la inclusión $K \hookrightarrow A/I$, la cual es inyectiva. Asimismo, A/I está finitamente generado como K-módulo, por lo que la inclusión también es finita.
Supóngamos ahora que $n > 0$ y que es cierto para $n - 1$.
Si $I = \langle 0 \rangle$, se tiene que $A/I \cong A$. Basta tomar $y = 0$ y $y_i = x_i$ para todo $i = 1, ..., n$,
Sea ahora $I \neq \langle 0 \rangle$, entonces se puede tomar $f \in I \setminus \{0\}$. Se puede escribir como $f = \sum_{\nu \geq m} f_\nu$, con f_ν un polinomio homogéneo y $m > 0$. Tomamos f_m, que es el polinomio homogéneo de menor grado. Por el Lema 3.1.5, como K es infinito, existen $a_1, ..., a_{n-1} \in K$ tales que $f_m(a_1, ..., a_{n-1}, 1) \neq 0$. Realizamos el cambio lineal de variables $x_i = y_i + a_i y_n$, $i = 1, ..., n-1$, $x_n = y_n$, lo cual corresponde a un cambio lineal invertible dado por una matriz $M \in \mathrm{GL}(n, K)$. Se puede aplicar el Lema 3.1.4 a $f_m(x_1, ..., x_n) = f_m(y_1 + a_1 y_n, ..., y_{n-1} + a_{n-1} y_n, y_n)$, ya que $f_m(a_1, ..., a_{n-1}, 1) \neq 0$. Esto nos dice que f es y_n-general de orden m. Por el Corolario 3.2.5, se obtiene que $K[[y_1, ..., y_n]]/\langle f \rangle$ es un $K[[y_1, ..., y_{n-1}]]$-módulo libre de rango m. Como $\langle f \rangle \subset I \subset A$, se tiene el morfismo de anillos $A/\langle f \rangle \to A/I$, por lo que A/I también es un módulo finito sobre $K[[y_1, ..., y_{n-1}]]$.
Consideremos $I' = K[[y_1, ..., y_{n-1}]] \cap I$.
Si $I' = \langle 0 \rangle$, la inclusión $K[[y_1, ..., y_{n-1}]] \hookrightarrow A/I$ es inyectiva y finita, ya que hemos visto que A/I es un módulo finito sobre $K[[y_1, ..., y_{n-1}]]$.
Si $I' \neq \langle 0 \rangle$, entonces por la hipótesis de inducción existe un $s' \leq n - 1$ y un cambio lineal de variables $(z_1, ..., z_{n-1})^T = N^{-1} \cdot (y_1, ..., y_{n-1})^T$, con $N \in \mathrm{GL}(n-1, K)$, tal que la inclusión $K[[z_{s'+1}, ..., z_n]] \hookrightarrow K[[y_1, ..., y_{n-1}]]/I'$ es inyectiva y finita. Como A/I es un módulo finito sobre $K[[y_1, ..., y_{n-1}]]$, que a su vez es finito sobre $K[[z_{s'+1}, ..., z_n]]$, por la transitividad de extensiones finitas, A/I está finitamente generado sobre $K[[z_{s'+1}, ..., z_n]]$.

□

Teorema 3.3.2 (Teorema de la Función Implícita)**.** *Sea* K *un cuerpo y sea*

$F \in K[[x_1, ..., x_n, y]]$ tal que

$$F(x_1, ..., x_n, 0) \in \langle x_1, ..., x_n \rangle \quad y \quad \frac{\partial F}{\partial y}(x_1, ..., x_n, 0) \notin \langle x_1, ..., x_n \rangle,$$

entonces existe una única serie $y(x_1, ..., x_n) \in \langle x_1, ..., x_n \rangle K[[x_1, ..., x_n]]$ tal que $F(x_1, ..., x_n, y(x_1, ..., x_n)) = 0$.

Demostración. Por las hipótesis sobre F, se deduce que $F(0, ..., 0, y) = c \cdot y +$ términos de mayor grado en y. Por tanto, F es y-general de orden 1. El Teorema de Preparación de Weierstrass nos dice que F se puede escribir como $F = u(y - y(x_1, ..., x_n))$, donde $y(x_1, ..., x_n) \in K[[x_1, ..., x_n]]$, y u es una unidad en $K[[x_1, ..., x_n, y]]$. □

Teorema 3.3.3 (Teorema de la Función Inversa)**.** *Sea K un cuerpo, y sean $f_1, ..., f_n \in K[[y_1, ..., y_n]]$ tales que $f_1(0) = ... = f_n(0) = 0$. Entonces, el homomorfismo de K-álgebras*

$$\varphi : K[[x_1, ..., x_n]] \to K[[y_1, ..., y_n]]$$
$$x_i \mapsto f_i$$

es un isomorfismo si, y solo si, $det\left(\frac{\partial f_i}{\partial y_j}(0)\right) \neq 0$.

Demostración. Supongamos que φ es un isomorfismo. Denotamos por ψ a su inverso y sea $g_i := \psi(y_i)$. Por tanto, $x_i = \psi \circ \varphi(x_i = \psi(f_i) = f_i(g_1, ..., g_n)$ para todo $i = 1, ..., n$. De aquí se obtiene

$$\delta_{ij} = \sum_{k=1}^{n} \frac{\partial f_i}{\partial y_k}(\psi) \frac{\partial g_k}{\partial x_j}.$$

Entonces, $(\delta_{ij}) = \left(\frac{\partial f_i}{\partial y_k}(0)\right)\left(\frac{\partial g_k}{\partial x_j}(0)\right)$, y en consecuencia

$$1 = \det(\delta_{ij}) = \det\left(\frac{\partial f_i}{\partial y_k}(0)\right) \cdot \det\left(\frac{\partial g_k}{\partial x_j}(0)\right) \Rightarrow \det\left(\frac{\partial f_i}{\partial y_k}(0)\right) \neq 0.$$

Recíprocamente, supongamos que $\det\left(\frac{\partial f_i}{\partial y_j}\right) \neq 0$. Esto implica que la matriz $\left(\frac{\partial f_i}{\partial y_j}\right)$ es invertible, lo que nos permite obtener $\left(\frac{\partial f_i}{\partial y_j}\right) = (\delta_{ij})$ la matriz identidad mediante ciertas combinaciones lineales.
Para demostrar que φ es un isomorfismo, vamos a construir su inversa ψ y ver que también es un isomorfismo. Para ello, vamos a aplicar de forma reiterada el Teorema de la Función Implícita 3.3.2 a las funciones:

$$F_1 := f_1(y_1, ..., y_n) - x_1, ..., F_n = f_n(y_1, ..., y_n) - x_n,$$

con $F_i \in K\left[[y_1, ..., y_n, x_i]\right]$, $\forall i = 1, ..., n$.
Se cumple que

$$F_1(0, y_2, ..., y_n, x_1) \in \langle y_2, ..., y_n, x_1\rangle,\ \frac{\partial F_1}{\partial y_1} = \frac{\partial f_1}{\partial y_1}(0, y_2, ..., y_n) \notin \langle y_2, ..., y_n, x_1\rangle$$

por hipótesis. Entonces, aplicando el teorema, existe $g \in \langle y_2, ..., y_n, x_1\rangle \cdot K\left[[y_2, ..., y_n, x_1]\right]$ tal que $f(g, y_2, ..., y_n) = x_1$. Sustituimos en F_i con $i = 2, ..., n$ y obtenemos:

$$\tilde{F}_2 = f_2(g, y_2, ..., y_n) - x_2, ..., \tilde{F}_n = f_n(g, y_2, ..., y_n) - x_n,$$

con $\tilde{F}_i \in K\left[[y_2, ..., y_n, x_1, x_i]\right]$ para todo $i = 2, ..., n$.
Como $\det\left(\frac{\partial \tilde{F}_i}{\partial y_j}(0)\right) \neq 0$, podemos obtener de nuevo mediante combinaciones lineales adecuadas $\left(\frac{\partial \tilde{F}_i}{\partial y_j}(0)\right) = (\delta_{ij})$. Por tanto, esto nos permite usar un procedimiento inductivo y suponer que tras aplicar el Teorema de la Función Implícita $n-1$ veces, obtendríamos $g_2, ..., g_n \in \langle x_1, ..., x_n\rangle \cdot K\left[[x_1, ..., x_n]\right]$ tales que $\tilde{F}_i(g_2, ..., g_n) = 0$ para $i = 2, ..., n$.
Sea ahora $g_1 := g(g_2, ..., g_n)$, definimos el morfismo entre K-álgebras $\psi : K\left[[y]\right] \to K\left[[x]\right]$ dado por $\psi(y_i) := g_i$, entonces

$$\psi \circ \varphi(x_i) = \psi(f_i) = f_i(g_1, ..., g_n) = x_i \tag{3.4}$$

para todo $i = 1, ..., n$. Por tanto, de aquí se obtiene que φ es inyectiva. Asimismo, $\det\left(\frac{\partial g_i}{\partial x_j}(0)\right) \neq 0$ debido a que al derivar en 3.4 y evaluar en 0, con un razonamiento análogo realizado en la otra implicación, se obtiene $\det\left(\frac{\partial f_i}{\partial y_j}(0)\right) \cdot \det\left(\frac{\partial g_i}{\partial x_j}(0)\right) = 1$, y por hipótesis $\det\left(\frac{\partial f_i}{\partial y_j}(0)\right) \neq 0$. Finalmente, ψ es un isomorfismo, y por ello $\varphi = \psi^{-1}$ también lo es, lo que concluye la demostración. □

Capítulo 4

Bases estándar

El objetivo de este capítulo es estudiar las bases estándar para ideales en anillos de series de potencias formales.
Para ello, hay que introducir conceptos análogos a los del anillo de polinomios, presentados en las Secciones 1.5 y 1.6. Sea K un cuerpo y $x = (x_1, ..., x_n)$. En este capítulo vamos a trabajar con un orden monomial local $>$ sobre $\text{Mon}(x_1, ..., x_n)$ dado por

$$x^\alpha > x^\beta \Rightarrow \text{w-deg}(x^\alpha) \leq \text{w-deg}(x^\beta),$$

para un vector de pesos $w = (w_1, ..., w_n)$, $w_i > 0$ adecuado. Este tipo de orden es compatible con la topología $\langle x \rangle$-ádica, por lo que podemos comparar bases estándar en $K[x]_{\langle x \rangle}$ y $K[[x]]$.
Un elemento $f \in K[[x]] \setminus \{0\}$ se puede escribir como $\sum_{\nu=0}^{\infty} a_\nu x^{\alpha(\nu)}$, donde $a_\nu \in K$, $a_0 \neq 0$ y $x^{\alpha(\nu)} > x^{\alpha(\nu+1)}$ para todo ν.

Definición 4.0.1. Sea $>$ un orden monomial, y $f \in K[[x]]$ una serie de potencias no nula representada de forma única como en el párrafo anterior. Se definen:

1) $\text{LM}(f) := x^{\alpha(0)}$, el monomio líder de f.

2) $\text{LE}(f) := \alpha(0)$, el exponente líder de f.

3) $\text{LT}(f) := a_0 x^{\alpha(0)}$, el término líder de f.

4) $\text{LC}(f) := a_0$, el coeficiente líder de f.

5) $\text{tail}(f) := f - \text{LT}(f) = \sum_{\nu=1}^{\infty} a_\nu x^{\alpha(\nu)}$, la cola de f.

El anillo localizado $K[x]_>$ definido en 1.5.8 satisface la siguiente cadena de inclusiones:

$$K[x]_> \subset K[x]_{\langle x \rangle} \subset K[[x]].$$

Definición 4.0.2. Sea $I \subset K[[x]]$ un ideal. Un conjunto finito $G \subset K[[x]]$ es una **base estándar** de I si

$$G \subset I, \text{ y } L(I) = L(G).$$

Por lo tanto, G es una base estándar, si los monomios líder de los elementos de G generan el ideal líder de I, es decir, si para cualquier $f \in I \setminus \{0\}$ existe un $g \in G$ tal que $\mathrm{LM}(g)|\mathrm{LM}(f)$.

La existencia de bases estándar en $K[[x]]$ viene garantizada por la Proposición 3.2.6, que afirma que el ideal líder está finitamente generado, ya que $K[[x]]$ es un anillo Noetheriano.

Definición 4.0.3. Sea $G \subset K[[x]]$ un subconjunto. G es **interreducido** si $0 \notin G$ y si $\mathrm{LM}(g) \nmid \mathrm{LM}(f)$ para todo $f, g \in G$ tales que $f \neq g$. Una base estándar interreducida también se dice **mínima**.

La existencia de una forma normal reducida viene garantizada por la versión formal del Teorema de División de Grauert, que consiste en una generalización del Teorema de División de Weierstrass 3.1.7.

Teorema 4.0.4 (Teorema de División de Grauert)**.** *Sean* $f, f_1, ..., f_m \in K[[x_1, ..., x_n]]$*, entonces existen* $q_j, r \in K[[x_1, ..., x_n]]$ *tales que*

$$f = \sum_{j=1}^{m} q_j f_j + r$$

y, para todo $j = 1, ..., m$*,*

1) ningún monomio de r *es divisible por* $\mathrm{LM}(f_j)$*,*

2) $\mathrm{LM}(q_j f_j) \leq \mathrm{LM}(f)$*.*

Demostración. Sin pérdida de generalidad, podemos asumir que $\mathrm{LC}(f_i) = 1$ para todo $i = 1, ..., m$. Denotamos por $\mathrm{LM}(f_i) := x^{\alpha(i)}$, $i = 1, ..., m$ y

$$\Gamma := \langle \alpha(1), ..., \alpha(m) \rangle := \{\alpha \in \mathbb{N}^n \mid \alpha - \alpha(i) \in \mathbb{N}^n \text{ para algún } i\}$$

el semimódulo en $\mathbb{N}^n$ generado por $\alpha(1), ..., \alpha(m)$.
Definimos de manera recursiva:

$$\Gamma_1 := \langle \alpha(1) \rangle, ..., \Gamma_i := \langle \alpha(i) \rangle \cap (\Gamma \setminus \langle \alpha(1), ..., \alpha(i-1) \rangle).$$

Sea ahora $w = \sum w_\alpha x^\alpha \in K[[x]]$, definimos

$$r(w) := \sum_{\alpha \notin \Gamma} w_\alpha x^\alpha, \quad q_j(w) := \frac{1}{x^{\alpha(j)}} \sum_{\alpha \in \Gamma_j} w_\alpha x^\alpha.$$

Se puede reescribir w como

$$w = \sum_{j=1}^{m} q_j(w)x^{\alpha(j)} + r(w). \tag{4.1}$$

Definimos de manera recursiva la sucesión $\{w_i\}_{i\in\mathbb{N}}$ tal que:

$$w_0 := f, \quad w_{i+1} := w_i - \sum_{j=1}^{m} q_j(w_i)f_j - r(w_i).$$

Queremos ver que la serie $w := \sum_{j=0}^{\infty} w_j$ converge en la topología $\langle x\rangle$-ádica. Aplicando 4.1 a w_i, se tiene que $w_i = \sum_{j=1}^{m} q_j(w_i)x^{\alpha(j)} + r(w_i)$. Por tanto, $w_{i+1} = \sum_{j=1}^{m} q_j(w_i)(x^{\alpha(j)} - f_j)$. Se cumple $\mathrm{LM}(w_{i+1}) < \mathrm{LM}(w_i)$, debido a $\mathrm{LT}(f_j) = x^{\alpha(j)}$. Esto implica que los órdenes con peso de los monomios líder crecen estrictamente. Por consiguiente, para todo $h \in \mathbb{N}$ existe $n_0 \in \mathbb{N}$ tal que $w_i \in \langle x\rangle^h$, $\forall i \geq n_0$. Asimismo, por hipótesis, el orden es compatible con la filtración $\langle x\rangle$-ádica.
Como $\sum_{j=0}^{\infty} w_j = w$, se tiene que $r(w) = \sum_{j=0}^{\infty} w(w_j)$ y $q_i(w) = \sum_{j=0}^{\infty} q_i(w_j)$. Para demostrar que f se puede descomponer como $f = \sum_{j=1}^{m} q_j(w)f_j + r(w)$, escribimos

$$f = \sum_{j=0}^{\infty}(w_j - w_{j+1}) = \sum_{j=0}^{\infty}\left(w_j - w_j + \sum_{k=1}^{m} q_k(w_j)f_k + r(w_j)\right) =$$
$$= \sum_{k=1}^{m}\left(\sum_{j=0}^{\infty} q_k(w_j)\right)f_k + \sum_{j=0}^{\infty} r(w_j) = \sum_{k=1}^{m} q_k(w)f_k + r(w).$$

Tiene sentido considerar $f = \sum_{j=0}^{\infty}(w_j - w_{j+1})$ ya que $f = w_0$ y por tanto, podemos escribir $f = w_0 = (w_0 - w_1) + (w_1 - w_2) + ... = \sum_{j=0}^{\infty}(w_j - w_{j+1})$. Es una serie telescópica bien definida por ser $\{w_j\}_{j\in\mathbb{N}}$ convergente.
Por construcción, ningún monomio de $r(w)$ es divisible por $\mathrm{LM}(f_j) = x^{\alpha(j)}$ para todo $j = 1, ..., m$.
Asimismo, $\mathrm{LM}(q_k(w)f_k) = \mathrm{LM}\left(\sum_{j=0}^{\infty} q_k(w_j)f_k\right) \leq \mathrm{LM}(q_k(w_0)f_k)$ ya que $\mathrm{LM}(w_{k+1}) < \mathrm{LM}(w_k)$ para todo k. Como hemos establecido $f = w_0$, se satisface $\mathrm{LM}(q_k(w)f_k) \leq \mathrm{LM}(f)$, lo que concluye la demostración. □

Definición 4.0.5. Con las notaciones del Teorema de División 4.0.4, definimos

$$\mathrm{NF}(f \mid \{f_1, ..., f_m\}) := r,$$

obteniendo una **forma normal reducida**.

La existencia de una forma normal reducida nos permite, de forma análoga al caso de los polinomios, obtener todas las propiedades fundamentales asociadas a las bases estándar en el anillo de series de potencias formales.
Ahora demostraremos un teorema que nos permite encontrar bases estándar para ideales en $K[[x]]$ a partir de ideales en $K[x]$, lo cual es clave en la geometría analítica local.

Teorema 4.0.6. *Sean $K[x] \subset K[[x]]$, dotados con órdenes locales compatibles. Sea $I \subset K[x]$ un ideal y S una base estándar de I, entonces S es una base estándar de $IK[[x]]$.*

Demostración. Sea $\{f_1, ..., f_m\}$ una base estándar de $I \subset K[x]$ y sea

$$\bar{f} = \sum_{j=1}^{m} \bar{h}_j f_j \in IK[[x]]$$

un elemento no nulo. Elegimos $c \in \mathbb{N}$ tal que $\mathrm{LM}(\bar{f}) \notin \langle x \rangle^c$ y todo monomio en $\langle x \rangle^c$ sea más pequeño que $\mathrm{LM}(\bar{f})$. Ahora tomamos $h_j \in K[x]$ tal que $\bar{h}_j - h_j \in \langle x \rangle^c$. Sea $f := \sum_{j=1}^{m} h_j f_j$, entonces $f \in I$ ya que $\{f_1, ..., f_m\}$ genera I por el Lema 1.6.4. Por tanto, $f - \bar{f} = \sum_{j=1}^{m} (h_j - \bar{h}_j) \in \langle x \rangle^c$. Esto implica que $\mathrm{LM}(f) = \mathrm{LM}(\bar{f})$, ya que todos los monomios en $\langle x \rangle^c$ son más pequeños que $\mathrm{LM}(\bar{f})$. Pero se tiene que $\mathrm{LM}(f) \in L(I) = \langle \mathrm{LM}(f_1), ..., \mathrm{LM}(f_m) \rangle$. De aquí se obtiene $\mathrm{LM}(\bar{f}) \in L(I)$. Por tanto, como esto se cumple para todo $\bar{f} \in IK[[x]]$ no nulo, se tiene que $L(IK[[x]]) = \langle \mathrm{LM}(f_1), ..., \mathrm{LM}(f_m) \rangle$, lo que concluye la demostración. □

Ejemplo 4.0.7. Vamos a usar SINGULAR para calcular una base estándar del ideal

$$\langle x^{10} + x^9 y^2, y^8 - x^2 y^7 \rangle \subseteq \mathbb{Q}[[x, y]]$$

respecto al orden lexicográfico negativo con peso con el vector de pesos $w = (-2, -7)$.
El orden con el que trabajamos es local, por lo que resulta compatible al considerarlo tanto en $\mathbb{Q}[x, y]$ como en $\mathbb{Q}[[x, y]]$. El código sería el siguiente:

```
ring Q1 = 0,(x,y),Ws(-2,-7);
poly f1 = x10 + x9y2;
poly f2 = y8 - x2y7;
ideal I = f1,f2;
ideal G = std(I);   //calculo base estandar
G;
//-> G[1]=x9y2 + x10
//-> G[2]=x16 + x13
```

```
//-> G[3]=x13 - x15
//-> G[4]=y8 - x2y7
```

Por el teorema 4.0.6, como también se tiene que $I \subset \mathbb{Q}[x, y]$, la base estándar G también es una base estándar en $I\mathbb{Q}[[x, y]] \subset \mathbb{Q}[[x, y]]$.
Si tomásemos el vector de pesos $w = (-1, -1)$, se obtendría una base estándar diferente:

```
ring Q2 = 0,(x,y),Ws(-1,-1);
ideal I = imap(Q1,I);
ideal G = std(I);   //calculo base estandar
G;
//-> G[1]=x2y7 - y8
//-> G[2]=x2y9 + x10
//-> G[3]=x12y + xy11
//-> G[4]=x13 - xy12
//-> G[5]=y14 + xy12
//-> G[6]=xy13 + y12
```

Y con el orden lexicográfico negativo:

```
ring Q3 = 0,(x,y),ls;
ideal I = imap(Q1,I);
ideal G = std(I);
G;
//-> G[1]=y8 - x2y7
//-> G[2]=x9y2 + x10
//-> G[3]=x13
```

Conclusión

A lo largo de este trabajo, se ha estudiado cómo están estructurados los anillos de series de potencias formales y cuáles son sus propiedades. Hemos podido apreciar que gran parte de los resultados ya conocidos para el caso de polinomios son válidos también para el caso de series, aunque en ciertas ocasiones sea necesario imponer alguna hipótesis adicional.

En particular, el Teorema 4.0.6 nos permite obtener bases estándar a partir de ideales generados únicamente por polinomios. Esto es de gran importancia, ya que se facilita la aplicación de ciertos algoritmos ya conocidos para el caso de polinomios, como el criterio de Buchberger, adaptándolos a este tipo de anillos.

En resumen, los anillos de series de potencias formales permiten extender al contexto local muchas herramientas clásicas del álgebra conmutativa, como la división, la noetherianidad o el uso de bases estándar. El estudio de sus propiedades, tanto algebraicas como topológicas, muestra la utilidad en el estudio local del álgebra y la geometría.

Bibliografía

[1] M. F. Atiyah e I. G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley, 1969. ISBN: 0201003619.

[2] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer, 1994. ISBN: 0387942696.

[3] M. Reid. *Undergraduate commutative algebra*. Cambridge University Press, 1995. ISBN: 1-139-17272-7.

[4] G.M. Greuel y G. Pfister. *A Singular Introduction to Commutative Algebra*. 2nd ed. 2008. Springer Berlin Heidelberg, 2008. ISBN: 3-540-73542-9.

[5] S. Bosch. *Algebraic Geometry and Commutative Algebra*. 1st ed. 2013. Springer London, 2013. ISBN: 1-4471-4829-0.

[6] A. Gathmann. *Class Notes: Commutative Algebra (TU Kaiserslautern, 2013/14)*. Accedido: 28-10-2024. 2013. URL: https://agag-gathmann.math.rptu.de/en/commalg.php.

[7] D. A. Cox, J. Little y D. O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 4th ed. 2015. Springer International Publishing, 2015.

[8] The Stacks Project Authors. *Stacks Project*. 2018. URL: https://stacks.math.columbia.edu.

[9] D. Gonzalez Jr. *Lemma in Atiyah and MacDonald and a Semi-Constructive Proof*. Tesis de máster, The Ohio State University. Accedido; 6-05-2025. 2024. URL: http://rave.ohiolink.edu/etdc/view?acc_num=osu1717856405854587.

[10] M. Mazur. *Notes: Weierstrass Division Theorem*. Accedido: 3-04-2025. URL: https://people.math.binghamton.edu/mazur/teach/weierstrass.pdf.