Pontificia Universidad Católica del Perú
Escuela de Posgrado

Los teoremas de estructura de Cohen para anillos locales completos

Tesis para optar el Grado de
Magíster en Matemáticas

VELÁSQUEZ ALARCÓN, JORGE DAVID

Asesor
FERNÁNDEZ SÁNCHEZ, PERCY BRAULIO

Jurado
NECIOSUP PUICAN, HERNÁN (PRESIDENTE)
MUÑOZ MÁRQUEZ, GABRIEL (MIEMBRO)

Lima - Perú
Septiembre - 2019

Los teoremas de estructura de Cohen para anillos locales completos

VELÁSQUEZ ALARCÓN, JORGE DAVID [1]

Tesis presentada a consideración del cuerpo docente de la Escuela de Posgrado, de la PUCP, como parte de los requisitos para obtener el grado académico de Magister en Matemáticas.

Miembros de Jurado:

Dr. Fernández Sánchez, Percy Braulio (Asesor)

Dr. Neciosup Puican, Hernán (presidente)

Dr. Muñoz Márquez, Gabriel (miembro)

Lima - Perú
Septiembre - 2019

[1] Proyecto DGI 2019-1-0021

RESUMEN

El presente trabajo se trata de que un anillo (A, m) local, noetheriano, regular, completo de dimensión d, cuya característica sea igual que la de su cuerpo residual (A/m), sea isomorfo al anillo de series formales de potencia en d variables con coeficientes en este cuerpo. Pero si las características son diferentes como por ejemplo la característica de A es cero y la característica de A/m es un número primo p, A no tiene esta estructura, en este caso p estará contenido en m y no estará en m^2, entonces se dice que A es inramificado, por lo tanto en este caso A queda completamente determinado por su cuerpo residual (A/m) y su dimensión.

ABSTRACT

The present work is about the fact that a local, noetherian, regular, complete ring (A, m) with dimension d, whose characteristic is the same as that of its residual field (A/m) is isomorphic to the ring of formal series of power in variable d with coefficientes in this field. But if the characteristics are different as for example the characteristic of A is zero and the characteristic of $A/m$is a prime number p, then A does not have this structure and in this case p will be contained in the maximal ideal m and will not be contained in m^2, then it is said that A is unramified, therefore in this case the ring A is completely determined by its residual field (A/m) and its dimension.

Dedicado a mi esposa Alessandra
y a mis hijos Mathias y Xiomara
que son mi vida y mi inspiración
para seguir adelante.

Índice general

Agradecimientos

Agradezco en primer lugar a Dios, por darme la oportunidad de realizar mis estudios de maestría en la PUCP y concluirla satisfactoriamente.

Agradezco a mis padres Victor y Albina por brindarme todo su amor, cariño y por enseñarme a no rendirme y siempre perseverar.

Agradezco a mi esposa Alessandra, que con su amor, paciencia y comprensión siempre me estimuló a que siga adelante en mis estudios. A mis hijos Mathias y Xiomara que son mi vida y mi inspiración para seguir adelante. A mis hermanos Carlos y Pilar por el amor y apoyo incondicional que siempre me brindaron.

Agradezco a mis amigos de la maestría, en especial a Jhon Suarez, Héctor Llanos y Jorge Condeña.

Agradezco a los profesores Jesús Zapata, Arturo Fernández y Jaime Cuadros, por impartirme sus enseñanzas y conocimientos en mi crecimiento y fortalecimiento académico.

Agradezco a los profesores Hernán Neciosup y Gabriel Muñoz por sus correcciones, observaciones y aportes para la realización de la presente tesis.

Quiero agradecer de manera especial al profesor Percy Fernández por brindarme sus conocimientos y enseñanzas en los distintos cursos que me dictó que me sirvieron para mi crecimiento académico. Además quiero agradecerle la asesoría y el tiempo brindado para la realización del presente trabajo.

Introducción

El concepto de anillo local fue dado por Krull, quién definió tal anillo como un anillo conmutativo A en el cual todo ideal tiene una base finita y el conjunto m de todas las no unidades es un ideal maximal. Krull también demostró que la intersección de todas las potencias de m es el ideal cero y si consideramos las potencias de m como un sistema de vecindades de cero, entonces A sería un anillo topológico.

El anillo local A es llamado completo si toda sucesión de Cauchy tiene un límite. Sea $m = (u_1, u_2, \ldots, u_n)$ y supongamos que ningún elemento de esta base puede ser omitido, si los ideales $(u_1, u_2, \ldots, u_i)$, $i = 1, 2, \ldots, n$, son todos primos, A es llamado anillo local regular de dimensión n.

Krull conjeturó que un anillo local, regular, completo A de dimensión n cuya característica p es igual que la de su cuerpo residual A/m es isomorfo al anillo de series formales de potencia en n variables con coeficientes en este cuerpo. Si las características son diferentes, como por ejemplo que la característica de R es cero y la característica de R/m es un número primo, entonces A no tiene esta estructura, en este caso notemos que p estará contenido en m, entonces Krull conjeturó que si A es inramificado ($p \not\subseteq m^2$) entonces A está únicamente determinado por su cuerpo residual y su dimensión.

Finalmente Krull conjeturó que todo anillo local, completo es una imagen homomórfica de un anillo local, regular, completo.

Cohen demostró los teoremas de estructura para anillos locales completos y otras propiedades de anillos locales.

Este trabajo está distribuido de la siguiente forma:

En el capítulo I hacemos una revisión de los conceptos y resultados elementales de anillos. Seguidamente revisaremos anillos locales, el proceso de localización que es una de las herramientas más importantes del álgebra conmutativa, los anillos noetherianos que son los anillos más importantes de álgebra conmutativa. Finalmente, revisamos los conceptos y propiedades de los anillos regulares y la teoría de dimensión.

En el capítulo II estudiaremos el anillo de series formales de potencia donde veremos que este anillo es un dominio, es un anillo local, noetheriano y regular. Seguidamente dotaremos al anillo de series formales de potencia de una métrica y determinaremos que este es un anillo completo, donde surge la inquietud de preguntarnos que si un anillo con estas propiedades será isomorfo al anillo de series formales de potencia.

En el capítulo III veremos la filtración de un anillo, métrica en un A-módulo filtrado, completación $\mathfrak{a}$-ádica de un anillo local, la suavidad formal de una A-álgebra B sobre A, extensiones separables de cuerpos, la suavidad formal entre anillos topológicos y el anillo de coeficientes de un anillo local.

En el capítulo IV veremos íntegramente las demostraciones del los Teoremas de estructura de Cohen para anillos locales completos. La demostración se divide en dos casos el equicaracterístico y el inequicaracterístico, donde usaremos e introduciremos los conceptos de anillo local ramificado e inramificado, conceptos que introdujo Krull.

En el cápitulo V visualizaremos una versión muy especializada acerca de el teorema de estructura para anillos locales completos que nos dice que cualquier anillo de ideales principales es suma directa de anillos, donde cada uno de los cuales es imagen homomórfica de un DIP. También veremos que dado una función f en el anillo $\mathcal{O}_{V,P}$ de funciones regulares en un punto liso $p \in V$ (Variedad) se le asocia su serie de Taylor en el anillo de series formales de potencia.

Capítulo 1

Preliminares

En este capítulo haremos una revisión de las definiciones y propiedades elementales de anillos y módulos. Después de esta revisión pasaremos a discutir sobre anillos locales y el proceso de localización que es una de las herramientas más importantes del álgebra conmutativa. Para seguir avanzando y ver resultados más fuertes consideraremos condiciones de finitud mediante las condiciones de cadena en los anillos y veremos también a los anillos más importantes en el álgebra conmutativa los anillos noetherianos, para finalmente revisar las definiciones y propiedades de la teoría de la dimensión y de anillos regulares.

1.1. Anillos e ideales

Un anillo A es un conjunto con dos operaciones, la adición y el producto, tal que es un grupo abeliano con la adición, es asociativa con el producto y verifica la propiedad distributiva. Cuando hablemos del anillo asumiremos que es un anillo conmutativo y con identidad.

Un divisor de cero en un anillo A es un elemento x que divide a cero, es decir existe un $y \neq 0$ en A tal que $xy = 0$. Un anillo sin divisores de cero no nulos se llama dominio de integridad. Por ejemplo: $\mathbb{Z}$, $\mathbb{Q}$.

Un subconjunto I de un anillo A, es un ideal de A si I es un subgrupo aditivo de A y AI es un subconjunto de I. Los elementos de A/I son las clases de I en A y la aplicación $\varphi : A \to A/I$ envía a cada elemento $x \in A$ a su clase $x + I$ es un homomorfismo de anillos suprayectivo y existe una correspondencia biunívoca que mantiene el orden entre los ideales J de A que contiene a I y los ideales $\bar{J}$ de A/I

por $J = \varphi^{-1}(\bar{J})$.

Un ideal I del anillo A es llamado principal si esta generado por un elemento, esto es, existe $x \in A$, tal que $I = \{rx \, ; r \in A\}$ y se denota $I = (x)$.

Al entero n positivo más pequeño tal que $na = 0$, $\forall\ a \in A$, es llamado la característica de A, si no existiera n, se dice que A es de característica cero, por ejemplo $\mathbf{Z}$ tiene característica cero, $\mathbf{Z}_n$ tiene característica n y si F es un cuerpo entonces tiene característica 0 o p, donde p es primo.

Un ideal p en A es primo si $p \neq (1)$ y si para todo $x, y \in A$ con $xy \in p$, entonces x pertenece a p o y pertenece a p. El conjunto $\mathrm{Spec}(A) = \{p \mid p$ es un ideal primo de $A\}$ es llamado el espectro de A. Un ideal m en A es maximal si $m \neq (1)$ y no existe ningún ideal a tal que $m \subset a \subset (1)$. Todo anillo A no nulo por lo menos tiene un ideal maximal.

p es un ideal primo de A si y solamente si A/p es un dominio. m es un ideal maximal si y solamente si A/m es un cuerpo.

Un dominio de ideales principales (D.I.P.) es un dominio de integridad en el que cada ideal es principal, en un anillo de este tipo todo ideal primo no nulo es maximal. Un dominio de integridad A, se dice que es un dominio de factorización única (D.F.U.) si cualquier elemento no nulo es unidad o puede escribirse como producto de un número finito de elementos irreducibles de A. Todo D.I.P. es un D.F.U. pero lo recíproco no es cierto, por ejemplo consideremos el anillo $F[x,y]$ con coeficientes en un cuerpo, claramente $F[x, y]$ es un D.F.U. pero no es D.I.P., pues (x, y) es un ideal de $F[x, y]$ que no es principal.

El conjunto N de los elementos nilpotentes de un anillo A forman un ideal y A/N no posee elementos nilpotentes diferentes de cero. El ideal N se llama el nilradical de A y se cumple que N es la intersección de los ideales primos de A. La intersección de los ideales maximales de un anillo A se llama el radical de Jacobson de A y se denota por R.

Proposición 1.1.1. $x \in R \Leftrightarrow 1 - xy$ es unidad en A para todo $y \in A$.

Demostración. Supongamos que $1 - xy$ no es unidad, luego existe un ideal maximal

m de A tales que $1 - xy \in m$, luego desde que $x \in R \subset m$ entonces $xy \in m \ \forall\ y \in A$, luego tenemos que $(1 - xy) + xy = 1 \in m$, lo cual es una contradicción, entonces $1 - xy$ es unidad.
Recíprocamente supongamos que $x \not\in R$, entonces $x \not\in m$, para algún ideal maximal m, luego x y m generan el ideal (1) entonces $xy + u = 1$, $u \in m$, $y \in A$, luego $u = 1 - xy \in m$, entonces $(1 - xy)$ no es unidad, lo cual es una contradicción, por lo tanto $x \in R$. □

1.2. Anillos locales e ideales primarios

Un anillo A que tiene solamente un ideal maximal m se llama anillo local. Por ejemplo, los cuerpos son anillos locales pues tienen como único ideal maximal el cero. El cuerpo $K = A/m$ recibe el nombre del cuerpo residual. Decir que (A, m, K) es un anillo local significa que A es un anillo local $m = \mathrm{rad}(A)$ y $K = A/m$.

Si (A, m) es un anillo local entonces los elementos de A no contenidos en m son unidades. En un anillo no nulo A, donde el conjunto de las no unidades son un ideal, es un anillo local.

Sea (A, m) y (B, n) anillos locales y $f : A \to B$ un homomorfismo de anillos, f será llamado homomorfismo local si $f(m) \subset n$.

Sea b un ideal del anillo A, $r(b) = \{x \in A : x^n \in b$, para algún $n > 0\}$ se denomina el radical de b y es un ideal de A. Si p es un ideal primo $r(p^n) = p$, para todo $n > 0$.

Un ideal q de un anillo A es llamado primario si q no contiene a 1 y para todo par de elementos x, y que pertenecen a A se tiene que si $xy \in q$, $x \not\in q$, entonces $y^n \in q$ para algún $n > 0$. Por ejemplo, los ideales primos son primarios, pero lo recíproco no es cierto.

Si q es un ideal primario, entonces $r(q)$ es el menor ideal primo conteniendo q. Si $p = r(q)$, entonces se dice que q es p-primario.

Ejemplo: Los ideales primarios en $\mathbf{Z}$ son (0) y (p^n), donde p es primo, pues son los únicos ideales de $\mathbf{Z}$ que tienen radical primo.

Si $r(\mathfrak{a})$ es maximal, entonces $\mathfrak{a}$ es primario, las potencias de un maximal $\mathfrak{m}$ son $\mathfrak{m}$-primarias.

Si p es un ideal primo en A, entonces $p[x]$ es primo en $A[x]$ y si q es un ideal p-primario en A, entonces $q[x]$ es $p[x]$-primario en $A[x]$.

1.3. Módulos

Sea A un anillo. Un A-módulo es un par (M, μ) donde M es un grupo abeliano y μ es una aplicación:

$$\begin{aligned} \mu : A \times M &\longrightarrow M \\ (a,x) &\longrightarrow \mu(a,x) = a \cdot x \end{aligned}$$

que $\forall\ a,b \in A$, $\forall\ x,y \in M$ se satisfacen los siguientes axiomas:

(i) $a \cdot (x+y) = a \cdot x + a \cdot y$

(ii) $(a+b) \cdot x = a \cdot x + b \cdot x$

(iii) $(ab) \cdot x = a \cdot (b \cdot x)$

(iv) $1 \cdot x = x$.

Ejemplos:

1. Si A es un cuerpo, entonces todo A-módulo es un A-espacio vectorial.
2. Un ideal $\mathfrak{a}$ de A es un A-módulo. El mismo A es un A-módulo.

Sean M, N A-módulos. $f : M \to N$ es un homomorfismo de A-módulos si $\forall\ a \in A$, $\forall\ x, y \in M$ se tiene:

(i) $f(x+y) = f(x) + f(y)$

(ii) $f(a \cdot x) = a \cdot f(x)$

Un submódulo M' de M es un subgrupo de M que es cerrado respecto a la multiplicación por elementos de A. El grupo M'/M tiene una estructura de A-módulo de M, definida por $a(x+M') = ax + M'$.

Sea $f : M \to N$ un homomorfismo de A-módulos.

1. El $\ker(f) = \{x \in M : f(x) = 0\}$ y es un submódulo de M.

2. La imagen de f es el conjunto $\mathbf{Im}(f) = f(M)$.

3. El $\operatorname{coker}(f) = N/\mathbf{Im}(f)$ que es un módulo cociente de N.

Observación: $M/\ker(f) \cong \mathbf{Im}(f)$.

Si M y N son A-módulos, una suma directa $M \oplus N$ es el conjunto de todos los pares (x, y) con $x \in M$, $y \in N$.

$M \oplus N$ es un A-módulo si se define la adición y la multiplicación por un escalar de la siguiente manera:

1. $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

2. $a(x, y) = (ax, ay)$

En general, si $(M_i)_{i\in I}$ es una familia de A-módulos, podemos definir su suma directa $\oplus_{i\in I}M_i$; donde sus elementos son de la forma $(x_i)_{i\in I}$ tal que $x_i \in M_i, \forall\ i \in I$ y casi todos los x_i son nulos (excepto un número finito de índices).

Un A-módulo libre es un A-módulo isomorfo a $\oplus_{i\in I}M_i$, donde $M_i \cong A$ como A-módulo, se denota $A^{(I)}$.

Un A-módulo libre finitamente generado es isomorfo a $A \oplus A \oplus \ldots \oplus A$ (n sumandos) y se denota por A^n. Por convenio, A^0 es el módulo cero y lo denotaremos por 0.

Si M es un A-módulo de generación finita, a un ideal de A tal que $a \subset R$. Entonces si $aM = M$ se tiene que $M = 0$. Este resultado es conocido como el Lema de Nakayama.

Sea (A, m, k) un anillo local y M un A-módulo de generación finita. Como M/mM es anulado por m se tiene que M/mM es un A/m-módulo y como $k = A/m$ es cuerpo se tiene que M/mM es un k-espacio vectorial de dimensión finita.

Una sucesión de A-módulos y A homomorfimos

$$\cdots \longrightarrow N_{i-1} \xrightarrow{f_i} N_i \xrightarrow{f_{i+1}} N_{i+1} \longrightarrow \cdots$$

se dice que es exacta en N_i si $\mathrm{Im}(f_i) = \ker(f_{i+1})$. La sucesión es exacta si es exacta en cada N_i. En particular:

$0 \longrightarrow N' \xrightarrow{h} N$ es exacta si y solamente si h es inyectiva.

$N \xrightarrow{\phi} N'' \longrightarrow 0$ es exacta si y solamente si ϕ es sobreyectiva.

$0 \longrightarrow N' \xrightarrow{h} N \xrightarrow{\phi} N'' \longrightarrow 0$ es exacta si y solamente si h es inyectiva y ϕ es sobreyectiva, ϕ induce un isomorfismo de $\mathrm{Coker}(h) = N/f(N')$ sobre N''.

Sean M, N A-módulos, el producto tensorial de M y N, denotado por $M \otimes_A N$, es generado como A-módulo por los productos $x \otimes y$. Si $(x_i)_{i\in I}$, $(y_j)_{j\in J}$ son generadores de M y N respectivamente, entonces los elementos $x_i \otimes y_j$ generan $M \otimes N$.

Sean M, N y P A-módulos, entonces tenemos los siguientes isomorfismos canónicos:

(i) $M \otimes N \cong N \otimes M$.

(ii) $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$.

(iii) $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$.

(iv) $A \otimes M \cong M$.

Sean A y B anillos, M un A-módulo, P un B-módulo y N un (A, B) bimódulo, entonces $M \otimes_A N$ es un B-módulo, $N \otimes_B P$ un A-módulo y se tiene:

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$$

Sean $f : M \to M'$, $g : N \to N'$ homomorfismos de A-módulos. Se define el homomorfismo de A-módulos $f \otimes g : M \otimes N \to M' \otimes N'$, tales que $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$, para $x \in M$, $y \in N$.

Sea $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$, una sucesión exacta de A-módulos y homomorfismos y sea N un A-módulo cualquiera. Entonces la sucesión: $M' \otimes N \xrightarrow{f\otimes 1} M \otimes N \xrightarrow{g\otimes 1} M'' \otimes N \longrightarrow 0$ es exacta.

En general no es cierto que, si $M' \longrightarrow M \longrightarrow M''$ es una sucesión exacta de A-

módulos y homomorfismos, la sucesión $M' \otimes N \longrightarrow M \otimes N \longrightarrow M'' \otimes N$ tensorizada con un A-módulo arbitrario N sea exacta.

Ejemplo: Si consideramos $A = \mathbb{Z}$ y tomamos la sucesión $0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$ donde $f(x) = 2x$, para todo $x \in \mathbb{Z}$ y si lo tensorizamos con $N = \mathbb{Z}/2\mathbb{Z}$, obtenemos la sucesión $0 \longrightarrow \mathbb{Z} \otimes N \xrightarrow{f\otimes 1} \mathbb{Z} \otimes N$, la cual no es exacta pues para cada $x \otimes y$ en $\mathbb{Z} \otimes N$ se tiene que $(f \otimes 1)(x \otimes y) = (f(x) \otimes 1(y)) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0$, obtenemos que $f \otimes 1$ es la aplicación nula, mientras que $\mathbb{Z} \otimes N \neq 0$.

Definición 1.3.1. Sea M un A-módulo, decimos que M es plano sobre A, si para toda sucesión exacta $\cdots \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow \cdots$ de A-módulos, la sucesión $\cdots \longrightarrow N' \otimes_A M \longrightarrow N \otimes_A M \longrightarrow N'' \otimes_A M \longrightarrow \cdots$ es también exacta.
M es fielmente plano si para toda sucesión exacta L, L es exacta si y solamante si $L \otimes_A M$ es exacta.

Proposición 1.3.2. Sea N un A-módulo, son equivalentes:

1. N es plano.
2. Si $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ es una sucesión exacta de A módulos, la sucesión tensorizada
   $0 \longrightarrow M' \otimes N \longrightarrow M \otimes N \longrightarrow M'' \otimes N \longrightarrow 0$ es exacta.
3. Si $f : M' \to M$ es inyectiva y M, M' son de generación finita, entonces $f \otimes 1 : M' \otimes N \to M \otimes N$ es inyectiva.

La demostración puede ser vista en [1], Proposición 2.19. $\square$

Sea $f : A \to B$ homomorfismo de anillos. Si $a \in A$ y $b \in B$, definimos el producto $a \cdot b := f(a)b$, esta definición convierte al anillo B en un A-módulo, de esta manera B tiene la estructura de A-módulo y la de anillo. El anillo B, con la estructura de A-módulo, se llama A-álgebra. De esta manera una A-álgebra es un anillo B junto con un homomorfismo de anillos $f : A \to B$.

Observación:

(i) Si A es un cuerpo k, B un anillo no nulo entonces f es inyectivo, luego k se identifica canónicamente con su imagen en B. Así un k-álgebra (k cuerpo) es un anillo conteniendo a k como subanillo.

(ii) Sea A un anillo con elemento identidad, existe un único homomorfismo de anillos de los enteros $\mathbb{Z}$ en A que es $n \mapsto n \cdot 1$, de esta forma cada anillo es un $\mathbb{Z}$-álgebra.

1.4. Anillo de fracciones y localización

La forma de construcción de $\mathbb{Q}$ a partir de los enteros $\mathbb{Z}$ se aplica a un dominio de integridad D y origina el cuerpo de fracciones de D. El proceso de construcción del anillo de fracciones y el de localización son las técnicas más utilizadas del álgebra conmutativa.

Sea D un dominio de integridad

$$K = \frac{D \times D - \{0\}}{\sim} = \left\{ \frac{a}{b} = [(a,b)] : a, b \in D, b \neq 0 \right\}$$

es el cuerpo de fracciones de D.

Sea A un anillo. Un subconjunto $S \subset A$ es multiplicativamente cerrado si:

i) $1 \in S$

ii) $\forall\ a, b \in S$, se tiene $ab \in S$

Ejemplos: Sea A un anillo:

1. $S = \{a \in A : a$ es unidad $\}$, S es multiplicativamente cerrado.
2. $S = \{a \in A : a$ no es divisor de cero $\}$ es multiplicativamente cerrado.

Sea $S \subset A$ multiplicativamente cerrado. Definimos una relación en $A \times S$; $(a,s) \cong (b,t) \Leftrightarrow \exists\ u \in S$ tal que $u(at - bs) = 0$, esta relación es reflexiva, simétrica y transitiva. La clase de equivalencia de (a,s) será denotado por $\frac{a}{s}$ y su conjunto cociente $S^{-1}A = A_S = \{\frac{a}{s} ; a \in A, s \in S\}$ es un anillo, luego $S^{-1}A$ es llamado anillo de fracciones de A por S.

Tenemos el morfismo natural $\begin{array}{rcl} f : A & \longrightarrow & S^{-1}A \\ a & \longrightarrow & \frac{a}{1} \end{array}$, que en general no es un monomorfismo.

En el homomorfismo $\begin{array}{rcl} f : A & \longrightarrow & S^{-1}A \\ a & \longrightarrow & \frac{a}{1} \end{array}$ se cumple:

i) $s \in S$, entonces $f(s)$ es unidad en $S^{-1}A$.

ii) $\ker(f) = \{a \in A : \exists\ s \in S, as = 0\}$

iii) Los elementos de $S^{-1}A$ son de la forma $f(a).f(s)^{-1}$, $a \in A$ y $s \in S$.

Observación:

1. I es un ideal primo en un anillo A y $S = A - I$ multiplicativamente cerrado, luego $A_I := S^{-1}A$ y $m = \{\frac{a}{s} : a \in I, s \in S\}$ es un ideal de A_I y si $\frac{b}{s} \not\subset m$, entonces $b \not\subset I$, esto es $b \in S$, luego $\frac{s}{b} \in S^{-1}A$ y $\frac{b}{s}.\frac{s}{b} = 1$, luego (A_I, m) es un anillo local.

   El método de pasar de A a A_I se llama localización en I.

2. $S^{-1}A$ es el anillo cero si y solamente si $0 \in S$.

La localización en un ideal primo I es un anillo local, cuyo ideal maximal es IA_I.

Ejemplo: Si $A = \mathbf{Z}$, $p = (p)$, p número primo; A_p es el conjunto de todos los números racionales m/n; tal que m es primo con p.

Observación: La localización de A en p, elimina todos los ideales primo excepto los contenidos en p, el cocientado de A por p, elimina todos los ideales primos excepto a los que contienen p.

1.5. Condiciones de cadena

Sea Σ un conjunto. Se dice que Σ es parcialmente ordenado por una relación $<$ si: $<$ es reflexiva, transitiva y es tal que si $x < y$ y $y < x$ entonces $x = y$.

Son equivalentes:

(i) Toda sucesión creciente $x_1 < x_2 < \cdots$ en Σ se estaciona, es decir existe un n tal que $x_n = x_{n+1} = x_{n+2} = \cdots$

(ii) Todo subconjunto no vacío de Σ tiene un elemento maximal.

Si Σ es el conjunto de submódulos de M, ordenado por la relación $\subseteq$, entonces la condición (*i*) de la proposición anterior se llama condición de cadena ascendente (c.c.a.) y (*ii*) condición maximal. Si M satisface estas dos condiciones equivalentes se denomina noetheriano.

Ejemplos:

1. Un grupo conmutativo finito (como $\mathbb{Z}$-módulo) satisface c.c.a.

2. El anillo de los enteros (como $\mathbb{Z}$-módulo) satisface c.c.a.

3. $k[x]$ (k cuerpo) satisface c.c.a.

4. $k[x_1, x_2, \ldots, x_n, \ldots]$ en un número infinito de indeterminadas x_n no satisface ninguna condición de cadena en los ideales; pues la sucesión $(x_1) \subset (x_1, x_2) \subset \cdots$ es creciente en sentido estricto.

En un A-módulo noetheriano M, los submódulos son de generación finita.

Proposición 1.5.1. Sea $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$ una sucesión exacta de A-módulos. Se tiene que N es noetheriano $\Leftrightarrow$ N' y N'' son noetherianos.

Demostración. Supongamos que N es noetheriano. Sea $N'_1 \subseteq N'_2 \subseteq N'_3 \subseteq \cdots$ una cadena ascendente de submódulos de N', luego se tiene $f(N'_1) \subseteq f(N'_2) \subseteq f(N'_3) \subseteq \cdots$ una cadena ascendente de submódulos de N, luego esta cadena se estaciona es decir, $\exists$ n tal que $f(N'_n) = f(N'_{n+1}) = \cdots$, entonces como f es sobreyectiva se tiene $N'_n = N'_{n+1} = \cdots$, entonces tenemos que $N'_1 \subseteq N'_2 \subseteq N'_3 \subseteq \cdots \subseteq N'_n = N'_{n+1}$ entonces N' es noetheriano. El proceso para demostrar que N'' es noetheriano es análogo utilizando la imagen inversa y aplicando que g es sobreyectiva.
Recíprocamente, sea $L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n \subseteq \cdots$ una cadena ascendente de submódulos de N, luego $(f^{-1}(L_n))_{n\geq 1}$ es una cadena ascendente en N' y $(g(L_n))_{n\geq 1}$ es una cadena ascendente en N'', luego para n suficientemente grande las dos cadenas se estacionan; y se deduce que (L_n) es estacional. □

Un anillo A es noetheriano si lo es como A-módulo, es decir si satisface la c.c.a. en ideales.

Ejemplo:

1. Todo cuerpo es noetheriano; también lo es el anillo $\mathbb{Z}/(n)$ ($n \neq 0$). El anillo $\mathbb{Z}$ es noetheriano.

2. Los DIP son noetherianos, pues cada ideal es de generación finita.

3. $k[x_1, x_2, \ldots, x_n, \ldots]$ no es noetheriano, pues tenemos la siguiente sucesión $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \cdots$ que no se estaciona.

Proposición 1.5.2. Sea A un anillo noetheriano, $\mathfrak{a}$ un ideal de A. Entonces $A/\mathfrak{a}$ es un anillo noetheriano.

Demostración. Sea $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ una sucesión exacta, entonces $A/\mathfrak{a}$ es noetheriano como A-módulo, luego también como $A/\mathfrak{a}$-módulo. □

Proposición 1.5.3. Si A es noetheriano y φ es un homomorfismo sobreyectivo de A en B. Entonces B es noetheriano.

Demostración. Sea $\varphi\colon A \to B$, luego por el Teorema Fundamental del Homomorfismo se tiene que $B \cong \frac{A}{\ker\varphi}$, luego de la siguiente sucesión exacta

$$0 \longrightarrow \ker\varphi \xrightarrow{i} A \xrightarrow{j} \frac{A}{\ker\varphi} \longrightarrow 0\,,$$

como A es noetheriano $A/\ker\varphi$ es noetheriano, entonces B es noetheriano. □

Teorema 1.5.4. Si A es un anillo noetheriano, entonces $A[x]$ es noetheriano.

Demostración. Supongamos que $A[x]$ no es noetheriano, entonces existe un ideal I de $A[x]$ que no es de generación finita.

Sea $f_1 \in I$ de grado mínimo en I.

Sea $f_2 \in I - (f_1)$ de grado mínimo en $I - (f_1)$.

.

Sea $f_{k+1} \in I - (f_1, \ldots, f_k)$ de grado mínimo en $I - (f_1, \ldots, f_k)$.

de acuerdo a la elección de los f_i tenemos que sus grados $n_i = \text{grad}(f_i)$ satisfacen que $n_1 \leq n_2 \leq \ldots$. Si a_i es el coeficiente principal de f_i, tenemos que $(a_1) \subset (a_1, a_2) \subset \cdots \subset (a_1, a_2, \ldots, a_k) \subset \cdots$ es una cadena en A que no es estable pero A es noetheriano, entonces $\exists\, k$ tal que $(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1})$ y tendríamos que $a_{k+1} = \sum_{i=1}^{k} r_i a_i$, $r_i \in A$, consideremos

$$g = f_{k+1} - \sum_{i=1}^{k} r_i x^{n_{k+1}-n_i} f_i \in I - (f_1, \ldots, f_k)$$

y $\text{grad}(g) < n_{k+1} = \text{grad}(f_{k+1})$ contradice la minimalidad de f_{k+1}, por lo tanto $A[x]$ es noetheriano. □

Si A es noetheriano, su anillo de fracciones es también noetheriano.

1.6. Teoría de la dimensión

Sea A un anillo, la máxima de las longitudes r, tomadas sobre las cadenas estrictamente decreciente $p_0 \supset p_1 \supset \cdots \supset p_r$ de ideales primos de A, es llamado la dimensión de Krull o simplemente dimensión de A y denotado como $\dim A$.

Sea p un ideal primo de A, la máxima de las longitudes, tomadas sobre todas las cadenas estrictamente decreciente de ideales primos $p = p_0 \supset p_1 \supset \cdots \supset p_r$ empezando de p, es llamado altura de p y denotado htp. La máxima de las longitudes, tomadas sobre todas las cadenas estrictamente creciente de ideales primos $p = p_0 \subset p_1 \subset \cdots \subset p_r$ empezando de p, es llamado la coaltura de p y denotado por $cohtp$.

De las definiciones tenemos:

$$htp = \dim A_p \quad ; \quad cohtp = \dim A/p \quad \textbf{y} \quad htp + cohtp \leq \dim A.$$

Ejemplo:

i) $\dim \mathbf{Z} = 1$, pues $(0) \subset (p)$; p primo.

ii) Si K es cuerpo $\dim K = 0$.

Si A es un anillo local, noetheriano, $\dim(A) < \infty$.

Sea A un subanillo de B, tal que 1 pertenece a A. Un elemento x que pertenece a B se dice que es entero sobre A si x es raíz de un polinomio mónico con coeficientes en A, es decir $x^n + a_1x^{n-1} + \cdots + a_n = 0$.

Sea C el subconjunto de elementos de B que son enteros sobre A. Si C es igual a A, se dice que A es integralmente cerrado en B y si C es igual a B, se dice que B es entero sobre A.

El teorema de Descenso dice, sean $A \subseteq B$ dominios de integridad, A integramente cerrado, B entero sobre A. Sean $p_1 \supseteq \cdots \supseteq p_n$ una cadena de ideales primos de A y $q_1 \supseteq \cdots \supseteq q_m$ $(m < n)$ una cadena de ideales primos de B tal que $q_i \cap A = p_i$ $(1 \leq i \leq m)$. Entonces la cadena $q_1 \supseteq \cdots \supseteq q_m$ puede extenderse a una cadena $q_1 \supseteq \cdots \supseteq q_n$ tal que $q_i \cap A = p_i$ $(1 \leq i \leq n)$.

El teorema de Descenso Plano dice, sea B un A-álgebra plana. Dada una inclusión de ideales primos $p \subset q$ de A y b un ideal de B sobre q, existe b' ideal primo de B tal que $b' \subset b$ y b' está sobre p.

Definición 1.6.1. Sea $\phi : A \to B$ un homomorfismo de anillos. Sea p ideal primo de A, escribiremos $k(p) = A_p/pA_p$, entonces $\mathrm{Spec}(B \otimes k(p))$ es llamada la fibra de ϕ sobre p. El anillo $B \otimes k(p)$ será llamado el anillo fibra sobre p. Cuando (A, m) es un anillo local, m es el único punto cerrado del $\mathrm{Spec}(A)$ y así el espectro de $B \otimes k(m) = B/mB$ es llamado la fibra cerrada de ϕ. Si A es dominio y K su cuerpo de fracciones entonces el espectro de $B \otimes_A K = B \otimes_A k(0)$ es llamado la fibra genérica de ϕ.

Teorema 1.6.2. Sea $\phi : A \to B$ un homomorfismo de anillos noetherianos y sea P un ideal primo de B entonces escribiendo $p = A \cap P$ tenemos:

(i) $\mathrm{ht}P \leq \mathrm{ht}p + \dim B_P/pB_P$.

(ii) Si ϕ es plano, o más generalmente si el teorema de Descenso se mantiene entre A y B entonces se tiene la igualdad en (i).

La demostración puede ser vista en [2], teorema 15.1.

Proposición 1.6.3. Si A es un anillo noetheriano entonces $\dim A[x_1, \ldots, x_n] = \dim A + n$.

Demostración. La prueba lo haremos por inducción sobre el número de indeterminadas. Si $n = 1$, probaremos que $\dim A[x] = \dim A + 1$.
Sea $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_t$ una cadena ascendente de ideales primos de A, cuya longitud es t, entonces $P_0[x] \subsetneq P_1[x] \subsetneq \cdots \subsetneq P_t[x] \subsetneq P_t + (x)$, es una cadena de ideales primos de $A[x]$, el ideal $P_t + (x)$ es un ideal primo de $A[x]$, pues es el núcleo del homomorfismo $A[x] \to \frac{A}{P_t}$, luego la cadena $P_0[x] \subsetneq P_1[x] \subsetneq \cdots \subsetneq P_t[x] \subsetneq P_t + (x)$, tiene longitud $t+1$, así tenemos que $\dim A[x] \geq \dim A + 1$.
Ahora veamos que $\dim A[x] \leq \dim A + 1$. Sea q un ideal maximal de $A[x]$ tal que $\dim A[x] = \dim A[x]_q$ y sea $p = q \cap A$ ideal primo de A. Como $A[x]$ es plano sobre A, tenemos que $A[x]_q$ es plano sobre A_p, luego tenemos:

$$\begin{aligned} \dim A[x] = \dim A[x]_q &= \dim A_p + \dim A[x]_q \otimes_A k(p) \\ &= \dim A_p + \dim k(p)[x]_q \leq \dim A + 1 \end{aligned}$$

entonces $\dim A[x] \leq \dim A + 1$. Por lo tanto $\dim A[x] = \dim A + 1$.

Supongamos que el teorema es válido para $(n-1)$ es decir, que A es noetheriano, se tiene que $\dim A[x_1, \ldots, x_{n-1}] = \dim A + (n-1)$. Ahora veamos para n. Desde que A es noetheriano y desde que $A[x_1, \ldots, x_n] = (A[x_1, \ldots, x_{n-1}])[x_n]$, se tiene que: $\dim A[x_1, \ldots, x_{n-1}, x_n] = \dim(A[x_1, \ldots, x_{n-1}])[x_n] = \dim A[x_1, \ldots, x_{n-1}] + 1 = \dim A + (n-1) + 1 = \dim A + n$. □

Observe que si k es cuerpo, entonces $\dim k[x_1, \ldots, x_n] = n$.

Definición 1.6.4. Sea A un anillo y M un A-módulo. Un ideal primo p de A es llamado un ideal primo asociado de M si p es el anulador $\mathrm{ann}(x) = \{a \in A \,/\, ax = 0\}$ para algún $x \in M$. El conjunto de ideales primos asociados de M se denota como $\mathrm{Ass}(M)$ o $\mathrm{Ass}_A(M)$. Para I un ideal de A, los primos asociados del A-módulo A/I son referidos como los divisores primos de I.

Proposición 1.6.5. Sea A un anillo, J, $P_1, \ldots, P_s$ ideales de A y supongamos que $P_3, P_4, \ldots, P_s$ son primos y J no está contenido en ningún P_i, entonces existe un elemento $x \in J$ no contenido en ninguno de los P_i.

La demostración puede ser vista en [2].

Teorema 1.6.6. Sea A un anillo noetheriano, $I = (a_1, \ldots, a_r)$ un ideal generado por r elementos, si p es un divisor primo minimal de I se tiene que $\mathrm{ht}p \leq r$.
La demostración puede ser vista en [2], Teorema 13.5. Q

Teorema 1.6.7. Sea p un ideal primo de longitud r en un anillo noetheriano A. Entonces:

i) p es un divisor primo minimal de algún ideal $(a_1, \ldots, a_r)$ generado por r elementos.

ii) Si $a_1, \ldots, a_r$ son como en (i) tenemos $\mathrm{ht}p/(a_1, \ldots, a_i) = r - i$, para $1 \leq i \leq r$.

Demostración. (i). La demostración puede ser vista en [2], teorema 13.6.
(ii). Sea $\bar{A} = A/(a_1, \ldots, a_r)$, el ideal $p/(a_1, \ldots, a_i)$ es un divisor primo minimal de $(\bar{a}_{i+1}, \ldots, \bar{a}_r)$ en $A/(a_1, \ldots, a_i)$, luego por el Teorema (1.6.6) tenemos que $\mathrm{ht}p/(a_1, \ldots, a_i) \leq r - i$. □

Definición 1.6.8. Sea (A, m) un anillo local, noetheriano de dimensión d. Si $x_1, x_2, \ldots, x_d$ generan un ideal m-primario, se denomina sistema de parámetros de A.

La existencia del sistema de parámetros está garantizado por el teorema 13.4 de [2].

Definición 1.6.9. Sean (A, m) un anillo local noetheriano r-dimensional y $k = A/m$ su cuerpo residual. El número más pequeño de elementos necesarios para generar m es igual al $\text{ran}_k m/m^2$; (esto es la dimensión de m/m^2 como k-espacio vectorial), este número es llamado la dimensión encajada de A y escribimos **emb** dim$A$. En general

$$\dim A \leq \textbf{emb} \dim A,$$

la igualdad se presenta cuando m es generado por r elementos, de ser así A es llamado anillo local regular y el sistema de parámetros que genera m es llamado sistema regular de parámetros.

Teorema 1.6.10. Sea (A, m) un anillo local noetheriano y $x_1, x_2, \dots, x_r$ un sistema de parámetros, entonces $\dim A/(x_1, \dots, x_i) = r - i$ para $1 \leq i \leq r$.

Demostración. Por el teorema (1.6.7)(ii) se tiene que $\text{ht}\dfrac{m}{(x_1, \dots, x_i)} = (r - i)$ y desde que $\dim A = \text{ht} m$ tenemos que $\text{ht}\dfrac{m}{(x_1, \dots, x_i)} = \dim\dfrac{A}{(x_1, \dots, x_i)} = r - i$. □

Teorema 1.6.11. Sea (R, m) un anillo local regular n-dimensional y $x_1, \dots, x_i$ elementos de m. Los siguientes ítems son equivalentes:

(i) $x_1, \dots, x_i$ es un subconjunto de un sistema de parámetros de R.

(ii) Las imágenes en m/m^2 de $x_1, \dots, x_i$ son linealmente independientes sobre R/m.

(iii) $R/(x_1, \dots, x_i)$ es un anillo local regular $(n - i)$-dimensional.

Demostración. *(i)⇒(ii).* Como $\{x_1, \dots, x_i\}$ es un subconjunto de un sistema regular de parámetros de R, entonces $\{x_1, \dots, x_i, x_{i+1}, \dots, x_n\}$ es un sistema regular de parámetros de R, entonces sus imágenes generan el R/m-espacio vectorial m/m^2 y desde que $\textbf{ran}_k m/m^2 = n$, entonces estas imágenes son l.i., luego se tiene que las imágenes de $x_1, \dots, x_i$ son linealmente independientes sobre R/m.

(i)⇒(iii). Por el Teorema (1.6.10) sabemos que $R/(x_1, \dots, x_i)$ es $(n - i)$ dimensional, luego las imágenes de $\{x_{i+1}, \dots, x_n\}$ general el ideal maximal de $R/(x_1, \dots, x_i)$, entonces $R/(x_1, \dots, x_i)$ es un anillo local regular $(n - i)$ dimensional.

(iii)⇒(i). Como $R/(x_1, \dots, x_i)$ es un anillo local regular $(n - i)$ dimensional, luego $m/(x_1, \dots, x_i)$ ideal maximal de $R/(x_1, \dots, x_i)$ es generado por las imágenes

de $y_1, \dots, y_{n-i} \in m$, entonces m es generado por $\{x_1, \dots, x_i, y_1, \dots, y_{n-i}\}$ luego $\{x_1, \dots, x_i\}$ es subconjunto de un sistema regular de parámetros.

(ii)⇒(i). Como $\mathbf{ran}_k m/m^2 = n$ y si tomamos $x_{i+1}, \dots, x_n$ tales que las imágenes de $x_1, x_2, \dots, x_i, x_{i+1}, \dots, x_n$ son una base para m/m^2, entonces $x_1, \dots, x_n$ generan m y así $x_1, \dots, x_n$ forman un sistema regular de parámetros de R, luego $x_1, \dots, x_i$ es un subconjunto de un sistema regular de parámetros de R. □

Teorema 1.6.12. Un anillo local regular es un dominio de integridad.

Demostración. Sea (A, m) un anillo local regular n-dimensional, la prueba la realizaremos por inducción sobre la dimensión. Si $n = 0$ entonces su ideal maximal m es generado por cero elementos, es decir $m = (0)$, de esta manera se tiene que A es un cuerpo y por lo tanto A es un dominio de integridad. Cuando $n = 1$, el ideal maximal tiene un solo generador $m = (x)$ y $htm = 1$, entonces existe un ideal primo $p \neq m$ con $m \supset p$. Si $y \in p$ entonces $y = xa$, $a \in A$ y desde que $x \not\in p$ se tiene que $a \in p$, luego $p = (x)$ y por el Lema de Nakayama tenemos que $p = (0)$, entonces A es un dominio. Cuando $n > 1$. Sean $p_1, p_2, \dots, p_r$ los ideales primos minimales de A, luego desde que $m \not\subset m^2$ y $m \not\subset p_i$ para todo i, entonces existe un elemento $x \in m$ que no está en m^2 ni $p_1, p_2, \dots, p_r$, ver Proposición (1.6.5), luego la imagen de x en m/m^2 es no nulo, luego $A/(x)$ es un anillo local regular $(n-1)$ dimensional, luego por hipótesis inductiva tenemos que $A/(x)$ es un dominio de integridad, luego (x) es un ideal primo de A. Si p_1 es uno de los ideales primos contenidos en (x) y desde que $x \not\in p_1$ y aplicando el mismo argumento que para $n = 1$, mostraremos que $p_1 = xp_1$ y por lo tanto $p_1 = 0$, entonces A es dominio. □

1.7. Valoración discreta

Un dominio de integridad R es un anillo de valoración si para todo elemento x de su cuerpo de fracciones k satisface $x \not\in R$ entonces $x^{-1} \in R$.

Proposición 1.7.1. Sea R un anillo de valoración de k (el cuerpo de fracciones de R) entonces R es un anillo local.

Demostración. Sea m el conjunto de elementos de R que no son unidades, entonces tenemos $x \in m$ si y solamente si $x = 0$ ó $x^{-1} \not\in R$. Ahora veamos que m es un ideal. Sea $a \in R$, $x \in m$, luego tenemos que $ax \in m$, pues de no ser así tendríamos que $(ax)^{-1} \in R$, luego $x^{-1} = a(ax)^{-1} \in R$ y esto será una contradicción, por lo tanto

$ax \in m$. Ahora dado $x, y \in m$, con x, y no nulos se tiene entonces que $xy^{-1} \in k$, luego como R es un anillo de valoración de k tenemos que $xy^{-1} \in R \vee x^{-1}y \in R$, luego en cualquiera de los casos tenemos $(x + y) = (xy^{-1} + 1)y \in Rm \subseteq m$, luego $(x+y) \in m$ y por lo tanto tenemos que m es un ideal y está formado por elementos no nulos que no son unidades, por lo tanto se tiene que (R, m) es un anillo local. $\square$

Un anillo de valoración cuyo grupo de valores es isomorfo a $\mathbf{Z}$ es llamado anillo de valoración discreta. Se le dice discreto por el hecho de que el grupo de valores es un subgrupo discreto de $\mathbf{R}$ y no tiene nada que ver con que la topología m-adica del anillo local sea discreta.

Teorema 1.7.2. Sea R un anillo, entonces las siguientes condiciones son equivalentes:

(i) R es un anillo de valoración discreta.

(ii) R es un dominio de ideales principal local y no es cuerpo.

(iii) R es un anillo local, noetheriano, $\dim R > 0$ y cuyo ideal maximal m_R es principal.

(iv) R es un anillo local, noetheriano uno dimensional.

La demostración puede ser vista en [2].

1.8. Anillos regulares

Un anillo regular es un anillo noetheriano tal que la localización en todo maximal es un anillo local regular.
Nota: Por el teorema de Serre [4], Teorema 19.3, podemos cambiar en esta definición los ideales maximales por ideales primos.

Teorema 1.8.1. Si A es un anillo regular entonces $A[x]$ es un anillo regular.

Demostración. Sea P un ideal maximal de $A[x]$ y consideremos $m = P \cap A$. Luego $A[x]_P$ es una localización de $A_m[x]$, así al reemplazar A por A_m, podemos considerar que A es un anillo local regular y escribiendo $A/m = K$ tenemos que $\frac{A[x]}{m[x]} = \frac{A}{m}[x] = K[x]$, así existe un polinomio mónico $f(x)$ con coeficientes en A tales que $P = (m, f(x))$ y f se reduce a un polinomio irreducible $\bar{f} \in K[x]$ módulo m, luego como $A[x]$ es un A-álgebra plano, por el Teorema (1.6.2) parte (ii), tenemos

$$\dim A[x]_P = \mathrm{ht}P = 1 + \mathrm{ht}m = 1 + \dim A,$$

entonces m es generado por $\dim A$ elementos y $P = (m, f)$ es generado por $\dim A + 1$ elementos, por lo tanto $A[x]_P$ es generado por $\dim A + 1$ elementos, entonces $A[x]$ es un anillo regular. □

Definición 1.8.2. Una resolución libre finita de un A-módulo M es una sucesión exacta $0 \to F_n \to \cdots \to F_1 \to F_0 \to M \to 0$ tal que cada F_i es un módulo libre finito y decimos que M es libremente estable si existen módulos libres finitos F y F' tal que $M \oplus F \cong F'$.

Teorema 1.8.3. Un dominio de integridad noetheriano A es un DFU si y solamente si todo ideal primo de longitud 1 es principal.

Demostración. Supongamos que A es un DFU y sea p un ideal primo de longitud 1. Sea $a \in p$ no nulo, desde que A es DFU, a se puede expresar como un producto de elementos primos, es decir $a = \prod p_i$, luego desde que p es primo algún p_i pertenece a p, entonces $(p_i) \subset p$, como p_i es un elemento primo, se tiene que (p_i) es un ideal primo, desde que $\mathrm{ht}p = 1$ y A es dominio tenemos que $p = (p_i)$, por lo tanto p es principal.
Recíprocamente, supongamos que todo ideal primo de longitud 1 es principal. Desde que A es noetheriano, todo elemento $a \in A$ que no es unidad ni cero se escribe como producto finito de irreducibles entonces para probar que A es DFU será suficiente ver que todo elemento irreducible es primo. Sea p el divisor primo minimal de (a), entonces por el teorema del ideal principal se tiene que $\mathrm{ht}p = 1$ luego por hipótesis inductiva se tiene que p es principal es decir $p = (r)$, luego como p es un divisor primo de (a) se tiene que $a = r.b$ y desde que a es irreducible b es unidad, luego $(a) = (r) = p$ entonces a es un elemento primo, por lo tanto A es un DFU. □

Teorema 1.8.4. Sea A un dominio noetheriano, Γ es un conjunto de elementos primos de A y sea S un conjunto multiplicativo generado por Γ. Si A_S es un D.F.U. entonces A es un D.F.U.

Demostración. Sea p un ideal primo de longitud 1. Si $p \cap S \neq \emptyset$ entonces p contiene un elemento $\pi \in \Gamma$ y desde (π) es un ideal primo no nulo tenemos que $p = (\pi)$. Si $p \cap S = \emptyset$ entonces pA_S es un ideal primo de longitud 1 de A_S, así tenemos que $pA_S = aA_S$, para algún $a \in p$ y entre todos los a elegimos uno tal que (a) sea maximal, entonces a no es divisible por $\pi \in \Gamma$. Ahora si $x \in p$ tenemos $sx = ay$ para algún $s \in S$, $y \in A$. Sea $s = \pi_1\pi_2 \cdots \pi_r$ con $\pi_i \in \Gamma$, entonces $a \notin (\pi_i)$ así $y \in (\pi_i)$ y por inducción sobre Γ se muestra $y \in (s)$ así $x \in (a)$, entonces $p = (a)$, luego A es D.I.P. y por lo tanto A es D.F.U. □

Lema 1.8.5. Sea A un dominio y $\mathfrak{a}$ un ideal de A tal que $\mathfrak{a} \oplus A^n \cong A^{n+1}$, entonces $\mathfrak{a}$ es principal.

La demostración puede ser vista en [2].

Teorema 1.8.6. Un anillo local regular es un DFU.

Demostración. Sea (A, m) un anillo local regular, la demostración lo realizaremos por inducción sobre su dimensión.
Si $\dim A = 0$. Como A es un anillo local regular, por el Teorema (1.6.12) A es un dominio de integridad, además como $\dim A = 0$ entonces A es un cuerpo, luego A es un D.F.U.
Si $\dim A = 1$. A es un anillo local regular entonces A es un anillo local noetheriano y como $\dim A = 1$, entonces m es principal, luego A es un Dominio de Valoración Discreta y por lo tanto A es un D.F.U.
Si $\dim A > 1$. Sea $x \in m - m^2$, luego (x) es un ideal primo de A, desde que $1 \not\in (x)$ y si para todo $ab \in (x)$ se tiene que $a \in (x)$ o $b \in (x)$. Aplicaremos el Teorema (1.8.4) a $\Gamma = \{x\}$, solamente necesitamos demostrar que A_x es un D.F.U. Sea P un ideal primo de A_x de altura uno y sea $p = P \cap A$, luego $P = pA_x$ y, desde que A es un anillo local regular, p como A-módulo tiene una resolución libre finita, de esta manera el A_x-módulo P tiene una resolución libre. Para algún ideal primo Q de A_x, el anillo $(A_x)_Q = A_{Q \cap A}$ es un anillo local regular de menor dimensión que la de A, así por inducción es un D.F.U., de esta manera P_Q es libre como $(A_x)_Q$-módulo, así P como A_x-módulo es proyectivo, luego P es establemente libre y por el Lema (1.8.5) P es un ideal principal de A_x, luego A_x es un D.F.U. $\square$

Capítulo 2

Series de potencia formales

Una serie de potencia formal puede ser pensado como un polinomio, pero con un número infinito de términos y lo podemos ver como una serie de potencia en la que ignoramos cuestiones de convergencia. En este capítulo veremos que el anillo de series formales de potencia es un anillo local, noetheriano, regular y lo dotaremos de una métrica para ver su completitud.

2.1. Anillos de series de potencia formales

Sea K un cuerpo y $x_1, \ldots, x_r$ indeterminadas sobre K. Denotemos por

$$R = K[[x_1, \ldots, x_r]]$$

el conjunto de todas las sumas formales del tipo

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

donde cada P_i es un polinomio homogéneo de grado i en las indeterminadas $x_1, x_2, \ldots, x_r$, con coeficientes en K, consideraremos el polinomio cero como un polinomio homogéneo de cualquier grado. Los elementos de R serán llamados series de potencias formales en las indeterminadas $x_1, \ldots, x_r$ con coeficientes en K.

Sean $f = P_0 + P_1 + \ldots$ y $g = Q_o + Q_1 + \ldots$ elementos de R. Por definición tenemos

$$f = g \Leftrightarrow P_i = Q_i \quad \forall \ i \in \mathbb{N}.$$

Definimos la suma y el producto en R.

$$f + g = \sum_{i=0}^{\infty} (P_i + Q_i) \qquad \textbf{y} \qquad fg = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} P_j Q_{i-j}$$

Entonces R con estas operaciones es un anillo conmutativo, con unidad y se le denomina el anillo de las series formales de potencia en r indeterminadas con coeficientes en K. Observe que podemos cambiar en el anillo de la series de potencias formales el cuerpo K por un anillo conmutativo y con identidad.

K y $K[x_1, \dots, x_r]$ son subanillos de R. Los elementos de R pueden ser representados más explícitamente en la forma

$$f = \sum_{i=0}^{\infty} \sum_{i_1+i_2+\cdots+i_r=i} a_{i_1\dots i_r} x_1^{i_1} x_2^{i_2} \dots x_r^{i_r} \quad ; \quad a_{i_1\dots i_r} \in K$$

Si $K = \mathbf{R} \vee K = \mathbf{C}$, podemos considerar el subanillo $A = K\{x_1, \dots, x_r\}$ de R constituido por las series de potencia absolutamente convergente en las vecindades del origen $(0, \dots, 0)$. Es decir, los elementos de A son las series

$$f = \sum_{i=0}^{\infty} \sum_{i_1+i_2+\cdots+i_r=i} a_{i_1\dots i_r} x_1^{i_1} x_2^{i_2} \dots x_r^{i_r}$$

para el cual existe un número real positivo p (dependiendo de f) tal que la serie

$$\sum_{i=0}^{\infty} \sum_{i_1+i_2+\cdots+i_r=i} |a_{i_1\dots i_r}| p^{i_1+\cdots+i_r}$$

es convergente.

Proposición 2.1.1. Sea A un anillo y $A[[x]]$ el anillo de las series de potencias formales $f = \sum_{n=0}^{\infty} a_n x^n$ con coeficientes en A. Entonces $f \in A[[x]]$ es unidad si y solamente si a_0 es unidad en A.

Demostración. Como $f \in A[[x]]$ es unidad, existe $g \in A[[x]]$ tales que $f \cdot g = 1$ entonces tenemos $(a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots)(b_0+b_1x+b_2x^2+\cdots+b_nx^n+\cdots) = 1$ $\Rightarrow a_0b_0 + (a_1b_0 + a_0b_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots = 1$ entonces se tiene:

$$a_0b_0 = 1; \quad a_0b_1 + a_1b_0 = 0; \quad a_0b_2 + a_1b_1 + a_2b_0 = 0; \quad \cdots$$

luego desde que $a_0b_0 = 1$, entonces a_0 es unidad en A.

Reciprocamente, sea $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots \in A[[x]]$, donde a_0 es unidad, tenemos que formar $g = b_0 + b_1x + b_2x^2 + \cdots + n_nx^n + \cdots \in A[[x]]$ tal que $f \cdot g = 1$.

Como a_0 es unidad existe $b_0 \in A$ tal que $a_0b_0 = 1$, entonces $b_0 = a_0^{-1}$

$$b_1 = -a_1b_0a_0^{-1}, \quad b_2 = (-a_1b_1 - a_2b_0)a_0^{-1}, \quad \cdots$$

tales que formamos $g = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n + \cdots$ donde

$$
\begin{aligned}
f \cdot g &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots)(b_0 + b_1x + b_2x^2 + \cdots + b_nx^n + \cdots) \\
&= a_0b_0 + (a_1b_0 + a_0b_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots \\
&= 1 + a_0(-a_1b_0a_0^{-1} + a_1b_0)x + (a_0(-a_1b_1 - a_2b_0)a_0^{-1} + a_1b_1 + a_2b_0)x^2 + \cdots \\
&= 1 + 0x + 0x^2 + 0x^3 + \cdots \\
&= 1
\end{aligned}
$$

por lo tanto f es unidad. □

Corolario 2.1.2. El elemento $f = \sum_{i=0}^{\infty} P_i$ en $R = K[[x_1, \ldots, x_r]]$ es invertible si y solamente si $P_0 \neq 0$.

Demostración. Solo hay que recordar que todo elemento no nulo en un cuerpo tiene inversa. □

Definición 2.1.3. Sea $f \in R\backslash\{0\}$. Supóngase que $f = P_n + P_{n+1} + \cdots$, donde P_j es un polinomio homogéneo de grado j y $P_n \neq 0$. El polinomio homogéneo P_n es llamado la forma inicial de f. El entero n es llamado la multiplicidad de f y es denotado por $\textbf{mult}(f)$. Si $f = 0$, escribiremos $\textbf{mult}(f) = \infty$.

Notemos que $f \in R$ es invertible si y solamente si $\textbf{mult}(f) = 0$. En la multiplicidad de las series de potencia se cumple, dado $f, g \in R$ tenemos:

i) $\textbf{mult}(f.g) = \textbf{mult}(f) + \textbf{mult}(g)$.

ii) $\textbf{mult}(f + g) \geq \min\{\textbf{mult}(f), \textbf{mult}(g)\}$.

Proposición 2.1.4. El anillo de series de potencia formales $K[[x_1, \ldots, x_r]]$ es dominio de integridad.

Demostración. El anillo de series de potencia formales $K[[x_1, \ldots, x_r]]$, donde K es un cuerpo, claramente posee elemento identidad y es conmutativo, nos faltaría ver que no tenga divisores de cero.

Sea $f, g \in R\backslash\{0\}$, luego $\textbf{mult}(f.g) = \textbf{mult}(f) + \textbf{mult}(g) < \infty$ entonces $f.g \neq 0$, luego R no tiene divisores de cero y por lo tanto $R = K[[x_1, \ldots, x_r]]$ es dominio de integridad. □

1. Denotaremos $M_R = (x_1, \ldots, x_r)$ el ideal de R generado por $x_1, x_2, \ldots, x_r$.

2. Denotaremos por M_R^i la i-ésima potencia de ideal M_R y escribiremos $M_R^0 = R$.

Proposición 2.1.5. El anillo de series de potencia formales (R, M_R) es un anillo local.

Demostración. Como el ideal $(x_1, x_2, \dots, x_r) \subset K[[x_1, \dots, x_r]]$ es el conjunto de las no unidades de $K[[x_1, \dots, x_r]]$, luego se tiene que $K[[x_1, \dots, x_r]]$ es un anillo local con $M_R = (x_1, \dots, x_r)$ como ideal maximal. □

Proposición 2.1.6. Si A es un anillo noetheriano entonces $A[[x]]$ es noetheriano.

Demostración. Sea I un ideal de $A[[x]]$, probaremos que I es un ideal de generación finita. Consideremos $I(r)$ al ideal de A formado por los coeficientes principales a_r de $f = a_r x^r + a_{r+1}x^{r+1} + \cdots \in A[[x]]$, como $f \in I \cap (x^r)$, tenemos que $I(0) \subset I(1) \subset I(2) \subset \cdots$. Como A es noetheriano existe un s tal que $I(s) = I(s+1) = \cdots$, además cada $I(i)$ es finitamente generado. Para cada i con $0 \leq i \leq s$ tomamos finitos elementos $a_{i,1}, \dots a_{i,l_i}$ que pertenecen a A y generan $I(i)$. Sean $g_{ij} \in I \cap (x^i)$ tal que a_{ij} sea su coeficiente de x^i, veamos que estos g_{ij} generan I. En efecto, para $f \in I$ podemos tomar una combinación lineal g_0 de los g_{0j} con coeficiente en A tal que $f - g_0 \in I \cap (x)$, entonces tomando una combinación lineal g_1 de los g_{1j} con coeficientes en A tal que $f - g_0 - g_1 \in I \cap (x^2)$, procediendo de la misma manera obtenemos

$$f - g_0 - g_1 - \cdots - g_s \in I \cap (x^{s+1}).$$

Sea a_{s+1} el coeficiente de x^{s+1} de esta última expresión, desde que $I(s+1) = I(s)$ tenemos $a_{s+1} = a_{s1}b_{s+1,1} + \cdots + a_{s,l_s}b_{s+1,l_s}$. Asi podemos tomar una combinación lineal $g_{s+1} = xg_{s1}b_{s+1,1} + \cdots + xg_{s,l_s}b_{s+1,l_s}$ de los xg_{sj} con coeficientes en A tal que $f - g_0 - g_1 - \cdots - g_{s+1} \in I \cap (x^{s+2})$. Por el mismo camino conseguimos $g_{s+2}, g_{s+3}, \dots$ tal que

$$f - g_0 - g_1 - \cdots - g_n \in I \cap (x^{n+1}) \text{ para todo } n. \tag{1}$$

Para $i \leq s$, cada g_i es combinación lineal de los g_{ij} cuyos coeficientes están en A y para $i > s$ tomamos una combinación de los elementos $x^{i-s}g_{sj}$. Para cada $i > s$ escribimos $g_i = \sum_{j=1}^{l_s} b_{ij}x^{i-s}g_{sj}$ y luego para cada j conseguimos $h_j = \sum_{i=s}^{\infty} b_{ij}x^{i-s}$ elemento de $A[[x]]$ y de (1) tenemos $f = g_0 + g_1 + \cdots + g_s + \sum_{j=1}^{l_s} h_j g_{sj}$. Por lo tanto $A[[x]]$ es un anillo noetheriano. □

Desde que el anillo de series formales de potencia en varias variables $A[[x_1, \dots, x_r]]$ puede ser visto como $(A[[x_1, \dots, x_{r-1}]])[[x_r]]$, luego utilizando el resultado: si A es noetheriano, entonces $A[[x]]$ es noetheriano, concluimos que $A[[x_1, \dots, x_r]]$ es noetheriano.

Proposición 2.1.7. Si A es un anillo noetheriano entonces $\dim A[x_1,\ldots,x_n] = \dim A + n$.

Demostración. La demostración la haremos por inducción sobre n.
Para $n = 1$, probaremos que si A es noetheriano, $\dim A[x] = \dim A + 1$. Si consideremos m como ideal maximal de A, se tiene que $A[x] \otimes k(m) = A[x] \otimes (A_m/mA_m) = A[x] \otimes A/m = A/m[x]$, luego $(A/m)[x]$, esto es uno dimensional y como todo ideal maximal M de $A[x]$ es $M = (m, x)$, donde $m = M \cap A$ es el ideal maximal de A y como $A[x]$ es A-álgebra plana, aplicamos el teorema (1.6.2)(ii) se tiene que:

$$\operatorname{ht} M = \operatorname{ht} m + \dim \frac{A[x]_M}{mA[x]_M}$$

por el Teorema del Descenso, tenemos

$$\dim A[x] = \dim A + \dim A[x] \otimes k(m)$$
$$\dim A[x] = \dim A + \dim A[x]_M \otimes \frac{A_m}{mA_m}$$
$$\dim A[x] = \dim A + \dim A[x]_M \otimes \frac{A}{m}$$
$$\dim A[x] = \dim A + \dim \frac{A}{m}[x]_M$$
$$\dim A[x] = \dim A + \dim \frac{A}{m}[x]$$
$$\dim A[x] = \dim A + 1$$

Supongamos válido para $(n-1)$, entonces $\dim A[x_1,\ldots,x_{n-1}] = \dim A + (n-1)$.
Ahora probaremos para n. Utilizamos el criterio de que $A[x_1,\ldots,x_n] = (A[x_1,\ldots,x_{n-1}])[x_n]$ y lo demostrado para $n=1$:

$$\begin{aligned}\dim A[x_1,\ldots,x_n] &= \dim(A[x_1,\ldots,x_{n-1}])[x_n] \\ &\overset{\text{Por H.I.}}{=} \dim A[x_1,\ldots,x_{n-1}] + 1 \\ &= \dim A + (n-1) + 1 \\ &= \dim A + n\end{aligned}$$

□

Proposición 2.1.8. Si A es un anillo regular entonces $A[x]$ es un anillo regular.

La demostración puede ser vista en [2], teorema 19.5. Compare este resultado con la proposición 3.3.3.

2.2. Métrica en el anillo de series formales de potencia

Sea $K[[x_1, \ldots, x_r]]$ el anillo de las series formales de potencia y $M_R = (x_1, x_2, \ldots, x_r)$ su ideal maximal. Sea $A > 1$ un número real y consideremos la siguiente aplicación

$$\begin{aligned} d : R \times R &\longrightarrow \mathbf{R} \\ (f, g) &\longrightarrow d(f, g) = A^{-\mathbf{mult}(f-g)}. \end{aligned}$$

Veamos que d es una métrica sobre $R = K[[x_1, \ldots, x_r]]$.

1. $d(f, g) \geq 0$, se cumple por definición de la aplicación d.

2. $d(f, g) = 0$ si y solamente si $\mathbf{mult}(f - g) = \infty$, el cual es equivalente a $f = g$.

3. $d(f, g) = d(g, f)$, ya que $d(f, g) = A^{-\mathbf{mult}(f-g)} = A^{-\mathbf{mult}(g-f)} = d(g, f)$.

4. $d(f, g) \leq d(f, h) + d(h, g)$
   Consideremos la siguiente desigualdad

   $$\mathbf{mult}(f - g) = \mathbf{mult}((f - h) - (g - h)) \geq \text{mín}\{\mathbf{mult}(f - h), \mathbf{mult}(g - h)\} := m$$

   luego

   $$d(f, g) = A^{-\mathbf{mult}(f-g)} < A^{-m} \leq A^{-\mathbf{mult}(f-h)} + A^{-\mathbf{mult}(g-h)} \leq d(f, h) + d(h, g)$$

   por lo tanto $(K[[x_1, \ldots, x_r]], d)$ es un espacio métrico.

Proposición 2.2.1. El anillo de series de potencia formales $K[[x_1, \ldots, x_r]]$ es un espacio métrico completo.

Demostración. Sea $(f_n)_{n\in\mathbf{N}}$ una sucesión de Cauchy en $K[[x_1, \ldots, x_r]]$ entonces, para todo $n \in \mathbf{N}$, existe un entero $\mathsf{V}(n)$ tal que

$$d(f_l, f_m) < A^{-n}, \qquad \forall\ l, m \geq \mathsf{V}(n)$$

y esto implica que $f_l - f_m \in M_R^n$; $\forall\ l, m \geq \mathsf{V}(n)$.

Podemos elegir el $\mathsf{V}(n)$ de tal manera que podamos formar una sucesión creciente, así tenemos

$$f_{\mathsf{V}(n)} - f_{\mathsf{V}(n+1)} \in M_R^n \qquad \forall\ n \in \mathbf{N}$$

Ahora, para todo $i \in \mathbb{N}$, escribimos

$$f_{\varphi(i)} = P_{i,0} + P_{i,1} + \cdots$$

donde cada $P_{i,j}$ es un polinomio homogéneo de grado j y definimos

$$f = P_{1,0} + P_{2,1} + \cdots + P_{i+1,i} + \cdots$$

Verificamos que

$$f - f_{\varphi(i)} \in M_R^{i+1}, \qquad \forall\, i \in \mathbb{N}$$

que a su vez implica que

$$\lim_{n \to \infty} f_{\varphi(n)} = f$$

esto muestra que la sucesión de Cauchy (f_n) tiene una subsucesión $(f_{\varphi(n)})$ que converge al elemento $f \in R$, por lo tanto, la sucesión misma converge a f. $\square$

Por lo tanto tenenos que el anillo de series de potencia formales $K[[x_1, \ldots, x_r]]$ es un anillo local, completo, noetheriano, regular, entonces nos hacemos la siguiente pregunta:

¿Será que un anillo con estas características sea isomorfo al anillo de series de potencia formales?

Esto fue conjeturado por Krull, acerca de los anillos locales, completos, noetherianos y regulares. El objetivo del presente trabajo es responder a esta inquietud.

Capítulo 3

Topología lineal, completación y suavidad formal

En este capítulo veremos la completación $\mathfrak{a}$-ádica de un anillo local, la suavidad formal y la separabilidad de cuerpos, además la relación entre las características de un anillo local y su cuerpo residual y si estos coinciden, se dice que A es equicaracterítico entonces A contiene un cuerpo.

3.1. Topología lineal

Una filtración en un anillo A es una sucesión descendente de ideales tal que $A = J_0 \supseteq J_1 \supseteq \cdots$ y $J_m J_n \subseteq J_{m+n}$. Un anillo con una filtración es llamado *anillo filtrado*.

Sea A un anillo filtrado con una filtración $\{A_n\}_{n\geq 0}$. Una filtración sobre un A-módulo M es una sucesión $\{M_n\}_{n\geq 0}$ de submódulos de M tales que $M_0 = M$, $M_{n+1} \subseteq M_n$, $A_m M_n \subseteq M_{m+n}$ para todo m, n en este caso M es llamado un *A-módulo filtrado*.

Ejemplos:

1. Si A es cualquier anillo e $I \subseteq A$ es un ideal, la filtración I-ádica de A está dada por $\{I^n\}_{n\geq 0}$. Si M es un A-módulo, la filtración I-ádica de M está dada por $M_n = I^n M$, para $n \geq 0$.
2. Si A es cualquier anillo, siempre se tiene la filtración trivial dada por

$$I_n = \begin{cases} A; & \textbf{si } n = 0 \\ 0; & \textbf{si } n > 0 \end{cases}$$

Las filtraciones más comunes que encontraremos son las a-ádicas filtraciones correspondientes al ideal a de A, está dada por $\{a^n\}_{n\geq 0}$ y si M es un A-módulo, la filtración a-ádica de M está dada por $M_n = a^n M$, para $n \geq 0$.

Si M, N son módulos filtrados sobre un anillo filtrado A, un morfismo de módulos filtrado es un A-morfismo $f : M \to N$ que respeta las filtraciones, es decir $f(M_n) \subseteq N_n$ para todo $n \in \mathbf{Z}$.

Sea A un anillo filtrado con filtración $\{A_n\}_{n\geq 0}$ y sea M un A-módulo filtrado con filtración $\{M_n\}_{n\geq 0}$, se define la función orden $\mathsf{V} : M \to \mathbf{Z} \cup \{\infty\}$.

$$\mathsf{V}(x) = \begin{cases} n, & \text{si } x \in M_n, \text{ pero } x \notin M_{n+1} \\ \infty, & \text{si } x \in \bigcap M_n \end{cases}$$

Si $\bigcap M_n = 0$, entonces se tiene $\mathsf{V}(0) = \infty$.

Si A es un número real tal que $0 < A < 1$, definamos una aplicación

$$d : M \times M \longrightarrow \mathbf{R}$$

$$(x, y) \longrightarrow d(x, y) = A^{\mathsf{V}(x-y)}$$

Entonces:

- $d(x, x) = 0$, tenemos $\mathsf{V}(x - x) = \mathsf{V}(0) = \infty$, $A^{\infty} = 0$.
- $d(x, y) = d(y, x)$, se tiene que si $x \in M_n$, $-x \in M_n$, entonces $\mathsf{V}(x) = \mathsf{V}(-x)$, luego $d(x, y) = A^{\mathsf{V}(x-y)} = A^{\mathsf{V}(y-x)} = d(y, x)$.
- $d(x, y) \leq \text{máx}\{d(x, z), d(y, z)\}$.
  Como los M_n son subgrupos aditivos de M , tenemos $\mathsf{V}(x + y) \geq \text{mín}\{\mathsf{V}(x), \mathsf{V}(y)\}$, $d(x, y) = A^{\mathsf{V}(x-y)} = A^{\mathsf{V}((x-z)+(z-y))} \leq A^{\text{mín}\{x-z, z-y\}} = \text{máx}\{d(x, z), d(y, z)\}$.

Así la filtración $\{M_n\}_{n\geq 0}$ nos da una topología sobre M vía la métrica d. Un anillo con una topología inducida por una filtración de la forma anterior se dice que está topologizado linealmente. Esta topología es de Haussdorff si $\cap_{n\geq 0} M_n = 0$. Si este fuera el caso, la topología y la filtración se dice que son separables.

Sea $\mathfrak{a}$ un ideal de A. La topología dada por la filtración $\mathfrak{a}$-ádica es llamada topología $\mathfrak{a}$-ádica. Si $(A, \mathfrak{m})$ es un anillo local, noetheriano entonces cualquier A-módulo de generación finita es separable por la topología $\mathfrak{m}$-ádica.

Sea M un A-módulo filtrado, la topología inducida es de Hausdorff y sea d la métrica asociada, una sucesión de Cauchy en M es una sucesión $\{x_n\}$ de elementos de M tal que para cada $s > 0$, existe un entero $k > 0$ tal que $d(x_m, x_n) < s$ para todo $m, n \geq k$. Si $\{x_n\}$ es una sucesión de Cauchy, entonces existe un entero $k > 0$ tal que $x_m - x_n \in M_k$ para todo $m, n \geq k$. Una sucesión $\{x_n\}$ converge a $A \in M$ si existe un entero $k > 0$ tal que $x_n - A \in M_n$, para todo $n \geq k$. Por lo tanto toda sucesión convergente es de Cauchy, pero lo recíproco no es cierto en general.

Definición 3.1.1. *(Completación).* Un anillo topologizado linealmente es completo si es separable y cualquier sucesión de Cauchy en él es convergente. Si el anillo es completo con respecto a la topología $\mathfrak{a}$-ádica entonces decimos que este es completo $\mathfrak{a}$-adicamente.

Proposición 3.1.2. Si M es un A-módulo con una filtración $\{M_k\}$ tal que la topología inducida es de Hausdorff y M es completo, entonces una serie $\sum_{n=0}^{\infty} x_n$ con $x \in M$ converge en M si y solo si la sucesión $\{x_n\}$ converge a cero.

Demostración. Supongamos que $\sum_{n=0}^{\infty} x_n = A$, entonces la sucesión de sumas parciales $S_n = x_0 + x_1 + \cdots + x_n$ converge a A, luego:

$$\lim_{n\to\infty} (S_n - S_{n-1}) = \lim_{n\to\infty} x_n = 0.$$

Reciprocamente, si $\{x_n\} \to 0$, entonces para todo $n \in \mathbf{Z}$ existe un entero $N = N(n)$ tal que si $k \geq n$, se tiene que $x_k \in M_n$ y por lo tanto $x_k + x_{k+1} + \cdots + x_{k+i} \in M_n$ para todo $i \geq 0$, luego la sucesión de sumas parciales es de Cauchy y como M es completo, entonces converge en M. □

Lema 3.1.3. Sea A un anillo filtrado con una filtración $\{A_n\}_{n\geq 0}$ y sea M un A-módulo filtrado con una filtración $\{M_n\}_{n\geq 0}$.

(i) El conjunto $x + M_n$ es abierto y cerrado en M para todo $x \in M$, $n \geq 0$.

(ii) La familia $\{x + M_n\}_{n\geq 0}$ es un sistema fundamental de vecindades de x en M.

(iii) La adición y la multiplicación en A son continuas, entonces A es un anillo topológico y M es un A-módulo topológico.

(iv) Para un subconjunto N de M, la clausura de N en M es $\bigcap_{n\geq 0}(N + M_n)$.

(v) Dos filtraciones $\{M_n\}_{n\geq 0}$ y $\{M'_n\}_{n\geq 0}$ definen la misma topología sobre M si y solamente si dado $r \geq 0$, existe $n(r) \geq 0$ y $n'(r) \geq 0$ tales que $M_n(r) \subseteq M'_r$ y $M'_{n'(r)} \subseteq M_r$.

(vi) Si dos ideales a y b definen la misma topología ádica sobre A entonces $\sqrt{a} = \sqrt{b}$. Lo recíproco es verdadero si el anillo es noetheriano.

(vii) Sea N un A-módulo linealmente topologizado con la topología dada por la filtración $\{N_n\}_{n\geq 0}$. Entonces un A-homomorfismo $f: M \to N$ es continuo si y solamente si dado $r \geq 0$, existe $n(r) \geq 0$ tal que $f(M_{n(r)}) \subseteq N_r$.
Todo A-homomorfismo $f: M \to N$ es continuo para la topología a-ádica sobre M y N.

(viii) Sea N un submódulo de M. Entonces la topología cociente sobre M/N es la misma definida por la filtración inducida $\{M_n \cap N\}_{n\geq 0}$. Si M tiene la topología a-ádica entonces la topología cociente es la topología a-ádica en M/N.

La demostración puede ser vista en [3].

Sea M un A-módulo topologizado linealmente. Una completación de M es un par $(\hat{M}, \phi)$ donde $\hat{M}$ es un A-módulo completo topologizado linealmente y $\phi: M \to \hat{M}$ es un A-homomorfismo continuo tal que dado cualquier (M', ψ) del mismo tipo, existe un único A-homomorfismo $\hat{\psi}: \hat{M} \to M'$ tales que $\psi = \hat{\psi}\phi$.

Ejemplos:

1. Sea $p\mathbf{Z} \subseteq \mathbf{Z}$, con p primo, tenemos la filtración p-ádica $\{p^n\mathbf{Z}\}_{n\geq 0}$ de $\mathbf{Z}$, donde $\cap p^n\mathbf{Z} = 0$, luego la topología correspondiente es de Hausdorff. La completación p-ádica de $\mathbf{Z}$, es el anillo de los enteros p-ádicos: $\mathbf{Z}_p$ y sus elementos son series infinitas $\sum_{n=0}^{\infty} a_n p^n$, $0 < a_n < p - 1$. Se tiene $p^n \to 0$ cuando $n \to \infty$.

2. La completación m-ádica de $A[x_1, \ldots, x_n]$ es el anillo de series formales de potencia $A[[x_1, \ldots, x_n]]$, donde A es conmutativo.

Proposición 3.1.4. Si A es un noetheriano, entonces $\hat{A}$ es A-plano.

La demostración puede ser vista en [3] .

3.2. Anillos y módulos graduados

Sea G un semigrupo abeliano con elemento identidad cero. Un anillo graduado es un anillo R junto con una descomposición en suma directa de R como grupos aditivos $R = \bigoplus_{i \in G} R_i$, satisfaciendo $R_iR_j \subset R_{i+j}$. Un R-módulo graduado es un R-módulo M junto con una descomposición en suma directa de $M = \bigoplus_{i \in G} M_i$, satisfaciendo $R_iM_j \subset M_{i+j}$.

Sea A un anillo filtrado con una filtración $E = \{A_n\}_{n\geq 0}$ y sea M un A-módulo filtrado con una filtración $F = \{M_n\}_{n\geq 0}$. $\mathbf{gr}_E(A)$, $\mathbf{gr}_F(M)$ denotan las graduaciones asociadas a estas filtraciones, $\mathbf{gr}_E(A)$ es el anillo graduado $\bigoplus_{n\geq 0} A_n/A_{n+1}$, mientras que $\mathbf{gr}_F(M)$ es el $\mathbf{gr}_E(A)$-módulo graduado $\bigoplus_{n\geq 0} M_n/M_{n+1}$.

Para $x \in M$, definimos la forma inicial $\mathbf{in}_F(x)$

$$\mathbf{in}_F(x) = \begin{cases} 0 & ; \ \mathbf{si}\ \mathbf{ord}_F(x) = \infty \\ \bar{x} \in M_n/M_{n+1} & ; \ \mathbf{si}\ n = \mathbf{ord}_F(x) < \infty \end{cases}$$

donde $\bar{x}$ es la imagen natural de x en M_n/M_{n+1}. Así $\mathbf{in}_F(x)$ es cero o un elemento homogéneo de $\mathbf{gr}_F(M)$ de grado $\mathbf{ord}_F(x)$. Para un submódulo N de M, el submódulo inicial, $\mathbf{in}_F(N)$, de N graduación asociada a F es la graduación $\mathbf{gr}_E(A)$-submódulo $\mathbf{gr}_F(M)$ generado por el conjunto $\{\mathbf{in}_F(x) \,/\, x \in N\}$.

Proposición 3.2.1. Sea A un anillo completo, con la topología definida por E y que M es separable para la topología definida por F. Sea N un submódulo de M y supongamos que $x_1, x_2, \ldots, x_s$ son elementos de N tal que el módulo inicial $\mathbf{in}_F(N)$ es generado como un A-módulo por $x_1, x_2, \ldots, x_s$.

La demostración puede ser vista en [4].

Como consecuencia inmediata de esta proposición tenemos los siguientes resultados:

i) Sea A un anillo completo con la topología definiada por $E = \{A_n\}_{n\geq 0}$, $\mathfrak{a}$ un ideal de A. Si $a_1, \ldots, a_s$ son elementos de $\mathfrak{a}$ tal que el ideal inicial $\mathbf{in}_E(\mathfrak{a})$ es generado por $\mathbf{in}_E(a_1), \mathbf{in}_E(a_2), \ldots, \mathbf{in}_E(a_s)$, etonces $\mathfrak{a}$ es generado por $a_1, \ldots, a_s$.

ii) Si A es un anillo completo para la topología definida por $E = \{A_n\}_{n\geq 0}$. Si $\mathbf{gr}_E(A)$ es noetheriano entonces A es noetheriano.

3.3. Completación de un anillo local

Si (A, m) es un anillo local, con la topología m-ádica, denotamos por $\hat{A}$ su completación m-ádica.

Proposición 3.3.1. Sea (A, m) un anillo local, sea $\psi : A \to \hat{A}$ el homomorfismo canónico. Entonces:

1) $\hat{A}$ es un anillo local con ideal maximal $\hat{m} =$ clausura de $\psi(m)$ en $\hat{A}$.

2) ψ es un homomorfismo de anillos locales.

3) ψ induce un isomorfismo $A/m^n \to \hat{A}/\hat{m}^n$, para todo $n \geq 0$. En particular, los cuerpos residuales de A y $\hat{A}$ son naturalmente isomorfos.
   Si m es finitamente generada, entonces:

4) $\hat{m} = m\hat{A}$.

5) La topología de $\hat{A}$ es la topología $\hat{m}$-ádica.

6) La aplicación $\mathrm{gr}\colon \mathrm{gr}_m(A) \to \mathrm{gr}_{\hat{m}}(\hat{A})$ es un isomorfismo de anillos graduados.

7) $\hat{A}$ es noetheriano.

La demostración puede ser vista en [4].

Teorema 3.3.2. Sea (A, m) un anillo local, noetheriano y sea $\hat{A}$ su completación m-ádica. Entonces:

1. $\mathrm{gr}_m(A)$ es isomorfo a $\mathrm{gr}_{\hat{m}}(\hat{A})$.

2. $\dim A = \dim \hat{A}$.

3. A es regular si y solo si $\hat{A}$ es regular.

La demostración puede ser vista en [4].

Proposición 3.3.3. 1. Si $u\colon A \to B$ es un homomorfismo local de anillos locales entonces existe un único homomorfismo local $\hat{u}\colon \hat{A} \to \hat{B}$ tal que $\psi u = \hat{u}\phi$ donde $\phi\colon A \to \hat{A}$ y $\psi\colon B \to \hat{B}$ son los homomorfismos canónicos.

2. Sea $u : (A, m) \to (B, n)$ un homomorfismo local de anillos locales y sea $\mathrm{gr}(u) : \mathrm{gr}_m(A) \to \mathrm{gr}_n(B)$ el homomorfismo inducido. Si $\mathrm{gr}(u)$ es inyectivo y A es separable entonces u es inyectiva y si $\mathrm{gr}(u)$ es suryectivo, entonces u es suryectivo.

3. Si A es un anillo local y completo, a es un ideal propio, entonces A/a es local y completo.
4. Si A es regular, local de dimensión d, entonces $A[[x_1, x_2, \ldots, x_r]]$ es local, regular de dimensión $d+r$.
5. Sea $u : A \to B$ un homomorfismo local de anillos. Si B es completo, $T_1, T_2, \ldots, T_r$ indeterminadas sobre A. Sean $x_1, x_2, \ldots, x_r$ elementos del ideal maximal de B. Entonces u se extiende a un único A-álgebra homomorfismo $v : A[[T_1, \ldots, T_r]] \to B$ tal que $v(T_i) = x_i$ para todo i.

La demostración puede ser vista en [2].

3.4. Suavidad formal

Un anillo topológico A es un anillo con una topología a-ádica para algún ideal a de A, tal ideal es llamado ideal de definición para la topología.

Decimos que B es una A-álgebra topológico si A y B son anillos topológicos, B es una A-álgebra y el homomorfismo $A \to B$ es continua.

Si A y B son anillos locales entonces el homomorfismo $A \to B$ es continua por la topología ideal maximal-ádica sobre A y B si y solamente si este es un homomorfismo local.

Decimos que B es un A-álgebra discreto, cuando B es una A-álgebra topológica tal que la topología de B es la topología discreta (esta es la 0-ádica topología).

Si (A, m) es un anillo local y supongamos que A tiene la topología m-ádica. Si B es una A-álgebra local entonces el homomorfismo $A \to B$ es continuo si y solo si este es un homomorfismo local.

En lo que sigue frecuentemente consideraremos el diagrama conmutativo

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "\psi"'] & B \arrow[d, "u"] \\ C \arrow[r, "\eta"'] \arrow[ur, dotted, "v"] & C/I \end{tikzcd} \qquad (3.1)$$

donde B es una A-álgebra topológico (ϕ es un homomorfismo), C es un anillo, I es un ideal de C y C/I tiene la topología discreta; ψ y u son homomorfismos de A-álgebras.

Lema 3.4.1. En el diagrama (3.1). Si I es nilpotente y u es continua entonces v y ψ son continuas.

Demostración. Tenemos el siguiente diagrama

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "\psi"'] & B \arrow[d, "u"] \arrow[dl, dotted, "v"'] \\ C \arrow[r, "\eta"'] & C/I \end{tikzcd}$$

donde B es una A-álgebra topológico, C es un anillo, I es un ideal de C, C y C/I tienen la topología discreta y ψ, u son homomorfismos de A-álgebras.
Como I es un ideal nilpotente, se tiene que $I^n = 0$, luego como C, C/I tienen la topología discreta son A-álgebras topológicos, entonces u es continua, entonces $u^{-1}(0)$ es una vecindad de cero en B, analogamente $(u^{-1}(0))^n$ también es una vecindad de cero en B. Desde que $v(u^{-1}(0)) \subset I$ e $I^n = 0$, tenemos que $(u^{-1}(0))^n \subset v^{-1}(0)$ es una vecindad de cero en B, por lo tanto v es continua. De la misma forma se procede para $u\phi$ en lugar de u y se muestra que ψ es continua. □

Definición 3.4.2. Sea B una A-álgebra topológica. Decimos que B es formalmente suave sobre A o que B/A es suave o más precisamente que la estructura del homomorfismo $A \to B$ es formalmente suave, si dado cualquier A-álgebra discreta C, un ideal I de C con $I^2 = 0$ y un homomorfismo de A-álgebra continua $u : B \to C/I$ (con C/I discreto), existe un homomorfismo de A-álgebra $v : B \to C$ tales que $u = \eta v$, donde $\eta : C \to C/I$ es el homomorfismo natural.

Nota 3.4.3.

1. v es necesariamente continua por el Lema (3.4.1).

2. B es formalmente suave sobre A si y solamente si dado un anillo discreto C, un ideal I de C con $I^2 = 0$, la topología discreta sobre C/I y el diagrama conmutativo (3.1) con ψ continua, existe v como se muestra en el diagrama.

Lema 3.4.4. Sea B formalmente suave sobre A. Entonces:

(i) Dado el diagrama (3.1) con I nilpotente, existe v como se muestra en el diagrama, además v es continua.

(ii) Si $(R, \mathfrak{n})$ es un anillo local, noetheriano y completo y $u : B \to R/\mathfrak{n}$ un homomorfismo de A-álgebra continua entonces existe un homomorfismo de A-álgebra $v : B \to R$ tales que $u = \eta v$, donde $\eta : R \to R/\mathfrak{n}$ es el homomorfismo natural.

Demostración. Prueba de (i). Como I es nilpotente, $\exists\, n$ tales que $I^n = 0$, usaremos inducción sobre n. Para $n \geq 3$, consideraremos el siguiente diagrama

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "\psi"'] & B \arrow[dl, dotted, "v"'] \arrow[d, "v'"] \arrow[dr, dotted, "u"] & \\ C \arrow[r, "\eta"'] & C/I^2 \arrow[r] & C/I \end{tikzcd}$$

Desde que el ideal I/I^2 de C/I^2 es el cuadrado del cero, existe v' y es continua. Ahora desde que $(I^2)^{n-1} = 0$ existe v por hipótesis inductiva.

Prueba de (ii). Por inducción sobre $n \geq 1$, mostramos que existe un homomorfismo de A-álgebra continua $v_n : B \to R/\mathfrak{n}^n$ tal que el diagrama

$$\begin{tikzcd} & B \arrow[dl, "v_{n+1}"'] \arrow[dr, "v_n"] & \\ R/\mathfrak{n}^{n+1} \arrow[rr] & & R/\mathfrak{n}^n \end{tikzcd}$$

es conmutativo para todo n. Para $n = 1$, tomamos $v_1 = u$, supongamos que existe v_n continuo. Desde que $\mathfrak{n}^n/\mathfrak{n}^{n+1}$ es un ideal de $R/\mathfrak{n}^{n+1}$ de cuadrado cero, implica la existencia de v_{n+1}. Esto muestra la existencia de los v_n para todo n, ahora desde que $\hat{R}$ es el límite inverso de $\{R/\mathfrak{n}^n\}$ conseguimos el homomorfismo $B \to R$. $\square$

Proposición 3.4.5. *(Algunas propiedades de suavidad formal).*

(1) La identidad $1_A : A \to A$ es formalmente suave.

(2) Si $\phi : A \to B$ y $\psi : B \to C$ son formalmente suaves entonces $\psi \circ \phi : A \to C$ es formalmente suave.

Demostración. (1) Se obtiene facilmente considerando $C = A$ e $I = 0$.

(2) Consideremos el diagrama

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "w"'] & B \arrow[r, "\psi"] \arrow[dl, dashed, "w'"] \arrow[dr, "u\psi"] & C \arrow[d, "u"] \arrow[dll, dashed, "v"] \\ {} & & {} \end{tikzcd}$$

$D^{CJ}{}'^{S}$ ———— $\cdot$ $D\overset{X}{/}$ I

donde D y D/I son discretos, $I^2 = 0$ y u, w son continuas. Desde que B es formalmente suave sobre A, existe w', luego existe v, haciendo que el diagrama conmute. □

Definición 3.4.6. Sea A un anillo y B un A-álgebra. Decimos que B es suave sobre A o B/A es suave o que la estructura homomórfica $A \to B$ es suave, si B es formalmente suave sobre A para la topología discreta sobre A y B.

B es suave sobre A si existe el homomorfismo v para cada diagrama dado (3.1) con $I^2 = 0$, sin referencia a ninguna topología.

Lema 3.4.7. *B es suave sobre A si y solamente si B es formalmente suave sobre A para todas las topologías sobre A y B para el cual la estructura homomórfica $A \to B$ es continua.*

Demostración. Es inmediato de la definición 3.4.6. □

Ejemplos.

1. Si A es un anillo, el anillo de polinomios en un número arbitrario de variables $A[x_i]_{i\in I}$ es suave sobre A.

2. Si S es un subconjunto multiplicativamente cerrado de un anillo A. Entonces $S^{-1}A$ es suave sobre A.
   Consideremos el diagrama:

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\psi"'] & S^{-1}A \arrow[d, "u"] \arrow[dl, "v"'] \\ C \arrow[r, "\eta"'] & C/I \end{tikzcd}$$

   Para mostrar la existencia de v, es suficiente probar que $\psi(t)$ es unidad en C, para todo $t \in S$. Desde que $\eta(\psi(t)) = u(t)$ es unidad en C/I, puesto que t pertenece a S y es unidad en $S^{-1}A$, entonces tenemos que $\eta(\psi(t))$ es unidad en C/I, por lo tanto $\psi(t)$ es una unidad en C.

3. Sea S un subconjunto multiplicativo de $A[x_i]_{i\in I}$, luego por el ejemplo (2) tenemos que $S^{-1}A[x_i]_{i\in I}$ es suave sobre A. Particularmente si k es un cuerpo, entonces el cuerpo de funciones racionales $K = k(x_i)_{i\in I}$ es suave sobre k, aplicando la proposición 3.4.5.

3.5. Extensiones separables de cuerpos

Definición 3.5.1. Sea K/k una extensión de cuerpo. Decimos que K/k es:

(1) Algebraicamente separable si este es algebraica y separable.

(2) Separablemente generado si este tiene una base de trascendencia $\{t_i\}_{i\in I}$ tales que K es algebraicamente separable sobre $k(\{t_i\})_{i\in I}$.

Nota 3.5.2. Respecto a la definición anterior:

(1) En el caso (2) el conjunto $\{t_i\}_{i\in I}$ es llamado una base de trascendencia de separación de K/k.

(2) Si K/k es separable entonces L/k es separable para todo cuerpo intermediario L. Por otro lado si L/k es separable para todo cuerpo intermediario finitamente generado L de K/k entonces K/k es separable. Así K/k es separable si y solo si toda subextensión finitamente generado de K/k es separable.

Teorema 3.5.3. Sea K/k una extensión de cuerpo finitamente generado. Sea p el exponente característico de k. Entonces las siguientes condiciones son equivalentes:

1. Todo conjunto generador de K/k contiene una base de trascendencia de separación.

2. K/k es separablemente generado.

3. $K \otimes_k A$ es reducido para todo k-álgebra A.

4. $K \otimes_k K^{1/p}$ es reducido.

5. K/k es separable.

La demostración puede ser vista en [4].

Definición 3.5.4. Un cuerpo k es llamado perfecto si toda extensión algebraica de k es algebraicamente separable.

Un cuerpo finito, un cuerpo algebraicamente cerrado y un cuerpo de característica cero son todos perfectos.

Proposición 3.5.5. Si k es un cuerpo perfecto entonces toda extensión de cuerpo K/k es separable.

Demostración. Si K/k es una extensión de cuerpos finitamente generado, entonces $K = k(\alpha_1, \alpha_2, \dots, \alpha_n)$, donde $\alpha_1, \dots, \alpha_n$ pertenecen a K, luego no todos son algebraicamente independientes ni algebraicos sobre K, entonces reordenando tenemos que $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ son algebraicamente independientes y $\{\alpha_{m+1}, \alpha_2, \dots, \alpha_n\}$ son algebraicos sobre k, luego $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ es una base de trascendencia tales que $k(\alpha_1, \alpha_2, \dots, \alpha_m, \alpha_{m+1}, \dots, \alpha_n)$ es algebraicamente separable sobre $k(\alpha_1, \dots, \alpha_m)$, puesto que $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ son separables sobre $k(\alpha_1, \dots, \alpha_m)$ y $\{\alpha_{m+1}, \dots, \alpha_n\}$ son algebraicos sobre k, luego como k es perfecto son separables sobre $k(\alpha_1, \dots, \alpha_m)$, por lo tanto K/k se separablemente generado, luego por el Teorema (3.5.3)(5) K/k se separable. Entonces tenemos que todo cuerpo intermediario L de K/k finitamente generado se separable sobre k entonces K/k es separable. □

Teorema 3.5.6. Sea K/k una extensión de cuerpo separable. Entonces K es suave sobre k.

Demostración. Probaremos, cuando K/k es finitamente generada, luego K/k es separablemente generada, así existe un cuerpo intermedio K' de K/k tal que K'/k es finitamente generada y puramente trascendental y K/K' es finito y algebraicamente separable. Por la proposición (3.4.5)(2) es suficiente probar que K es suave sobre K' y K' suave sobre k. La suavidad de K'/k se observó en el ejemplo 3 de la página 38, luego sea K/k finita y algebraicamente separable. Entonces $K = k[t] = k[T]/(f(T))$, donde $f(T)$ es un polinomio separable irreducible y mónico en $k[T]$. Sea el diagrama

$$\begin{tikzcd}
k \arrow[r] \arrow[d, dash] & K = k[t] = k[T]/(f(T)) \arrow[d, "u"] \arrow[dl, dotted, "v"'] \\
C \arrow[r, "\eta"'] & C/I
\end{tikzcd}$$

donde $I^2 = 0$ y C, C/I son discretos. Tenemos que mostrar que v existe. Elegimos $c \in C$ tal que $u(t) = \eta(c)$, entonces $f(c) \in I$. Para la existencia de v, es suficiente hallar $c' \in C$ tal que $f(c') = 0$ y $c - c' \in I$. Desde que $f(T)$ es separable, $f'(t)$ es una unidad en K. Por lo tanto, $\eta(f'(c)) = f'(\eta(c)) = f'(u(t)) = u(f'(t))$ es una unidad en C/I. Por lo tanto, desde que $I^2 = 0$, $f'(c)$ es una unidad en C.
Ahora, sea $a \in I$, entonces desde que $a^2 = 0$, tenemos $f(c + a) = f(c) + af'(c)$, por lo tanto tomando $a = -f'(c)^{-1}f(c) \in I$, conseguimos $f(c + a) = 0$. Así, $c' = c + a$ cumple el requerimiento. Esto completa la prueba cuando K/k es finitamente generado. □

Para el caso general ver [4] B. Singh, pag. 21.

3.6. Anillo y cuerpo de coeficientes de un anillo local

Sea (A, m) un anillo local. Decimos que A es equicaracterístico si la característica de A coincide con la característica de su cuerpo residual (A/m), es decir $\mathbf{char}(A) = \mathbf{char}(A/m)$, en otros casos se dice que A es inequicaracterístico. Existen solamente las siguientes posibilidades con respecto a la característica de A y de su cuerpo residual:

(i) $\mathbf{char}(A) = 0$; $\mathbf{char}(A/m) = 0$

(ii) $\mathbf{char}(A) = p$; $\mathbf{char}(A/m) = p, p > 0$

(iii) $\mathbf{char}(A) = 0$; $\mathbf{char}(A/m) = p, p > 0$

(iv) $\mathbf{char}(A) = p^n$; $\mathbf{char}(A/m) = p, p > 0, n \geq 2$

En los casos *(i)* y *(ii)* se tiene que A es equicaracterístico y en los casos *(iii)* y *(iv)* se tiene que A es inequicaracterístico.

Nota: A es equicaracterístico si y solamente si A contiene un cuerpo.

Definición 3.6.1. Sea A un anillo local. Un subanillo R de A es llamado anillo de coeficientes de A si este satisface las siguientes tres condiciones:

(i) R es un anillo local completo.

(ii) La aplicación inclusión $i : R \to A$ es un homomorfismo local e induce un isomorfismo de sus cuerpos residuales.

(iii) El ideal maximal de R es pR, donde $p = \mathbf{char}(A/m)$.

Notemos que desde que R es completo y su ideal maximal es finitamente generado, R es noetheriano.

Si un anillo de coeficientes es un cuerpo, entonces este es llamado cuerpo de coeficientes.

Proposición 3.6.2. Un anillo local es equicaracterístico si y solamente si contiene un cuerpo.

Demostración. Sea (A, m) un anillo local equicaracterístico, entonces se tiene que $\mathbf{char}(A) = \mathbf{char}(A/m)$. Luego desde que A es un anillo con identidad $\exists!$ homomorfismo $\phi : \mathbf{Z} \to A$, tal que a cada $n \in \mathbf{Z}$, $\phi(n) = n1_A$, luego por el teorema fundamental del homomorfismo tenemos $\mathrm{Im}\phi \cong \frac{\mathbf{Z}}{\ker\phi}$.

$$\ker \phi = \{x \in \mathbf{Z} : \phi(x) = 0_A\}$$
$$\ker \phi = \{x \in \mathbf{Z} : x.1_A = 0_A\},$$

entonces los elementos del $\ker(\phi)$ anulan a 1_A, luego $\ker(\phi) = \{0\} \vee \ker(\phi) = (p)$.

- Si $\ker\phi = (p)$, entonces la $\mathrm{Im}\phi \subset A$ es un cuerpo. Tenemos que $\mathrm{Im}\phi = \mathbf{Z}_p$.
- Si $\ker(\phi) = \{0\}$, se tiene que $\mathbf{Z} \subset A$, luego tenemos que $\mathbf{Z} \xrightarrow{\phi} A \longrightarrow A/m$.

Afirmación: Cualquier elemento no nulo en $\mathbf{Z}$ no es un cero en A/m. $(\phi(x) \not\in m)$.

Sea $x \in \mathbf{Z}$, con $x \neq 0$, entonces se tiene:

- $\bar{x} = \bar{0}$, luego $x.\bar{1} = \bar{0}$, entonces $\mathbf{char}(A/m) \neq 0$ $(\Rightarrow\Leftarrow)$.
- $\bar{x} \neq \bar{0}$, entonces $\phi(x) \not\in m$, luego $\phi(x)$ es unidad en A pues A es local, entonces $\phi(\mathbf{Z}) = \mathbf{Q}$ es un cuerpo.

Por lo tanto tenemos que si (A, m) es equicaracterístico, entonces A contiene un cuerpo K, donde $K = \mathbf{Q} \vee K = \mathbf{Z}_p$.

Recíprocamente, supongamos que $K \subset A$, es un cuerpo, luego desde que K es un cuerpo y $K \subset A$ se tiene que $\mathbf{char}(A) = \mathbf{char}(K)$ (lo que le sucede a 1_K le va a suceder a 1_A), luego tenemos $K \longrightarrow A \longrightarrow A/m$, donde $K \longrightarrow A$ es un homomorfismo inyectivo entonces $i(K) = K \subset A/m$, entonces tendríamos que $\mathbf{char}(K) = \mathbf{char}(A/m)$, por lo tanto tendríamos que $\mathbf{char}(A) = \mathbf{char}(A/m)$. □

Lema 3.6.3. Sea R un anillo de coeficientes de A. Entonces R es de dimensión a lo mas uno. Más precisamente.

1. Si A es equicaracterístico entonces R es un cuerpo.
2. Si A es inequicaracterístico y $\mathbf{char}(A) = 0$, entonces R es un anillo de valoración discreta con parámetro regular p, donde $p = \mathbf{char}(A/m)$.
3. Si A es inequicaracterístico y $\mathbf{char}(A) = p^n$, para algún $n \geq 2$, entonces R es un anillo local artiniano.

Demostración. En primer lugar veremos que $\mathbf{char}(A) = \mathbf{char}(R)$.
Desde que A y R son anillos locales tenemos que sus características son cero o potencias de un primo.

- Si $\mathbf{char}(A) = 0$, entonces $\mathbf{char}(R) = 0$ o $\mathbf{char}(R) = p^k$. Si $\mathbf{char}(A) = 0$, ya estaría probado lo que queremos. Si $\mathbf{char}(R) = p^k$, se tiene de que R es un anillo de coeficientes de A tales que $(A/m) \cong R/(0)$, entonces p^k pertenece al ideal (0), luego p^k es una potencia de (0), luego $p^k = 0$, de esta manera tendríamos que si $\mathbf{char}(A) = 0$, entonces $\mathbf{char}(R) = 0$.

$$\therefore\ \mathbf{char}(A) = \mathbf{char}(R).$$

- Si $\mathbf{char}(A) = p^k$, de manera análoga $\mathbf{char}(R) = 0$ o $\mathbf{char}(R) = p^A$, con p primo y $A > 0$, no puede suceder que la $\mathbf{char}(R) = 0$ puesto que se tendría que $0|p^k$ (la característica del subanillo divide a la característica del anillo) y esto es una contradicción, entonces tendríamos que $\mathbf{char}(R) = p^A$, luego $p^A|p^k$ entonces $A \leq k$, si $A < k$ tendríamos una contradicción puesto que se tiene que $(A/m) \cong \frac{R}{p^k R}$; entonces A tendría que ser un múltiplo de p^k, luego tendríamos que $A = k$ entonces tenemos que $\mathbf{char}(A) = \mathbf{char}(R)$.

Prueba de 1. Como A es equicaracterístico se tiene que $\mathbf{char}(A) = \mathbf{char}(A/m)$ y desde que R es un anillo de coeficientes de A se tiene que $(A/m) \cong (R/pR)$ donde p es la característica de (A/m), además tenemos que $\mathbf{char}(A) = \mathbf{char}(R)$, todo esto implica

$$\mathbf{char}(R) = \mathbf{char}(A) = \mathbf{char}(A/m) = \mathbf{char}(R/pR)$$

por lo tanto R es equicaracterístico, entonces R contiene un cuerpo y desde que $(A/m) \cong (R/pR)$, tenemos que el ideal maximal de R es cero, puesto que si $x \in pR$ tendríamos que $x = pr$, para algún $r \in R \subset A$, entonces $x = 0$ desde que $\mathbf{char}(A) = \mathbf{char}(A/m) = p$, entonces el ideal maximal de R es cero, por lo tanto R es un cuerpo.

Prueba de 2. Tenemos $\mathbf{char}(A) = 0$ entonces $\mathbf{Z} \subseteq R$, donde p no es nilpotente de R. Así $\dim(R) \geq 1$, se sigue que R es un anillo de valoración discreta con parámetro regular p, desde que R es un anillo de coeficientes de A.

Prueba de 3. Si $\mathbf{char}(R) = p^n$, entonces el ideal maximal de R es nilpotente. También, R es noetheriano, por lo tanto R es artiniano. $\square$

Capítulo 4

Teoremas de Estructura de Cohen

Aquí veremos integramente las demostraciones de los Teoremas de estructura de Cohen o teoremas de estructura para anillos locales para los casos equicaracterístico e inequicaracterístico.

4.1. Caso equicaracterístico

Teorema 4.1.1. Sea $(A, \mathfrak{m})$ un anillo local, noetheriano, completo y equicaracterístico con dimensión d. Entonces existe un subcuerpo K' de A tal que:

1. K' es un cuerpo de coeficientes de A.

2. $A \cong K'[[T_1, \dots, T_n]]/\mathfrak{a}$ como K'-álgebras para algún ideal $\mathfrak{a}$.

3. Si A es regular entonces $A \cong K'[[T_1, \dots, T_d]]$ como K'-álgebra.

Además, si A contiene un cuerpo k tales que $A/\mathfrak{m}$ es separable sobre k entonces todas las afirmaciones anteriores se mantienen con K' un cuerpo que contiene k.

Para la prueba del Teorema 4.1.1 necesitaremos los lemas siguientes:

Lema 4.1.2. Sea $(B, \mathfrak{n})$ un anillo local, noetheriano y completo, sea M un B-módulo. Supongamos que $M/\mathfrak{n}M$ es finitamente generado como B-módulo y que $\bigcap_{n\geq 1} \mathfrak{n}^n M = 0$ entonces M es finitamente generado como B-módulo.

Demostración. Sean $x_1, \dots, x_r \in M$ tal que sus imágenes $\bar{x}_1, \dots, \bar{x}_r$ generan $M/\mathfrak{n}M$ como B-módulo. Entonces, desde que $\mathbf{gr}_{\mathfrak{n}}(M)$ es generado por $M/\mathfrak{n}M$ como un $\mathbf{gr}_{\mathfrak{n}}(B)$-módulo, $\bar{x}_1, \dots, \bar{x}_r$ generan $\mathbf{gr}_{\mathfrak{n}}(M)$ como un $\mathbf{gr}_{\mathfrak{n}}(B)$-módulo. Ahora, desde que B es completo y $\bigcap_{n\geq 1} \mathfrak{n}^n M = 0$, luego tenemos que $x_1, \dots, x_r$ generan M como un B-módulo, por la proposición (3.2.1). □

Lema 4.1.3. Sea $(W, \mathfrak{p}) \to (A, \mathfrak{m})$ un homomorfismo local de anillos locales noetherianos completos induciendo un isomorfismo entre sus cuerpos residuales. Sean $x_1, \ldots, x_n \in \mathfrak{m}$ y $B = W⟦T_1, \ldots, T_n⟧$ el anillo de series de potencia formales en n variables sobre W. Entonces

1. Existe un único homomorfismo de W-álgebra local $\theta\colon B \to A$ tal que $\theta(T_i) = x_i$ para todo i.

2. Si $\mathfrak{m} = \theta(\mathfrak{p})A + (x_1, \ldots, x_n)A$ entonces θ es sobreyectivo.

3. Si $\{x_1, \ldots, x_n\}$ es un sistema de parámetros de A entonces θ convierte a A en un B-módulo finitamente generado.

Demostración. Prueba de 1. Por la proposición (3.3.3)(5), se tiene que existe un único W-álgebra homomorfismo $\theta : B \to A$ tales que $\theta(T_i) = x_i$.

Prueba de 2. Sea $\mathfrak{n}$ el ideal maximal de $B = W⟦T_1, T_2, \ldots, T_n⟧$, luego tenemos $\theta : B \to A$ homomorfismo local de anillos locales noetherianos completos y el homomorfismo inducido $\mathrm{gr}(\theta) : \mathrm{gr}_{\mathfrak{n}}(B) \to \mathrm{gr}_{\mathfrak{m}}(A)$ y desde que $\mathfrak{m} = \theta(\mathfrak{p})A + (x_1, \ldots, x_n)A$ se tiene que $\mathrm{gr}(\theta)$ es suryectivo y como A es completo aplicando la proposición (3.3.3)(2) tenemos que θ es sobreyectivo.

Prueba de 3. Sea $K = A/\mathfrak{m}$. Tenemos que $\theta\colon B \to A$ es sobreyectivo, luego como la proyección natural $A \to A/\mathfrak{m} = K$ es sobreyectivo, tenemos que el homomorfismo $B \to K$ es sobreyectivo, entonces los K-módulos $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ finitamente generados son finitamente generados como B-módulos, luego $A/\mathfrak{m}^i$ es finitamente generado para cada i. Desde que $\mathfrak{n}A$ está contenido en $\mathfrak{m}$, se tiene que $\mathfrak{n}A$ es $\mathfrak{m}$-primario, luego existe i tales que $\mathfrak{m}^i \subseteq \mathfrak{n}A$, entonces tenemos que $A/\mathfrak{n}A$ es finitamente generada como un B-módulo, luego tenemos que $\bigcap_{n\geq 1} \mathfrak{n}^n A \subseteq \bigcap_{n\geq 1} \mathfrak{m}^n = 0$, entonces $\bigcap_{n\geq 1} \mathfrak{n}^n A = 0$ y por el lema (4.1.2) se tiene que A es finitamente generado como B-módulo. □

Prueba del teorema (4.1.1).

Demostración. Prueba de 1. Consideremos $\mathbf{K} = A/\mathfrak{m}$. Desde que A es equicaracterístico se tiene que A contiene un cuerpo k contenido en A, consideremos a este cuerpo como el cuerpo primo, entonces $k = \mathbf{Q}$ o $k = \mathbf{Z}_p$, luego como k es perfecto, tenemos que $\mathbf{K}/k$ es separable, entonces $\mathbf{K}$ es suave sobre k por el teorema (3.5.6), luego tenemos el siguiente diagrama

$$\begin{tikzcd}
k \arrow[r] \arrow[d, "\mathbf{i}"'] & \mathbf{K} \arrow[d, "\mathbf{id}"] \arrow[dl, dotted, "\nu"'] \\
A \arrow[r, "\eta"'] & \mathbf{K}
\end{tikzcd}$$

Por el lema (3.4.4)(ii) existe $v : \mathbf{K} \to A$ (homomorfismo de k-álgebra) donde $v(\mathbf{K}) \subset A$ y $v(\mathbf{K})$ es un subanillo de A.

Afirmación: $v(K) = K'$ es un cuerpo.

Sea $u \neq 0$, $u \in v(\mathbf{K})$, existe $r \in \mathbf{K}$ tal que $v(r) = u$ y desde que $\mathbf{K}$ es cuerpo existe $t \in \mathbf{K}$ tal que $rt = 1_{\mathbf{K}}$, luego aplicando v, tenemos

$$\begin{aligned} v(rt) &= v(1_{\mathbf{K}}) \\ v(r)v(t) &= 1_A \\ uv(t) &= 1_A \end{aligned}$$

entonces u es unidad, por lo tanto $v(\mathbf{K}) = K'$ es un cuerpo.

Afirmación 2: $K' \subset A$ es el cuerpo de coeficientes de A.

- K' es local: Desde que K' es cuerpo, K' tiene un solo ideal maximal y por lo tanto K' es local.

- K' es completo. Se tiene que m es abierto, $A - m$ es cerrado, como $\{0\}$ es cerrado, tenemos $(A - m) \cup \{0\} = K'$ es cerrado. Cualquier sucesión de Cauchy en K' converge en A, puesto que A es completo y como K' es cerrado, esta sucesión converge en K', por lo tanto K' es completo.

- El morfismo $(K', 0) \xrightarrow{i} (A, m)$ es local e induce un isomorfismo entre ss cuerpos residuales.

  - $i(0) = 0 \subset m$, entonces i es local
  - $A/m \cong \frac{K'}{\{0\}} \cong K'$. En efecto, tenemos $v : K \to A$, por el teorema fundamental del homomorfismo $\dfrac{K}{\ker(v)} \cong \mathbf{Im}(v)$. Como $\mathbf{Im}(v) = K'$, tenemos $\dfrac{K}{\ker(v)} = K'$, como K es un cuerpo y A 0, entonces el homomorfismo v es inyectivo entonces $\ker(v) = 0$, entonces tenemos $\dfrac{K}{\{0\}} \cong K' \Rightarrow K' \cong K = A/m$, por lo tanto $K' \cong A/m$.

- El ideal maximal de K' es pK', donde $p = \mathbf{char}(A/m)$. En efecto, desde que K' es cuerpo, su ideal maximal es el $\{0\}$.

  - Si $p = 0$, entonces $pK' = 0.K' = \{0\}$.

- Si $p \neq 0$, entonces por demostrar que $pK' = \{0\}$.
  Tenemos $\{0\} \subset pK'$, faltaría ver que $pK' \subset \{0\}$.
  Sea $x \in pK' \subset K' \subset A$, entonces $x = pr$, para algún $r \in K' \subset A$, luego $x = 0$, puesto que $p = \mathbf{char}(A)$, por lo tanto $pK' = \{0\}$.

Con estas condiciones satisfechas K' es el cuerpo de coeficientes de A.

Prueba de 2. Tenemos $(K', 0) \xrightarrow{i} (A, m)$ es un homomorfismo local, (A, m) es noetheriano, local y completo, K' es local, noetheriano completo, además sean $x_1, \dots, x_n$ generadores de m, luego por el Lema (4.1.3) existe un único homomorfismo de K'-álgebra $\theta\colon K'[\![T_1, \dots, T_n]\!] \to A$, donde $\theta(T_i) = x_i$, para $1 \leq i \leq n$ y además desde que $m = \theta(0) + (x_1, \dots, x_n)A = (x_1, \dots, x_n)A$, entonces θ es suryectivo, luego por el teorema fundamental del homomorfismo tenemos que

$$\frac{K'[\![T_1, \dots, T_n]\!]}{\ker(\theta)} \cong A$$

donde $\ker(\theta)$ es un ideal de $K'[\![T_1, \dots, T_n]\!]$.

Prueba de 3. Como A es regular y $\dim A = d$, entonces el mínimo número de generadores de m es d, es decir $x_1, \dots, x_d$ generan m, luego por el resultado anterior tendríamos:

$$\frac{K'[\![T_1, \dots, T_d]\!]}{\ker(\theta)} \cong A. \tag{4.1}$$

Desde que K' es cuerpo, la dimensión del anillo $K'[\![T_1, \dots, T_d]\!]$ es d y la dimensión de A es d, comparando dimensiones tenemos que $\mathrm{ht}(\ker(\theta)) = 0$ luego $\ker(\theta) = \{0\}$ entonces tendríamos

$$A \cong \frac{K'[\![T_1, \dots, T_d]\!]}{\{0\}} \cong K'[\![T_1, \dots, T_d]\!].$$

Por lo tanto $A \cong K'[\![T_1, \dots, T_d]\!]$. □

4.2. Álgebras de Cohen

Lema 4.2.1. Sea $A \to B$ un homomorfismo local de anillos locales noetherianos. Sea m el ideal maximal de A. Si B/m^nB es A/m^n plano para todo $n \geq 1$, entonces B es A-plano.

Demostración. Para probar que B es A-plano será suficiente probar que si dado $\mathfrak{a}$ un ideal de A, entonces la aplicación natural $f\colon \mathfrak{a} \otimes_A B \to B$ es inyectiva. Desde que el homomorfismo $A \to B$ es local, B es noetheriano y $a \otimes_A B$ es de generación finita como B-módulo, tenemos que $\bigcap_{n\geq 1} m^n(a \otimes_A B) = 0$, por lo tanto es suficiente probar que $\ker(f) \subseteq m^n(a \otimes_A B)$ $\forall\ n \geq 1$. Para $n \geq 1$ fijo por el lema de Artin-Rees existe $r \geq n$ tal que $m^r \cap a \subseteq m^n a$ y desde que $B/m^r B$ es A/m^r-plano, la sucesión exacta $0 \longrightarrow a/(m^r \cap a) \longrightarrow A/m^r$ nos da la siguiente sucesión exacta:

$$0 \longrightarrow (a/m^r \cap a) \otimes_{A/m^r} (B/m^r B) \xrightarrow{g} (A/m^r) \otimes (B/m^r B)$$

$$0 \longrightarrow (a/m^r \cap a) \otimes_{A/m^r} (B/m^r B) \xrightarrow{g} (B/m^r B)$$

la cual es isomorfa a la sucesión exacta $0 \longrightarrow (a/m^r \cap a) \otimes B \longrightarrow B/m^r B$ y desde que $(m^r \cap a) \subseteq m^n a$ tenemos que el siguiente diagrama conmuta:

$$\begin{tikzcd} a \otimes B \arrow[r, "u"] \arrow[d, "f"'] & (a/m^r \cap a) \otimes B \arrow[r, "v"] \arrow[d, "g"] & a/m^n a \otimes B \\ B \arrow[r] & B/m^r B & \end{tikzcd}$$

donde todas las aplicaciones son naturales, sea $x \in \ker(f)$, como el diagrama conmuta tenemos que $gu(x) = 0$, desde que g es inyectiva se tiene $u(x) = 0$, luego tenemos que $v(u(x)) = 0$, entonces $x \in \ker(vu)$, por lo tanto desde que $(a/m^n a) \otimes_A B = (A/m^n) \otimes_A a \otimes_A B = (a \otimes_A B)/m^n(a \otimes_A B)$, tenemos que $x \in m^n(a \otimes_A B)$, $\forall\ n \geq 1$ luego $x \in \bigcap_{n\geq 1} m^n(a \otimes_A B) = 0$, entonces $x = 0$. $\therefore$ $\ker(f) = 0$, entonces f es inyectiva, por lo tanto B es A-plano. $\square$

Lema 4.2.2. Sea $\{A_i, f_{ij}\}$ un sistema inductivo de anillos locales (A_i, m_i, K_i) y homomorfismo locales $f_{ij} : A_i \to A_j$ para $i \leq j$. Sea $A = \varinjlim A_i$, entonces:

(1) A es un anillo local, cuyo ideal maximal $m = \varinjlim m_i$ y con cuerpo residual $K = \varinjlim K_i$.

(2) Si A_j es A_i-plano para todo $i \leq j$, entonces A es A_i-plano para todo i.

(3) Si $m_j = m_i A_j$ para todo $i \leq j$ entonces $m = m_i A$ para todo i.

(4) Si A_j es A_i-plano y $m_j = m_i A_j$ para todo $i \leq j$ y A_i es noetheriano para todo i entonces A es noetheriano.

La demostración puede ser vista en [4].

Teorema 4.2.3. Sea (R, n) un anillo local, noetheriano y sea K una extensión de cuerpos de R/n. Entonces existe un anillo local noetheriano (A, m) y un homomorfismo local $R \to A$ tales que A es R-plano, $m = nA$ y $A/m \cong K$ sobre R/n.

La demostración puede ser vista en [4].

Definición 4.2.4. 1. Sea $(R, n) \to (A, m)$ un homomorfismo local de anillos noetherianos locales. Decimos que A es un R-álgebra de Cohen si se tiene las siguientes tres condiciones:

i) A es completo.

ii) A es R-plano.

iii) $m = nA$ y A/m es separable sobre R/n.

Ejemplo: Sea (R, n) un anillo local noetheriano, entonces $\hat{R}$ es un R-álgebra de Cohen.

Sea $(R, n) \to (\hat{R}, \hat{n})$ un homomorfismo local de anillos locales noetherianos, luego se tiene:

i) $\hat{R}$ es completo.

ii) $\hat{R}$ es R-plano, pues R es noetheriano.

iii) $\hat{n} = n\hat{R}$ y como $(\hat{R}/\hat{n}) \cong (R/n)$ entonces $(\hat{R}/\hat{n})$ es separable sobre (R/n). Este resultado lo tenemos de la proposición (3.3.1). Por lo tanto, se tiene que $\hat{R}$ es un R-álgebra de Cohen.

2. Sea $p \geq 0$ un entero primo. Por anillo local, primo, completo p-ádico nos referimos al anillo $\Gamma_p = \hat{\mathbf{Z}}_p$ (Notemos que $\Gamma_0 = \mathbf{Q}$ es un cuerpo, para $p > 0$, Γ_p es un anillo de valoración discreta con parámetro regular p).

3. Un Γ_p-álgebra de Cohen es llamado un anillo p-ádico de Cohen.

Observación: Si (A, m) es un anillo local noetheriano completo con $\mathbf{char}(A/m) = p$ entonces existe un único homomorfismo local $\Gamma_p \to A$.

Lema 4.2.5. Sea (A, m) un anillo p-ádico de Cohen. Si $p = 0$ entonces A es un cuerpo. Si $p > 0$ entonces A es un anillo de valoración discreta completo con parámetro regular p.

Demostración. Desde que (A, m) es un anillo p-ádico de Cohen, tenemos que $m = pA$, luego si $p = 0$, entonces $m = 0$ luego A es un cuerpo. Por otro lado si $p > 0$ entonces p no es un divisor de cero en Γ_p y desde que A es Γ_p-plano, p no es un divisor de cero en A, así $\dim(A) \geq 1$, luego desde que el ideal maximal m de A es principal, se tiene que A es un anillo de valoración discreta y finalmente como $m = pA$, se tiene que p es un parámetro regular de A. $\square$

Teorema 4.2.6. Sea (R, n) un anillo local, noetheriano y sea K una extensión de cuerpo separable sobre R/n. Entonces existe un R-álgebra de Cohen (A, m) tales que $A/m \cong K$ sobre R/n.

Demostración. Por el teorema (4.2.3), existe un anillo local, noetheriano (A, m) y un homomorfismo local $R \xrightarrow{\psi} A$ tales que A es R-plano, $m = nA$ y (A/m) es isomorfo a K sobre R/n. Como (A, m) es un anillo local, noetheriano, tenemos que $(\hat{A}, \hat{m})$ es un anillo local, noetheriano, luego tenemos el siguiente homomorfismo:

$$\underbrace{(R, n) \xrightarrow{\psi} (A, m) \xrightarrow{\phi} (\hat{A}, \hat{m})}_{\eta = \phi \circ \psi}$$

donde η es local, pues $\eta(n) = \phi(\psi(n)) \subset \phi(m) \subset \hat{m}$, entonces η es un homomorfismo local entre anillos locales y noetherianos. Queremos determinar que $\hat{A}$ es un R-álgebra de Cohen, para esto veamos

a) $\hat{A}$ es completo.

b) $\hat{A}$ es R-plano, desde que $\hat{A}$ es A-plano y A es R-plano entonces $\hat{A}$ es R-plano.

c) i) $\hat{m} = m\hat{A} = (nA)\hat{A} = n\hat{A}$.

   ii) Se tiene que K es una extensión separable sobre (R/n) además $K \cong (A/m)$ y como $(A/m) \cong (\hat{A}/\hat{m})$ entonces tenemos $(\hat{A}/\hat{m}) \cong K$ y como K es separable sobre (R/n) entonces $\hat{A}/\hat{m}$ es separable sobre (R/n) entonces $(\hat{A}, \hat{m})$ es un R-álgebra de Cohen, la cual prueba el teorema.

□

Corolario 4.2.7. *(Teorema de Hasee - Schmidt)* Sea K un cuerpo de característica $p \geq 0$, entonces existe un anillo p-ádico de Cohen W tales que $K \cong W/pW$.

Demostración. Si $p = 0$, tomamos $W = K$. Ahora si $p > 0$, consideremos al anillo p-ádico de Cohen $(\Gamma_p, p\Gamma_p)$, luego tenemos que $\Gamma_p/p\Gamma_p = \mathbf{F}_p$ cuerpo primo de característica p, luego como $\mathbf{F}_p$ es perfecto, se tiene que $K/\mathbf{F}_p$ es separable, luego por el teorema (4.2.6) se tiene que existe un Γ_p-álgebra de Cohen (es decir, un anillo p-ádico de Cohen) W tal que $K \cong W/pW$. □

Lema 4.2.8. Sea $(S, n) \to (B, m)$ un homomorfismo local. Asumamos que S es artiniano (así n es nilpotente y la topología n-ádica sobre S es discreta) y que la topología m-ádica sobre B es discreta. Asumamos también que B es S-plano. Sea I un ideal de S tales que $I^2 = 0$ y B/IB es suave sobre S/I. Entonces B es suave sobre S.

La demostración puede ser vista en [4]. Q

Definición 4.2.9. Sea (A, m) un anillo local inequicaracterístico y sea $p = \mathbf{char}(A/m)$. Decimos que A es inramificado si $p \notin m^2$ y ramificado en otros casos.

Teorema 4.2.10. Sea $(R, n) \to (A, m)$ un homomorfismo local de anillos locales noetherianos. Donde R y A tienen la topología ádica del ideal maximal. Supongamos que A es R-plano, que nA es m-primario y que a sea un ideal n-primario de R. Si A/aA es suave sobre R/a, entonces A es formalmente suave sobre R.

Demostración. Sea un diagrama de homomorfismos de anillos que es conmutativo,

$$\begin{tikzcd}
(R, n) \arrow[r, "\phi"] \arrow[d, "w"'] & (A, m) \arrow[d, "u"] \arrow[dl, dashed, "v"'] \\
C \arrow[r, "\eta"'] & C/I
\end{tikzcd}$$

donde A es un R-álgebra, I es un ideal de C, C y C/I tienen la topología discreta, $I^2 = 0$, η el homomorfismo natural, u y w continuas. Tenemos que mostrar la existencia de v. Se tiene que w es continua, luego $w^{-1}(0)$ es una vecindad de cero en R y como R tiene la topología n-ádica, se tiene que $a^n \subset w^{-1}(0)$ para algún $n \geq 1$ por lo tanto, $u(a^nA) = 0$ y así obtenemos el siguiente diagrama conmutativo

$$\begin{tikzcd}
R \arrow[rr, "\phi"] \arrow[dr] \arrow[dd, "w"'] & & A \arrow[dd, "u"] \arrow[dr, "\xi"] \arrow[ddll, dashed, "v"'] & \\
& R/a^n \arrow[rr] \arrow[dl, "w_n"] & & A/a^nA \arrow[dl, "u_n"] \arrow[dlll, dashed, "v_n"'] \\
C \arrow[rr] & & C/I &
\end{tikzcd}$$

luego desde que R/a^n y A/a^nA son discretos, se tiene que w_n y u_n son continuas, luego por hipótesis tenemos que A/aA es suave sobre R/a, luego afirmamos que A/a^nA es suave sobre R/a^n, la demostración lo haremos por inducción sobre n. Si $n = 1$ el teorema se cumple por hipótesis, veamos para $n \geq 2$ y escribiendo $S = R/a^n$, $B = A/a^nA$ y $I = a^{n-1}/a^n$, luego cocientando con I obtenemos $S/I = R/a^{n-1}$ y $B/IB = A/a^{n-1}A$. Por hipótesis inductiva tenemos que B/IB es suave sobre S/I, entonces $B = A/a^nA$ es suave sobre $S = R/a^n$ por el Lema (4.2.8), de esta manera obtenemos el homorfismo v_n mostrado en la gráfica luego, tomando $v = v_n\xi$ conseguimos el homomorfismo deseado y de esta manera probamos que R es suave sobre A. □

Corolario 4.2.11. Sea $(R, n) \to (A.m)$ un homomorfismo local de anillos locales noetherianos tales que A es R-plano, $m = nA$ y A/m es separable sobre R/n. Entonces A es formalmente suave sobre R. En particular un R-álgebra de Cohen es formalmente suave sobre R.

Demostración. Desde que A/m es separable sobre R/n se tiene que A/m es formalmente suave sobre R/n y por el teorema (4.2.10) la prueba es inmediata. □

4.3. Caso inequicaracterístico

Teorema 4.3.1. *(Teorema de Estructura de Cohen - Caso inequicaracterístico).* Sea (A, m) un anillo local, noetheriano, completo, inequicaracterístico de dimensión d. Sea $p = \mathbf{char}(A/m)$, entonces existe una subanillo R de A y un anillo de valoración discreta W con parámetro regular p tal que:

(i) R es un anillo de coeficientes de A.

(ii) $R \cong W \vee R \cong W/p^m W$ para algún $m \geq 2$.

(iii) $A \cong W$¢$T_1, \dots, T_n$¢$/a$ para algún ideal a.

(iv) Si A es regular e inramificado entonces $A \cong W$¢$T_1, \dots, T_{d-1}$¢

(v) Si A es regular y ramificado entonces $A \cong W$¢$T_1, \dots, T_d$¢$/(f)$ para algún ideal principal (f) y el anillo W¢$T_1, \dots, T_d$¢ es inramificado.

En *(iii)*-*(v)*, $T_1, T_2, \dots$ son algebraicamente independientes sobre W.

Demostración. Prueba de (i). Sea $K = A/m$ el cuerpo residual de A. Tenemos que $\mathbf{char}(K) = p$, luego por el teorema de Hasse-Schmidt, existe un anillo p-ádico de Cohen W tal que $\frac{W}{pW} \cong K$, luego como W es un anillo p-ádico de Cohen tenemos el siguiente homomorfismo local $(\Gamma_p, p\Gamma_p) \to (W, pW)$ de anillos locales noetherianos. Luego por el corolario (4.2.11) tenemos que W es formalmente suave sobre Γ_p, así tenemos el siguiente diagrama

$$\begin{tikzcd} W \arrow[r, "j"] \arrow[dr, dashed, "\psi \circ j = u"'] & W/pW \arrow[d, "\psi"] \\ & K \end{tikzcd}$$

u es W-álgebra continua.

Sea $x \in pW$, luego $j(x) = \bar{x} = \bar{0} \Rightarrow \psi(j(x)) = \psi(\bar{0}) = 0_K \Rightarrow u(x) = 0_K$ entonces $u(pW) \subset \{0\}$, luego u es un W-álgebra local, por lo tanto se tiene que u es continua.

Por otro lado como W/Γ_p es suave, (A, m) es un anillo local, noetheriano y completo y $u\colon W \to K = A/m$ es un Γ_p-álgebra homomorfismo continuo, entonces por el lema (3.4.4)(ii) existe $v\colon W \to A$ un Γ_p-álgebra homomorfismo tal que $u = \eta v$ donde $\eta\colon A \to K$ es el homomorfismo natural, luego tenemos el siguiente diagrama

$$\begin{tikzcd} \Gamma_p \arrow[r] \arrow[d, no head] & W \arrow[d, no head, "u"] \arrow[dl, dashed, no head, "v"'] \\ A \arrow[r, "\eta"'] & K \end{tikzcd}$$

Luego $v(W) = R$ es un subanillo de A.

Afirmación: R es un anillo de coeficientes de A.

- $v(W) = R$ es un anillo local completo.

  Tenemos $v\colon W \to A$ (Γ_p-álgebra homomorfismo), luego por el Teorema fundamental del homomorfismo se tiene que $R = \mathbf{Im}(v) \cong \dfrac{W}{\ker(v)}$, luego como W es local completo y $\ker(v)$ es un ideal propio de W entonces por la observación anterior $\dfrac{W}{\ker(v)} = R$ es local y completo.

- $(R, n) \xrightarrow{i} (A, m)$ es local e induce un isomorfismo entre sus cuerpos residuales.

  Sea $x \in n$, luego $i(x) = x \in A$, luego tenemos que $x \in m \vee x \notin m$. Si $x \notin m$, entonces x es unidad, luego $x \notin n$ y esto es una contradicción, entonces $x \in m$. Es decir, i es local.

  Ahora veamos que $A/m \cong R/n$.

$$R/n \xrightarrow{j} A/m$$
$$\bar{x}_R \longmapsto \bar{x}_A$$

i) Como j es un homomorfismo de cuerpos y j es no nulo, pues $j(\bar{1}_R) = \bar{1}_A$, entonces j es inyectivo.

ii) Sea $\bar{x} \in A/m$, $\bar{x} \neq \bar{0}$, entonces $x \in (A - m)$, entonces x es unidad en A, luego x es unidad en R o x no es unidad en R. Si x no es unidad, en R, entonces $x \in n$, luego $x \in m$ y esto es una contradicción, por lo tanto x es unidad, es decir $x \in (R - n)$, luego existe $\bar{x}_R \in R/n$ tal que $j(\bar{x}_R) = \bar{x}_A$. Por lo tanto, j es sobreyectivo, entonces por el teorema fundamental del homomorfismo tenemos que

$$A/m \cong \frac{R/n}{\ker(j)} \cong \frac{R/n}{\{0\}} \cong R/n \Longrightarrow A/m = R/n$$

Nota: j es inyectivo desde que R/n es cuerpo y $A/m \neq \{0\}$.

- El ideal maximal de R es pR donde $p = \mathbf{char}(A/m)$.

Sea $\bar{x} \in R/pR$ con $\bar{x} \neq 0$, luego $x \notin pR$, entonces $x \in R \subset A$, luego $x \in m \vee x \notin m$. Si $x \in m$, $\bar{x} = \bar{0}$, entonces $x = py, \forall\ y \in A$ desde que $\mathbf{char}(A/m) = p$, pero si $y \in R$ tenemos $x \in pR$ y esto es una contradicción, luego $x \notin m$, entonces x es unidad, entonces existe $r \in A$ tal que $x.r = 1$, tomando clases tenemos $\bar{x}.\bar{r} = \bar{1}$, entonces $\bar{x}$ es unidad, entonces R/pR es un cuerpo, por lo tanto pR es ideal maximal de R.

Por lo tanto R es un anillo de coeficientes de A.

Nota: (W, pW) es un anillo p-ádico de Cohen, desde que $p > 0$ y por el lema (4.2.5), se tiene que W es un anillo de valoración discreta con parámetro regular p.

Prueba de (*ii*). Tenemos que existe $v : W \to A$ un Γ_p-álgebra homomorfismo luego por el Teorema Fundamental del homomorfismo tenemos $R \cong \dfrac{W}{\ker(v)}$; $\ker(v)$ ideal de W.

- Si $\ker(v) = 0 \Rightarrow R \cong \frac{W}{\{0\}} \cong W \Rightarrow R \cong W$
- Si $\ker(v) \neq 0 \Rightarrow R \cong \dfrac{W}{\ker(v)}$ y como todos los ideales de W son de la forma p^nW, luego $\ker(v) = p^nW$, para $n \geq 2$ pues si $n = 1$, R sería un cuerpo luego A sería equicaracterístico y esto no puede suceder puesto que A es inequicaracterístico.

Prueba de (*iii*). Tenemos:

$$v : (W, pW) \to (A, m) \quad \text{un } \Gamma_p\text{-álgebra homomorfismo}$$

- v es local.

Sea $x \in pW$, luego $v(x) \in A$, entonces $v(x) \in m \vee v(x) \not\in m$ pues A local, si $v(x) \not\in m$, entonces tenemos que $v(x)$ es unidad luego existe $r \in A$ tales que:

$$\begin{aligned} v(x).r &= 1 \\ \eta(v(x))\eta(r) &= \eta(1) && \text{como } u \text{ es local} \\ \overline{0} = u(x)\eta(r) &= \overline{1}_K && \text{esto es una contradicción} \end{aligned}$$

desde que $x \in pW$ y u es local, entonces $v(x) \in m$, por lo tanto v es local.

Entonces v es un homomorfismo local de anillos locales noetherianos completos que inducen un isomorfismo entre sus cuerpos residuales y sean $x_1, \dots, x_n \in m$ generadores del ideal m, luego por el Lema (4.1.3) tenemos que existe un único homomorfismo local de W-álgebra

$$\theta : W[[T_1, \dots, T_n]] \to A \text{ tales que } \theta(T_i) = x_i \quad \forall\, i$$

y desde que $m \subset \underbrace{\theta(pW)}_{\in m} A + \underbrace{(x_1, \dots, x_n)}_{\in m} A \subset m \Rightarrow m = \theta(pW)A + (x_1, \dots, x_n)A$, por el teorema (4.1.3)(2), θ es sobreyectivo, luego aplicando el teorema fundamental del homomorfismo tenemos que $A \cong \dfrac{W[[T_1, \dots, T_n]]}{\ker(\theta)}$.

Prueba de (*iv*). Como A es regular e inramificado, se tiene que $p \in m$ y $p \not\in m^2$, entonces p es un generador de m, luego $(p, x_1, \dots, x_{d-1})$ es un sistema regular de parámetros de A, por el lema (4.1.3) tenemos que existe un homomorfismo de W-álgebra suryectivo $\theta : W[[x_1, \dots, x_{d-1}]] \to A$, por el teorema fundamental del homomorfismo tenemos

$$A \cong \frac{W[[T_1, \dots, T_{d-1}]]}{\ker(\theta)}$$

como W es noetheriano y W es un dominio de valoración discreta, la dim $W = 1$, entonces la dim $W[[T_1, \dots, T_{d-1}]] = d$, comparando dimensiones se tiene que $ht(\ker(\theta)) = 0$. Entonces $A \cong W[[T_1, \dots, T_{d-1}]]$.

Prueba de (*v*). Ahora A es regular y ramificado. Como A es regular y $\dim A = d$ tenemos que $n = d$ en (*iii*) y $p \in m^2$ desde que A es ramificado, entonces p no es generador de m, luego tenemos que $\{x_1, \dots, x_d\}$ es un sistema de generadores de A, por el lema (4.1.3) tenemos que existe un único homomorfismo suryectivo de W-álgebra $\theta : W[[T_1, \dots, T_d]] \to A$, por el teorema fundamental homomorfismo tenemos

$$A \cong \frac{W[[T_1, \dots, T_d]]}{\ker(\theta)},$$

desde que A es regular y local tenemos que A es un dominio de integridad, entonces $\frac{W[[T_1, \dots, T_d]]}{\ker(\theta)}$ es un dominio, luego $\ker(\theta)$ es un ideal primo de $W[[T_1, \dots, T_d]]$, comparando dimensiones tenemos $ht(\ker(\theta)) = 1$. Queremos aplicar teorema (1.8.3):

Nos faltaría ver que $W[[T_1, \dots, T_d]]$ sea D.F.U., puesto que $W[[T_1, \dots, T_d]]$ ya es noetheriano y dominio (puesto que W lo es), para ver esto aplicaremos el teorema (1.8.6).

Veamos que $W[[T_1, \dots, T_d]]$ es local, como W es de valoración discreta los únicos ideales de W son (0) y potencias del ideal maximal. Como W es local, el único ideal maximal sería (pW), luego sus ideales son (0) y p^nW, los ideales de $W[[T_1, \dots, T_d]]$ serían el (0) y $p^nW[[T_1, \dots, T_d]]$, el ideal maximal de $W[[T_1, \dots, T_d]]$ sería $pW[[T_1, \dots, T_d]]$ y es el único por lo tanto $W[[T_1, \dots, T_d]]$ es local y como W es regular entonces $W[[T_1, \dots, T_d]]$ es regular.

Por lo tanto $W[[T_1, \dots, T_d]]$ es D.F.U. entonces $\ker(\theta)$ es principal.

Luego para terminar de probar (v), tendríamos que probar que $W[[T_1, \dots, T_d]]$ es inramificado.

El ideal maximal de $W[[T_1, \dots, T_d]]$ es $(p, T_1, \dots, T_d)$, luego $\{p, T_1, \dots, T_d\}$ es un sistema regular de parámetros de $W[[T_1, \dots, T_d]]$, tenemos que $\textbf{char}(\frac{W[[T_1, \dots, T_d]]}{(p, T_1, \dots, T_d)}) = p$; $p \in (p, T_1, \dots, T_d)$ y $p \notin (p, T_1, \dots, T_d)^2$, por lo tanto $W[[T_1, \dots, T_d]]$ es inramificado. $\square$

Capítulo 5

Aplicaciones

En este capítulo veremos una versión muy especializada acerca del teorema de estructuras para anillos locales completos. Además, veremos que dado $f \in \mathcal{O}_{V,p}$ el anillo de funciones regulares en un punto liso $p \in V$ (Variedad), se le asocia su serie de Taylor en el anillo de series formales de potencia.

5.1. Estructura principal de anillos de ideales principales

Nuestro objetivo principal es probar que cualquier anillo de ideales principales es una suma directa de anillos, donde cada uno de los cuales es imagen homomorfica de un dominio de ideales principales. Tengamos presente que un anillo de ideales principales no es un dominio de integridad.

Proposición 5.1.1. Sea R un anillo local cuyo ideal maximal M es principal $M = (a)$, entonces R es un anillo de ideales principales y todo elemento no nulo de R puede escribirse de la forma $a^k u$, con u unidad.

Demostración. Sea $x \in R$, luego desde que $\cap(a^i) = 0$, existe una máxima potencia dividiendo x, esto es $x = a^k u$, veamos que u es unidad, supongamos que u no es unidad, entonces $u \in M = (a)$, lo cual implica que $a|u$, luego $a.a^k|ua^k$, entonces $a^{k+1}|x$, esto es una contradicción, pues la máxima potencia que divide x es a^k, entonces u es unidad. Sea I un ideal de R, como todo elemento de I puede escribirse de la forma $a^i u$, donde u es unidad, podemos elegir un elemento minimal i, como todo x en I es de la forma $x = a^k u = a^i a^{k-i} u$, entonces tenemos que $I = (a^i)$. □

Definición 5.1.2. Un v-anillo es un anillo D tal que D es un dominio de integridad local, completo de característica cero, cuyo ideal maximal N es generado por p, donde $p \neq 0$ es la característica del cuerpo residual D/N.

Observación. Por la proposición anterior se tiene que D es un DIP.

El siguiente resultado es un caso particular del teorema de estructura para anillos locales debido a Cohen.

Teorema 5.1.3. Sea R un anillo local completo cuyo ideal maximal M es principal, $M = (a)$. Entonces R es la imagen homomórfica de $D[[X]]$, que envía $X \in D[[X]]$ hacia $a \in R$, donde D es el cuerpo R/M (Si **char** R = **char** R/M), o D es un v-anillo cuyo cuerpo residual $D/(p)$ es naturalmente isomorfo a R/M (si **char** $R \neq$ **char** R/M).

Demostración. Por la proposición 5.1.1, tenemos que R es un anillo de ideales principales, entonces R es noetheriano, por lo tanto tenemos que (R, M) es un anillo local, noetheriano y completo.
Supongamos que (R, M) es un anillo equicaracterístico, entonces por el teorema 4.1.1 parte (1) se tiene que existe $K' = v(K)$ cuerpo de coeficientes de R, donde $K = \frac{R}{M}$ y $v : K \to R$ (homomorfismo), luego tenemos el homomorfismo local $(K', 0) \to (R, M)$ entre anillos locales, noetherianos y completos que inducen un isomorfismo entre sus cuerpos residuales (probado en el teorema 4.1.1) y como $M = (a)$ por el lema 4.1.3 parte (1) se tiene que existe un único homomorfismo de K'-álgebra $\theta : K'[[x]] \to R$ tal que $\theta(x) = a$ y como $M = \theta(0)R + (a)R$, aplicando la parte (2) del lema 4.1.3 tenemos que θ es sobreyectivo, luego

$$R = \theta(K'[[x]])$$
$$R = \theta(v(K)[[x]])$$
$$R = \theta(v(K[[x]]))$$
$$R = \theta \circ v(K[[x]])$$

Entonces R es la imagen homomórfica de $K[[x]]$. □

Para el caso inequicaracterístico la demostración es análoga, en este caso aplicando el teorema 4.3.1 y lema 4.1.3.

Definición 5.1.4. *Un anillo R de ideales principales es especial si R tiene un único ideal primo y este es nilpotente.*

Desde que todo anillo de ideales principales es noetheriano y como los ideales maximales son primos, tenemos que un anillo de ideales principales especial es local, además la nilpotencia del ideal maximal implica que toda sucesión de Cauchy es eventualmente constante y por lo tanto convergente. Entonces tenemos que anillos de ideales principales especial es un anillo local y completo.

Definición 5.1.5. Se dice que el anillo R es la suma directa de ideales $R_1, R_2, \ldots, R_n$ si:

1. $R = R_1 + R_2 + \cdots + R_n$.

2. $R_i \cap (R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n) = (0)$; $i = 1, \ldots, n$.

Escribiremos

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n, \tag{5.1}$$

notemos que los ideales en (5.1) se anulan mutuamente, esto es $R_iR_j = (0)$ para $i \neq j$, se sigue que $R_iR_j \subset R_i \cap R_j = (0)$ para $i \neq j$. Por lo tanto un ideal en R_i (considerando R_i como anillo) es también un ideal en R.

Definición 5.1.6. Sea R un anillo con identidad. A un conjunto de ideales $u_1, u_2, \ldots, u_n$ en R, se dice que son comaximales dos a dos si cada $u_i \neq R$ y $u_i + u_j = R$ para cada $i \neq j$. Si $n = 2$, decimos simplemente que u_1 y u_2 son comaximales.

La definición implica que $u_i \neq u_j$, para $i \neq j$ y también $u_i \neq 0$.

Teorema 5.1.7. Sea R un anillo con identidad. Sea $u_1, \ldots, u_n$ ideales tales que:

1. $u_1 \cap u_2 \cap \cdots \cap u_n = (0)$.

2. $u_i + u_j = R$, para $i \neq j$.

y si $R_i = u_1 \cap \cdots \cap u_{i-1} \cap u_{i+1} \cap \cdots \cap u_n$, $i = 1, \ldots, n$ entonces

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n; \quad R_i \cong R/u_i$$

$u_i = R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n$.
La demostración puede ser vista en [5]. $\square$

Teorema 5.1.8. La suma directa de anillos de ideales principales es un anillo de ideales principales.

Demostración. Sea R un anillo tales que $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$, donde cada R_i es un anillo de ideales principales.

Sea I un ideal de R, entonces $I = RI = R_1I + R_2I + \cdots R_nI$, luego desde que cada R_iI es un ideal en R_i se tiene que $R_iI = R_ix_i$; $x_i \in R_i$, $1 \leq i \leq n$, entonces se tiene que $I = R(x_1 + x_2 + \cdots + x_n)$, de esta manera R es un anillo de ideales principales. □

Lema 5.1.9. Sea R un anillo de ideales principales, si q y q' ideales primos tal que $q' \subset q \subset R$, entonces q no contiene otros ideales primos que q y q' y cualquier ideal primario contenido en q contiene q'. Dos ideales primos en R son ambos comaximales o uno de ellos contiene al otro.

La demostración puede ser vista en [5]. Q

Lema 5.1.10. Si R es un anillo de ideales principales, R es la suma directa de dominios de ideales principales y de anillos de ideales principales especial.

Demostración. Como R es un anillo de ideales principales, R es noetheriano, luego ideal de R tiene una descomposición primaria, en el caso del ideal (0) este tiene una descomposición primaria minimal, es decir $(0) = \bigcap_{i=1}^{n} q_i$ y sea $r(q_i) = p_i$, donde los p_i son los menores ideales primos que contienen a q_i, luego por el Lema (5.1.9) tenemos que los ideales de p_i son dos a dos comaximales, pues si no lo fuesen tendríamos que uno de ellos contiene al otro, es decir $p_i \subset p_j$ luego como p_i no es maximal no tiene ideales primarios propios pero $q_i \subset p_i$ entonces tendríamos que $p_i = q_i$, luego como todo ideal primario de p_j contiene a p_i, entonces $q_i \subset q_j$ y esto es una contradicción a la minimalidad de la descomposición primaria. Por lo tanto, p_i y p_j son comaximales y de esto resulta que los ideales q_i son también dos a dos comaximales, luego por el Teorema (5.1.8) se tiene que R es una suma directa de anillos respectivamente isomorfos a los anillos R/q_i es decir: $R = \frac{R}{q_1} \oplus \frac{R}{q_2} \oplus \cdots \oplus \frac{R}{q_n}$ luego cada $\frac{R}{q_i}$ es un anillo de ideales principales y si p_i es maximal, entonces q_i no está contenido en otro ideal primo que p_i, así R/q_i tiene un solo ideal primo y sea p_i/q_i por lo tanto es un anillo de ideales principales especial y si p_i no fuera maximal tendríamos que $p_i = q_i$ y R/q_i sería un DIP. □

Teorema 5.1.11. Si A es un anillo de ideales principales, A es suma directa de anillos, donde cada uno de los cuales es la imagen homomórfica de un dominio de ideales principales.

Demostración. Por el Lema (5.1.10) tenemos que todo anillo es la suma directa de un DIP y de un anillo de ideales principales especial, entonces el teorema quedaría probado si obtenemos que cualquier anillo de ideales principales especial es imagen homomórfica de un D.I.P.

Sea R un anillo de ideales principales especial que es local y completo cuyo ideal maximal $M = (a)$, luego por el Teorema (5.1.3), tenemos que R es la imagen homomórfica de $D[[x]]$, donde D es un cuerpo o D es un v-anillo. Si D es cuerpo entonces $D[[x]]$ es un DIP y ya estaría probado. Si D es un v-anillo, $D[[x]]$ no es un DIP, entonces para completar la demostración debemos mostrar que cuando D es un v-anillo R es la imagen homomórfica de un DIP.

Como $D[[x]]$ es la imagen homomórfica de R tenemos el siguiente epimorfismo de anillos $\phi : D[[x]] \to R$ tales que $\phi(x) = a$, luego como D es un v-anillo tenemos por el Teorema (5.1.3) que $\mathbf{char}(A) \neq \mathbf{char}(R/M) = \mathbf{char}(D/(p)) = p \neq 0$, entonces $p \in R$ y p es no nulo y no unidad, luego desde que R es local con ideal maximal $M = (a)$ principal, entonces $p = a^k u$, donde $k > 0$, u es unidad en R, como ϕ es sobreyectivo existe $c \in D[[x]]$ tales que $\phi(c) = u$, luego tenemos el elemento $f = -cx^k + p \in D[[x]]$ tal que $\phi(f) = \phi(-cx^k + p) = -ua^k + p = -ua^k + a^k u = 0$ pertenece al $\ker(\phi)$, así mismo desde que el término constante de f es p, el cual es irreducible en D, se tiene que f es irreducible en $D[[x]]$, veamos que f es irreducible.

$$f = -cx^k + p,$$

tomemos p tales que:

- $p \mid p$
- $p \nmid c$

Supongamos que $p|c$, luego existe $r \in D$ tales que $p.r = c$, luego:

$$\begin{aligned} \phi(p)\phi(r) &= \phi(c) \\ p.\phi(r) &= u \\ p.\underbrace{\phi(r)u^{-1}}_{q} &= 1 \\ pq &= 1 \end{aligned}$$

entonces p es unidad, y esto es una contradicción, por lo tanto $p \nmid c$.

- $p^2 \nmid p$

Luego por el criterio de Eiseinstein, se tiene que f es irreducible.

Como D es un v-anillo, tenemos que $D[[x]]$ es un dominio de factorización única, como f es irreducible, f es primo, luego (f) es un ideal primo así tenemos que $\dfrac{D¢x¢}{(f)}$ es un dominio de integridad, tenemos el siguiente diagrama:

$$\begin{tikzcd} D¢x¢ \arrow[rr, "\phi"] \arrow[dr, "n"'] & & R \\ & \dfrac{D¢x¢}{(f)} \arrow[ur, "\psi"'] & \end{tikzcd}$$

- ψ es sobreyectivo

Sea $r \in R$, luego como ϕ es sobreyectivo, existe $q \in R¢x¢$ tales que $\phi(q) = r$, luego existe $n(q) = \bar{q} \in \frac{D¢x¢}{(f)}$ tal que $r = \phi(q) = \psi(n(q)) = \psi(\bar{q})$, por lo tanto ψ es sobreyectiva.

Ya tenemos que R es imagen homomórfica de $\frac{D¢x¢}{(f)}$, nos faltaría probar que $\frac{D¢x¢}{(f)}$ sea DIP.

Tenemos que $\phi(x) = a$, luego $n(x) = \bar{x}$, entonces $\psi(\bar{x}) = a$, el cual no es unidad en R entonces $\bar{x}$ no es unidad en $\frac{D¢x¢}{(f)}$, por lo tanto $(\bar{x})$ es un ideal propio de $\frac{D¢x¢}{(f)}$.

Desde que $\bar{f} = \overline{-cx^k + p} = \overline{-cx^k} + \bar{p} = 0$, entonces $\bar{p} \in (\bar{x})$.

Ahora sea $\bar{h}$ no unidad en $\frac{D¢x¢}{(f)}$, entonces h no es unidad en $D¢x¢$, entonces el término constante de h es no unidad en D, desde que (p) es el ideal de todas las no unidades en D, se tiene que el término constante de h pertenece a (p), entonces tenemos $h = t + s$, $t \in (x)$, $s \in (p)$, luego $\bar{h} = \bar{t} + \bar{s}$; $\bar{t} \in (\bar{x})$, $\bar{s} \in (\bar{p})$ y desde que $(\bar{p}) \subseteq (\bar{x})$ se tiene que $\bar{h} \in (\bar{x})$, entonces $(\bar{x})$ contiene todas las no unidades de $\frac{D¢x¢}{(f)}$, entonces $\frac{D¢x¢}{(f)}$ es local con ideal maximal principal $(\bar{x})$, entonces $\frac{D¢x¢}{(f)}$ es un DIP, por lo tanto hemos probado que todo anillo es suma directa de anillos donde cada uno de ellos es imagen homomórfica de un DIP. □

5.2. Expansión en serie de potencias

Sea $V \subseteq A^n_K$ una variedad algebraica, $K[V]$ el anillo de coordenadas de V, $K[V]$ es un dominio de integridad desde que V es una variedad algebraica. Al cuerpo de fracciones de $K[V]$ se le denomina el campo de funciones de V y lo denotamos como $K(V)$, cuyos elementos son llamados funciones racionales en V.

$$K(V) = \{g/h : g, h \in K[V] \wedge h \neq 0\}$$

Sea $f \in K(V)$, se dice que f es regular en $p \in V$, si $f = g/h$, $g, h \in K[V]$ con $h(p) \neq 0$.

A las funciones regulares en $p \in V$, las agruparemos y la denotaremos como:

$$\mathcal{O}_{V,p} = \{f \in K(V) : f \text{ es regular en } p\}$$

$\mathcal{O}_{V,p}$ es un subanillo de $K(V)$ y es un anillo local y noetheriano cuyo ideal maximal es $m_p = \{\phi \in \mathcal{O}_{V,p} : \phi(p) = 0\}$.

Lema 5.2.1. Si $V \subset \mathbf{A}^n_k$ es una variedad algebraica afín, $p \in V$ y $m_p \subseteq K[V]$ ideal maximal del conjunto de funciones polinomiales que se hacen cero en p. Se tiene que $\mathcal{O}_{V,p} \cong K[V]_{m_p}$.

Demostración. Definimos

$$\begin{aligned} \psi : \mathcal{O}_{V,p} &\dashrightarrow K[V]_{m_p} \\ g/h &\longrightarrow \psi(g/h) = [g,h]; \quad h \not\in m_p \end{aligned}$$

donde claramente, ψ es un isomorfismo. □

Gérmenes. Sea $V \subseteq \mathbf{A}^n_k$ una variedad algebraica y p un elemento de V, si g/h es un elemento de $\mathcal{O}_{V,p}$, la funcion racional g/h es regular en el abierto distinguido $D(h) = \{p \in \mathbf{P}^n_k : h(p) \neq 0\}$. Por el lema (5.2.1) para $g/h \in \mathcal{O}_{V,p}$, lo puedo ver como una clase $[g,h] \in K[V]_{m_p}$, los elementos de esta clase son pares ordenados (g,h) que pertenecen a $K[V]\times(K[V]-m_p)$, tal que se cumple la siguiente relación de equivalencia $(g,h) \sim (g', h')$ si y solo si existe $r \in K[V] - m_p$ tal que $r(gh' - hg') = 0$. Es decir el conjunto de pares ordenados (s,U), donde U es una vecindad abierta de p y $s \in \mathcal{O}_V(U)$[1], se define la relación $(s,U) \sim (s', U')$ si y solo si existe una vecindad abierta U'' de p tal que $U'' \subset U$ y $U'' \subset U'$ y $s|_{U''} = s'|_{U''}$, esta relación es de equivalencia. Las clases $[s,U]$ reciben el nombre de gérmenes de funciones regulares en p. Dos gérmenes son iguales si y solo si coinciden en una vecindad.

Parámetros locales. Sea V una variedad algebraica, p un punto liso de V y sea d la dimensión de V. Un sistema local de parámetros en p es un conjunto $\{f_1, f_2, \ldots, f_d\}$ de gérmenes que generan el ideal maximal m_p de $\mathcal{O}_{V,p}$.

Proposición 5.2.2. Sea p un punto liso de V y $\{f_1, f_2, \ldots, f_d\}$ un sistema local de parámetros en p. Por lo tanto existe una vecindad abierta U de p tal que los gérmenes $\{f_1, f_2, \ldots, f_d\}$ son representados por pares $(\tilde{f}_1, U), (\tilde{f}_2, U), \ldots, (\tilde{f}_d, U)$, tal que $f = (\tilde{f}_1, \ldots, \tilde{f}_d) : U \to \mathbf{A}^d_K$ es un morfismo étale.

La demostración puede ser vista en [6]. □

[1] Sea $U \subseteq V$ abierto, denotaremos por $\mathcal{O}_U$ al conjunto de funciones regulares definidas en U, por lo tanto $\mathcal{O}_U = \bigcap_{p\in U} \mathcal{O}_{V,p}$.

Sea V una variedad algebraica de dimensión n, $p \in V$ y f un elemento de $\mathcal{O}_{V,p}$, luego haciendo

$$f(p) = a_0$$

$$f_1 = f - a_0 \,,$$

tenemos que $f_1 \in m_p$, pues $f_1(p) = 0$. Sean $u_1, \ldots, u_n \in m_p$ parámetros locales en p, entonces sus clases laterales $u_i + m_p^2$ generan el espacio vectorial m_p/m_p^2. Entonces para $f_1 \in m_p$ existen $a_1, \ldots, a_n \in K$, tal que

$$f_1 + m_p^2 = \sum_{i=1}^{n} a_i u_i (\textbf{mod } m_p^2),$$

entonces tenemos $f_1 - \sum_{i=1}^{n} a_i u_i \in m_p^2$, hagamos entonces:

$$f_2 = f_1 - \sum_{i=1}^{n} a_i u_i = f - a_o - \sum_{i=1}^{n} a_i u_i$$

luego como $f_2 \in m_p^2$, podemos escribir $f_2 = \sum_j g_j h_j$, con $g_j, h_j \in m_p$.

Como $g_j, h_j \in m_p$, haciendo lo mismo que con $f_1 \in m_p$, tenemos:

$$g_j - \sum_{k=1}^{n} b_{jk} u_k \in m_p^2 \quad \text{y} \quad h_j - \sum_{k=1}^{n} c_{jk} u_k \in m_p^2$$

luego

$$f_2 = \sum_j g_j h_j = \sum_j \Big(\sum_k b_{jk} u_j\Big)\Big(\sum_k c_{jk} u_j\Big) = \sum_{1 \le s,t \le n} a_{st} u_s u_t$$

con $a_{st} \in K$, por lo tanto

$$f_2 - \sum_{s,t} a_{st} u_s u_t \in m_p^2,$$

de esta manera encontramos polinomios homogéneos $F_i \in K[x_1, x_2, \ldots, x_n]$ de grados $\textbf{gr } F_i = i$ tales que

$$f - \sum_{i=0}^{k} F_i(x_1, \ldots, x_n) \in m_p^{k+1}$$

luego, a f que pertenece a $\mathcal{O}_{V,p}$ se le puede escribir como una serie de potencias $f = F_0 + F_1 + F_2 + \cdots$ tal que para sumas parciales

$$S_k = \sum_{i=1}^{k} F_i$$

se verifica que al evaluar la diferencia en $(u_1, \ldots, u_n)$ tenemos que $f - S_k(u_1, \ldots, u_n) \in m_p^{k+1}$, por lo tanto la serie anterior es una serie de Taylor para

f.

Para $\mathcal{O}_{V,p}$ y $m_p \subset \mathcal{O}_{V,p}$, tenemos la filtración m_p-ádica $\{m_p^k\}$, tales que

$$m_p^{k+1} \subseteq m_p^k, \text{ para } k \geq 0.$$

Esta filtración es una base de vecindades del cero que pertenece a $\mathcal{O}_{V,p}$; con lo cual dotamos de una topología a este anillo, que es compatible con las operaciones del anillo. Como el anillo $\mathcal{O}_{V,p}$ es noetheriano, tenemos que $\cap_{k\geq 0} m_p^k = 0$, luego la topología es de Hausdorff. Definimos:

$$\begin{aligned} \nu : \mathcal{O}_{V,p} &\longrightarrow \mathbb{N} \cup \{0\} \\ f &\longrightarrow \nu(f) = \begin{cases} k, & \text{si } f \in m_p^k \text{ y } f \notin m_p^{k+1} \\ \infty, & \text{si } f = 0 \end{cases}, \end{aligned}$$

tal que se verifica

(i) $\nu(f-g) \geq \text{mín}\{\nu(f), \nu(g)\}$

(ii) $\nu(f.g) \geq \nu(f) + \nu(g)$

(iii) $m_p^k = \{f \in \mathcal{O}_{V,p} : k \leq \nu(f)\}$

Observación:
De las propiedades *(i)* y *(ii)* obtenemos que ν es una valoración en $\mathcal{O}_{V,p}$ y de *(iii)* obtenemos que la filtración se recupera de la valoración.

Sea e número real tal que $0 < e < 1$, definimos una métrica en el anillo $\mathcal{O}_{V,p}$

$$d(f,g) = e^{\nu(f-g)}$$

y esta es una ultramétrica, pues satisface

$$d(f,g) \leq \text{máx}\{d(f;h), d(h;g)\} \qquad \forall\ h \in \mathcal{O}_{V,p}$$

Con esta métrica podemos definir el límite de sucesiones y sucesiones de Cauchy en el anillo $\mathcal{O}_{V,p}$. Podemos completar $\mathcal{O}_{V,p}$ mediante la convergencia de las sucesiones de Cauchy en este anillo, el cual denotaremos por $\hat{\mathcal{O}}_{V,p}$ con la topología m_p-ádica.

La elección de parámetros $u_1, u_2, \ldots, u_n \in m_p$ en un punto liso p induce, por la proposición (5.2.2), un morfismo:

$$\mathcal{O}_{V,p} \longrightarrow K[x_1, \ldots, x_n]$$

que proviene de un morfismo étale[2]:

$$(\tilde{u}_1, \tilde{u}_2, \dots, \tilde{u}_n) \colon U \longrightarrow \mathbb{A}^n_K$$

donde U es una vecindad abierta y lisa de p.

El morfismo $\mathcal{O}_{V,p} \longrightarrow K[x_1, \dots, x_n]$ envía el ideal maximal m_p en el ideal maximal M_p, luego lo podemos ver como

$$\mathcal{O}_{V,p} \longrightarrow K[x_1, \dots, x_n]_{M_p}$$

el cual es un morfismo de anillos locales. Pasando a las completaciones correspondientes tenemos el siguiente morfismo

$$\hat{\mathcal{O}}_{V,p} \longrightarrow K[[x_1, \dots, x_n]],$$

donde usamos que la completación de $K[x_1, \dots, x_n]$ en $(x_1, \dots, x_n)$ es el anillo de series de potencia formales $K[[x_1, \dots, x_n]]$ donde sus elementos son de la forma

$$F = \sum a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n}, \qquad i_j \geq 0$$

y los coeficientes $a_{i_1,\dots,i_n} \in K$.

Tenemos que la elección de los parámetros locales $u_1, u_2, \dots, u_n \in m_p$ en p (punto liso) induce un morfismo

$$\hat{\mathcal{O}}_{V,p} \longrightarrow K[[x_1, \dots, x_n]],$$

que componiendo con $\mathcal{O}_{V,p} \hookrightarrow \hat{\mathcal{O}}_{V,p}$ nos da el siguiente morfismo

$$\Phi \colon \mathcal{O}_{V,p} \longrightarrow K[[x_1, \dots, x_n]]$$

tal que para $f \in \mathcal{O}_{V,p}$, $\Phi(f)$ es la serie de Taylor asociada a f. Desde que p es liso implica que la serie de Taylor asociada a f es única, que es equivalente a que Φ es inyectivo,

$$\ker \Phi = \{f \in \mathcal{O}_{V,p} : f - \sum_{j=0}^{k} F_j(u_1, u_2, \dots, u_n) \in m_p^{k+1}, \ \forall\, k \geq 0\} = \bigcap_{k\geq 0} m_p^k$$

luego $\bigcap_{k\geq 0} m_p^k = 0$ puesto que $\mathcal{O}_{V,p}$ es noetheriano, luego hemos probado el siguiente resultado

Teorema 5.2.3. Sea V una variedad, $\dim V = n$ y $p \in V$ un punto liso, entonces existe

$$\psi \colon \mathcal{O}_{V,p} \longrightarrow K[[x_1, \dots, x_n]]$$

morfismo inyectivo, donde si $f \in \mathcal{O}_{V,p}$, $\psi(f)$ es la serie de Taylor asociada a f.

[2] Sea V, W variedades afines lisas, la aplicación regular $f \colon V \to W$ es un morfismo étale en $p \in V$ si $df_p \colon T_pV \to T_{f(p)}W$ es un isomorfismo.

Bibliografía

[1] M. F. Atiyah and I. G. Macdonald, *Introducción al álgebra conmutativa*. Reverté, 1973.

[2] H. Matsumura, *Commutative ring theory*. Cambridge university press, 2000.

[3] F. Zaldivar, *Introducción al álgebra conmutativa*. México, 2011.

[4] B. Singh, *Completion, formal smoothness and Cohen structure theorems*.

[5] O. Zariski and P. Samuel, *Commutative algebra*. Springer Science & Business Media, 1965.

[6] F. Zaldivar, *Notas de geometría algebraica*.