UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

TESIS

ÁLGEBRA LOCAL Y ALGORITMOS

PARA OBTENER EL TÍTULO DE:

Maestro en Matemática Fundamental

Director:
María Emilia Alonso García

Presentado por:
Mario Alexis Ruiz Mejía

Abril 2017

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSc. Roger Armando Arias

VICE-RECTOR ADMINISTRATIVO INTERINO:

Dr. Manuel de Jesús Joya

SECRETARIO GENERAL:

MSc. Cristobal Ríos

FISCAL GENERAL:

Licda. Beatriz Mélendez

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

DECANO:

Lic. Mauricio Hernán Lovo Córdova

VICE-DECANO:

Lic. Carlos Antonio Quintanilla Aparicio

SECRETARIA:

Licda. Damaris Melany Herrera Turcios

ESCUELA DE MATEMÁTICA

DIRECTOR DE ESCUELA:

Dr. José Nerys Funes Torres

ASESOR:

Dra. María Emilia Alonso García (Universidad Complutense de Madrid)

Índice

Introducción

En la literatura clásica sobre anillos locales y anillos henselianos, la henselización de un anillo local, se construye como límite inductivo sobre la familia de anillos que resulta "extendiendo" el anillo base con raíces simples de polinomios.
El interés de estudiar en geometría la henselización R^h de un anillo local $(R, \mathfrak{m}, \kappa)$, es que para el caso $\kappa = \mathbb{R}$ ó $\mathbb{C}$, las propiedades analíticas de las variedades algebraicas en un punto se pueden estudiar en el anillo henseliano R^h, que se encuentra comprendido entre el anillo R y su completado $\hat{R}$: $R \subset R^h \subset \hat{R}$. Este anillo R^h tiene la característica de ser el "más pequeño" donde el Teorema de la Función Implícita (TFI) se verifica.
El objetivo es hacer efectivo el teorema que llamamos de representación, el cual permite hacer división en anillos henselianos en sentido débil pues no hay unicidad. La demostración se hace aplicando técnicas y herramientas computacionales, la cual permite formular un algoritmo. Terminamos nuestro trabajo, explicando en un ejemplo particular cómo se aplica el algoritmo formulado.

1. La Henselización en geometría algebraica

Este capítulo se desarrolla en el contexto del apéndice A e inicia (§1.I) con el concepto planitud para álgebras, luego (§1.II) se construye la henselización R^h de anillos locales como el límite inductivo sobre la familia de anillos que resulta de adjuntar "raíces simples de polinomios de una variable a R". Finalmente (§1.III) explicamos que la henselización R^h de un anillo local es también el límite de álgebras de Hensel. Este resultado es el Lema de Hensel Multivariado (LHM) del cual damos el esquema de una demostración para un caso particular, a saber: el anillo $R = \kappa[X_1, \ldots, X_n]_{\langle X_1,\ldots,X_n\rangle}$, la demostración del caso más general se encuentra en [1]. Finalmente ilustramos con un ejemplo la dificultad de asociar explícitamente *o constructivamente* a un código de Hensel multivariado un código univariado.

1.I. Álgebras planas y fielmente planas

El concepto de planitud fue introducido en álgebra conmutativa por Serre en los años 1950, en esta sección damos nuestra definición (efectiva) de álgebra plana y álgebra fielmente plana, que es equivalente a la que se encuentra en los libros de textos.
Intuitivamente hablando, una R_1-álgebra R_2, es plana sobre R_1 si los sistemas lineales de ecuaciones homogéneas sobre R_1 no tienen "más" soluciones en R_2 que las que tienen en R_1, y es fielmente plano cuando esta afirmación también se verifica para sistemas de ecuaciones lineales no homogéneos.

(1.1) DEFINICIÓN: Sea $\varphi : R_1 \to R_2$ una R_1-álgebra.

1. El álgebra R_2, diremos que es **plana** (sobre R_1) cuando cualquier relación de dependencia R_2-lineal entre elementos de R_1 es una combinación R_2-lineal de relaciones de dependencia R_1-lineales entre estos mismos elementos.

   En otras palabras, para $a_1, \ldots, a_n \in R_1$ y cualesquiera aplicaciones lineales

   $$\begin{array}{lll} \alpha : R_1^n \to R_1 & & \text{y} \quad \alpha_* : R_2^n \to R_2 \\ \quad \boldsymbol{x} \mapsto \alpha(\boldsymbol{x}) := a_1x_1 + \ldots + a_nx_n & & \quad \boldsymbol{y} \mapsto \alpha_*(\boldsymbol{y}) := \varphi(a_1)y_1 + \ldots + \varphi(a_n)y_n, \end{array}$$

   se tiene que $\ker \alpha_* = \langle \varphi(\ker \alpha)\rangle_{R_2}$.

   Se dice también que el anillo R_2 es plano sobre R_1 o que φ es un homomorfismo plano.

2. Sea R_2 un R_1-álgebra plana, diremos que es **fielmente plana** si para cualquier aplicación lineal $\alpha : R_1^n \to R_1$ y todo $r \in R_1$, si la ecuación lineal $\alpha_*(\boldsymbol{y}) = \varphi(r)$ tiene una solución en R_2^n, entonces la ecuación lineal $\alpha(\boldsymbol{x}) = r$ tiene una solución en R_1^n.

   Se dice también que el anillo R_2 es fielmente plano sobre R_1 o que φ es un homomorfismo fielmente plano.

(1.2) OBSERVACIONES:

1. Si R_2 es fielmente plano sobre R_1, entonces R_2 es plano sobre R_1.

2. Si R_2 es un R_1-álgebra fielmente plana, del caso $n = 1$ y $\alpha = 0$, se deduce que si $\alpha_*(y) = \varphi(r) = 0$ tiene solución en R_2, entonces $0 = \alpha(x) = r$ tiene una solución en R_1, esto comprueba que φ es un homomorfismo inyectivo, esto permite identificar R_1 como subanillo de R_2. Aún más, si $\varphi(a_1)$ divide a $\varphi(a_2)$ en R_2 entonces a_1 divide a a_2 en R_1 y si $\varphi(u) \in R_2^\times$ entonces $u \in R_1^\times$.

La definición 1.1 tiene la propiedad $\mathfrak{a}^{\mathrm{ec}} = \mathfrak{a}$ respecto a extensión contracción de ideales $\mathfrak{a}$ de R_1. En efecto, siempre se tiene que $\mathfrak{a}^{\mathrm{ec}} \supset \mathfrak{a}$, veamos que $\mathfrak{a}^{\mathrm{ec}} \subset \mathfrak{a}$, sea $r \in \mathfrak{a}^{\mathrm{ec}}$, entonces $\varphi(r) \in \mathfrak{a}^{\mathrm{e}}$, existen $x_i \in R_1$ y $a_i \in \mathfrak{a}$ para $i = 1, 2, \ldots, n$ tales que $\varphi(r) = \sum_{i=1}^{n} x_i \varphi(a_i)$. Así la ecuación $\alpha_*(\boldsymbol{x}) = \varphi(r)$ tiene solución en R_2^n, por ser fielmente plana, la ecuación $\alpha(\boldsymbol{x}) = r$ tiene solución en R_1^n, así $r \in \mathfrak{a}$.

(1.3) DEFINICIÓN: Un morfismo $\varphi : (A, \mathfrak{m}_A) \to (B, \mathfrak{m}_B)$ de anillos locales se dice que es **local** cuando refleja unidades, i.e. si $\varphi(a) \in B^\times \Rightarrow a \in A^\times$.

Observemos que $A = \mathfrak{m}_A \sqcup A^\times$ y $B = \mathfrak{m}_B \sqcup B^\times$ y si $\varphi(a) \notin \mathfrak{m}_B \Rightarrow \varphi(a) \in B^\times \Rightarrow a \in A^\times \Rightarrow \varphi(a) \in \varphi(A^\times) \subset B^\times \Rightarrow \varphi(a) \notin B \setminus \varphi(A^\times) \supset \varphi(A \setminus A^\times) = \varphi(\mathfrak{m}_A) \Rightarrow \varphi(a) \notin \varphi(\mathfrak{m}_A)$. Lo anterior dice que φ es local si $\varphi(\mathfrak{m}_A) \subset \mathfrak{m}_B$.

(1.4) LEMA: Sean $(R_1, \mathfrak{m}_1)$, $(R_2, \mathfrak{m}_2)$ anillos locales y $\varphi : (R_1, \mathfrak{m}_1) \to (R_2, \mathfrak{m}_2)$ morfismo local. Entonces R_2 es R_1-álgebra plana si y sólo si R_2 es R_1-álgebra fielmente plana.

Demostración. $\Rightarrow$ Recordemos que $\varphi : R_1 \to R_2$ sea local quiere decir que $\varphi(\mathfrak{m}_1) \subset \mathfrak{m}_2$.

Sean $x, a_i \in R_1$ y consideremos la ecuación

$$\sum_{i=1}^{n} a_i x_i = x \quad \text{en } R_1 \tag{1}$$

y

$$\sum_{i=1}^{n} \varphi(a_i) x_i = \varphi(x) \quad \text{en } R_2 \tag{2}$$

Supongamos que $\boldsymbol{y} = (y_1, \ldots, y_n)$ es solución de (2) y consideremos $\tilde{\boldsymbol{y}} = (y_1, \ldots, y_n, y_{n+1})$ solución de la ecuación homogénea

$$\sum_{i=1}^{n} \varphi(a_i) x_i + \varphi(-x) x_{n+1} = 0 \tag{3}$$

Como R_2 es R_1-álgebra plana, las soluciones de (3) están generadas como R_2-submódulo de R_2^n por las soluciones de $\sum_{i=1}^{n} a_i x_i + (-x) x_{n+1} = 0$, i.e. existen $\boldsymbol{S}_j = (s_{j,1}, \ldots, s_{j,n}, s_{j,n+1}) \in R_1^{n+1}$, $\lambda_i \in R_1$, $j = 1, \ldots, r$ y cierto $r \in \mathbb{N}$ tales que:
$(y_1, \ldots, y_n, 1) = \sum_{j=1}^{r} \varphi(\lambda_j) \boldsymbol{S}_j$ y

$$\sum_{i=1}^{n} a_i s_{j,i} + (-x) s_{j,n+1} = 0 \quad \forall j = 1, \ldots, r. \tag{4}$$

Esto quiere decir que $\boldsymbol{S}_j$ es solución de $\sum_{i=1}^{n} a_i x_i + (-x) x_{n+1} = 0$, como $1 = \sum_{j=1}^{r} \varphi(\lambda_j) s_{j,n+1}$, $\lambda_j \in R_1$. Llamando $\mathfrak{a} = \langle s_{1,n+1}, \ldots, s_{r,n+1} \rangle R_1$ ideal de R_1 generado por $s_{1,n+1}, \ldots, s_{r,n+1}$, tenemos $1 \in \varphi(\mathfrak{a}) R_2$, i.e. $\mathfrak{a}^e = \varphi(\mathfrak{a}) R_2 = R_2$, así $\mathfrak{a} \not\subset \mathfrak{m}_1$, pues si $\mathfrak{a} \subset \mathfrak{m}_1 \Rightarrow \varphi(\mathfrak{a}) \subset \varphi(\mathfrak{m}_1) \subset \mathfrak{m}_2 \Rightarrow \varphi(\mathfrak{a}) R_2 \subset \mathfrak{m}_2 \Rightarrow R_2 = \varphi(\mathfrak{a}) R_2 \subset \mathfrak{m}_2 \neq R_2$, contradicción. Así existen $\mu_j \in R_1$ $(j = 1, \ldots, r)$ tales que $1 = \sum_{j=1}^{r} \mu_j s_{j,n+1}$.

Multiplicando (4) por μ_j tenemos

$$\sum_{i=1}^{n} a_i \mu_j s_{j,i} + \mu_j s_{j,n+1} (-x) = 0 \qquad j = 1, \ldots, r$$

sumando sobre j

$$\sum_{i=1}^{n} a_i(\sum_{j=1}^{r} \mu_j s_{j,i}) + \sum_{j=1}^{r} \mu_j s_{j,n+1}(-x) = 0$$

si $x_i := \sum_{j=1}^{r} \mu_j s_{j,i}$

$$\sum_{i=1}^{n} a_i x_i + 1(-x) = 0$$

i.e. $\boldsymbol{x} = (x_1, \ldots, x_n)$ es solución de $\sum_{i=1}^{n} a_i x_i = x$.

$\Leftarrow$ Se sigue de la observación 1.2.1.

□

(**1.5**) **OBSERVACIÓN:** Geométricamente, una R_1-álgebra plana R_2 corresponde a una familia $\mathrm{Spec}(R_2) \to \mathrm{Spec}(R_1)$ que varía continuamente. La fibra de $\mathrm{Spec}(R_2)$ en un punto $\mathfrak{p} \in \mathrm{Spec}(R_1)$ es $\mathrm{Spec}(R_2 \otimes_{R_1} \boldsymbol{\kappa}(\mathfrak{p}))$, donde $\boldsymbol{\kappa}(\mathfrak{p})$ es el campo residual del anillo local $(R_1)_{\mathfrak{p}}$, o equivalentemente, el campo de fracciones del dominio $R_1/\mathfrak{p}$. Esto es que la fibra "varía continuamente" al variar $\mathfrak{p}$.

1.II. Henselización de un anillo local

Los anillos henselianos son los anillos "más pequeños" que verifican el TFI, en ellos se pueden estudiar localmente propiedades geométricas y analíticas de manera algebraica.
Dado un conjunto algebraico $V \subset K^n$ y un punto $\boldsymbol{p} \in V$, el anillo local de V en el punto p es el conjunto $\mathcal{O}_p$, la henselización $\mathcal{O}_p^h$ del anillo local $\mathcal{O}_p$ es la menor extensión local que verifica el TFI.

(**1.6**) **DEFINICIÓN:** Sea $(R, \mathfrak{m}, \kappa)$ un anillo local.

1. Se dice que f es un **polinomio de Hensel** si es mónico, $f(0) \in \mathfrak{m}$ y $f'(0) \in R^\times$.
2. Diremos que R es un anillo **henseliano** si cualquier polinomio de Hensel tiene una raíz en $\mathfrak{m}$.

Observemos que si $f(X) = X^n + \ldots + a_1 X + a_0$, con $a_1 \in R^\times$ y $a_0 \in \mathfrak{m}$ tiene una raíz en $\mathfrak{m}$, entonces esta raíz es única. En efecto, sea $\alpha \in \mathfrak{m}$ una raíz de f, $f(X) = (X - \alpha)g(X)$, con $g(X) = X^{n-1} + \ldots + b_1 X + b_0 \in R[X]$ y $b_0 - \alpha b_1 = a_1 \in R^\times$, así $b_0 \in R^\times$. Si $\beta \in \mathfrak{m}$ es otra raíz de f, entonces $f(\beta) = 0$, pero $g(\beta) \in R^\times$, por lo tanto $\alpha = \beta$.
Mostremos ahora que todo polinomio $f(X) = a_n X^n + \ldots + a_1 X + a_0$ con $a_1 \in R^\times$ y $a_0 \in \mathfrak{m}$ tiene una (única) raíz en $\mathfrak{m}$: esta es una manera de suprimir en la definición 1.6 la hipótesis que f sea mónico. Parece claro que este tipo de resultado debe ser la consecuencia de algún cambio de variable; y de hecho este es el caso, curiosamente este cambio de variable parece que está ausente en la literatura clásica.
El siguiente lema indica el cambio de variable sugerido.

(**1.7**) **LEMA:** Sea $f(X) = a_n X^n + \ldots + a_1 X + a_0$, con $a_1 \in R^\times$ y $a_0 \in \mathfrak{m}$. Entonces existe un polinomio mónico $g(X) \in R[X]$, $g(X) = X^n + \ldots + b_1 X + b_0$, con $b_1 \in R^\times$ y $b_0 \in \mathfrak{m}$, de manera que la siguiente igualdad tiene sentido en $R(X)$:

$$a_0 g(X) = (X+1)^n f(\frac{-a_0 a_1^{-1}}{X+1}),$$

donde $R(X)$ denota la localización de Nagata de $R[X]$.

Demostración. Tenemos

$$X^n f(\frac{-a_0 a_1^{-1}}{X}) = a_0(X^n - X^{n-1} + a_0 \sum_{j=2}^{n}(-1)^j a_j a_0^{j-2} a_1^{-j} X^{n-j}) = a_0 h(X)$$

donde

$$h(X) = X^n - X^{n-1} + a_0 \sum_{j=2}^{n}(-1)^j a_j a_0^{j-2} a_1^{-j} X^{n-j} = X^n - X^{n-1} + a_0 \ell(X)$$

Escogemos $g(X) = h(X+1) = X^n + \ldots + b_1 X + b_0$. Este polinomio es mónico con término constante $b_0 = g(0) = h(1) = a_0\ell(1) \in \mathfrak{m}$ y término lineal $b_1 = g'(0) = h'(1) = 1 + a_0\ell'(1) \in 1 + \mathfrak{m}$. □

(1.8) COROLARIO: Sea $(R, \mathfrak{m}, \kappa)$ un anillo henseliano, $f(x) = a_n X^n + \ldots + a_1 X + a_0 \in R[X]$ un polinomio tal que $\overline{f}(X) \in \kappa[X]$ tiene una raíz simple $a \in \kappa$. Entonces existe una única raíz $\alpha \in R$ de f tal que $\overline{\alpha} = a$.

Demostración. Consideremos el polinomio $h(X) = f(X + \gamma)$, donde $\overline{\gamma} = a$, como $\overline{f}(a) = 0$, entonces $\gamma \in \mathfrak{m}$, si construimos $g(X)$ a partir de $h(X)$ como en el lema anterior, tenemos $g(0) = h(1) = f(\gamma) \in \mathfrak{m}$ y $g'(0) = h'(1) = f'(\gamma) \in R^\times$. El resultado sigue de aplicar el lema anterior al polinomio h. □

(1.9) DEFINICIÓN: Un **código de Hensel** sobre R es una terna de uplas $(\boldsymbol{X}, \boldsymbol{f}, \boldsymbol{0})$ donde $(\boldsymbol{X}, \boldsymbol{f})$ es un sistema de polinomios sobre R y $\overline{\boldsymbol{0}}$ es una raíz simple del sistema en el campo residual κ, i.e. una **raíz residual** tal que $|\frac{\partial \boldsymbol{f}}{\partial \boldsymbol{X}}(\overline{\boldsymbol{0}})| \in \kappa^\times$.
Si $\overline{\boldsymbol{0}}$ se levanta a una única raíz simple $\boldsymbol{u}$ del sistema $(\boldsymbol{X}, \boldsymbol{f})$ i.e. $\overline{u_i} = \overline{0}$ para cada i, diremos que $\boldsymbol{u}$ es una **raíz de Hensel en R del código** $(\boldsymbol{X}, \boldsymbol{f}, \boldsymbol{0})$.
Un **código de Hensel univariado** es un código de la forma $(Z, g, 0)$ donde g es un polinomio de Hensel.

En lo que sigue dado un anillo local $(R, \mathfrak{m}, \kappa)$ vamos a construir la menor extensión henseliana de R que domina a $(R, \mathfrak{m}, \kappa)$ y tiene el mismo cuerpo residual κ, en la literatura esto se llama henselización del anillo R (ver 1.14)

(1.10) DEFINICIÓN: Sea $f(X) = X^n + \ldots + a_1 X + a_0 \in R[X]$ un polinomio de Hensel. Definimos $R[\overline{X}] := R[X]/\langle f(X)\rangle$, donde $\overline{X}$ es la clase de equivalencia de X en el anillo cociente, sea S el subconjunto multiplicativo de $R[\overline{X}]$ definido por

$$S := \{g(\overline{X}) \in R[\overline{X}] : g(X) \in R[X], g(0) \in R^\times\}.$$

Definimos R_f como $R[\overline{X}]$ localizado en $R \setminus S$, esto es:

$$R_f := S^{-1} R[\overline{X}].$$

(1.11) LEMA: El anillo R_f es un anillo local con ideal maximal $\mathfrak{m}R_f$ y su campo residual $\boldsymbol{\kappa}_f$ es canónicamente isomorfo al campo residual $\boldsymbol{\kappa}$ del anillo $R[X]/\langle f(X)\rangle$, además es fielmente plano sobre R y en particular puede identificarse R con su imagen en R_f y escribir $R \subseteq R_f$.

Demostración. Como f es mónico, entonces $B := R[X]/\langle f(X)\rangle$ es $R-$ libre y por consiguiente plano sobre R.
Además $S^{-1}(R[X]/\langle f(X)\rangle)$ es $R[X]/\langle f(X)\rangle-$plano, siempre que $S^{-1}B$ es B plano para cualquier localización y por transitividad $S^{-1}(R[X]/\langle f(X)\rangle)$ es plano sobre R
Los elementos de R_f pueden escribirse como fracciones formales $r(\overline{X})/s(\overline{X})$ con $r, s \in R[X]$, $s(0) \in R^\times$, $r(\overline{X}), s(\overline{X}) \in R[\overline{X}]$. Consideremos una fracción arbitraria $a = r(\overline{X})/s(\overline{X}) \in R_f$, para probar que R_f es local, mostraremos que $a \in R_f^\times$ o $a \in \mathcal{J}_{R_f}$. Si $r(0) \in R^\times$, entonces $a \in R_f^\times$; si $r(0) \in \mathfrak{m}$, consideremos otra fracción arbitraria $b = r_1(\overline{X})/s_1(\overline{X}) \in R_f$, tenemos

$$1 + ab = (s(\overline{X})s_1(\overline{X}) + r(\overline{X})r_1(\overline{X}))/(s(\overline{X})s_1(\overline{X})) = p(\overline{X})/q(\overline{X})$$

y $p(0) \in R^\times$, entonces $1 + ab \in R_f^\times$. Ahora mostraremos que $\mathfrak{m}_{R_f}$ es el conjunto de todas las fracciones $r(\overline{X})/s(\overline{X})$ tales que $r(0) \in \mathfrak{m}$ (en particular $\mathfrak{m} \subseteq \mathfrak{m}_{R_f}$) y $R_f^\times$ es el conjunto de todas las fracciones $r(\overline{X})/s(\overline{X})$ tales que $r(0) \in R^\times$. En este sentido, para demostrar que $\mathfrak{m}_{R_f} = \mathfrak{m}R_f$ es suficiente mostrar que $\overline{X}/1 \in \mathfrak{m}R_f$. Sea

$$\overline{Y} = \overline{X}^{n-1} + a_{n-1}\overline{X}^{n-2} + \ldots + a_2\overline{X} + a_1$$

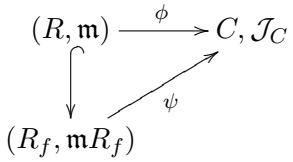
Tenemos $\overline{Y} \in R_f^\times$ y $\overline{YX} = -a_0$, así $\overline{X} = -a_0\overline{Y}^{-1} \in \mathfrak{m}R_f$. Por lo tanto $\mathfrak{m}_{R_f} = \mathfrak{m}R_f$.
Hemos mostrado que el morfismo $R \to R_f$ es local y por lo tanto R_f es fielmente plano sobre R (Lema 1.4), así se puede considerarse R como subanillo de R_f.
Una igualdad $r(\overline{X})/s(\overline{X}) = p(\overline{X})/q(\overline{X})$ en R_f quiere decir $(X)(p(X)s(X) - r(X)q(X)) \in \langle f(X)\rangle$ en $R[X]$ con $u(0) \in R^\times$ y esto implica que $p(0)s(0) - r(0)q(0) \in \mathfrak{m}$. Observamos que $R_f \ni r(X)/s(X) \mapsto \overline{r(0)/s(0)} \in \kappa$ es un homomorfismo de anillos bien definido con núcleo $\mathfrak{m}_{R_f}$, así obtenemos que el campo residual de R_f es canónicamente isomorfo a κ. □

(1.12) LEMA: Sea $(R, \mathfrak{m}, \kappa)$ un anillo local y $(X, f, 0)$ un código de Hensel univariado, entonces el morfismo $R \to R_f$ es fielmente plano.

Demostración. El álgebra $R[\overline{X}] := R[X]/\langle f(X)\rangle$ es libre, en un principio R_f es localización de $R[\overline{X}]$. Por último, los dos anillos son locales y el morfismo refleja las unidades. □

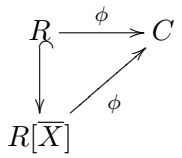
En lo que resta del capítulo haremos como lo hicimos al final de la demostración de 1.11, denotaremos por $\overline{X}$ al elemento $\overline{X}/1$ de R_f. Este es un cero de f en $\mathfrak{m}_{R_f}$, además identificaremos $R[\overline{X}/1]$ como subanillo de R_f el cual es un anillo cociente de $R[\overline{X}]$.

(1.13) LEMA: Sea $(R, \mathfrak{m}, \kappa)$ un anillo henseliano, sea C un anillo con radical de Jacobson $\mathcal{J}_C$, $\phi : R \to C$ un homomorfismo de anillos y $f(X) = X^n + \ldots + a_1X + a_0 \in R[X]$ un polinomio de Hensel.
Si $\phi(f) = X^n + \ldots + \phi(a_1)X + \phi(a_0) \in C[X]$ tiene una raíz $\xi \in \mathcal{J}_C$, entonces existe un único morfismo $\psi : R_f \to C$ tal que $\psi(\overline{X}) = \xi$ y el siguiente diagrama conmuta:

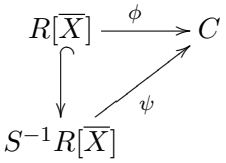


En el caso que C sea un anillo local y ϕ un morfismo local, entonces ψ es un morfismo local.

Demostración. Se ha construido R_f exactamente para este propósito. En efecto, primero, como $\phi(f)(\xi) = 0$, entonces existe un único homomorfismo de anillos $\phi : R[\overline{X}] \to C$ factorizando ϕ:



Segundo, como $\xi \in \mathcal{J}_C$ y $\phi(R^\times) \subseteq C^\times$, para cualquier elemento $g(\overline{X}) = g(0) + \overline{X}\ h(\overline{X}) \in S$ ($g(0) \in R^\times$) tenemos que $\phi(g(\overline{X})) = \phi(g(0)) + \xi\ h(\xi) \in C^\times$. Por lo que existe un único homomorfismo de anillos $\psi : S^{-1}R[\overline{X}] \to C$ factorizando ϕ:



Supongamos que C es un anillo local y ϕ un morfismo local. Si $\psi(g(\overline{X})/s(\overline{X})) \in C^\times$, entonces debemos mostrar que $g(\overline{X})/s(\overline{X}) \in R_f^\times$. Tenemos que $\psi(g(\overline{X})) = \phi(g(0)) + \xi\ h(\xi) \in C^\times$. Como $\xi \in \mathfrak{m}_C$ tenemos que $\phi(g(0)) \in C^\times$. Como ϕ es un morfismo local, $g(0) \in R^\times$. Así $g(\overline{X}) \in S$ y $g(\overline{X})/1 \in R_f^\times$. □

Definición inductiva

Ahora definimos un sistema inductivo. Sea $\mathcal{S}$ la menor familia de anillos locales $(Z, \mathfrak{m}_Z)$ tal que

I- $(R, \mathfrak{m}) \in \mathcal{S}$;

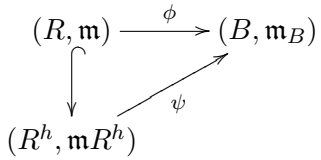
II- si $(Z, \mathfrak{m}_Z) \in \mathcal{S}$, $f(X) = X^n + \ldots + a_1X + a_0 \in Z[X]$ con $a_1 \in Z^\times$ y $a_0 \in \mathfrak{m}_Z$, entonces $(Z_f, \mathfrak{m}_{Z_f}) \in \mathcal{S}$.

Veamos que $\mathcal{S}$ es un sistema inductivo. El anillo R se incluye canónicamente en cada anillo local $(Z, \mathfrak{m}_Z) \in \mathcal{S}$, y $\mathfrak{m}_Z = \mathfrak{m}Z$. De manera similar, cada anillo local en $\mathcal{S}$ se incluye canónicamente en otro que construye a partir de el.
Dados dos anillos locales $(B, \mathfrak{m}_B), (C, \mathfrak{m}_C) \in \mathcal{S}$, el primero de ellos es construido agregando sucesivamente raíces de Hensel de polinomios $f_1, \ldots, f_k$ en extensiones sucesivas, el segundo es construido agregando sucesivamente raíces de Hensel de los polinomios $g_1, \ldots, g_\ell$ en extensiones sucesivas.
Ahora podemos agregar sucesivamente las raíces de Hensel de los polinomios $f_1, \ldots, f_k$ a C y agregar sucesivamente las raíces de Hensel de los polinomios $g_1, \ldots, g_\ell$ a B. Observamos que la extensión C' de C y la extensión B' de B construidas son canónicamente isomorfas.
Así tenemos un sistema inductivo filtrado cuyos morfismos son inyectivos y el límite inductivo es un anillo local que "contiene" todos los elementos de $\mathcal{S}$ como subanillos. Este tipo de construcciones siempre funciona cuando tenemos la propiedad de unicidad que describe el lema 1.13.
La construcción anterior permite definir también la **henselización** R^h de R como el límite

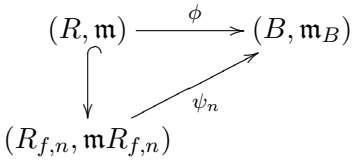
$$R^h := \varinjlim_{Z \in \mathcal{S}} Z.$$

Tenemos el siguiente teorema.

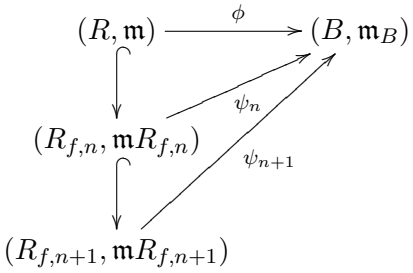
(1.14) TEOREMA: La henselización R^h del anillo R es un anillo local henseliano con ideal maximal $\mathfrak{m}R_h$. Si $(B, \mathfrak{m}_B)$ es un anillo local henseliano y $\phi : R \to B$ es un morfismo local, entonces $\exists!\psi$ tal que el siguiente diagrama es conmutativo:



Demostración. El caso base es la conclusión del lema 1.13. Supongamos entonces que al hacer repetidamente (1.II) n veces existe un único morfismo local ψ_n de manera que el siguiente diagrama es conmutativo.



Como $\psi_n : (R_{f,n}, \mathfrak{m}R_{f,n}) \to (B, \mathfrak{m}_B)$, es un morfismo local y $(B, \mathfrak{m}_B)$ es un anillo local, construimos $(R_{f,n+1}, \mathfrak{m}R_{f,n+1})$ agregando las raíces de Hensel de los polinomios $p_1, \ldots, p_r$ a $(R_{f,n}, \mathfrak{m}R_{f,n})$ tenemos por el lema 1.13 que existe un único morfismo local ψ_{n+1} tal que el diagrama es conmutativo.



□

1.III. Lema de Hensel Multivariado

Para un anillo local hemos construido la henselización y demostrado ciertas propiedades. A continuación justificamos que todo anillo henseliano verifica el LHM o TFI.
Comenzamos generalizando la definición 1.10. Dado un código de Hensel $(\boldsymbol{Y}, \boldsymbol{f}, \mathbf{0})$, donde $\boldsymbol{f} = (f_1, \ldots, f_n)$, y para cada i: $f_i \in R[Y_1, \ldots, Y_p]$, $f_j(\mathbf{0}) = 0$ y $|\frac{\partial(f_1,\ldots,f_p)}{\partial(Y_1,\ldots,Y_p)}(\overline{\mathbf{0}})| \in R^\times$ podemos asociarle un álgebra que llamaremos **álgebra de Hensel**:

$$R_{\boldsymbol{f}} := (R[\boldsymbol{Y}]/\langle \boldsymbol{f} \rangle)_{(\mathfrak{m},\langle \boldsymbol{Y} \rangle)} = (R[Y_1, \ldots, Y_p]/\langle f_1, \ldots, f_p \rangle)_{(\mathfrak{m},\langle Y_1,\ldots,Y_p \rangle)}.$$

En particular, para un código de Hensel univariado $(Z, g, 0)$ podemos asociarle un álgebra que llamaremos **álgebra de Hensel univariada**:

$$R_g := (R[Z]/\langle g(Z) \rangle)_{\langle Z \rangle}$$

(1.15) LEMA DE HENSEL MULTIVARIADO: Sea $(R, \mathfrak{m})$ un anillo local con campo residual κ y $(\boldsymbol{Y}, \boldsymbol{f}, \mathbf{0})$ un código de Hensel sobre R. Entonces, existe un código de Hensel

univariado $(Z, g, 0)$ y ω una raíz de Hensel en R_f tal que, llamando z a Z mód $\mathfrak{m}$ la aplicación

$$\begin{aligned}(R[Z]/\langle g(Z)\rangle)_{(\mathfrak{m},z)} &\to R_f\\ z &\mapsto \omega \in R_f\end{aligned}$$

es un isomorfismo.

Una consecuencia del lema 1.15 la henselización del anillo local $(R, \mathfrak{m})$ es también el límite inductivo de álgebras de Hensel univariadas asociadas a códigos de Hensel multivariados. Como se ha enunciado este lema, para anillos más generales, es consecuencia del Teorema Principal de Zariski (ZMT por su nombre en inglés) en su versión abstracta "a la Peskine" (1946).
Una demostración constructiva del lema se encuentra en [1, Teorema 4.4], la cual permite dar un algoritmo (de alta complejidad) para definir el isomorfismo que se establece en el lema.
En los capítulos siguientes, para trabajar con el henselizado del anillo local $R := \kappa[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$, usaremos de manera dinámica la henselización como límite inductivo de estas álgebras de Hensel. Nótese que para este anillo R una de esas álgebras será: $K[\boldsymbol{X}, \boldsymbol{Y}]/\langle \boldsymbol{H}\rangle$, donde $(\boldsymbol{Y}, \boldsymbol{H}, \boldsymbol{0})$ es un código de Hensel, $\boldsymbol{X} = \{X_1, \ldots, X_n\}$, $\boldsymbol{Y} = \{Y_1, \ldots, Y_p\}$, $\boldsymbol{H} = \{H_1, \ldots, H_p\}$. Por ello a continuación damos una demostración del LHM para este caso particular:

(1.16) TEOREMA: Sea K un campo, $\boldsymbol{X} := \{X_1, \ldots, X_n\}$, $\boldsymbol{Y} := \{Y_1, \ldots, Y_p\}$. Consideremos el anillo local

$$\mathcal{O} := K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$$

y un código de Hensel dado por $H_1, \ldots, H_p \in \mathcal{O}[\boldsymbol{Y}]$, con $H_j(\boldsymbol{0}, \boldsymbol{0}) = 0$ y $|\frac{\partial(H_1,\ldots,H_p)}{\partial(Y_1,\ldots,Y_p)}(\boldsymbol{0}, \boldsymbol{0})| \neq 0$. Sin pérdida de generalidad suponemos que $H_j \in K[\boldsymbol{X}, \boldsymbol{Y}]$. Entonces el álgebra de Hensel

$$(\mathcal{O}[\boldsymbol{Y}]/\langle \boldsymbol{H}\rangle_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle} = K[\boldsymbol{X}, \boldsymbol{Y}]/\langle \boldsymbol{H}\rangle^e$$

es isomorfa a un álgebra de Hensel univariada de $\mathcal{O}$.

Demostración. Sea $C := K[\boldsymbol{X}, \boldsymbol{Y}]/\langle H_1, \ldots, H_p\rangle$ y $\mathfrak{m} := \mathfrak{m}_A = \langle \boldsymbol{x}\rangle$. El corolario A.11 comprueba que el anillo $C_{\mathfrak{m}}$ es local regular.
La variedad asociada a $I := \langle H_1, \ldots, H_p\rangle$ por el $(\boldsymbol{0}, \boldsymbol{0})$ solo pasa una componente pues el anillo es DI y al localizar desaparecen todos los ideales que no están contenidos en $\mathfrak{m}$ que corresponden a variedades que no contienen a $(\boldsymbol{0}, \boldsymbol{0})$.
Esto dice que si antes de localizar el ideal I tiene la descomposición primaria $I = \mathfrak{p}_0 \cap \ldots \cap \mathfrak{p}_r$, entre todos esos primos existe solamente un $\mathfrak{p}$ que está contenido en el maximal. Al localizar todos desaparecen excepto $\mathfrak{p}$, así

$$I^e = I \cdot K[\boldsymbol{X}, \boldsymbol{Y}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle} = \mathfrak{p} \cdot K[\boldsymbol{X}, \boldsymbol{Y}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle},$$

al localizar en $\mathfrak{m}$ tenemos que:

$$A = C_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle} = (K[\boldsymbol{X}, \boldsymbol{Y}]/I)_{\langle \boldsymbol{x},\boldsymbol{y}\rangle} = (K[\boldsymbol{X}, \boldsymbol{Y}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle})/I^e = (K[\boldsymbol{X}, \boldsymbol{Y}]/\mathfrak{p})_{\langle \boldsymbol{x},\boldsymbol{y}\rangle}.$$

Por lo tanto el cuerpo de fracciones de A es igual al cuerpo de fracciones de $(K[\boldsymbol{X}, \boldsymbol{Y}]/\mathfrak{p})_{\mathfrak{m}}$. Tenemos que

$$K[\boldsymbol{X}] \subset K[\boldsymbol{X}, \boldsymbol{Y}]/\mathfrak{p} \overset{i}{\hookrightarrow} (K[\boldsymbol{X}, \boldsymbol{Y}]/\mathfrak{p})_{\langle \boldsymbol{x},\boldsymbol{y}\rangle} = (K[\boldsymbol{X}, \boldsymbol{Y}]/\langle H_1, \ldots, H_p\rangle)_{\langle \boldsymbol{x},\boldsymbol{y}\rangle} = A,$$

donde i es inyectiva, porque $K[\boldsymbol{X}]$ es DI, cuando se va localizando se van encontrando anillos más grandes hasta el cuerpo de fracciones, y además la aplicación del DI en su cuerpo de fracciones es inyectiva y por tanto las aplicaciones intermedias también.

Como $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle} \hookrightarrow A$, tenemos que

$$\begin{aligned} n &= \dim_{\text{krull}} A \\ &= \dim_{\text{krull}} (K[\boldsymbol{X},\boldsymbol{Y}]/\mathfrak{p})_{\langle \boldsymbol{x},\boldsymbol{y}\rangle} \\ &= \dim_{\text{krull}} K[\boldsymbol{X},\boldsymbol{Y}]/\mathfrak{p} \\ &= \text{grado de trascendencia de } K[\boldsymbol{X},\boldsymbol{Y}]/\mathfrak{p} \end{aligned}$$

Esto quiere decir que, $K[\boldsymbol{X}] \hookrightarrow K[\boldsymbol{X},\boldsymbol{Y}]/\mathfrak{p}$, y los grados de trascendencia de $K[\boldsymbol{X}]$ y $K[\boldsymbol{X},\boldsymbol{Y}]/\mathfrak{p}$ es n, esto es, que las $\boldsymbol{y}$'s son algebraicas. Por lo tanto el cuerpo de fracciones $Q(A)$ es L y es una extensión finitamente generada de K, de hecho, es una extensión algebraica de $K(\boldsymbol{X}) = Q(K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle})$.
Como $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle} \subset L$, sea $\mathcal{O}$ el cierre íntegro de $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$ en L, por [3, Proposición 5.17] tenemos que $\mathcal{O}$ es un $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}-$finitamente generado.
Además A es local regular, por tanto DI, y por tanto íntegramente cerrado en L, como el cierre íntegro es el menor anillo del cuerpo de fracciones que es entero sobre $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$ que es $\mathcal{O}$, luego necesariamente $\mathcal{O} \subset A$. Así

$$K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle} \subset \mathcal{O} \subset A,$$

claramente el ideal maximal $\mathfrak{m}$ de $\mathcal{O}$ se contrae de $\mathfrak{m}_A$: $\mathfrak{m} = \mathfrak{m}_A \cap \mathcal{O}$.
Ahora vamos a probar que

$$\mathcal{O}_{\mathfrak{m}} = A.$$

Bastará probar que y_j está en $\mathcal{O}$, por la siguiente observación.
Todo elemento de A se puede escribir como $\frac{g(\boldsymbol{x},\boldsymbol{y})}{1+h(\boldsymbol{x},\boldsymbol{y})}$, donde $h(\mathbf{0},\mathbf{0}) = 0$ i.e. $h \in \mathfrak{m}_A$, Como $\mathcal{O}$ contiene a K, $\boldsymbol{x}$, $\boldsymbol{y}$, se tendrá que $h \in \mathcal{O}$ (por ser polinomio) y entonces $h \in \mathcal{O} \cap \mathfrak{m}_A = \mathfrak{m}$. Luego $h \in \mathfrak{m}$, de donde $1 + h \notin \mathfrak{m}$.
Para probar y_j está en $\mathcal{O}$, debemos probar que dependen íntegramente sobre $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$. Para ello usaremos la caracterización dada por el teorema A.3 y su corolario, que juntos afirman que el cierre integro de un anillo es intersección de AVD, cuando la valoración es discreta de rango uno podemos simplificar a que haya solo una y. Así la técnica, es deducir las variables $\boldsymbol{y}$ a una sola y.

$$K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle} \subset \mathcal{O} \subset A \subset qf(A) = L$$

Claramente $y_j \in L$, también $y_j \in A$, y queremos ver que $y_j \in \mathcal{O}$, como $\mathcal{O}$ es un anillo noetheriano, local regular, íntegramente cerrado y DI. Es suficiente probar que para para cualquier AVD, $V = \mathcal{O}_{\mathfrak{b}}$, se tiene que $y_j \in V$, donde $\mathfrak{b}$ un ideal primo de altura 1 de $\mathcal{O}$.
Por el teorema del ascenso [3, Teorema 5.16] entre $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$ y $\mathcal{O}$ tenemos que $V^* := K[\boldsymbol{X}]_{\langle \boldsymbol{X},\mathfrak{a}\rangle}$, donde $\mathfrak{a} := \mathfrak{b} \cap K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$ es un un AVD de rango uno (de $K(\boldsymbol{X})$) dominando a V. Así podemos asumir que la valoración asociada a V es inducida por un morfismo inyectivo $\phi : \mathcal{O} \to k(\mathfrak{b})[[t]]$ y hace conmutativo el diagrama

$$\begin{array}{ccccc} K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle} & \subset & \mathcal{O} & \subset & L \\ \downarrow & & \downarrow \phi & & \\ k(\mathfrak{a})[[t]] & \subset & k(\mathfrak{b})[[t]] & \subset & k(\mathfrak{b})((t)) \end{array}$$

Como $\phi(\boldsymbol{x}) \in k(\mathfrak{b})[[t]]$, por la hipótesis sobre el jacobiano y el teorema de la función implícita en una variable, existe una única solución $y(t) \in k(\mathfrak{b})[[t]]$ que satisface el sistema

$$H_i(\phi(x_1), \ldots, \phi(x_n), \boldsymbol{y}) = 0, \qquad i = 1, \ldots, p.$$

Por lo tanto $y_j \in V^*$.
Hemos visto que $\mathcal{O}$ es un $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$- módulo finitamente generado, es decir, $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle} \subset \mathcal{O}$ es una extensión finita. Sea $\mathfrak{q}$ el ideal $\langle \boldsymbol{X} \rangle K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$ del anillo $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$. Así $\mathcal{O}/\mathfrak{q} \cdot \mathcal{O}$ es un $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}/\mathfrak{q} = K$ espacio vectorial de dimensión finita y por el teorema de estructura de anillos de Artin [3, pág. 8.7] es producto directo finito de sus localizaciones en ideales maximales de $\mathcal{O}$ que contienen a $\mathfrak{q} \cdot \mathcal{O}$.
Como $\mathfrak{q}$ es ideal maximal de $k[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$, los ideales maximales que contienen a $\mathfrak{q} \cdot \mathcal{O}$ son los ideales maximales de $\mathcal{O}$ que yacen sobre $\mathfrak{q}$ en $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$, denotaremos a estos ideales de $\mathcal{O}$ que yacen sobre $\mathfrak{q}$ por $\mathfrak{m}_1, \ldots, \mathfrak{m}_\ell$. Recordemos que uno de ellos es $\mathfrak{m}$ y era la contracción del maximal de A, por lo que sin pérdida de generalidad supondremos que es $\mathfrak{m}_1 = \mathfrak{m}$.
Tenemos

$$K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}/\mathfrak{q} = K \hookrightarrow \mathcal{O}/\mathfrak{q} \cdot \mathcal{O} \cong (\mathcal{O}_{\mathfrak{m}}/\mathfrak{q} \cdot \mathcal{O}_{\mathfrak{m}}) \times \cdots \times (\mathcal{O}_{\mathfrak{m}_\ell}/\mathfrak{q} \cdot \mathcal{O}_{\mathfrak{m}_\ell}) \tag{5}$$

y de hecho por las propiedades de los anillos artinianos,

$$\mathcal{O}_{\mathfrak{m}_j}/\mathfrak{q} \cdot \mathcal{O}_{\mathfrak{m}_j} = \mathcal{O}_{\mathfrak{m}_j}/\mathfrak{m}_j^{e_j} \cdot \mathcal{O}_{\mathfrak{m}_j} \tag{6}$$

para ciertos e_j. En el caso de $j = 1$, $\mathfrak{m}_1 = \mathfrak{m}$ veremos que $e_1 = 1$.
En efecto, usando el hecho que $\mathcal{O}_{\mathfrak{m}} = A$ y ocupando la hipótesis sobre la condición del Jacobiano tenemos que $A/\mathfrak{q} \cdot A$ es

$$K[\boldsymbol{X}, Y_1, \ldots, Y_p]/(\boldsymbol{X}, H_1, \ldots, H_p)_{\langle \boldsymbol{X}, \boldsymbol{Y} \rangle} \cong K[Y_1, \ldots, Y_p]/(F_1(0, \boldsymbol{Y}), \ldots, F_p(0, \boldsymbol{Y}))_{\langle \boldsymbol{Y} \rangle} \cong K.$$

Por otra parte, cuando hay una descomposición de un anillo en producto de otros, que hay un sistema de idempotentes. Así por (5) deducimos que existe un idempotente $\xi \in \mathcal{O}$, correspondiente del factor $\mathcal{O}_{\mathfrak{m}}/\mathfrak{q}\mathcal{O}_{\mathfrak{m}}$ tal que $\xi \in \mathfrak{m}_2^{e_2}, \ldots, \xi \in \mathfrak{m}_l^{e_l}$ pero $\xi \notin \mathfrak{m}$. Es decir $\overline{\xi} := \xi \mod \mathfrak{q} \cdot \mathcal{O}$ con la descomposición anterior es $(1, 0, \ldots, 0)$. y por tanto tenemos:

$$\mathcal{O}_{\mathfrak{m}}/\mathfrak{q} \cdot \mathcal{O}_{\mathfrak{m}} \cong K[\overline{\xi}]$$

Ahora tenemos una extensión finita $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle} \subset K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]$ y las extensiones:

$$K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle} \subset K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi] \subset \mathcal{O}.$$

Sea $\mathfrak{n}$ la contracción de $\mathfrak{m}$ a $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]$, $\mathfrak{n} := \mathfrak{m} \cap K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]$ y como $\mathfrak{m}$ se contrae a $\mathfrak{q}$ que era $\langle \boldsymbol{X} \rangle K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$, tenemos que, $R := K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]_{\mathfrak{n}}$ es un anillo local y las siguientes extensiones de anillos locales

$$K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle} \subset R = K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]_{\mathfrak{n}} \subset \mathcal{O}_{\mathfrak{m}}$$

verifican que el maximal de cada anillo local se contrae al maximal del anterior. En principio la segunda de estas extensiones no tiene por qué ser finita, pero en este caso, veremos que sí lo es.
Sea $S := R \setminus \mathfrak{n}$, consideramos el anillo de fracciones $S^{-1}\mathcal{O}$, tenemos que:

$$R = K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]_{\mathfrak{n}} \subset S^{-1}\mathcal{O} \tag{7}$$

es una extensión finita del anillo local R, tal que, solo hay un único ideal maximal $(\mathfrak{m})$ que está sobre el ideal maximal del anillo local. En esta situación (por la afirmación siguiente) $S^{-1}\mathcal{O} = \mathcal{O}_{\mathfrak{m}}$.
Por otro lado (7) es una extensión finita y la inclusión $R \subset S^{-1}\mathcal{O} = \mathcal{O}_{\mathfrak{m}}$ es residualmente una igualdad $R/\mathfrak{n}^e = S^{-1}\mathcal{O}/\mathfrak{n} \cdot S^{-1}\mathcal{O}$, por la elección de ξ. Finalmente por el lema de Nakayama se levanta a una igualdad y así $R = \mathcal{O}_{\mathfrak{m}} = A$. Como queríamos demostrar. □

La afirmación usada en la demostración es la siguiente

(1.17) AFIRMACIÓN: Si R es local con ideal maximal m, y $R \subset O$ es DI y extensión finita. Si solo hay un ideal maximal m' de O sobre m, entonces $(R \setminus m)^{-1}O = O_{m'}$.

Ahora sea $P(T)$ el polinomio mínimo de ξ sobre $K(\boldsymbol{X})$ (tiene todo sentido pues $\xi \in \mathcal{O}$, el cual es DI y se considera el polinomio mínimo sobre un cuerpo).
Como ξ es entero sobre $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$ y este último es íntegramente cerrado en su cuerpo de fracciones, $K\langle \boldsymbol{X} \rangle$, el polinomio mínimo es un polinomio que tiene coeficientes en $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$ (véase [3, Proposición 5.15]).
Afirmamos lo siguiente

(1.18) AFIRMACIÓN: $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]$ es isomorfo a $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[T] \diagup \langle P(T) \rangle$.

Demostración. En efecto, la evaluación

$$\begin{aligned} K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[T] &\to K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi] \\ T &\mapsto \xi \end{aligned}$$

tiene núcleo el ideal generado por $\langle P(T) \rangle$ (es un ejercicio fácil usando el Lema de Gaus y que $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$ es DFU, por ser localización de DFU. □

Así tenemos $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[T] \diagup \langle P(T) \rangle = K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]$ y existe un ideal primo $\mathfrak{c}$ de $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[T]$ tal que

$$K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle} \subset (K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[T] \diagup \langle P(T) \rangle)_{\mathfrak{c}} \cong K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[\xi]_{\mathfrak{n}} \cong \mathcal{O}_{\mathfrak{m}} \cong A.$$

(1.19) AFIRMACIÓN: El ideal $\mathfrak{c}$ es $(\boldsymbol{X}, a)$ con a raíz simple de $P(T) \mod \langle \boldsymbol{X} \rangle$.

Demostración. En primer lugar nótese que $P(T)$ tiene coeficientes que dependen de las $\boldsymbol{X}$'s y denominadores que dependen de las $\boldsymbol{X}$'s pero no se anulan en $\boldsymbol{X} = (0, \ldots, 0)$.
Además $\mathfrak{q} = \langle \boldsymbol{X} \rangle K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle} \subset \mathfrak{c}$, por tanto tiene sentido considerar $P(T) \mod \langle \boldsymbol{X} \rangle$, el cual es un polinomio con coeficientes en K, que denotaremos por $p(T)$.
Entonces tomando cocientes en la sucesión anterior de anillos locales:

$$K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle} \diagup \mathfrak{q} = K \subset (K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[T] \diagup \langle P(T) \rangle)_{\mathfrak{c}} \diagup \mathfrak{c}^e \subset A \diagup \mathfrak{m}_A \cong K$$

Así necesariamente $(K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}[T] \diagup \langle P(T) \rangle)_{\mathfrak{c}} \diagup \mathfrak{c}^e = K$, esto muestra necesariamente que $\mathfrak{c} \supset (\boldsymbol{X}, a)$ para cierta raíz simple $a \in K$ del polinomio $p(T) = P(T) \mod \langle \boldsymbol{X} \rangle$. □

Por consiguiente hemos demostrado que $A \cong (K[\boldsymbol{X}, T] \diagup \langle P(T) \rangle)_{(\boldsymbol{X}, a)}$, con a raíz simple de $P(T)$; o equivalentemente que toda álgebra de Hensel multivariada del anillo $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$ es isomorfa a una univariada.
Para demostrarlo, hemos utilizado fuertes resultados del álgebra conmutativa y muchas propiedades del anillo $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$, esto sigue siendo cierto aún para anillos locales arbitrarios (véase [1]).
Terminamos el capítulo con un ejemplo que ilustra lo difícil que resulta asociar a un código de Hensel multivariado un código univariado.

(1.20) EJEMPLO: Sea $\boldsymbol{H} := \left\{ \begin{array}{l} H_1 : -X_1 + Y_1 + X_2Y_1Y_2 + 2X_2Y_1^2 = 0, \\ H_2 : -X_2 + Y_2 + X_1Y_1^2 + X_1Y_1Y_2 + X_2Y_2^2 = 0 \end{array} \right\}$ y consideremos el código de Hensel $((Y_1, Y_2), (H_1, H_2), (0, 0))$ definiendo las series $h_1(X_1, X_2)$, $h_2(X_1, X_2)$.
Para representar a $B := (K[\boldsymbol{X}, \boldsymbol{Y}] \diagup \langle \boldsymbol{H} \rangle)_{\langle \boldsymbol{X}, \boldsymbol{Y} \rangle}$ como $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}-$álgebra de Hensel debemos encontrar adecuados elementos T que sean enteros sobre $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$ y que permitan escribir la representación

$$B \cong (K[\boldsymbol{X}, Z] \diagup \langle g(Z) \rangle)_{\langle \boldsymbol{X}, Z \rangle},$$

donde g es un polinomio de Hensel.
De H_1 se obtiene $T := X_1/Y_1 = 1 + X_2Y_2 + 2X_2Y_1 \notin \langle \boldsymbol{X}, \boldsymbol{Y} \rangle$, al despejar Y_2 de

$$T = 1 + X_2Y_2 + 2X_2Y_1 = 1 + X_2Y_2 + 2X_2\frac{X_1}{T}$$

se obtiene una función racional que al sustituirla en H_2 resulta

$$T^4 - T^3 - X_2^2T^2 + X_1^2T^2 - 4X_1X_2T^2 - X_1^2T + 2X_1X_2T - X_2X_1^3 + 4X_2^2X_1^2 = 0$$

que claramente no depende Y_2, así T es entero sobre $K[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$.
Además $z := T - 1 \in \langle \boldsymbol{X}, \boldsymbol{Y} \rangle$ es raíz del polinomio

$$\begin{aligned} g(Z) := Z^4 + 3Z^3 + 3Z^2 + X_1^2Z^2 - X_2^2Z^2 - 4X_1X_2Z^2 - 6X_1X_2Z + Z \\ + X_1^2Z - 2X_2^2Z - X_2^2 - 2X_1X_2 - X_2X_1^3 + 4X_2^2X_1^2 = 0 \end{aligned}$$

el cual es de Hensel, pues es mónico, $g(0) = -X_2^2 - 2X_1X_2 - X_2X_1^3 + 4X_2^2X_1^2 \in \langle \boldsymbol{X} \rangle$ y $g'(0) = 1 \in K^\times$. Sea $U := X_1Y_1$, $V := X_2Y_2$, de H_2 se obtiene $Y_2(1+U+V) = X_2 - UX_1$, por lo tanto $Y_2(1+U+V)T^2 = X_2T^2 - X_1^3$. Si $W := (1+U+V)T^2 = (1+U+V)(z+1)^2$, obtenemos $W := TX_1^2 + T^3 - 2X_1X_2T \in K[\boldsymbol{X}, Z]$ y $W \notin \langle \boldsymbol{X}, z \rangle K[\boldsymbol{X}, Z]_{\langle \boldsymbol{X}, z \rangle}$. Por lo tanto

$$Y_1 = \frac{X_1}{T} = \frac{X_1}{z+1}, Y_2 = \frac{Y_2W}{W} = \frac{X_2(z+1)^2 - X_1^3}{(z+1)X_1^2 + (z+1)^3 - 2X_1X_2(z+1)}.$$

Así $B \cong (K[\boldsymbol{X}, Z] \diagup \langle g(Z) \rangle)_{\langle \boldsymbol{X}, z \rangle}$.

2. Algoritmos en la henselización de un anillo local

Comenzamos definiendo las notaciones a utilizar (§2.I) en el resto del capítulo, luego (§2.II) hacemos un resumen del modelo computacional de series algebraicas que se desarrolla en [2]. Además (§2.III) estudiamos las bases estándar y el Algoritmo del Cono Tangente (ACT), la cual es la principal herramienta computacional que utilizamos para realizar los cálculos.

2.I. Preliminares y notaciones

Comenzamos con las notaciones que utilizaremos. Sea $\boldsymbol{X} := (X_1, \ldots, X_n)$ un conjunto de variables y $\mathbb{T}_{\boldsymbol{X}} := \langle \boldsymbol{X} \rangle$ el semigrupo multiplicativo de monomios en X_i's.
Para denotar a los elementos del semigrupo $\mathbb{T}_{\boldsymbol{X}}$ introducimos la notación de multiexponentes $\boldsymbol{X}^{\boldsymbol{\alpha}} := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, donde $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.
Consideraremos un órden $<$ de semigrupo en $\mathbb{T}_{\boldsymbol{X}}$ compatible con un grado o peso, dado por un vector $\boldsymbol{w} \in (\mathbb{R}^+)^n$ (cf. [9]) una matriz $\mathtt{W} \in GL(n, \mathbb{R})$, $\mathtt{W}(\boldsymbol{\alpha}) := \sum_{i=1}^n \alpha_i \cdot w_i$, y $\boldsymbol{X}^{\boldsymbol{\alpha}} < \boldsymbol{X}^{\boldsymbol{\beta}}$ si $\mathtt{W}(\boldsymbol{\alpha}) < \mathtt{W}(\boldsymbol{\beta})$. Diremos que w_i es el peso de la variable X_i.
Aveces suele escribirse $\boldsymbol{X}^{\boldsymbol{\alpha}} = \boldsymbol{\alpha}$ por la identificación natural de $\mathbb{T}_{\boldsymbol{X}}$ con $\mathbb{N}_0^n$. Es claro que para cada $\ell \in \mathbb{N}_0$, solamente hay una cantidad finita de términos $\boldsymbol{X}^{\boldsymbol{\alpha}}$ tales que $\mathtt{M}(\boldsymbol{X}^{\boldsymbol{\alpha}}) = \ell$.
De ahora en adelante usaremos el peso usual: el peso de cada variable es igual a 1.
Sea K un campo de característica cero, denotemos por $K[[\boldsymbol{X}]]$ el anillo de series formales.

(**2.1**) **DEFINICIÓN:** Una serie formal $h \in K[[\boldsymbol{X}]]$ se dice **algebraica**, si es un elemento algebraico sobre el anillo de polinomios $K[\boldsymbol{X}]$, esto es, si existe un polinomio no nulo $Q \in K[\boldsymbol{X}, T]$ tal que $Q(\boldsymbol{X}, h(\boldsymbol{X})) = 0$.

El polinomio en la definición anterior no necesariamente debe ser mónico en T, pero puede suponerse irreducible.
Denotaremos por $K[[\boldsymbol{X}]]_{alg}$ al subanillo de series algebraicas de $K[[\boldsymbol{X}]]$, específicamente estamos interesados en el anillo de series algebraicas

$$K[[\boldsymbol{X}]]_{alg} := \{h \in K[[\boldsymbol{X}]] : h \text{ es algebraico sobre } K[\boldsymbol{X}]\}.$$

Sea $h \in K[[\boldsymbol{X}]]$, escribimos $h = \sum_{\boldsymbol{\alpha}\in\mathbb{N}_0^n} h_{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\alpha}}$, donde $h_{\boldsymbol{\alpha}} \in K$; sea $h_{(i)} := \sum_{\mathtt{M}(\boldsymbol{\alpha})=i} h_{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\alpha}}$, entonces

$$h = \sum_{i=0}^{\infty} h_{(i)},$$

y definimos:

(2.2) DATOS PRINCIPALES:

$$\begin{aligned}
\mathtt{Supp}(h) &:= \{\boldsymbol{X}^{\boldsymbol{\alpha}} : h_{\boldsymbol{\alpha}} \neq 0\}, \text{ el soporte de } h,\\
\mathtt{LT}(h) &:= \min_{<}\{\boldsymbol{X}^{\boldsymbol{\alpha}} : h_{\boldsymbol{\alpha}} \neq 0\}, \text{ el término líder de } h,\\
\mathtt{LM}(h) &:= h_{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\alpha}}, \text{ el monomio líder de } h \text{ donde } \boldsymbol{X}^{\boldsymbol{\alpha}} = \mathtt{LT}(h),\\
\mathtt{lc}(h) &:= h_{\boldsymbol{\alpha}}, \text{ el coeficiente líder de } h \text{ donde } \boldsymbol{X}^{\boldsymbol{\alpha}} = \mathtt{LT}(h),\\
\mathtt{in}(h) &:= h_{(i)}, \text{ la forma inicial de } h \text{ donde } h_{(j)} = 0\ \forall j < i,\\
\mathtt{ord}(h) = \mathtt{ord}_{\mathtt{M}}(h) &:= \min\{\mathtt{M}(\boldsymbol{\alpha}) : h_{\boldsymbol{\alpha}} \neq 0\}, \text{ el orden de } h.
\end{aligned}$$

Si R es cualquier $K-$álgebra tal que $K[\boldsymbol{X}] \subset R \subset K[[\boldsymbol{X}]]$, asociamos

- el conjunto multiplicativamente cerrado

$$S := \{f \in R \setminus \{0\} : \mathtt{LT}(f) = 1\},$$

- y el subanillo

$$S^{-1}R = \{\frac{f}{g} : f, g \in R, \mathtt{LT}(g) = 1\},$$

usaremos la notación:

$$R_{\mathfrak{m}} = \{\frac{f}{1+g} : f, g \in R, g \in \mathfrak{m} \text{ i.e. } g(\mathbf{0}) = 0\},$$

donde $\mathfrak{m} := \langle \boldsymbol{X}\rangle K[[\boldsymbol{X}]] \cap R$.
Para $h = (1+g)^{-1}f \in R_{\mathfrak{m}}$, y un ideal $I \subset R_{\mathfrak{m}}$, definimos

$$\begin{aligned}
\mathtt{LM}(h) &:= \mathtt{LM}(f)\\
\mathtt{LT}(h) &:= \mathtt{LT}(f)\\
\mathtt{LM}(I) &:= \langle \mathtt{LM}(h) : h \in I\rangle \subset K[\boldsymbol{X}]
\end{aligned}$$

2.II. Modelo computacional para series algebraicas

A continuación hacemos un resumen del modelo computacional para series algebraicas desarrollado en [2], el modelo se basa en considerar elementos de $K[[\boldsymbol{X}]]_{alg}$ como la única solución obtenida por el TFI a un *adecuado* sistema de ecuaciones polinomiales en varias variables:
Dados p polinomios

$$H_1, \ldots, H_p \in (K[\boldsymbol{X}])[\boldsymbol{Y}] = K[X_1, \ldots, X_n, Y_1, \ldots, Y_p]$$

que se anulan en el origen y los términos lineales del jacobiano de $H_1, \ldots, H_p$ con respecto a $Y_1, \ldots, Y_p$ son linealmente independientes, i.e. $\det((c_{i,j})_{i,j=1,\ldots,p}) \neq 0$, donde $c_{i,j} := \frac{\partial H_i}{\partial Y_j}(\mathbf{0}, \mathbf{0})$, $i, j = 1, \ldots, p$ y cada H_i se expresa como

$$H_i(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{j=1}^{p} c_{i,j} Y_j + A_i(\boldsymbol{X}, \boldsymbol{Y}), \qquad A_i \in \langle \boldsymbol{X} \rangle + \langle \boldsymbol{Y} \rangle^2, \qquad i = 1, \ldots, p;$$

con estas notaciones el Teorema de la Función Implícita (TFI) asegura que existen únicas series $h_1, \ldots, h_p \in K[[\boldsymbol{X}]]_{alg}$ tales que

- $h_j(\mathbf{0}) = 0$, para $j = 1, \ldots, p$, y
- $H_i(\boldsymbol{X}, h_1, \ldots, h_p) = 0$, para $i = 1, \ldots, p$.

Siguiendo con la misma notación para los polinomios $H_1, \ldots, H_p$, sin perder generalidad (cf. [2, Lema 2.1]) podemos asumir que el jacobiano $(c_{i,j})$ en el origen es una matriz triangular inferior i.e. $c_{i,j} = 0$ para $i < j$ y no singular.
En efecto, aplicamos eliminación gaussiana por filas a la matriz $C := (c_{i,j})$ obtenemos una matriz invertible $D := (d_{i,j})$ con entradas en K tal que $D\,C =: (t_{i,j})$ es triangular y no singular. Sea $H_i^*(\boldsymbol{X}, \boldsymbol{Y}) := \sum_{j=1}^{r} d_{i,j} H_j(\boldsymbol{X}, \boldsymbol{Y})$. Entonces $H_i^*(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{j=1}^{r} t_{i,j} Y_j + A_i^*(\boldsymbol{X}, \boldsymbol{Y})$, con $A_i^* \in \langle \boldsymbol{X} \rangle + \langle \boldsymbol{Y} \rangle^2$ y $H_i^*(\boldsymbol{X}, h_1, \ldots, h_p) = 0$, $\forall i = 1, \ldots, p$.

(2.3) DEFINICIÓN: El conjunto $\boldsymbol{H} := \{H_1, \ldots, H_p\}$ es llamado un **sistema localmente suave** (LSS por sus siglas en inglés *locally smooth system*) si satisface

$$\det(c_{i,j}) \neq 0 \qquad \wedge \qquad (i < j \Rightarrow c_{i,j} = 0).$$

Sea $h_1, \ldots, h_p \in K[[X_1, \ldots, X_n]]_{alg}$ la única solución del sistema de polinomios

$$H_1 = 0, \ldots, H_p = 0$$

anulándose en el origen; diremos que $\boldsymbol{H}$ es un LSS que define las h_j's; o que las h_j's están definidas por el LSS $\boldsymbol{H}$.

Según lo anterior, dado un código de Hensel siempre podemos suponer que es LSS.
Sea $(\boldsymbol{Y}, \boldsymbol{H}, \mathbf{0})$ un código de Hensel definiendo las series $h_1, \ldots, h_p \in K[[\boldsymbol{X}]]_{alg}$.
Consideramos los anillos

$$K[X_1, \ldots, X_n, h_1, \ldots, h_p] = (K[\boldsymbol{X}])[h_1, \ldots, h_p] =: P[\boldsymbol{H}],$$

donde $P := K[\boldsymbol{X}]$ es el anillo de polinomios y

$$K[X_1, \ldots, X_n, h_1, \ldots, h_p]_{\langle \boldsymbol{X}, \boldsymbol{h} \rangle} =: P[h_1, \ldots, h_p]_{\langle \boldsymbol{X}, \boldsymbol{h} \rangle} \subset K[[\boldsymbol{X}]]_{alg}.$$

Para hacer cálculos efectivos en este anillo, consideramos el morfismo de evaluación

$$\begin{aligned} \sigma_{\boldsymbol{H}} : (K[\boldsymbol{X}, \boldsymbol{Y}] / \langle \boldsymbol{H} \rangle)_{\langle \boldsymbol{X}, \boldsymbol{Y} \rangle} &\to K[[X_1, \ldots, X_n]] \\ Y_j &\mapsto \sigma_{\boldsymbol{H}}(Y_j) := h_j, \qquad j = 1, \ldots, p \end{aligned}$$

que tiene las propiedades

- $\ker(\sigma_{\boldsymbol{H}}) \supset \langle \boldsymbol{H} \rangle$, Im $(\sigma_{\boldsymbol{H}}) = P[\boldsymbol{H}]$,
- $\langle \ker(\sigma_{\boldsymbol{H}}) \rangle P[Y_1, \ldots, Y_p]_{\langle \boldsymbol{X}, \boldsymbol{Y} \rangle} = \langle \boldsymbol{H} \rangle P[Y_1, \ldots, Y_p]_{\langle \boldsymbol{X}, \boldsymbol{Y} \rangle}$,

- $P[\boldsymbol{H}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle} = P[h_1,\ldots,h_p]_{\langle \boldsymbol{X},\boldsymbol{h}\rangle} \cong P[Y_1,\ldots,Y_r]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}/\langle \boldsymbol{H}\rangle$.
  En efecto, el ideal $\langle \boldsymbol{H}\rangle$ en $P[\boldsymbol{Y}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}$ es un ideal primo, pues la $(n+p)-$upla $(\boldsymbol{0},\boldsymbol{0})$ es un punto regular de la variedad $\mathcal{V}(H_1,\ldots,H_p)$, así $\ker(\sigma_{\boldsymbol{H}}) = \langle \boldsymbol{H}\rangle P[Y_1,\ldots,Y_p]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}$, de donde $P[\boldsymbol{H}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle} \cong P[Y_1,\ldots,Y_p]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}/\langle \boldsymbol{H}\rangle$.

Por lo tanto $\sigma_{\boldsymbol{H}}$ se extiende naturalmente a un morfismo

$$P[Y_1,\ldots,Y_p]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle} \to P[h_1,\ldots,h_p]_{\langle \boldsymbol{X},\boldsymbol{h}\rangle}$$

que seguiremos denotando por $\sigma_{\boldsymbol{H}}$.
Lo anterior también demuestra que, a pesar que el código de Hensel $(\boldsymbol{Y},\boldsymbol{H},\boldsymbol{0})$ que define o *codifica* las series $\boldsymbol{h} := (h_1,\ldots,h_p)$ no es único, el ideal generado por $\boldsymbol{H}$ en el anillo local $K[\boldsymbol{X},\boldsymbol{Y}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}$ sí que lo es, pues

$$(K[\boldsymbol{X},\boldsymbol{Y}]/\langle \boldsymbol{H}\rangle)_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle} \cong K[\boldsymbol{X},\boldsymbol{h}]_{\langle \boldsymbol{X},\boldsymbol{h}\rangle}.$$

(2.4) DEFINICIÓN: Para un código de Hensel $(\boldsymbol{Y},\boldsymbol{H},\boldsymbol{0})$ dado, diremos que el **anillo de Hensel** $\mathbb{A}_{\boldsymbol{H}}$ que define es un anillo de la forma

$$\mathbb{A}_{\boldsymbol{H}} := (K[\boldsymbol{X},\boldsymbol{Y}]/\langle \boldsymbol{H}\rangle)_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}.$$

Ahora reformulamos [2, Proposición 2.2] para establecer el siguiente resultado.

(2.5) LEMA: Sea $\boldsymbol{H} := \{H_1,\ldots,H_p\} \subset K[\boldsymbol{X},\boldsymbol{Y}]$ un LSS definiendo las series $h_1,\ldots,h_p \in K[[\boldsymbol{X}]]_{alg}$, $d_i := \mathtt{deg}(H_i)$, $d := \prod_{i=1}^{p} d_i$. Entonces:

1. Para cada $j = 1,\ldots,p$, existe un polinomio $Q_j \in P[T]$ con $\mathtt{deg}(Q_j) \leq d$ tal que $Q(\boldsymbol{X}, h_j(\boldsymbol{X})) = 0$.

2. Sea $G \in P[Y_1,\ldots,Y_p]$ de grado m, y $g = \sigma_{\boldsymbol{H}}(G)$, existe un polinomio $Q \in P[T]$ de grado $\mathtt{deg}(Q) \leq dm$ tal que
   $$Q(\boldsymbol{X}, g(\boldsymbol{X})) = 0.$$
   Notar que $g(\boldsymbol{X}) = G(\boldsymbol{X}, h_1(\boldsymbol{X}),\ldots,h_p(\boldsymbol{X})) \in P[\boldsymbol{H}]$.

3. Sea $G := \frac{G_0}{1+G_1} \in P[Y_1,\ldots,Y_p]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}$, $\mathtt{deg}(G_0) \leq m$, $\mathtt{deg}(G_1) \leq m$, $G_1(\boldsymbol{0},\boldsymbol{0}) = 0$ y sea $g := \sigma_{\boldsymbol{H}}(G) \in P[\boldsymbol{H}]_{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}$, entonces existe $Q \in P[T]$, polinomio irreducible de grado $\mathtt{deg}(Q) \leq (m+1)d$ tal que
   $$Q(\boldsymbol{X}, g(\boldsymbol{X})) = 0.$$

El lema anterior permite demostrar el siguiente teorema (cf. [7, p. 600] y [2, págs. 2.3, 2.4, 2.5]).

(2.6) TEOREMA: Con la información:

- $\boldsymbol{H} := \{H_1,\ldots,H_p\}$ un LSS definiendo las series $h_1,\ldots,h_p \in K[[\boldsymbol{X}]]_{alg}$
- $d_i := \mathtt{deg}(H_i)$, $i = 1,\ldots,p$
- $d := \prod_{i=1}^{p} d_i$
- $G \in P[\boldsymbol{Y}]$
- $m := \mathtt{deg}(G)$
- $g = \sum_{i=0}^{\infty} g_{(i)} := \sigma_{\boldsymbol{H}}(G)$ expresada como suma de componentes homogéneas $g_{(i)}$ de grado i

- $Q(\boldsymbol{X},T) := \sum_{i=0}^{s} q_i T^i \in P[\boldsymbol{X},T]$, $s \leq dm$, y para cada $i = 0,1,\ldots,s$: $q_i \in P$, $\mathtt{deg}(q_i) \leq dm - i$.
  $Q(\boldsymbol{X},T)$ polinomio irreducible tal que $Q(\boldsymbol{X}, g(\boldsymbol{X})) = 0$.
- $Q^*(\boldsymbol{X},T) := T^s + \sum_{i=1}^{s} q_s^{s-i-1} q_i T^i \in P[T]$
- $u(\boldsymbol{X}) = \sum_{i=0}^{\infty} u_{(i)} := q_s g \in K[[\boldsymbol{X}]]_{alg}$

se pueden responder las siguientes cuestiones

1. $g = 0 \quad \Leftrightarrow \quad g_{(i)} = 0$ para cada $i \leq dm$;
2. $g \in P \quad \Leftrightarrow \quad g_{(i)} = 0$ para cada $i : dm < i \leq d^2m^2$;
3. $g \in P_{\langle \boldsymbol{X} \rangle} \quad \Leftrightarrow \quad u \in P$
   $\Leftrightarrow \quad u_{(i)} = 0$ para cada $i : (dm+1)^2/4 \leq i \leq (dm+1)^4/16$.

Demostración. 1. Es inmediato a partir del lema 2.5.(2).

2. Si $g \in P$, entonces $T - g$ es factor de Q y $\mathtt{deg}(T-g) \leq \mathtt{deg}(Q) \leq dm$.
   Ahora para demostrar el recíproco, escribimos

$$g = \sum_{i=0}^{\infty} g_{(i)} = g^* + g^{**}, \text{ donde}$$
$$g^* := \sum_{i=0}^{dm} g_{(i)}$$
$$g^{**} := \sum_{i=dm+1}^{\infty} g_{(i)} = \sum_{i=d^2m^2+1}^{\infty} g_{(i)}.$$

   Escribiendo $Q(\boldsymbol{X},T) = \sum_{i=0}^{s} q_i T^i$, $s \leq dm$ y para cada $i = 0,1,\ldots,s$: $q_i \in P$, $\mathtt{deg}(q_i) \leq dm - i$.

   Ahora,

$$\begin{aligned} 0 = Q(\boldsymbol{X}, g(\boldsymbol{X})) &= Q(\boldsymbol{X}, g^*(\boldsymbol{X}) + g^{**}(\boldsymbol{X})) \\ &= Q(\boldsymbol{X}, g^*(\boldsymbol{X})) + g^{**}(\boldsymbol{X}) g^{***}(\boldsymbol{X}) \end{aligned}$$

   para alguna serie $g^{***}(\boldsymbol{X}) \in K[[\boldsymbol{X}]]_{alg}$.

   Como $\mathtt{deg}(Q(\boldsymbol{X}, g^*)) \leq d^2m^2$ y $\mathtt{ord}(g^{**}) > d^2m^2$, tenemos que $Q(\boldsymbol{X}, g^*(\boldsymbol{X})) = 0$.

   Así $T - g^*$ divide a $Q(\boldsymbol{X},T)$, pero Q es irreducible, por lo tanto $T - g^* = Q = T - g$, de donde $g = g^*$.

3. Claramente $u = q_s g$ anula al polinomio $Q^*(\boldsymbol{X}, T)$:

$$\begin{aligned} Q^*(\boldsymbol{X}, q_s(\boldsymbol{X})g(\boldsymbol{X})) &= q_s^s g^s + \sum_{i=1}^{s} q_s^{s-i-1} q_i q_s^i g^i \\ &= q_s^s g^s + \sum_{i=1}^{s} q_s^{s-1} q_i g^i \\ &= q_s^{s-1}(q_s g^s + \sum_{i=1}^{s} q_i g^i) \\ &= q_s^{s-1}(\sum_{i=0}^{s} q_i g^i) \\ &= q_s^{s-1} Q(\boldsymbol{X}, g(\boldsymbol{X})) = 0. \end{aligned}$$

Además la desigualdad

$$(a+1)^2 - 4b(a-b+1) = (a-2b+1)^2 \geq 0 \Rightarrow b(a-b+1) \leq (a+1)^2/4$$

ayuda a comprobar que $\texttt{deg}(Q^*) \leq s(dm-s+1) \leq (dm+1)^2/4$.
Si $g = (1+G_1)^{-1}G_0 \in P_{\langle \boldsymbol{X} \rangle}$ tenemos que $1+G_1$ divide a q_s y $u = (1+G_1)^{-1}G_0 q_s \in P$.
Recíprocamente, supongamos que u es un polinomio que anula a $Q^*(\boldsymbol{X}, T)$, entonces:

$$g = \frac{u}{q_s} \in K(\boldsymbol{X}) \cap K[[\boldsymbol{X}]]_{alg} = P_{\langle \boldsymbol{X} \rangle}.$$

Finalmente la parte 2 que acabamos de demostrar, comprueba que

$$u \in P \quad \Leftrightarrow \quad u_{(i)} = 0 \text{ para cada } i : (dm+1)^2/4 \leq i \leq (dm+1)^4/16.$$

□

El siguiente procedimiento es una interpretación del teorema que acabamos de demostrar.

(**2.7**) **ALGORITMO:** Dado G como en el teorema anterior, es posible

- responder si $g := \sigma_{\boldsymbol{H}}(G)$ es idénticamente cero, un polinomio o una función racional,
- si $g \neq 0$ calcular $\texttt{ord}(g)$ y
- un polinomio irreducible $Q \in P[T]$, $\texttt{deg}(Q) \leq dm$ tal que $Q(\boldsymbol{X}, g(\boldsymbol{X})) = 0$.

Demostración.
- Para averiguar si g es idénticamente igual a cero es suficiente calcular $g^* = \sum_{i=0}^{dm} g_{(i)}$, entonces $g = 0 \Leftrightarrow g^* = 0$.
- si $g \neq 0$, entonces $\texttt{ord}(g) = \texttt{ord}(g^*)$.
- Para averiguar si g es un polinomio es suficiente calcular la expansión de Taylor de grado d^2m^2.
- Para averiguar si g es una función racional es suficiente calcular la expansión de Taylor de grado $(dm+1)^4/16$.
- Para encontrar el polinomio $Q = \sum_{i=0}^{dm} q_i T^i$ se suponen sus coeficientes como incógnitas cuyos valores se determinan resolviendo los sistemas lineales obtenidos cuando se iguala a cero la expresión $\sum_{i=0}^{dm} q_i \cdot (g^*)^i$.

□

2.III. Bases estándar y algoritmo del cono tangente

Aquí definimos y demostramos algunos resultados básicos sobre bases estándar para subanillos del anillo de series formales.

(2.8) DEFINICIÓN: Sea R un anillo tal que $K[\boldsymbol{X}] \subset R \subset K[[\boldsymbol{X}]]$. Sea I un ideal en R y $\{g_1, \ldots, g_s\} \subset I$. Diremos que:

1. Un elemento $g \in R$ tiene una $R-$**representación estándar** en términos de $\{g_1, \ldots, g_s\}$ si $g \in R^{\times}$ y existen $h_i \in R$ tales que $g = \sum_i h_i g_i$ y $\mathtt{LT}(h_i)\mathtt{LT}(g_i) \geq \mathtt{LT}(g), \forall i$.

2. Un elemento $h \in R$ es una $R-$**forma normal** con respecto a $\{g_1, \ldots, g_s\}$ si $g - h$ tiene una $R-$representación estándar en términos de $\{g_1, \ldots, g_s\}$ y $h = 0$ o bien $\mathtt{LM}(h) \notin \langle \mathtt{LM}(g_1), \ldots, \mathtt{LM}(g_s) \rangle$. En tal caso escribiremos $h \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$.

3. Más aún, si consideramos $\mathtt{LM}(I) := \langle \mathtt{LM}(g) : g \in I \rangle \subset K[\boldsymbol{X}]$, diremos que: $\{g_1, \ldots, g_s\}$ es una $R-$**base estándar** para I si y sólo si $\{\mathtt{LM}(g_1), \ldots, \mathtt{LM}(g_s)\}$ genera el ideal $\mathtt{LM}(I)$.

4. El anillo R tiene la **propiedad (NF)** si

   para cada $\{g_1, \ldots, g_s\}$, $g \in R$, existe alguna $R-$forma normal de g respecto a $\{g_1, \ldots, g_s\}$. (NF)

Una de las principales aplicaciones de las bases de Gröbner para anillos de polinomios consiste en responder de forma efectiva la pertenencia a un ideal:
Dado un polinomio p, un ideal I y una base de Gröbner $\mathcal{G} := \{g_1, \ldots, g_s\}$ del ideal I, entonces:

- 0 es una forma normal de g respecto a $\mathcal{G}$ si y sólo si $g \in I$,
- g tiene una forma normal no nula con a $\mathcal{G}$ si y sólo si $g \notin I$.

Un resultado similar puede obtenerse también en el caso de bases estándar; sin más restricciones, los dos casos anteriores no son excluyen mutuamente, ocurre una tercera posibilidad: que no exista forma normal de g respecto a la base estándar.

(2.9) PROPOSICIÓN: Sea R un anillo satisfaciendo (NF), $g \in R$, $I = \langle g_1, \ldots, g_s \rangle$ y supongamos que $\{g_1, \ldots, g_s\}$ es una base estándar. Entonces:

1. Si $0 \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$, entonces $g \in I$; en este caso $\mathtt{NF}(g, \{g_1, \ldots, g_s\}, R) = \{0\}$;

2. si existe $h \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R) \backslash \{0\}$, entonces $h \notin I$; en este caso si $h' \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$, entonces $h' \neq 0$, $\mathtt{LM}(h) = \mathtt{LM}(h')$, $\mathtt{LT}(h) = \text{máx}\{\mathtt{LT}(f) : g - f \in I\}$.

Demostración. 1. Si $0 \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$, entonces g tiene una $R-$representación estándar en términos de $\{g_1, \ldots, g_s\}$ y en particular pertenece a I. Supongamos que $f \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$ y $f \neq 0$, entonces $g - f$ tiene una $R-$representación estándar en términos de $\{g_1, \ldots, g_s\}$, entonces $g - f \in I$, como también $g \in I$, implica que $f \in I$, así $\mathtt{LM}(f) \in \mathtt{LM}(I)$, contradicción, pues $\mathtt{LM}(f) \notin \mathtt{LM}(I)$ porque f es una forma normal.

2. Si existe $h \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R) \setminus \{0\}$, entonces $h \notin I$, porque $\mathtt{LM}(h) \notin \mathtt{LM}(I)$, del hecho que $g - h \in I$ se sigue que $g \notin I$. Por (1) entonces $0 \notin \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$. En el caso que $h' \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$, entonces $h' \neq 0$, claramente $h - h' \in I$ y por lo tanto si $\mathtt{LM}(h) \neq \mathtt{LM}(h')$, (asumiendo por ejemplo que $\mathtt{LT}(h) \leq \mathtt{LT}(h')$), concluimos que $\mathtt{LM}(h - h') = c\,\mathtt{LM}(h)$ para cierto $c \in K \setminus \{0\}$, así $\mathtt{LM}(h) \in \mathtt{LM}(I)$, contradicción. De manera similar concluimos que no existe f tal que $h - f \in I$ y $\mathtt{LT}(f) > \mathtt{LT}(h)$.

□

(2.10) PROPOSICIÓN [2, Proposición 1.2]: Sea R un anillo satisfaciendo (NF). Sea $g_1, \ldots, g_s \in R$, $I = \langle g_1, \ldots, g_s \rangle R$. Entonces las siguientes condiciones son equivalentes:

1. $\{g_1, \ldots, g_s\}$ es una $R-$base estándar para I,
2. $\forall g \in R$: $g \in I$ si y sólo si g tiene alguna $R-$representación estándar en términos de $\{g_1, \ldots, g_s\}$,
3. $\forall g \in R$: $g \in I$ si y sólo si $0 \in \mathtt{NF}(g, \{g_1, \ldots, g_s\}, R)$.

Una consecuencia de los resultados anteriores es que al calcular bases estándar de ideales y formas normales, entonces podemos responder la pertenencia a un ideal basándonos en la propiedad 2.10.3.
Dados dos ordenes, uno $<_{\boldsymbol{X}}$ en $\mathbb{T}_{\boldsymbol{X}}$ y otro $<_{\boldsymbol{Y}}$ en $\mathbb{T}_{\boldsymbol{Y}}$ definimos el **orden producto** $<_\times := (<_{\boldsymbol{X}}, <_{\boldsymbol{Y}})$ en $\mathbb{T}_{\boldsymbol{X},\boldsymbol{Y}}$ de la siguiente manera:

$$\boldsymbol{X}^{\boldsymbol{\alpha}}\boldsymbol{Y}^{\boldsymbol{\beta}} <_\times \boldsymbol{X}^{\boldsymbol{\alpha}'}\boldsymbol{Y}^{\boldsymbol{\beta}'} \Leftrightarrow \boldsymbol{X}^{\boldsymbol{\alpha}} <_{\boldsymbol{X}} \boldsymbol{X}^{\boldsymbol{\alpha}'} \vee (\boldsymbol{X}^{\boldsymbol{\alpha}} = \boldsymbol{X}^{\boldsymbol{\alpha}'} \wedge \boldsymbol{Y}^{\boldsymbol{\beta}} <_{\boldsymbol{Y}} \boldsymbol{Y}^{\boldsymbol{\beta}'})$$

El conjunto $S_{<_\times} := \{f \in K[\boldsymbol{X}, \boldsymbol{Y}] : \mathtt{LT}_{<_\times}(f) = 1\}$ es multiplicativamente cerrado y coincide con $\{f \in K[\boldsymbol{Y}]_{<_{\boldsymbol{Y}}} : \mathtt{LT}_{<_{\boldsymbol{Y}}}(f) = 1\}$.
Por lo que

$$\begin{aligned} K[\boldsymbol{X}, \boldsymbol{Y}]_{<_\times} &:= S^{-1}_{<_\times} K[\boldsymbol{X}, \boldsymbol{Y}] \\ &= \{\frac{f}{g} : f, g \in K[\boldsymbol{X}, \boldsymbol{Y}], \mathtt{LT}_{<_\times}(g) = 1\} \\ &= \{\frac{f}{g} : f \in K[\boldsymbol{X}, \boldsymbol{Y}], g \in (K[\boldsymbol{Y}]_{<_{\boldsymbol{Y}}})^\times\} \\ &= (S^{-1}_{<_{\boldsymbol{Y}}} K[\boldsymbol{Y}])[\boldsymbol{X}] \\ &= (K[\boldsymbol{Y}]_{<_{\boldsymbol{Y}}})[\boldsymbol{X}]. \end{aligned}$$

Además el orden $<_\times$ tiene la siguiente propiedad de *eliminación* para $\boldsymbol{X}$

$$f \in K[\boldsymbol{X}, \boldsymbol{Y}], \mathtt{LM}_{<_\times}(f) \in K[\boldsymbol{Y}] \Rightarrow f \in K[\boldsymbol{Y}].$$

En efecto, si $f \notin K[\boldsymbol{Y}]$, entonces $\exists i = 1, \ldots, n; \exists m \in \mathtt{Supp}(f) : X_i$ divide a m, por lo que $\mathtt{LM}_{<_\times}(f) = t \notin K[\boldsymbol{Y}]$, lo cual es una contradicción.
Bajo las condiciones y notaciones anteriores podemos probar

(2.11) LEMA: Sea $I \subset K[\boldsymbol{X}, \boldsymbol{Y}]_{<_\times}$ un ideal. Si $G := \{g_1, \ldots, g_s\}$ es una base estándar de I, entonces

$$G' := \{g \in G : \mathtt{LM}(g) \in K[\boldsymbol{Y}]\}$$

es una base estándar para $I' := I \cap K[\boldsymbol{Y}]$. En particular, $\{g_1 \mod \langle \boldsymbol{Y} \rangle, \ldots, g_s \mod \langle \boldsymbol{Y} \rangle\}$ genera al ideal I'.

Demostración. Sea $f \in I' \subset I$, como G es una base estándar para I respecto a $<_\times$, $\exists i = 1, \ldots, s$ tal que $\mathtt{LM}_{<_\times}(g_i)$ divide a $\mathtt{LM}_{<_\times}(f)$.
Como $\mathtt{LM}_{<_\times}(f) \in K[\boldsymbol{Y}]$, tenemos que $\mathtt{LM}_{<_\times}(g_i) \in K[\boldsymbol{Y}]$ y esto implica que $g_i \in G'$.
De $\mathtt{LM}_{<_\times}(g_i) \in K[\boldsymbol{Y}]$ también se deduce (por la propiedad de eliminación que) $g_i \in K[\boldsymbol{Y}]$ y así $g_i \in I'$, de donde $G' \subset I'$. Esto demuestra que G' es una base para el ideal I'.
La última observación sigue del hecho que $I \cap \langle \boldsymbol{Y} \rangle \subset I \cap K[\boldsymbol{Y}] = I'$.

□

El siguiente teorema permite formular (cf. [8]) el Algoritmo del Cono Tangente (ACT) el cual será nuestra principal herramienta computacional para calcular bases estándar.

(2.12) TEOREMA DEL CONO TANGENTE Y ALGORITMO:

1. $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$ satisface (NF).
2. En $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$ las condiciones 1, 2 y 3 de la proposición (2.10) son equivalentes.
3. Dados $G, H_1, \ldots, H_p \in K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$, hay un algoritmo que:
   a) calcula polinomios $U, W \in K[\boldsymbol{X}]$ tales que U es una unidad de $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}$, i.e. $U(\mathbf{0}) = 1$, de manera que $U^{-1}W$ es una $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}-$forma normal de G en términos de $\{H_1, \ldots, H_p\}$,
   b) calcula polinomios $F_1, \ldots, F_r$ tales que $\{F_1, \ldots, F_r\}$ es una $K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}-$base estándar para $\langle H_1, \ldots, H_p\rangle$,
   c) responde $G \in \langle H_1, \ldots, H_p\rangle$.

(2.13) DEFINICIÓN: Sea R, I y $\{g_1, \ldots, g_s\}$ como en la definición 2.8. Diremos que:

1. Un elemento $h \in R$ es una $R-$**forma canónica** de g con respecto a $\{g_1, \ldots, g_s\}$ si $g - h$ tiene una $R-$representación estándar en términos de $\{g_1, \ldots, g_s\}$ y $h = 0$ o bien $\mathtt{Supp}(h) \cap \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_s)\rangle = \emptyset$.
2. El anillo R tiene la **propiedad (CF)** si

   para cada $\{g_1, \ldots, g_s\}$, $g \in R$, existe alguna $R-$forma canónica de g con respecto a $\{g_1, \ldots, g_s\}$. (CF)

(2.14) OBSERVACIONES:

1. El anillo $K[\boldsymbol{X}]_{loc}$ tiene la propiedad (NF) (teorema 2.12.1), sin embargo no tiene la propiedad (CF) .
2. La noción de forma canónica tiene algunas dificultades:
   - Desde el punto de vista teórico, ya que (CF) implica (NF) y el recíproco es falso, la forma canónica se puede utilizar en menos situaciones que las formas normales.
   - Desde el punto de vista computacional, la propiedad de CF no es factible, en el sentido que hasta ahora, no se conoce algún algoritmo que dados polinomios $g, g_1, \ldots, g_s$, permita responder si, $\mathtt{CF}(g, \{g_1, \ldots, g_s\}, K[[\boldsymbol{X}]]) = 0$, ni un algoritmo para calcular $K[[\boldsymbol{X}]]-$bases estándar de ideales generados por polinomios.

El modelo computacional clásico consiste en, considerar una serie algebraica $g(\boldsymbol{X})$ definida por el polinomio $Q(\boldsymbol{X}, T)$ i.e. $Q(\boldsymbol{X}, g(\boldsymbol{X})) = 0$, pero es claro que en general (incluso en el caso cuando Q es irreducible) puede que haya más de una serie anulándose en el origen y satisfaciendo $Q(\boldsymbol{X}, T) = 0$, así tendríamos que añadir a esa representación un algoritmo que permita calcular la expansión de Taylor de g hasta orden d, para todo $d \in \mathbb{N}$.
Más generalmente, dado un LSS $\boldsymbol{H}$ definiendo $\boldsymbol{h} := (h_1, \ldots, h_p)$ es posible calcular las expansiones de Taylor de las h_j's de cualquier grado, bastará entonces con determinar las derivadas de H_j respecto a las variables $\boldsymbol{X}$, esto se logra introduciendo formalmente las derivadas parciales de las "funciones" Y_j, y evaluándolas en el origen (asumiendo $Y_j(0) = 0$ obtenemos los valores de $\frac{\partial^{\boldsymbol{\alpha}} Y_j}{\partial \boldsymbol{X}^{\boldsymbol{\alpha}}}$ para multiexponentes $\boldsymbol{\alpha} \in \mathbb{N}^n$).

Recíprocamente, cualquier serie algebraica h_1 surge de esta manera: Existe un sistema de ecuaciones polinomiales multivariado $\boldsymbol{H} = \mathbf{0}$ que satisface el TFI de manera que la única solución $\boldsymbol{h}$ a este sistema tiene por primera componente a h_1. Este resultado se conoce como teorema de Artin-Mazur (cf. [2, Apéndice]), lo anterior permite codificar series algebraicas por códigos de Hensel.
La ventaja de trabajar con códigos de Hensel y no con el polinomio mínimo radica en el hecho de que este último determina la serie algebraica sólo por *conjugación*, por lo que se necesita información adicional para especificar la serie, en general un truncamiento suficientemente grande de la expansión de Taylor. En contraste con un código de Hensel, que determina *completamente* y de forma única la serie h y es relativamente más sencillo de manejar algebraicamente.
En el siguiente capítulo utilizamos lo desarrollado en esta sección para establecer el algorimo 3.12.

3. Teorema de representación

3.I. Bases del borde

El lema de Dickson [4, Teorema 5, pág 72] establece que cualquier ideal $I \subset K[\boldsymbol{X}]$ es una unión finita de octantes

$$E := \cup_{\boldsymbol{\theta}\in\mathbb{P}}(\boldsymbol{\theta} + \mathbb{N}^n), \qquad \#\mathbb{P} < \infty.$$

A los monomios que están "debajo de la escalera" (los que se identifican con $\mathbb{N}^n \setminus E$) los llamaremos **monomios estándar**. En este sentido definimos el borde de E como el conjunto

$$\Lambda(E) := \{\gamma \in E : (\exists i \in \{1,\ldots,n\})(X_i \mid \boldsymbol{X}^{\gamma} \wedge \frac{\boldsymbol{X}^{\gamma}}{X_i} \notin E)\}$$

Recursivamente definimos $j > 0$: $\Lambda^j(E) := \Lambda(E \setminus \cup_{i=1}^{j-1}\Lambda^i(E))$ y $\Lambda^0(E) = \emptyset$.
Existe una identificación natural entre $\mathbb{T}^n_{\langle \boldsymbol{X}\rangle}$ con $\mathbb{N}^n$. Por lo que para efectos formales denotaremos por $\mathtt{E} := \{\boldsymbol{X}^{\boldsymbol{\gamma}} : \boldsymbol{\gamma} \in E\}$ y por $\Lambda^j(\mathtt{E}) := \{\boldsymbol{X}^{\boldsymbol{\gamma}} : \boldsymbol{\gamma} \in \Lambda^j(E)\}$.
Tenemos varias observaciones

(3.1) PROPIEDADES:

1. La familia $\{\Lambda^i(E)\}_{i\in\mathbb{N}}$ es una partición de E.
2. Para $i \in \mathbb{N}$, si $\boldsymbol{X}^{\boldsymbol{\alpha}} \in \Lambda^i(\mathtt{E})$, entonces $\forall j = 1,\ldots,n$ se cumple que $X_j\boldsymbol{X}^{\boldsymbol{\alpha}} \in \Lambda^{i+1}(\mathtt{E})$.

2′. Inductivamente, para $\boldsymbol{\delta} \in \mathbb{N}^n$, $i \in \mathbb{N}$, si $\boldsymbol{X}^{\boldsymbol{\alpha}} \in \Lambda^i(\mathtt{E})$, entonces $\forall j = 1,\ldots,n$ se cumple que $\boldsymbol{X}^{\boldsymbol{\delta}}\boldsymbol{X}^{\boldsymbol{\alpha}} = \boldsymbol{X}^{\boldsymbol{\alpha}+\boldsymbol{\delta}} \in \Lambda^{i+\|\boldsymbol{\delta}\|_1}(\mathtt{E})$, donde $\|\boldsymbol{\delta}\|_1 = \delta_1 + \delta_2 + \ldots + \delta_n$.

3. $E \setminus \cup_{i=1}^{j-1}\Lambda^i(E)$ es un subconjunto de $\mathbb{N}^n$ cerrado bajo la suma.
4. $\Lambda^j(E) = \{\boldsymbol{\gamma} \in \mathbb{N}^n : (\exists \boldsymbol{\delta} \in \mathbb{N}^n, \|\boldsymbol{\delta}\|_1 = j)(\boldsymbol{X}^{\boldsymbol{\delta}} \mid \boldsymbol{X}^{\boldsymbol{\gamma}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\gamma}}}{\boldsymbol{X}^{\boldsymbol{\delta}}} \notin E)\}$

Probaremos la propiedad 4. Sea $F_j := \{\boldsymbol{\gamma} \in \mathbb{N}^n : (\exists \boldsymbol{\delta} \in \mathbb{N}^n, \|\boldsymbol{\delta}\|_1 = j)(\boldsymbol{X}^{\boldsymbol{\delta}} \mid \boldsymbol{X}^{\boldsymbol{\gamma}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\gamma}}}{\boldsymbol{X}^{\boldsymbol{\delta}}} \notin E)\}$.
Procedemos por inducción, para $j = 0$ el resultado es trivial
Ahora supongamos que $\forall j \leq k : \Lambda^j(E) = F_j$, y probaremos que para $j = k+1$ se cumple que $\Lambda^{k+1}(E) = F_{k+1}$. En efecto,

"$\subseteq$" Sea $\boldsymbol{\xi} \in \Lambda^{k+1}(\mathtt{E}) = \Lambda(E \setminus \cup_{i=1}^{k}\Lambda^i(E))$, entonces $\boldsymbol{\xi} \in E \wedge \boldsymbol{\xi} \notin \cup_{i=1}^{k}\Lambda^i(E)$ y $\exists i' = 1,\ldots,n$ tal que $X_{i'} \mid \boldsymbol{X}^{\boldsymbol{\xi}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{X_{i'}} \notin \mathtt{E} \setminus \cup_{i=1}^{k}\Lambda^i(\mathtt{E})$, esto implica junto con la hipótesis inductiva que

$$\frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{X_{i'}} \in \Lambda^k(\mathtt{E}) = F_k. \tag{8}$$

Por lo que, $\exists \boldsymbol{\delta} \in \mathbb{N}^n : \|\boldsymbol{\delta}\|_1 = k$, tal que $\boldsymbol{X}^{\boldsymbol{\delta}} \mid \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{X_{i'}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\xi}}/\boldsymbol{X}^{\boldsymbol{\delta}}}{X_{i'}} \notin \mathtt{E}$, equivalentemente $\boldsymbol{X}^{\boldsymbol{\delta}'} := \boldsymbol{X}^{\boldsymbol{\delta}} X_{i'} \mid \boldsymbol{X}^{\boldsymbol{\xi}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}} X_{i'}} = \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}'}} \notin \mathtt{E}$, donde $\|\boldsymbol{\delta}\|_1 = k+1$, entonces $\boldsymbol{\xi} \in F_{k+1}$.

Ahora razonamos por contradicción para probar (8). Si $\forall i = 1, \ldots, k-1$ se tiene que $\frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{X_{i'}} \in \Lambda^i(\mathtt{E}) = F_i$, entonces $\exists \boldsymbol{\delta} \in \mathbb{N}^n : \|\boldsymbol{\delta}\|_1 = i, \boldsymbol{X}^{\boldsymbol{\delta}} \mid \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{X_{i'}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}} X_{i'}} \notin \mathtt{E}$, entonces $\boldsymbol{X}^{\boldsymbol{\delta}'} \mid \boldsymbol{X}^{\boldsymbol{\xi}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}'}} \notin \mathtt{E}$, de donde $\boldsymbol{X}^{\boldsymbol{\xi}} \in \Lambda^{i+1}(\mathtt{E})$ y por lo tanto $\boldsymbol{\xi} \in \cup_{i=1}^{k} \Lambda^i(E)$, lo cual claramente es un absurdo.

"$\supseteq$" Ahora la otra inclusión. Sea $\boldsymbol{\xi} \in F_{k+1}$, entonces existe $\boldsymbol{\delta} \in \mathbb{N}^n$, tal que $\|\boldsymbol{\delta}\|_1 = k+1$, $\boldsymbol{X}^{\boldsymbol{\delta}} \mid \boldsymbol{X}^{\boldsymbol{\xi}} \wedge \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}}} \notin \mathtt{E}$.

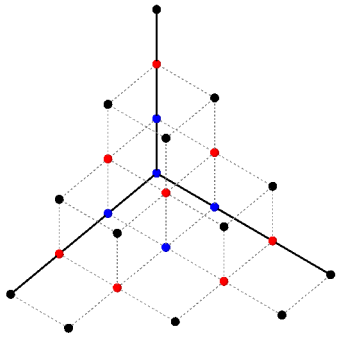
Como $\|\boldsymbol{\delta}\|_1 = k+1 > 0$, entonces $\exists i = 1, \ldots, n : \boldsymbol{X}^{\boldsymbol{\delta}} = X_i \boldsymbol{X}^{\boldsymbol{\delta}'}$, donde $\boldsymbol{\delta}' \in \mathbb{N}^n$, $\|\boldsymbol{\delta}'\|_1 = k$.

Así $X_i \mid \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}'}}$ y $\frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}}} = \frac{\boldsymbol{X}^{\boldsymbol{\xi}}/\boldsymbol{X}^{\boldsymbol{\delta}'}}{X_i} \notin \mathtt{E}$, entonces $\frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}'}} \in \Lambda(\mathtt{E})$. Por la propiedad $2'$, tenemos que $\boldsymbol{X}^{\boldsymbol{\delta}'} \frac{\boldsymbol{X}^{\boldsymbol{\xi}}}{\boldsymbol{X}^{\boldsymbol{\delta}'}} = \boldsymbol{X}^{\boldsymbol{\xi}} \in \Lambda^{1+\|\boldsymbol{\delta}'\|_1}(\mathtt{E}) = \Lambda^{k+1}(\mathtt{E})$. Entonces $\boldsymbol{\xi} \in \Lambda^{k+1}(E)$, de donde $F_{k+1} \subset \Lambda^{k+1}(E)$.

Por lo tanto $\Lambda^j(E) = F_j$, para todo $j \in \mathbb{N}$.

Los ideales que especialmente nos interesan son los cero-dimensionales, i.e. aquellos que $d := \#(\mathbb{N}^n \setminus E) < \infty$. La referencia general para bases del borde es [6, §6.6], nosotros aquí discutimos lo necesario para enmarcar la demostraciones de los resultados que enunciamos en la siguiente sección.

(3.2) EJEMPLO: Para el ideal $\langle X^2, Y^2, Z^2, XZ, YZ \rangle$, tenemos:



$$\mathcal{B} := \{1, X, Y, Z, XY\}$$
$$\Lambda(\mathcal{B}) := \{X^2, X^2Y, XY^2, Y^2, XZ, XYZ, YZ, Z^2\}$$
$$\Lambda^2(\mathcal{B}) := \{X^3, X^3Y, X^2Y^2, XY^3, Y^3, X^2Z, X^2YZ, XY^2Z, Y^2Z, XZ^2, XYZ^2, YZ^2, Z^3\}$$

De acuerdo a la ilustración del ejemplo anterior, es intuitivo una noción de proximidad de un monomio t a $\Lambda(\mathcal{B})$, esto lo formalizamos en la siguiente definición.

(3.3) DEFINICIÓN: Sea $\mathcal{B} \subset \mathbb{T}_{\langle \boldsymbol{X} \rangle}$ los monomios estándar que se identifican con F. Definimos

1. para $t \in \mathbb{T}_{\langle \boldsymbol{X} \rangle}$ el **índice de t respecto a $\mathcal{B}$** y lo denotamos por $\mathtt{ind}_{\mathcal{B}}(t)$ o simplemente $\mathtt{ind}(t)$ cuando no haya peligro de confusión al único $i \in \mathbb{N}$ tal que $t \in \Lambda^i(\mathcal{B})$.

2. para $p \in K[\boldsymbol{X}] \setminus \{0\}$ el **índice de p respecto a $\mathcal{B}$ (o el $\mathcal{B}$-índice de p)** a $\mathtt{ind}_{\mathcal{B}}(p) :=$ máx$\{\mathtt{ind}_{\mathcal{B}}(t) : t \in \mathtt{Supp}(p)\}$

Observemos que si $t \in \mathcal{B}$, entonces $\mathtt{ind}_{\mathcal{B}}(t) = 0$, en cierto sentido entonces hemos formalizado una "*medida*" o "*distancia*" que permite hablar de proximidad al borde.
El conjunto $\mathbb{T}_{\langle \boldsymbol{X} \rangle} \setminus \mathcal{B}$ es un ideal monomial, y sabemos [4, Definición 5, pág 92] que todo ideal monomial tiene un conjunto minimal de generadores, a este conjunto minimal de generadores las llamaremos **esquinas**.

3.II. Enunciado y demostración

Sea $(\mathcal{V}, \mathfrak{m}, \kappa)$ un anillo henseliano con ideal maximal $\mathfrak{m}$ y cuerpo residual $\kappa := \mathcal{V}/\mathfrak{m}$, sean $\boldsymbol{X} := (X_1, \ldots, X_n)$ variables y consideremos el anillo de polinomios $\mathcal{V}[\boldsymbol{X}]$. Dado $F \in \mathcal{V}[\boldsymbol{X}]$, denotamos por $\overline{F} \in \kappa[\boldsymbol{X}]$, al polinomio $F \mod \mathfrak{m}$ obtenido tomando módulo el ideal $\mathfrak{m}$. Asumimos que $\mathcal{V}$ contiene un cuerpo infinito. Dado un ideal I de $\mathcal{V}[\boldsymbol{X}]_{\langle \mathfrak{m}, \boldsymbol{X} \rangle}$, denotamos $I_0 = \overline{I}$ al ideal de $\kappa[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}$ generado por $\overline{F}$, para $F \in I$.
En esta situación podemos enunciar y demostrar lo siguiente:

(3.4) TEOREMA DE REPRESENTACIÓN:
Supongamos que I_0 es cero dimensional i.e. que $\kappa[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}/I_0$ es $\kappa-$espacio vectorial de dimensión finita, entonces $\mathcal{V}[X]_{\langle \mathfrak{m}, \boldsymbol{X} \rangle}/I$ es finitamente generado como $\mathcal{V}$-módulo.

Para demostrar el teorema aplicaremos las afirmaciones que hacemos y demostramos, comenzamos fijando el contexto en que haremos la demostración
Consideremos un orden total $<$ compatible con el grado en el semigrupo de las variables $\mathbb{T}_{\langle \boldsymbol{X} \rangle}$ (por ejemplo el orden lexicográfico graduado). En la sección anterior hemos visto que el conjunto E definido en el teorema se puede poner como una unión finita de octantes

$$E = \cup_{i=1}^{s} (\boldsymbol{\beta}_i + \mathbb{N}^n)$$

los $\boldsymbol{\beta}_i$ se pueden calcular de forma efectiva utilizando el (2.12-ACT). Definimos el conjunto complementario de E y lo denotaremos por $F := \mathbb{N}^n \setminus (E + \mathbb{N}^n)$.
La hipótesis de cero dimensionalidad, se traduce en que F es finito, y como conjunto de monomios forman una base del $\kappa-$espacio vectorial finito dimensional $\kappa[\boldsymbol{X}]_{\langle \boldsymbol{X} \rangle}/I_0$.
Entonces todo monomio $\boldsymbol{X}^{\boldsymbol{\beta}} \in I_0$ se puede expresar $\mod I_0$ como combinación lineal con coeficientes en κ de monomios en F. Tal combinación lineal es única.
En este caso (cero dimensional) la *forma canónica* de $\boldsymbol{X}^{\boldsymbol{\beta}}$ respecto al ideal I_0 existe porque podemos aplicar el algoritmo de Buchberger, como se hace para polinomios, tomando el término mínimo en lugar del máximo y las potencias de $\boldsymbol{X}$ suficientemente grandes son cero módulo I_0 (pues estamos en un álgebra artiniana), pero para comprobar que es cero necesitamos de una unidad. A esta forma canónica la denotamos por $\mathtt{CF}(\boldsymbol{X}^{\boldsymbol{\alpha}}, I_0)$.
Sea $B := \Lambda(E)$ el *borde* de E. Una *base standard* de I_0 es un conjunto de polinomios $g_{\boldsymbol{\alpha}}$ tales que el conjunto $\{\mathtt{LM}(g_{\boldsymbol{\alpha}})\}$ genera a I_0. Llamamos *base canónica standard del borde* al conjunto $\{g_{\boldsymbol{\alpha}} := \boldsymbol{X}^{\boldsymbol{\alpha}} - \mathtt{CF}(\boldsymbol{X}^{\boldsymbol{\alpha}}, I_0) : \boldsymbol{\alpha} \in B\}$. Tenemos que

$$g_{\boldsymbol{\alpha}} = \boldsymbol{X}^{\boldsymbol{\alpha}} + \sum_{\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}} c_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}}$$

donde $c_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \in \kappa$ y $F_{\boldsymbol{\alpha}} := \{\boldsymbol{\gamma} \in F : \boldsymbol{\gamma} < \boldsymbol{\alpha}\}$.
Para cada $\boldsymbol{\alpha} \in B$, por el ACT tenemos que existen polinomios $q_{\boldsymbol{\alpha},i} \in \kappa[\boldsymbol{X}]$, para $i = 1, \ldots, r$ y $P_{\boldsymbol{\alpha}}(\mathbf{0}) = 0$, tales que tenemos una expresión de la forma:

$$(1 + P_{\boldsymbol{\alpha}}) g_{\boldsymbol{\alpha}} = \sum_{i=1}^{r} q_{\boldsymbol{\alpha},i} \overline{F_i}$$

Definimos el **levantamiento** de $g_{\boldsymbol{\alpha}}$ (de hecho es "levantar" $(1 + P_{\boldsymbol{\alpha}}) g_{\boldsymbol{\alpha}}$ a I) y lo denotamos por

$G_{\boldsymbol{\alpha}}$:

$$\begin{aligned} G_{\boldsymbol{\alpha}} :&= \sum_{i=1}^{r} q_{\boldsymbol{\alpha},i} F_i \\ &= \sum_{i=1}^{r} q_{\boldsymbol{\alpha}} (\overline{F_i} + m_{\boldsymbol{\alpha},i} F^*_{\boldsymbol{\alpha},i}) \qquad m_{\boldsymbol{\alpha},i} \in \mathfrak{m}, F^*_{\boldsymbol{\alpha},i} \in \mathcal{V}[\boldsymbol{X}] \\ &= \sum_{i=1}^{r} q_{\boldsymbol{\alpha},i} \overline{F_i} + \sum_{i=1}^{r} q_{\boldsymbol{\alpha},i} m_{\boldsymbol{\alpha},i} F_{\boldsymbol{\alpha},i} \\ &= g_{\boldsymbol{\alpha}}(1 + P_{\boldsymbol{\alpha}}) + m_{\boldsymbol{\alpha}} H_{\boldsymbol{\alpha}} \qquad m_{\boldsymbol{\alpha}} \in \mathfrak{m}, H_{\boldsymbol{\alpha}} \in \mathcal{V}[\boldsymbol{X}] \end{aligned}$$

Observar que el coeficiente de $\boldsymbol{X}^{\boldsymbol{\alpha}}$ en $G_{\boldsymbol{\alpha}}$ es una unidad de $\mathcal{V}[\boldsymbol{X}]$, i.e. es de la forma $1 + d_{\boldsymbol{\alpha}}$, para algún $d_{\boldsymbol{\alpha}} \in \mathfrak{m}$, y en $G_{\boldsymbol{\alpha}}$ pueden aparecer términos $\boldsymbol{X}^{\boldsymbol{\beta}}$ con $\boldsymbol{\beta} < \boldsymbol{\alpha}$, pero sus coeficientes serán elementos de $\mathfrak{m}$.

Demostración. Introducimos un conjunto de nuevas indeterminadas $\boldsymbol{A} := \{A_{\boldsymbol{\alpha},\boldsymbol{\gamma}}\}$, y consideramos *polinomios formales* i.e. los coeficientes son también variables. Para cada $\boldsymbol{\alpha} \in B$ definimos:

$$\widetilde{G_{\boldsymbol{\alpha}}} := \boldsymbol{X}^{\boldsymbol{\alpha}} + \sum_{\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}} (c_{\boldsymbol{\alpha},\boldsymbol{\gamma}} - A_{\boldsymbol{\alpha},\boldsymbol{\gamma}}) \boldsymbol{X}^{\boldsymbol{\gamma}}.$$

Simplificamos cada $G_{\boldsymbol{\alpha}}$ que daba lugar residualmente a un elemento de la base estándar del borde (por la respectiva unidad) con los polinomios formales $\{\widetilde{G_{\boldsymbol{\alpha}}}\}$, reduciendo cada monomio $\boldsymbol{X}^{\boldsymbol{\beta}}$ del soporte de $G_{\boldsymbol{\alpha}}$ que es múltiplo de algún $\boldsymbol{X}^{\boldsymbol{\alpha}'} : \boldsymbol{\alpha}' \in B$ i.e. $\boldsymbol{X}^{\boldsymbol{\beta}} = \boldsymbol{X}^{\boldsymbol{\mu}} \boldsymbol{X}^{\boldsymbol{\alpha}'}$ con $\boldsymbol{X}^{\boldsymbol{\mu}} \widetilde{G_{\boldsymbol{\alpha}'}}$.
Esta reducción la hacemos recursivamente considerando como coeficientes los $\boldsymbol{A}$'s y los elementos de $\mathcal{V}$.
Veamos que este proceso es finito: un monomio de la forma $\boldsymbol{X}^{\boldsymbol{\beta}}$ tiene las siguientes posibilidades:

1. $\boldsymbol{\beta} \in F$, ya está reducido y pasa directamente al resto,
2. $\boldsymbol{\beta} \in B$, se reduce en un paso con $\widetilde{G_{\boldsymbol{\beta}}}$, este caso aporta al resto $\sum_{\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}} A_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}}$,
3. $\boldsymbol{\beta} \in E \setminus B$:
   - 3.1 Si $\boldsymbol{\beta}$ está a distancia 1 del borde i.e. $\boldsymbol{X}^{\boldsymbol{\beta}} = X_i \boldsymbol{X}^{\boldsymbol{\alpha}}$, restamos $X_i \widetilde{G_{\boldsymbol{\alpha}}}$ y esto aporta términos $X^{\boldsymbol{\gamma}} X_i$ con $X^{\boldsymbol{\gamma}} \in F$, que o están en F o están en el borde de E, por tanto a distancia 0.
   - 3.2 Recursivamente según la distancia al borde de E.

Siguiendo con este proceso podemos reducir monomios que están a cualquier distancia del borde y como la escalera es finita, logramos reducir monomio de cualquier grado.
Notemos que en cada paso introducimos un producto de la forma

- $m_{\boldsymbol{X}} \widetilde{G_{\boldsymbol{\alpha}}}; m_{\boldsymbol{X}} \in \langle \boldsymbol{X} \rangle$ (tipo de reducción 3.1),
- $m_{\boldsymbol{X}} v; v \in \mathcal{V}$ (tipo de reducción 2),
- $m_{\boldsymbol{X}} m_{\boldsymbol{A}}; m_{\boldsymbol{A}} \in \langle \boldsymbol{A} \rangle$ (tipo de reducción 3.2).

Por tanto, después de una cantidad finita de reducciones, llegamos a una igualdad de la forma:

$$G_{\boldsymbol{\alpha}} = \sum_{\boldsymbol{\alpha}' \in B} Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}(\boldsymbol{A},\ \boldsymbol{X}) \widetilde{F}_{\boldsymbol{\alpha}'} + \sum_{\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}} R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}(\boldsymbol{A}, \boldsymbol{X}) \boldsymbol{X}^{\boldsymbol{\gamma}} \tag{9}$$

donde $Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'} \in \mathcal{V}[\boldsymbol{A}, \boldsymbol{X}]$ y $R_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \in \mathcal{V}[\boldsymbol{A}]$.
Esta igualdad tiene las siguientes propiedades:

(3.5) PROPIEDAD:

$$\mathtt{in}(G_{\boldsymbol{\alpha}}) = \sum_{\boldsymbol{\alpha}' \in B} \mathtt{in}(Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'})\mathtt{in}(\widetilde{G_{\boldsymbol{\alpha}'}})$$

Demostración. Es consecuencia del proceso de reducción que hemos hecho. □

(3.6) PROPIEDAD: En el proceso de reducción de $G_{\boldsymbol{\alpha}}$ nunca se usa para reducir una expresión de la forma $m_{\boldsymbol{A}} u_{\mathcal{V}} \widetilde{G_{\boldsymbol{\beta}}}$, con $\boldsymbol{\beta} < \boldsymbol{\alpha}$, $m_{\boldsymbol{A}} \in \langle \boldsymbol{A} \rangle$, $u_{\mathcal{V}}$ unidad de $\mathcal{V}$.

Demostración. Los monomios a reducir de

$$G_{\boldsymbol{\alpha}} = g_{\boldsymbol{\alpha}} + g_{\boldsymbol{\alpha}} P_{\boldsymbol{\alpha}} + m_{\boldsymbol{\alpha}} H_{\boldsymbol{\alpha}}$$

provienen de:

- $g_{\boldsymbol{\alpha}}$, para reducirlos no se una un monomio $m_{\boldsymbol{A}}$.
- $m_{\boldsymbol{\alpha}} H_{\boldsymbol{\alpha}}$, para reducir un monomio del soporte de $m_{\boldsymbol{\alpha}} H_{\boldsymbol{\alpha}}$ es necesario introducir un elemento del ideal maximal $\mathfrak{m}$, por lo tanto no es de la forma descrita.
- $g_{\boldsymbol{\alpha}} P_{\boldsymbol{\alpha}}$, sea $\boldsymbol{X}^{\boldsymbol{\sigma}}$ un monomio del soporte de $g_{\boldsymbol{\alpha}} P_{\boldsymbol{\alpha}}$. Claramente su coeficiente en $G_{\boldsymbol{\alpha}}$ es una unidad u de $\mathcal{V}$ (pues residualmente aparece).
  - si $\boldsymbol{\sigma} < \boldsymbol{\alpha}$ ya está reducido,
  - sin $\boldsymbol{\sigma} \geq \boldsymbol{\alpha}$ debemos reducirlo, lo reducimos $u\boldsymbol{X}^{\boldsymbol{\sigma}}$ con $u\boldsymbol{X}^{\boldsymbol{\sigma}-\boldsymbol{\alpha}_1}\widetilde{G_{\boldsymbol{\alpha}_1}}$, lo cual produce monomios de la forma $u m_{\boldsymbol{A}} \boldsymbol{X}^{\sigma-\boldsymbol{\alpha}_1+\boldsymbol{\alpha}_2}$, con $\boldsymbol{\alpha}_2 \leq \boldsymbol{\alpha}_1$ si ya están reducidos, no se utilizó un reductor de la forma descrita. En el caso que necesiten ser reducidos, su reductor es de la forma $u\ m'_{\boldsymbol{A}} \boldsymbol{X}^{\boldsymbol{\sigma}'} \widetilde{G_{\bullet}}$ el cual no es de la forma descrita.

□

(3.7) PROPIEDAD: En el proceso de reducción de $G_{\boldsymbol{\alpha}}$ sólo se usa $(1+d_{\boldsymbol{\alpha}})\widetilde{G_{\boldsymbol{\alpha}}}$, donde $1+d_{\boldsymbol{\alpha}}$ es el coeficiente de $\boldsymbol{X}^{\boldsymbol{\alpha}}$.

Demostración. En efecto, recordemos que $d_{\boldsymbol{\alpha}} \in \mathfrak{m}$, si se una como reductor una expresión de la forma $(1+_{\boldsymbol{\alpha}})m_{\boldsymbol{A}}\widetilde{G_{\boldsymbol{\beta}}}$, con $\boldsymbol{\alpha} \leq \boldsymbol{\beta}$ es porque en la reducción anterior se hizo la reducción $(1+d_{\boldsymbol{\alpha}})\widetilde{G_{\boldsymbol{\alpha}}}$ (para reducir $\boldsymbol{X}^{\boldsymbol{\alpha}}$ y esta reducción produce monomios de la forma $m_{\boldsymbol{A}}(1+d_{\boldsymbol{\alpha}})\boldsymbol{X}^{\boldsymbol{\sigma}}$ con $\boldsymbol{\sigma} < \boldsymbol{\alpha}$ los cuales ya están reducidos, con lo que $\boldsymbol{\sigma} < \boldsymbol{\beta}$, lo cual es absurdo, pues $\boldsymbol{\beta} < \boldsymbol{\sigma}$ (las reducciones bajan el grado). □

(3.8) PROPIEDAD: El sistema $\boldsymbol{S} := \{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}} = 0 : \boldsymbol{\alpha} \in B, \boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}\}$ es cuadrado.

Demostración. La cantidad de variables es $\ell := \#\{(\boldsymbol{\alpha},\boldsymbol{\gamma}) \in B \times F : \boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}\}$.
Para cada $\boldsymbol{\alpha} \in B$ salen $\#F_{\boldsymbol{\alpha}}$ ecuaciones, así la cantidad de ecuaciones es $\#\{(\boldsymbol{\alpha},\boldsymbol{\gamma}) \in B \times F : \boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}\}$, i.e. hay ℓ ecuaciones. □

(3.9) PROPIEDAD: Cuando pasamos al cuerpo residual i.e. en $\kappa[\boldsymbol{A}]$ el sistema $\boldsymbol{S}$ tiene por solución $\boldsymbol{0} \in \kappa^{\ell}$.

Demostración. En efecto,

$$\begin{aligned}\overline{G_{\boldsymbol{\alpha}}} &= \overline{g_{\boldsymbol{\alpha}}(1+P_{\boldsymbol{\alpha}}) + m_{\boldsymbol{\alpha}}H_{\boldsymbol{\alpha}}} \\ &= g_{\boldsymbol{\alpha}}(1+\overline{P_{\boldsymbol{\alpha}}}) \\ &= \sum_{\boldsymbol{\alpha}'\in B} \overline{Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}}(\mathbf{0},\boldsymbol{X})\widetilde{\overline{g_{\boldsymbol{\alpha}'}}} + \sum_{\boldsymbol{\gamma}\in F_{\boldsymbol{\alpha}}} \overline{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}}(\mathbf{0})\boldsymbol{X}^{\boldsymbol{\gamma}} \\ &= \sum_{\boldsymbol{\alpha}'\in B} \overline{Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}}(\mathbf{0},\boldsymbol{X})g_{\boldsymbol{\alpha}'} + \sum_{\boldsymbol{\gamma}\in F_{\boldsymbol{\alpha}}} \overline{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}}(\mathbf{0})\boldsymbol{X}^{\boldsymbol{\gamma}}\end{aligned}$$

como $\{g_{\boldsymbol{\alpha}}\}$ son una base estándar de I_0 tenemos que $\overline{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}}(\mathbf{0})$ tienen que ser cero. □

Ahora vamos a probar que el término lineal de las ecuaciones del sistema $\boldsymbol{S}$ es una matriz triangular superior con 1's en la diagonal. Esto implicará que $\mathbf{0}$ es la única solución del sistema. Para ver esto, la clave está ordenar las ecuaciones $R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}$ en orden creciente para los $\boldsymbol{\gamma}$'s y decreciente para los $\boldsymbol{\alpha}$'s es decir, ordenamos las parejas

$$(\boldsymbol{\alpha},\boldsymbol{\gamma}) <^* (\boldsymbol{\alpha}',\boldsymbol{\gamma}') \Leftrightarrow \boldsymbol{\gamma} < \boldsymbol{\gamma}' \vee (\boldsymbol{\gamma}' = \boldsymbol{\gamma}' \wedge \boldsymbol{\alpha} > \boldsymbol{\alpha}').$$

Más específicamente demostraremos:

(3.10) LEMA: Para $\boldsymbol{\alpha} \in B$ y $\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}$, se tiene que en la parte de lieneal del polinomio $\overline{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}}$ aparece $A_{\boldsymbol{\alpha},\boldsymbol{\gamma}}$ con coeficiente 1, y eventualmente otros $A_{\boldsymbol{\alpha}',\boldsymbol{\gamma}'}$, con $(\boldsymbol{\alpha}',\boldsymbol{\gamma}') <^* (\boldsymbol{\alpha},\boldsymbol{\gamma})$.

Demostración. Esto es consecuencia del proceso de reducción: Comenzamos reduciendo $\boldsymbol{X}^{\boldsymbol{\alpha}}$ con $\widetilde{G_{\boldsymbol{\alpha}}}$ esto aporta al resto $-\sum_{\boldsymbol{\gamma}'\in F_{\boldsymbol{\alpha}}} A_{\boldsymbol{\alpha},\boldsymbol{\gamma}'}\boldsymbol{X}^{\boldsymbol{\gamma}'}$. Entonces $A_{\boldsymbol{\alpha},\boldsymbol{\gamma}}$ forma parte del coeficiente de $\boldsymbol{X}^{\boldsymbol{\gamma}}$ en $R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}$ y por tanto al pasar al cuerpo residual también es parte del coeficiente de $\boldsymbol{X}^{\boldsymbol{\gamma}}$ en $\overline{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}}$.
Ahora reducimos $\boldsymbol{X}^{\boldsymbol{\beta}} \in \mathtt{Supp}G_{\boldsymbol{\alpha}} \cap E$, existen $\boldsymbol{\alpha}_1 \in B$ y $\boldsymbol{\mu}_1 \in \mathbb{N}^n$ tales que $\boldsymbol{\beta} = \boldsymbol{\alpha}_1 + \boldsymbol{\mu}_1$, el reductor es $\boldsymbol{X}^{\boldsymbol{\mu}_1}\widetilde{G_{\boldsymbol{\alpha}_1}}$ produciendo términos de la forma $A_{\boldsymbol{\alpha}_1,\boldsymbol{\gamma}'}\boldsymbol{X}^{\boldsymbol{\mu}_1+\boldsymbol{\gamma}'}$.
Si para algún $\boldsymbol{\gamma}_1 : \boldsymbol{\mu}_1+\boldsymbol{\gamma}_1 = \boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}$, entonces este monomio ya está reducido y pasa directamente al resto, apareciendo en la parte lineal de $R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}$ y por tanto en la parte lineal de $\overline{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}}$.
Observemos que

- si $\boldsymbol{\mu}_1 \neq \mathbf{0}$ entonces $\boldsymbol{\gamma}_1 < \boldsymbol{\gamma}$
- si $\boldsymbol{\mu}_1 = \mathbf{0}$ entonces $\boldsymbol{\alpha}_1 = \boldsymbol{\beta} > \boldsymbol{\alpha}$

Además todos los términos de grado uno en las $\boldsymbol{A}$'s aparecen de esta forma: a saber, en el primer paso de reducción de un monomio $\boldsymbol{X}^{\boldsymbol{\sigma}} \in \mathtt{Supp}\widetilde{G_{\boldsymbol{\alpha}}}$.
Nótese también que los términos reducidos que aparecen en $g_{\boldsymbol{\alpha}}$ $(c_{\boldsymbol{\alpha},\boldsymbol{\gamma}}\boldsymbol{X}^{\boldsymbol{\gamma}} : \boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}})$ no pasan al resto, sino que se cancelan en la primera reducción con $\widetilde{G_{\boldsymbol{\alpha}}}$ i.e. $R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}$ no tiene término independiente.
Otros términos que van al resto son términos ya reducidos de $\widetilde{G_{\boldsymbol{\alpha}}}$ que ya estaban reducidos cuyos coeficientes son elementos del maximal $\mathfrak{m}$, o bien términos de grado mayor que uno en las $\boldsymbol{A}$'s. □

Por el LHM la solución $(A_{\boldsymbol{\alpha},\boldsymbol{\gamma}})$ se levanta en $\mathcal{V}^\ell$ a una única solución $\boldsymbol{\xi} := (\xi_{\boldsymbol{\alpha},\boldsymbol{\gamma}})_{\boldsymbol{\alpha}\in B,\boldsymbol{\gamma}\in F_{\boldsymbol{\alpha}}}$ tal que para cada $(\boldsymbol{\alpha},\boldsymbol{\gamma}) \in B \times F_{\boldsymbol{\alpha}}$:

$$\xi_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \in \mathcal{V}, \quad \overline{\xi_{\boldsymbol{\alpha},\boldsymbol{\gamma}}} = A_{\boldsymbol{\alpha},\boldsymbol{\gamma}} = 0 \quad \text{y} \quad R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}(\boldsymbol{\xi}) = 0.$$

Denotaremos por $Q^{\boldsymbol{\xi}}_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}(\boldsymbol{X}) := Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}(\boldsymbol{\xi},\boldsymbol{X})$, de la misma forma escribiremos $\widetilde{G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}}} \in \mathcal{V}[\boldsymbol{X}]$, al resultado de especializar $\widetilde{G_{\boldsymbol{\alpha}}}$ en $\boldsymbol{\xi}$. Como $\boldsymbol{A}_{\boldsymbol{\alpha},\boldsymbol{\gamma}} = 0$, resulta que $\widetilde{\overline{G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}}}} = g_{\boldsymbol{\alpha}}$ y $R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}(\boldsymbol{\xi}) = 0$, $\forall \alpha \in B, \boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}$. Además

(3.11) LEMA: $\det(Q^{\boldsymbol{\xi}}_{\boldsymbol{\alpha},\boldsymbol{\alpha}'})$ es una unidad en $\mathcal{V}[\boldsymbol{X}]_{\langle \boldsymbol{X},\mathfrak{m}\rangle}$.

Demostración. Es suficiente probar que $\overline{Q^{\boldsymbol{\xi}}_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}(\mathbf{0})} = \overline{Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}}(\mathbf{0},\mathbf{0}) = \delta_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}$, para $\boldsymbol{\alpha}' \leq \boldsymbol{\alpha}$, esto implicará que $Q^{\boldsymbol{\xi}}_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}(\mathbf{0}) \notin \mathfrak{m}$, y por tanto $\det(Q^{\boldsymbol{\xi}}_{\boldsymbol{\alpha},\boldsymbol{\alpha}'})$, es una unidad en $\mathcal{V}[\boldsymbol{X}]_{\langle \boldsymbol{X},\mathfrak{m}\rangle}$, como queremos ver.
En efecto, por la propiedad 3.6 tenemos que $\overline{Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}}(\mathbf{0},\mathbf{0})$ para todo $\boldsymbol{\alpha}' < \boldsymbol{\alpha}$, y la propiedad 3.7 implica que $\overline{Q_{\boldsymbol{\alpha},\boldsymbol{\alpha}}}(\mathbf{0},\mathbf{0}) = 1$. □

Sustituyendo en la ecuación (9) se obtiene:

$$G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}} = \sum_{\boldsymbol{\alpha}' \in B} Q^{\boldsymbol{\xi}}_{\boldsymbol{\alpha},\boldsymbol{\alpha}'}(\boldsymbol{X})\widetilde{G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}'}}$$

y por tanto, para todo $\boldsymbol{\alpha} \in B$ se tiene que $G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}} \in I$. Además, para todo $\boldsymbol{\alpha}' \in B$

$$\widetilde{G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}'}} = \boldsymbol{X}^{\boldsymbol{\alpha}'} + \sum_{\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}'}} \xi_{\boldsymbol{\alpha}',\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}} \in I$$

Entonces, cada monomio en las $\boldsymbol{X}$'s se expresa en $\mathcal{V}[\boldsymbol{X}]/I$ como una combinación lineal de monomios $\{\boldsymbol{X}^{\boldsymbol{\alpha}} : \alpha \in F\}$ con coeficientes en $\mathcal{V}$.
Para terminar de probar (3.4), debemos comprobar que es posible representar cualquier una unidad como combinación de estos mismos monomios, y así probaremos que el conjunto $\{\boldsymbol{X}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in F\}$ genera a $\mathcal{V}_{\langle \boldsymbol{X},\mathfrak{m}\rangle}[\boldsymbol{X}]/I$.
En efecto, sea $H/(1+Q)$, $H, Q \in \mathcal{V}[\boldsymbol{X}]$, con $\overline{Q}(\mathbf{0}) = 0$ esto es, $Q \in \langle \mathfrak{m}, \boldsymbol{X}\rangle$. Sean $\boldsymbol{D} := \{D_{\boldsymbol{\gamma}} : \boldsymbol{\gamma} \in F\}$, un conjunto de nuevas indeterminadas.
Definimos el polinomio en las $\boldsymbol{X}$'s y $\boldsymbol{D_\gamma}$'s con coeficientes en $\mathcal{V}$

$$H - (1+Q)(\sum_{\gamma \in F} D_\gamma \boldsymbol{X}^\gamma) \tag{10}$$

Aplicando el proceso de reducción con los polinomios formales $\{\widetilde{G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}}} = \boldsymbol{X}^{\boldsymbol{\alpha}} + \sum_{\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}} \xi_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}} : \boldsymbol{\alpha} \in B\}$, y reduciendo como hemos descrito los monomios en las $\boldsymbol{X}$'s que están en E, conseguimos un resto $\sum R_{\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}}$, donde $R_{\boldsymbol{\gamma}}$'s son polinomios en las $D_{\boldsymbol{\gamma}}$'s con coeficientes en $\mathcal{V}$. La parte lineal del sistema $\{R_{\boldsymbol{\gamma}} = 0\}$ es triangular en las $D_{\boldsymbol{\gamma}}$'s, por el 1 de $(1+Q)$ en la ecuación (10), tiene una única solución $\boldsymbol{d} := (d_{\boldsymbol{\gamma}})$ con $d_{\boldsymbol{\gamma}} \in \mathcal{V}$. Entonces, $H = (1+Q)(\sum_{\boldsymbol{\gamma} \in F} d_{\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}})$ mód $\langle \widetilde{G^{\boldsymbol{\xi}}_{\boldsymbol{\alpha}}} \rangle$ y por tanto mód I.

□

En el caso particular que $\mathcal{V}$ es un anillo de series de potencias formales, algebraicas o analíticas con coeficientes en K, este teorema es consecuencia del teorema de división de Mather. También es un caso particular de la división de Weierstrass con parámetros. Nuestro caso es muy particular, puesto que módulo el ideal maximal $\mathfrak{m}$ de $\mathcal{V}$ tenemos un anillo cero dimensional. Este hecho, junto con la propiedad de ser henseliano (más concretamente el TFI) nos permitió dar una prueba constructiva del siguiente teorema. Por otro lado, no hemos asumido ninguna propiedad de finitud sobre $\mathcal{V}$, como ser noetheriano, etc.

3.III. Algoritmo

Ahora retomamos las ideas fundamentales de las secciones anteriores para formular un algoritmo que permite trabajar y representar de forma dinámica series algebraicas, esto con el objetivo de hacer efectivo nuestro teorema de representación.
Comenzamos demostramos que la forma canónica existe en el anillo local cuando se hace respecto a un ideal cero dimensional.
En efecto, I un ideal de polinomios, generado por los polinomios $F_1, \ldots, F_r$, denotaremos por I^e al ideal generado en $K[X]_{(X)}$, si este es cero dimensional existe una potencia $\boldsymbol{X}^m \subset IK[X]_{(X)}$, así para cada monomio $\boldsymbol{X}^\alpha$ tal que el grado: $\alpha_1 + \ldots + \alpha_n = m$ existe una expresión:

$$u_\alpha \cdot \boldsymbol{X}^\alpha = \sum_{i=1}^{r} Q_i F_i,$$

donde u_α, Q_i, F_i son polinomios, y u_α unidades i.e. $u_\alpha(0, \ldots, 0) = 1$.
Además la expresión anterior se puede encontrar con el algoritmo del Cono Tangente de Mora (ver algoritmo 3.12), en particular dividiendo por u_α, el algoritmo 3.12 da una representación estándar de $\boldsymbol{X}^\alpha$ en función de la base estándar (los coeficientes, serán Q_i/u_α que claramente están en el anillo local).

(3.12) ALGORITMO: Notación $\mathtt{LM}_<(f)$ representa el término mínimo.

1. Se determina $\mathtt{LM}_<(I^e)$ para un orden local $<$, calculando una base estándar (formada por polinomios) $F_1, \ldots, F_r$ (por ejemplo con el algoritmo de Mora)

2. Se comprueba que $\mathtt{LM}_<(I^e) = \langle M(F_1), \ldots, M(F_r)\rangle$ tiene complementario finito, es decir, contiene una potencia $\boldsymbol{X}^{m'}$. Entonces los términos mínimos de los F_i deben tener grados menor o igual que m'.

3. Sea $\boldsymbol{X}^\alpha \in \boldsymbol{X}^{m'}$, $\alpha_1 + \ldots + \alpha_n = m'$, donde g es polinomio y veamos que $x^\alpha \in I^e$.
   Con el algoritmo de forma normal de Mora se escribe:

$$\boldsymbol{x}^\alpha \cdot u_\alpha = \sum_{i=1}^{r} F_i Q_i + h \tag{11}$$

   donde Q_i, h son polinomios y $\mathtt{LM}(Q_i)\mathtt{LM}(F_i) \geq \mathtt{LM}\langle \boldsymbol{x}^\alpha\rangle = x^\alpha$ y $M(h) \notin M(I^e)$ y $u_\alpha(0, \ldots, 0) = 1$.

¿Si $h \neq 0$ quien es $\mathtt{LM}(h)$?

- Si $\mathtt{LM}(h) < x^\alpha$ como $x^\alpha \leq M(Q_i)M(F_i)$ no podrá $M(h)$ irse con nada en el miembro d e de la derecha ni tampoco de la izquierda de 11.

- Si $\mathtt{LM}(h) > \boldsymbol{x}^\alpha$ el grado de $\mathtt{LM}(h)$ es mayor que m' o igual por ser el orden compatible (porque hablamos de mínimo si fuera de máximo sería anticompatible) con el grado. Entonces también los otros términos del soporte de h que son mayores que $\mathtt{LM}(h)$ tendrán grado mayor o igual que m' y por tanto $h \in \langle \boldsymbol{X}^{m'}\rangle = \mathtt{LM}(I^e)$.

Entonces $h = 0$ y tengo $\boldsymbol{x}^\alpha \cdot u_\alpha = \sum_{i=1}^{r} F_i Q_i$ con $\mathtt{LM}(Q_i)\mathtt{LM}(F_i) \geq \mathtt{LM}(\boldsymbol{x}^\alpha) = \boldsymbol{x}^\alpha$.
Ahora dado un polinomio $G(\boldsymbol{X})$ polinomio se simplifica "a la Buchberger" con los F_i de la base estándar y el resto tiene términos ya simplificados (y por tanto debajo de la escalera) que se agrupan en h_0 o bien otros de grados cada vez mayor, pues son cada vez mayores respecto al orden $<$ (ya que consideramos el mínimo y en grado son compatibles).

Asi se obtiene

$$G = \sum_{i=1}^{r} H_i F_i + h_0 + h_1 \tag{12}$$

con $\mathtt{LM}(H_i)\mathtt{LM}(F_i) \geq \mathtt{LM}(G)$ y $\mathtt{LM}(h_1)$ es de grado mayor o igual que m' y $\mathtt{LM}(h_0)$ tiene todos sus términos que no están en $\mathtt{LM}(I^e)$ es decir por debajo de la escalera.
Por lo que hemos visto antes $h_1 \in I^e$. Entonces G mód $I^e = h_0$ con todos los términos debajo de la escalera y si se quiere mas h_1 tiene una representación estándar en términos de la base estándar $\{F_i : i = 1, \ldots, r\}$ (obviamente lo que acompaña a los F_i son elementos del anillo local no polinomios).
Por tanto usando 12, también la $G - h_0$ tiene una representación estándar en términos de los F_i, es claro que los coeficientes que acompañan a los F_i también pertenecen al anillo local.
h_0 es la forma canónica de G respecto de I^e.

3.IV. Aplicación

En el caso que el anillo henseliano $\mathcal{V}$ se la henselización del anillo local $(R := K[\boldsymbol{T}], \mathfrak{m} := \langle \boldsymbol{T} \rangle)$, donde $\boldsymbol{T} := (T_1, \ldots, T_n)$.
Hemos visto en el capítulo 1, sabemos que R^h es el límite de álgebras elementales de Hensel, i.e.

$$R^h = \lim A[Z]_{\mathfrak{q}} \diagup \langle g(Z) \rangle$$

donde $g(Z)$ es un polinomio de Hensel, y $\mathfrak{q}$ un ideal primo de $A[Z]$ que está sobre el ideal maximal $\mathfrak{m}_A$.
Entonces, teóricamente se pueden considerar códigos de Hensel univariados $(Z, g, 0)$, pero en la práctica dados $\boldsymbol{G} := \{G_1, \ldots, G_s\} \subset \mathcal{V}[\boldsymbol{X}]$ existe un código de Hensel multivariado

$$(\boldsymbol{Y} := (Y_1, \ldots, Y_p), \boldsymbol{H} := \{H_i(\boldsymbol{T}, \boldsymbol{Y}) = 0 : i = 1, \ldots, p\}, \boldsymbol{0})$$

definiendo el anillo

$$A_{\boldsymbol{H}} = K[\boldsymbol{T}, \boldsymbol{Y}]_{\langle \boldsymbol{T}, \boldsymbol{Y} \rangle} \diagup \langle \boldsymbol{H} \rangle$$

de manera que $G_j(\boldsymbol{T}, \boldsymbol{Y}; \boldsymbol{X}) \in K[\boldsymbol{T}, \boldsymbol{Y}][\boldsymbol{X}]$ son polinomios en las $\boldsymbol{X}$'s con coeficientes en las T's y las $\boldsymbol{Y}$'s, donde las $\boldsymbol{Y}$'s definen (por el TFI) define únicas series codificadas $y_1, \ldots, y_p \in K[[\boldsymbol{T}]]_{alg}$.
Así, $\mathcal{V}$ es una extensión de tipo esencialmente finita y concretamente podemos suponer que cada ideal de $\mathcal{V}[\boldsymbol{X}]$ involucra una cantidad finita de polinomios en $\mathcal{V}[\boldsymbol{X}]$, y por tanto una cantidad finita de monomios cuyos coeficientes vienen dados en un anillo de Hensel $A_{\boldsymbol{H}}$ y existe una base estándar para el ideal $I := \langle \boldsymbol{G} \rangle$ definida por polinomios.
Al considerar el siguiente diagrama

$$\begin{array}{ccc} K[[\boldsymbol{T}]] & \hookrightarrow & K[[\boldsymbol{T}, \boldsymbol{X}]] \\ \uparrow & & \uparrow \\ K[\boldsymbol{T}]_{\langle \boldsymbol{T} \rangle} & \hookrightarrow & (K[\boldsymbol{T}, \boldsymbol{Y}, \boldsymbol{X}] \diagup \langle \boldsymbol{H} \rangle)_{\langle \boldsymbol{T}, \boldsymbol{Y}, \boldsymbol{X} \rangle} \end{array}$$

las inclusiones verticales tienen la propiedad que son fielmente planas pues son entre anillos noetherianos, locales y $K[[\boldsymbol{T}]]$ (resp. $K[[\boldsymbol{T}, \boldsymbol{X}]]$) es el completado de $K[\boldsymbol{T}]_{\langle \boldsymbol{T} \rangle}$ (resp. $(K[\boldsymbol{T}, \boldsymbol{Y}, \boldsymbol{X}] \diagup \langle \boldsymbol{H} \rangle)_{\langle \boldsymbol{T}, \boldsymbol{Y}, \boldsymbol{X} \rangle}$) con la topología $\langle \boldsymbol{T} \rangle-$ádica (resp. $\langle \boldsymbol{T}, \boldsymbol{X} \rangle-$ádica), por lo que son planas y por (1.4) son fielmente planas.
El diagrama anterior, implica que las inclusiones del siguiente diagrama

$$\begin{array}{ccc} K[[\boldsymbol{T}]]_{alg} & \hookrightarrow & \mathcal{V}[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}/I \\ \uparrow & & \uparrow \\ K[\boldsymbol{T}]_{\langle \boldsymbol{T}\rangle} & \hookrightarrow & (\mathcal{V}[\boldsymbol{Y},\boldsymbol{X}]/\langle \boldsymbol{H},\boldsymbol{G}\rangle)_{\langle \boldsymbol{T},\boldsymbol{Y},\boldsymbol{X}\rangle} \end{array}$$

tienen las mismas propiedades. Tomando módulo el ideal maximal de $\mathbb{A}_{\boldsymbol{H}}$ (que en nuestro caso equivale hacer $(\boldsymbol{T},\boldsymbol{Y}) = (\boldsymbol{0},\boldsymbol{0})$), denotamos

$$\begin{aligned} \text{para } j = 1,\ldots,s: \qquad \overline{G_j} &:= G_j(\boldsymbol{T},\boldsymbol{Y};\boldsymbol{X}) \mod \langle \boldsymbol{T},\boldsymbol{Y}\rangle \\ &= G_j(\boldsymbol{0},\boldsymbol{0};\boldsymbol{X}) \in K[\boldsymbol{X}] \end{aligned}$$

obtenemos:

$$\begin{array}{ccc} K & \hookrightarrow & D := \mathcal{V}[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}/I \\ & \searrow & \uparrow \\ & & C := K[\boldsymbol{X}]_{\langle \boldsymbol{X}\rangle}/I_0 \end{array}$$

donde

$$I_0 := \{G_j(\boldsymbol{0},\boldsymbol{0};\boldsymbol{X}) : j = 1,\ldots,s\}.$$

Residualmente podemos verificar si D es cero dimensional i.e. $d := \dim_K C < \infty$, en tal caso C es un $K-$espacio vectorial de dimensión finita. Denotando por B al conjunto de multiexponentes de $\mathbb{T}_{\boldsymbol{X}}$ de monomios que están por debajo de la escalera de I_0, podemos encontrar una base reducida de I_0 y por tanto tener expresiones, (reglas de reescritura) de la forma

$$\boldsymbol{X}^{\boldsymbol{\alpha}} + \sum_{\boldsymbol{\gamma}\in F_{\boldsymbol{\alpha}}} \xi_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}}, \qquad \boldsymbol{\alpha} \in B,$$

donde $F_{\boldsymbol{\alpha}}$ es un subconjunto de multiexponentes por debajo de la escalera de I_0 y $\xi_{\boldsymbol{\alpha},\boldsymbol{\gamma}} \in V = K[[\boldsymbol{T}]]_{alg}$ son series que vienen definidas explícitamente por el código (en general más grande al primero $\mathbb{A}_{\boldsymbol{H}} \subset \mathbb{A}_{\boldsymbol{H}'}$)

$$(\{A_{\boldsymbol{\alpha},\boldsymbol{\gamma}}, Y_i : (\boldsymbol{\alpha},\boldsymbol{\gamma}) \in B\times F_{\boldsymbol{\alpha}}, i = 1,\ldots,p\}, \boldsymbol{H}' := \{R_{\boldsymbol{\alpha},\boldsymbol{\gamma}}(\boldsymbol{T},\boldsymbol{Y};\boldsymbol{A}), H_j : (\boldsymbol{\alpha},\boldsymbol{\gamma}) \in B\times F_{\boldsymbol{\alpha}}, j = 1,\ldots,p\}, \boldsymbol{0}).$$

Pues hemos visto que ordenando adecuadamente las ecuaciones del sistema $\boldsymbol{H}'$ el jacobiano es una matriz triangular.
Estas expresiones bajo la hipótesis de cero-dimensionalidad permiten reescribir cualquier elemento de $\Theta \in \mathcal{V}[\boldsymbol{X}]$ módulo I como combinación de monomios $\boldsymbol{X}^{\boldsymbol{\gamma}}$ debajo de la escalera ($\boldsymbol{\gamma} \in F_{\boldsymbol{\alpha}}$) con coeficientes en $\mathcal{V}$:

$$\Theta \mod I = \sum_{\boldsymbol{\gamma}\in F} v_{\boldsymbol{\gamma}} \boldsymbol{X}^{\boldsymbol{\gamma}}.$$

Para hacer todos estos cálculos necesitamos determinar si un elemento es cero o no es cero en $\mathbb{A}_{\boldsymbol{H}'}$ y es ahí donde hacemos uso del algoritmo 3.12.

3.V. Ejemplo

Terminamos exponiendo un ejemplo concreto adaptando la notación para que la lectura sea más fluida, hemos hecho uso de un CAS para realizar los cálculos que indicamos.

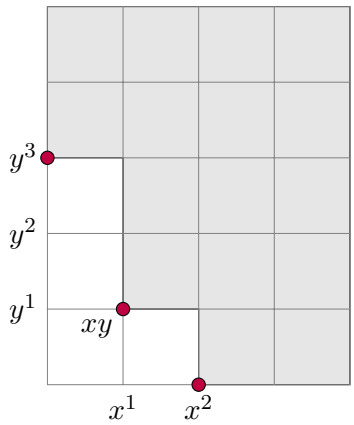
Sea $(\mathcal{V}, \mathfrak{m}, \kappa) := (K[z]_{\langle z\rangle}, \langle z\rangle, K)$, $\mathcal{V}[\boldsymbol{X}] := \mathcal{V}[x, y]$, con ideal maximal $\langle x, y, z\rangle$,

$$\begin{aligned} F_1 &:= xy + xy^2 + y^3 + 2x^3y + xyz^2 & \overline{F_1} &:= xy + xy^2 + y^3 + 2x^3y \\ F_2 &:= x^2 + xy^2 + y^3 + x^3y + xy^2z^3 & \overline{F_2} &:= x^2 + xy^2 + y^3 + x^3y \\ F_3 &:= x^2 + xy + 2xy^2 + x^3y - y^3z^4 & \overline{F_3} &:= x^2 + xy + 2xy^2 + x^3y \\ I &:= \langle F_1, F_2, F_3\rangle & I_0 &:= \langle \overline{F_1}, \overline{F_2}, \overline{F_3}\rangle \end{aligned}$$

Calculamos una base estándard para I_0

$$\begin{aligned} \overline{F_1} - \overline{F_2} + \overline{F_3} &= 2xy(\underbrace{1 + x^2 + y}_{u}) \Rightarrow xy \in I_0 \\ \overline{F_3} - \overline{F_2} &= xy(\underbrace{1 + y}_{v}) - y^3 \Rightarrow y^3 \in I_0 \\ \overline{F_3} &= x^2 + xy(\underbrace{1 + 2y + x^2}_{w}) \Rightarrow x^2 \in I_0 \end{aligned}$$

El ideal $\mathtt{LM}(I_0) := \langle x^2, xy, y^3\rangle$ es cero dimensional, el borde es $\Lambda(I_0) = \{y^3, xy^2, xy, x^2\}$ y su respectiva escalera es $\{1, x, y, y^2\}$.



Por las igualdades anteriores tenemos que

$$\begin{aligned} 2u \cdot xy &= \overline{F_1} - \overline{F_2} + \overline{F_3} \\ 2u \cdot y^3 &= v\overline{F_1} + (2u - v)\overline{F_2} + (v - 2u)\overline{F_3} \\ 2u \cdot x^2 &= -w\overline{F_1} + w\overline{F_2} + (2u - w)\overline{F_3} \\ 2u \cdot xy^2 &= y(\overline{F_1} - \overline{F_2} + \overline{F_3}) \end{aligned}$$

Definimos los levantamientos de cada elemento de la base canónica del borde (recordemos que "levantamos" el elemento del borde multiplicado por su respectiva unidad):

$$
\begin{aligned}
G_1 &:= F_1 - F_2 + F_3 \\
&= 2xy + 2x^3y + 2xy^2 + xyz^2 - xy^2z^3 - y^3z^4
\end{aligned}
$$

$$
\begin{aligned}
G_2 &:= vF_1 + (2u - v)F_2 + (v - 2u)F_3 \\
&= 2y^3 + 2x^2y^3 + 2y^4 + xyz^2 + xy^2z^2 + xy^2z^3 + 2x^3y^2z^3 + xy^3z^3 + y^3z^4 + 2x^2y^3z^4 + y^4z^4
\end{aligned}
$$

$$
\begin{aligned}
G_3 &:= -wF_1 + wF_2 + (2u - w)F_3 \\
&= 2x^2 + 2x^4 + 2x^2y - xyz^2 - x^3yz^2 - 2xy^2z^2 + xy^2z^3 + x^3y^2z^3 + 2xy^3z^3 - y^3z^4 - x^2y^3z^4
\end{aligned}
$$

$$
\begin{aligned}
G_4 &:= y(F_1 - F_2 + F_3) \\
&= 2xy^2 + 2x^3y^2 + 2xy^3 + xy^2z^2 - xy^3z^3 - y^4z^4
\end{aligned}
$$

Ahora definimos los polinomios formales:

$$
\begin{aligned}
\widetilde{G_1} &:= xy - (a_0 + a_1x + a_2y + a_3y^2) \\
\widetilde{G_2} &:= y^3 - (b_0 + b_1x + b_2y + b_3y^2) \\
\widetilde{G_3} &:= x^2 - (c_0 + c_1x + c_2y + c_3y^2) \\
\widetilde{G_4} &:= xy^2 - (d_0 + d_1x + d_2y + d_3y^2)
\end{aligned}
$$

donde $a_0, a_1, a_2, a_3, b_0, \ldots, d_3$ son 16 variables cuyos valores vamos a determinar.
El siguiente paso es reducir los G_1, G_2, G_3 y G_4 con los $\widetilde{G_i}$'s

1. Reducción de G_1 con los $\widetilde{G_i}$'s
   Al reducir G_1 respectivamente con $\widetilde{G_2}$, $\widetilde{G_4}$, $\widetilde{G_3}$, $\widetilde{G_3}$, $\widetilde{G_4}$, $\widetilde{G_1}$ y $\widetilde{G_2}$, obtenemos:

   $-z^4b_0 - d_0z^3 + 2a_0c_1^2 + 2a_0c_3d_1 + a_0z^2 + 2b_0c_1c_3 + 2b_0c_3d_3 + 2a_0c_0 + 2c_2d_0 + 2a_0 + 2d_0 + (-b_1z^4 - d_1z^3 + 2a_1c_1^2 + 2a_1c_3d_1 + a_1z^2 + 2b_1c_1c_3 + 2b_1c_3d_3 + 2a_1c_0 + 2c_2d_1 + 2a_1 + 2d_1)x + (-b_2z^4 - d_2z^3 + 2a_2c_1^2 + 2a_2c_3d_1 + a_2z^2 + 2b_2c_1c_3 + 2b_2c_3d_3 + 2a_2c_0 + 2c_0c_1 + 2c_2d_2 + 2c_3d_0 + 2a_2 + 2d_2)y + (-b_3z^4 - d_3z^3 + 2a_3c_1^2 + 2a_3c_3d_1 + a_3z^2 + 2b_3c_1c_3 + 2b_3c_3d_3 + 2a_3c_0 + 2c_1c_2 + 2c_2d_3 + 2c_3d_2 + 2a_3 + 2d_3)y^2 =: E_1 + E_2x + E_3y + E_4y^2$

2. Reducción de G_2 con los $\widetilde{G_i}$'s
   Al reducir G_2 respectivamente con $\widetilde{G_2}$, $\widetilde{G_2}$, $\widetilde{G_4}$, $\widetilde{G_4}$, $\widetilde{G_4}$, $\widetilde{G_3}$, $\widetilde{G_3}$, $\widetilde{G_4}$, $\widetilde{G_2}$, $\widetilde{G_4}$, $\widetilde{G_1}$ y $\widetilde{G_2}$, obtenemos:

   $2b_0c_0z^4 + b_1c_0z^3 + 2c_0d_0z^3 + 2b_3c_0d_1 + 2b_1c_0c_1z^4 + 2c_0c_1d_1z^3 + 2b_1c_0c_1 + 2d_0b_1c_3 + a_0z^2 + 2a_0b_1 + (2a_3b_1c_2z^4 + 2a_3b_2c_1z^4 + 2a_3b_3d_2z^4 + 2b_1c_1c_3z^4 + 2b_1c_3d_3z^4 + 2b_2b_3c_3z^4 + 2b_3c_3d_1z^4 + 2b_3d_3^2z^4 + a_3b_1z^4 + 2a_3c_1d_2z^3 + 2a_3c_2d_1z^3 + 2a_3d_2d_3z^3 + 2b_0c_3z^4 + 2b_2c_2z^4 + b_3^2z^4 + 2b_3c_3d_2z^3 + 2c_1c_3d_1z^3 + 4c_3d_1d_3z^3 + 2d_3^3z^3 + a_3b_2z^3 + b_1c_3z^3 + b_2z^4 + b_3d_3z^3 + b_3z^4 + 2c_2d_2z^3 + 2c_3d_0z^3 + d_3z^3 + 2a_3b_1c_2 + 2a_3b_2c_1 + 2a_3b_3d_2 + a_3z^2 + 2b_1c_1c_3 + 2b_1c_3d_3 + 2b_2b_3c_3 + 2b_3c_3d_1 + 2b_3d_3^2 + d_3z^2 + 2a_3b_1 + 2b_0c_3 + 2b_2c_2 + 2b_3^2 + 2b_2 + 2b_3)y^2 + (2a_2b_1c_2z^4 + 2a_2b_2c_1z^4 + 2a_2b_3d_2z^4 + 2b_1c_1c_2z^4 + 2b_1c_3d_2z^4 + 2b_2^2c_3z^4 + 2b_3c_2d_1z^4 + 2b_3d_2d_3z^4 + a_2b_1z^4 + 2a_2c_1d_2z^3 + 2a_2c_2d_1z^3 + 2a_2d_2d_3z^3 + 2b_0c_2z^4 + b_2b_3z^4 + 2b_2c_0z^4 + 2b_2c_3d_2z^3 + 2c_1c_2d_1z^3 + 2c_2d_1d_3z^3 + 2c_3d_1d_2z^3 + 2d_2d_3^2z^3 + a_2b_2z^3 + b_0z^4 + b_1c_2z^3 + b_2z^4 + b_3d_2z^3 + 2c_0d_2z^3 + 2c_2d_0z^3 + d_2z^3 + 2a_2b_1c_2 + 2a_2b_2c_1 + 2a_2b_3d_2 + a_2z^2 + 2b_1c_1c_2 + 2b_1c_3d_2 + 2b_2^2c_3 + 2b_3c_2d_1 + 2b_3d_2d_3 + d_2z^2 + 2a_2b_1 + 2b_0c_2 + 2b_2b_3 + 2b_2c_0 + 2b_0 + 2b_2)y + 2b_0b_3 + 2b_0b_2c_3z^4 + 2b_0c_3d_2z^3 + 2a_0b_1c_2z^4 + 2a_0b_3d_2z^4 + 2a_0c_1d_2z^3 + 2a_0c_2d_1z^3 + 2a_0d_2d_3z^3 + 2a_0b_2c_1z^4 + 2d_0b_3d_3z^4 + 2b_3c_0d_1z^4 + 2c_0d_1d_3z^3 + d_0b_3z^3 + (2a_1b_1c_2z^4 + 2a_1b_2c_1z^4 + 2a_1b_3d_2z^4 +$

$2b_1b_2c_3z^4+2b_1c_1^2z^4+2b_1c_3d_1z^4+2b_3c_1d_1z^4+2b_3d_1d_3z^4+a_1b_1z^4+2a_1c_1d_2z^3+2a_1c_2d_1z^3+2a_1d_2d_3z^3+2b_0c_1z^4+b_1b_3z^4+2b_1c_0z^4+2b_1c_3d_2z^3+2b_3d_0z^4+2c_1^2d_1z^3+2c_1d_1d_3z^3+2c_3d_1^2z^3+2d_1d_3^2z^3+a_1b_2z^3+b_1c_1z^3+b_1z^4+b_3d_1z^3+2c_0d_1z^3+2c_1d_0z^3+2d_0d_3z^3+b_0z^3+d_1z^3+2a_1b_1c_2+2a_1b_2c_1+2a_1b_3d_2+a_1z^2+2b_1b_2c_3+2b_1c_1^2+2b_1c_3d_1+2b_3c_1d_1+2b_3d_1d_3+d_1z^2+2a_1b_1+2b_0c_1+2b_1b_3+2b_1c_0+2b_3d_0+2b_1)x+2b_0b_2c_3+a_0b_2z^3+d_0z^2+2a_0b_2c_1+2a_0b_1c_2+2a_0b_3d_2+a_0b_1z^4+d_0z^3+b_0b_3z^4+2d_0b_1c_3z^4+2d_0c_3d_1z^3+z^4b_0+2d_0b_3d_3+2d_3^2z^3d_0+2b_0c_0+2b_0=:E_5+E_6x+E_7y+E_8y^2$

3. Reducción de G_3 con los $\widetilde{G_i}$'s
   Al reducir G_3 respectivamente con $\widetilde{G_2}$, $\widetilde{G_4}$, $\widetilde{G_4}$, $\widetilde{G_4}$, $\widetilde{G_3}$, $\widetilde{G_3}$, $\widetilde{G_4}$, $\widetilde{G_1}$, $\widetilde{G_2}$, $\widetilde{G_1}$ y $\widetilde{G_2}$, obtenemos:

   $-b_0c_0z^4+2b_1c_0z^3+c_0d_0z^3-b_0b_2c_3z^4+b_0c_3d_2z^3-b_0c_1c_3z^2-b_0c_3d_3z^2-b_1c_0c_1z^4+c_0c_1d_1z^3+4b_0c_2c_3-a_0z^2+(-a_1b_1c_2z^4-a_1b_2c_1z^4-a_1b_3d_2z^4-b_1b_2c_3z^4-b_1c_1^2z^4-b_1c_3d_1z^4-b_3c_1d_1z^4-b_3d_1d_3z^4+a_1c_1d_2z^3+a_1c_2d_1z^3+a_1d_2d_3z^3-b_0c_1z^4-b_1c_0z^4+b_1c_3d_2z^3-b_3d_0z^4+c_1^2d_1z^3+c_1d_1d_3z^3+c_3d_1^2z^3+d_1d_3^2z^3+2a_1b_2z^3-a_1c_1^2z^2-a_1c_3d_1z^2-b_1c_1c_3z^2+2b_1c_1z^3-b_1c_3d_3z^2-b_1z^4+2b_3d_1z^3+c_0d_1z^3+c_1d_0z^3+d_0d_3z^3+2a_1b_1c_3^2-a_1c_0z^2+2b_0z^3+2b_1b_3c_3^2-c_2d_1z^2+d_1z^3+4a_1c_1c_2-a_1z^2+4b_1c_2c_3+2c_1^3+4c_1c_3d_1-2d_1z^2+2a_1c_1+2b_1c_3+4c_0c_1+2c_1)x+2b_0b_3c_3^2-a_0b_1c_2z^4-a_0b_3d_2z^4+a_0c_1d_2z^3+a_0c_2d_1z^3+a_0d_2d_3z^3-a_0b_2c_1z^4+2b_1c_3^2a_0-d_0b_3d_3z^4-b_3c_0d_1z^4+c_0d_1d_3z^3-a_0c_3d_1z^2+2c_0c_1^2+2d_0b_3z^3+2a_0b_2z^3-2d_0z^2+2c_0^2+d_0z^3-d_0b_1c_3z^4+d_0c_3d_1z^3-a_0c_1^2z^2-a_0c_0z^2+4a_0c_1c_2+2a_0c_1-z^4b_0+2b_0c_3+d_3^2z^3d_0-c_2d_0z^2+4c_1d_0c_3+2c_0+(-a_3b_1c_2z^4-a_3b_2c_1z^4-a_3b_3d_2z^4-b_1c_1c_3z^4-b_1c_3d_3z^4-b_2b_3c_3z^4-b_3c_3d_1z^4-b_3d_3^2z^4+a_3c_1d_2z^3+a_3c_2d_1z^3+a_3d_2d_3z^3-b_0c_3z^4-b_2c_2z^4+b_3c_3d_2z^3+c_1c_3d_1z^3+2c_3d_1d_3z^3+d_3^3z^3+2a_3b_2z^3-a_3c_1^2z^2-a_3c_3d_1z^2+2b_1c_3z^3-b_3c_1c_3z^2-b_3c_3d_3z^2+2b_3d_3z^3-b_3z^4+c_2d_2z^3+c_3d_0z^3+2a_3b_1c_3^2-a_3c_0z^2+2b_3^2c_3^2-c_1c_2z^2-c_2d_3z^2-c_3d_2z^2+d_3z^3+4a_3c_1c_2-a_3z^2+2b_2c_3^2+4b_3c_2c_3+2c_1^2c_3+4c_1c_3d_3-2d_3z^2+2a_3c_1+2b_3c_3+4c_0c_3+2c_2^2+2c_2+2c_3)y^2+(-a_2b_1c_2z^4-a_2b_2c_1z^4-a_2b_3d_2z^4-b_1c_1c_2z^4-b_1c_3d_2z^4-b_2^2c_3z^4-b_3c_2d_1z^4-b_3d_2d_3z^4+a_2c_1d_2z^3+a_2c_2d_1z^3+a_2d_2d_3z^3-b_0c_2z^4-b_2c_0z^4+b_2c_3d_2z^3+c_1c_2d_1z^3+c_2d_1d_3z^3+c_3d_1d_2z^3+d_2d_3^2z^3+2a_2b_2z^3-a_2c_1^2z^2-a_2c_3d_1z^2+2b_1c_2z^3-b_2c_1c_3z^2-b_2c_3d_3z^2-b_2z^4+2b_3d_2z^3+c_0d_2z^3+c_2d_0z^3+2a_2b_1c_3^2-a_2c_0z^2+2b_2b_3c_3^2-c_0c_1z^2-c_2d_2z^2-c_3d_0z^2+d_2z^3+4a_2c_1c_2-a_2z^2+2b_0c_3^2+4b_2c_2c_3+2c_1^2c_2+4c_1c_3d_2-2d_2z^2+2a_2c_1+2b_2c_3+4c_0c_2+2c_0+2c_2)y=:E_9+E_{10}x+E_{11}y+E_{12}y^2$

4. Reducción de G_4 con los $\widetilde{G_i}$'s
   Al reducir G_4 respectivamente con $\widetilde{G_2}$, $\widetilde{G_2}$, $\widetilde{G_4}$, $\widetilde{G_4}$, $\widetilde{G_4}$, $\widetilde{G_3}$, $\widetilde{G_3}$, $\widetilde{G_4}$, $\widetilde{G_1}$ y $\widetilde{G_2}$, obtenemos:

   $-a_0b_1z^4-b_0b_3z^4-a_0b_2z^3-b_1c_0z^3-d_0b_3z^3+2a_0c_1d_2+2a_0c_2d_1+2a_0d_2d_3+2b_0c_3d_2+2c_0c_1d_1+2c_0d_1d_3+2c_3d_1d_0+2d_3^2d_0+d_0z^2+2a_0b_2+2b_1c_0+2b_3d_0+2c_0d_0+2d_0+(-a_1b_1z^4-b_1b_3z^4-a_1b_2z^3-b_1c_1z^3-b_3d_1z^3-b_0z^3+2a_1c_1d_2+2a_1c_2d_1+2a_1d_2d_3+2b_1c_3d_2+2c_1^2d_1+2c_1d_1d_3+2c_3d_1^2+2d_1d_3^2+d_1z^2+2a_1b_2+2b_1c_1+2b_3d_1+2c_0d_1+2c_1d_0+2d_0d_3+2b_0+2d_1)x+(-a_2b_1z^4-b_2b_3z^4-a_2b_2z^3-b_0z^4-b_1c_2z^3-b_3d_2z^3+2a_2c_1d_2+2a_2c_2d_1+2a_2d_2d_3+2b_2c_3d_2+2c_1c_2d_1+2c_2d_1d_3+2c_3d_1d_2+2d_2d_3^2+d_2z^2+2a_2b_2+2b_1c_2+2b_3d_2+2c_0d_2+2c_2d_0+2d_2)y+(-a_3b_1z^4-b_3^2z^4-a_3b_2z^3-b_1c_3z^3-b_2z^4-b_3d_3z^3+2a_3c_1d_2+2a_3c_2d_1+2a_3d_2d_3+2b_3c_3d_2+2c_1c_3d_1+4c_3d_1d_3+2d_3^3+d_3z^2+2a_3b_2+2b_1c_3+2b_3d_3+2c_2d_2+2c_3d_0+2d_3)y^2=:E_{13}+E_{14}x+E_{15}y+E_{16}y^2$

Observamos que el sistema $H:=\{E_i=0:i=1,\dots,16\}$ tiene jacobiano no nulo en el origen, esto implica que el sistema H determina únicos valores para las variables $a_0,a_1,a_2,a_3,b_0,\dots,d_3$. Por lo tanto H codifica únicas series algebraicas

$$\boldsymbol{h}:=(h_1,h_2,\dots,h_{16})\in\mathcal{V}^{16}.$$

Así, hemos determinado los coeficientes de los polinomios "*formales* $\widetilde{G_i}$'s":

$$\begin{aligned}
\widetilde{G_1} &:= xy - (h_1 + h_2x + h_3y + h_4y^2)\\
\widetilde{G_2} &:= y^3 - (h_5 + h_6x + h_7y + h_8y^2)\\
\widetilde{G_3} &:= x^2 - (h_9 + h_{10}x + h_{11}y + h_{12}y^2)\\
\widetilde{G_4} &:= xy^2 - (h_{13} + h_{14}x + h_{15}y + h_{16}y^2)
\end{aligned}$$

las cuales son "reglas de reescritura", pues permiten reescribir cualquier elemento de $\mathcal{V}[\boldsymbol{X}]_{\langle \mathfrak{m}, \boldsymbol{X}\rangle}$ en términos de la base del espacio vectorial $(\mathcal{V}/\mathfrak{m})[\boldsymbol{X}]/I_0$ y coeficientes en $\mathcal{V}$, como lo explicamos a continuación.

Supongamos que queremos representar $\dfrac{1+z}{1+x^2+z^2}$. Para ello, introducimos las variables D_0, D_1, D_2, D_3, tales que

$$\frac{1+z}{1+x^2+z^2} = D_0 + D_1x + D_2y + D_3y^2, \tag{13}$$

y definimos el polinomio

$$P := 1 + z - (1 + x^2 + z^2)(D_0 + D_1x + D_2y + D_3y^2).$$

Luego, reducimos a P con los polinomios $\widetilde{G_1}$, $\widetilde{G_2}$, $\widetilde{G_2}$, $\widetilde{G_3}$, $\widetilde{G_3}$, $\widetilde{G_3}$, $\widetilde{G_4}$, $\widetilde{G_4}$, $\widetilde{G_3}$, $\widetilde{G_3}$ y $\widetilde{G_1}$ obteniendo:
$-D_1h_1h_{12}h_{16} - D_1h_{16}h_{10}h_9 - D_2h_1h_{12}^2 - D_2h_{12}h_{10}h_9 - D_0z^2 - D_1h_{13}h_{14} - D_1h_{15}h_9 - D_2h_{10}h_{13} - D_2h_{11}h_9 - D_3h_{13}h_6 - D_3h_8h_5 - D_3h_7h_9 - D_0h_{13} - D_0 + z + 1 + (-D_1h_{10}^2h_{16} - D_1h_{12}h_{16}h_2 - D_2h_{10}^2h_{12} - D_2h_{12}^2h_2 - D_1h_{10}h_{15} - D_1h_{14}^2 - D_1z^2 - D_2h_{10}h_{11} - D_2h_{10}h_{14} - D_3h_{10}h_7 - D_3h_{14}h_6 - D_3h_6h_8 - D_0h_{14} - D_1h_{13} - D_2h_9 - D_3h_5 - D_1)x + (-D_1h_{10}h_{11}h_{16} - D_1h_{12}h_{16}h_3 - D_2h_{10}h_{11}h_{12} - D_2h_{12}^2h_3 - D_1h_{11}h_{15} - D_1h_{14}h_{15} - D_1h_{16}h_9 - D_2h_{10}h_{15} - D_2h_{11}^2 - D_2h_{12}h_9 - D_2z^2 - D_3h_{11}h_7 - D_3h_{15}h_6 - D_3h_7h_8 - D_0h_{15} - D_2)y + (-D_1h_{10}h_{12}h_{16} - D_1h_{12}h_{16}h_4 - D_2h_{10}h_{12}^2 - D_2h_{12}^2h_4 - D_1h_{11}h_{16} - D_1h_{12}h_{15} - D_1h_{14}h_{16} - D_2h_{10}h_{16} - 2D_2h_{11}h_{12} - D_3h_{12}h_7 - D_3h_{16}h_6 - D_3h_8^2 - D_3z^2 - D_0h_{16} - D_3)y^2 =: S_1 + S_2x + S_3y + S_4y^2$.
Al resolver el sistema lineal $\{S_1 = 0, S_2 = 0, S_3 = 0, S_4 = 0\}$ en D_0, D_1, D_2, D_3, determinamos únicos valores en términos de $h_1, \ldots, h_{12}$, que permiten escribir la representación (13) deseada.

A. Teoremas sobre dimensión de anillos locales

En este apéndice recordamos algunos teoremas y resultados de Álgebra Conmutativa que involucran dimensión de anillos locales noetherianos o localizaciones y completaciones y que en cierto modo han formado parte de nuestro curso de Máster o que, siendo un poco más específicos, hemos tenido que utilizar en el texto.
Las referencias para las demostraciones de estos resultados son [3, 10].

(A.1) TEOREMA [3, Teorema 9.2]: Sea A un dominio local noetheriano de dimensión 1, $\mathfrak{m}$ su ideal maximal y $k := A/\mathfrak{m}$ su cuerpo de fracciones. Son equivalentes:

1. A es un Anillo de Valoración Discreta (AVD).
2. A es íntegramente cerrado.
3. $\mathfrak{m}$ es un ideal principal.
4. $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$

El siguiente es el *Teorema del Ideal Principal* (TIP), cuya interpretación geométrica es que si intersecamos un conjunto algebraico con una hipersuperficie que no contiene ninguna componente irreducible, y no es constante en dicho conjunto, la dimensión baja exactamente en 1.

(A.2) TEOREMA TIP - [3, Teorema 11.17]: Sea A un anillo, $a \in A$ no unidad ni divisor de cero. Los asociados primos minimales de aA tienen altura 1.

Enunciamos ahora una caracterización en el conjunto de anillos noetherianos, debida a Serre, de aquellos que son íntegramente cerrados en su anillo total de fracciones (eg. normales). Nos dice que además de la propiedad de ser las localizaciones en ideales primos de altura 1 anillos regulares (como afirma el teorema mencionado arriba [3, Teorema 9.2]), los anillos normales verifican la propiedad (2) del teorema siguiente, cuya interpretación geométrica es que las funciones racionales con indeterminación de codimensión ≥ 2 se extienden a funciones regulares.

(A.3) TEOREMA [5, Teorema 4.4.11]: Sea R un anillo noetheriano reducido $Q(R)$ su anillo total de fracciones. Entonces R es normal en $Q(R)$ si y solamente si se verifican las dos condiciones siguientes:

1. **(R1)** Para todo $\mathfrak{p} \in \operatorname{Spec} R$ tal que $\mathtt{ht}(\mathfrak{p}) = 1$, $R_{\mathfrak{p}}$ es un anillo local regular.
2. **(S2)** Para todo $f \in R$, f no divisor de cero, el ideal $\langle f \rangle$ no tiene ideales primos asociados sumergidos[1].

Demostración. Demostramos únicamente la parte que utilizamos en (1.16), es decir que la propiedad (A.3.2) es condición necesaria para la normalidad. Que (A.3.1) es consecuencia de la normalidad viene de [3, Teorema 9.2].
Supongamos que R es normal, sea $f \in R$ un no divisor de cero y $\mathfrak{p}$ un asociado primo del ideal $\langle f \rangle$. Tenemos que demostrar que $\mathfrak{p}$ es minimal entre los asociados primos de $\langle f \rangle$. Si demostramos que la altura de $\mathfrak{p}$ es 1, por el TIP el ideal $\mathfrak{p}$ es necesariamente minimal.
Por la definición de asociado primo $\mathfrak{p} = \operatorname{Anul} b + \langle f \rangle$ en $R/\langle f \rangle$. Consideremos el anillo local $R_{\mathfrak{p}}$ y su maximal $\mathfrak{p}^e := \mathfrak{p}R_{\mathfrak{p}}$. Definimos $(\mathfrak{p}^e)^{-1} := \{x \in Q(R) : x \cdot \mathfrak{p}^e \subset R_{\mathfrak{p}}\}$. Claramente $R_{\mathfrak{p}} \subset (\mathfrak{p}^e)^{-1}$ y $\frac{b}{f}$ que es un elemento de $Q(R)$ por ser f no divisor de cero, también pertenece a $(\mathfrak{p}^e)^{-1}$. En efecto, dado un elemento de $(\mathfrak{p}^e)^{-1}$, que necesariamente es de la forma $\frac{t_1}{t_2}$, con $t_1 \in \mathfrak{p}$ y $t_2 \notin \mathfrak{p}$, por la definición de b será $t_1 \cdot b = \lambda f$ para cierto $\lambda \in R$. Así $\frac{b}{f} \cdot \frac{t_1}{t_2} = \frac{\lambda}{t_2} \in R_{\mathfrak{p}}$. Por consiguiente

[1] En consecuencia, por el TIP, sus asociados primos tienen altura 1

tenemos $\frac{b}{f} \in (\mathfrak{p}^e)^{-1}$. Por otra parte $(\mathfrak{p}^e)^{-1} \cdot \mathfrak{p}^e$ es un ideal de $R_\mathfrak{p}$ que contiene a b (pues $b = \frac{b}{f} \cdot f$) y como $b \notin \mathfrak{p}$, es por tanto una unidad en $R_\mathfrak{p}$. Concluimos que el ideal $(\mathfrak{p}^e)^{-1} \cdot \mathfrak{p}^e$ es todo el anillo $R_\mathfrak{p}$.
Demostramos ahora que $\mathfrak{p}^e$ es un ideal principal. Sea $t \in \mathfrak{p}^e \setminus (\mathfrak{p}^e)^2$, que existe pues sino por el lema de Nakayama $\mathfrak{p}^e = 0$ y $\mathfrak{p} = 0$. Como $t \in \mathfrak{p}^e$, $t \cdot (\mathfrak{p}^e)^{-1} \subset R_\mathfrak{p}$ y es un ideal de $R_\mathfrak{p}$. No puede ser $t \cdot (\mathfrak{p}^e)^{-1} \subset \mathfrak{p}^e$ pues sino $t \cdot (\mathfrak{p}^e)^{-1} \cdot \mathfrak{p}^e = tR_\mathfrak{p} \subset (\mathfrak{p}^e)^2$, que contradice la elección de t. En conclusión $t \cdot (\mathfrak{p}^e)^{-1} = R_\mathfrak{p}$ y $tR_\mathfrak{p} = \mathfrak{p}^e$.
Con todo ello hemos visto que $\mathfrak{p}^e$ es principal en $R_\mathfrak{p}$; es decir $\mathfrak{p}^e = \langle a \rangle R_\mathfrak{p}$ para cierto a que podemos suponer en R. Además por las propiedades de la localización $\mathfrak{p}^e$ es asociado primo de $\langle f \rangle R_\mathfrak{p}$. Si a fuera divisor de cero en $R_\mathfrak{p}$, f (es decir $\frac{f}{1}$) que es múltiplo suyo sería divisor de cero en $R_\mathfrak{p}$. Entonces f también divisor de cero en R. Por consiguiente a no es divisor de cero en $R_\mathfrak{p}$ y como $\mathfrak{p}^e$ es el único asociado primo de si mismo es decir de $\langle a \rangle R_\mathfrak{p}$, por el TIP tiene altura 1. Como la altura de $\mathfrak{p}$ en R coincide con la de $\mathfrak{p}^e$ en $R_\mathfrak{p}$, hemos terminado la prueba. □

La manera en que utilizamos este resultado es para establecer el siguiente corolario.

(**A.4) COROLARIO:** Sea R un DI noetheriano íntegramente cerrado. Entonces $R = \cap_{\mathtt{ht}(\mathfrak{p})=1} R_\mathfrak{p}$.

Demostración. Sea $Q(R)$ el cuerpo de fracciones de R y sea $x := \frac{x_1}{x_2} \in Q(R)$, $x_i \in R$ tal que $x_1 \notin x_2 R$. Veamos que para algún primo $\mathfrak{p}$ de altura 1, $x \notin R_\mathfrak{p}$.
Claramente x_2 no es unidad en R ni cero, así por la proposición anterior los asociados primos de $x_2 R$ son todos minimales y tienen todos altura 1. Sea $x_2 R = \cap_{i=1}^r \mathfrak{q}_i$ su descomposición primaria y $\mathfrak{p}_i$ el primo asociado al primario $\mathfrak{q}_i$. Como $x_1 \notin x_2 R$, digamos que $x_1 \notin \mathfrak{q}_1$. Entonces $x_1 \notin x_2 R_{\mathfrak{p}_1} = \mathfrak{q}_1 R_{\mathfrak{p}_1}$ □

El siguiente resultado se denomina *Teorema de la Dimensión para anillos locales noetherianos*:

(**A.5) TEOREMA [3, Teorema 11.14]:** Sea $(A, \mathfrak{m}, k)$ un anillo local noetheriano, coinciden:

1. La dimensión de Krull de A.
2. El menor número de generadores de un ideal $\mathfrak{m}$-primario.

Observar que

$$\begin{pmatrix}\text{Menor número de generadores de un}\\ \text{ideal } \mathfrak{m}-\text{primario}\end{pmatrix} \overset{A}{\leq} \begin{pmatrix}\text{menor número de gene-}\\ \text{radores de } \mathfrak{m}\end{pmatrix} \overset{B}{=} \left(\dim_{k=A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2\right)$$

A. Porque $\mathfrak{m}$ es $\mathfrak{m}-$primario y el menor número de generadores lo puede dar otro $\mathfrak{m}-$primaro que no necesariamente es $\mathfrak{m}$.

B. Es una aplicación del lema de Nakayama, tal y como lo establece la siguiente proposición.

(**A.6) PROPOSICIÓN:** Si M es un $A-$módulo finitamente generado y $\xi_1, \ldots, \xi_\ell \in M$, tales que $\overline{\xi}_1, \ldots, \overline{\xi}_r$, $(r \leq \ell)$ en $M/\mathfrak{m}M$ son generadores del $A/\mathfrak{m}-$espacio vectorial, entonces $\xi_1, \ldots, \xi_\ell$ son generadores de M.

Demostración. Sea $N = \langle \xi_1, \ldots, \xi_r \rangle A$ submódulo de M $(N \subseteq M)$, probaremos que $N + \mathfrak{m}M = M$.

$\subseteq$ Es claro.

$\supseteq$ Sea $x \in M$, $x + \mathfrak{m}M$ está generado en $M/\mathfrak{m}$ por $\overline{\xi}_1, \ldots, \overline{\xi}_r$, por lo que existen $\lambda_1, \ldots, \lambda_r \in A$: $x + \mathfrak{m}M = \sum_{i=1}^r \lambda_i \overline{\xi}_i$, entonces $x - \sum_{i=1}^r \lambda_i \overline{\xi}_i \in \mathfrak{m}M$.

Por lo tanto, $N + \mathfrak{m}M = M \Rightarrow N = M$. □

(**A.7) DEFINICIÓN:** Un anillo local noetheriano $(A, \mathfrak{m}, k := A/\mathfrak{m})$ se dice **local regular** si su ideal maximal $\mathfrak{m}$ está generado por un número de elementos igual a la dimensión de Krull de A, es decir, si

$$\begin{aligned} d := \dim_{\text{krull}} A &= \text{menor número de generadores de } \mathfrak{m} \\ &= \dim_k \mathfrak{m}/\mathfrak{m}^2 \end{aligned}$$

Un sistema de generadores de $\mathfrak{m}$ formado por d elementos (i.e. minimal) se denomina **sistema regular de parámetros**.

(**A.8) TEOREMA [3, Teorema 11.22]:** Dado un anillo local noetheriano $(A, \mathfrak{m}, k)$ son equivalentes:

1. A es regular.
2. Su graduado $\mathfrak{m}-$ádico es un anillo de polinomios: $\mathtt{GR}_{\mathfrak{m}}(A) \cong k[X_1, \ldots, X_r]$.
3. Su completado $\mathfrak{m}-$ádico es un anillo de series formales: $\hat{A} \cong k[[X_1, \ldots, X_r]]$.

En ambos casos el r coincide con la dimensión de Krull de A o equivalentemente el menor número de generadores de $\mathfrak{m}$.

(**A.9) EJEMPLO:** Si A es dominio local noetheriano y normal, y $\mathfrak{p}$ es un ideal primo de altura 1, $A_{\mathfrak{p}}$ como hemos visto es un AVD. La valoración de un elemento es la $\mathfrak{p}^e-$ádica es decir, viene dada por la mayor potencia del maximal a la cual pertenece el elemento. Por otra parte su completado $\hat{A}_{\mathfrak{p}}$ es por (A.8) isomorfo a $k(\mathfrak{p})[[T]]$, donde $k(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}^e$. Claramente la composición $A_{\mathfrak{p}} \hookrightarrow \hat{A}_{\mathfrak{p}} = k(\mathfrak{p})[[T]]$ permite ver el anillo $A_{\mathfrak{p}}$ como sub anillo del anillo de series y la valoración $\mathfrak{p}^e-$ádica como tomar el orden en la T de una serie.

Otro resultado que usamos en la demostración de 1.16 es la versión formal del Teorema de la Función Implícita (TFI). Con la misma notación e hipótesis del teorema 1.16 tenemos el siguiente resultado:

(**A.10) TEOREMA TFI:** Existen únicas series $h_1, \ldots, h_p \in K[[\boldsymbol{X}]]_{alg}$ tales que

- $h_j(\mathbf{0}) = 0$, para $j = 1, \ldots, p$, y
- $H_i(\boldsymbol{X}, h_1, \ldots, h_p) = 0$, para $i = 1, \ldots, p$.

El teorema anterior afirma que el ideal maximal $\mathfrak{m}_A$ de A está generado por $x_i := X_i \mod \langle H_1, \ldots, H_p \rangle$, $i = 1, \ldots, n$, es decir,

$$\mathfrak{m}_A = \langle x_1, \ldots, x_n \rangle.$$

Así tenemos el siguiente corolario.

(**A.11) COROLARIO:** El anillo A del teorema (1.16) es local regular.

También damos la siguiente demostración más "geométrica" de este resultado, y el desarrollo en serie se puede construir siguiendo la demostración del teorema A.10.

Demostración. Consideramos la aplicación lineal

$$\begin{aligned} \nabla_{\boldsymbol{X}} : (K[\boldsymbol{Y}])[\boldsymbol{X}] &\to K^n \\ F &\mapsto \nabla_{\boldsymbol{X}}(F) := \left(\frac{\partial F}{\partial X_1}(\mathbf{0}, \mathbf{0}), \ldots, \frac{\partial F}{\partial X_n}(\mathbf{0}, \mathbf{0})\right) \end{aligned}$$

el gradiente formal en las $\boldsymbol{X}$'s i.e. tomamos "derivadas parciales formales" rescpecto a $\boldsymbol{X}$'s y las evaluamos en $(\mathbf{0}, \mathbf{0})$.

Observar que $\nabla_{\boldsymbol{X}}(X_i) = (0, \ldots, \underbrace{1}_{i}, \ldots, 0) =: e_i$, se tiene que $\{\nabla_{\boldsymbol{X}}(X_1), \ldots, \nabla_{\boldsymbol{X}}(X_n)\}$ son base de K^n.
Además

$$\frac{\partial}{\partial X_k}(X_i X_j) = \begin{cases} 0 & k \neq i, k \neq j, \\ X_i & k = i, \\ X_j & k = j, \\ 2X_k & k = i = j, \end{cases}$$

en los cuatros casos tenemos que $\frac{\partial}{\partial X_k}(X_i X_j)$ es idénticamente cero al evaluar en $(\mathbf{0})$. Si $I := \langle \boldsymbol{X}, \boldsymbol{Y} \rangle$

$$\varphi : K[\boldsymbol{X}, \boldsymbol{Y}] \to K^n$$

$$F := \sum_{i=1}^{n} a_i X_i + \sum_{j=1}^{p} b_j Y_j + P(\boldsymbol{X}, \boldsymbol{Y}) \mapsto \varphi(F) := (a_1, \ldots, a_n)$$

donde $P \in \langle \boldsymbol{X}^2, \boldsymbol{Y}^2 \rangle$.
Por la hipótesis $|\frac{\partial H_i}{\partial Y_j}| \in K^\times$ tenemos que $\ker \varphi = I^2$. Así la aplicación $I/I^2 \xrightarrow{\varphi} K^n$ es isomorfismo entonces

$$\dim_{\text{krull}} A = \dim_k I/I^2 = n.$$

Por lo tanto A es local regular y $x_1, \ldots, x_n$ es un sistema regular de parámetros. □

Referencias

[1] Maria Emilia Alonso, Thierry Coquand y Henri Lombardi. "Revisiting Zariski main theorem from a constructive point of view." English. En: *J. Algebra* 406 (2014), págs. 46-68. ISSN: 0021-8693.

[2] Maria Emilia Alonso, Teo Mora y Mario Raimondo. "A computational model for algebraic power series." English. En: *J. Pure Appl. Algebra* 77.1 (1992), págs. 1-38. ISSN: 0022-4049.

[3] M.F. Atiyah e I.G. MacDonald. *Introducción al álgebra conmutativa*. Publicaciones científicas y de tecnología aplicada. Reverté, 1973. ISBN: 9788429150087.

[4] D.A. Cox, J. Little y D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. ISBN: 9783319167213.

[5] T. de Jong y G. Pfister. *Local Analytic Geometry: Basic Theory and Applications*. Advanced Lectures in Mathematics. Vieweg+Teubner Verlag, 2013. ISBN: 9783322901590.

[6] M. Kreuzer y L. Robbiano. *Computational Commutative Algebra 2*. Computational Commutative Algebra. Springer Berlin Heidelberg, 2005. ISBN: 9783540255277.

[7] T. Mora. *Solving Polynomial Equation Systems*. Encyclopedia of Mathematics and its Applications v. 4. Cambridge University Press, 2016. ISBN: 9781107109636.

[8] Teo Mora, Gerhard Pfister y Carlo Traverso. "An introduction to the tangent cone algorithm". En: *Issues in non-linear geometry and robotics, CM Hoffman ed* (1992).

[9] Lorenzo Robbiano. "Term orderings on the polynomial ring". En: *EUROCAL'85*. Springer. 1985, págs. 513-517.

[10] O. Zariski y P. Samuel. *Commutative Algebra II*. Commutative Algebra. Springer, 1976. ISBN: 9780387901718.