Una Prueba Autocontenida del Nullstellenstaz Efectivo de Z. Jelonek

(A self-contained proof of Jelonek's Effective Nullstellensatz)

Pablo Echegoyen Ruiz

Trabajo de Fin de Grado

para acceder al

Grado en Matemáticas

Facultad de Ciencias

Universidad de Cantabria

Director: Luis Miguel Pardo Vasallo

Octubre - 2020

A mi familia,
a los compañeros de la facultad de ciencias,
y a los profesores, en especial a Luis Miguel Pardo.

Abstract. Hilbert's Nullstellensatz (Zero-locus-theorem) is one of the most important theorems of mathematics history, and it not only establishes a fundamental relationship between geometry and algebra but also is involved in algorithmic problems too. The usual proofs of the Nullstellensatz are not constructive, and they do not give any way to compute the multivariable polynomials related to the Nullstellensatz. To solve this problem, it suffices to provide an upper bound of the degrees of the polynomials in the Bézout's identity, and the problem is reduced to a finite system of linear equations. The results that provide upper bounds of the degrees are called Effective Nullstellensätze.

The objective of this memory is to give a self-contained proof of the best bound up to date, achieved by Z. Jelonek in 2005 (cf. [**Je, 2005**]). This implies the undersanding of a paper publishied in one of the top ten mathematics magazines, Inventions mathematicae. Futhermore, this memory has not only completed some undetailed results of Jelonek's paper but also gives an original proof.

In order to do that, we first generalize Perron's theorem and we prove the result for the overdeterminated case (Chapter 1). Then, we prove Jelonek's Elimination Theorem in an original way and we finally obtained the Effective Nullstellensatz (Chapter 2).

Key Words. Hilbert's Nullstellensatz, algebraic geometry, conmutative algebra, Bézout's Identity.

Resumen. El Nullstellensatz de Hilbert (Teorema de los Ceros) es uno de los theoremas más importantes en la historia de las matemáticas, no solo porque establece una relación fundamental entre geometría y álgebra, sino porque también está involucrado en problemas algorítmicos. Normalmente las pruebas del Nullstellensatz no son constructivas, y no proporcionan un método para calcular los polinomios multivariables del Nullstellensatz. Para solucionarlo, es suficiente con dar una cota superior a los grados de los polinomios en la Identidad de Bézout, y el problema se reduce a un sistema de ecuaciones lineales. Los resultados que proporcionan cotas superiores son los llamados Nullstellensätze Efectivos.

El objetivo de esta memoria es dar una prueba autocontenida de la mejor cota hasta la fecha, lograda por Z. Jelonek en 2005 (cf. [**Je, 2005**]). Esto implica comprender un paper publicado en una de las diez mejores revistas matemáticas del mundo. Además, esta memoria no solo ha completado algunos resultados no detallados en el paper de Jelonek, sino que también proporciona una prueba original.

Para lograrlo, primero generalizamos el teorema de Perron y probamos el resultado para el caso subdeterminado (Capítulo 1). Después, probamos el teorema de Eliminación de Jelonek de forma original, y por último obtenemos el Nullstellensatz Efectivo (Capítulo 2).

Palabras Clave. Nullstellensatz de Hilbert, geometría algebraica, álgebra conmutativa, Identidad de Bézout.

Índice

Introducción y Resumen del Contenido de la Memoria

Índice

Este Trabajo Fin de Grado aporta una demostración rigurosa y pormenorizada del Nullstellensatz efectivo de Z. Jelonek, publicado en 2005 (cf. [**Je, 2005**]). Este resultado, que supone la exposición más refinada del Nullstellensatz Efectivo hasta la fecha, requiere un esfuerzo más que notable en la comprensión de su contenido científico y en su potencial impacto. Por ello, hemos diseñado una "Introducción y Resumen de Resultados" que contemplan los siguientes apartados distinguidos e interrelacionados:

i) En la primera sección haremos un breve resumen del impacto e influencia del Nullstellensatz de Hilbert-Kronecker, conocido también como el "Teorema de los Ceros de Hilbert".
ii) En la segunda sección explicaremos qué son los Nullstellensätze Efectivos, su motivación y un poco de su historia, desde los trabajos de la alumna de Hilbert G. Hermann (cf. [**He, 1996**]) hasta el resultado de Jelonek que se exhibe en esta memoria.
iii) En la tercera sección expondremos un resumen de los principales resultados que se demuestran en esta memoria y de los términos esencialmente utilizados.
iv) En la cuarta sección se comparan las cotas obtenidas por parte de Jelonek con resultados previos.

Aprovecharemos esta presentación de resultados para *fijar algunas de las notaciones y términos básicos que se usarán a lo largo de las restantes páginas.*

El Nullstellensatz de Hilbert-Kronecker en su contexto

Para poder enmarcar con alguna propiedad el Nullstellensatz de Hilbert-Kronecker, necesitamos fijar algunas de las notaciones que se irán usando a lo largo de la memoria.
Así, denotaremos por K un cuerpo cualquiera y por $\mathbb{K}$ su clausura algebraica como cuerpo. Denotaremos, respectivamente, por $K[X_1, \ldots, X_m]$ y por $\mathbb{K}[X_1, \ldots, X_m]$ los anillos de polinomios en m variables con coeficientes en K, o respectivamente, en $\mathbb{K}$. Para cada subconjunto S de un anillo cualquiera R denotaremos por (S) el ideal que genera. Igualmente, para cada anillo R denotaremos por $Spec(R)$ y $Spm(R)$ los respectivos *espectro primo* y *espectro maximal* de R. Es decir,

- $Spec(R) = \{\mathfrak{p} \subseteq R : \mathfrak{p}$ *es ideal primo*$\} = \{\mathfrak{p} \subseteq R : \mathfrak{p}$ *es ideal y* $R/\mathfrak{p}$ *es dominio*$\}$.
- $Spm(R) = \{\mathfrak{m} \subseteq R : \mathfrak{m}$ *es ideal maximal*$\} = \{\mathfrak{m} \subseteq R : \mathfrak{m}$ *es ideal y* $R/\mathfrak{m}$ *es cuerpo*$\}$.

Denotaremos por $\mathbb{A}^m(\mathbb{K})$ (o, cuando no haya confusión, simplemente por $\mathbb{A}^m$) al *espacio afín de dimensión* m *sobre* $\mathbb{K}$.
Como $\mathbb{K}$ es un cuerpo de cardinal infinito, podemos identificar los polinomios f en $\mathbb{K}[X_1, \ldots, X_m]$ con las *funciones polinomioales sobre* $\mathbb{A}^m$ que definen. Por ello, si $f \in \mathbb{K}[X_1, \ldots, X_m]$, también denotaremos por f a la aplicación siguiente:

$$\begin{aligned} f : \mathbb{A}^m &\longrightarrow \mathbb{K} \\ x &\longmapsto f(x). \end{aligned}$$

Dado un ideal $\mathfrak{a} \subseteq \mathbb{K}[X_1, \ldots, X_m]$, denotaremos mediante $V_{\mathbb{A}}(\mathfrak{a}) \subseteq \mathbb{A}^m$ el conjunto de los ceros comunes de todos los elementos de $\mathfrak{a}$ en $\mathbb{A}^m$. Es decir,

$$V_{\mathbb{A}}(\mathfrak{a}) := \{x \in \mathbb{A}^m : g(x) = 0, \forall g \in \mathfrak{a}\}.$$

Llamaremos *variedad algebraica afín* a todos los subconjuntos $V \subseteq \mathbb{A}^m$ del espacio afín m-dimensional tal que existe un ideal $\mathfrak{a} \subseteq \mathbb{K}[X_1, \ldots, X_m]$ verificando $V = V_{\mathbb{A}}(\mathfrak{a})$. Nótese que $\mathbb{A}^m = V_{\mathbb{A}}((0))$ y $\emptyset = V_{\mathbb{A}}((1))$ son, respectivamente, variedades algebraicas afines definidas por los ideales (0) y $(1) = \mathbb{K}[X_1, \ldots, X_m]$ del anillo $\mathbb{K}[X_1, \ldots, X_m]$.
Dado un elemento $f \in \mathbb{K}[X_1, \ldots, X_m]$, denotaremos por $V_{\mathbb{A}}(f)$ al conjunto de los ceros en $\mathbb{A}^m$ de f, es decir,

$$V_{\mathbb{A}}(f) := \{x \in \mathbb{A}^m : f(x) = 0\}.$$

Claramente, $V_{\mathbb{A}}(f) = V_{\mathbb{A}}((f))$, donde (f) es el ideal generado por (f), por lo que los conjuntos de la forma $V_{\mathbb{A}}(f)$ son variedades algebraicas. Usualmente, se usa la expresión *hiper-superficie* para las variedades algebraicas de la forma $V_A(f)$. Aunque, hablando con propiedad para excluir $\mathbb{A}^m$ y $\emptyset$, hablaremos de hiper-superficies solamente para los conjuntos $V_{\mathbb{A}}(f)$ cuando $f \in \mathbb{K}[X_1, \ldots, X_m] \setminus \mathbb{K}$. Obviamente, juntando los usos terminológicos, toda variedad algebraica afín es la intersección de una cantidad, posiblemente infinita, de hipersuperfices. Es la obvia relación siguiente:

$$V_{\mathbb{A}}(\mathfrak{a}) = \bigcap_{f \in \mathfrak{a}} V_{\mathbb{A}}(f).$$

Más aún, si $G = \{g_i : i \in I\}$ es un sistema generador de un ideal $\mathfrak{a}$ de $\mathbb{K}[X_1, \ldots, X_m]$ se tiene la obvia relación:

$$V_{\mathbb{A}}(\mathfrak{a}) = \bigcap_{g_i \in G} V_{\mathbb{A}}(g_i).$$

Esto justifica el uso de ideales y no solamente de sistemas de ecuaciones a la hora de definir variedades algebraicas: dadas $S, S' \subseteq \mathbb{K}[X_1, \ldots, X_m]$ dos familias, potencialmente infinitas, de polinomios, si generan el mismo ideal (i.e. si $(S) = (S')$) entonces se tiene:

$$\bigcap_{g \in S} V_{\mathbb{A}}(g) = \bigcap_{f \in S'} V_{\mathbb{A}}(f),$$

dado que ambas intersecciones coinciden con $V_{\mathbb{A}}(\mathfrak{a})$, donde $\mathfrak{a} = (S) = (S')$.
En su trabajo de 1890 ([**Hi, 1890**]), D. Hilbert prueba un resultado, conocido hoy en día como *Basissatz* o Teorema de la Base, al que E. Noether dio un contexto moderno (en [**Noe, 1921**]) con la teoría de anillos que hoy llamamos noetherianos en su honor. Un anillo se dice notheriano si todos sus ideales son finitamente generados. Y el Basissatz establece que todo anillo de polinomios sobre un cuerpo es noetheriano y, en particular, que todo ideal $\mathfrak{a}$ de $\mathbb{K}[X_1, \ldots, X_m]$ es finitamente generado. La noción de anillo noetheriano tiene un impacto mayor a lo largo del tiempo (como lo prueban referencias tan diversas como [**AM, 1969**], [**Ei, 1995**], [**Ha, 1977**], [**Ma, 1980**], [**Pa,20a**] o [**Sha, 1974**] entre muchas otras) que la referencia a anillos de la forma $\mathbb{K}[X_1, \ldots, X_m]$.
En todo caso, y por lo que respecta a esta memoria, como todo ideal $\mathfrak{a}$ de $\mathbb{K}[X_1, \ldots, X_m]$ es finitamente generado, toda variedad algebraica afín es intersección de un número finito de hiper-superficies. Si $\mathfrak{a} = (f_1, \ldots, f_s)$, entonces

$$V_{\mathbb{A}}(\mathfrak{a}) = V_{\mathbb{A}}(f_1) \cap \cdots \cap V_{\mathbb{A}}(f_s).$$

El conjunto de las variedades algebraicas afines en $\mathbb{A}^m(\mathbb{K})$ es estable por uniones finitas e intersecciones cualesquiera, como consecuencia de las siguientes identidades:

i) Dados dos ideales $\mathfrak{a}, \mathfrak{b}$ en un anillo R, se define el *ideal producto* $\mathfrak{a} \cdot \mathfrak{b}$ como el ideal generado por los productos de elementos de $\mathfrak{a}$ por elementos de $\mathfrak{b}$. Es decir,

$$\mathfrak{a} \cdot \mathfrak{b} = (\{f \cdot g : f \in \mathfrak{a}, g \in \mathfrak{b}\}).$$

Dadas $\mathfrak{a}, \mathfrak{b}$ dos ideales en $\mathbb{K}[X_1, \ldots, X_m]$ se tiene:

$$V_{\mathbb{A}}(\mathfrak{a} \cdot \mathfrak{b}) = V_{\mathbb{A}}(\mathfrak{a}) \cup V_{\mathbb{A}}(\mathfrak{b}).$$

ii) Dada una familia cualquiera de ideales $\{\mathfrak{a}_i : i \in I\}$ de un anillo R, el *ideal suma* $\sum_{i\in I} \mathfrak{a}_i \subseteq R$ es el ideal generado por las sumas finitas de elementos cada uno de los cuales está en algún $\mathfrak{a}_i$. Dicho de otro modo,

$$\sum_{i\in I} \mathfrak{a}_i = \left(\bigcup_{i\in I} \mathfrak{a}_i\right).$$

Si $\{\mathfrak{a}_i : i \in I\}$ es una familia de ideales en $\mathbb{K}[X_1, \ldots, X_m]$ se tiene:

$$V_{\mathbb{A}}\left(\sum_{i\in I} \mathfrak{a}_i\right) = \bigcap_{i\in I} V_{\mathbb{A}}(\mathfrak{a}_i).$$

Dado que $\emptyset$ y $\mathbb{A}^m$ son también variedades algebraicas, existirá una única topología en $\mathbb{A}^m(\mathbb{K})$ cuyos cerrados son, precisamente, las variedades algebraicas afines: es la llamada *topología de Zariski* en $\mathbb{A}^m$. Los abiertos en esa topología de Zariski serán los complementarios de las variedades algebraicas. Dado $f \in \mathbb{K}[X_1, \ldots, X_m]$ se define el *abierto Zariski distinguido determinado por* f como el complementario de la hiper-superficie definida por f, es decir,

$$D(f) := \mathbb{A}^m \setminus V_{\mathbb{A}}(f) = \{x \in \mathbb{A}^m : f(x) \neq 0\}.$$

De hecho, el Basissatz nos garantizará que todo abierto en la topología de Zariski es una unión finita de abiertos distinguidos. Más aún, el Basissatz nos garantiza que el espacio $\mathbb{A}^m(\mathbb{K})$ con la topología de Zariski es un *espacio topológico noetheriano*. Un espacio topológico (X, Z) se dice noetheriano si todo abierto es quasi-compacto, es decir, si dado un cubrimiento abierto $\{A_i : i \in I\}$ de un abierto $A \in \tau$, existe un subcubrimiento de A finito $\{A_j : j \in J\} \subseteq \{A_i : i \in I\}$, con $J \subseteq I$ finito. (cf. [**AM, 1969**], por ejemplo). Los espacios topológicos noetherianos poseen varias propiedades singulares que exploraremos más adelante. Por ahora, diremos en ocasiones *cerrado Zariski* en $\mathbb{A}^m$ en lugar de variedad algebraica afín. Hablaremos de conjuntos *localmente cerrados* para referirnos a la intersección de un abierto y un cerrado de la topología de Zariski. Llamaremos *conjunto constructible* a toda unión finita de localmente cerrados. No todo constructible es localmente cerrado como, por ejemplo, el constructible

$$C = \{(x, y) \in \mathbb{C}^2 : xy \neq 0\} \cup \{(x, y) \in \mathbb{C}^2 : x^2 + y^2 - 1 = 0\},$$

que no es localmente cerrado. Dado un subconjunto $S \subseteq \mathbb{A}^m(\mathbb{K})$, llamaremos *clausura Zariski de* S, y lo denotaremos por $\overline{S}^z$, a su clausura para la topología de Zariski, que es, obviamente, una variedad algebraica.

En ocasiones se añade el adjetivo *K-definible* a todos los términos precedentes. Una variedad algebraica $V \subseteq \mathbb{A}^m$ se dice K-definible si existe un ideal $\mathfrak{a}$ de $\mathbb{K}[X_1, \ldots, X_m]$ generado por un subconjunto $S \subseteq K[X_1, \ldots, X_m]$ tal que

$$V = V_{\mathbb{A}}(\mathfrak{a}) = V_{\mathbb{A}}((S)) = \bigcap_{f\in S} V_{\mathbb{A}}(f).$$

La *topología de Zariski K-definible* es la topología cuyos cerrados son las variedades algebraicas K-definibles. Del mismo modo se habla de abiertos K-definibles, localmente cerrados K-definibles o constructibles K-definibles. Nótese que si $\mathfrak{b} \subseteq K[X_1, \ldots, X_m]$ es un ideal y $\mathfrak{b}^e \subseteq \mathbb{K}[X_1, \ldots, X_m]$ es su *extensión* a $\mathbb{K}[X_1, \ldots, X_m]$ (es decir, el ideal que genera en $\mathbb{K}[X_1, \ldots, X_m]$), entonces $V_{\mathbb{A}}(\mathfrak{b}) = V_{\mathbb{A}}(\mathfrak{b}^e)$. Por tanto, las variedades algebraicas K-definibles son las variedades algebraicas afines en la clase:

$$\{V_{\mathbb{A}}(\mathfrak{b}^e) : \mathfrak{b} \subseteq \mathbb{K}[X_1, \ldots, X_m] \text{ es ideal}\},$$

y la topología de Zariski K-definible en $\mathbb{A}^m$ es menos fina que la topología de Zariski de $\mathbb{A}^m$(que podría llamarse $\mathbb{K}$-definible, aunque usualmente se omite el adjetivo).

Una terminología clásica de la geometría algebraica del siglo XIX es el uso de la expresión "genérico" con la topología de Zariski.

Comencemos hablando de la *topología de Zariski en V*, para un subconjunto $V \subseteq \mathbb{A}^m$, como la topología inducida en V por la topología de Zariski en $\mathbb{A}^m$. Así, usaremos expresiones como *cerrado Zariski en V*, *abierto Zariski en V*, etc. para referirnos a cerrados, abiertos, etc. en la topología de V inducida por la de $\mathbb{A}^m$.

Una propiedad $\Phi(x)$, definida para elementos $x \in V \subseteq \mathbb{A}^m$ se dice que se *satisface genéricamente en V* si existe un abierto Zariski en V: $\mathcal{U} \subseteq V$ tal que $\Phi(x)$ se satisface para cada punto

$x \in V$. En cierto sentido, la idea de que una propiedad se satisface genéricamente en $\mathbb{A}^m$ es una formalización más clásica de la expresión " almost everywhere" (a.e.) o "salvo un conjunto de medida nula ", de uso habitual en Teoría de la Medida. Este concepto no sólo tendrá interés en $\mathbb{A}^m$, noción que recordaremos más adelante en esta misma Sección.
Hasta este momento nos hemos esforzado en introducir una sencilla terminología que responde a dos clases de objetos:

i) *Objetos Semánticos:* Son los objetos geométricos. Los subconjuntos de $\mathbb{A}^m(\mathbb{K})$ que se encuentran en el entorno de la topología de Zariski: cerrados, abiertos, localmente cerrados, constructibles, etc.
ii) *Objetos Sintácticos:* El objeto sintáctico por excelencia es el polinomio $f \in \mathbb{K}[X_1, \ldots, X_m]$. Consecuentemente son objetos sintácticos los objetos asociados: el anillo $\mathbb{K}[X_1, \ldots, X_m]$, sus ideales, etc.

Cada una de esas clases de objetos viene con su correspondiente conjunto de operaciones.
El propósito subyacente esencial del Nullstellensatz consiste en resolver el problema siguiente:

PROBLEMA 1 (**Problema Motivacional del Nullstellensatz**). *¿Cuál es la exacta naturaleza de la interacción entre los objetos semánticos propios de la topología de Zariski y los objetos sintácticos asociados a* $\mathbb{K}[X_1, \ldots, X_m]$*?*

La respuesta a esta interacción entre un universo semántico y otro sintáctico se obtiene en [**Hi, 1893**] y está implícita en [**Kr, 1882**]. Si bien D. Hilbert, como era su costumbre, halla una prueba axiomático-deductiva, L. Kronecker trabaja de manera más constructiva al presentar las variedades algebraicas equi-dimensionales mediante isomorfismos birracionales con hiper-superficies en espacios de dimensión apropiada. En todo caso, ambos conducen al siguiente enunciado:

TEOREMA 0.0.1 (**Nullstellensatz**). *Con las notaciones precedentes, dado* $\mathfrak{a} \subseteq \mathbb{K}[X_1, \ldots, X_m]$ *un ideal, se verifica:*

$$V_{\mathbb{A}}(\mathfrak{a}) = \emptyset \text{ si y solamente si } 1 \in \mathfrak{a}.$$

Nótese que se trata de una generalización no trivial del hecho siguiente: Dado un polinomio univariado $f \in \mathbb{K}[X]$, entonces

$$\exists z \in \mathbb{K}, f(z) = 0 \text{ si y solamente si } f \notin \mathbb{K} \setminus \{0\},$$

que no es otra cosa que la naturaleza misma de los cuerpos algebraicamente cerrados.
Obviamente, el Nullstellensatz no sería cierto si $\mathbb{K}$ no fuera algebraicamente cerrado. Así el ideal $\mathfrak{a} = (X^2 + Y^2 + 1) \subseteq \mathbb{R}[X, Y]$ es un ideal propio, $1 \notin \mathfrak{a}$, y, sin embargo, sus ceros en $\mathbb{A}^2(\mathbb{R})$ (espacio afín sobre $\mathbb{R}$) son el conjunto vacío, i.e.

$$V_{\mathbb{A}}(\mathfrak{a}) \cap \mathbb{A}^2(\mathbb{R}) = \emptyset \text{ y } 1 \notin \mathfrak{a}.$$

Una sencilla demostración con argumentos muy elementales del anterior Nullstellensatz puede seguirse en [**Pa,20a**] donde se completa y precisan los sencillos argumentos de [**Ar, 2006**].
Como consecuencia del Basissatz, una versión equivalente al anterior enunciado es la siguiente:

TEOREMA 0.0.2 (**Nullstellensatz: Identidad de Bézout**). *Con las notaciones precedentes, sean* $f_1, \ldots, f_s \in \mathbb{K}[X_1, \ldots, X_m]$. *Son equivalentes:*

i) $V_{\mathbb{A}}(f_1, \ldots, f_s) = \cap_{i=1}^{s} V_{\mathbb{A}}(f_i) = \emptyset$.
ii) $\neg(\exists x \in \mathbb{A}^m(\mathbb{K}), f_1(x) = f_2(x) = \cdots = f_s(x) = 0)$.
iii) Existen $g_1, \ldots, g_s \in \mathbb{K}[X_1, \ldots, X_m]$ *tales que*

$$1 = g_1 f_1 + g_2 f_2 + \cdots + g_s f_s. \tag{0.0.1}$$

Las identidades de la forma 0.0.1 son las llamadas *Identidad de Bézout*. Obviamente, generalizan al caso multi-variado la clásica Identidad de Bézout univariada que se estudia en cualquier curso elemental de cualquier grado en Matemáticas. El estudio de estas identidades de Bézout *será el objeto de estudio de los Nullstellensätze Efectivos* al que pertenece esta memoria.
La presentación del Nullstellensatz bajo las dos formas precedentes no parece responder tan claramente a la cuestión de emplear la identificación entre objetos sintácticos y semánticos reclamada en el Problema Motivacional precedente. Por eso, se suelen interpretar formulaciones, equivalentes a cualquiera de las dos anteriores, que permitan ver más de cerca cómo se produce esa identificación.

Una de esas formulaciones es el Nullstellensatz débil que pasaremos a describir a continuación (y que es totalmente equivalente a las anteriores).
Para comenzar, consideramos $z = (z_1, \ldots, z_m) \in \mathbb{A}^m(\mathbb{K})$ y tendremos un morfismo suprayectivo de anillos (de hecho, morfismo de $\mathbb{K}$-álgebras) dado por la *evaluación en el punto* z:

$$\begin{aligned} ev_z : \mathbb{K}[X_1, \ldots, X_m] &\longrightarrow \mathbb{K}^1 \\ f &\longmapsto f(z). \end{aligned}$$

El núcleo de ese morfismo de anillos $\ker(ev_z)$ será un ideal de $\mathbb{K}[X_1, \ldots, X_m]$ que denotaremos mediante:

$$\mathfrak{m}_z := \ker(ev_z) = \{f \in \mathbb{K}[X_1, \ldots, X_m] : f(z) = 0\},$$

Claramente, $\mathfrak{m}_z \in Spm(\mathbb{K}[X_1, \ldots, X_m])$, es decir, es un ideal maximal en ese anillo porque el anillo residual es un cuerpo:

$$\mathbb{K}[X_1, \ldots, X_m] \Big/ \mathfrak{m}_z \cong \mathbb{K}.$$

De hecho, se puede probar de manera sencilla que $\mathfrak{m}_z$ es el ideal generado por los polinomios $\{X_1 - z_1, \ldots, X_m - Z_m\}$:

$$\mathfrak{m}_z = (X_1 - z_1, \ldots, X_m - z_m).$$

La forma débil del Nullstellensatz (que no es más débil sino equivalente a las anteriores formulaciones) es la siguiente:

Teorema 0.0.3 (**Nullstellensatz débil**). *Con las notaciones precedentes, el conjunto de los ideales maximales de* $\mathbb{K}[X_1, \ldots, X_m]$ *es el siguiente*

$$\{\mathfrak{m}_z \in \mathbb{A}^m(\mathbb{K})\} = Spm(\mathbb{K}[X_1, \ldots, X_m]).$$

Este resultado propone una primera identifiación entre objetos semánticos (puntos) y objetos sintácticos (ideales maximales) que se plasma mediante la siguiente biyección:

$$\begin{aligned} \mathbb{A}^m &\longrightarrow Spm(\mathbb{K}[X_1, \ldots, X_m]) \\ z &\longmapsto \mathfrak{m}_z. \end{aligned}$$

De otro lado, y pese a su obvia dificultad, el lector podrá fácilmente intuir que esta versión del Nullstellensatz es una generalización al caso multi-variado del clásico Teorema del Resto del caso univariado (asignado erróneamente a Ruffini en buena parte de la matemática española de secundaria y bachillerato).
Si bien el Nullstellensatz generaliza al Teorema del Resto, en su forma débil ha sido generalizado a través del clásico *Teorema de Banach-Stone-Čech-Gelfand-Kolmogorov*, en ocasiones denominado simplemente Teorema de Stone-Čech (cf. [**GJ, 1976**] o [**GJW, 2002**], por ejemplo).
Sea X un espacio topológico y denotemos por $\mathscr{C}(X)$ al anillo de funciones continuas a valores reales definidas en X.

Teorema 0.0.4 (**Banach-Stone-Čech-Gelfand-Kolmogorov**). *Con las notaciones precedentes,* X *es un espacio topológico compacto si y solamente si la siguiente es una biyección*

$$\begin{aligned} X &\longrightarrow Spm(\mathscr{C}(X)) \\ x &\longmapsto \mathfrak{m}_x = \{f \in \mathscr{C}(x) : f(x) = 0\}. \end{aligned}$$

En particular, dos espacios topológicos compactos X *e* Y *son homeomorfos si y solamente si los anillos* $\mathscr{C}(X)$ *y* $\mathscr{C}(Y)$ *son isomorfos como* $\mathbb{R}$*-álgebras.*

Muchas otras variaciones de los Nullstellensätze anteriores en muy diversos contextos hacen evidente el impacto que tales resultados han tenido allí donde se han conocido. Así hay Nullstellensatz para funciones analíticas complejas, Nullstellensätze reales para polinomios, funciones de Nash o funciones analíticas reales, Nullstellensatz aritméticos, relacionados con la altura en Geometría Diofántica, etc.
Pero es en Geometría Algebraica donde los Nullstellensätze anteriores han tenido un mayor impacto, a través de la obra de la escuela francesa de A. Grothendieck y sus seguidores. Una forma de entender ese impacto pasa por profundizar la respuesta al Problema Motivacional original.

[1] Obsérvese la fuerte relación de ev_z con el núcleo K_z en la teoría de Espacios de Hilbert con Núcleo Reproductor.

Lo haremos estableciendo un *Diccionario Álgebra-Geometría* a través del sencillo truco de G. Y. Rainich, quien firmaba su trabajo más popular como J. L. Rabinowitsch y que quedó en la historia de la matemática como el *truco de Rabinowitsch*.
Dado un subconjunto $S \subseteq \mathbb{A}^m(\mathbb{K})$, llamaremos ideal asociado a S al ideal de las funciones polinomiales que se anulan idénticamente en S. Notacionalmente,

$$I(S) := \{f \in \mathbb{K}[X_1, \ldots, X_m] : f|_S \equiv 0\}.$$

Es claro que $I(S)$ es un ideal en $\mathbb{K}[X_1, \ldots, X_m]$ y que si $S = \{z\}$ es un sólo punto de $\mathbb{A}^m(\mathbb{K})$, entonces $I(\{z\}) = \mathfrak{m}_z$, donde $\mathfrak{m}_z$ es el ideal maximal descrito justo antes del Nullstellensatz en forma débil. Una primera propiedad, sencilla de establecer, es la siguiente:

$$V_{\mathbb{A}}(I(S)) = \overline{S}^z, \tag{0.0.2}$$

donde $\overline{S}^z$ es la clausura de S en la topología de Zariski de $\mathbb{A}^m(\mathbb{K})$. Más aún, retomemos una clásica propiedad de los espacios topológicos noetherianos. Un subconjunto cerrado $V \subseteq \mathbb{A}^m(\mathbb{K})$ se dice *irreducible* si no admite una descomposición de la forma siguiente:

$$V = W_1 \cup W_2, \emptyset \subsetneq W_i \subsetneq V, i = 1, 2, \tag{0.0.3}$$

donde W_1 y W_2 son cerrados para la topología de Zariski de $\mathbb{A}^m(\mathbb{K})$. Un cerrado se dice *reducible* si admite una descomposición como 0.0.3 con W_1 y W_2 cerrados. Los irreducibles poseen muy buenas cualidades cuando se interpretan en un espacio topológico noetheriano.
Si $V \subseteq \mathbb{A}^m$ es una variedad algebraica irreducible y $U \subseteq V$ es un abierto no vacío en la topología de Zariski de V, entonces U es denso en V para la topología de Zariski, i.e.

$$\overline{U}^z = V.$$

Esta propiedad se sigue inmediatamente de la definición. Dado que U es abierto en V, $V \setminus U \subseteq V$ es un cerrado Zariski de $\mathbb{A}^m$ y tenemos la igualdad

$$V = \overline{U}^z \cup (V \setminus U)$$

Como V es irreducible, o bien $V \setminus U = V$, con lo que $U = \emptyset$ (lo cual no es posible si $U \neq \emptyset$) o bien $\overline{U}^z = V$, con lo que tenemos 0.0.1.
Los irreducibles (las variedades algebraicas irreducibles) son los átomos naturales de la topología de Zariski por ser un espacio topológico noetheriano: en todo espacio topológico noetheriano, todo cerrado admite una única descomposición minimal como unión finita de cerrados irreducibles. A los cerrados irreducibles que aparecen en tal descomposición se les denomina *componentes irreducibles*. El argumento que garantiza la existencia de componentes irreducibles es el clásico argumento de Noether que se reencuentra en la existencia de descomposición primaria de ideales (también conocido como Teorema de Lasker-Noether).
Otro sencillo resultado de fácil prueba es el siguiente:

PROPOSICIÓN 0.0.5. *Una variedad algebraica $V \subseteq \mathbb{A}^m$ es irreducible si y solamente si $I(V)$ es un ideal primo en $\mathbb{K}[X_1, \ldots, X_m]$.*

Esta última propiedad junto con la identidad 0.0.3 nos lleva a pensar que debe haber una mayor identificación entre los elementos geométricos y los ideales, que relaciona irreducibles con primos y que responde a las pautas del Nullstellensatz. Esto es lo que se logra a través del Truco de Rabinowitsch.
En nuestra ayuda viene la noción de *radical de un ideal*. Dado un ideal $\mathfrak{a}$ de un anillo R definiremos su radical como el conjunto de todos los elementos $f \in R$ tales que sus clases residuales $f + \mathfrak{a}$ son nilpotentes en $R/\mathfrak{a}$. Esto es,

$$\sqrt{\mathfrak{a}} = \{f \in R : \exists n \in \mathbb{N}, f^n \in \mathfrak{a}\}.$$

El radical de un ideal es también un ideal y coincide con la intersección de todos los ideales primos que le contienen. Es decir, si $\mathfrak{a} \subseteq R$ es un ideal,

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{p} \subseteq R : \mathfrak{p} \in Spec(R), \mathfrak{p} \supseteq \mathfrak{a}\}.$$

Un ideal $\mathfrak{a}$ se dice *radical* si coincide con su radical (i.e. si $\mathfrak{a} = \sqrt{\mathfrak{a}}$).

- Los ideales primos y maximales son radicales.
- Si $S \subseteq \mathbb{A}^m$ es un subconjunto cualquiera $I(S)$ es un ideal radical en $\mathbb{K}[X_1, \ldots, X_m]$.

- Si $V = V_1 \cup \cdots \cup V_s$ es la descomposición de V en componentes irreducibles, entonces $I(V) = I(V_1) \cap \cdots \cap I(V_s)$. En particular, $I(V)$ es una intersección de ideales primos: los asociados a sus componentes irreducibles.
- Es claro que $V_{\mathbb{A}}(\mathfrak{a}) = V_{\mathbb{A}}(\sqrt{\mathfrak{a}})$ para cualquier ideal $\mathfrak{a}$ de $\mathbb{K}[X_1, \ldots, X_m]$.

En general, en anillos noetherianos cualesquiera, el radical de un ideal es siempre una intersección finita de ideales primos como consecuencia del Teorema de Lasker-Noether. La clave de nuestras reflexiones es el siguiente resultado debido a G. Rainich:

TEOREMA 0.0.6 (**Nullstellnsatz: Truco de Rabinowitsch)**. *Dado un ideal* $\mathfrak{a} \subseteq \mathbb{K}[X_1, \ldots, X_m]$, *entonces*

$$I(V_{\mathbb{A}}(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

Poniendo juntos los resultados precedentes, podemos establecer la verdadera formulación clásica del Nullstellensatz de Hilbert-Kronecker en la forma siguiente. Definamos los conjuntos siguientes:

i) $Z(\mathbb{A}^m(\mathbb{K}))$ la clase formada por los cerrados en $\mathbb{A}^m(\mathbb{K})$ para la topología de Zariski.
ii) $Rad(\mathbb{K}[X_1, \ldots, X_m])$ la clase formada por los ideales radicales del anillo $\mathbb{K}[X_1, \ldots, X_m]$.

TEOREMA 0.0.7 (**Nullstellensatz: Diccionario Conjuntista)**. *Con las notaciones precedentes, la siguiente aplicación es una biyección:*

$$\begin{aligned} I : Z(\mathbb{A}^m(\mathbb{K})) &\longrightarrow Rad(\mathbb{K}[X_1, \ldots, X_m]) \\ V &\longmapsto I(V) \end{aligned}$$

La aplicación inversa I^{-1} *es precisamente la aplicación* $V_{\mathbb{A}}$ *siguiente:*

$$\begin{aligned} V_{\mathbb{A}} : Rad(\mathbb{K}[X_1, \ldots, X_m]) &\longrightarrow Z(\mathbb{A}^m(\mathbb{K})) \\ \mathfrak{a} &\longmapsto V_{\mathbb{A}}(\mathfrak{a}). \end{aligned}$$

Además:

i) La biyección I identifica los ideales primos en $Spec(\mathbb{K}[X_1, \ldots, X_m])$ *con las variedades algebraicas irreducibles.*
ii) La biyección I identifica los ideales maximales en $Spm(\mathbb{K}[X_1, \ldots, X_m])$ *con puntos de* $\mathbb{A}^m(\mathbb{K})$.

Además de esta completa formulación como Diccionario Algebro-Geométrico, podemos usar el Nullstellensatz para establecer una equivalencia natural entre dos categorías, lo que nos servirá para hablar de morfismos entre variedades.
Dada $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica, una *función polinomial* sobre V (también llamado función regular) es una función $\Phi : V \longrightarrow \mathbb{K}$ tal que existe un polinomio $f \in \mathbb{K}[X_1, \ldots, X_m]$ tal que

$$\Phi(x) = f(x), \forall x \in V.$$

Una clásica observación nos muestra que el conjunto $\mathbb{K}[V]$ de *funciones polinomiales* sobre una variedad algebriaca V es una $\mathbb{K}$-álgebra y se puede identificar con el cociente:

$$\mathbb{K}[V] = \mathbb{K}[X_1, \ldots, X_m] \Big/ I(V).$$

Supongamos $V \subseteq \mathbb{A}^m$ una variedad algebraica irreducible. Una *función racional* sobre V es un par (f, g), donde $f, g \in \mathbb{K}[V]$ y g no es idénticamente cero sobre V. El par (f, g) define una función parcial

$$\begin{aligned} \frac{f}{g} : D(g) \subseteq V &\longrightarrow \mathbb{K} \\ x &\longmapsto \frac{f(x)}{g(x)}, \end{aligned}$$

donde $D(g) = \{x \in V : g(x) \neq 0\}$ es el abierto distinguido en V definido por g. De manera natural, podemos definir una relación de equivalencia entre dos cualesquiera de esos pares del modo siguiente: dados $(f, g), (p, q)$ dos de tales pares, diremos que son equivalentes si existe un abierto Zariski U en V tal que

- $U \subseteq D(g) \cap D(q)$.
- $\forall x \in U, \frac{f(x)}{g(x)} = \frac{p(x)}{q(x)}$.

Como los abiertos Zariski U en V irreducible son densos Zariski en V, dos de tales funciones parciales son equivalentes si y solamente si

$$q(x)f(x) - p(x)g(x) = 0 \ \forall x \in V. \tag{0.0.4}$$

De una parte, se llama *función racional en* V a la clase de equivalencia de uno de los pares (f, g) antes descrito. Además 0.0.4 nos indica que dos funciones (f, g) y (q, p) son equivalentes si y solamente si se da la siguiente igualdad en $\mathbb{K}[V]$:

$$qg - pg = 0$$

Como $\mathbb{K}[V]$ es un dominio de integridad (porque $I(V)$ es un ideal primo) las funciones racionales, como clases de equivalencia, están identificados con los elementos del cuerpo de fracciones $\mathbb{K}(V) := qf(\mathbb{K}[V])$ de $\mathbb{K}[V]$ que pasará a denominarse el *cuerpo de funciones racionales sobre* V, noción que utilizaremos a lo largo del texto. Además de las funciones regulares y las funciones racionales, hay una manera natural de interrelacionar dos variedades algebraicas afines. Sean $V \subseteq \mathbb{A}^m$ y $W \subseteq \mathbb{A}^n$ dos variedades algebraicas afines. Una *aplicación polinomial entre* V *y* W es una aplicación $f : V \longrightarrow W$ tal que existen $f_1, \ldots, f_n \in \mathbb{K}[V]$ funciones polinomiales tales que

$$f(x) = (f_1(x), \ldots, f_n(x)) \ \forall x \in V.$$

Las aplicaciones polinomiales inducen de manera natural un morfismo de $\mathbb{K}$-álgebras del modo siguiente: Dada $f : V \longrightarrow W$ sea $f^* : \mathbb{K}[W] \longrightarrow \mathbb{K}[V]$ dada mediante

$$\begin{aligned} f^* : \mathbb{K}[W] &\longrightarrow \mathbb{K}[V] \\ h &\longmapsto h \circ f. \end{aligned}$$

Una aplicación polinomial $f : V \longrightarrow W$ se dice *dominante* si la imagen $f(V)$ es denso en W la topología de Zariski de W, es decir, si

$$\overline{f(V)}^z = W.$$

Nótese que $f : V \longrightarrow W$ es dominante si y solamente si f^* es un monomorfismo de $\mathbb{K}$- álgebras. En particular, si $V \subseteq \mathbb{A}^m$ es una variedad algebraica irreducible, $f : V \longrightarrow \mathbb{A}^n$ una aplicación polinomial y $W = \overline{f(V)}^z$ es la clausura Zariski de la imagen, entonces podemos restringir el rango de f y verla como $f : V \longrightarrow W$ que será dominante. Luego $f^* : \mathbb{K}[W] \longrightarrow \mathbb{K}[V]$ será un monomorfismo. como $\mathbb{K}[V]$ es un domino de integridad, también lo será $f^*(\mathbb{K}[W])$ y $\mathbb{K}[W]$. Habremos probado así que si $V \subseteq \mathbb{A}^m$ es irreducible y $f : V \longrightarrow \mathbb{A}^n$ es una aplicación polinomial, entonces $\overline{f(V)}^z$ es una variedad algebraica irreducible.
De otro lado, consideremos un *morfismo de* $\mathbb{K}$*-álgebras* $\Phi : \mathbb{K}[W] \longrightarrow \mathbb{K}[V]$. Es decir, un morfismo de anillos tal que $\Phi(\lambda) = \lambda$, $\forall \lambda \in \mathbb{K}$. Supongamos

$$\mathbb{K}[W] = {}^{\mathbb{K}[Y_1, \ldots, Y_n]}\Big/_{I(W)},$$

$$\mathbb{K}[V] := {}^{\mathbb{K}[X_1, \ldots, X_m]}\Big/_{I(V)}.$$

Consideremos los elementos $\{Y_1 + I(W), \ldots, Y_n + I(W)\}$. Y definamos las funciones polinomiales

$$f_i := \Phi(Y_i + I(W)), 1 \leq i \leq n.$$

Definamos la aplicación polinomial

$$\begin{aligned} \Psi_* : V &\longrightarrow W \\ x &\longmapsto (f_1(x), \ldots, f_n(x)), \end{aligned}$$

Observamos que si $f : V \longrightarrow W$ es una aplicación polinomial se tendrá

$$(f^*)_* = f.$$

Y si $\Phi : \mathbb{K}[W] \longrightarrow \mathbb{K}[V]$ es un morfismo de $\mathbb{K}$-álgebras se tiene:

$$(\Phi^*)_* = \Phi.$$

Esta idea se transmite, salvo isomorfismo, a través del Nullstellensatz a una equivalencia natural de categorías. Un anillo R se dice *reducido* si no posee elementos nilpotentes no nulos o, equivalentemente, si $\sqrt{(0)} = (0)$ en R. Si $\mathfrak{a}$ no es un ideal propio de un anillo R entonces $R \,/\, \sqrt{\mathfrak{a}}$ es un anillo reducido y, en particular, si $\mathfrak{a}$ es radical, el anillo cociente $R \,/\, \mathfrak{a}$ es reducido. En particular, todos los anillos de funciones polinomiales $\mathbb{K}[V]$ son anillos reducidos. Una

$\mathbb{K}$-*álgebra finitamente generada* es un anillo R que contiene al cuerpo $\mathbb{K}$ y tal que existe un morfismo suprayectivo de $\mathbb{K}$-álgebras

$$\Pi : \mathbb{K}[X_1, \ldots, X_m] \longrightarrow R.$$

Es decir, una $\mathbb{K}$-álgebra finitamente generada es un anillo isomorfo al anillo residual de un anillo de polinomios por algún ideal $\mathfrak{a}$. En otras palabras, una $\mathbb{K}$-álgebra finitamente generada es un anillo R isomorfo a una $\mathbb{K}$-álgebra de la forma siguiente:

$$R \cong \mathbb{K}[X_1, \ldots, X_m] \Big/ \mathfrak{a}.$$

Una $\mathbb{K}$-*álgebra finitamente generada reducida* es una $\mathbb{K}$-álgebra finitamente generada que es reducido como anillo. Nótese que, por el Nullstellensatz en la versión Truco de Rabinowitsch, una $\mathbb{K}$-álgebra finitamente generada reducida es cualquier $\mathbb{K}$-álgebra R isomorfa a un anillo de la forma $\mathbb{K}[V]$, donde V es una variedad algebraica afín.
Esto nos da lugar a definir dos categorías:

- La categoría $\mathscr{V}_{\mathbb{A}}^{\mathbb{K}}$: formada por los elementos siguientes:
  - Los objetos de la categoría son las variedades algebraicas afines V contenidas en algún espacio afín de dimensión finta sobre $\mathbb{K}$.
  - Los morfismos entre dos objetos V y W son las aplicaciones polinomiales $f : V \longrightarrow W$.
- La categoría $\mathbb{K} - Alg_{red}$: formada por los elementos siguientes:
  - Los objetos de la categoría son las $\mathbb{K}$-álgebras finitamente generadas reducidas.
  - Los morfismos entre dos de tales $\mathbb{K}$-álgebras R y R' son los morfismos de anillos $\Phi : R \longrightarrow R'$ tales que
$$\Phi|_{\mathbb{K}} = Id_{\mathbb{K}}.$$

Una última interpretación del Nullstellensatz sería el enunciado siguiente:

Teorema 0.0.8 (**Nullstellensatz: Equivalencia Natural**). *El functor contravariante siguiente define una equivalencia natural en $\mathscr{V}_{\mathbb{A}}^{\mathbb{K}}$ y $\mathbb{K} - Alg_{red}$: $F_{\mathbb{K}}$ es un functor dado mediante:*

i) A cada variedad $V \subseteq \mathbb{A}^m(\mathbb{K})$, asocia su anillo de funciones polinomiales:

$$F_{\mathbb{K}}(V) := \mathbb{K}[V].$$

ii) A cada aplicación polinomial $f : V \longrightarrow W$, asocia el morfismo de $\mathbb{K}$-álgebras

$$F_{\mathbb{K}}(f) := f^* : \mathbb{K}[W] \longrightarrow \mathbb{K}[V].$$

En particular, dos variedades algebraicas afines $V \subseteq \mathbb{A}^m$ y $W \subseteq \mathbb{A}^n$ son isomorfas (se dice *birregularemnte isomorfas*) si y solamente si las $\mathbb{K}$-álgebras $\mathbb{K}[V]$ y $\mathbb{K}[W]$ son isomorfas como $\mathbb{K}$-álgebras.
La combinación de los diversos enunciados del Nullstellensatz expuestos resultarán esencial para el diseño del concepto de *esquema* que será la noción clave para el fundamento de la Geometría Algebraica de Grothendieck y Dieudonné (ver [**Ha, 1977**] para una ligera introducción).
Sin embargo, no es la exploración de este amplio cambio el objetivo de este Trabajo Fin de Grado. No vamos hacia la abstracción que se sigue del Nullstellensatz, sino que retomaremos la formulación original (especialmente bajo la forma de Identidad de Bézout) a través de los llamados *Nullstellensätze Efectivos*.

Nullstellensätze Efectivos: antecedentes

La larga pelea ideológica entre Hilbert y Kronecker hizo que Hilbert no tuviera un excesivo interés en disponer de un Nullstellensatz constructivo (o efectivo) hasta que se lo encarga a su alumna G. Hermann quien publicará sus resultados en 1926.
Las cotas obtenidas por G. Hermann eran tan impracticables (como veremos más adelante) que hacían del Nullstellensatz "Efectivo" un herramienta inútil como instrumento algorítmico. Será con el resurgimiento de la Teoría de la Eliminación, a través de la naciente Computación Simbólica, que el tema retomará interés en los año 80 del pasado siglo. Con el tiempo la motivación algorítmica se diluyó, convirtiéndose el estudio de los Nullstellensätze Efectivos en una especie de "competición de élite" en la que muchas participan no con un sentido científico de fondo sino como simple "competición olímpica" para intentar disponer de la cota más fina posible. El resultado de Jelonek pertenece en esta segunda clase de "competición olímpica".

Pero vamos a tratar de dar un contexto que explique los antecedentes de la perspectiva de la búsqueda de algoritmos eficientes en Teoría de la Eliminación.
Comencemos, por tanto, con las motivaciones de Hilbert para lograr algoritmos que *eliminen* bloques de cuantificadores en fórmulas de primer orden. Ya en su famosa conferencia del año 1900 en París, Hilbert establece entre sus 23 problemas el siguiente:

PROBLEMA X DE HILBERT. *Diseñar un procedimiento algorítmico que realice la siguiente tarea: Dada una lista de polinomios* $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$*, decidir si es o no cierta la siguiente fórmula:*

$$\exists x_1 \in \mathbb{Z}, \ldots, \exists x_n \in \mathbb{Z}, f_1(X_1, \ldots, X_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0. \tag{0.0.5}$$

Este enunciado y su resolución tendrán un impacto decisivo en la sociedad moderna por razones muy distintas a las pensadas originalmente por Hilbert. Así, el trabajo de K. Gödel en su tesis ([**Gö, 1931**]) demostrará que la Teoría Elemental de Números es incompleta e indecidible. La "incompletitud" exhibe las limitaciones del método deductivo en la decisión de verdad o falsedad, lo que tendrá una influencia en los fundamentos filosóficos de la Ciencia que afectará a muchos otros contextos. La "indecidibilidad" será la prueba que existen problemas que no admiten algoritmos para su resolución: muestra el límite de la algorítmica para alcanzar no ya la verdad sino ni siquiera lo demostrable. Como la pregunta de Hilbert afecta a una parte de la Teoría Elemental de Números (son fórmulas con un bloque de cuantificadores existenciales), muchos autores comienzan el camino de la respuesta negativa al Problema X de Hilbert. En ese camino hay una búsqueda fundamental: *para probar que algo no es algoritmizalbe, primero habrá que definir claramente que es un algoritmo.*
En los años 30 del pasado siglo, A. Church, A. Turing y S. C. Kline, entre otros muchos autores, desarrollarán teorías propias de la noción de algoritmo (cf., por ejemplo [**Ch, 1936**], [**Tu, 1937**], [**Kl, 1936**]) e irán demostrando que sus nociones son equivalentes a la noción de "función recursiva" de Göedel, mientras exhiben menos problemas indecidibles. Todas las definiciones serán probadas como equivalentes, lo que concluirá a la definición de algoritmo conocida como *Tesis de Church-Turning.* Pero la definición de A. Turing tendrá un mayor impacto social: por primera vez en la historia de la ciencia, una noción abstracta (la *máquina de Turing*) se transforma en un objeto físico que no existía con anterioridad (el *ordenador*). Es innegable la influencia de este sencillo paso en la *revolución digital* que estamos viviendo. Mientras la obra de Göedel genera una tal influencia en varios planos de la sociedad, muchos autores continúan con el enunciado tal y como lo propuso Hilbert. Autores como E. L. Post, D. Putnam, M. Davis contribuyen en una u otra medida al progreso de ese estudio. Pero serán dos autores quienes, fundamentalmente, resuelven el Problema X de Hilbert: J. Robinson (en realidad Julia Bowman, Robinson es su nombre de casada) en la serie de trabajos que publicará a lo largo de los años 50 del pasado siglo (y que ella resume en [**Ro, 1966**]) y J.V. Matijasévic quien, usando los avances de Robisnon, culmina la respuesta al Problema X de Hilbert en su trabajo [**Mtj, 1970**].
La respuesta de los autores citados al problema X de Hilbert es negativa. Entonces, ¿qué podría tener en mente Hilbert cuando establece su enunciado? En la respuesta a esta pregunta subyace la motivación del Nullstellensatz Efectivo.
Cambiemos la formulación de la expresión 0.0.5 y descubriremos un mundo de preguntas que afecta, entre otras cosas, al 33% de los problemas abiertos del Instituto Clay.

i) La expresión original es indecidible

$$\exists x_1 \in \mathbb{Z}, \ldots, \exists x_n \in \mathbb{Z}, f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0.$$

ii) CONJETURA DE BIRCH Y SWINNERTON-DYER: Supongamos que $V_{\mathbb{A}}(f_1, \ldots, f_s) \subseteq \mathbb{A}^n(\mathbb{C})$ satisface alguna propiedad adicional, por ejemplo, que sea una variedad abeliana (i.e. que tenga estructura de grupo abeliano), ¿será entonces posible hallar un algoritmo que responda a la pregunta original de Hilbert?.

iii) PRINCIPIO DE TARSKI: Cambiemos un poco la fórmula, en especial los dominios a los que afectan los cuantificadores, escribiendo:

$$\exists x_1 \in \mathbb{R}, \ldots, \exists x_n \in \mathbb{R}, f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0. \tag{0.0.6}$$

Entonces, existe un algoritmo que decide si 0.0.6 es cierta o falsa. El resultado fue obtenido por A. Tarski en los años 30 del pasado siglo.

iv) *Conjetura de Cook:* modifiquemos la identidad 0.0.5 suponiendo que los polinomios dados poseen coeficientes en un cuerpo finito. Y preguntemos por un algoritmo que resuelva la siguiente pregunta: Dadas $f_1, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_n]$, decidir

$$\exists x_1 \in \mathbb{F}_q, \ldots, \exists x_n \in \mathbb{F}_q, f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0. \tag{0.0.7}$$

Obviamente existe un algoritmo que consiste en probar que los q^n puntos de $\mathbb{F}_q^n$. Pero eso es un algoritmo de tipo exponencial en tiempo. La Conjetura de Cook pregunta si este problema (que es NP-completo) admite un algoritmo en tiempo polinomial $(qn)^{O(1)}$ cuando los grados de los polinomios $f_1, \ldots, f_s$ estén acotados, por ejemplo, por 3.

v) Hilbert, en su cabeza modificaba todas las sustituciones por las siguientes: Tomemos un cuerpo K (por ejemplo, los cuerpos primos) y su clausura algebraica $\mathbb{K}$. Entonces, *existe un algoritmo que decide si es cierta o falsa la afirmación siguiente*:

$$\exists x_1 \in \mathbb{K}, \ldots, \exists x_n \in \mathbb{K}, f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0. \tag{0.0.8}$$

La afirmación de Hilbert sobre la existencia del algoritmo está, en realidad, en la obra de L. Kronecker [**Kr, 1882**]. Pero Hilbert quiere su propia aproximación y esa es la razón de su encargo a G. Hermann: el *Nullstellensatz Efectivo*.

Retomemos por un momento la clásica Identidad de Bézout univariada. Para un entero $d \in \mathbb{N}$, denotemos por $K[X]_d$ el K-espacio vectorial de dimensión $d+1$ formado por todos los polinomios de grado acotado por d. Consideremos la base monomial B formada por $\{1, X, \ldots, X^d\}$ de $K[X]_d$. La formulación habitual de la Identidad de Bézout debería darse con cotas de grado (y no como se acostumbra). Este enunciado sería el siguiente:

TEOREMA 0.0.9. *Con las notaciones precedentes, sean $f, g \in K[X]$ dos polinomios de grados respectivos $m, n \in \mathbb{N}$, ambos positivos. Son equivalentes:*

i) El máximo común divisor de f y g es 1 en $\mathbb{K}[V]$.

ii) Existen $h_1 \in K[X]_{n-1}$ y $h_2 \in K[X]_{m-1}$ tales que

$$1 = h_1 f + h_2 g.$$

iii) No existe $z \in \mathbb{K}$ tal que $f(z) = 0$ y $g(z) = 0$.

Observemos que *iii)* es un Nullstellensatz univariado y podemos usar *ii)* para definir la siguiente aplicación lineal:

$$\begin{aligned} \Phi : K[X]_{n-1} \times K[X]_{m-1} &\longrightarrow K[X]_{n+m-1} \\ (h_1, h_2) &\longmapsto h_1 f + h_2 g. \end{aligned}$$

Observemos que Φ es aplicación K-lineal entre dos espacios vectoriales de la misma dimensión. Además, se observa que $1 \in Im(\Phi)$ si y solamente si Φ es un epimorfismo de espacios vectoriales. Por tanto, las afirmaciones *i)*, *ii)* y *iii)* anteriores son equivalentes a la siguiente:

iv) La aplicación lineal Φ anterior es un isomorfismo de espacios vectoriales.

A mediados del siglo XIX, J. J. Sylvester toma en [**Syl, 1853**], las ideas de Bézout en [**Bez, 1779**], que llegan a él a través de Sturm, y comprueba que esta afirmación *iv)* tiene una fácil construcción. Diseña la matriz de Φ en las respectivas bases monomiales, que acabará llamándose *matriz de Sylvester de fg*, y la resultante univariada:

$$Res_X(f, g) := \det(Sylv(f, g)).$$

Obtiene así propiedades equivalentes a *i)*, *ii)*, *iii)*, y *iv)* como son:

v) La matriz de Sylvester de f y g es una matriz de rango máximo.

vi) La resultante $Res_X(f, g) \neq 0$.

Las formulaciones *v)* y *vi)* son formulaciones más eficientes en términos algorítmicos que el uso del algoritmo de Euclides (lo que no podrá hacerse en el caso $\mathbb{Z}$) y da una versión algorítmica (en Álgebra Lineal elemental) que permite trabajar con la expresión

$$\exists z \in \mathbb{K}, f(z) = 0, g(z) = 0.$$

Hilbert se plantea una generalización de esa idea con las formulaciones de su identidad de Bézout (ver Teorema 0.0.9 anterior). Para lo cual, encarga a G. Hermann una primera versión histórica del Nullstellensatz Efectivo. La contribución principal de G. Hermann es la siguiente:

TEOREMA 0.0.10. *Existe una función $D : \mathbb{N}^3 \longrightarrow \mathbb{R}_+$ que satisface la siguiente propiedad: Dada una familia $f_1, \ldots, f_s \in K[X_1, \ldots, X_m]$ de polinomios con coeficientes en un cuerpo K, en univariables, de grado acotado por d. Son equivalentes:*

i) $\neg(\exists x \in \mathbb{K}^m, f_1(x) = 0, \ldots, f_s(x) = 0)$.

ii) Existen polinomios $g_1, \ldots, g_s \in K[X_1, \ldots, X_m]$ tales que

- $1 = g_1 f_1 + \cdots + g_s f_s$.
- $\deg(g_i f_i) \leq D(m, s, d)$.

Además, la función D puede elegirse de tal modo que

$$D(m, s, d) \leq (sd)^{2^m}.$$

La mera existencia de la función $D(n, s, d)$ permite algoritmizar el Nullstellensatz del modo en que lo pensó Sylvester pero en el caso multivariado. Veamos cómo se interpreta la aplicación algorítmica de este resultado de G. Hermann.
Sea $d \in \mathbb{N}$ un entero positivo. Con las notaciones precedentes, dado un cuerpo L cualquiera, denotaremos por $P_d^L(X_1, \ldots, X_m)$ al conjunto de los polinomios con coeficientes en L de grado acotado por d en las variables $\{X_1, \ldots, X_m\}$. Esto es,

$$P_d^L := P_d^L(X_1, \ldots, X_m) = \{f \in L[X_1, \ldots, X_m] : \deg(f) \leq d\}.$$

Es sencillo verificar que P_d^L es un espacio vectorial de dimensión finita sobre el cuerpo L. Es sencillo, además, verificar que una base de P_d^L es la *base monomial*:

$$B_{d,m} := \{X_1^{\mu_1} \cdots X_m^{\mu_m} : \mu_1 + \cdots + \mu_m \leq d\}.$$

Se tiene, además, la siguiente identidad:

$$\dim_L P_d^L = \#(B_{d,m}) = \binom{d+m}{m}.$$

Supongamos ahora que tenemos una cota $D := D(m, s, d)$ como la descrita por G. Hermann. Supongamos que nos dan una lista de polinomios $f_1, \ldots, f_s \in K[X_1, \ldots, X_m]$ y definimos la siguiente aplicación lineal:

$$\begin{aligned} \Phi : \prod_{i=1}^{s} (P_{D-d_i}^K) &\longrightarrow P_D^K \\ (g_1, \ldots, g_s) &\longmapsto g_1 f_1 + \cdots + g_s f_s, \end{aligned}$$

donde $d_i = \deg(f_i)$ para cada $i, 1 \leq i \leq s$. Entonces, son equivalentes:

i) Existe $x \in V_{\mathbb{A}}(f_1, \ldots, f_s)$ o, equivalentemente,

$$\exists x \in \mathbb{A}^m(\mathbb{K}), f_1(x) = 0, \ldots, f_s(x) = 0.$$

ii) $1 \notin Im(\Phi)$.

Más aún, como Φ es lineal, podremos construir la matriz de Φ con respecto a las bases monomiales respectivas de los espacios producto $\prod_{i=1}^s P_{D-d_i}^K$ y de P_D^K. Llamaremos M_Φ a esa matriz. Entonces, las propiedades i) y ii) anteriores son equivalentes a

iii) El vector $1 = (1, 0, \ldots, 0) \in P_D^K$ en base monomial, no está en la imagen de M_Φ.

La respuesta no es tan elegante como el caso univariado pero puede construirse un *sistema de ecuaciones lineales* del modo siguiente. Para cada i, $1 \leq i \leq s$, denotemos por $\underline{Z}_i$ a la lista de variables asociadas a las coordenadas en $P_{D-d_i}^K$:

$$\underline{Z}_i = (z_i^\mu : \mu \in \mathbb{N}^m, |\mu| = \mu_1 + \cdots + \mu_m \leq D - d).$$

Denotemos por $\underline{Z}$ a la agrupación de todas estas variables

$$\underline{Z} = (\underline{Z}_1, \ldots, \underline{Z}_s).$$

y sea $e = (1, 0, \ldots, 0) \in P_D^K$ la lista de coordenadas de $1 \in P_D^K$ en la base monomial.
Entonces, serán equivalentes:

i) $\exists x \in \mathbb{A}^m(\mathbb{K}), f_1(x) = 0, \ldots, f_s(x) = 0$.

ii) El sistema de ecuaciones lineales con coeficientes en K siguiente es incompatible

$$M_\Phi \cdot \underline{Z} = e.$$

Dado que decidir si un sistema de ecuaciones lineales es compatible o no se conoce desde los tiempos de C. F. Gauss, el Nullstellensatz Efectivo se transforma en la siguiente lista de conclusiones:

i) Es posible decidir algorítmicamente si dadas $f_1, \ldots, f_s \in K[X_1, \ldots, X_m]$ poseen una solución común en $\mathbb{A}^m(\mathbb{K})$.
ii) El algoritmo que responde a la existencia de soluciones en $\mathbb{K}^n$ no requiere usar nunca elementos de $\mathbb{K}$: basta con hacer operaciones aritméticas sobre el cuerpo de base K.
iii) La complejidad en tiempo, entendida como la cantidad de operaciones aritméticas en K que realiza el algoritmo, depende fuertemente de la cota D expresada en nuestro Nullstellensatz Efectivo.

Es el apartado *iii*) el que impulsó inicialmente los estudios de posibles mejoras de la cota $D(m, s, d)$ original de G. Hermann. Veamos un poco el significado de esa cota.
Descartemos la dificultad inicial de que, contrariamente al caso univariado, escribir las coordenadas de la matriz M_Φ a partir de los coeficientes de $f_1, \ldots, f_s$ tiene un coste significativo no trivial. *Asumamos que la matriz M_Φ es obtenible sin coste adicional significativo.*
Para escribir M_Φ y para decidir si un sistema cuya matriz de coeficientes es M_Φ es o no compatible, la cantidad esencial a considerar es el máximo del número de filas y columnas de M_Φ. Sea N_Φ ese máximo. Escribir M_Φ costaría un tiempo del orden $O(N_\Phi^2)$ y decidir si el sistema $M_\Phi \underline{Z} = e$ es o no compatible requerirá un número de operaciones aritméticas del orden $O(N_\Phi^w)$ donde w es la constante del Álgebra Lineal de la cual se conoce, donde los trabajos de V. Strassen, que vale:

$$2 \leq w \leq \log_2 7.$$

Por tanto, la acotación de N_Φ es la esencia del estudio del número de operaciones aritméticas por hacer en el algoritmo inspirado por un Nullstellensatz Efectivo. Ahora bien, tenemos

- Número de columnas de M_Φ es dado por

$$\sum_{i=1}^{s} \dim_K(P^K_{D-d_i}) = \sum_{i=1}^{s} \binom{D - d_i + m}{m}.$$

- Número de filas de M_Φ es dado por

$$\dim_K(P^K_D) = \binom{D+m}{m}.$$

Grosso modo, podemos acotar N_Φ mediante

$$N_\Phi \leq s\binom{D+m}{m} \approx sD^m.$$

En el caso de la cota $D(m, s, d)$ de G. Hermann tendríamos:

$$N_\Phi \leq s(sd)^{2^m m}. \tag{0.0.9}$$

Nótese que no existe ningún ordenador conocido (ni de los del Top 500) capaz de realizar un número de operaciones aritméticas del orden descrito en 0.0.9 cuando $m \geq 10$, incluso con $m \geq 6$. Esto es debido a que la cota de Hermann es doblemente exponencial en el número de variables, lo cual lo hace impracticable.
Surge así la necesidad de buscar mejoras de la cota $D(m, s, d)$ de G. Hermann. Esta carrera, que estuvo interrumpida durante casi 50 años, se retoma en los años 70 y se logran los primeros avances significativos hacia finales de los años 80.

- Los primeros en retomar las ideas de G. Hermann fueron D. W. Masser y G. Wüsholtz en 1971 (c.f. [**MaWü, 1971**]). Su cota para $D(m, d, s)$ será muy similar a la de [**He, 1996**]:

$$D(m, d, s) \leq sd^{d^m}.$$

- A finales de los 80 del pasado siglo, de manera independiente todos ellos, llegan a una acotación fina de la función de G. Hermann. Son W. D. Brownawell (en [**Br, 1987**]), L. Caniglia, A. Galligo y J. Hertz (en [**CGH, 1989**]) y J. Kollàr (en [**Kol, 1988**]). Su acotación será de la forma:

$$D(m, d, s) \leq (\max\{3, d\})^m.$$

- Un famoso ejemplo, encontrado independientemente por varios autores, como T. Mora, D. Lazard, G.W. Masser o P. Philippen, permitirá concluir que
$$d^{m-1} \leq D(m,s,d).$$
- El caso de sistemas de ecuaciones con grado $d = 2$ (para el cual la cota sería 3^m) fue discutido en [**Som, 1999**], quien prueba:
$$D(m,s,d) \leq 2d^m.$$
- En [**KrPa, 1996**] dos nuevas interpretaciones del Nullstellensatz Efectivo aparecen para cambiar la perspectiva:
  - Se pueden obtener y calcular los coeficientes de una identidad de Bézout sobre K con un número total de operaciones del orden $sd^{O(m)}$ y con grados finales $D(m,d,s) \leq d^{O(m)}$.
  - Lo que es más importante: No es necesario usar el Nullstellensatz Efectivo para decidir la veracidad de la fórmula

$$\exists x \in \mathbb{A}^m(\mathbb{K}), f_1(x) = 0, \ldots, f_s(x) = 0. \tag{0.0.10}$$

Para explicar este último avance, nótese lo siguiente. supongamos la cota de Brownawell-Canigla-Gallego-Heintz-Kollàr $D := D(m,s,d) = \max\{s,d\}^m$. Supongamos $d \geq s$.
Retomamos la construcción de la aplicación lineal

$$\begin{aligned}\Phi : \prod_{i=1}^{s}(P^K_{D-d_i}) &\longrightarrow P^K_D \\ (g_1,\ldots,g_s) &\longmapsto g_1f_1 + \cdots + g_sf_s,\end{aligned}$$

Entonces, decidir 0.0.10 se hará mediante un sistema de ecuaciones lineales
$$M_\Phi \underline{Z} = e$$
donde el máximo número de filas y columnas de M_Φ es la cantidad
$$N_\Phi \approx s\binom{d^m+m}{m} \approx sd^{m^2}.$$
Además, el Ejemplo de Mara-Lazard-Masser-Philippen garantiza que hay casos en los que no se puede mejorar
$$N_\Phi \approx s\binom{d^{m-1}+m}{m} \approx sd^{m(m-1)}.$$
En suma, la estrategia algorítmica basada en el Nullstellensatz Efectivo está condenada a ejecutar algoritmos de Álgebra Lineal con matrices de tamaño N_Φ y no puede hacerse en menos de
$$sd^{2m^2}$$
operaciones. La contribución de [**KrPa, 1996**] mostrará un algoritmo que no hace uso del Nullstellensatz Efectivo y que permitirá decidir una expresión como 0.0.10 con un número total de operaciones aritméticas acotado por:
$$s^{o(1)}d^{O(m)},$$
donde los exponentes $O(\cdot)$ esconden una constante independiente de todos los ingredientes que intervienen. A partir de este punto, el estudio del Nullstellensatz Efectivo se separa de sus aplicaciones algorítmicas: no sirve ya, como pensaba Hilbert, para tener algoritmos eficientes. Pero, por otro lado, sigue siendo un lindo problema como "competición olímpica": se trata de ver quién tiene la mejor cota que, en todo caso, no mejorará el d^{m-1}. Para mostrar la bifurcación entre ambos campos, resumamos los siguientes:

- A mediados de los años 90, en la serie [**Pa, 1995**], [**GHMP, 1995**], [**GHMP, 1997a**], [**GHHMMP, 1997b**], [**GHMMP, 1998**], se desarrolla toda una nueva serie de algoritmos de *naturaleza intrínseca* para la resolución de sistemas de ecuaciones polinomiales y para la decisión de fórmulas como 0.0.10 cuya complejidad estará acotada por un polinomio en
$$smd\delta L,$$

donde L es el coste de evaluar en un punto los polinomios $f_1, \ldots, f_s$ y $\delta := \delta(f_1, \ldots, f_s)$ es una cantidad intrínseca (conocida como grado geométrico del sistema $\{f_1, \ldots, f_s\}$) que satisface $\delta \leq d^{m-1}$. Esta línea será ampliamente seguida por muchos autores hasta la actualidad, pero se aleja del propósito de este TFG.

- La cantidad intrínseca δ será utilizada en [**HMPS, 2000**] para dar un Nullstellensatz Efectivo con cotas dependientes del grado intrínseco del sistema.
- En [**KPS, 2001**] se usará δ y una noción de altura intrínseca del sistema $\eta := \eta(f_1, \ldots, f_s)$ para acotar el grado y altura (talla de los coeficientes del sistema).

Sin embargo, esta línea se aleja ya del propósito de esta TFG y nos quedaremos con las reflexiones propias de los Nullstellensatz Efectivos dentro de la *"carrera olímpica por la mejor cota"*.
J.Kollàr o M. Sombra seguirán en esa carrera a la que se unirá Z. Jelonek en el año 2005, que es el objeto de esta memoria.

Resumen de los Principales contenidos de la Memoria

Como ya se ha señalado en esta larga Introducción, el principal objetivo de este Trabajo Fin de Grado consiste en exponer una prueba, tan autocontendio como sea posible, del Nullstellensatz Efectivo de Z. Jelonek (presentado en [**Je, 2005**]). El trabajo de probar con todo detalle este Teorema se ha estructurado en dos capítulos que pasamos a resumir a continuación:
En el Capítulo 1 vamos a presentar las pruebas completas, tan autocontenidas como sea posible, de dos resultados técnicos clave para el desarrollo del Nullstellensatz Efectivo de Jelonek, que describiremos en el Capítulo siguiente:

- El Teorema de Perron (Generalizado) (cf. Teorema 1.2.3).
- El Nullstellensatz Efectivo en el caso sub-determinado (cf. Teorema 1.3.3).

Usaremos libremente las notaciones ya descritas en la Introducción así como algunos resultados y nociones básicas descritas en el Apéndice.
Como en la Introducción, K será un cuerpo y $\mathbb{K}$ será su clausura algebraica.
El primer resultado del que nos ocupamos en este Capítulo es una generalización de un Teorema clásico sobre proyecciones e imágenes de variedades algebraicas afines. En general, dada cualquier aplicación polinomial $f : V \longrightarrow \mathbb{A}^n$, la imagen $f(V)$ no suele ser una variedad algebraica. De hecho, un Teorema clásico de Chevalley prueba que si $V \subseteq \mathbb{A}^m$ es una variedad algebraica afín y si $f : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ es una aplicación polinomial, entonces $f(V)$ es un conjunto constructible (unión finita de localmente cerrados en $\mathbb{A}^n$). Es fácil construir ejemplos en los que la imagen de una variedad algebraica no es ni variedad algebraica ni localmente cerrado.
Por eso, el interés se suele focalizar en disponer de valores cuantitativos de $\overline{f(V)}^z$ más que de $f(V)$. El Teorema de Perron trata justamente de probar, bajo ciertas hipótesis, que se puede controlar el grado de una hiper-superficie que contiene a $\overline{f(V)}^z$. Aquí presentaremos una generalización debida a Jelonek.
Sean $V \subseteq \mathbb{A}^m, W \subseteq \mathbb{A}^m$ dos variedades algebraicas irreducibles $f : V \longrightarrow W$ se llama dominante si $\overline{f(V)}^z = W$. Se dice que un morfismo $f : V \longrightarrow \mathbb{A}^n$ es *genéricamente finito* si existe un abierto Zariski no vacío $U \subseteq \overline{f(V)}^z = W$ tal que para cada $y \in U$, la fibra $f^{-1}(\{y\})$ es una variedad cero-dimensional (i.e. un conjunto finito de puntos). El Teorema que probaremos en la Sección 1.2 es el siguiente:

TEOREMA 1 (**Teorema de Perron Generalizado**). *Sean $Q_1, \ldots, Q_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios no constantes con $\deg Q_i = d_i$. Sea $V \subset \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equidimensional afín de dimensión n y grado D. Si la aplicación $Q = (Q_1, \ldots, Q_{n+1}) : V \longrightarrow \mathbb{A}^{n+1}(\mathbb{K})$ es genéricamente finita, entonces existe un polinomio no nulo $W(T_1, \ldots, T_{n+1}) \in \mathbb{K}[T_1, \ldots, T_{n+1}]$ tal que:*

i) $W(Q_1, \ldots, Q_{n+1}) = 0$ *en* V.
ii) $\deg W(T_1^{d_1}, T_2^{d_2}, \ldots, T_{n+1}^{d_n+1}) \leq D \prod_{j=1}^{n+1} d_j$.

En esta misma Sección daremos una variante del Lema de Normalización de Noether a través de combinaciones lineales de coordenadas definidas por matrices triangulares superiores con unos en la diagonal principal (ver Lema 1.2.4).

Seguidamente, en la Sección 1.3, pasaremos a enunciar y probar con detalle el Nullstellensatz Efectivo de Jelonek *en el caso sub-determinado*. Aquí, el término sub-determinado hace referencia a que disponemos de, como mucho, tantas ecuaciones como la dimensión del espacio en el que viven las soluciones. En el caso genérico, es decir, con los coeficientes en un abierto Zariski, una sucesión $f_1, \dots, f_k$ de $k \leq n$ polinomios definen una variedad de dimensión $n-k$ en $\mathbb{A}^n(\mathbb{K})$. Esta intuición se rompe en el caso afín para ciertas ecuaciones que viven en un cerrado-Zariski del espacio de coeficientes. Se necesitará $k = n+1$ para que genéricamente en los coeficientes, una sucesión $f_1, \dots, f_{n+1}$ de ecuaciones defina la variedad vacía. El siguiente resultado hace referencia a la situación "sub-determinada" a la que $k \leq n$ ecuaciones carecen de cero en común.

TEOREMA 2 (**Nullstellensatz Efectivo, caso sub-determinado**). *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equi-dimensional afín de dimensión n y de grado D. Sean $f_1, \dots, f_k \in \mathbb{K}[X_1, \dots, X_m]$ polinomios no nulos con $k \leq m$. Sea $\deg f_i = d_i$ y $d_1 \geq \cdots \geq d_k$, $1 \leq i \leq k$. Si $V_{\mathbb{A}}(f_1, \dots, f_k) \cap V = \emptyset$, entonces existen polinomios $g_1, \dots, g_k \in \mathbb{K}[X_1, \dots, X_m]$ tales que:*

i) La siguiente identidad se verifica en $\mathbb{K}[V]$:

$$1 = \sum_{i=1}^{k} f_i g_i.$$

ii) Los grados de los productos $g_i f_i$ verifican la siguiente desigualdad, para cada $i \in \{1, \dots, k\}$:

$$\deg(f_i g_i) \leq D \prod_{i=1}^{k} d_i.$$

Grosso modo, la contribución de Jelonek consiste en lo siguiente: Introducimos un parámetro de deformación, una nueva variable Z. Construimos un morfismo de la forma siguiente:

$$\begin{aligned} \Phi : V \times \mathbb{K} &\longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^k(\mathbb{K}) \\ (x, z) &\longmapsto (x, f_1(x)z, \dots, f_k(x)z) \end{aligned}$$

Construimos una normalización de Noether de la imagen de Φ dependiente de $\underline{x}$ y de los $f_i \cdot Z$. Llamemos $\Psi_1, \dots, \Psi_{n+1}$ a los elementos de esa normalización de Noether. Consideramos la ecuación de dependencia entera de Z sobre $\mathbb{K}[\Psi_1, \dots, \Psi_{n+1}]$ y acotemos su grado a través del Teorema de Perron Generalizado. Esa ecuación de dependencia entera tendrá la forma:

$$P_Z(\Psi_1, \dots, \Psi_{n+1}, Z) = Z^\delta + \sum_{i=0}^{\delta-1} P_i(\Psi_1, \dots, \Psi_{n+1}) Z^i \in I(V \times \mathbb{K}).$$

Reescribiendo esa ecuación en $\mathbb{K}[X_1, \dots, X_m, Z]$ tomará la forma:

$$P_Z(\Psi_1, \dots, \Psi_{n+1}, Z) = (1 + A_\delta) Z^\delta + \sum_{r \neq \delta} A_r Z^r.$$

Ahora, la propiedad de que $P(\Psi_1, \dots, \Psi_{n+1}, Z) = 0$ significa que los coeficientes de esta última expresión están en $I(V)$. Así concluimos

$$1 + A_\delta \in I(V).$$

Verificando que $A_\delta = \sum_{i=1}^{s} g_i \cdot f_i$ y que los grados de los $g_i \cdot f_i$ son los apropiados, Jelonek prueba su resultado. Verificar que todos los detalles son correctos (algunos aparecen de modo confuso, casi errado, en la prueba original) es la principal contribución de este Capítulo.
En el Capítulo 2 culminaremos el objeto final de este Trabajo Fin de Grado, demostrando el Nullstellensatz Efectivo de [**Je, 2005**]. La primera parte del Capítulo se centra en probar un Teorema de Eliminación con cotas de grado, presente en [**Je, 2005**]. Ese Teorema es el siguiente:

TEOREMA 3. [**Teorema de Eliminación de** [**Je, 2005**]] *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica irreducible de dimensión n y grado D. Sean $k \leq n$ y $f_1, \dots, f_k \in \mathbb{K}[X_1, \dots, X_m]$ polinomios tales que la siguiente variedad es cero-dimensional:*

$$A = V \cap V_{\mathbb{A}}(f_1, \dots, f_k).$$

Entonces, existe un abierto Zariski $\mathcal{U}_1 \subseteq \mathscr{M}_m(\mathbb{K})$ *formado por matrices regulares tales que para cada* $B \in \mathcal{U}_1$*, el cambio de variables que determina:*

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix},$$

satisface las siguientes propiedades:

i) Y_1 *es un elemento separante sobre* A *y existe un polinomio univariado* $\Phi_1(T)$ *tal que si* $\Phi_1(z) = 0$*, entonces* $\exists a \in A$ *tal que*

$$z = Y_1(a).$$

ii) Existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ *tales que*

$$\Phi_1(Y_1) - \sum_{i=1}^{k} g_i f_i \in I(V).$$

iii) $\deg(g_i f_i) \leq D \cdot \prod_{i=1}^{k} \deg(f_i)$*,* $\deg(\Phi_1(Y_1)) \leq D \prod_{i=1}^{k} \deg(f_i)$*.*

La prueba del enunciado es completamente original, aunque está inspirada en [**Pa,19**]. Jelonek, en [**Je, 2005**], hace uso de su caracterización de los puntos de "impropiedad" en la imagen de morfismos dominantes y genéricamente finitos de su trabajo previo [**Je, 2001**].
Nosotros hemos desarrollado una prueba propia partiendo de la noción de *forma lineal separante* de una variedad cero-dimensional. Observamos que existe un abierto Zariski de matrices apropiadas (triangulares superiores con unos en la diagonal) que permiten poner las coordenadas en posición de Noether, de tal forma que cada una de las nuevas variables sea elemento separante (ver Proposición 2.2.2). Una vez probado ésto, usando la misma función Φ del Capítulo precedente

$$\begin{aligned} \Phi : V \times \mathbb{K} &\longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K}) \\ (x, z) &\longmapsto (x, f_1(x)z, \ldots, f_n(x)z), \end{aligned}$$

con el parámetro de deformación z, construimos un abierto distinguido $D(q_A)$ sobre una normalización de Noether de $\overline{\Phi(V \times \mathbb{K})}^z$, de tal modo que q_A sea el polinomio mínimo de una forma lineal separante, de grado controlado, y de tal modo que tengamos una extensión entera de anillos para las localizaciones:

$$\mathbb{K}[T_1, \ldots, T_{n+1}] \hookrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A}.$$

Esto se describe en la Proposición 2.2.6. Lo que se hace para una forma lineal separante es extensible a todas (Corolario 2.2.7) las variables nuevas de una normalización de Noether. Finalmente, usando una reflexión análoga a la hecha en el Capítulo precedente con el caso sub-determinado, no sólo podemos acotar el grado de las ecuaciones minimales de las formas lineales separantes sino también su presentación en la forma de combinación lineal de las clases de $\{f_1, \ldots, f_n\}$ en $\mathbb{K}[V]$. Este es el enunciado precedente destacado en esta introducción al Capítulo (el Teorema 2.2.8 del cuerpo del Capítulo).
Con estas herramientas estamos en condiciones de probar el enunciado Nullstellensatz Efectivo que es el Teorema siguiente y que se describe y prueba como Teorema 2.3.5 en la Sección 2.3 a continuación:

TEOREMA 4. **[Nullstellensatz Efectivo de** [**Je, 2005**]**]** *Sea* $V \subseteq \mathbb{A}^m(\mathbb{K})$ *una variedad algebraica afín irreducible de dimensión* n*. Sean* $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ *polinomios tales que* $d_i = \deg(f_i)$ *y se tiene*

- $d_1 \geq d_2 \geq \cdots \geq d_k$.
- $V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) = \emptyset$.

Entonces, existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ *tales que*

i) $1 - \sum_{i=1}^{k} g_i f_i \in I(V)$.

ii) $\deg(g_i f_i) \leq 2DN(d_1,\ldots,d_k;n) - 1$, *donde*

$$N(d_1,\ldots,d_k;n) = \begin{cases} \prod_{i=1}^{k} d_i & si\ k < n, n > 1 \\ \prod_{i=1}^{n} d_i & si\ n < k, n > 1 \\ d_1 & si\ n = 1. \end{cases}$$

El resultado ya se había probado en el caso sub-determinado $k \leq n$. Por tanto, queda la prueba del caso $k \geq n+1$. Usando un método clásico de combinaciones lineales que respetan los grados, se reduce el problema al caso $k = n+1$ (véase Lema 2.3.3 y la Observación 2.3.4). Así, nos encontramos, en el caso defectivo, con la situación en que podemos construir sucesiones $\{F_1,\ldots,F_{n+1}\}$ y $\{G_1,\ldots,G_{n+1}\}$ de combinaciones lineales genéricas de $\{f_1,\ldots,f_{n+1}\}$ tales que se verifique:

i) $V \cap V_{\mathbb{A}}(F_1,\ldots,F_n)$ es una variedad cero-dimensional.
ii) $V \cap V_{\mathbb{A}}(G_1,\ldots,G_n)$ es una variedad cero-dimensional.
iii) $V \cap V_{\mathbb{A}}(F_1,\ldots,F_n) \cap V \cap V_{\mathbb{A}}(G_1,\ldots,G_n) = \emptyset$.

Esta construcción, que hemos llamado *construcción cruzada* en la subsección 2.3.1, permite construir una forma lineal separante Y_1 para la unión $V \cap V(F_1,\ldots,F_n) \cup V \cap V(G_1,\ldots,G_n)$. Aplicando el Teorema de Eliminación a Y_1 sobre cada uno de ellos, obtendremos

- Un polinomio univariado $\Phi_1(Y_1)$ de grado apropiado y minimal tal que $\Phi_1(Y_1)$ se anula en $V \cap V(F_1,\ldots,F_n)$ y satisface las condiciones del Teorema de Eliminación precedente.
- Un polinomio univariado $\Phi_2(Y_1)$ de grado apropiado y minimal tal que $\Phi_2(Y_1)$ se anula en $V \cap V(G_1,\ldots,G_n)$ y satisface las condiciones del Teorema de Eliminación precedente.

Como Y_1 es separante para ambos y $V \cap V(F_1,\ldots,F_n) \cup V \cap V(G_1,\ldots,G_n) = \emptyset$, no es posible que $\Phi_1(T)$ y $\Phi_2(T)$ tengan ceros comunes. Por tanto, su máximo común divisor en $\mathbb{K}[T]$ es 1 y, aplicando la identidad de Bézout univariada tendremos:

$$1 = Q_1(Y_1)\Phi_1(Y_1) + Q_2(Y_1)\Phi_2(Y_1),$$

con grados de Q_1 y Q_2 acotados por los grados de Φ_1 y Φ_2. El Teorema de Eliminación precedente nos dice, además, que Φ_1 y Φ_2 se presentan como combinaciones de $F_1,\ldots,F_n$ y $G_1,\ldots,G_n$ respectivamente, de grados controlados, en el anillo $\mathbb{K}[V]$

$$\Phi_1(Y_1) = \sum_{i=1}^{n} h_{i,1}F_i, \Phi_2(Y_1) = \sum_{i=1}^{n} h_{i,2}G_i.$$

Por tanto, obtenemos una expresión de la forma siguiente, válida en $\mathbb{K}[V]$:

$$1 = \sum_{i=1}^{n}(Q_1(Y_1)h_{i,1})F_i + \sum_{i=1}^{n}(Q_2(Y_1)h_{i,2})G_i,$$

donde todas las cotas de grado han sido controladas. Recordando ahora que tanto $\{F_1,\ldots,F_n\}$ como $\{G_1,\ldots,G_n\}$ son combinaciones lineales de $\{f_1,\ldots,f_k\}$ se obtiene la expresión final:

$$1 = \sum_{i=1}^{k} g_i f_i \text{ en } \mathbb{K}[V],$$

con las cotas de grado que se siguen de las cotas de Φ_1, Φ_2, $h_{i,j}$, Q_1 y Q_2 antes citadas.

Comparación de las cotas obtenidas con resultados previos

Se va a realizar un repaso de las cotas que se obtuvieron en algunos de los resultados previos al de Jelonek, y se va a comparar con los obtenidos por este, resultando en la mayoría de ellos menores o con menos restricciones que en los casos anteriores.

- Para el caso de $V = \mathbb{K}^n$, Kollàr en [**Kol, 1988**] demostró que para el caso de que los grados de los polinomios fuesen mayores o iguales a 3, es decir, $d_i \geq 3, 1 \leq i \leq k$, y que la variedad V cumpliera $\deg(V) \geq 2$ se alcanza la cota $N(d_1,\ldots,d_k;n)$. Por tanto, el resultado de Jelonek mejora el caso $k \leq n$ al exigir menos condiciones, pero es mayor en el caso $k > n$.

- Por otra parte, Sombra en [**Som, 1999**] para el caso de $V = \mathbb{K}^n$ con la única restricción de que la variedad V cumpliera $\deg(V) \geq 2$ obtuvo una cota de $2N(d_1, \ldots, d_k; n)$. Por tanto el resultado de Jelonek es mejor, especialmente en el caso $k \leq n$.
- En el caso general de una variedad algebraica afín $V \subseteq \mathbb{K}^m$ cualquiera, de dimensión n y grado D, Kollàr en [**Kol, 1999**] obtuvo la cota $(m+1)DN(d_1, \ldots, d_k; n+2)$, inferior a la de Jelonek.
- Por otra parte, para el caso general, imponiendo que la clausura proyectiva de V fuera una variedad Cohen-Macaulay, Sombra en [**Som, 1999**] obtuvo la cota $(n+1)^2 Dd^{n+1}$ siendo $d = \max\{d_i, 1 \leq i \leq k\}$, donde, de nuevo, la cota de Jelonek es mejor.

Sobre el estilo y la ortografía usados en este TFG

En algún caso precedente se ha discutido el estilo y la ortografía de las memorias presentadas como Trabajo de Fin de Grado en Matemáticas. En evitación de intervenciones innecesarias, queremos clarificar algunos aspectos relativos al estilo elegido en este texto.
Se ha elegido el formato de libro (book) de la *American Mathematical Society (AMS)*. Aunque el idioma utilizado es el español, hemos tratado de seguir lo más fielmente posible las recomendaciones del Libro de Estilo de esta asociación[2], juntamente con las reglas de estilo recomendadas por D. E. Knuth y co-autores para la *Mathematical Asociation of America (MAA)*[3].
Específicamente, hemos tratado de seguir atentamente las siguientes dos reglas:

- *"Numbered theorems, lemmas, etc. are proper nouns and, thus, are capitalized: Theorem 2.3, Lemma 3.1, Figure 4.5"* (p. 79 del *AMS Style Guide*).
- *"Rule 19. Capitalize names like Theorem 1, Lemma 2, Algorithm 3, Method 4"'* (en D. E. Knuth *et al.*).

[2] M. Letourneau, J. Wright Sharp, *AMS Style Guide, Journals, October 2017*, AMS, Providence, 2017
[3] D. E. Knuth, T. Larrabee, P. M. Roberts, *Mathematical Writing*, MAA, 1989

CAPíTULO 1

El Teorema de Perron (Generalizado) y un Nullstellensatz Efectivo en el caso Sub-determinado

Índice

1.1. Introducción.

En este primer Capítulo vamos a presentar las pruebas completas, tan autocontenidas como sea posible, de dos resultados técnicos clave para el desarrollo del Nullstellensatz Efectivo de Jelonek, que describiremos en el Capítulo siguiente:

- El Teorema de Perron (Generalizado) (cf. Teorema 1.2.3).
- El Nullstellensatz Efectivo en el caso sub-determinado (cf. Teorema 1.3.3).

Usaremos libremente las notaciones ya descritas en la Introducción así como algunos resultados y nociones básicas descritas en el Apéndice.
Como en la Introducción, K será un cuerpo y $\mathbb{K}$ será su clausura algebraica.
El primer resultado del que nos ocupamos en este Capítulo es una generalización de un Teorema clásico sobre proyecciones e imágenes de variedades algebraicas afines. En general, dada cualquier aplicación polinomial $f : V \longrightarrow \mathbb{A}^n$, la imagen $f(V)$ no suele ser una variedad algebraica. De hecho, un Teorema clásico de Chevalley prueba que si $V \subseteq \mathbb{A}^m$ es una variedad algebraica afín y si $f : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ es una aplicación polinomial, entonces $f(V)$ es un conjunto constructivo (unión finita de localmente cerrados en $\mathbb{A}^n$). Es fácil construir ejemplos en los que la imagen de una variedad algebraica no es ni variedad algebraica ni localmente cerrado.
Por eso, el interés se suele localizar en disponer de valores cuantitativos de $\overline{f(V)}^z$ más que de $f(V)$. El Teorema de Perron trata justamente de probar, bajo ciertas hipótesis, que se puede controlar el grado de una hiper-superficie que contiene a $\overline{f(V)}^z$. Aquí presentaremos una generalización debida a Jelonek.
Sean $V \subseteq \mathbb{A}^m, W \subseteq \mathbb{A}^m$ dos variedades algebraicas irreducibles $f : V \longrightarrow W$ se llama dominante si $\overline{f(V)}^z = W$. Se dice que un morfismo $f : V \longrightarrow \mathbb{A}^n$ es *genéricamente finito* si existe un abierto Zariski no vacío $\subseteq \overline{f(V)}^z = W$ tal que para cada $y \in U$, la fibra $f^{-1}(\{y\})$ es una variedad cero-dimensional (i.e. un conjunto finito de puntos). El Teorema que probaremos en la Sección 1.2 es el siguiente:

Teorema 5 (**Teorema de Perron Generalizado**). *Sean $Q_1, \ldots, Q_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios no constantes con $\deg Q_i = d_i$. Sea $X \subset \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equidimensional afín de dimensión n y grado D. Si la aplicación $Q = (Q_1, \ldots, Q_{n+1}) : X \longrightarrow \mathbb{A}^{n+1}(\mathbb{K})$ es genéricamente finita, entonces existe un polinomio no nulo $W(T_1, \ldots, T_{n+1}) \in \mathbb{K}[T_1, \ldots, T_{n+1}]$ tal que:*

i) $W(Q_1, \ldots, Q_{n+1}) = 0$ *en* X.
ii) $\deg W(T_1^{d_1}, T_2^{d_2}, \ldots, T_{n+1}^{d_{n+1}}) \leq D \prod_{j=1}^{n+1} d_j$.

En esta misma Sección daremos una variante del Lema de Normalización de Noether a través de combinaciones lineales de coordenadas definidas por matrices triangulares superiores con unos en la diagonal principal (ver Lema 1.2.4).

Seguidamente, en la Sección 1.3, pasaremos a enunciar y probar con detalle el Nullstellensatz Efectivo de Jelonek *en el caso sub-determinado*. Aquí, el término sub-determinado hace referencia a que disponemos de, como mucho, tantas ecuaciones como la dimensión del espacio en el que viven las soluciones. En el caso genérico, es decir, con los coeficientes en un abierto Zariski, una sucesión $f_1, \ldots, f_k$ de $k \leq n$ polinomios definen una variedad de dimensión $n-k$ en $\mathbb{A}^n(\mathbb{K})$. Esta intuición se rompe en el caso afín para ciertas ecuaciones que viven en un cerrado-Zariski del espacio de coeficientes. Se necesitará $k = n+1$ para que genéricamente en los coeficientes, una sucesión $f_1, \ldots, f_{n+1}$ de ecuaciones defina la variedad vacía. El siguiente resultado hace referencia a la situación "sub-determinada" en la que $k \leq n$ ecuaciones carecen de cero en común.

Teorema 6 (**Nullstellensatz Efectivo, caso sub-determinado**). *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equi-dimensional afín de dimensión n y de grado D. Sean $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios no nulos con $k \leq m$. Sea $\deg f_i = d_i$ y $d_1 \geq \cdots \geq d_k$, $1 \leq i \leq k$. Si $V_{\mathbb{A}}(f_1, \ldots, f_k) \cap V = \emptyset$, entonces existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que:*

i) La siguiente identidad se verifica en $\mathbb{K}[V]$:

$$1 = \sum_{i=1}^{k} f_i g_i.$$

ii) Los grados de los productos $g_i f_i$ verifican la siguiente desigualdad, para cada $i \in \{1, \ldots, k\}$:

$$\deg(f_i g_i) \leq D \prod_{i=1}^{k} d_i.$$

Grosso modo, la contribución de Jelonek consiste en lo siguiente. Introducimos un parámetro de deformación, una nueva variable Z. Construimos un morfismo de la forma siguiente:

$$\begin{aligned} \Phi : V \times \mathbb{K} &\longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^k(\mathbb{K}) \\ (x, z) &\longmapsto (x, f_1(x)z, \ldots, f_k(x)z) \end{aligned}$$

Construimos una normalización de Noether apropiada dependiente de $\underline{x}$ y de los $f_i \cdot Z$. Llamemos $\Psi_1, \ldots, \Psi_{n+1}$ a los elementos de esa normalización de Noether. Consideramos la ecuación de dependencia entera de Z sobre $\mathbb{K}[\Psi_1, \ldots, \Psi_{n+1}]$ y acotemos su grado a través del Teorema de Perron Generalizado. Esa ecuación de dependencia entera tendrá la forma:

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = Z^\delta + \sum_{i=0}^{\delta-1} P_i(\Psi_1, \ldots, \Psi_{n+1}) Z^i \in I(V \times \mathbb{K}).$$

Reescribiendo esa ecuación en $\mathbb{K}[X_1, \ldots, X_m, Z]$ tomará la forma:

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = (1 + A_\delta) Z^\delta + \sum_{r \neq \delta} A_r Z^r.$$

Ahora, $P(\Psi_1, \ldots, \Psi_{n+1}, Z) = 0$ supera que los coeficientes de esta última expresión están en $I(V)$. Así concluimos

$$1 + A_\delta \in I(V).$$

Verificando que $A_\delta = \sum_{i=1}^{s} g_i \cdot f_i$ y que los grados de los $g_i \cdot f_i$ son los apropiados, Jelonek prueba su resultado. Verificar que todos los detalles son correctos (algunos aparecen de modo confuso, casi errado, en la prueba original) es la principal contribución de este Capítulo.

1.2. El Teorema de Perron Generalizado.

En esta Sección trataremos algunos resultados técnicos importantes para la prueba del Teorema fundamental de esta Memoria. Así, tras una sencilla caracterización de los polinomios multivariados libres de cuadrados y con coeficientes en un cuerpo algebraicamente cerrado (Lema 1.2.1), pasaremos a una generalización de un Teorema clásico de Perron, que caracteriza el grado de la imagen de una variedad irreducible por un morfismo finito (ver Teorema 1.2.3). La Sección incluye también una generalización y adaptación de producción propia del clásico Lema de Normalización de Noether, (ver Lema 1.2.4 para su uso en la demostración del principal Teorema de esta Memoria).

Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado, notación que usaremos a lo largo de toda la Sección. Por el clásico Lema de Gauss, el anillo de polinomios $\mathbb{K}[X_1, \ldots, X_m]$ es un dominio de factorización única. Un elemento $f \in \mathbb{K}[X_1, \ldots, X_m]$ se dice *libre de cuadrados (o reducido)* si no posee factores irreducibles en multiplicidad mayor que 1 o, equivalentemente, si admite una factorización única:

$$f = f_1 \cdots f_r,$$

donde cada $f_i \in \mathbb{K}[X_1, \ldots, X_m]$ es un polinomio irreducible y $gcd(f_i, f_j) = 1$ para cada $i \neq j$. De otro lado, dado $f \in \mathbb{K}[X_1, \ldots, X_m]$, podemos definir la aplicación polinomial gradiente

$$\begin{aligned} \nabla f : \mathbb{A}^m(\mathbb{K}) &\longrightarrow \mathbb{A}^m(\mathbb{K}) \\ x &\longmapsto \nabla_x f = \left(\frac{\partial f}{\partial X_1}(x), \ldots, \frac{\partial f}{\partial X_m}(x) \right). \end{aligned}$$

La condición de ser libre de cuadrados se relaciona con el comportamiento de la aplicación polinomial gradiente del modo siguiente. Nótese que $\mathbb{K}$ es algebraicamente cerrado de cualquier característica. En otro caso si $\mathbb{K}$ no fuera algebraicamente cerrado (o, por lo menos, perfecto) habría dificultades obvias por causa de la inseparabilidad en el caso de característica positiva.

Lema 1.2.1. *Con las notaciones precedentes, el polinomio f es libre de cuadrados si y solo si ∇f no es idénticamente nulo en cada componente irreducible de $V_{\mathbb{A}}(f)$.*

Demostración. Supongamos que f es libre de cuadrados. Tendrá una expresión en irreducibles:

$$f = f_1 \ldots f_r,$$

con f_i irreducible $\forall i \in \{1, \ldots, r\}$. La derivada de f con respecto a una variable X_j será:

$$\frac{\partial f}{\partial X_j} = \frac{\partial f_1}{\partial X_j} f_2 \ldots f_r + \cdots + f_1 \ldots f_{s-1} \frac{\partial f_s}{\partial X_j} f_{s+1} \ldots f_r + \cdots + f_1 \ldots f_{r-1} \frac{\partial f_r}{\partial X_j}.$$

Las componentes irreducibles de $V_{\mathbb{A}}(f)$ son precisamente $V_{\mathbb{A}}(f_i)$ $\forall i \in \{1, \ldots, r\}$. Por tanto, el gradiente en los puntos de una $V_{\mathbb{A}}(f_i)$ cualquiera es:

$$\nabla f = \left(\prod_{j \neq i} f_j \right) \nabla f_i = \left(\prod_{j \neq i} f_j \right) \left(\frac{\partial f_i}{\partial X_1}, \ldots, \frac{\partial f_i}{\partial X_n} \right),$$

pero, por la Proposición B.3.11, como los puntos lisos son densos y no vacíos en las variedades irreducibles, ∇f_i no se puede anular en todo $V_{\mathbb{A}}(f_i)$.
Por otra parte, si f no es libre de cuadrados, entonces se puede expresar como $f = g^2 h$ con g irreducible, y por tanto $\nabla f = g(2\nabla g h + g \nabla h)$ se anula en la componente irreducible $V_{\mathbb{A}}(g)$ de $V_{\mathbb{A}}(f)$. □

Corollario 1.2.2. *Sean $m_1, \ldots, m_m \in \mathbb{N}$ enteros positivos. Supongamos que se da una de las dos propiedades siguientes:*

- *O bien la característica de $\mathbb{K}$ es distinta de 2.*
- *O bien la característica de $\mathbb{K}$ es 2 pero $m_i \geq 2$, para cada i, $1 \leq i \leq m$.*

Sea $f \in \mathbb{K}[X_1, \ldots, X_m]$ un polinomio libre de cuadrados. Supongamos que la hipersuperficie que define $V_{\mathbb{A}}(f) \subseteq \mathbb{A}^m(\mathbb{K})$ no contiene a hiperplanos verticales de la forma $\{X_i = a_i\}$ para algún $i \in \{1, \ldots, m\}$ y para algún $a_i \in \mathbb{K}$.
Entonces, el polinomio $F(T_1, \ldots, T_m) := f(T_1^{m_1} + T_1, \ldots, T_n^{m_m} + T_m) \in \mathbb{K}[T_1, \ldots T_m]$ es también libre de cuadrados.

Demostración. Consideremos la siguiente aplicación polinomial:

$$\begin{aligned} \tau : \mathbb{A}^m(\mathbb{K}) &\longrightarrow \mathbb{A}^m(\mathbb{K}) \\ (t_1, \ldots, t_m) &\longmapsto (t_1^{m_1} + t_1, \ldots, t_m^{m_m} + t_m), \end{aligned}$$

y el correspondiente morfismo de $\mathbb{K}$-álgebras.

$$\begin{aligned} \tau^* : \mathbb{K}[X_1, \ldots, X_m] &\longrightarrow \mathbb{K}[T_1, \ldots, T_m] \\ X_i &\longmapsto T_i^{m_i} + T_i. \end{aligned}$$

Nótese que en el caso $caract(\mathbb{K}) = 2$, como $m_i \neq 1$ en este caso, τ no es constante en ninguna coordenada. Si $caract(\mathbb{K}) \neq 2$, incluso tomando $m_i = 1$, $2t_i$ no es constante porque 2 es unidad en $\mathbb{K}$.
Comencemos observando que, bajo nuestras hipótesis, la aplicación polinomial τ es suprayectiva. Como $\mathbb{K}$ es algebraicamente cerrado, dado $a \in \mathbb{K}$ un elemento cualquiera, el polinomio siguiente siempre posee raíces en $\mathbb{K}$:

$$P_a(T) := T^{m_i} + T - a.$$

Si $m_i \geq 2$ es claro que $P_a(T)$ es un polinomio no nulo que posee raíces en $\mathbb{K}$. Si la característica de $\mathbb{K}$ es distinta de 2, y si $m_i = 1$ entonces:

$$P_a(T) = T^{m_i} + T - a = T + T - a = 2T - a,$$

este polinomio también es el polinomio no nulo (2 es inversible en $\mathbb{K}$) y también posee una raíz en $\mathbb{K}$. El caso $m_i = 1$ y $caract(\mathbb{K}) = 2$ ha sido excluido intencionadamente en nuestro enunciado.
En particular, bajo las hipótesis del enunciado, dado $a \in \mathbb{K}$ y dado uno cualquiera de los m_i, siempre existe $z \in \mathbb{K}$ tal que:

$$z^{m_i} + z - a = 0.$$

Del mismo modo, dado $(a_1, \ldots, a_m) \in \mathbb{A}^m(\mathbb{K})$ existirán $(z_1, \ldots, z_m) \in \mathbb{A}^m(\mathbb{K})$ tales que:

$$z_i^{m_i} + z_i - a_i = 0, 1 \leq i \leq m.$$

En conclusión, τ es suprayectiva y, por tanto, τ^* es un monomorfismo de $\mathbb{K}$-álgebras. Además, podemos identificar $\mathbb{K}[X_1, \ldots, X_m]$ con un subanillo de $\mathbb{K}[T_1, \ldots, T_m]$. Adicionalmente, τ^* permite definir una extensión entera de anillos. Claramente, dado $T_i \in \mathbb{K}[T_1, \ldots, T_m]$ la siguiente es una ecuación de dependencia entera de T_i sobre $\mathbb{K}[X_1, \ldots, X_m]$ (identificado con $\tau^*(\mathbb{K}[X_1, \ldots, X_m])$):

$$T_i^{m_i} + T_i - \tau^*(X_i) = 0.$$

Es claro que si $caract(K) \neq 2$ y $m_i \in \mathbb{N}$, $m_i \geq 2$, esta es una ecuación de dependencia entera de grado m_i. Si $caract(K) \neq 2$ y $m_i = 1$, también es una ecuación de dependencia entera, porque $2 \in \mathbb{K}$ es no nulo en $\mathbb{K}$ y es unidad en $\mathbb{K}[X_1, \ldots, X_m]$. Si $caract(\mathbb{K}) = 2$ y $m_i \geq 2$, también es una ecuación de dependencia entera. Dado que $\{T_1, \ldots, T_m\}$ son elementos enteros sobre $\mathbb{K}[X_1, \ldots, X_m]$, la $\mathbb{K}$-álgebra finitamente generada que engendran (i.e. $\mathbb{K}[T_1, \ldots, T_m]$) es también una extensión entera de $\mathbb{K}[X_1, \ldots, X_m]$ (identificado con $\tau^*(\mathbb{K}[X_1, \ldots, X_m])$). Por la Proposición A.3.2, si $R \subseteq B$ es una extensión de anillos, $B = R[\alpha_1, \ldots, \alpha_r]$, R-álgebra finitamente generada, y $\{\alpha_1, \ldots, \alpha_r\}$ enteros sobre R, entonces B es entero sobre R. Por los Teoremas del Ascenso y Descenso de Krull-Cohen-Seidenberg (ver el Corolario A.3.9), dado que $\tau^* : \mathbb{K}[X_1, \ldots, X_m] \hookrightarrow \mathbb{K}[T_1, \ldots, T_m]$ es una extensión entera de anillos y ambos son dominios de factorización única, consideramos la propiedad siguiente: Para cada ideal primo $\mathfrak{p} \in Spec(\mathbb{K}[T_1, \ldots, T_m])$, sean $\mathfrak{p}^c = (\tau^*)^{-1}(\mathfrak{p}) \in Spec(\mathbb{K}[X_1, \ldots, X_m])$ su contracción a $\mathbb{K}[X_1, \ldots, X_m]$. Entonces, las alturas y coalturas satisfacen

$$ht(\mathfrak{p}) = ht(\mathfrak{p}^c),$$

$$coht(\mathfrak{p}) = coht(\mathfrak{p}^c).$$

Recordemos, además, que si $V \subseteq \mathbb{A}^n(\mathbb{K})$ es una variedad irreducible, $\varphi : \mathbb{A}^n(\mathbb{K}) \longrightarrow \mathbb{A}^m(\mathbb{K})$ una aplicación polinomial, $\varphi^* : \mathbb{K}[Y_1, \ldots, Y_m] \longrightarrow \mathbb{K}[X_1, \ldots, X_n]$ el morfismo de $\mathbb{K}$-álgebras asociado y $\mathfrak{p} = I(V)$ el ideal primo asociado a V, entonces, si $\mathcal{W} = \overline{\varphi(V)}^z$ es la clausura Zariski de la imagen de V por φ se tiene que:

$$I(\mathcal{W}) = \mathfrak{p}^c.$$

Por tanto, consideremos $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad irreducible, y sea $\mathcal{W} = \overline{\tau(V)}^z$ la clausura Zariski de la imagen por τ de V. Se tiene:

$$\dim(V) = \dim(\mathbb{K}[V]) = coht(\mathfrak{p}) = coht(\mathfrak{p}^c) = \dim(\mathbb{K}[\mathcal{W}]) = \dim(\mathcal{W}).$$

Es decir, para el morfismo τ definido al comienzo de esta prueba y para cualquier variedad algebraica irreducible $V \subseteq \mathbb{A}^m(\mathbb{K})$ se tiene que

$$\dim(V) = \dim(\overline{\tau(V)}^z).$$

Consideremos ahora el polinomio $F(T_1,\ldots,T_m)=f(T_1^{m_1}+T_1,\ldots,T_m^{m_m}+T_m)$ del enunciado. Observemos que:

$$F=\tau^*(f)=(f\circ\tau)(T_1,\ldots,T_m).$$

Como $f\in\mathbb{K}[X_1,\ldots,X_m]$ es no nulo y τ^* es monomorfismo en nuestras condiciones, entonces $F\neq 0$ es un polinomio no nulo. En particular, $V_{\mathbb{A}}(F)\subseteq\mathbb{A}^m(\mathbb{K})$ es una hiper-superficie no trivial. Por el Teorema del Ideal Principal de Krull (ver Teorema A.2.5), $V_{\mathbb{A}}(F)$ es de dimensión $m-1$ y todas sus componentes irreducibles son de dimensión $m-1$. En particular, por lo visto anteriormente, si $V\subseteq V_{\mathbb{A}}(F)$ es una componente irreducible de $V_{\mathbb{A}}(F)$, se tiene que:

$$m-1=\dim(V)=\dim(\overline{\tau(V)}^z),$$

además, por el Lema 1.2.1 anterior, $\overline{\tau(V)}^z$ es una variedad algebraica irreducible. Adicionalmente, tenemos la siguiente igualdad

$$V_{\mathbb{A}}(F)=\{(t_1,\ldots,t_m)\in\mathbb{A}^m(\mathbb{K}):\tau(t_1,\ldots,t_m)\in V_{\mathbb{A}}(f)\}=\tau^{-1}(V_{\mathbb{A}}(f)).$$

De otro lado, como τ es suprayectivo, tenemos que

$$\tau(V_{\mathbb{A}}(F))=V_{\mathbb{A}}(f).$$

En particular, consideremos que si $V\subseteq V_{\mathbb{A}}(F)$ es una componente irreducible de $V_{\mathbb{A}}(F)\subseteq\mathbb{A}^m(\mathbb{K})$, entonces $\overline{\tau(V)}^z\subseteq V_{\mathbb{A}}(f)$ es una variedad algebraica irreducible. Además, de nuevo por el Teorema del Ideal Principal de Krull, las componentes irreducibles de $V_{\mathbb{A}}(f)$ son todas de dimensión $m-1$. Esto significa que si $V\subseteq V_{\mathbb{A}}(F)$ es una componente irreducible, entonces $\overline{\tau(V)}^z\subseteq V_{\mathbb{A}}(f)$ es una componente irreducible de $V_{\mathbb{A}}(f)$. Tenemos así una aplicación bien definida:

$$\{V\subseteq V_{\mathbb{A}}(F):V\text{es irreducible},\dim(V)=m-1\}\longrightarrow\{\mathcal{W}\subseteq V_{\mathbb{A}}(f):\mathcal{W}\text{ irreducible},\dim(\mathcal{W})=m-1\}$$
$$V\longmapsto\overline{\tau(V)}^z.$$

Consideremos ahora $i\in\{1,\ldots,m\}$ y el polinomio:

$$\frac{\partial(T_i^{m_i}+T_i)}{\partial T_i}=m_iT_i^{m_i-1}+1\in\mathbb{K}[T_1,\ldots,T_m].$$

El polinomio $m_iT_i^{m_i-1}+1$ no se anula idénticamente en ninguna componente irreducible de $V_{\mathbb{A}}(F)$. Para probar esta afirmación, procedemos por reducción al absurdo. Supongamos que existe $V\subseteq V_{\mathbb{A}}(F)$ una componente irreducible de $V_{\mathbb{A}}(F)$ sobre la que se anula idénticamente el polinomio $m_iT_i^{m_i-1}+1$. Por nuestra elección de $m_1,\ldots,m_m$, en cualquier caso éste es un polinomio univariado no nulo con coeficientes en un cuerpo algebraicamente cerrado $\mathbb{K}$. Entonces, se descompone completamente en $\mathbb{K}$, es decir, existen $\{z_{i,1},\ldots,z_{i,m_i-1}\}\subseteq\mathbb{K}$ no necesariamente todos distintos tales que:

$$m_iT_i^{m_i-1}+1=m_i\cdot\prod_{k=1}^{m_i-1}(T_i-z_{i,k}),$$

como $m_iT_i^{m_i-1}+1$ se anula idénticamente en V, entonces,

$$V\subseteq V_{\mathbb{A}}(m_iT_i^{m_1-1}+1)=\bigcup_{k=1}^{m_i-1}V_{\mathbb{A}}((T_i-z_{i,k})).$$

Como V es irreducible, existiría $k_0\in\{1,\ldots,m_i-1\}$ tal que

$$V\subseteq V_{\mathbb{A}}((T_i-z_{i,k_0})).$$

Entonces, sea $a_i=z_{i,k_0}^{m_i}+z_{i,k_0}\in\mathbb{K}$ y tendríamos que

$$\tau(V)\subseteq\tau(V_{\mathbb{A}}((T_i-z_{i,k_0})))=V_{\mathbb{A}}((X_i-a_i)).$$

Por tanto, $\overline{\tau(V)}^z\subseteq V_{\mathbb{A}}((X_i-a_i))$. Pero como $\overline{\tau(V)}^z$ es una componente irreducible de $V_{\mathbb{A}}(f)$, habríamos llegado a contradicción con una de las hipótesis de nuestro enunciado.

Consideremos ahora la aplicación polinomial $\nabla F:\mathbb{A}^m(\mathbb{K})\longrightarrow\mathbb{A}^m(\mathbb{K})$ y supongamos que existe una componente irreducible $V\subseteq V_{\mathbb{A}}(F)$ sobre la que este gradiente se anula completamente. Escribamos $\tau=(\tau_1,\ldots,\tau_m)$ donde

$$\tau_i=T_i^{m_i}+T_i,1\leq i\leq m.$$

Observemos que

$$\frac{\partial \tau_i}{\partial T_k} = \begin{cases} \text{si } i \neq k & 0 \\ \text{si } i = k & m_k T_k^{m_k - 1} + 1. \end{cases}$$

Además, se tiene la siguiente igualdad para cada $z \in \mathbb{A}^m(\mathbb{K})$

$$\frac{\partial F}{\partial T_i}(z) = \sum_{k=1}^{n} \frac{\partial f}{\partial X_k}(\tau(z)) \cdot \frac{\partial \tau_k}{\partial T_i}(z).$$

Luego

$$\frac{\partial F}{\partial T_i}(z) = \frac{\partial f}{\partial X_i}(\tau(z)) \cdot \frac{\partial \tau_i}{\partial T_i}(z) = \frac{\partial f}{\partial X_i}(\tau(z)) \cdot (m_i T_i^{m_i - 1} + 1),$$

donde $z = (z_1, \ldots, z_m)$. En forma matricial, tenemos $\forall z \in \mathbb{A}^m(\mathbb{K})$:

$$\begin{pmatrix} \frac{\partial F}{\partial T_1}(z) \\ \vdots \\ \frac{\partial F}{\partial T_m}(z) \end{pmatrix} = \begin{pmatrix} m_1 z_1^{m_1 - 1} + 1 & 0 & \cdots & 0 \\ & m_2 z_2^{m_2 - 1} + 1 & & \\ & & \ddots & \vdots \\ 0 & & & m_m z_m^{m_m - 1} + 1 \end{pmatrix} \begin{pmatrix} \frac{\partial f}{\partial X_1}(\tau(z)) \\ \vdots \\ \frac{\partial f}{\partial X_m}(\tau(z)) \end{pmatrix}, \tag{1.2.1}$$

Hemos visto que existe un abierto Zariski $\mathcal{U} \subseteq V$ en el que $\forall z = (z_1, \ldots, z_m) \in \mathcal{U}$ se tiene:

$$m_i \cdot z_i^{m_i - 1} + 1 \neq 0.$$

En particular, para cada $z = (z_1, \ldots, z_m) \in \mathcal{U}$, la matriz de coeficientes del sistema de ecuaciones lineales 1.2.1 es una matriz no singular. Como $\mathcal{U} \subseteq V$ y ∇F se anula idénticamente en V, a partir de 1.2.1 tendremos que $\forall z = (z_1, \ldots, z_m) \in \mathcal{U}$ se verifica el siguiente sistema de ecuaciones lineales homogéneo:

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} m_1 z_1^{m_1 - 1} + 1 & 0 & \cdots & 0 \\ & m_2 z_2^{m_2 - 1} + 1 & & \\ & & \ddots & \vdots \\ 0 & & & m_m z_m^{m_m - 1} + 1 \end{pmatrix} \begin{pmatrix} \frac{\partial f}{\partial X_1}(\tau(z)) \\ \vdots \\ \frac{\partial f}{\partial X_m}(\tau(z)) \end{pmatrix}. \tag{1.2.2}$$

Como la matriz diagonal de coeficientes tiene rango n, concluiremos que para todo $z \in \mathcal{U}$:

$$\nabla_{\tau(z)} f = \left(\frac{\partial f}{\partial X_i}(\tau(z)), \ldots, \frac{\partial f}{\partial X_m}(\tau(z)) \right) = (0, \ldots, 0).$$

Por tanto, habremos concluido que ∇f se anula completamente en $\tau(\mathcal{U})$, con $\mathcal{U}$ abierto Zariski no vacío de V. Por tanto, ∇f se anula completamente en la clausura Zariski $\overline{\tau(\mathcal{U})}^z$ de la imagen $\tau(\mathcal{U})$. Como V es irreducible, $\overline{\mathcal{U}}^z = V$ y como τ es continua para la topología de Zariski, tendremos que $\tau(\overline{\mathcal{U}}^z) \subseteq \overline{\tau(\mathcal{U})}^z$ luego

$$\overline{\tau(V)}^z = \overline{\tau(\overline{\mathcal{U}}^z)}^z \subseteq \overline{\overline{\tau(\mathcal{U})}^z}^z = \overline{\tau(\mathcal{U})}^z.$$

En conclusión, ∇f se anula en $\overline{\tau(V)}^z$. Por lo probado anteriormente, $\overline{\tau(V)}^z$ es una componente irreducible de $V_{\mathbb{A}}(f)$. Habríamos probado así que ∇f se anule en alguna componente irreducible de $V_{\mathbb{A}}(f)$. Usando el Lema 1.2.1, esto contradice la hipótesis de que f es un polinomio libre de cuadrados. En conclusión, ∇F no se anula completamente en ninguna componente irreducible de $V_{\mathbb{A}}(F)$ y, por tanto, F es un polinomio libre de cuadrados.

□

Teorema 1.2.3 (**Teorema de Perron Generalizado**). *Sean $Q_1, \ldots, Q_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios no constantes con $\deg Q_i = d_i$. Sea $V \subset \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equidimensional afín de dimensión n y grado D. Si la aplicación $Q = (Q_1, \ldots, Q_{n+1}) : V \longrightarrow \mathbb{A}^{n+1}(\mathbb{K})$ es genéricamente finita, entonces existe un polinomio no nulo $W(T_1, \ldots, T_{n+1}) \in \mathbb{K}[T_1, \ldots, T_{n+1}]$ tal que:*

i) $W(Q_1, \ldots, Q_{n+1}) = 0$ *en* V.
ii) $\deg W(T_1^{d_1}, T_2^{d_2}, \ldots, T_{n+1}^{d_n+1}) \leq D \prod_{j=1}^{n+1} d_j$.

Demostración. Sin pérdida de generalidad, supongamos que el cuerpo $\mathbb{K}$ es algebraicamente cerrado y que V es irreducible. Sea el morfismo $Q : V \longrightarrow \mathbb{A}^{n+1}(\mathbb{K})$. Sea $Q(V)$ la imagen de V y $\mathcal{Z} = \overline{Q(V)}^z$ su clausura Zariski. Una simple comprobación muestra que como V es irreducible, $\mathcal{Z}$ es una variedad irreducible también. Por definición de $\mathcal{Z}$, $Q : V \longrightarrow \mathcal{Z}$ es dominante. Además, por ser genéricamente finita existe un abierto Zariski $\mathcal{U} \subseteq \mathcal{Z}$ tal que $\mathcal{U}$ es denso Zariski en $\mathcal{Z}$, $\mathcal{U} \subseteq Q(V)$ y para cada $z \in \mathcal{U}$ la fibra $Q^{-1}(\{z\})$ es cero-dimensional (i.e. un conjunto finito de puntos). Por el Teorema de la Dimensión de la Fibra (véase Teorema B.1.6), existe $\mathcal{U}' \subseteq \mathcal{Z}$ otro abierto Zariski tal que $\forall z' \in \mathcal{U}'$, se satisface la siguiente igualdad:

$$\dim Q^{-1}(\{z'\}) = \dim(V) - \dim(\mathcal{Z}).$$

Como $\mathcal{Z}$ es irreducible, $V = \mathcal{U} \cap \mathcal{U}' \neq \emptyset$ y por tanto, $\forall z \in V$ se tiene:

$$0 = \dim Q^{-1}(\{z\}) = \dim(V) - \dim(\mathcal{Z}),$$

y por tanto, $\mathcal{Z}$ es irreducible y de dimensión igual a la dimensión de V. Además, $\dim(V) = n$, luego, por el Teorema del Ideal Principal de Krull (véase Teorema A.2.5), $\mathcal{Z}$ es una hipersuperficie irreducible en $\mathcal{A}^{n+1}(\mathbb{K})$. Por tanto, $I(\mathcal{Z})$ es un ideal principal generado por un polinomio $w \in \mathbb{K}[Z_1, \ldots, Z_{n+1}]$ que, necesariamente, es irreducible en $\mathbb{K}[Z_1, \ldots, Z_{n+1}]$.
Por el Corolario 1.2.2 precedente el siguiente polinomio p es irreducible en $\mathbb{K}[T_1, \ldots, T_{n+1}]$:

$$p(T_1, \ldots T_{n+1}) = w(T_1^{d_1} + T_1, \ldots, T_{n+1}^{d_{n+1}} + T_{n+1}) \in \mathbb{K}[T_1, \ldots T_{n+1}].$$

Consideremos $W \subseteq \mathbb{A}^{n+1}(\mathbb{K})$ la hipersuperficie de los ceros de p:

$$W = V_{\mathbb{A}}(p) = \{w \in \mathbb{A}^{n+1}(\mathbb{K}) : p(w) = 0\}.$$

De nuevo, W es una hipersuperficie (i.e. de dimensión n) en $\mathbb{A}^{n+1}(\mathbb{K})$. Consideremos $\widetilde{\mathcal{Z}} \subseteq \mathbb{A}^{n+1}(\mathbb{K}) \times \mathbb{A}^{n+1}(\mathbb{K})$ la siguiente variedad algebraica:

$$\widetilde{\mathcal{Z}} = \{(z, w) \in \mathbb{A}^{n+1}(\mathbb{K}) \times \mathbb{A}^{n+1}(\mathbb{K}) : z_i = w_i^{d_i} + w_i, 1 \leq i \leq n+1, z \in \mathcal{Z}\},$$

y consideremos la proyección canónica

$$\begin{aligned} \pi_1 : \mathbb{A}^{n+1}(\mathbb{K}) \times \mathbb{A}^{n+1}(\mathbb{K}) &\longrightarrow \mathbb{A}^{n+1}(\mathbb{K}). \\ (z, w) &\longmapsto w. \end{aligned}$$

Veamos que $\pi_1(\widetilde{\mathcal{Z}}) = W$. Claramente, si $(z, w) = (z_1, \ldots, z_{n+1}, w_1, \ldots, w_{n+1}) \in \widetilde{\mathcal{Z}}$. Tenemos las siguientes ecuaciones:

$$\begin{aligned} w(z_1, \ldots, z_{n+1}) &= 0, \\ z_i &= w_i^{d_i} + w_i, \forall\ 1 \leq i \leq n+1. \end{aligned}$$

Por tanto $w(w_1^{d_1} + w_1, \ldots, w_{n+1}^{d_{n+1}} + w_{n+1}) = p(w_1, \ldots, w_{n+1}) = 0$ y habremos concluido que $\pi_1(\widetilde{\mathcal{Z}}) \subseteq W$.
Por otro lado, sea $w = (w_1, \ldots, w_{n+1}) \in W$ un punto cualquiera. Definimos los siguientes puntos:

$$z_i := w_i^{d_i} + w_i \in \mathbb{K}, 1 \leq i \leq n+1.$$

Como $p(w_1, \ldots, w_{n+1}) = 0$ entonces $w(z_1, \ldots, z_{n+1}) = 0$ y $z = (z_1, \ldots, z_{n+1}) \in \mathcal{Z}$, con lo que concluimos que $\exists (z, w) \in \widetilde{\mathcal{Z}}$ tal que $\pi_1(z, w) = w$ y habremos concluido $\pi_1(\widetilde{\mathcal{Z}}) = W$.
Definimos finalmente la variedad algebraica

$$\widetilde{V} := \{(u, w) \in \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^{n+1}(\mathbb{K}) : u \in V, (Q(u), w) \in \widetilde{\mathcal{Z}})\}.$$

Como $Q : V \longrightarrow \mathcal{Z}$ era dominante, entonces también es dominante

$$\begin{aligned} \widetilde{Q} : \widetilde{V} &\longrightarrow \widetilde{\mathcal{Z}} \\ (u, w) &\longmapsto (Q(u), w). \end{aligned}$$

Como π_1 es suprayectiva sobre W, tenemos un morfismo dominante:

$$\begin{aligned} \pi := \pi_1 \circ \widetilde{Q} : \widetilde{V} &\longrightarrow W \\ (u, w) &\longmapsto w. \end{aligned}$$

Además π es una proyección lineal, por la Proposición B.2.7 tendremos que

$$\deg(W) = \deg(\overline{\pi(\widetilde{V})}^z) \leq \deg(\widetilde{V}).$$

Por la Desigualdad de Bézout (cf. Teorema B.2.9), tenemos que:

$$\deg(\widetilde{V}) \leq \deg(V) \left(\prod_{i=1}^{n+1} d_i \right).$$

Como W es una hipersuperficie, por la Proposición B.2.4, su polinomio mínimo (en este caso el polinomio p) verifica que el grado geométrico de Y coincide con el de p, es decir,

$$\deg(W) = \deg(p).$$

En conclusión, se tiene la siguiente desigualdad:

$$\deg(p) = \deg(Y) \leq \deg(\widetilde{V}) \leq D \left(\prod_{i=1}^{n+1} d_i \right).$$

□

El siguiente resultado muestra una versión con matriz triangular de la Normalización de Noether.

LEMA 1.2.4. *Sea $\mathfrak{a}$ un ideal no mezclado (i.e. todos sus primos asociados tienen la misma altura, ver Definición 11) en el anillo de polinomios $\mathbb{K}[X_1, \ldots, X_m]$. Entonces, existe una matriz B triangular superior de la forma siguiente:*

$$B = \begin{pmatrix} 1 & b_{1,2} & b_{1,3} & \ldots & b_{1,m} \\ & 1 & & & \\ & & \ddots & & \vdots \\ & \mathit{0} & & 1 & b_{m-1,m} \\ & & & & 1 \end{pmatrix} \in \mathscr{M}_m(\mathbb{K}),$$

tal que se verifican las siguientes propiedades:

i) Consideramos las formas lineales:

$$l_i := X_i + \sum_{k=i+1}^{m} b_{i,k} X_k,$$

y las clases que definen modulo $\mathfrak{a}$:

$$\bar{l}_i := l_i + \mathfrak{a} \in {}^{\mathbb{K}[X_1, \ldots, X_m]}\Big/_{\mathfrak{a}},\ 1, \leq i \leq m.$$

Si $k = coht(\mathfrak{a}) = \dim(\mathbb{K}[X_1, \ldots, X_m] / \mathfrak{a})$, entonces, las clases siguientes:

$$\{\bar{l}_1, \ldots, \bar{l}_k\},$$

son algebraicamente independientes sobre $\mathbb{K}$.

ii) La siguiente es una extensión entera de anillos:

$$\mathbb{K}[\bar{l}_1, \ldots, \bar{l}_k] \hookrightarrow {}^{\mathbb{K}[X_1, \ldots, X_m]}\Big/_{\mathfrak{a}}.$$

Más aún, si $V \in \mathbb{A}^m(\mathbb{K})$ es una variedad algebraica equi-dimensional afín, la proyección siguiente es un morfismo finito y suprayectivo:

$$\begin{aligned} \pi_A : V &\longrightarrow \mathbb{A}^k(\mathbb{K}) \\ (x_1, \ldots, x_m) &\longrightarrow (l_1(x_1, \ldots x_m), \ldots, l_k(x_1, \ldots, x_m)), \end{aligned}$$

donde $k = \dim(V)$ es la dimensión de Krull de V.

DEMOSTRACIÓN. Como $\mathbb{K}[X_1, \ldots, X_m]$ es un anillo catenario y $\mathfrak{a}$ es un anillo no mezclado, entonces $ht(\mathfrak{a}) + coht(\mathfrak{a}) = m$ (véase el Corolario A.4.9). Demostraremos el enunciado por inducción en la altura de $\mathfrak{a}$.
Para el caso $ht(\mathfrak{a}) = 1$, como el Lema de Gauss afirma que $\mathbb{K}[X_1, \ldots, X_m]$ es un dominio de factorización única y, además, es noetheriano, se tiene que todo ideal primo de altura 1 es principal (véase la Proposición A.2.6). Como $\mathfrak{a}$ es un ideal no mezclado de altura 1, tendrá una descomposición en ideales primarios como la siguiente:

$$\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_s,$$

con cada $\mathfrak{a}_i$ ideal $\mathfrak{p}_i$-primario cumpliendo que $coht(\mathfrak{p}_i) = coht(\mathfrak{a})$ y por tanto, en este caso, $ht(\mathfrak{p}_i) = 1$. Como en todo domino noetheriano se cumple que todo ideal $\mathfrak{p}$-primario, con $\mathfrak{p}$ principal, es principal (véase Lema A.2.7), se cumple por tanto que todo $\mathfrak{a}_i, 1 \leq i \leq s$ es principal, y por último, $\mathfrak{a}$ será principal y no nulo. Es decir, existe $f \in \mathbb{K}[X_1, \ldots, X_m]$ no nulo tal que $\mathfrak{a} = (f)$. Consideremos la descomposición en componentes homogéneas siguiente:

$$f = f_d(X_1, \ldots, X_m) + f_{d-1}(X_1, \ldots, X_m) + \cdots + f_0(X_1, \ldots, X_m),$$

donde $f_i \in \mathbb{K}[X_1, \ldots, X_m]$ es un polinomio homogéneo de grado i y, además, podemos suponer $f_d(X_1, \ldots, X_m) \neq 0$. Consideremos la matriz siguiente:

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 & -a_1 \\ & 1 & & & \\ & & \ddots & & \vdots \\ & 0 & & 1 & -a_{m-1} \\ & & & & 1 \end{pmatrix} \in \mathscr{M}_m(\mathbb{K}),$$

que es triangular superior con unos en la diagonal principal. Consideremos un nuevo conjunto de variables $\{Y_1, \ldots, Y_m\}$ dadas por el cambio lineal de coordenadas que representa A:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = A \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

En términos de ecuaciones, se están considerando las variables:

$$\begin{cases} Y_1 &= & X_1 - a_1 X_m \\ Y_2 &= & X_2 - a_2 X_m \\ & \vdots & \\ Y_{m-1} &= & X_{m-1} - a_{m-1} X_m \\ Y_m &= & X_m \end{cases}$$

y la inversa de la matriz A se obtiene despejando de las anteriores igualdades:

$$\begin{cases} X_1 &= & Y_1 + a_1 Y_m \\ X_2 &= & Y_2 + a_2 Y_m \\ & \vdots & \\ X_{m-1} &= & Y_{m-1} + a_{m-1} Y_m \\ X_m &= & Y_m \end{cases}$$

que, en términos de matrices, quiere decir que la matriz inversa de A es:

$$A^{-1} = \begin{pmatrix} 1 & 0 & \ldots & 0 & a_1 \\ & 1 & & & \\ & & \ddots & & \vdots \\ & 0 & & 1 & a_{m-1} \\ & & & & 1 \end{pmatrix} \in \mathscr{M}_m(\mathbb{K}),$$

Consideramos el cambio de variables determinado por la matriz A. Por tratarse de una matriz inversible, se trata de un isomorfismo de anillos y $\mathbb{K}$-álgebras:

$$\begin{aligned} \Phi : \mathbb{K}[X_1, \ldots, X_m] &\longrightarrow \mathbb{K}[Y_1, \ldots, Y_m] \\ g &\longmapsto g \circ A^{-1}. \end{aligned}$$

Consideremos ahora las componentes homogéneas $f_i, 0 \leq i \leq d$ del polinomio f. Supongamos que tienen la siguiente forma:

$$f_i(X_1, \ldots, X_m) = \sum_{|\mu|=i} a_\mu^{(i)} X_1^{\mu_1} \cdots X_m^{\mu_m}, \tag{1.2.3}$$

para cada $i, 0 \leq i \leq d$. Reemplazando las variables $\{X_1, \ldots, X_m\}$ por las $\{Y_1, \ldots, Y_m\}$ según la transformación que define A tendremos su imagen:

$$g_i := \Phi(f_i) = \sum_{|\mu|=i} a_\mu^{(i)} (Y_1 + a_1 Y_m)^{\mu_1} \cdots (Y_{m-1} + a_{m-1} Y_m)^{\mu_{m-1}} Y_m^{\mu_m},$$

que, desarrollando y reordenando, se llega a la expresión:

$$g_i = \sum_{|\mu|=i} a_\mu^{(i)} a_1^{\mu_1} \cdots a_{m-1}^{\mu_{m-1}} Y_m^{\mu_1+\cdots+\mu_m} + h_i(Y_1, \ldots, Y_m),$$

donde $h_i \in \mathbb{K}[Y_1, \ldots, Y_m]$ cumple $\deg_{Y_m} h_i \leq i-1$ (donde $\deg_{Y_m}$ es el grado con respecto a la variable Y_m). Como $|\mu| = i$, la identidad anterior queda:

$$g_i = \left(\sum_{|\mu|=i} a_\mu^{(i)} a_1^{\mu_1} \cdots a_{m-1}^{\mu_{m-1}} \right) Y_m^i + h_i(Y_1, \ldots, Y_m).$$

Precisamente el coeficiente del término Y_m^i en la anterior expresión es, sustituyendo en la Expresión 1.2.3:

$$f_i(a_1, \ldots, a_{m-1}, 1) = \sum_{|\mu|=i} a_\mu^{(i)} a_1^{\mu_1} \cdots a_{m-1}^{\mu_{m-1}}.$$

Haciendo uso del isomorfismo Φ, se tiene:

$$g := \Phi(f) = \sum_{i=0}^{d} \Phi(f_i),$$

y como se ha visto que se cumple $\deg_{Y_m}(\Phi(f_i)) \leq i$, se tiene:

$$\Phi(f) = f_d(a_1, \ldots, a_{m-1}, 1) Y_m^d + H(Y_1, \ldots, Y_m),$$

donde

$$H(Y_1, \ldots, Y_m) := h_d(Y_1, \ldots, Y_m) + \sum_{i=0}^{d-1} \Phi(f_i),$$

es un polinomio de grado a lo sumo $d-1$ con respecto a la variable Y_m. Es decir, podemos escribir

$$\Phi(f) = f_d(a_1, \ldots, a_{m-1}, 1) Y_m^d + \sum_{i=0}^{d-1} F_i(Y_1, \ldots, Y_{m-1}) Y_m^i.$$

Se escoge un punto $(a_1, \ldots, a_{m-1}) \in \mathbb{A}^{m-1}(\mathbb{K})$ tal que $f_d(a_1, \ldots, a_{m-1}, 1) \neq 0$. Este punto existe porque el espacio afín es denso como subespacio del espacio proyectivo con la topología de Zariski. Por tanto, sea la expresión siguiente del polinomio homogéneo $f_d(X_1, \ldots, X_m)$:

$$f_d(X_1, \ldots, X_m) = \sum_{j=0}^{d} \tilde{f}_j(X_1, \ldots, X_{m-1}) X_m^j$$

donde $\deg(\tilde{f}_j) = d - j$. En caso de que $f_d(a_1, \ldots, a_{m-1}, 1) = 0$ para todo $(a_1, \ldots, a_{m-1}) \in \mathbb{A}^{m-1}(\mathbb{K})$, se tendría la siguiente igualdad:

$$f_d(X_1, \ldots, X_{m-1}, 1) = \sum_{j=0}^{d} \tilde{f}_j(X_1, \ldots, X_{m-1}) = 0$$

y como cada $\tilde{f}_j(X_1, \ldots, X_{m-1})$ tiene grado distinto, la anterior igualdad implica la siguiente:

$$\tilde{f}_j(X_1, \ldots, X_{m-1}) = 0 \; \forall j, \; 0 \leq j \leq d$$

y por tanto el polinomio $f_d(X_1, \ldots, X_m)$ sería el polinomio nulo, contradiciendo la hipótesis. Por tanto, sea $(a_1, \ldots, a_{m-1}) \in \mathbb{A}^{m-1}(\mathbb{K})$ tal que $f_d(a_1, \ldots, a_{m-1}, 1) \neq 0$. El polinomio siguiente define una ecuación de dependencia entera de Y_m sobre $\mathbb{K}[Y_1, \ldots, Y_{m-1}]$:

$$g(Y_1, \ldots, Y_m) = f_d(a_1, \ldots, a_m, 1) Y_m^d + \sum_{i=0}^{d-1} F_i(Y_1, \ldots Y_{m-1}) Y_m^i.$$

Nótese que la expresión anterior es mónica con respecto a la variable Y_m ($f_d(a_1,\dots,a_{m-1},1) \in \mathbb{K}\setminus\{0\}$). Equivalentemente, la siguiente extensión de anillos es entera:

$$\mathbb{K}[Y_1,\dots,Y_{m-1}] \hookrightarrow \mathbb{K}[Y_1,\dots,Y_{m-1}][Y_m] \cong \mathbb{K}[Y_1,\dots,Y_m],$$

Por otra parte, como la siguiente extensión es entera:

$$\mathbb{K}[Y_1,\dots,Y_m] \hookrightarrow \mathbb{K}[Y_1,\dots,Y_m]\Big/_{(g)},$$

y como $g=\Phi(f)$ y $\Phi(\mathfrak{a})=(\Phi(f))$, entonces se tiene una extensión entera de anillos:

$$\mathbb{K}[Y_1,\dots,Y_{m-1}] \hookrightarrow \mathbb{K}[Y_1,\dots,Y_m] \hookrightarrow \mathbb{K}[Y_1,\dots,Y_m]\Big/_{(g)} \cong \mathbb{K}[X_1,\dots,X_m]\Big/_{\mathfrak{a}}.$$

Sea $l_i = Y_i = X_i - a_iX_m, 1, \leq i \leq m-1$. Al ser $\{X_1,\dots,X_m\}$ algebraicamente independientes sobre $\mathbb{K}$, también lo son $\{X_1+\mathfrak{a},\dots,X_{m-1}+\mathfrak{a}\}$ y por estar ante una extensión entera (y por tanto algebraica) también $\{l_1+\mathfrak{a},\dots,l_{m-1}+\mathfrak{a}\}$. Para el paso inductivo, sea $\mathfrak{a}$ un ideal no mezclado con $ht(\mathfrak{a})\geq 2$. Como no es el ideal nulo, existe un polinomio $f\in\mathfrak{a}$ que no es ni nulo ni unidad. Por un razonamiento análogo al caso anterior, existen unas variables $\{Y_1,\dots,Y_m\}$ dadas por la matriz siguiente:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = A \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 & -a_1 \\ & 1 & & & \\ & & \ddots & & \vdots \\ & 0 & & 1 & -a_{m-1} \\ & & & & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix}, \tag{1.2.4}$$

tales que la siguiente es una extensión entera de anillos:

$$\mathbb{K}[Y_1,\dots,Y_{m-1}] \hookrightarrow \mathbb{K}[X_1,\dots,X_m]\Big/_{(f)}.$$

Consideremos ahora el ideal $\mathfrak{b} := \mathfrak{a}/(f)$ en $\mathbb{K}[X_1,\dots,X_m]/(f)$. Como $\mathbb{K}[X_1,\dots,X_m]$ es catenario, se cumple:

$$ht(\mathfrak{b}) = ht\left(\mathfrak{a}\Big/_{(f)}\right) = ht(\mathfrak{a}) - ht((f)),$$

y por el Teorema del Ideal principal de Krull (ver Teorema A.2.5), se tiene:

$$ht(\mathfrak{b}) = ht(\mathfrak{a}) - 1.$$

Sea la contracción $\mathfrak{b}^c = \mathfrak{b}\cap\mathbb{K}[Y_1,\dots,Y_{m-1}]$. Por los Teoremas Going-up y Going-Down de Krull-Cohen-Seidenberg (ver Corolario A.3.9) se tiene:

$$ht(\mathfrak{b}^c) = ht(\mathfrak{b}) = ht(\mathfrak{a}) - 1.$$

Como $\mathfrak{b}$ es no mezclado, $\mathfrak{b}^c$ también lo es. Aplicando la hipótesis inductiva, existirá una matriz del tipo siguiente:

$$B = \begin{pmatrix} 1 & b_{1,2} & b_{1,3} & \dots & b_{1,m-1} \\ & 1 & & & \\ & & \ddots & & \vdots \\ & 0 & & 1 & b_{m-2,m-1} \\ & & & & 1 \end{pmatrix} \in \mathscr{M}_{m-1}(\mathbb{K}),$$

tal que considerando las nuevas variables:

$$\begin{pmatrix} Z_1 \\ \vdots \\ Z_{m-1} \end{pmatrix} = B \begin{pmatrix} Y_1 \\ \vdots \\ Y_{m-1} \end{pmatrix}, \tag{1.2.5}$$

se tiene una extensión entera de anillos, siendo el primero un anillo de polinomios en las variables $\{Z_1,\dots,Z_r\}$ algebraicamente independientes sobre $\mathbb{K}$:

$$\mathbb{K}[Z_1,\dots,Z_r] \hookrightarrow \mathbb{K}[Y_1,\dots,Y_{m-1}]\Big/_{\mathfrak{b}^c},$$

donde r es la dimensión del anillo cociente $\mathbb{K}[Y_1,\ldots,Y_{m-1}]\,/\,\mathfrak{b}^c$. Además, por el segundo teorema de Isomorfía se tiene:

$$\mathbb{K}[X_1,\ldots,X_m]\Big/_{(f)}\Big/_{\mathfrak{b}} \cong \mathbb{K}[X_1,\ldots,X_m]\Big/_{(f)}\Big/_{\mathfrak{a}}\Big/_{(f)} \cong \mathbb{K}[X_1,\ldots,X_m]\Big/_{\mathfrak{a}}.$$

Por propiedades de las extensiones enteras (Proposición A.3.2), la siguiente extensión es entera: (1.2.6)

$$i : \mathbb{K}[Z_1,\ldots,Z_r] \hookrightarrow \mathbb{K}[Y_1,\ldots,Y_{m-1}]\Big/_{\mathfrak{b}^c} \hookrightarrow \mathbb{K}[X_1,\ldots,X_m]\Big/_{(f)}\Big/_{\mathfrak{b}^c} \cong \mathbb{K}[X_1,\ldots,X_m]\Big/_{\mathfrak{a}}.$$

Como la composición de extensiones enteras es entera, la extensión $i : \mathbb{K}[Z_1,\ldots,Z_r] \hookrightarrow \mathbb{K}[X_1,\ldots,X_m]\,/\,\mathfrak{a}$ es entera y como $r = \dim \mathbb{K}[Y_1,\ldots,Y_{m-1}]\,/\,\mathfrak{b}^c$, y por las propiedades de las extensiones enteras, se tiene la siguiente igualdad:

$$\dim \mathbb{K}[Y_1,\ldots,Y_{m-1}] = \dim \mathbb{K}[X_1,\ldots,X_m]\Big/_{(f)},$$

y por tanto, se tiene:

$$\dim \mathbb{K}[Y_1,\ldots,Y_{m-1}]\Big/_{\mathfrak{b}^c} = \dim \mathbb{K}[X_1,\ldots,X_m]\Big/_{(f)}\Big/_{\mathfrak{b}^c},$$

y por tanto, se concluye que $r = coht(\mathfrak{a}) = \dim\left(\mathbb{K}[X_1,\ldots,X_m]\,/\,\mathfrak{a}\right)$.
Por último, combinando las matrices de las expresiones 1.2.4 y 1.2.5, la extensión i se expresa en forma matricial:

$$\begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix} = \left(\begin{array}{c|c} B & 0 \\ \hline 0 & Id \end{array}\right) A \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} = C \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix},$$

y como A y $\left(\begin{array}{c|c} B & 0 \\ \hline 0 & Id \end{array}\right)$ son matrices triangulares superiores con unos en la diagonal principal, el producto C también. De nuevo, escogiendo las formas lineales l_i según esta matriz, se tienen las propiedades $i)$ y $ii)$.
Para la última interpretación geométrica, sean la matriz C:

$$C = \begin{pmatrix} 1 & c_{1,2} & c_{1,3} & \cdots & c_{1,m} \\ & 1 & & & \\ & & \ddots & & \vdots \\ & 0 & & 1 & c_{m-1,m} \\ & & & & 1 \end{pmatrix},$$

y las formas lineales $l_i := X_i + \sum_{j=i+1}^{m} c_{i,j}X_j$ obtenidas de aplicar el teorema al ideal $\mathfrak{a} := I(V)$, que por ser V equi-dimensional, es no mezclado (Proposición A.2.4). Definimos la proyección:

$$\begin{aligned} \pi : V &\longrightarrow \mathbb{A}^r(\mathbb{K}) \\ (x_1,\ldots,x_m) &\mapsto (l_1(x_1,\ldots,x_m),\ldots,l_r(x_1,\ldots,x_m)). \end{aligned}$$

Es claro que la transformación asociada entre las respectivas $\mathbb{K}$-álgebras:

$$\pi^* : \mathbb{K}[\mathbb{A}^r(\mathbb{K})] \cong \mathbb{K}[Z_1,\ldots,Z_r] \longrightarrow \mathbb{K}[V] \cong \mathbb{K}[X_1,\ldots,X_m]\Big/_{I(V)},$$

es precisamente la inclusión i de la expresión 1.2.6. Por tanto $\pi^* = i$ define una extensión entera de anillos, o equivalentemente, π es un morfismo finito suprayectivo. □

1.3. El Nullstellensatz de Jelonek en el caso sub-determinado.

Siguiendo una tradición terminológica no siempre bien aceptada, trataremos en esta sección de probar el Nullstellensatz efectivo de Jelonek en el caso subdeterminado. El caso "subdeterminado" hace referencia al caso en el que se discuten propiedades de una familia $\{f_1,\ldots,f_k\}$ de funciones definidas en un espacio de dimensión n con $k \leq n$. En este caso, la adaptación es imprecisa pero ilustrativa: dispondremos de un número de ecuaciones k, con k menor que la dimensión del espacio ambiente n, y que de modo no genérico, carecen de un cero en común. Lo usual (y genérico) es el caso $k = n+1$ para, genéricamente, no tener ceros comunes.

LEMA 1.3.1. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equi-dimensional afín. Sea $I(V)$ el ideal asociado, y sea $I(V \times \mathbb{K}) \subseteq \mathbb{K}[X_1, \dots X_m, Z]$, donde Z es una nueva variable, algebraicamente independiente de $\{X_1, \dots, X_m\}$. Dada la inclusión de anillos siguiente:*

$$\mathbb{K}[X_1, \dots, X_m] \hookrightarrow \mathbb{K}[X_1, \dots, X_m, Z],$$

sea $I(V)^e$ la extensión a $\mathbb{K}[X_1, \dots, X_m, Z]$ del ideal $I(V) \subseteq \mathbb{K}[X_1, \dots, X_m]$. Entonces, se tiene:

$$I(V)^e = I(V \times \mathbb{K}).$$

Más aún, con la identificación $\mathbb{K}[X_1, \dots, X_m, Z] = \mathbb{K}[X_1, \dots, X_m][Z]$ se tiene un isomorfismo natural de $\mathbb{K}$-álgebras como el siguiente:

$$\mathbb{K}[V \times \mathbb{K}] = \mathbb{K}[X_1, \dots X_m][Z] \Big/ I(V \times \mathbb{K}) \longrightarrow \mathbb{K}[V][Z],$$

$$\sum_{i=0}^{\delta} P_i(X_1, \dots, X_m) Z^i + I(V \times \mathbb{K}) \longmapsto \sum_{i=0}^{\delta} (P_i + I(V)) Z^i,$$

donde $\mathbb{K}[V] = \mathbb{K}[X_1, \dots, X_m] / I(V)$ es el anillo de funciones polinomiales definidas en V.

DEMOSTRACIÓN. Sea $P \in \mathbb{K}[X_1, \dots, X_m, Z]$ un polinomio cualquiera. Supongamos que su expresión como polinomio en $\mathbb{K}[X_1, \dots, X_m][Z]$ es dada por la siguiente expresión:

$$P = \sum_{i=0}^{\delta} P_i(X_1, \dots, X_m) Z^i, \ P_i(X_1, \dots, X_m) \in \mathbb{K}[X_1, \dots, X_m]. \tag{1.3.1}$$

Probemos que las afirmaciones siguientes son equivalentes:

i) $P(X_1, \dots, X_m, Z) \in I(V \times \mathbb{K})$.
ii) $P_i(X_1, \dots, X_m) \in I(V)$ para cada $i \in \{0, \dots, \delta\}$.

Si $f(X_1, \dots, X_m) \in I(V)$ es un polinomio dependiente solamente de las variables $\{X_1, \dots, X_m\}$, que se anula en V, entonces se cumple:

$$f(x_1, \dots, x_m, z) = f(x_1, \dots, x_m) = 0, \ \forall (x_1, \dots, x_m) \in V, \forall z \in \mathbb{K}.$$

Luego $I(V) \subseteq I(V \times \mathbb{K})$ y por definición de la extensión de un ideal, se tiene que $I(V)^e \subseteq I(V \times \mathbb{K})$. En particular, si $P \in \mathbb{K}[X_1, \dots, X_m, Z]$ es dado por la expresión:

$$P = \sum_{i=0}^{\delta} P_i(X_1, \dots, X_m) Z^i,$$

y si $P_i \in I(V)$ para cada $i \in \{1, \dots, \delta\}$, entonces, $P_i \in I(V)^e$ y $P_i(X_1, \dots, X_m) Z^i \in I(V)^e \subseteq I(V \times \mathbb{K})$ para todo $i \in \{1, \dots, \delta\}$. Por tanto, la suma $P = \sum_{i=0}^{\delta} P_i(X_1, \dots, X_m) Z^i \in I(V)^e \subseteq I(V \times \mathbb{K})$. Para la otra implicación, se hace uso de que $\mathbb{K}$ es un cuerpo infinito. Supongamos que el grado con respecto a la variable Z de P está acotado por δ debido a la expresión 1.3.1. Sea ahora $\{z_1, \dots, z_{\delta+1}\} \subseteq \mathbb{K}$ una familia de $\delta + 1$ puntos distintos de $\mathbb{K}$, que existen por tener cardinal infinito. Sea $x \in V$ un punto cualquiera y consideremos el polinomio:

$$P_x := P(x_1, \dots, x_m, Z) = \sum_{i=0}^{\delta} P_i(x_1, \dots, x_m) Z^i \in \mathbb{K}[Z].$$

Nótese que P_x es un polinomio univariado dependiente de Z, y con grado acotado por δ. Por construcción, los siguientes puntos son puntos de $V \times \mathbb{K}$:

$$\{(x, z_1), \dots, (x, z_{\delta+1})\} \subseteq V \times \mathbb{K}.$$

Como $P \in I(V \times \mathbb{K})$, se tiene que $P(x, z_i) = 0$, para cada $i \in \{1, \dots, \delta\}$. Entonces, $P_x(Z)$ verifica:

$$P_x(z_i) = P(x, z_i) = 0, \forall i \in \{1, \dots, \delta + 1\}.$$

Pero si un polinomio univariado de grado menor o igual que δ tiene $\delta + 1$ raíces distintas, debe ser el polinomio nulo, es decir, todos sus coeficientes son nulos. Como los coeficientes son precisamente los valores $P_i(x_1, \dots, x_m)$ y por tanto se ha probado la otra implicación. Por tanto, si $P = \sum_{i=0}^{\delta} P_i Z^i \in I(V \times \mathbb{K})$, entonces $P_i \in I(V)$, con lo que $P_i Z^i \in I(V)^e$ y concluimos que $P \in I(V)^e$. En conclusión, la equivalencia anterior significa $I(V \times \mathbb{K}) \subseteq I(V)^e$ y tenemos

la igualdad del enunciado. Para el isomorfismo, comencemos considerando la identificación siguiente:

$$\begin{aligned} i : \mathbb{K}[X_1, \ldots, X_m][Z] &\longrightarrow \mathbb{K}[X_1, \ldots, X_m, Z], \\ \sum_{i=0}^{\delta} P_i Z^i &\longmapsto \sum_{i=0}^{\delta} P_i(X_1, \ldots, X_m) Z^i, \end{aligned}$$

y consideramos la proyección canónica π sobre el anillo cociente siguiente:

$$\begin{aligned} \pi : \mathbb{K}[X_1, \ldots, X_m, Z] &\longrightarrow \mathbb{K}[V \times \mathbb{K}] \cong {\mathbb{K}[X_1, \ldots, X_m, Z]}\Big/{I(V \times \mathbb{K})} \\ P &\mapsto P + I(V \times \mathbb{K}). \end{aligned}$$

Consideremos la composición $\pi \circ i : \mathbb{K}[X_1, \ldots, X_m][Z] \longrightarrow \mathbb{K}[X_1, \ldots, X_m, Z] \,/\, I(V \times \mathbb{K})$. Como i es isomorfismo, entonces $\pi \circ i$ sigue siendo suprayectiva. Por la equivalencia demostrada, el núcleo son los polinomios $P \in \mathbb{K}[X_1, \ldots, X_m][Z]$ de la forma:

$$P = \sum_{i=0}^{\delta} P_i Z^i, P_i \in \mathbb{K}[X_1, \ldots, X_m],$$

de tal modo que $P \in I(V \times \mathbb{K})$. Por tanto, el núcleo de $\pi \circ i$ son los polinomios P de la forma precedente tales que $P_i \in I(V)$. En conclusión, por el Teorema de Isomorfía se tiene:

$$\mathbb{K}[V][Z] = \left({\mathbb{K}[X_1, \ldots, X_m]}\Big/{I(V)}\right)[Z] = {\mathbb{K}[X_1, \ldots, X_m, Z]}\Big/{\ker(\pi \circ i)} \cong \mathbb{K}[V \times \mathbb{K}].$$

□

LEMA 1.3.2. *Sean $k, n, m \in \mathbb{N}$ tres enteros positivos verificando $k \leq n \leq m$. Sea $\mu = (\mu_1, \ldots, \mu_{n+1}) \in \mathbb{N}^{n+1}$ un exponente monomial y sea $N = |\mu| = \mu_1 + \cdots + \mu_{n+1}$ su grado total.*
Sean $\{X_1, \ldots, X_m, Z\}$ un conjunto de $m+1$ variables algebraicamente independientes sobre $\mathbb{K}$. Sean $\{f_1, \ldots, f_k\} \subseteq \mathbb{K}[X_1, \ldots, X_m]$ polinomios que dependen solamente de las variables $\{X_1, \ldots, X_n\}$, tales que $\deg(f_i) = d_i, 1 \leq i \leq k$, y se tiene:

$$d_1 \geq d_2 \geq \cdots \geq d_k \geq 1.$$

Supongamos, además, que se verifica la siguiente desigualdad:

$$\mu_1 d_1 + \cdots + \mu_k d_k + \mu_{k+1} + \cdots + \mu_{n+1} \leq D \cdot \prod_{i=1}^{k} d_i,$$

donde $D \in \mathbb{N}$ es otro entero positivo. Consideremos una matriz triangular superior con unos en la diagonal principal de la forma siguiente:

$$\begin{pmatrix} 1 & a_{1,2} & a_{1,3} & \ldots & a_{1,n+1} & a_{1,n+2} & \ldots & a_{1,m+k} \\ & 1 & & & a_{2,n+1} & a_{2,n+2} & \ldots & a_{2,m+k} \\ & & \ddots & & \vdots & \vdots & & \vdots \\ & \mathit{0} & & 1 & a_{n,n+1} & a_{n,n+2} & \ldots & a_{n,m+k} \\ & & & & 1 & a_{n+1,n+2} & \ldots & a_{n+1,m+k} \end{pmatrix} \in \mathscr{M}_{(n+1)\times(m+k)}(\mathbb{K}).$$

Definamos la siguiente familia de polinomios:

i) Para cada $i, 1 \leq i \leq k$, definamos:

$$\tilde{l_i} := \sum_{j=k+1}^{m+k} a_{i,j} X_{j-k} \in \mathbb{K}[X_1, \ldots, X_m].$$

ii) Para cada $i, k+1 \leq i \leq n+1$:

$$\tilde{l_i} := \sum_{j=i+1}^{m+k} a_{i,j} X_{j-i} \in \mathbb{K}[X_1, \ldots, X_m].$$

iii) Para cada $i, 1 \leq i \leq k$ *definamos*

$$\Psi_i := Z \cdot f_i + \sum_{j=i+1}^{k} a_{i,j} Z \cdot f_j + \tilde{l_i} \in \mathbb{K}[X_1, \ldots, X_m, Z].$$

iv) Para cada $i, k+1 \leq i \leq n+1$, *definamos:*

$$\Psi_i := X_i + \tilde{l_i} \in \mathbb{K}[X_1, \ldots, X_m].$$

Consideremos el polinomio asociado a μ *y a las anteriores funciones dado por la siguiente identidad:*

$$H_\mu(X_1, \ldots, X_m, Z) = \prod_{i=1}^{n+1} \Psi_i^{\mu_i}.$$

Entonces, el polinomio H_μ *admite una representación de la forma siguiente:*

$$H_\mu(X_1, \ldots, X_m, Z) = \sum_{j=1}^{N} \left(\sum_{i=1}^{k} H_{\mu,i}^{(j)} f_i \right) \cdot Z^j + H_\mu^{(0)},$$

donde $N = |\mu|$ *y se tiene:*

i) $H_{\mu,i}^{(j)} = H_{\mu,i}^{(j)}(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$.
ii) $H_\mu^{(0)} = H_\mu^{(0)}(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$.
iii) $\deg(H_{\mu,i}^{(j)} f_i) \leq \sum_{i=1}^{k} \mu_i d_i + \sum_{i=k+1}^{n+1} \mu_i, i \in \{1, \ldots, k\}$ *y* $j \in \{1, \ldots, N\}$.
iv) $\deg(H_\mu^{(0)}) \leq |\mu|$.

Demostración. Haremos la demostración por inducción en $N = |\mu|$.
En el caso $N = 1$, las condiciones se siguen de manera inmediata. Así, si $N = 1$ podemos suponer, sin pérdida de generalidad, que $\mu_1 = 1$ y $\mu_i = 0$, para $2 \leq i \leq n+1$ o bien que $\mu_{n+1} = 1$ y $\mu_j = 0, 1 \leq j \leq n$. En el segundo caso, $H_\mu = \Psi_{n+1}$ es una forma lineal en $\mathbb{K}[X_1, \ldots, X_m]$ y, obviamente, se siguen las propiedades indicadas. En el primer caso, tendremos

$$H_\mu = \Psi_1 = Z \cdot \left(f_1 + \sum_{j=2}^{k} a_{1,j} \cdot f_j \right) + \tilde{l_1},$$

y también se verifican las propiedades indicadas. Supongamos, entonces, que $N \geq 2$ y que la propiedad se verifica para cualquier $\theta \in \mathbb{N}^{n+1}$ tal que $|\theta| \leq N - 1$. Si $\mu = (\mu_1, \ldots, \mu_{n+1})$ tendremos dos casos:

i) Existe i, $1 \leq i \leq k$ con $\mu_i \geq 1$.
ii) Para cada i, $1 \leq i \leq k$, $\mu_i = 0$.

El segundo caso se verifica de manera obvia, y sin necesidad de aplicar inducción, dado que:

$$H_\mu = \prod_{i=1}^{n+1} \Psi_i^{\mu_i} = \prod_{i=k+1}^{n+1} \Psi_i^{\mu_i} = \prod_{i=k+1}^{n+1} (X_i + \tilde{l_i})^{\mu_i}.$$

Como $(X_i + \tilde{l_i})$ es una forma lineal de grado 1, $H_\mu = H_\mu^{(0)}$ y la cota de grado del enunciado se satisface trivialmente. Para probar el caso i), podemos suponer, sin pérdida de generalidad, que $\mu_1 \geq 1$. Así pues, definiremos $\theta = (\theta_1, \ldots, \theta_{n+1}) \in \mathbb{N}^{n+1}$ dado mediante:

$$\theta_1 = \mu_1 - 1, \theta_i = \mu_i, 1 \leq i \leq n+1.$$

Claramente $|\theta| = |\mu| - 1 = N - 1$. Por hipótesis inductiva, tendremos:

$$H_\theta = \prod_{i=1}^{n+1} \Phi_i^{\theta_i} = \sum_{j=1}^{N-1} (\sum_{i=1}^{k} H_{\theta,i}^{(j)} f_i) Z^j + H_\theta^{(0)}, \tag{1.3.2}$$

donde $H_{\theta,i}^{(j)} \in \mathbb{K}[X_1, \ldots, X_m], H_\theta^{(0)} \in \mathbb{K}[X_1, \ldots, X_m]$ y los grados verifican las desigualdades siguientes:

$$\deg_X(H_\theta^{(0)}) \leq N - 1,$$

$$\deg_X(H_{\theta,i}^{(j)} \cdot f_i) \leq \sum_{i=1}^{k} \theta_i d_i + \sum_{i=k+1}^{n+1} \theta_i. \tag{1.3.3}$$

Tenemos que $\mu = \theta + (1, \ldots, 0)$, luego se tiene:

$$H_\mu = \left(Z \cdot (f_1 + \sum_{i=2}^{k} a_{1,i} f_i) + \tilde{l_1} \right) \cdot H_\theta.$$

Efectuando el producto a partir de la identidad 1.3.2 obtendremos
(1.3.4)

$$H_\mu = \sum_{j=1}^{N-1} \left((f_1 + \sum_{i=2}^{k} a_{1,i} f_i) \cdot (\sum_{i=1}^{k} H_{\theta,i}^{(j)} f_i) \right) Z^{j+1} + Z \cdot \left(f_1 + \sum_{i=2}^{k} a_{1,i} f_i \right) \cdot H_\theta^{(0)} + \sum_{j=1}^{N-1} \tilde{l_i} \left(\sum_{i=1}^{k} H_{\theta,i}^{(j)} f_i \right) Z^j + \tilde{l_1} H_\theta^{(0)}.$$

Tomando cada uno de los términos separadamente, observamos que:

- El grado de los coeficientes de Z en los sumandos del primer término satisface que, como $\deg(f_1 + \sum_{i=2}^{k} a_{1,i} f_i) \leq d_1 = \max\{d_1, \ldots, d_k\}$, tenemos:

$$\deg_X \left((f_1 + \sum_{i=2}^{k} a_{1,i} f_i) \cdot H_{\theta,i}^{(j)} \cdot f_i \right) \leq d_i + \deg(H_{0,i}^{(j)} f_i).$$

  Luego, por la hipótesis inductiva 1.3.3, se tiene:

$$\deg_X \left((f_1 + \sum_{i=2}^{k} a_{1,i} f_i) H_{\theta,i}^{(j)} f_i \right) \leq d_1 + (\mu_1 - 1) d_1 + \sum_{i=2}^{k} \mu_i d_i + \sum_{i=k+1}^{n+1} \mu_i = \sum_{i=1}^{k} \mu_i d_i + \sum_{i=k+1}^{n+1} \mu_i \leq D \prod_{i=1}^{k} d_i.$$

- Los grados de los coeficientes de Z en el segundo término satisfacen:

$$\deg(H_\theta^{(0)} f_i) \leq |\theta| + d_i \leq (\mu_1 - 1) + \sum_{i=2}^{k} \mu_i + \sum_{i=k+1}^{n+1} \mu_i + d_i \leq \sum_{i=1}^{k} \mu_i d_i + \sum_{i=k+1}^{n+1} \mu_i \leq D \prod_{i=1}^{k} d_i.$$

- Los grados de los coeficientes de Z^j en el tercer término satisfacen:

$$\deg(\tilde{l_i} H_{\theta,i}^{(j)} f_i) \leq 1 + \deg(H_{\theta,i}^{(j)} f_i) \leq 1 + (\mu_1 - 1) d_1 + \sum_{i=2}^{k} \mu_i d_i + \sum_{i=k+1}^{n+1} \mu_i \leq \sum_{i=1}^{k} \mu_i d_i + \sum_{i=k+1}^{n+1} \mu_i \leq D \prod_{i=1}^{k} d_i.$$

- Por último, el cuarto término de la suma precedente satisface:

$$\deg(\tilde{l_1} H_\theta^{(0)}) \leq 1 + \deg H_\theta^{(0)} \leq 1 + |\theta| = |\mu| \leq N.$$

  Ahora, si expresamos H_μ como polinomio en $\mathbb{K}[X_1, \ldots, X_n, Z]$, tendremos una presentación de la forma:

$$H_\mu = \sum_{i=1}^{N} \left(\sum_{i=1}^{k} H_{\mu,i}^{(j)} f_i \right) Z^j + H_\mu^{(0)}.$$

  Los polinomios $H_{\mu,i}^{(j)}$ se obtienen agrupando coeficientes de Z^j que pueden aparecer en alguna de las descripciones de los tres primeros términos de la expresión 1.3.4. Por las cotas de grado que acabamos de explicar se tendrá

$$\deg(H_{\mu,i}^{(j)} f_i) \leq \sum_{i=1}^{k} \mu_i d_i + \sum_{i=k+1}^{n+1} \mu_i \leq D \prod_{i=1}^{k} d_i,$$

  y se sigue el paso inductivo y el Lema.

□

TEOREMA 1.3.3. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equi-dimensional afín de dimensión n y de grado D. Sean $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios no nulos con $k \leq m$. Sea $\deg f_i = d_i$ y $d_1 \geq \cdots \geq d_k$, $1 \leq i \leq k$.*
Si $V_{\mathbb{A}}(f_1, \ldots, f_k) \cap V = \emptyset$, entonces existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que:

i) La siguiente identidad se verifica en $\mathbb{K}[V]$:

$$1 = \sum_{i=1}^{k} f_i g_i.$$

ii) Los grados de los productos $g_i f_i$ verifican la siguiente igualdad para cada $i \in \{1, \ldots, k\}$:

$$\deg(f_i g_i) \leq D \prod_{i=1}^{k} d_i.$$

Demostración. Consideremos $I(V) \subseteq \mathbb{K}[X_1, \ldots, X_m]$ el ideal de todos los polinomios que se anulan en V, $I(V)+(f_1, \ldots, f_k) \subseteq \mathbb{K}[X_1, \ldots, X_m]$ el ideal suma de $I(V)$ con el ideal generado por $\{f_1, \ldots, f_k\}$. Consideremos $\mathbb{K}[V]$ como el anillo de funciones polinomiales definidas sobre V, esto es,

$$\mathbb{K}[V] = \mathbb{K}[X_1, \ldots, X_m] \Big/ I(V).$$

Recordando que $V_{\mathbb{A}}(\mathfrak{a} + \mathfrak{b}) = V_{\mathbb{A}}(\mathfrak{a}) \cap V_{\mathbb{A}}(\mathfrak{b})$, las siguientes afirmaciones son equivalentes:

i) $V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) = \emptyset$.
ii) $I(V) + (f_1, \ldots, f_k) = (1)$ en $\mathbb{K}[X_1, \ldots, X_m]$.
iii) El ideal generado por las clases $\{f_1 + I(V), \ldots, f_k + I(V)\}$ en el anillo cociente $\mathbb{K}[V]$ es el ideal trivial, es decir,
$$(f_1 + I(V), \ldots, f_k + I(V)) = (1 + I(V)) \text{ en } \mathbb{K}[V].$$
iv) Existen polinomios $A_1, \ldots, A_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que:
$$1 - \sum_{i=1}^{k} A_i \cdot f_i \in I(V).$$

Dividiremos la prueba en varias partes que se entrelazarán para dar la prueba completa de nuestro enunciado.

Parte 1: *Construcción de una deformación a través de un isomorfismo birregular de $V \times \mathbb{K}$ con una subvariedad $W \subseteq \mathbb{A}^{m+k}(\mathbb{K})$.*

Comencemos definiendo la siguiente aplicación polinomial:

$$\begin{aligned} \Phi : V \times \mathbb{K} &\longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^k(\mathbb{K}) \\ (x, z) &\longmapsto (x, f_1(x)z, \ldots, f_k(x)z) \end{aligned}$$

Probemos la siguiente afirmación:

Afirmación. *El morfismo Φ anterior es un isomorfismo birregular con la clausura Zariski de la imagen $W = \overline{\Phi(V \times \mathbb{K})}^z$. En particular, $\Phi(V \times \mathbb{K}) \subseteq \mathbb{A}^{m+k}(\mathbb{K})$ es una variedad equidimensional afín y Φ es un embebimiento de $V \times \mathbb{K}$ en $\mathbb{A}^{m+k}(\mathbb{K})$.*

Prueba de la afirmación. Observemos que se tienen las siguientes afirmaciones:

i) $\Phi(V \times \mathbb{K}) \subseteq V \times \mathbb{A}^k(\mathbb{K})$.
ii) Se definen los polinomios $H_{i,j} \in \mathbb{K}[X_1, \ldots, X_m, Y_1, \ldots Y_k], i, j \in \{1, \ldots, k\}$, mediante las identidades siguientes:
$$H_{i,j}(X_1, \ldots, X_m, Y_1, \ldots, Y_k) = f_i(X_1, \ldots, X_m) \cdot Y_j - f_j(X_1, \ldots, X_m) \cdot Y_i.$$
De forma sencilla se comprueba que estos polinomios se anulan en $\Phi(V \times \mathbb{K})$. Sea $(x, z) \in V \times \mathbb{K}$ y sea $\Phi(x, z) = (x, f_1(x)z, \ldots, f_k(x)z)$ su imagen:
$$H_{i,j}(\Phi(x, z)) = f_i(x) \cdot f_j(x)z - f_j(x) \cdot f_i(x)z = 0.$$
iii) Dado que los polinomios $H_{i,j}$ se anulan en $\Phi(V \times \mathbb{K})$, entonces se anulan también en su clausura Zariski $W := \overline{\Phi(V \times \mathbb{K})}^z$, por definición de clausura Zariski. Por tanto,
$$\forall (a, b_1, \ldots, b_k) \in W := \overline{\Phi(V \times \mathbb{K})}^z,$$
se tiene:
   - $a \in V$.
   - $f_i(a)b_j - b_i f_j(a) = 0$ para cada par $i, j \in \{1, \ldots, k\}$.
iv) Además, se tiene la igualdad siguiente:
$$W = \overline{\Phi(V \times \mathbb{K})}^z = \Phi(V \times \mathbb{K}),$$
y $\Phi(V \times \mathbb{K}) \subseteq \mathbb{A}^{m+k}(\mathbb{K})$ es una variedad algebraica afín y el morfismo
$$\Phi : V \times \mathbb{K} \longrightarrow W,$$

es suprayectivo.
Obviamente basta con que probemos que $W \subseteq \Phi(V \times \mathbb{K})$. Así, sea $(a, b_1, \ldots, b_k) \in W$. Por $i)$ sabemos que $a \in V$ y por $iii)$ sabemos que para cada par $i, j \in \{1, \ldots, k\}$ se verifica

$$f_i(a)b_j - f_j(a)b_i = 0.$$

Definimos, entonces, el elemento $u \in \mathbb{K}$ siguiente:

$$u := \sum_{j=1}^{k} A_j(a) \cdot b_j \in \mathbb{K}.$$

Entonces se tiene:

$$b_i = u \cdot f_i(a) \; \forall i \in \{1, \ldots, k\}.$$

Para verlo, recordemos que como $a \in V$, se tiene:

$$1 = \sum_{j=1}^{k} A_j(a) \cdot f_j(a).$$

Por tanto, se tiene:

$$A_i(a) \cdot f_i(a) = 1 - \sum_{j \neq i} A_j(a) \cdot f_j(a).$$

En conclusión,

$$\begin{aligned} u \cdot f_i(a) &= \left(\sum_{j=1}^{k} A_j(a) \cdot b_j \right) f_i(a) = A_i(a) \cdot b_i \cdot f_i(a) + \sum_{j \neq i} A_j(a) \cdot b_j \cdot f_i(a) = \\ &= \left(1 - \sum_{j \neq i} A_j(a) \cdot f_j(a) \right) \cdot b_i + \sum_{j \neq i} A_j(a) \cdot b_j \cdot f_i(a) = \\ &= b_i + \sum_{j \neq i} A_j(a) \cdot (f_i(a) \cdot b_j - f_i(a) \cdot b_i) = \\ &= b_i + \sum_{j \neq i} A_j(a) \cdot H_{i,j}(a, b_1, \ldots, b_m) = b_i. \end{aligned}$$

Por tanto, dado el punto $(a, b_1, \ldots, b_m) \in W$, el punto $(a, u) \in V \times \mathbb{K}$ satisface

$$\Phi(a, u) = (a, f_1(a) \cdot u, \ldots, f_m(a) \cdot u) = (a, b_1, \ldots, b_m),$$

y, por tanto, $(a, b_1, \ldots, b_m) \in \Phi(V \times \mathbb{K})$ para cualquier $(a, b_1, \ldots, b_m) \in W$. Tenemos así probada la igualdad anunciada $W = \Phi(V \times \mathbb{K})$.

v) Además, podemos considerar la siguiente aplicación polinomial:

$$\begin{aligned} \Psi : W = \Phi(V \times \mathbb{K}) &\longrightarrow V \times \mathbb{K}. \\ (a, b_1, \ldots, b_k) &\longmapsto \left(a, \sum_{i=1}^{k} A_i(a) \cdot b_i \right). \end{aligned}$$

Con los mismos argumentos descritos en $iv)$, se comprueba que

$$\Phi \circ \Psi = Id_W.$$

vi) Además, se cumple que

$$\Psi \circ \Phi = Id_{V \times \mathbb{K}}.$$

Así, sea $(x, z) \in V \times \mathbb{K}$ y su imagen $\Phi(x, z) = (x, f_1(x)z, \ldots, f_k(x)z)$. Entonces $\Phi^{-1}(\Phi(x, z)) = (x, \sum_{i=1}^{k} A_i(x) \cdot f_i(x) \cdot z) = (x, z)$ porque $\sum_{i=1}^{k} A_i(x) \cdot f_i(x) = 1$.

Por tanto, $\Phi^{-1} = \Psi$, y Φ es un isomorfismo birregular entre $V \times \mathbb{K}$ y $W = \overline{\Phi(V \times \mathbb{K})}^{z}$.

En particular, y dado que Φ es un isomorfismo birregular (o un embebimiento de $V \times \mathbb{K}$ en $\mathbb{A}^{m+k}(\mathbb{K})$), tenemos que se preservan también las respectivas dimensiones de Krull:

$$\dim(W) = \dim(V \times \mathbb{K}) = \dim(V) + 1 = n + 1.$$

Parte 2: *Una Normalización de Noether apropiada a través del isomorfismo* Φ.
En esta segunda parte vamos a construir una normalización de Noether de $V \times \mathbb{K}$, obtenida a través del isomorfismo birregular Φ.
Para ello, comencemos construyendo una normalización de Noether de W conforme al Lema 1.2.4. Como $W \subseteq \mathbb{A}^{m+k}(\mathbb{K})$ es la imagen de $V \times \mathbb{K}$ por un embebimiento y al ser V equidimensional, W también lo es, y por tanto existe una matriz triangular superior, con unos en la diagonal principal $A \in \mathscr{M}_{m+k}(\mathbb{K})$ tal que verifica lo siguiente:

i) Sean $\{T_1, \ldots, T_{m+k}\}$ las variables de $\mathbb{A}^{m+k}(\mathbb{K})$ dadas por la matriz A mediante:

$$\begin{pmatrix} T_1 \\ \vdots \\ T_{m+k} \end{pmatrix} = A \cdot \begin{pmatrix} Y_1 \\ \vdots \\ Y_k \\ X_1 \\ \vdots \\ X_m \end{pmatrix} = \begin{pmatrix} 1 & a_{1,2} & a_{1,3} & \cdots & a_{1,m+k} \\ & 1 & & & \\ & & \ddots & & \vdots \\ & 0 & & 1 & a_{m+k-1,m+k} \\ & & & & 1 \end{pmatrix} \begin{pmatrix} Y_1 \\ \vdots \\ Y_k \\ X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

ii) Consideremos la submatriz A_1 de A formada por sus $n+1$ primeras filas y las variables

$$\begin{pmatrix} T_1 \\ \vdots \\ T_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a_{1,2} & & \cdots & & a_{1,m+k} \\ & 1 & & & & \\ & & \ddots & & & \vdots \\ & 0 & & 1 & a_{n+1,n+2} & \cdots & a_{n+1,m+k} \end{pmatrix} \begin{pmatrix} Y_1 \\ \vdots \\ Y_k \\ X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

Escribamos en forma de transformaciones lineales estas mismas variables:

$$l_i(Y_1, \ldots, Y_k, X_1, \ldots, X_m) = Y_i + \sum_{r=i+1}^{k} a_{i,r} Y_r + \sum_{r=k+1}^{k+m} a_{i,r} X_{r-k},$$

para cada $i, 1 \leq i \leq k \leq n$. Y para cada j con $k+1 \leq j \leq n+1$, se tendrá que $l_j \in \mathbb{K}[X_1, \ldots, X_m]$ y no depende de las variables $Y_1, \ldots, Y_m$, es decir, si $k+1 \leq j \leq n+1$, tendremos

$$l_j = X_{j-k} + \sum_{r=j+1}^{m} a_{j,r} X_{r-k}.$$

iii) La proyección siguiente es un morfismo finito y suprayectivo:

$$\begin{aligned} \pi : W \subseteq \mathbb{A}^{m+k}(\mathbb{K}) &\longrightarrow \mathbb{A}^{n+1}(\mathbb{K}) \\ (x, y) &\longmapsto (l_1(x, y), \ldots, l_{n+1}(x, y)). \end{aligned}$$

iv) Dado que $\Phi : V \times \mathbb{K} \longrightarrow W$ es un isomorfismo birregular, también será un morfismo finito y suprayectivo el siguiente:

$$\Psi = \pi \circ \Phi : V \times \mathbb{K} \longrightarrow \mathbb{A}^{n+1}(\mathbb{K}).$$

En particular, tendremos la expresión siguiente para $\pi \circ \Phi$:

$$\pi \circ \Phi(x, z) = (\Psi_1(x, z), \ldots, \Psi_{n+1}(x, z)),$$

donde

$$\Psi_i(x, z) := l_i(x, zf_1(x), \ldots, zf_k(x)),\ 1 \leq i \leq n+1.$$

v) En particular, tenemos una extensión entera de anillos, que define la normalización de Noether de $V \times \mathbb{K}$ buscada siguiente:

$$\begin{aligned} \Psi^* : \mathbb{K}[T_1, \ldots, T_{n+1}] &\longhookrightarrow \mathbb{K}[V \times \mathbb{K}] \\ h(T_1, \ldots, T_{n+1}) &\longmapsto h(\Psi_1, \ldots, \Psi_{n+1}) + I(V \times \mathbb{K}). \end{aligned}$$

Obsérvese, además, que los polinomios $\Psi_i \in \mathbb{K}[X_1, \ldots, X_m, Z]$ que definen Ψ son de la forma siguiente:

- Para $1 \leq i \leq k$, recordando que $k \leq n$, se tiene:

$$\Psi_i(X_1, \ldots, X_m, Z) = Zf_i(X_1, \ldots, X_m) + \sum_{r=i+1}^{k} a_{i,r} Z f_r(X_1, \ldots, X_m) + \sum_{r=k+1}^{k+m} a_{i,r} \cdot X_{r-k}.$$

- Mientras que para cada j, $k+1 \leq j \leq n+1$ se tiene

$$\Psi_j(X_1, \ldots, X_m, Z) = X_{j-k} + \sum_{r=k+1}^{m} a_{j,r} \cdot X_{j-k}.$$

Dado que las ecuaciones $f_1, \ldots, f_k$ han sido dadas con grados decrecientes, tendremos las siguientes estimaciones de los grados de $\Psi_1, \ldots, \Psi_{n+1}$:

i) Si $\deg_X(h)$ denota el grado en las variables $\{X_1, \ldots, X_m\}$, sin tener en cuenta la variable Z, de un polinomio $h \in \mathbb{K}[X_1, \ldots, X_m, Z]$, se tiene:
   - $\deg_X(\Psi_i) = d_i$, para cada i, $1 \leq i \leq k$.
   - $\deg_X(\Psi_j) = 1$, para cada j, $k+1 \leq j \leq n+1$.

   Las primeras igualdades se sigue porque:

$$\deg_X(\Psi_i) = \max\{\deg_X(Z \cdot f_i), \deg_X(Z \cdot f_{i+1}), \ldots, \deg_X(Z \cdot f_k), 1\}.$$

   Las segundas igualdades se siguen porque $\Psi_j \in \mathbb{K}[X_1, \ldots, X_m]$ es lineal para cada j, $1 \leq j \leq n+1$.

ii) Si $\deg_Z(h)$ denota el grado en la variable Z de un polinomio $h \in \mathbb{K}[X_1, \ldots, X_m, Z]$, se tendrá que

$$\deg_Z(\Psi_i) = 1, \ 1 \leq i \leq n+1.$$

Parte 3: *Una ecuación de dependencia entera y ciertas cotas de grado.*
Por construcción, tenemos que $\{\Psi_1, \ldots, \Psi_{n+1}\}$ son algebraicamente independientes sobre $\mathbb{K}$, luego $\mathbb{K}[\Psi_1, \ldots, \Psi_{n+1}] \cong \mathbb{K}[T_1, \ldots, T_{n+1}] \cong \mathbb{K}[\mathbb{A}^{n+1}(\mathbb{K})]$. Además, tenemos la extensión entera de anillos siguiente:

$$\begin{aligned} &\mathbb{K}[T_1, \ldots, T_{n+1}] \hookrightarrow \mathbb{K}[V \times \mathbb{K}], \\ &h(T_1, \ldots, T_{n+1}) \longmapsto h(\Psi_1, \ldots, \Psi_{n+1}) + I(V \times \mathbb{K}). \end{aligned}$$

Por el Lema 1.3.1, podemos identificar $\mathbb{K}[V \times \mathbb{K}]$ con el anillo de polinomios univariados con coeficientes en $\mathbb{K}[V]$ siguiente:

$$\mathbb{K}[V \times \mathbb{K}] \cong \mathbb{K}[V][Z].$$

Como $Z + I(V \times \mathbb{K}) \in \mathbb{K}[V \times \mathbb{K}]$ es un elemento del segundo anillo de la extensión entera precedente, entonces existirá un polinomio $P \in \mathbb{K}[T_1, \ldots, T_{n+1}][U]$, mónico con respecto a la variable U, es decir,

$$P_Z(T_1, \ldots, T_{n+1}, U) := U^\delta + \sum_{i=0}^{\delta-1} P_i(T_1, \ldots, T_{n+1}) U^i, \tag{1.3.5}$$

de tal modo que

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = Z^\delta + \sum_{i=0}^{\delta-1} P_i(\Psi_1, \ldots, \Psi_{n+1}) Z^i \in I(V \times \mathbb{K}).$$

De hecho, podremos tener una descripción de P_Z como elemento de $\mathbb{K}[X_1, \ldots, X_m, Z]$ con la forma siguiente:

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = (1 + A_\delta) Z^\delta + \sum_{r \neq \delta} A_r Z^r,$$

con $A_i \in \mathbb{K}[X_1, \ldots, X_m]$. Nuestro principal objetivo consiste en determinar ciertas propiedades de estos polinomios A_i.
Para comenzar, vamos a tratar de determinar una cota superior de los grados de los polinomios $P_i(T_1, \ldots, T_{n+1})$, para lo cual retomaremos el Teorema de Perron Generalizado (Teorema 1.2.3 anterior).

Consideremos el cuerpo $\mathbb{L} = \mathbb{K}(Z) = qf.(\mathbb{K}[Z])$ como cuerpo de fracciones del anillo de polinomios $\mathbb{K}[Z]$ (véase la Subsección A.1 un breve resumen de las propiedades esenciales). Consideremos los polinomios $\Psi_1, \ldots, \Psi_{n+1} \in \mathbb{K}(Z)[X_1, \ldots, X_m] = \mathbb{L}[X_1, \ldots, X_m]$ como elementos de ese anillo. Por el Teorema de Perron Generalizado (Teorema 1.2.3) existe un polinomio $W \in \mathbb{L}[T_1, \ldots, T_{n+1}]$, verificando las siguientes propiedades:

i) $W(\Psi_1, \ldots, \Psi_{n+1}) = 0$ en $\mathbb{K}[V]$,
ii) $\deg_T(W(T_1^{d_1}, \ldots, T_k^{d_k}, T_{k+1}, \ldots, T_{n+1})) \leq D \prod_{i=1}^k d_i$.

Los elementos de $\mathbb{L} = \mathbb{K}(Z)$ son cocientes de la forma $\frac{p}{q}$, con p y q en $\mathbb{K}[Z]$ y $q \neq 0$. Del mismo modo los coeficientes de W son elementos de $\mathbb{L}$ y, por tanto, están definidos por un número finito de elementos en $\mathbb{K}[Z]$. Como $\mathbb{K}[Z]$ es DFU, podemos definir $D(Z) \in \mathbb{K}[Z]$ como el mínimo común múltiplo de los denominadores de los coeficientes (no nulos) de W como elemento de $\mathbb{L}[T_1, \ldots, T_{m+1}]$. Nótese que $D(Z)$ sólo depende de la variable Z y que, multiplicando,

$$D(Z) \cdot W \in \mathbb{K}[Z][T_1, \ldots, T_{n+1}] = \mathbb{K}[T_1, \ldots, T_{n+1}, Z].$$

Más aún, el grado con respecto a las variables $\{T_1, \ldots, T_{n+1}\}$ de $D(Z) \cdot W$ no cambia porque sólo multiplicamos por un polinomio en $\mathbb{K}[Z]$. Así, habremos probado lo siguiente:
Existe un polinomio $W'(T_1, \ldots, T_{n+1}, Z) \in \mathbb{K}[T_1, \ldots, T_{n+1}, Z]$ tal que se verifica lo siguiente:

i) $W'(\Psi_1, \ldots, \Psi_{n+1}, Z) = 0$ en $\mathbb{K}[V \times \mathbb{K}]$,
ii) $\deg_T W'(T_1^{d_1}, \ldots, T_k^{d_k}, T_{k+1}, \ldots, T_{n+1}, Z) \leq D \prod_{i=1}^k d_i$.

Ahora, recordamos que $P_Z \in \mathbb{K}[T_1, \ldots, T_{n+1}, Z]$ es la ecuación mínima de dependencia entera de Z sobre $\mathbb{K}[T_1, \ldots, T_{n+1}]$ de la extensión entera

$$\mathbb{K}[T_1, \ldots, T_{n+1}] \hookrightarrow \mathbb{K}[V \times \mathbb{K}].$$

Por tanto, P_Z divide al polinomio $W'(T_1, \ldots, T_{n+1}, Z)$. Es decir, existe $h \in \mathbb{K}[T_1, \ldots, T_{n+1}, Z]$ tal que, por ser P_Z mónico con respecto a Z,

$$W'(T_1, \ldots, T_{n+1}, Z) = h(T_1, \ldots, T_{n+1}, Z) \cdot P_Z(T_1, \ldots, T_{n+1}, Z).$$

Luego

$$W'(T_1^{d_1}, \ldots, T_k^{d_k}, T_{k+1}, \ldots, T_{n+1}, Z) = h(T_1^{d_1}, \ldots, T_k^{d_k}, T_{k+1}, \ldots, T_{n+1}, Z) \cdot P_Z(T_1^{d_1}, \ldots, T_k^{d_k}, T_{k+1}, \ldots, T_{n+1}, Z).$$

Finalmente

$$\deg_T(P_Z(T_1^{d_1}, \ldots, T_k^{d_k}, T_{k+1}, \ldots, T_{n+1}, Z)) \leq \deg_T(W'(T_1^{d_1}, \ldots, T_k^{d_k}, T_{k+1}, \ldots, T_{n+1}, Z)) \leq D \prod_{i=1}^k d_i.$$

Dados los polinomios $P_i(T_1, \ldots, T_{n+1}) \in \mathbb{K}[T_1, \ldots, T_{n+1}], 0 \leq i \leq \delta$, de la expresión 1.3.5 anterior, supongamos $Supp_i := Supp(P_i)$ su soporte (i.e. el conjunto $Supp(P_i) \subseteq \mathbb{N}^{n+1}$ de los exponentes con coeficiente no nulo). Juntando todos los soportes, podemos suponer un conjunto finito de exponentes monomiales

$$Supp := \cup_{i=0}^{\delta-1} Supp_i \subseteq \mathbb{N}^{n+1},$$

de tal modo que, añadiendo coeficientes nulos si fuera necesario, podemos expresar para cada $i, 0 \leq i \leq \delta - 1, P_i(T_i \ldots, T_{n+1}) \in \mathbb{K}[T_1, \ldots, T_{n+1}]$ del modo siguiente:

$$P_i(T_1, \ldots, T_{n+1}) = \sum_{\mu \in Supp} a_\mu^{(i)} T_1^{\mu_1} \cdots T_{n+1}^{\mu_{n+1}}.$$

Sea $N = \max\{|\mu| : \mu \in Supp\}$ y, por el Teorema de Perron Generalizado, sabemos que

$$d_1\mu_1 + \cdots + d_k\mu_k + \mu_{k+1} + \cdots + \mu_{n+1} \leq D \prod_{i=1}^k d_i, \forall \mu \in Supp.$$

Más aún, también tendremos $N \leq D \prod_{i=1}^k d_i$. Consideremos ahora la especialización $P_i(\Psi_1, \ldots, \Psi_{n+1}) \in \mathbb{K}[X_1, \ldots, X_m][Z]$ y tendremos

$$P_i(\Psi_1, \ldots, \Psi_{n+1}) = \sum_{\mu \in Supp} a_\mu^{(i)} \Psi_1^{\mu_1} \cdots \Psi_{n+1}^{\mu_{n+1}}.$$

Para cada $i, 0 \leq i \leq \delta - 1$, y para cada $\mu \in Supp$, aplicando el Lema 1.3.2, se verificará la identidad siguiente:

$$a_\mu^{(i)} \Psi_1^{\mu_1} \cdots \Psi_{n+1}^{\mu_{n+1}} = a_\mu^{(i)} \left[\sum_{j=1}^{|\mu|} \left(\sum_{l=1}^{k} H_{\mu,l}^{(i,j)} f_l \right) Z^j + H_{\mu,0}^{(i,0)} \right],$$

donde $H_{\mu,l}^{(i,j)} \in \mathbb{K}[X_1, \ldots, X_m]$ y se verifica:

$$\deg(H_{\mu,l}^{(i,j)} f_l) \leq D \prod_{i=1}^{k} d_i,$$

$$\deg(H_{\mu,0}^{(i,0)}) \leq |\mu| \leq D \prod_{i=1}^{k} d_i.$$

A partir de estas identidades, obtendremos:

$$P_i(\Psi_1, \ldots, \Psi_{n+1}) = \sum_{\mu \in Supp} a_\mu^{(i)} \left[\sum_{j=1}^{|\mu|} \left(\sum_{l=1}^{k} H_{\mu,l}^{(i,j)} f_j \right) Z^j + H_{\mu,0}^{(i,0)} \right].$$

Reordenando los coeficientes, añadiendo ceros si fuera necesario, podemos reescribir esta última identidad del modo siguiente:

$$P_i(\Psi_1, \ldots, \Psi_{n+1}) = \sum_{r=1}^{N} A_r^{(i)} Z^r + A_0^{(i)}, \tag{1.3.6}$$

donde $A_r^{(i)}, A_0^{(i)} \in \mathbb{K}[X_1, \ldots, X_m]$ y se tiene para $r \geq 1$,

$$A_r^{(i)} := \sum_{\mu \in Supp} a_\mu^{(i)} \left(\sum_{l=1}^{k} H_{\mu,l}^{(i,r)} f_l \right),$$

y para $r = 0$

$$A_0^{(i)} = \sum_{\mu \in Supp} a_\mu^{(i)} H_{\mu,0}^{(i,0)}.$$

Escribamos, reordenando los sumandos

$$A_r^{(i)} := \sum_{l=1}^{k} A_{r,l}^{(i)} f_l,$$

donde

$$A_{r,l}^{(i)} = \left(\sum_{\mu \in Supp} a_\mu^{(i)} H_{\mu,l}^{(i,r)} \right). \tag{1.3.7}$$

Tendremos que

$$\deg(A_r^{(i)} f_l) \leq \max\{\deg(H_{\mu,l}^{(i,r)} f_l) : \mu \in Supp\} \leq D \prod_{i=1}^{k} d_i,$$

mientras que $\deg(A_0^{(i)}) \leq N \leq D \prod_{i=1}^{k} d_i$. A partir de la identidad 1.3.6 obtendremos

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = Z^\delta + \sum_{i=0}^{\delta-1} \left(\sum_{r=1}^{N} A_r^{(i)} Z^r + A_0^{(i)} \right) Z^i.$$

Esto nos permite descomponer P_Z en tres trozos, sacando Z^l como factor común.

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = (1 + A_\delta) Z^\delta + \sum_{l \neq \delta} Z^l \Big(\sum_{\substack{i+r=l \\ 1 \leq i}} A_r^{(i)} \Big) + \sum_{i=1}^{\delta-1} A_0^{(i)} Z^i, \tag{1.3.8}$$

donde, sacan

$$A_\delta = \sum_{\substack{i+r=\delta \\ 1 \leq i}} A_r^{(i)} \in \mathbb{K}[X_1, \ldots, X_m].$$

Observamos lo siguiente:

- El polinomio A_δ tiene la forma siguiente:

$$A_\delta = \sum_{\substack{i+r=\delta \\ 1\leq i}} A_r^{(i)} = \sum_{\substack{i+r=\delta \\ 1\leq i}} \left(\sum_{l=1}^{k} A_{r,l}^{(i)} f_l \right) = \sum_{l=1}^{k} (\sum_{\substack{i+r=\delta \\ 1\leq i}} A_{r,l}^{(i)}) f_l = \sum_{l=1}^{k} A_\delta^{(l)} f_l \tag{1.3.9}$$

  donde

$$\deg(A_\delta^{(l)} f_l) \leq Supp\{\deg(A_{r,l}^{(i)} f_l) : i + r = \delta, 1 \leq i\} \leq D \prod_{i=1}^{k} d_i.$$

- En A_δ no aparece ningún sumando de tipo $A_0^{(i)}$ dado que $A_0^{(i)}$ multiplica a Z^i con $0 \leq i \leq \delta - 1$.

Parte 4: *La última observación.* Tomamos la expresión 1.3.8:

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = (1 + A_\delta) Z^\delta + \sum_{l \neq \delta} Z^l \left(\sum_{\substack{i+r=l \\ 1\leq i}} A_r^{(i)} \right) + \sum_{i=1}^{\delta-1} A_0^{(i)} Z^i,$$

y supondremos

$$P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) = \sum_{i=0}^{\tilde{\delta}} Q_i(X_1, \ldots, X_m) Z^i,$$

con $Q_i \in \mathbb{K}[X_1, \ldots, X_m]$. Por construcción, $P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) \in I(V \times \mathbb{K})$ y por el Lema 1.3.1, concluiremos que

$$Q_i(X_1, \ldots, X_m) \in I(V) \text{ para cada } i, 0 \leq i \leq \tilde{\delta}.$$

Nos interesa especialmente el coeficiente Q_δ que, por la identidad 1.3.8 satisface

$$Q_\delta(X_1, \ldots, X_m) = 1 + A_\delta \in I(V).$$

Finalmente, tomando la identidad 1.3.9 anterior y escribiendo $g_l = A_\delta^{(l)}$ tendremos que

$$1 + \sum_{l=1}^{k} g_i \cdot f_i \in I(V),$$

verificando

$$\deg(g_i f_i) = \deg(A_\delta^{(l)} f_l) \leq D \prod_{i=1}^{k} d_i,$$

lo que concluye la demostración del Teorema.

□

CAPíTULO 2

Un Teorema de Eliminación y el Nullstellensatz Efectivo de Jelonek

Índice

2.1. Introducción.

En este segundo capítulo culminaremos el objeto final de este Trabajo Fin de Grado, demostrando el Nullstellenstaz Efectivo de [Je, 2005].
La primera parte del Capítulo se centra en probar un Teorema de Eliminación con cotas de grado, presente en [Je, 2005]. Ese Teorema es el siguiente:

TEOREMA 7. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica irreducible de dimensión n y grado D. Sean $k \leq n$ y $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios tales que la siguiente variedad es cero-dimensional:*

$$A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_k).$$

Entonces, existe un abierto Zariski $\mathcal{U}_1 \subseteq \mathscr{M}_m(\mathbb{K})$ formado por matrices regulares tales que para cada $B \in \mathcal{U}_1$, el cambio de variables que determina:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix},$$

satisface las siguientes propiedades:

i) Y_1 es un elemento separante sobre A y existe un polinomio univariado $\Phi_1(T)$ tal que si $\Phi_1(z) = 0$, entonces $\exists a \in A$ tal que

$$z = Y_1(a).$$

ii) Existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que

$$\Phi_1(Y_1) - \sum_{i=1}^{k} g_i f_i \in I(V).$$

iii) $\deg(g_i f_i) \leq D \cdot \prod_{i=1}^{k} \deg(f_i)$, $\deg(\Phi_1(Y_1)) \leq D \prod_{i=1}^{k} \deg(f_i)$.

La prueba del enunciado es completamente original, aunque está inspirada en [Pa,19]. Jelonek en [Je, 2005], hace uso de su caracterización de los puntos de "impropiedad" en la imagen de morfismos dominantes y genéricamente finitos de su trabajo previo [Je, 2001].
Nosotros hemos desarrollado una prueba propia partiendo de la noción de *forma lineal separante* de una variedad cero-dimensional. Observamos que existe un abierto Zariski de matrices apropiadas (triangulares superiores con unos en la diagonal) que permiten poner las coordenadas en posición de Noether, de tal forma que cada una de las nuevas variables sea elemento separante (ver Proposición 2.2.2). Una vez probado ésto, usando la misma función Φ del Capítulo

precedente

$$\begin{aligned}\Phi : V \times \mathbb{K} &\longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K}) \\ (x, z) &\longmapsto (x, f_1(x)z, \ldots, f_n(x)z),\end{aligned}$$

con el parámetro de deformación z, construimos un abierto distinguido $D(q_A)$ sobre una normalización de Noether de $\overline{\Phi(V \times \mathbb{K})}^z$, de tal modo que q_A sea el polinomio mínimo de una forma lineal separante, de grado controlado, y de tal modo que tengamos una extensión entera de anillos para las localizaciones:

$$\mathbb{K}[T_1, \ldots, T_{n+1}]_{q_A} \hookrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A}.$$

Esto se describe en la Proposición 2.2.6. Lo que se hace para una forma lineal separante es extensible a todas (Corolario 2.2.7) las variables nuevas de una normalización de Noether. Finalmente, usando una reflexión análoga a la hecha en el Capítulo precedente con el caso sub-determinado, no sólo podemos acotar el grado de las ecuaciones minimales de las formas lineales separantes sino también su presentación en la forma de combinación lineal de las clases de $\{f_1, \ldots, f_n\}$ en $\mathbb{K}[V]$. Este es el enunciado precedente destacado en esta introducción al Capítulo (el Teorema 2.2.8 del cuerpo del Capítulo).
Con estas herramientas estamos en condiciones de probar el enunciado Nullstellensatz Efectivo que es el Teorema siguiente y que se describe y prueba como Teorema 2.3.5 en la Sección 2.3 a continuación:

TEOREMA 8. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín irreducible de dimensión n. Sean $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios tales que $d_i = \deg(f_i)$ y se tiene*

- *$d_1 \geq d_2 \geq \cdots \geq d_k$.*
- *$V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) = \emptyset$.*

Entonces, existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que

i) $1 - \sum_{i=1}^k g_i f_i \in I(V)$.
ii) $\deg(g_i f_i) \leq 2DN(d_1, \ldots, d_k; n) - 1$, *donde*

$$N(d_1, \ldots, d_k; n) = \begin{cases} \prod_{i=1}^k d_i & \text{si } k < n, n > 1 \\ \prod_{i=1}^n d_i & \text{si } n < k, n > 1 \\ d_1 & \text{si } n = 1. \end{cases}$$

El resultado ya se había probado en el caso sub-determinado $k \leq n$. Por tanto, queda la prueba del caso $k \geq n + 1$. Usando un método clásico de combinaciones lineales que respetan los grados, se reduce el problema al caso $k = n+1$ (véase Lema 2.2.4 y la Observación 2.3.4). Así, nos encontramos, en el caso defectivo, con la situación en que podemos construir sucesiones $\{F_1, \ldots, F_{n+1}\}$ y $\{G_1, \ldots, G_{n+1}\}$ de combinaciones lineales genéricas de $\{f_1, \ldots, f_{n+1}\}$ tales que se verifique:

i) $V \cap V_{\mathbb{A}}(F_1, \ldots, F_n)$ es una variedad cero-dimensional.
ii) $V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$ es una variedad cero-dimensional.
iii) $V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) \cap V \cap V_{\mathbb{A}}(G_1, \ldots, G_n) = \emptyset$.

Esta construcción, que hemos llamado *construcción cruzada* en la subsección 2.3.1, permite construir una forma lineal separante Y_1 para la unión $V \cap V(F_1, \ldots, F_n) \cup V \cap V(G_1, \ldots, G_n)$. Aplicando el Teorema de Eliminación a Y_1 sobre cada uno de ellos, obtendremos

- Un polinomio univariado $\Phi_1(Y_1)$ de grado apropiado y minimal tal que $\Phi_1(Y_1)$ se anula en $V \cap V(F_1, \ldots, F_n)$ y satisface las condiciones del Teorema de Eliminación precedente.
- Un polinomio univariado $\Phi_2(Y_1)$ de grado apropiado y minimal tal que $\Phi_2(Y_1)$ se anula en $V \cap V(G_1, \ldots, G_n)$ y satisface las condiciones del Teorema de Eliminación precedente.

Como Y_1 es separante para ambos y $V \cap V(F_1, \ldots, F_n) \cup V \cap V(G_1, \ldots, G_n) = \emptyset$, no es posible que $\Phi_1(T)$ y $\Phi_2(T)$ tengan ceros comunes. Por tanto, su máximo común divisor en $\mathbb{K}[T]$ es 1 y, aplicando la identidad de Bézout univariada tendremos:

$$1 = Q_1(Y_1)\Phi_1(Y_1) + Q_2(Y_1)\Phi_2(Y_1),$$

con grados de Q_1 y Q_2 acotados por los grados de Φ_1 y Φ_2. El Teorema de Eliminación precedente nos dice, además, que Φ_1 y Φ_2 se presentan como combinaciones de $F_1, \ldots, F_n$ y $G_1, \ldots, G_n$ respectivamente, de grados controlados, en el anillo $\mathbb{K}[V]$

$$\Phi_1(Y_1) = \sum_{i=1}^{n} h_{i,1} F_i, \Phi_2(Y_1) = \sum_{i=1}^{n} h_{i,2} G_i.$$

Por tanto, obtenemos una expresión de la forma siguiente, válida en $\mathbb{K}[V]$:

$$1 = \sum_{i=1}^{n} (Q_1(Y_1) h_{i,1}) F_i + \sum_{i=1}^{n} (Q_2(Y_1) h_{i,2}) G_i,$$

donde todas las cotas de grado han sido controladas. Recordando ahora que tanto $\{F_1, \ldots, F_n\}$ como $\{G_1, \ldots, G_n\}$ son combinaciones lineales de $\{f_1, \ldots, f_k\}$ se obtiene la expresión final:

$$1 = \sum_{i=1}^{k} g_i f_i \text{ en } \mathbb{K}[V],$$

con las cotas de grado que se siguen de las cotas de Φ_1, Φ_2, $h_{i,j}$, Q_1 y Q_2 antes citadas.

2.2. Un Teorema de Eliminación en [Je, 2005]

2.2.1. Forma lineal separante o elemento primitivo. Sea $A \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín cero-dimensional, es decir, un conjunto finito de puntos.
Una aplicación lineal $l : \mathbb{A}^m(\mathbb{K}) \longrightarrow \mathbb{K}$ se dice forma separante de A (o elemento primitivo de $\mathbb{K}[A]$) si

$$\forall x, y \in A, x \neq y \Longrightarrow l(x) \neq l(y).$$

Las formas lineales separantes de una variedad cero-dimensional son genéricamente densas. En términos teóricos:

PROPOSICIÓN 2.2.1. *Sea $A \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica cero-dimensional. Entonces, existe un abierto Zariski no vacío $\mathcal{U} \subseteq \mathbb{A}^m(\mathbb{K})$ tal que para cada $\underline{\theta} = (\theta_1, \ldots, \theta_m) \in \mathcal{U}$, la aplicación lineal*

$$l_{\underline{\theta}}(X_1, \ldots, X_m) = \theta_1 X_1 + \cdots + \theta_m X_m, \tag{2.2.1}$$

es una forma separante de A.

DEMOSTRACIÓN. Vamos a construir $\mathcal{U}$ de forma sencilla. Supongamos

$$A = \{a_1, \ldots, a_\delta\},$$

y, para cada $i, 1 \leq i \leq \delta$, supongamos

$$a_i = (a_{i,1}, \ldots, a_{i,m}).$$

Definimos para cada par $i, j \in \{1, \ldots, \delta\}$, con $i \neq j$ el polinomio

$$F_{i,j}(T_1, \ldots, T_m) = \sum_{k=1}^{m} (a_{i,k} - a_{j,k}) \cdot T_k \in \mathbb{K}[T_1, \ldots, T_m].$$

Observamos que $F_{i,j}$ es lineal. Pero, además, $F_{i,j}$ es un polinomio no nulo. Como $a_i \neq a_j$, entonces existe una coordenada $k \in \{1, \ldots, m\}$ en la que difieren a_i y a_j. Es decir, existe $k \in \{1, \ldots, m\}$ tal que $(a_{i,k} - a_{j,k}) \neq 0$. Por tanto F_{ij} es un polinomio en las variables $\{T_1, \ldots, T_m\}$ que tiene un coeficiente no nulo, es decir, $F_{ij} \neq 0$. Definimos el polinomio multivariado

$$F_A := \prod_{i \neq j} F_{ij}(T_1, \ldots, T_m) \in \mathbb{K}[T_1, \ldots, T_m].$$

Como F_A es un polinomio no nulo, entonces el abierto distinguido que define

$$\mathcal{U} := D_{\mathbb{A}^m(\mathbb{K})}(F_A) := \{\underline{\theta} \in \mathbb{A}^m(\mathbb{K}) : F_A(\underline{\theta}) \neq 0\}$$

es un abierto Zariski no vacío. Veamos que para cada $\overline{\theta} \in \mathcal{U}$, la función lineal $l_{\underline{\theta}}$ es separante para los elementos de A. Para ello, sean $a_i, a_j \in A$ con $i \neq j$. Tendremos que

$$l_{\underline{\theta}}(a_i) - l_{\underline{\theta}}(a_j) = \sum_{k=1}^{m} \theta_k a_{i,k} - \sum_{k=1}^{m} \theta_k a_{j,k} = \sum_{k=1}^{m} \theta_k (a_{i,k} - a_{j,k}) = F_{ij}(\underline{\theta}).$$

Pero como $F_A(\theta) \neq 0$ y $F_A(\theta) = \prod_{i \neq j} F_{ij}(\underline{\theta})$, sabemos que $F_{ij}(\underline{\theta}) \neq 0$, con lo que

$$l_{\underline{\theta}}(a_i) - l_{\underline{\theta}}(a_j) \neq 0,$$

o, equivalentemente, $l_{\underline{\theta}}(a_i) \neq l_{\underline{\theta}}(a_j) \forall i, j, i \neq j$. Por tanto, $l_{\underline{\theta}}$ es separante. □

No solamente podemos elegir genéricamente una forma lineal separante para una variedad 0-dimensional sino que genéricamente todo cambio lineal de coordenadas en $\mathbb{A}^m(\mathbb{K})$ puede elegirse de tal modo que cada nueva coordenada sea separante. Técnicamente, esto se enuncia como sigue:

PROPOSICIÓN 2.2.2. *Sea $A \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica cero-dimensional (i.e. un conjunto finito). Entonces, existe un abierto Zariski $\mathcal{U}_A \subseteq \mathscr{M}_m(\mathbb{K})$ en el espacio de matrices cuadradas tal que*

i) Para cada $B \in \mathcal{U}_A, det(B) \neq 0$ (i.e. la matriz B es regular y define un cambio lineal de coordenadas en $\mathbb{A}^m(\mathbb{K})$).

ii) Para cada $B \in \mathcal{U}_A$, sean $\{Y_1, \ldots, Y_m\}$ las nuevas coordenadas determinadas por B como cambio de variables, esto es,

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

Entonces, para cada $i, 1 \leq i \leq m$, Y_i es una forma lineal con respecto a las variables $\{X_1, \ldots, X_m\}$

$$Y_i = \sum_{j=1}^{m} b_{i,j} \cdot X_j,$$

entonces Y_i es separante con respecto a A.

DEMOSTRACIÓN. Es la misma que la precedente, construyendo un polinomio $F_A^{(i)}$ con respecto a la fila i-ésima de la matriz genérica $\mathscr{M}_m(\mathbb{K})$

$$F_A^{(i)} = \prod_{r \neq s} F_{r,s}^{(i)}(T_{i,1}, \ldots, T_{i,m}),$$

siendo

$$F_{r,s}^{(i)}(T_{i,1}, \ldots, T_{i,m}) = \sum_{k=1}^{m} (a_{r,k} - a_{s,k}) T_{i,k}.$$

Entonces $\mathcal{U}_A$ será el abierto Zariski dado por

$$\mathcal{U}_A = \{B = (b_{i,j})_{1 \leq i,j \leq m} \in \mathbb{A}^{m^2}(\mathbb{K}) : F_A^{(i)}(b_{i,1}, \ldots, b_{i,m}) \neq 0, 1 \leq i \leq m\}.$$

□

En otras palabras, dada una variedad algebraica cero-dimensional, podemos elegir genéricamente un cambio de variables de tal modo que cada coordenada sea separante con respecto a esa variedad.

2.2.2. Hacia el Teorema de Eliminiación de [Je, 2005].

PROPOSICIÓN 2.2.3. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica irreducible de dimensión n y grado D. Sean $f_1, \ldots, f_n \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios tales que la intersección $A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_n)$ sea una variedad algebraica cero-dimensional. Sea $\Phi : V \times \mathbb{K} \longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K})$ el morfismo dado mediante:*

$$\Phi(X_1, \ldots, X_m, Z) = (X_1, \ldots, X_m, f_1(X)Z, \ldots, f_n(X)Z).$$

Entonces, se tiene:

i) La clausura Zariski de la imagen $\mathcal{W} = \overline{\Phi(V \times \mathbb{K})}^z$ es una variedad algebraica irreducible de dimensión $n+1$ y $\Phi : V \times \mathbb{K} \longrightarrow \mathcal{W}$ es un morfismo dominante.

ii) Existe un abierto $\mathcal{U}_1 \subseteq \mathscr{M}_m(\mathbb{K})$ en el espacio de matrices cuadradas $m \times m$ sobre $\mathbb{K}$ tal que para cada $B \in \mathcal{U}_1$, B define un cambio lineal de coordenadas (en particular $det(B) \neq 0$):

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

de tal modo que Y_1 es un elemento separante sobre A.

iii) Existe un polinomio univariado $q_A(Y_1) \in \mathbb{K}[Y_1], deg(q_A) \leq D\prod_{i=1}^{n} \deg(f_i)$ tal que el siguiente es un isomorfismo de $\mathbb{K}$-álgebras

$$\Phi^* : \mathbb{K}[\mathcal{W}]_{q_A(Y_1)} \longrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A(Y_1)}.$$

Demostración. i) Es claro que como $V \times \mathbb{K}$ es irreducible, $\mathcal{W} = \overline{\Phi(V \times \mathbb{K})}^z$ es también irreducible y que $\Phi : V \times \mathbb{K} \longrightarrow \mathcal{W}$ es dominante. Nos queda por ver que $\dim(\mathcal{W}) = n + 1$. Para ello, construyamos para cada $i, 1 \leq i \leq n$, el siguiente abierto Zariski en V, posiblemente vacío

$$V_i = \{x \in V : f_i(x) \neq 0\}.$$

Consideremos también el abierto Zariski $V' = V \setminus A \subseteq V$. Observamos que V' es no vacío (porque A es cero dimensional y V tiene dimensión n) y

$$V' = \cup_{i=1}^{n} V_i. \tag{2.2.2}$$

Es claro que si $x \in V_i$ entonces, como $f_i(x) \neq 0, x \notin V_{\mathbb{A}}(f_1, \ldots, f_n)$ luego $x \notin A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_n)$ por lo que $x \in V'$. De otro lado, si $x \in V'$ es porque $x \notin V_{\mathbb{A}}(f_1, \ldots, f_n)$, luego ha de existir i tal que $f_i(x) \neq 0$ con lo que $x \in V_i$. La igualdad 2.2.2 anterior nos dice que alguno de los V_i ha de ser no vacío. Como V es irreducible, $V_i \neq \emptyset$ implicaría que V_i es denso en V y, por tanto, si $V_i \neq \emptyset$

$$\overline{V_i \times \mathbb{K}}^z = V \times \mathbb{K},$$

con lo que la dimensión de $V_i \times \mathbb{K}$ es $\dim(V) + 1 = n + 1$. Considero ahora los abiertos Zariski de $\mathcal{W}$ dados por la siguiente identidad

$$\mathcal{W}_i := \{(x, y_1, \ldots, y_m) \in \mathcal{W} : y_i \neq 0, f_i(x) \neq 0\}.$$

De nuevo $\mathcal{W}_i$ es un abierto Zariski y si es no vacío, entonces es denso Zariski en $\mathcal{W}$, con lo que

$$\mathcal{W}_i \neq \emptyset \Rightarrow \dim(\mathcal{W}_i) = \dim(\mathcal{W}).$$

Finalmente, considero la restricción

$$\Phi|_{V_i \times (\mathbb{K} \setminus \{0\})} : V_i \times \mathbb{K} \setminus \{0\} \longrightarrow \mathcal{W},$$
$$(x_1, \ldots, x_m, z) \longmapsto (x_1, \ldots, x_m, f_1(x)z, \ldots, f_n(x)z).$$

Observamos que

$$\Phi(V_i \times \mathbb{K} \setminus \{0\}) = \mathcal{W}_i.$$

Obviamente, si $(x, z) \in V_i \times \mathbb{K} \setminus \{0\}$, $f_i(x)z \neq 0$ con lo que, por construcción, su imagen está contenida en $\mathcal{W}_i$. Pero, recíprocamente, podemos definir la siguiente función racional:

$$\tilde{\Phi} : \mathcal{W}_i \longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{K}$$
$$(x_1, \ldots, x_m, y_1, \ldots, y_n) \longmapsto (x_1, \ldots, x_m, \frac{y_i}{f_i(x)}),$$

que está bien definida en $\mathcal{W}_i$ y se tiene que $\tilde{\Phi}(\mathcal{W}_i) \subseteq V_i \times \mathbb{K} \setminus \{0\}$. Más aún, es fácil verificar que $\tilde{\Phi}$ es una función racional que es la inversa de $\Phi|_{V_i \times \mathbb{K} \setminus \{0\}}$:

$$\begin{aligned} \tilde{\Phi} \circ \Phi &= Id_{V_i \times \mathbb{K} \setminus \{0\}}, \\ \Phi \circ \tilde{\Phi} &= Id_{\mathcal{W}_i}. \end{aligned} \tag{2.2.3}$$

Por tanto $\Phi|_{V_i \times (\mathbb{K} \setminus \{0\})}$ define un isomorfismo birracional entre $V_i \times (\mathbb{K} \setminus \{0\})$ es también un abierto de Zariski en $\mathcal{W}$ irreducible y $\mathcal{W}_i \neq \emptyset$. En ese caso, $\mathcal{W}_i$ es denso en

$\mathcal{W}$ y $\dim(\mathcal{W}_i) = \dim(\mathcal{W})$. Pero como, además, $\mathcal{W}_i$ es birracionalmente isomorfo a $V_i \times \mathbb{K} \setminus \{0\}$. Consideremos si $V_i \neq \emptyset$, $\dim(\overline{V_i \times \mathbb{K} \setminus \{0\}}^z) = \dim(\overline{\mathcal{W}_i}^z) = \dim(\mathcal{W})$.

ii) La propiedad se sigue de la Proposición 2.2.2 precedente sobre los elementos separantes.

iii) Sin pérdida de generalidad supongamos que $X_1 = Y_1$ es la primera coordenada y que es un elemento separante de A. Por tanto, si suponemos $A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_n)$, tenemos que A es finito, $\#(A) = \deg(A)$ y por la desigualdad de Bézout de [**He, 1983**],

$$\delta = \deg(A) \leq \deg(V) \prod_{i=1}^{n} \deg(f_i) \leq D \prod_{i=1}^{n} d_i.$$

Supongamos, además, $A = \{a_1, \ldots, a_\delta\}$, donde $a_i = (a_{i,1}, \ldots, a_{i,m}) \in \mathbb{A}^m(\mathbb{K})$, para cada $i, 1 \leq i \leq m$. Tendremos que $a_{i,1} \neq a_{j,1} \forall i \neq j$. Consideremos el polinomio

$$q_A(Y_1) = \prod_{i=1}^{\delta} (Y_1 - a_{i,1}) \in \mathbb{K}[X_1, \ldots, X_n, Z].$$

Por la definición de Φ, como $Y_1 \in \mathbb{K}[X_1, \ldots, X_m]$, entonces dada

$$\begin{aligned} \Phi^* : \mathbb{K}[\mathcal{W}] &\longrightarrow \mathbb{K}[V \times \mathbb{K}] \\ h &\longmapsto h \circ \Phi, \end{aligned}$$

tendremos que $\Phi^*(q_A) = q_A \in \mathbb{K}[\mathcal{W}]$. Tiene sentido, pues, considerar las dos localizaciones por $q_A(Y_1)$ y extender Φ^* a las localizaciones

$$\begin{aligned} \Phi^* : \mathbb{K}[\mathcal{W}]_{q_A} &\longrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A} \\ \frac{h}{q_A^r} &\longmapsto \frac{\Phi^*(b)}{q_A^r}. \end{aligned}$$

Para simplificar la notación, escribamos $q = q_A$ y probemos que Φ^* es un isomorfismo de anillos.

Recordemos que si R es un dominio de integridad $S \subseteq R$ es un sistema multiplicativamente cerrado, los ideales maximales de la localización $S^{-1}R$ son las extensiones de los ideales maximales de R. Ahora dado $q \in \mathbb{K}[X_1, \ldots, X_m]$ tendremos que

$$\mathbb{K}[V \times \mathbb{K}]_q = \mathbb{K}[V]_q[Z]$$

es un anillo de polinomios en la variable Z con coeficientes en $\mathbb{K}[V]_q$. Como $\mathbb{K}[V]_q$ es una localización de una $\mathbb{K}$-álgebra finitamente generada, los ideales maximales de $\mathbb{K}[V]_q$ son las localizaciones en q de algunos primos $\mathfrak{p} \in Spec(\mathbb{K}[V])$ tales que $q \notin \mathfrak{p}$. Ahora bien, si $\mathfrak{p} \in Spec(\mathbb{K}[V])$ es un ideal primo tal que $q \notin \mathfrak{p}$, entonces existe un punto $\underline{\alpha} \in V_{\mathbb{A}}(\mathfrak{p}) \subseteq V$ tal que $q(\underline{\alpha}) \neq 0$, como consecuencia del Nullstellenstaz. En ese caso, $\mathfrak{p} \subseteq \mathfrak{m}_{\underline{\alpha}}$, donde $\mathfrak{m}_{\underline{\alpha}} \subseteq \mathbb{K}[V]$ es el ideal maximal dado por la siguiente identidad:

$$\mathfrak{m}_{\underline{\alpha}} = \{f \in \mathbb{K}[V] : f(\underline{\alpha}) = 0\}.$$

En suma, los ideales maximales de $\mathbb{K}[V]_q$ son las extensiones de aquellos primos $\mathfrak{p} \in \mathbb{K}[V]$ que son maximales entre los que no contienen a q. Pero, por el Nullstellensatz, esos primos $\mathfrak{p} \in \mathbb{K}[V]$ maximales entre los que no contienen a q son precisamente los maximales asociados a puntos $\underline{\alpha}$ en el abierto distinguido $D(q)$. Formalmente,

$$Spm(\mathbb{K}[V]_q) = \{\mathfrak{m}_{\underline{\alpha}}^e : q(\underline{\alpha}) \neq 0\},$$

donde $\mathfrak{m}_{\underline{\alpha}}^e$ es la extensión a $\mathbb{K}[V]_q$ de $\mathfrak{m}_{\underline{\alpha}} \subseteq \mathbb{K}[V]$.

Consideramos ahora el ideal generado por $\{f_1, \ldots, f_n\}$ en $\mathbb{K}[V]_q$ que denotaremos por $(f_1, \ldots, f_n)$. Si $(f_1, \ldots, f_n) \subsetneq \mathbb{K}[V]_q$ (esto es, si fuera un ideal propio), existiría $\underline{\alpha} \in V$ tal que $q(\underline{\alpha}) = q(\alpha_1) \neq 0$ y $(f_1, \ldots, f_n) \subseteq \mathfrak{m}_{\underline{\alpha}}^e$. Es decir, si $(f_1, \ldots, f_n)$ fuera un ideal propio tendría que estar contenido en algún ideal maximal de $\mathbb{K}[V]$. Pero, entonces, si $(f_1, \ldots, f_n) \subseteq \mathfrak{m}_{\underline{\alpha}}^e \Rightarrow f_i(\underline{\alpha}) = 0$ para cada $i, 1 \leq i \leq n$. Con lo que $\underline{\alpha} \in V \cap V_{\mathbb{A}}(f_1, \ldots, f_n) = A$. Recordando ahora que $q_A = \prod_{i=1}^{\delta}(Y_1 - a_{i,1})$ concluiríamos que $\exists i : \underline{\alpha} = a_i$ (porque $\underline{\alpha} \in A$) y $q_A(\underline{\alpha}) = 0$, con lo que $q = q_A \in \mathfrak{m}_{\underline{\alpha}}$ contradiciendo

la hipótesis de que $q_A \notin \mathfrak{m}_{\underline{\alpha}}$. Por tanto, $(f_1, \ldots, f_n)$ no es un ideal propio en $\mathbb{K}[V]_q$. Por tanto, existen $A_1, \ldots, A_n \in \mathbb{K}[V]_q$ tales que

$$1 = \sum_{i=1}^{n} A_i f_i \in (f_1, \ldots, f_n). \tag{2.2.4}$$

Como $A_i = \frac{b_i}{q^r}$ para algún $r \in \mathbb{N}$ común a todos ellos y algún $b_i \in \mathbb{K}[V]$, tendremos también

$$q^r = \sum_{i=1}^{n} b_i f_i \text{ en } \mathbb{K}[V].$$

La identidad 2.2.4 permite probar, de modo análogo a la prueba de la Afirmación de la Parte 1 de la Demostración del Teorema 1.3.3, que Φ es una biyección entre los abiertos distinguidos

$$D_{V\times\mathbb{K}}(q) = \{(x,z) \in V \times \mathbb{K} : q(x) \neq 0\},$$
$$D_q(\mathcal{W}) = \{(x,y) \in \mathcal{W} : q(x) \neq 0\},$$

y, además, que Φ es un isomorfismo birregular entre ambos localmente cerrados. Dicho de otra forma

$$\Phi^* : \mathbb{K}[\mathcal{W}]_q \to \mathbb{K}[V \times \mathbb{K}]_q$$

es monomorfismo de anillos porque ya lo era $\Phi^* : \mathbb{K}[\mathcal{W}] \longrightarrow \mathbb{K}[V]$ por ser Φ dominante. De otro lado, los polinomios

$$H_{i,j}(X_1, \ldots, X_m, Y_1, \ldots, Y_n) = f_i(X_1, \ldots, X_m)Y_j - f_j(X_1, \ldots, X_m)Y_i \in I(\mathcal{W})$$

por la propia definición de $I(\mathcal{W})$. Observemos que el morfismo Φ^* viene dado por la forma siguiente donde $\bar{\cdot}$ significa clase módulo $I(\mathcal{W})$ o $I(V \times \mathbb{K})$ según el caso.

Tenemos que

$$\Phi^*(\overline{X_i}) = \overline{X}_i, 1 \leq i \leq m$$
$$\Phi^*(\overline{f_j(X_1, \ldots, X_m)}) = \overline{f_j}, 1 \leq j \leq n$$

porque Φ deja invariantes las coordenadas $X_1, \ldots, X_m$ y $f_j(X_1, \ldots, X_m)$ está en $\mathbb{K}[X_1, \ldots, X_m]$.

De otro lado,

$$\Phi^*(\overline{Y_i}) = \overline{f_i Z}$$

Y además, tenemos

$$1 = \sum_{i=1}^{n} \overline{A_i f_i}.$$

Veamos que

$$\overline{Z} - \Phi^*(\sum_{j=1}^{n} \overline{A_j Y_j}) = 0 \text{ en } \mathbb{K}[V]_q. \tag{2.2.5}$$

La prueba es análoga a la ya citada Parte 1 del Teorema 1.3.3, aunque simplificada:

$$\Phi^*\left(\sum_{j=1}^{n} \overline{A_j Y_j}\right) = \sum_{j=1}^{n} \Phi^*(\overline{A_j})\Phi^*(\overline{Y_j}) = \sum_{j=1}^{n} \overline{A_j f_j Z}.$$

Luego

$$\Phi^*(\sum_{j=1}^{n} \overline{A_j Y_j}) = \overline{Z}(\sum_{j=1}^{n} \overline{A_j f_j}) = \overline{Z} \text{ en } \mathbb{K}[V \times \mathbb{K}]_q.$$

Como $\overline{X_i} = \Phi^*(\overline{X_i}), 1 \leq i \leq m$ y por 2.2.5, $\overline{Z} = \Phi^*(\sum_j \overline{A_j Y_j})$, tendremos que $\{\overline{X_1}, \ldots, \overline{X_m}, \overline{Z}\} \subseteq \Phi^*(\mathbb{K}[\mathcal{W}]_q)$. Finalmente, todo elemento de $\mathbb{K}[V \times \mathbb{K}]_q$ tiene la forma

$$u = \frac{P[\overline{X_1}, \ldots, \overline{X_m}, \overline{Z}]}{q^t}.$$

□

En la línea del Lema 1.2.4, sean dados $m \neq n \in \mathbb{N}$ dos enteros positivos. Consideremos el conjunto de matrices con (n+1) filas y (m+n) columnas $\mathscr{M}_{(n+1)\times(m+n)}(\mathbb{K})$. Y consideremos el subconjunto formado por las matrices que tienen la estructura siguiente:

$$T_{(n+1)\times(m+n)}(\mathbb{K}) = \left\{ \left(\begin{array}{ccccc|ccc} 1 & a_{1,2} & \dots & a_{1,n} & a_{1,n+1} & a_{1,n+2} & \dots & a_{1,n+m} \\ & 1 & & & & & & \\ & & \ddots & & \vdots & & & \\ & 0 & & 1 & a_{n,n+1} & & & \\ & & & & 1 & a_{n+1,n+2} & \dots & a_{n+1,m+n} \end{array} \right) : a_{ij} \in \mathbb{K} \right\}$$

Podemos identificar $T_{(n+1)\times(m+n)}(\mathbb{K})$ con el espacio afín $\mathbb{A}^t(\mathbb{K})$ donde

$$t = \frac{n(n+1)}{2} + (n+1)(m-1).$$

Es decir, t es el número de constantes libres en las matrices de la forma dada por $T_{(n+1)\times(m+n)}(\mathbb{K})$. De hecho, al ser como un espacio afín, podemos hablar de los abiertos Zariski en $T_{(n+1)\times(m+n)}(\mathbb{K})$ y referirnos a abiertos Zariski en $\mathbb{A}^t(\mathbb{K})$ que definen las matrices en $T_{(n+1)\times(m+n)}(\mathbb{K})$.

LEMA 2.2.4. *Sea $\mathcal{W} \subseteq \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible de dimensión n+1. Entonces, existe un abierto Zariski no vacío $\mathcal{U}' \subseteq T_{n+1,m+n}(\mathbb{K})$ tal que para cada matriz $M \in \mathcal{U}$, las formas lineales*

$$\begin{pmatrix} T_1 \\ \vdots \\ T_{n+1} \end{pmatrix} = M \cdot \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \\ X_1 \\ \vdots \\ X_m \end{pmatrix},$$

verifican que $\{T_1, \dots, T_{n+1}\}$ son algebraicamente independientes sobre $\mathbb{K}$ y la siguiente es una extensión entera de anillos

$$\mathbb{K}[T_1, \dots, T_{n+1}] \hookrightarrow \mathbb{K}[\mathcal{W}].$$

DEMOSTRACIÓN. Por el Lema de Normalización de Noether (ver el Teorema A.4.8), existe un abierto $\mathcal{U} \subseteq \mathscr{M}_{(n+1)\times(n+m)}(\mathbb{K})$ tal que para cada matriz $M \in \mathcal{U}$ las variables

$$\begin{pmatrix} T_1 \\ \vdots \\ T_{n+1} \end{pmatrix} = M \cdot \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \\ X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

están en posición de Noether con respecto a $\mathcal{W}$. De otro lado, el Lema 1.2.4 nos dice que hay matrices en $\mathcal{U}$ con la forma de matriz en $T_{(n+1)\times(m+n)}(\mathbb{K})$ que definen una normalización de Noether de $\mathcal{W}$. En particular, tendremos que

$$\mathcal{U} \cap T_{(n+1)\times(m+n)}(\mathbb{K}) \neq \emptyset.$$

Claramente $\mathcal{U} \cap T_{(n+1)\times(m+n)}(\mathbb{K})$ es un abierto Zariski no vacío y satisface la tesis del Lema. □

Obsérvese que T_{n+1} es una forma lineal que sólo depende de las variables $\{X_1, \dots, X_m\}$. Esto implica el siguiente:

COROLLARIO 2.2.5. *Sea $\mathcal{W} \subseteq \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible de dimensión $n+1$. Sea $A \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica cero dimensional (i.e. un conjunto finito de puntos) tal que $A \times \{0\}^n \subseteq \mathcal{W}$.*

Entonces, existe un abierto Zariski $\mathcal{U} \subseteq T_{(n+1)\times(n+m)}$ *tal que para cada* $B \in \mathcal{U}$ *se verifica lo siguiente: Sean* $\{T_1, \ldots, T_{n+1}\}$ *las formas lineales dadas por*

$$\begin{pmatrix} T_1 \\ \vdots \\ T_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \\ X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

de tal manera que:

i) $\{T_1, \ldots, T_{n+1}\}$ *son algebraicamente independientes sobre* $\mathbb{K}$.

ii) $T_{n+1} = X_1 + b_{n+1,2}X_2 + \cdots + b_{n+1,m}X_m \in \mathbb{K}[X_1, \ldots, X_m]$ *es una forma lineal en* $\mathbb{K}[X_1, \ldots, X_m]$ *que separa los puntos de* A.

iii) La siguiente es una extensión entera de anillos

$$\mathbb{K}[T_1, \ldots, T_{n+1}] \hookrightarrow \mathbb{K}[\mathcal{W}].$$

Demostración. Basta con combinar el Lema 2.2.4 precedente con una condición abierta en los elementos de la última fila: $(0, \ldots, 0, 1, b_{n+1,2}, \ldots, b_{n+1,m})$. Para ello consideramos

$$A = \{a_1, \ldots, a_\delta\},$$

de tal modo que para cada $i, 1 \leq i \leq \delta, a_i = (a_{i,1}, \ldots, a_{1,m})$. Consideremos los polinomios no nulos en variables $\{u_2, \ldots, u_m\}$ algebraicamente independientes sobre $\mathbb{K}$:

$$G_{ij}(u_2, \ldots, u_m) = (a_{i,1} - a_{j,1}) + (a_{i,2} - a_{j,2})u_2 + \cdots + (a_{i,m} - a_{j,m})u_m.$$

Es no nulo porque no todos sus coeficientes (en $u_2, \ldots, u_m$ o en 1) son idénticamente nulos. Definamos

$$G_A(u_2, \ldots, u_m) = \prod_{i \neq j} G_{ij}(u_2, \ldots, u_m).$$

Ahora, dado $\mathcal{U}' \subseteq T_{(n+1)\times(n+m)}(\mathbb{K})$ el abierto Zariski del Lema 2.2.4 precedente y definimos

$$\mathcal{U} := \mathcal{U}' \cap \{B \in T_{(n+1)\times(n+m)}(\mathbb{K}) : G_A(b_{n+1,2}, \ldots, b_{n+1,m}) \neq 0\}.$$

Si $G_A(\theta_2, \ldots, \theta_m) \neq 0$ la forma lineal

$$l_\theta = X_1 + \theta_2 X_2 + \cdots + \theta_m X_m$$

separa los puntos de A con lo que toda matriz $B \in \mathcal{U}$ satisface las propiedades indicadas en el enunciado. □

Proposición 2.2.6. *Sea* $V \subseteq \mathbb{A}^m(\mathbb{K})$ *una variedad algebraica irreducible de dimensión* n *y grado* D. *Sean* $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ *polinomios con* $k \leq n$ *tales que* $A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_k)$ *es una variedad algebraica cero-dimensional. Entonces, se tiene:*

i) $k = n$.

ii) Sea $\Phi : V \times \mathbb{K} \longrightarrow \mathbb{A}^m(\mathbb{K}) \times \mathbb{A}^n(\mathbb{K})$ *el morfismo dado mediante:*

$$\Phi(x_1, \ldots, x_m, z) = (x_1, \ldots, x_m, f_1(x)z, \ldots, f_n(x)z).$$

La clausura Zariski de la imagen $\mathcal{W} = \overline{\Phi(V \times \mathbb{K})}^z$ *es una variedad algebraica irreducible de dimensión* $n+1$ *y* $\Phi : V \times \mathbb{K} \longrightarrow \mathcal{W}$ *es un morfismo dominante.*

iii) Existe un abierto Zariski $\mathcal{U}_2 \subseteq T_{(n+1)\times(n+m)}(\mathbb{K})$ *tal que para cada matriz* $M \in \mathcal{U}_2$, *el cambio de variables*

$$\begin{pmatrix} T_1 \\ \vdots \\ T_{n+1} \end{pmatrix} = M \cdot \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \\ X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

verifica

iii)-1 $\{T_1, \ldots, T_{n+1}\}$ *son algebraicamente independientes sobre* $\mathbb{K}$, *con* $T_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$.

iii)-2 La siguiente es una extensión entera de anillos

$$\Pi^* : \mathbb{K}[T_1, \ldots, T_{n+1}] \hookrightarrow \mathbb{K}[\mathcal{W}].$$

iii)-3 La forma lineal $T_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$ es una forma separante sobre A.

iv) Existe un polinomio univariado $q_A \in \mathbb{K}[T]$ tal que $\deg(q_A) \leq D \prod_{i=1}^{k} \deg(f_i)$, $q_A(T_{n+1}) \notin I(V)$ y la siguiente es una extensión entera de anillos:

$$\Phi^* \circ \Pi^* : \mathbb{K}[T_1, \ldots, T_{n+1}]_{q_A} \hookrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A}.$$

Demostración. Probemos, en primer lugar, que $k = n$.
En primer lugar, como $A \cap V_{\mathbb{A}}(f_1, \ldots, f_k) \neq \emptyset$, por el Teorema del Ideal Principal de Krull (ver Teorema A.2.5), tendremos que $V_{\mathbb{A}}(f_1, \ldots, f_k) \neq 0$ y $\dim V_{\mathbb{A}}(f_1, \ldots, f_k) \geq m - k$. De otro lado, $\dim(V) = n$ y $A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) \neq \emptyset$, luego por el Teorema de la Dimensión de la Intersección (ver Teorema B.1.5) tendremos que toda componente irreducible C de $A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) \neq \emptyset$ satisface

$$\dim(C) \geq \dim(V) + \dim(V_{\mathbb{A}}(f_1, \ldots, f_k)) - m \geq n + (m - k) - m = n - k.$$

Como A es un conjunto finito de puntos (y cero-dimensional) toda componente irreducible de A tiene dimensión cero, con lo que habremos probado que $0 \geq n - k$ o, equivalentemente, $n \leq k$. Como, por hipótesis, $k \leq n$, tendremos $k = n$ y habremos probado *i*).
Para la Propiedad *ii*), ésta se sigue de la Proposición 2.2.3 probada en páginas precedentes, dado que $k = n$.
La Propiedad *iii*) se sigue, en sus tres aspectos, del Corolario 2.2.5, probado en páginas anteriores.
La propiedad *iv*) es la que buscamos. Para empezar, obsérvese que T_{n+1} es una forma lineal que sólo depende de las variables $\{X_1, \ldots, X_m\}$ y que está en $\mathbb{K}[X_1, \ldots, X_m]$. Además,

$$T_{n+1} = l(X_1, \ldots, X_m) = X_1 + b_{n+1,1}X_2 + \cdots + b_{n+1,m}X_m,$$

satisface que $l(a) \neq l(a') \forall a, a' \in A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_n)$, con $a \neq a'$. Considero el polinomio

$$q_A(\mathcal{U}) = \prod_{i=1}^{\delta} (\mathcal{U} - l(a_i)),$$

donde $A = \{a_1, \ldots, a_\delta\}$ con $\delta \leq \deg(A) \leq D \prod_{i=1}^{n} \deg(f_i)$. Tenemos que $q_A(T_{n+1}) \in \mathbb{K}[V]$ y, por tanto, en $\mathbb{K}[V \times \mathbb{K}]$. Además, $q_A(T_{n+1}) \notin I(V)$. En otro caso, $q_A(T_{n+1}) \in I(V \times \mathbb{K})$, $\Phi^*(q_A) = q_A$ (porque $q_A \in \mathbb{K}[X_1, \ldots, X_m]$) y tendríamos que $q_A \in I(\mathcal{W})$. Pero si $q_A \in I(\mathcal{W})$, entonces $\Pi(\mathcal{W}) \subseteq \{(t_1, \ldots, t_{n+1}) \in \mathbb{A}^{n+1}(\mathbb{K}) : q_A(t_{n+1}) = 0\} = S$. Pero $q_A \in \mathbb{K}[T_1, \ldots, T_{n+1}]$ es un polinomio no nulo, luego, por la Proposición B.2.10 , $\Pi(\mathcal{W})$ estaría contenido en una hipersuperficie de $\mathbb{A}^{n+1}(\mathbb{K})$ de dimensión $(n+1) - 1 = n$, lo que contradice el hecho de que $\Pi(\mathcal{W}) = \mathbb{A}^{n+1}(\mathbb{K})$. En particular, $q_A(T_{n+1})$ verifica que:

- Su clase módulo $I(V \times \mathbb{K})$ en $\mathbb{K}[V \times \mathbb{K}]$ es no nulo y, por tanto, no es divisor de cero ni nilpotente porque $\mathbb{K}[V \times \mathbb{K}]$ es un dominio de integridad.
- $\Phi^*(\overline{q_A}) = q_A(T_{n+1}) \in \mathbb{K}[\mathcal{W}]$ es no nulo y no es divisor de cero ni nilpotente en $\mathbb{K}[\mathcal{W}]$.
- $\Pi^*(\overline{q_A}) = q_A(T_{n+1}) \in \mathbb{K}[T_1, \ldots, T_{n+1}]$ es no divisor de cero ni es nilpotente.

Tienen sentido considerar las localizaciones

$$\mathbb{K}[T_1, \ldots, T_{n+1}]_{q_A}, \mathbb{K}[\mathcal{W}]_{q_A}, \mathbb{K}[V \times \mathbb{K}]_{q_A}.$$

Tenemos que

$$\Phi^* : \mathbb{K}[\mathcal{W}]_{q_A} \longrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A},$$

es una biyección por la Proposición 2.2.3. Como $\Pi^* : \mathbb{K}[T_1, \ldots, T_{n+1}] \hookrightarrow \mathbb{K}[\mathcal{W}]$ es una extensión entera de anillos, localizando por $\{q_A^n : n \in \mathbb{N}\}$, la siguiente es una extensión entera de anillos

$$\Pi^* : \mathbb{K}[T_1, \ldots, T_{n+1}]_{q_A} \hookrightarrow \mathbb{K}[\mathcal{W}]_{q_A}.$$

Definiendo $\Psi = \pi \circ \Phi : V \times \mathbb{K} \longrightarrow \mathbb{A}^{n+1}(\mathbb{K})$, tendremos que

$$\Psi^* : \mathbb{K}[T_1, \ldots, T_{n+1}]_{q_A} \hookrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A}$$

es una extensión entera de anillos. □

COROLLARIO 2.2.7. *Con las notaciones de la Proposición precedente, sea $B \in \mathcal{U}_2$ una matriz en el abierto Zariski $\mathcal{U}_2 \subseteq T_{(n+1)\times(n+m)}(\mathbb{K})$, satisfaciendo las propiedades indicadas en iii). Sea $q_A(T_{n+1})$ el polinomio de la propiedad iv) y sea $\prod : \mathcal{W} \to \mathbb{A}^{n+1}(\mathbb{K})$ la aplicación suparayectiva definida por B. Sea*

$$\begin{aligned}\Psi : V \times \mathbb{K} &\longrightarrow \mathbb{A}^{n+1}(\mathbb{K})\\ (x,z) &\longmapsto \Pi(\Phi(x,z)).\end{aligned}$$

Entonces,

i) Ψ es un morfismo dominante.

ii) La extensión de cuerpos $\mathbb{K}(T_1,\ldots,T_{n+1}) \subseteq \mathbb{K}(V\times\mathbb{K})$ es algebraica.

iii) Para cada $H \in \mathbb{K}[V\times\mathbb{K}]$, sea $\tilde{P}_H \in \mathbb{K}(T_1,\ldots,T_{n+1})[\mathcal{U}]$ su polinomio mínimo (irreducible) sobre $\mathbb{K}(T_1,\ldots,T_{n+1})$. Sea $P_H \in \mathbb{K}[T_1,\ldots,T_{n+1}][\mathcal{U}]$ el polinomio primitivo irreducible asociado a $\tilde{P}_H$ por el Lema de Gauss. Entonces

$$P_H(T_1,\ldots,T_{n+1},\mathcal{U}) = P_D(T_{n+1})\mathcal{U}^D + \sum_{i=0}^{D-1} P_i(T_1,\ldots,T_{n+1})\mathcal{U}^i.$$

Es decir, el coeficiente director de P_H es un polinomio univariado dependiendo solamente de la variable T_{n+1}.

iv) Además

$$\{t \in \mathbb{K} : P_D(t) = 0\} \subseteq \{t \in \mathbb{K} : q_A(t) = 0\}.$$

DEMOSTRACIÓN. i) Como Ψ es la composición de un morfismo dominante con una aplicación suprayectiva, se tiene que sigue siendo un morfismo dominante.

ii) Por la Proposición 2.2.6 precedente tenemos una extensión entera de anillos

$$\Phi^* : \mathbb{K}[T_1,\ldots,T_{n+1}]_{q_A(T_{n+1})} \hookrightarrow \mathbb{K}[V\times\mathbb{K}]_{q_A(T_{n+1})}.$$

Pasando a cuerpos de fracciones, como

$$\begin{aligned}qf(\mathbb{K}[T_1,\ldots,T_{n+1}]_{q_A(T_{n+1})}) &= \mathbb{K}(T_1,\ldots,T_{n+1})\\ qf(\mathbb{K}[V\times\mathbb{K}]_{q_A(T_{n+1})}) &= \mathbb{K}(V\times\mathbb{K}),\end{aligned}$$

tendremos una extensión algebraica de cuerpos, que será finita en grado.

iii) Ahora, dado $H \in \mathbb{K}[V\times\mathbb{K}]$, como Ψ^* define una extensión entera, existirá un polinomio mónico con coeficientes en $\mathbb{K}[T_1,\ldots,T_{n+1}]_{q_A}$ de la forma siguiente:

$$q_H(\mathcal{U}) = \mathcal{U}^D + \sum_{i=0}^{D-1} Q_i\mathcal{U}^i,$$

tal que $q_H(H) = 0$ en $\mathbb{K}[V\times\mathbb{K}]_{q_A}$. El polinomio mínimo mónico de la forma q_H tiene que ser un polinomio irreducible y, por tanto, q_H ha de ser asociado a $\tilde{P}_H$. Pero como ambos son mónicos, la extensión es entera y ambos son irreducibles, tendremos que

$$q_H = \tilde{P}_H.$$

Ahora observemos que existen polinomios $q_i(T_1,\ldots,T_{n+1}) \in \mathbb{K}[T_1,\ldots,T_{n+1}]$ y existe $r \in \mathbb{N}$ tales que

$$Q_i = \frac{q_i}{q_A^r}.$$

Definamos $\tilde{q}_H$ al polinomio

$$\tilde{q}_H = q_A^r\mathcal{U}^D + \sum_{i=0}^{D-1} q_i\mathcal{U}^i = q_A^r q_H \in \mathbb{K}[T_1,\ldots,T_{n+1}][\mathcal{U}].$$

Por el Lema de Gauss, existe el máximo común divisor de los coeficientes de $\tilde{q}_H$ y dejemos su parte principal. Sea

$$\begin{aligned}P_H = pp(\tilde{q}_H) = P_0\mathcal{U}^D + \sum_{i=0}^{D-1} P_i\mathcal{U}^i,\\ c = cont(\tilde{q}_H),\end{aligned}$$

de tal modo que $\tilde{q}_H = cP_H$. Entonces

- $c \in \mathbb{K}[T_{n+1}]$ por ser un divisor de $q_A^r(T_{n+1})$.
- $P_0 \in \mathbb{K}[T_{n+1}]$ por ser un divisor de $q_A^r(T_{n+1})$.
- $P_H \in \mathbb{K}[T_1, \ldots, T_{n+1}][\mathcal{U}]$ es irreducible (por ser asociado a $\tilde{P}_H$ y ser primitivo, aplicando el Lema de Gauss).

iv) Como $P_0 | q_A^r(T_{n+1})$, entonces

$$\{t \in \mathbb{K} : p_0(t) = 0\} \subseteq \{t \in \mathbb{K} : q_A(t) = 0\}.$$

□

TEOREMA 2.2.8. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica irreducible de dimensión n y grado D. Sean $k \leq n$ y $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios tales que la siguiente variedad es cero-dimensional:*

$$A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_k).$$

Entonces, existe un abierto Zariski $\mathcal{U}_1 \subseteq \mathscr{M}_m(\mathbb{K})$ formado por matrices regulares tales que para cada $B \in \mathcal{U}_1$, el cambio de variables que determina:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix},$$

satisface las siguientes propiedades:

i) Y_1 es un elemento separante sobre A y existe un polinomio univariado $\Phi_1(T)$ tal que si $\Phi_1(z) = 0$, entonces $\exists a \in A$ tal que

$$z = Y_1(a).$$

ii) Existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que

$$\Phi_1(Y_1) - \sum_{i=1}^{k} g_i f_i \in I(V).$$

iii) $\deg(g_i f_i) \leq D \cdot \prod_{i=1}^{k} \deg(f_i)$, $\deg(\Phi_1(Y_1)) \leq D \prod_{i=1}^{k} \deg(f_i)$.

DEMOSTRACIÓN. Usaremos los resultados precedentes y sabemos que, bajo nuestras hipótesis, $k = n$. Además, hay un abierto Zariski de normalización de Noether de $\Phi(V \times \mathbb{K})$ tales que $T_{n+1} = Y_1$ es un elemento separante de A. Además, tomamos el polinomio univariado $q_A(\mathcal{U}) = \mathbb{K}[\mathcal{U}]$ tal que

$$q_A(T_{n+1}) = q_A(Y_1) = \prod_{a \in A} (Y_1 - Y_1(a)),$$

donde $Y_1(a)$ es el resultado de aplicar la forma lineal Y_1 al punto a, es decir

$$\begin{pmatrix} Y_1(a) \\ \vdots \\ Y_m(a) \end{pmatrix} = B \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \forall a = (a_1, \ldots, a_m) \in \mathbb{A}^m(\mathbb{K}).$$

Luego $q_A(Y_1(a)) = 0, \forall a \in A$. Además, la siguiente es una extensión entera de anillos

$$\Phi^* : \mathbb{K}[T_1, \ldots, T_{n+1}]_{q_A(T_{n+1})} \hookrightarrow \mathbb{K}[V \times \mathbb{K}]_{q_A(Y_1)},$$

Si consideramos $P_Z \in \mathbb{K}[T_1, \ldots, T_{n+1}][\mathcal{U}]$ el polinomio mínimo primitivo de Z sobre $\mathbb{K}[T_1, \ldots, T_{n+1}]$ que, por el Corolario 2.2.7 precedente, tiene la forma

$$P_Z(T_1, \ldots, T_{n+1}, \mathcal{U}) = P_N(T_{n+1})\mathcal{U}^N + \sum_{i=0}^{N-1} P_i(T_1, \ldots, T_{n+1})\mathcal{U}^i,$$

donde P_N es un polinomio univariado, dependiendo solamente de la variable T_{n+1} y tal que P_N es un divisor de $(q_A(T_{n+1}))^r$ para algún $r \in \mathbb{N}$. Obviamente, si $z \in \mathbb{K}$ es tal que $P_N(z) = 0 \Rightarrow q_A(z) = 0$, luego, por construcción de $q_A(z)$ tendremos que $\exists a \in A$ con $z = Y_1(a)$.
Elijamos $\Phi_1 := P_N(Y_1)$. A partir de aquí procederemos como en la Demostración del Teorema 1.3.3. Consideremos el polinomio:

$$q(X_1, \ldots, X_m, Z) = P_Z(\Psi_1, \ldots, \Psi_{n+1}, Z) \in \mathbb{K}[X_1, \ldots, X_m][Z],$$

donde

$$\Psi = (\Psi_1, \ldots, \Psi_{n+1}) = \Pi \circ \Phi,$$

para una normalización de Noether Π de $\mathcal{W} = \overline{\Phi(V \times \mathbb{K})}^z$ tal que $\Pi = (T_1, \ldots, T_{n+1})$ con $T_{n+1} = Y_1$. Entonces, podremos escribir

$$q(X_1, \ldots, X_m, Z) = (P_N(Y_1) + A_N)Z^N + \sum_{r \neq N} A_r Z^r,$$

y $q(X_1, \ldots, X_m, Z) \in I(V \times \mathbb{K})$ o, equivalentemente,

- $(P_N(Y_1) + A_N) \in I(V)$.
- $A_r \in I(V), \forall r \neq N$.

Siguiendo exactamente los mismos argumentos que en el Nullstellensatz Efectivo subdeterminado (Teorema 1.3.3 precedente) concluiremos que existen $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que

$$A_N = \sum_{i=1}^{k} g_i f_i,$$

con $\deg(g_i f_i) \leq D \prod_{i=1}^{k} \deg(f_i)$. Con lo cual habríamos probado las propiedades 2 y 3 del enunicado para $\Phi_1(Y_1) = P_N(Y_1)$. Queda por ver que $\deg_{Y_1}(\Phi_1) \leq D \prod_{i=1}^{n} \deg(f_i)$. Procedemos como en el Teorema 1.3.3. Consideremos el cuerpo $\mathbb{L} = \mathbb{K}(Z)$ y los polinomios $\Psi_1, \ldots, \Psi_{n+1} \in \mathbb{L}[X_1, \ldots, X_m]$. Por el Teorema de Perron Generalizado, aplicado como en la demostración del Teorema 1.3.3, existe un polinomio $W'(T_1, \ldots, T_{n+1}, \mathcal{U}) \in \mathbb{K}[T_1, \ldots, T_{n+1}, \mathcal{U}]$ tal que se verifica lo siguiente:

i) $W'(\Psi_1, \ldots, \Psi_{n+1}, Z) = 0$ en $\mathbb{K}[V \times \mathbb{K}]$.
ii) $\deg_T(W'(T_1^{d_1}, \ldots, T_n^{d_n}, T_{n+1}, \mathcal{U})) \leq D \prod_{i=1}^{n} d_i$.

Ahora como $P_Z(T_1, \ldots, T_{n+1}, \mathcal{U})$ es el polinomio mónico primitivo de Z sobre $\mathbb{K}[T_1, \ldots, T_{n+1}]$, tendremos que $P_Z | W'$ y, por tanto,

$$\deg_T(P_Z(T_1^{d_1}, \ldots, T_n^{d_n}, T_{n+1}, \mathcal{U})) \leq \deg_T(W'(T_1^{d_1}, \ldots, T_n^{d_n}, T_{n+1}, \mathcal{U})) \leq D \prod_{i=1}^{n} d_i.$$

En particular, como

$$P_Z = P_N(T_{n+1})\mathcal{U}^n + \sum_{i=0}^{N-1} P_i(T_1, \ldots, T_{n+1})\mathcal{U}^i,$$

tendremos que

$$\deg_{Y_1}(\Phi_1) = \deg_{T_{n+1}}(P_N) \leq \deg_T(P_Z(T_1^{d_1}, \ldots, T_n^{d_n}, T_{n+1}, \mathcal{U})) \leq D \prod_{i=1}^{n} d_i.$$

□

Corollario 2.2.9 (**Teorema de Eliminación de [Je, 2005]**). *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica irreducible de dimensión n y grado D. Sean $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios de grados respectivos $d_1 = \deg(f_1), \ldots, d_k = \deg(f_k)$ con $k \leq n$. Supongamos que la siguiente intersección*

$$A = V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) \subseteq \mathbb{A}^m(\mathbb{K}),$$

es una variedad algebraica cero dimensional (i.e. un conjunto finito de puntos).
Entonces, existe un abierto Zariski de matrices regulares $\mathcal{U} \subseteq \mathscr{M}_m(\mathbb{K})$ tal que para cada $B \in \mathcal{U}$ se verifica las siguientes propiedades: Sean $\{Y_1, \ldots, Y_m\}$ las variables determinadas por B y las variables originales $\{X_1, \ldots, X_m\}$ mediante:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

Cada $Y_1, \ldots, Y_m$ es una forma lineal en las coordenadas originales de los puntos y para cada punto $\underline{x} = (x_1, \ldots, x_m) \in \mathbb{A}^m(\mathbb{K})$ denotamos

$$\begin{pmatrix} Y_1(\underline{x}) \\ \vdots \\ Y_m(\underline{x}) \end{pmatrix} = B \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Entonces se verifica:

i) Para cada $i, 1 \leq i \leq m, Y_i$ es una forma separante de la variedad cero-dimensional A.

ii) Para cada $i, 1 \leq i \leq m$, existe un polinomio univariado $\Phi_i \in \mathbb{K}[T]$, $\deg(\Phi_i) \leq D \prod_{i=1}^{k} \deg(f_i)$, tal que $\forall z \in \mathbb{K}$, si $\Phi(z) = 0$, entonces $\exists \underline{a} \in A$ tal que $z = \Phi_i(Y_i(\underline{a}))$.

iii) Para cada $i, 1 \leq i \leq m$, existen polinomios $\{g_{i,1}, \ldots, g_{i,k}\} \subseteq \mathbb{K}[X_1, \ldots, X_m]$ tales que

- *$\Phi_i(Y_i) - \sum_{j=1}^{k} g_{i,k} f_k \in I(V)$.*
- *$\deg(g_{i,j} f_j) \leq D \prod_{r=1}^{k} d_r$.*

Demostración. El resultado se sigue de modo casi inmediato del Teorema precedente. Cambiando el subíndice 1 por cualquier otro índice $i \in \{1, \ldots, m\}$, repitiendo la demostración para Y_i, concluiríamos que existe un abierto $\mathcal{U}_i \subseteq \mathscr{M}_m(\mathbb{K})$ un abierto Zariski no vacío de matrices $m \times m$ regulares tal que para cada $B \in \mathcal{U}_i$ el cambio de variables

$$\begin{pmatrix} Y_1(\underline{x}) \\ \vdots \\ Y_m(\underline{x}) \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix}.$$

verifica:

i) La nueva variable Y_i es un elemento separante de A y existe un polinomio univariado $\Phi_i \in \mathbb{K}[T]$ tal que para cada $z \in \mathbb{K}$ si $\Phi_i(z) = 0$, existe $a \in A$ tal que $z = Y_i(a)$. Además, $\deg(\Phi_i) \leq D \prod_{r=1}^{n} \deg(f_i)$.

ii) Existen polinomios $g_{i,1} \ldots, g_{i,k} \in \mathbb{K}[X_1, \ldots, X_m]$ tales que

- $\Phi_i(Y_i) - \sum_{r=1}^{k} g_{i,r} f_r \in I(V)$.
- $\deg(g_{i,r} f_r) \leq D \prod_{j=1}^{k} d_j$.

Como $\mathscr{M}_m(\mathbb{K}) = \mathbb{A}^{m^2}(\mathbb{K})$ es irreducible, todos los abiertos Zariski son densos y todo intersección de dos abiertos Zariski es no vacía. Por tanto, el conjunto

$$\mathcal{U} := \cap_{i=1}^{m} \mathcal{U}_i \subseteq \mathscr{M}_m(\mathbb{K})$$

es un abierto Zariski no vacío. Obviamente, cada matriz $B \in \mathcal{U}$ es una matriz no singular y la colección $\{\Phi_1(Y_1), \ldots, \Phi_m(Y_m)\}$ satisface la tesis del enunciado.

□

2.3. El Nullstellensatz Efectivo de [Je, 2005]

Comencemos probando algunos resultados preliminares.

Lema 2.3.1. *Sean $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_n]$ polinomios no nulos y no constantes tales que*

- *Para cada $i, 1 \leq i \leq k$, se tiene $d_i = \deg(f_i)$ y, además,*

$$d_1 > d_2 > \cdots > d_k.$$

- *$V_{\mathbb{A}}(f_1, \ldots, f_k) = \emptyset$.*

Si $k \geq n + 1$, existe una matriz con $n + 1$ filas y k columnas triangular superior de la forma siguiente:

$$B = \begin{pmatrix} 1 & b_{1,2} & \ldots & b_{1,k} & b_{1,n+1} & b_{1,n+2} & \ldots & b_{1,k} \\ & b_{2,2} & \ldots & b_{2,k} & b_{2,n+1} & b_{2,n+2} & \ldots & b_{2,k} \\ & & \ddots & & \vdots & \vdots & & \vdots \\ & \mathit{0} & & b_{n,n} & b_{n,n+1} & b_{n,n+2} & \ldots & b_{n,k} \\ & & & & b_{n+1,n+1} & b_{n+1,n+2} & \ldots & b_{n+1,k} \end{pmatrix},$$

tal que $\prod_{i=2}^{n+1} b_{i,i} \neq 0$ *(i.e. la matriz tiene rango* $n+1$ *y los elementos de la diagonal principal son no nulos) y si consideramos la familia de polinomios*

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix}$$

verifican:

i) $\deg(g_i) = d_i, 1 \leq i \leq n+1$.
ii) $V_{\mathbb{A}}(g_1, \ldots, g_{n+1}) = \emptyset$.

Demostración. Construyamos la matriz B inductivamente, fila por fila, del modo siguiente: Para la primera fila, como f_1 es un polinomio no nulo y no constate, por la Proposición B.2.10 cada componente irreducible de la hipersuperfice $V_{\mathbb{A}}(f_1)$ tiene dimensión $n-1$. Como $V_{\mathbb{A}}(f_1, \ldots, f_k) = \emptyset$, si C es una componente irreducible de $V_{\mathbb{A}}(f_1)$, entonces existe $i, 2 \leq i \leq k$, tal que f_i no se anula idénticamente en C. En caso contrario, si $f_i|_C \equiv 0$ para cada $i, 2 \leq i \leq k$, tendríamos que $C \equiv V_{\mathbb{A}}(f_2, \ldots, f_k) \cap V_{\mathbb{A}}(f_1) \neq \emptyset$.
Supongamos entonces $x_C \in C$ tal que $x_C \notin V_{\mathbb{A}}(f_2, \ldots, f_k)$ y definamos $\mathcal{C}$ el conjunto (finito) de todas las componentes irreducibles de $V_{\mathbb{A}}(f_1)$. Definamos el polinomio en las variables $\{\mathcal{U}_2, \ldots, \mathcal{U}_k\}$ dado mediante

$$F_1(\mathcal{U}_2, \ldots, \mathcal{U}_k) = \prod_{C \in \mathcal{C}} (\mathcal{U}_2 f_2(x_C), \ldots, +\mathcal{U}_k f_k(x_C)).$$

Nótese que como, para cada $C \in \mathcal{C}, \exists i : f_i(x_C) \neq 0$, la forma lineal

$$u_2 f_2(x_C) + \cdots + u_k f_k(x_C) \neq 0.$$

Luego F_1 es un polinomio no nulo. Sean $b_2, \ldots, b_k \in \mathbb{K}$ valores tales que $F_1(b_2, \ldots, b_k) \neq 0$, con $b_2 \neq 0$. Existen porque $\{F_1 \neq 0, u_2 \neq 0\}$ es un abierto Zariski no vacío en $\mathbb{A}^{n-1}(\mathbb{K})$.

$$\begin{aligned} g_1 &= f_1, \\ g_2 &= b_2 f_2 + \cdots + b_k f_k, \end{aligned}$$

$$B_2 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & b_2 & b_3 & \ldots & b_k \end{pmatrix}.$$

Se tiene que

i)

$$\begin{pmatrix} g_1 \\ g_2 \end{pmatrix} = B_2 \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix}.$$

ii) $V_{\mathbb{A}}(g_1, g_2, f_3, \ldots, f_k) = V_{\mathbb{A}}(f_1, f_2, f_3, \ldots, f_k) = \emptyset$. Como $b_2 \neq 0$, tendremos que

$$f_2 = b_2^{-1} g_2 - \sum_{i=2}^{k} b_2^{-1} b_i f_i \in (g_2, f_2, \ldots, f_k).$$

Luego $f_2 \in (g_1, g_2, f_3, \ldots, f_k) = (f_1, g_2, f_3, \ldots, f_k)$. Con lo que

$$(f_1, f_2, f_3, \ldots, f_k) \subseteq (g_1, g_2, f_3, \ldots, f_k).$$

Como, por definición, $(g_1, g_2, f_3, \ldots, f_k) \subseteq (f_1, f_2, f_3, \ldots, f_k)$ concluiremos que ambos ideales son iguales, luego

$$(g_1, g_2, f_3, \ldots, f_k) = (f_1, f_2, f_3, \ldots, f_k) \Rightarrow V_{\mathbb{A}}(g_1, g_2, f_3, \ldots, f_k) = V_{\mathbb{A}}(f_1, f_2, f_3, \ldots, f_k).$$

iii) $V_{\mathbb{A}}(g_1, g_2)$ es o bien vacío o su dimensión de Krull es $n-2$.

Supongamos que $V_{\mathbb{A}}(g_1, g_2) \neq \emptyset$, entonces g_2 no es divisor de cero en el anillo cociente

$$\mathbb{K}[X_1, \ldots, X_n] \Big/ (g_1) = \mathbb{K}[X_1, \ldots, X_n] \Big/ f_1.$$

Si g_2 fuera divisor de cero, existiría un ideal primo minimal $\mathfrak{p}$ sobre (f_1) tal que $g_2 \in \mathfrak{p}$. Pero si $\mathfrak{p}$ es minimal sobre (f_1), entonces $C = V_{\mathbb{A}}(\mathfrak{p})$ es una componente irreducible de

$V(f_1)$. Por tanto si $g_2 \in \mathfrak{p}$, tendremos $g_2(z) = 0, \forall z \in C$ y en particular $g_2(x_C) = 0$. Pero

$$F_1(b_2, \ldots, b_m) = g_2(x_C) \prod_{\substack{C' \in \mathcal{C} \\ C' \neq C}} g_2(x_{C'}) \neq 0,$$

lo que nos lleva a contradicción. Como g_2 no es divisor de cero en $\mathbb{K}[X_1, \ldots, X_m] / (g_1)$ por el Teorema del Ideal Principal de Krull (ver Teorema A.2.5), la altura de cualquier primo minimal sobre (g_1, g_2) es 2, luego para cada primo minimal $\mathfrak{p}$ sobre (g_1, g_2) se tendrá

$$\dim V_{\mathbb{A}}(\mathfrak{p}) = n - ht(\mathfrak{p}) = n - 2.$$

iv) Finalmente como $d_1 > d_2 > \cdots > d_k$,

$$\deg(g_2) = \deg(f_2) = d_2.$$

Supongamos, por hipótesis inductiva, que hemos constuido una matriz

$$B = \begin{pmatrix} 1 & b_{1,2} & \ldots & b_{1,r} & \ldots & b_{1,k} \\ & b_{2,2} & \ldots & b_{2,r} & \ldots & b_{2,k} \\ & & \ddots & \vdots & & \vdots \\ & 0 & & b_{r,r} & \ldots & b_{r,k} \end{pmatrix} \in \mathscr{M}_{r \times k}(\mathbb{K}),$$

tal que la secuencia de polinomios

$$\begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix}$$

verifica:

i) $V_{\mathbb{A}}(g_1, \ldots, g_r, f_{r+1}, \ldots, f_k) = \emptyset$.
ii) $\deg(g_i) = d_i$.
iii) $V_{\mathbb{A}}(g_1, \ldots, g_r)$ es o bien vacío o bien tiene dimensión $n - r \geq 0$.

Si $V_{\mathbb{A}}(g_1, \ldots, g_r) = \emptyset$ y $r \leq n + 1$, completando, si fuera necesario con $f_{r+1}, \ldots, f_{n+1}$.

$$g_i = f_i \text{ para } r + 1, \ldots, n + 1,$$

obtendríamos la familia $(g_1, \ldots, g_{n+1})$ con las propiedades pretendidas. Si, por el contrario, $V_{\mathbb{A}}(g_1, \ldots, g_r)$ tiene dimensión $n - r$, por el Teorema de la Pureza de Macaulay (ver Teorema B.2.11), todos los primos minimales sobre $(g_1, \ldots, g_r)$ tienen altura r y todas las componentes irreducibles C de $V_{\mathbb{A}}(g_1, \ldots, g_r)$ tienen dimensión $n - r$. De nuevo sea $\mathcal{C}$ el conjunto de las componentes irreducibles de $V_{\mathbb{A}}(g_1, \ldots, g_r)$ y para cada $C \in \mathcal{C}$ existe $x_C \notin V_{\mathbb{A}}(f_{r+1}, \ldots, f_k)$. Por las mismas razones del caso 1, consideremos el polinomio

$$F_r(\mathcal{U}_{r+1}, \ldots, \mathcal{U}_k) := \prod_{C \in \mathcal{C}} (\mathcal{U}_{r+1} f_{r+1}(x_C) + \cdots + \mathcal{U}_k f_k(x_C)).$$

Será un polinomo no nulo y para $(t_{r+1}, \ldots, t_k) \in \mathbb{K}^{k-r}$ tal que $t_{r+1} \neq 0$ y $F_r(t_{r+1}, \ldots, t_k) \neq 0$, tendremos que el polinomio

$$g_{r+1} = t_{r+1} f_{r+1} + \cdots + t_k f_k,$$

verifica que $g_{r+1}(x_C) \neq 0 \; \forall C \in \mathcal{C}$, luego g_{r+1} no es divisor de cero módulo $\mathbb{K}[X_1, \ldots, X_n] / (g_1, \ldots, g_r)$ por argumentos similares a los anteriores.
Además, como $t_{r+1} \neq 0$, $\deg(g_{r+1}) = d_{r+1}$ y

$$(g_1, \ldots, g_r, g_{r+1}, f_{r+2}, \ldots, f_k) = (f_1, \ldots, f_r, f_{r+1}, \ldots, f_k),$$

con lo cual

- $V_{\mathbb{A}}(g_1, \ldots, g_{r+1}, f_{r+2}, \ldots, f_k) = \emptyset$.
- $\dim V_{\mathbb{A}}(g_1, \ldots, g_{r+1}) = n - (r + 1)$ o $V_{\mathbb{A}}(g_1, \ldots, g_{r+1}) = \emptyset$.

por los mismos argumentos usando el Teorema de Ideal Principal de Krull (Teorema A.2.5). Nótese que si $n - r = 0$, entonces no puede darse $V_{\mathbb{A}}(g_1, \ldots, g_{r+1}) \neq \emptyset$, de dimensión $-1 = n - (n + 1)$ con lo que, en ese caso, $V_{\mathbb{A}}(g_1, \ldots, g_{n+1}) = \emptyset$. □

Observación 2.3.2. En el anterior resultado ajustando los elementos de la diagonal principal $1, b_{2,2}, \ldots, b_{n+1,n+1}$ se pueden adaptar al caso

$$d_1 \geq d_2 \geq \cdots \geq d_k$$

de tal modo que $\deg(g_i) = d_i$ y se satisfagan el resto de condiciones.

Igualmente, reemplazando $\mathbb{A}^n(\mathbb{K})$ por una variedad algebraica irreducible $V \subseteq \mathbb{A}^m(\mathbb{K})$ de dimensión n se obtiene el siguiente resultado:

Lema 2.3.3. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín irreducible de dimensión n. Sean $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios de grado $\deg(f_i) = d_i$ tales que*

$$d_1 \geq d_2 \geq \cdots \geq d_k.$$

Supongamos que $V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) = \emptyset$. Si $k \geq n+1$, existe una matriz triangular superior

$$B = \begin{pmatrix} 1 & b_{1,2} & \ldots & b_{1,r} & \ldots & b_{1,,k} \\ & b_{2,2} & \ldots & b_{2,r} & \ldots & b_{2,k} \\ & & \ddots & \vdots & & \vdots \\ & \mathit{0} & & b_{n+1,n+1} & \ldots & b_{n+1,k} \end{pmatrix} \in \mathscr{M}_{n+1\times k}(\mathbb{K})$$

tal que $b_{i,i} \neq 0 \forall i, 1 \leq i \leq n+1$ y los polinomios $g_1, \ldots, g_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$ dados mediante:

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix} \in \mathbb{K}[X_1, \ldots, X_m]^{n+1}$$

satisfacen:

i) $\deg(g_i) = d_i, 1 \leq i \leq n+1$.
ii) $V_{\mathbb{A}}(g_1, \ldots, g_{n+1}) \cap V = \emptyset$.

Observación 2.3.4. Nótese que el procedimiento descrito en los dos Lemas precedentes permite también hacer una construcción como la siguiente: Supongamos $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín irreducible. Sean $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios de grado $d_i = \deg(f_i), 1 \leq i \leq n+1$, tales que

$$d_1 \geq d_2 \geq \cdots \geq d_{n+1}.$$

Supongamos $V \cap V_{\mathbb{A}}(f_1, \ldots, f_{n+1}) = \emptyset$. Entonces, considero la matriz B triangular inferior y los nuevos polinomios

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix}$$

Entonces, para cada $r, 1 \leq r \leq n$, cada

$$V_{\mathbb{A}}(g_1, \ldots, g_r)$$

es o bien vacío o una variedad de dimensión $n - r$. En particular, o existe $k < n$ tal que $V_{\mathbb{A}}(g_1, \ldots, g_k) = \emptyset$ o bien $V_{\mathbb{A}}(g_1, \ldots, g_n)$ es una variedad de dimensión 0 (i.e. un conjunto finito de puntos).

2.3.1. Una construcción cruzada. Sea $V \in \mathbb{A}^m(\mathbb{K})$ una variedad algebraica irreducible de dimensión n. Sean dados $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios de grado $d_i = \deg(f_i), 1 \leq i \leq n+1$ tales que:

- $d_1 \geq d_2 \geq \cdots \geq d_{n+1}$.
- $V \cap V_{\mathbb{A}}(f_1, \ldots, f_{n+1}) = \emptyset$.

Supongamos que no existe una matriz triangular superior

$$B = \begin{pmatrix} b_{1,1} & b_{1,2} & \ldots & b_{1,n+1} \\ & b_{2,2} & \ldots & b_{2,n+1} \\ & & \ddots & \vdots \\ & 0 & & b_{n+1,n+1} \end{pmatrix} \in \mathscr{M}_{n+1}(\mathbb{K}), \text{ con } b_{i,i} \neq 0, 1 \leq i \leq n+1,$$

tal que $\exists k$, con $k \leq n$, tal que si definimos

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix},$$

se tiene que $V_{\mathbb{A}}(g_1, \ldots, g_k) \cap V = \emptyset$. En otras palabras, supongamos que no existe una matriz B (como las precedentes) de tal modo que $V \cap V_{\mathbb{A}}(g_1, \ldots, g_k) = \emptyset$ es vacío antes de llegar al caso $k = n+1$. Equivalentemente, si no es posible recuperar en caso subdeterminado del Nullstellensatz usando combinaciones lineales de los polinomios en $\{f_1, \ldots, f_{n+1}\}$. En este caso, las variedades intermedias $V_{\mathbb{A}}(g_1, \ldots, g_k)$ tendrían siempre dimensión $n-k$ para $1 \leq k \leq n$. Supongamos, pues, que este es nuestro caso. Entonces, existen dos matrices triangulares superiores

$$B = \begin{pmatrix} b_{1,1} & & \cdots & b_{1,n+1} \\ & b_{2,2} & \cdots & b_{2,n+1} \\ & & \ddots & \vdots \\ & 0 & & b_{n+1,n+1} \end{pmatrix} \in \mathscr{M}_{n+1}(\mathbb{K}),$$

y

$$B' = \begin{pmatrix} b'_{1,1} & & \cdots & b'_{1,n+1} \\ & b'_{2,2} & \cdots & b'_{2,n+1} \\ & & \ddots & \vdots \\ & 0 & & b'_{n+1,n+1} \end{pmatrix} \in \mathscr{M}_{n+1}(\mathbb{K}),$$

tales que si definimos los polinomios

$$\begin{pmatrix} G_1 \\ \vdots \\ G_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix},$$

$$\begin{pmatrix} G'_1 \\ \vdots \\ G'_{n+1} \end{pmatrix} = B' \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix},$$

se tenga que $V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$ y $V \cap V_{\mathbb{A}}(G'_1, \ldots, G'_n)$ son variedades algebraicas cero-dimensionales y, además,

$$V \cap V_{\mathbb{A}}(G_1, \ldots, G_n) \cap V_{\mathbb{A}}(G'_1, \ldots, G'_n) = \emptyset.$$

La construcción sería, por ejemplo, la siguiente. Supongamos que hemos construido $g_1, \ldots, g_{n-1}$ de la forma

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n-1} & b_{1,n} & b_{1,n+1} \\ & b_{2,2} & \cdots & b_{2,n-1} & b_{2,n} & b_{2,n+1} \\ & & \ddots & \vdots & & \vdots \\ & 0 & & b_{n-1,n-1} & b_{n-1,n} & b_{n-1,n+1} \end{pmatrix} \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix},$$

tales que $V \cap V_{\mathbb{A}}(g_1, \ldots, g_{n-1})$ es, bien vacío o tiene dimensión 1. Como no puede ser vacío por hipótesis,

$$\dim(V \cap V_{\mathbb{A}}(g_1, \ldots, g_{n-1})) = 1,$$

y si $\mathcal{C}$ es el conjunto de todas las componentes irreducibles de $V_{\mathbb{A}}(g_1, \ldots, g_{n-1}) \cap V$ entonces $\dim(C) = 1$ para cada $C \in \mathcal{C}$. Construyamos ahora un polinomio

$$g_n = \theta_n f_n + \theta_{n+1} f_{n+1},$$

tal que $V \cap V_{\mathbb{A}}(g_1, \ldots, g_n)$ es una variedad cero dimensional con el mismo procedimiento que en Lemas precedentes. Ahora, observamos que si $C \in \mathcal{C}$ es una componente de $V_{\mathbb{A}}(g_1, \ldots, g_{n-1}) \cap V$ existe $x_C \in C$ tal que $x_C \notin V \cap V_{\mathbb{A}}(f_n, f_{n+1})$. De otro lado, como $V \cap V_{\mathbb{A}}(g_1, \ldots, g_n) \neq \emptyset$ (por nuestra hipótesis), entonces es cero dimensional (i.e. finito) y supongamos:

$$V \cap V_{\mathbb{A}}(g_1, \ldots, g_n) = \{y_1, \ldots, y_\delta\},$$

tendremos que $y_i \notin V \cap V_{\mathbb{A}}(f_n, f_{n+1})$ puesto que, con la construcción de los Lemas precedentes, $V \cap V_{\mathbb{A}}(g_1, \ldots, g_n, f_n, f_{n+1}) = V \cap V_{\mathbb{A}}(g_1, \ldots, g_{n+1}, f_n, f_{n+1}) = \emptyset$. Definamos el polinomio bivariado siguiente

$$H(T_n, T_{n+1}) = \prod_{C \in \mathcal{C}} (T_n f_n(x_C) + T_{n+1} f_{n+1}(x_C)) \prod_{i=1}^{\delta} (T_n f_n(y_i) + T_{n+1} f_{n+1}(y_i)).$$

Este polinomio es un producto de formas lineales, ninguna de las cuales es idénticamente cero. Luego H es un polinomio no nulo. Sean $(b_n, b_{n+1}) \in \mathbb{K}^2$ tales que $H(b_n, b_{n+1}) \neq 0$ y definamos

$$g'_n(X_1, \ldots, X_m) = b_n f_n + b_{n+1} f_{n+1} \in \mathbb{K}[X_1, \ldots, X_m].$$

Nótese que

- Para cada $C \in \mathcal{C}, g'_n(x_C)$ verifica.

$$g'_n(x_C) \prod_{\substack{C' \in \mathcal{C} \\ C' \neq C}} g'_n(x_{C'}) \prod_{i=1}^{\delta} g'_n(y_i) = H(b_n, b_{n+1}), \neq 0,$$

  luego $g'_n(x_C) \neq 0$.
- Para cada $i, 1 \leq i \leq \delta$, por el mismo argumento,

$$g'_n(y_i) \prod_{C \in \mathcal{C}} g'_n(x_C) \prod_{\substack{j=1 \\ j \neq i}}^{\delta} g'_n(y_j) = H(b_n, b_{n+1}) \neq 0.$$

Definamos

$$\begin{aligned} G_i &= g_i, 1 \leq i \leq n, \\ G'_i &= g_i, 1 \leq i \leq n-1, \\ G'_n &= g'_n. \end{aligned}$$

Como g'_n no se anula en ningún x_C, entonces g'_n no es divisor de cero módulo $\mathbb{K}[V] / (g_1, \ldots, g_{n-1})$. Como, por hipótesis, $V \cap V_{\mathbb{A}}(g_1, \ldots, g_{n-1}, g'_n) \neq \emptyset$ (no es reducible al caso subdeterminado) entonces

$$V \cap V_{\mathbb{A}}(G'_1, \ldots, G'_n) = V \cap V_{\mathbb{A}}(g_1, \ldots, g_{n-1}, g'_n),$$

es cero-dimensional. Como $g'_n(y) \neq 0, \forall y \in V \cap V_{\mathbb{A}}(g_1, \ldots, g_n)$ tendremos, obviamente, que G'_n no se anula en ningún punto de $V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$ con lo que

$$(V \cap V_{\mathbb{A}}(G'_1, \ldots, G'_n)) \cap (V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)) = \emptyset,$$

y tenemos la construcción buscada.

Teorema 2.3.5 (cf. [Je, 2005]). *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín irreducible de dimensión n y grado D. Sean $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ polinomios tales que $d_i = \deg(f_i)$ y se tiene*

- $d_1 \geq d_2 \geq \cdots \geq d_k$.
- $V \cap V_{\mathbb{A}}(f_1, \ldots, f_k) = \emptyset$.

Entonces, existen polinomios $g_1, \ldots, g_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que

i) $1 - \sum_{i=1}^{k} g_i f_i \in I(V)$.
ii) $\deg(g_i f_i) \leq 2DN(d_1, \ldots, d_k; n) - 1$, *donde*

$$N(d_1, \ldots, d_k; n) = \begin{cases} \prod_{i=1}^{k} d_i & \text{si } k < n, n > 1 \\ \prod_{i=1}^{n} d_i & \text{si } n < k, n > 1 \\ d_1 & \text{si } n = 1. \end{cases}$$

Demostración. Siguiendo los argumentos de las construcciones de los Lemas precedentes, comencemos suponiendo que $k = n + 1$. En caso contrario, eligiendo una combinación lineal de los polinomios $\{f_1, \ldots, f_k\}$ conforme al Lema 2.3.3 precedente, podemos elegir una combinación

lineal $\{g_1, \ldots, g_{n+1}\}$ tal que $V \cap V_{\mathbb{A}}(g_1, \ldots, g_{n+1})$ y seguir desde este punto. Supongamos pues que $k = n + 1$ y consideremos el conjunto de matrices

$$T_{(n+1)}(\mathbb{K}) = \left\{ \begin{pmatrix} b_{1,1} & \ldots & b_{1,n+1} \\ & \ddots & \vdots \\ 0 & & b_{n+1,n+1} \end{pmatrix} \in \mathscr{M}_{n+1}(\mathbb{K}). \prod_{i=1}^{n+1} b_{i,i} \neq 0 \right\}$$

Se trata de matrices triangulares no singulares. Consideremos dos casos:

i) Existe $B \in T_{n+1}(\mathbb{K})$ tal que definiendo los polinomios

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix},$$

existe $k \leq n$ tal que $V \cap V_{\mathbb{A}}(g_1, \ldots, g_k) = \emptyset$. En este caso, el resultado se sigue de manera inmediata por el Teorema 1.3.3 del caso sub-determinado desarrollado en la Sección 1.3.

ii) En el otro caso, supongamos que para toda $B \in T_{n+1}(\mathbb{K})$, si definimos los polinomios

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix},$$

para cada $k \leq n, V \cap V_{\mathbb{A}}(g_1, \ldots, g_k) \neq \emptyset$. Aplicamos la construcción descrita en la Subsección 2.3.1. Existirán dos matrices $B, B' \in T_{n+1}(\mathbb{K})$ tales que definiendo

$$\begin{pmatrix} F_1 \\ \vdots \\ F_{n+1} \end{pmatrix} = B \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix}, \begin{pmatrix} G_1 \\ \vdots \\ G_{n+1} \end{pmatrix} = B' \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{n+1} \end{pmatrix}$$

se verifiquen las propiedades siguientes:

(a) $V \cap V_{\mathbb{A}}(F_1, \ldots, F_n)$ es una variedad cero-dimensional.
(b) $V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$ es una variedad cero-dimensional.
(c) $V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) \cap V \cap V_{\mathbb{A}}(G_1, \ldots, G_n) = \emptyset$.

Aplicamos ahora el Teorema de Eliminación (i.e. Teorema 2.2.8 precedente) a los casos de las variedades cero-dimensionales

$$V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) \text{ y } V \cap V_{\mathbb{A}}(G_1, \ldots, G_n).$$

Para empezar, nótese que el Teorema de Eliminación 2.2.8 concluye la existencia de un abierto Zariski no vacío $\mathcal{U}_1 \subseteq \mathscr{M}_m(\mathbb{K})$ cuyas matrices satisfacen una serie de propiedades con respecto a la variedad cero-dimensional $V \cap V_{\mathbb{A}}(F_1, \ldots, F_n)$. De otro lado, existirá otro abierto Zariski $\mathcal{U}_2 \subseteq \mathscr{M}_m(\mathbb{K})$ de matrices que satisfacen similares propiedades pero en relación a los datos $V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$. Adicionalmente, como consecuencia de la Proposición 2.2.6 de la existencia de forma lineal separante, como $A = V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) \cup V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$ es también una variedad algebraica cero-dimensional, podemos suponer que existe un abierto Zariski no vacío $\mathcal{U}_3 \subseteq \mathscr{M}_m(\mathbb{K})$ tal que considerando el cambio lineal de coordenadas con $B'' \in \mathcal{U}_3$

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B'' \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

la forma lineal $Y_1 = b_{11}X_1 + \cdots + b_{1,m}X_m$ es una forma lineal separante de A. Es decir, dados $a, b \in A$, si $Y_1(a) = Y_1(b)$, entonces $a = b$. Como $\mathscr{M}_m(\mathbb{K})$ es una variedad algebraica afín irreducible, la intersección de cualquiera tres abiertos no vacíos en la topología de Zariski de $\mathscr{M}_m(\mathbb{K})$ es también no vacío. Definamos, finalmente, $\mathcal{U} = \mathcal{U}_1 \cap \mathcal{U}_2 \cap \mathcal{U}_3$ y sea $B \in \mathcal{U}$ una matriz regular en esa intersección. Definamos el

cambio de variable

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = B \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

y para cada $\underline{x} = (x_1, \ldots, x_m) \in \mathbb{A}^m(\mathbb{K})$ denotemos:

$$\begin{pmatrix} Y_1(\underline{x}) \\ \vdots \\ Y_m(\underline{x}) \end{pmatrix} = B \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Tendremos las siguientes propiedades:

(a) Como $B \in \mathcal{U}_3$, la forma lineal Y_1 es una forma separante de $A = V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) \cup V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$, es decir $\forall \underline{a}, \underline{b} \in A$ si $Y_1(\underline{a}) = \underline{Y}(\underline{b})$, entonces $\underline{a} = \underline{b}$.

(b) Como $B \in \mathcal{U}_1$ se tiene:

(b)-1 La forma lineal Y_1 es separante para $V \cap V_{\mathbb{A}}(F_1, \ldots, F_n)$.

(b)-2 Existe un polinomio univariado $\Phi_1 \in \mathbb{K}[T]$ tal que

$$\forall z \in \mathbb{K}, \text{si } \Phi_1(z) = 0, \exists \underline{a} \in V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) : z = Y_1(\underline{a})$$

(b)-3 Existen polinomios $g_1, \ldots, g_n \in \mathbb{K}[X_1, \ldots, X_n]$ tales que

- $\Phi_1(Y_1) - \sum_{i=1}^n g_i F_i \in I(V)$.
- $\deg(g_i F_i) \leq D \prod_{i=1}^n \deg(F_i) \leq D \prod_{i=1}^n \deg(f_i)$,

siendo la última desigualdad cierta por la construcción hecha de la sucesión $\{F_1, \ldots, F_n\}$ en la subsección 2.3.1 anterior.

(c) Como $B \in \mathcal{U}_2$ se tiene:

(c)-1 La forma lineal Y_1 es separante para $V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$.

(c)-2 Existe un polinomio univariado $\Phi_1' \in \mathbb{K}[T]$ tal que

$$\forall z \in \mathbb{K}, \text{si } \Phi_1'(z) = 0, \exists \underline{b} \in V \cap V_{\mathbb{A}}(G_1, \ldots, G_n) : z = Y_1(\underline{b}).$$

(c)-3 Existen polinomios $h_1, \ldots, h_n \in \mathbb{K}[X_1, \ldots, X_n]$ tales que

- $\Phi_1'(Y_1) - \sum_{i=1}^n h_i G_i \in I(V)$.
- $\deg(h_i G_i) \leq D \prod_{i=1}^n \deg(G_i) \leq D \prod_{i=1}^n \deg(f_i)$

siendo, de nuevo, la última desigualad cierta por la construcción hecha de la sucesión $\{G_1, \ldots, G_n\}$ en la Subsección 2.3.1 anterior.

Veamos que Φ_1 y Φ_1' no pueden poseer raíces comunes en $\mathbb{K}$. Pues si existiera $z \in \mathbb{K}$ tal que $\Phi_1(z) = 0$ y $\Phi_1'(z) = 0$, entonces, por el Teorema de Eliminación 2.2.8 tendríamos

$$\exists \underline{a} \in V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) : z = Y_1(\underline{a}),$$
$$\exists \underline{b} \in V \cap V_{\mathbb{A}}(G_1, \ldots, G_n) : z = Y_1(\underline{b}).$$

Pero como Y_1 es separante en $A = V \cap V_{\mathbb{A}}(F_1, \ldots, F_n) \cup V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)$, entonces dado que $z = Y_1(\underline{a}) = Y_1(\underline{b})$ concluiríamos

$$\underline{a} = \underline{b} \in (V \cap V_{\mathbb{A}}(F_1, \ldots, F_n)) \cap (V \cap V_{\mathbb{A}}(G_1, \ldots, G_n)) = \emptyset.$$

Con lo que llegaríamos a contradicción. Si dos polinomios univariados carecen de ceros comunes un un cuerpo algebraicamente cerrado es porque su máximo común divisor es 1. Por tanto, aplicando la Identidad de Bézout con cotas para el caso univariado (cf. [Pa,20a]), existirán $P, Q \in \mathbb{K}[T]$ tales que $\deg(P) \leq \deg(\Phi_1) - 1$ y $\deg(Q) \leq \deg(\Phi_1') - 1$ y se verifica

$$1 = P(Y_1)\Phi_1(Y_1) + Q(Y_1)\Phi_1'(Y_1).$$

Ahora bien, por las sucesivas iteraciones de los Teoremas de Eliminación de la Sección precedente, hemos visto que

$$\deg_{Y_1}(\Phi_1) \leq D \prod_{i=1}^n \deg(f_i),$$
$$\deg_{Y_1}(\Phi_1') \leq D \prod_{i=1}^n \deg(f_i).$$

En conclusión, tenemos

$$1 = P(Y_1)\Phi(Y_1) + Q(Y_1)\Phi_1'(Y_1), \tag{2.3.1}$$

donde $\deg_{Y_1}(P)$ y $\deg_{Y_1}(Q)$ están acotados por $D\prod_{i=1}^{n} d_i - 1$. Desarrollando la identidad 2.3.1 tendremos que

$$1 - P(Y_1)\left(\sum_{i=1}^{n} g_i F_i\right) - q(Y_1)\left(\sum_{i=1}^{n} h_i G_i\right) \in I(V),$$

donde los polinomios $F_1, \ldots, F_n$ y $G_1, \ldots, G_n$ son combinaciones lineales con coeficientes en $\mathbb{K}$ de $\{f_1, \ldots, f_{n+1}\}$.
Quedará entonces:

$$1 - \sum_{i=1}^{n+1} H_i f_i \in I(V),$$

donde $H_i = P(Y_1)\sum_{j=i}^{n} b_{j,i} g_j + Q(Y_1)\sum_{j=i}^{n} b'_{j,i} h_j$.
Luego

$$\deg(H_i f_i) \leq \max\{\deg_{Y_1} P(Y_1), \deg_{Y_1} Q(Y_1)\} + \max\{\deg(g_j f_i), \deg(h_j f_i)\} \leq$$
$$\leq D\prod_{i=1}^{n} d_i + D\prod_{i=1}^{n} d_i - 1.$$

Y el teorema queda demostrado.

□

APÉNDICE A

Algunos Resultados Elementales de Álgebra Conmutativa

Índice

En este Apéndice vamos a tratar de resumir algunos resultados de Álgebra Conmutativa elemental que se usan en el cuerpo del Trabajo Fin de Grado. En algún caso, daremos la pronta interpretación geométricoa de los mismos, en otros casos dejaremos para el Apéndice B la interpretación más pormenorizada de algunos de estos resultados.

A.1. Localización de anillos y módulos

Como la clásica construcción del cuerpo de los racionales $\mathbb{Q}$ desde el anillo de los enteros $\mathbb{Z}$, una construcción similar se hace para el estudio de anillos de propiedades locales: *localización de anillos.*

Definición 1 (Sistema multiplicativamente cerrado). *Sea R un anillo y $S \subset R$ un subconjunto. Se dice que S es un sistema multiplicativamente cerrado de R si es un submonoide de $(R, \cdot)$ que no contiene a $0 \in R$. En otras palabras, S es sistema multiplicativamente cerrado en R si verifica:*

- $1 \in S, 0 \notin S$.
- $\forall r, s \in S,\ r \cdot s \in S$.

Si R es un dominio de integridad el conjunto $S = R \setminus \{0\}$ es un sistema multiplicativamente cerrado en R. De hecho, es fácil observar que la condición clave para que $R \setminus \{0\}$ sea sistema multiplicativamente cerrado en R es que $(0) = \{0\}$ sea un ideal primo de R. De ahí que concluyamos que si R es un anillo cualquiera y $\mathfrak{p} \in Spec(R)$ es un ideal primo de R, entonces $R \setminus \mathfrak{p}$ es un sistema multiplicativamente cerrado.
Sea, pues, R un anillo cualquiera y $S \subseteq R$ un sistema multiplicativamente cerrado en R. Definimos la siguiente relación entre los elementos de $R \times S$:

$$(a, s) \sim (a', s') \Leftrightarrow \exists u \in S, u(as', a's) = 0.$$

Es fácil verificar que ésta es una relación de equivalencia en $R \times S$. Nótese que si R es un dominio de integridad y $S \subseteq R$ es un sistema multiplicativamente cerrado, esta relación de equivalencia se convierte en la siguiente:

$$(a, s) \sim (a', s') \Leftarrow \exists u \in S, u(as' - a's) = 0 \Leftrightarrow as' - a's = 0,$$

y el papel del elemento $u \in S$ desaparece.
Denotemos por $S^{-1}R$ al conjunto cociente para R anillo cualquiera y $S \subseteq R$ sistema multiplicativamente cerrado en R:

$$S^{-1}R := {R \times S}\Big/{\sim}.$$

Las clases de equivalencia del conjunto cociente $S^{-1}R$ se representan como fracciones:

$$\frac{r}{s} := [(r, s)]_{\sim}.$$

Aunque debemos ser cuidadosos, especialmente en el caso en que R no es dominio de integridad, porque, en general, no son propiamente fracciones en el sentido usual.

A partir de esta notación y del conjunto $S^{-1}R$ podemos definir las correspondencias siguientes:

$$+ : S^{-1}R \times S^{-1}R \longrightarrow S^{-1}R, \qquad \cdot : S^{-1}R \times S^{-1}R \longrightarrow S^{-1}R$$
$$\left(\frac{a}{s}, \frac{a'}{s'}\right) \longmapsto \frac{a \cdot s' + a' \cdot s}{s \cdot s'}, \qquad \left(\frac{a}{s}, \frac{a'}{s'}\right) \longmapsto \frac{a \cdot a'}{s \cdot s'}.$$

PROPOSICIÓN A.1.1. *Las anteriores correspondencias son aplicaciones y definen una estructura que hace que $(S^{-1}R, +, \cdot)$ sea un anillo conmutativo con unidad, usualmente denominado la localización de R en el sistema multiplicativamente cerrado S.*

Por comodidad, usualmente se escribe $S^{-1}R$ para resumir toda la construcción anterior.

EJEMPLO A.1.2.
i) El ejemplo más usual es la localización en un primo. Así, si R es un anillo cualquiera y $\mathfrak{p} \in Spec(R)$, entonces $S_{\mathfrak{p}} = R \backslash \mathfrak{p}$ es un sistema multiplicativamente cerrado y la localización $S_{\mathfrak{p}}^{-1}R$ se suele denotar $R_{\mathfrak{p}}$ y se denomina localización de R en el primo $\mathfrak{p}$.

ii) Si R es un anillo cualquiera y $f \in R$ es un elemento no nilpotente (i.e. $f^n \neq 0, \forall n \in \mathbb{N}$), el siguiente es un sistema multiplicativamente cerrado en R:

$$S_f := \{f^n : n \in \mathbb{N}\} = \{1, f, f^2, \dots\}$$

A la localización $S_f^{-1}R$ se la suele denotar mediante R_f y se denomina localización de R en el elemento $f \in R$.

iii) Un caso particular de i) es el caso de los cuerpos de fracciones de los dominios de integridad. Un anillo R es dominio de integridad si y solo si el ideal (0) es un ideal primo de R. Entonces, la localización $R_{(0)}$ es especial: se trata de un cuerpo conocido como el cuerpo de fracciones de R *y que se denota mediante $qf(R)$*

El anillo $R_{\mathfrak{p}}$, donde $\mathfrak{p} \in Spec(R)$, es un anillo especial. Para ello, recordemos la noción de anillo local.

DEFINICIÓN 2 (Anillo local). *Un anillo R se dice local si posee un único ideal maximal.*

Normalmente, escribiremos "sea $(R, \mathfrak{m})$ un anillo local", destacando que el espectro maximal $Spm(R)$ satisface $Spm(R) = \{\mathfrak{m}\}$.

PROPOSICIÓN A.1.3. *Si R es un anillo cualquiera y $\mathfrak{p} \in Spec(R)$, entonces $R_{\mathfrak{p}}$ es un anillo local cuyo único ideal maximal es dado por la siguiente igualdad:*

$$\mathfrak{p}R_{\mathfrak{p}} = \left\{\frac{r}{s} : r \in \mathfrak{p}, s \in S\right\}.$$

De hecho, la relación entre R y $S^{-1}R$ es más intensa, como se prueba en la siguiente proposición.

PROPOSICIÓN A.1.4. *Sea R un anillo, $S \subseteq R$ un sistema multiplicativamente cerrado. Entonces, el siguiente es un morfismo de anillos, no necesariamente inyectivo:*

$$c_S : R \longrightarrow S^{-1}R.$$
$$a \longmapsto \frac{a}{1}.$$

Este morfismo permite identificar el espectro primo de $S^{-1}R$ con las extensiones a $S^{-1}R$ de los primos de R que no intersecan a S. Es decir, la siguiente es una biyección:

$$\{\mathfrak{p} \in Spec(R) : \mathfrak{p} \cap S = \emptyset\} \longrightarrow Spec(S^{-1}R)$$
$$\mathfrak{p} \longmapsto \mathfrak{p}^e = S^{-1}\mathfrak{p} = \left\{\frac{r}{s} : r \in \mathfrak{p}, s \in S\right\}.$$

Así, por ejemplo, si $\mathfrak{p}$ es un primo en un anillo R, existe una biyección entre $Spec(R_{\mathfrak{p}})$ y los primos de R que tienen intersección vacía con $R \setminus \mathfrak{p}$. Es decir, entre los primos de $R_{\mathfrak{p}}$ y los primos de R contenidos en $\mathfrak{p}$:

$$\{\mathfrak{q} \in Spec(R) : \mathfrak{q} \subseteq \mathfrak{p}\} \longrightarrow Spec(R_{\mathfrak{p}})$$
$$\mathfrak{q} \longmapsto \mathfrak{q} \cdot R_{\mathfrak{p}} = \left\{\frac{r}{s} : r \in \mathfrak{q}, s \notin \mathfrak{p}\right\}.$$

Del mismo modo, si $f \in R$ es un elemento no nilpotente, entonces existe una biyección entre los ideales primos de R_f y los ideales primos de R que no contienen a f:

$$\{\mathfrak{p} \in Spec(R) : f \notin \mathfrak{p}\} \longrightarrow Spec(R_f)$$
$$\mathfrak{p} \longmapsto \mathfrak{p}R_f = \left\{ \frac{r}{f^m} : r \in \mathfrak{p}, m \in \mathbb{N} \right\}.$$

Un cuerpo de fracciones clásico, además de $\mathbb{Q}$ con respecto a $\mathbb{Z}$, es el de las funciones racionales. Así, consideremos el dominio de integridad $K[X_1, \ldots, X_n]$ de polinomios sobre un cuerpo. Al cuerpo de fracciones $qf(K[X_1, \ldots, X_n])$ se le denota usualmente mediante $K(X_1, \ldots, X_n)$ y sus elementos toman la forma siguiente:

$$K(X_1, \ldots, X_n) = \left\{ \frac{p}{q} : p, q \in K[X_1, \ldots, X_n], q \neq 0 \right\}.$$

COROLLARIO A.1.5. *Los ideales primos de $R_\mathfrak{p}$ están en biyección con los ideales primos de R contenidos en $\mathfrak{p}$ y por tanto, para cada ideal $\mathfrak{p} \in Spec(R)$, el anillo $R_\mathfrak{p}$ es un anillo local, cuyo único ideal maximal es el ideal generado por $\mathfrak{p}$ en $R_\mathfrak{p}$ y que denotaremos:*

$$\mathfrak{p}R_\mathfrak{p} := \left\{ \frac{r}{s} \in R_\mathfrak{p} : r \in \mathfrak{p}, s \in R \setminus \mathfrak{p} \right\}.$$

A.2. Dimensión de Krull de anillos y espacios topológicos

DEFINICIÓN 3 (Dimensión de Krull de un espacio topológico). *Sea X un espacio topológico noetheriano. Llamaremos dimensión de X al valor $\dim X \in \mathbb{N} \cup \{\infty\}$ máximo de las longitudes de cadenas de irreducibles de X, es decir, máximo de los n que cumplen:*

$$\emptyset \neq V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n \subset X,$$

donde V_i es un conjunto cerrado e irreducible $\forall i \in \{1, \ldots, n\}$.

DEFINICIÓN 4 (Variedad equi-dimensional). *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica afín. Diremos que V es una variedad equi-dimensional si tiene una descomposición de la forma:*

$$V = V_1 \cup \cdots \cup V_s,$$

donde V_i es un variedad algebraica afín irreducible, y se cumple que $\dim V_i = m \ \forall i \in \{1, \ldots, s\}$.

La dimensión de Krull es un invariante de las variedades algebraicas y se cumple:

PROPOSICIÓN A.2.1. *Sea $f : V \longrightarrow W$ una aplicación polinomial entre variedades algebraicas y sea $Z = \overline{f(V)}$. Entonces $\dim_{Krull} Z \leq \dim_{Krull} V$.*

DEFINICIÓN 5 (Dimensión de Krull de un anillo). *Sea A un anillo. Llamaremos dimensión de Krull de A a la dimensión de Krull de $Spec(A)$ dotado con la topología de Zariski.*

DEFINICIÓN 6 (Altura y coaltura de ideales primos). *Sea R un anillo, $\mathfrak{p}$ un ideal primo de R*

i) Llamaremos altura de $\mathfrak{p}$ al máximo de las longitudes de cadenas de ideales primos de R contenidos en $\mathfrak{p}$ y se denotará por $ht(\mathfrak{p})$, es decir, al máximo de los números naturales $n \in \mathbb{N}$ tales que existe:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq \mathfrak{p},$$

donde $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ son ideales primos de R.

ii) Llamaremos coaltura de $\mathfrak{p}$ al máximo de las longitudes de cadenas de ideales primos de R que contienen a $\mathfrak{p}$ y se denotará por $coht(\mathfrak{p})$, es decir, al máximo de los números naturales $n \in \mathbb{N}$ tales que existe:

$$\mathfrak{p} \subsetneq \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq R,$$

donde $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ son ideales primos de R.

DEFINICIÓN 7 (Altura y coaltura de ideales arbitrarios). *Sea un anillo A y $\mathfrak{a}$ un ideal.*

i) Llamaremos altura de $\mathfrak{a}$ al ínfimo de las alturas de los ideales primos que contienen a $\mathfrak{a}$ y se denotará por $ht(\mathfrak{a})$.

ii) Llamaremos coaltura de $\mathfrak{a}$ al máximo de las alturas de los ideales primos que contienen a $\mathfrak{a}$. Lo denotaremos por $coht(\mathfrak{a})$.

DEFINICIÓN 8 (Codimensión de un cerrado irreducible). *Sea X un espacio topológico, $Y \subset X$ un conjunto cerrado e irreducible. Llamaremos codimensión de Y en X al valor $codim_X Y \in \mathbb{N} \cup \{\infty\}$ supremo de todos los $n \in \mathbb{N}$ que cumplen:*

$$Y \subseteq Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_n \subset X,$$

donde Y_i es un conjunto cerrado e irreducible $\forall i \in \{1, \ldots, n\}$.

Se introducen los términos necesarios para entender la definición de ideal no mezclado.

DEFINICIÓN 9. *Sea M un R-módulo.*

- *Para cada elemento $a \in R$, se denota por $\eta_{a,M} : M \longrightarrow M$ a la homotecia de razón a sobre M, es decir, al endomorfismo dado mediante $\eta_a(m) := am$, $\forall m \in M$.*
- *Un endomorfismo de R-módulos, $\phi : M \longrightarrow M$, se denomina nilpotente si existe $n \in \mathbb{N}$, $n \geq 1$ tal que $\phi^n \equiv 0$.*
- *Un submódulo N de M se denomina primario si $N \neq M$ y para cada $a \in R$, la homotecia $\eta_{a,M\,/\,N}$ es o bien inyectiva o bien nilpotente.*
- *Un ideal $\mathfrak{q}$ de R se dice primario si es primario como submódulo (del módulo R).*

PROPOSICIÓN A.2.2. *Si N es un submódulo primario de un R-módulo M, entonces el conjunto:*

$$\mathfrak{p} := \{a \in R : \eta_{a,M\,/\,N} \text{ no es inyectiva}\},$$

es un ideal primo de R. Diremos que el submódulo N es $\mathfrak{p}$-primario.

DEFINICIÓN 10 (Ideales asociados a un módulo). *Sea M un R-módulo. Un ideal primo $\mathfrak{p} \in Spec(R)$ se denomina asociado a M si existe $x \in M$ tal que $x \neq 0$ y*

$$\mathfrak{p} = Ann(\{x\}) := \{a \in R : ax = 0\}.$$

Denotaremos por $Ass(M)$ al conjunto de todos los ideales primos asociados a M.

DEFINICIÓN 11 (Ideal no mezclado). *Un ideal $\mathfrak{a}$ de un anillo noetheriano R se dice no mezclado si admite una descomposición en ideales primarios*

$$\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_s,$$

donde cada $\mathfrak{a}_i$ es $\mathfrak{p}_i$-primario, $\mathfrak{p}_i \in Spec(R)$ es primo, los asociados del ideal $\mathfrak{a}$ son $Ass(\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ y todos tienen la misma coaltura, es decir,

$$coht(\mathfrak{p}_1) = \cdots = coht(\mathfrak{p}_s) = \dim\left(R \Big/ \mathfrak{a}\right).$$

PROPOSICIÓN A.2.3. *Sea $\mathfrak{a} \subseteq R$ un ideal no mezclado de un anillo noetheriano R. Sea $\mathfrak{b} \subseteq R$ otro ideal y $R' \subseteq R$ una extensión de anillos. Entonces se verifican las propiedades siguientes:*

i) El ideal $\mathfrak{a} \,/\, \mathfrak{b}$ es no mezclado.
ii) La contracción $\mathfrak{a}^c = \mathfrak{a} \cap R'$ es no mezclada.

PROPOSICIÓN A.2.4. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica equi-dimensional afín. Entonces, su ideal $I(V) \subseteq \mathbb{K}[X_1, \ldots X_m]$ es un ideal no mezclado.*

El siguiente es un resultado clásico debido a W. Krull:

TEOREMA A.2.5 (**Teorema del Ideal Principal de Krull**). *Sea R un anillo noetheriano, $a \in R$ no es divisor de cero, $\mathfrak{p}$ un ideal primo mínimo sobre (a), entonces $ht(\mathfrak{p})=1$*

El siguiente resultado se puede encontrar en [**Ma, 1980**].

PROPOSICIÓN A.2.6. *Sea A un dominio de integridad noetheriano. A es un dominio de factorización única si y solo si todo ideal primo de altura 1 es principal.*

LEMA A.2.7. *Si A es un dominio noetheriano y $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario, donde $\mathfrak{p}$ es un ideal principal, entonces existe $n \in \mathbb{N}$ tal que $\mathfrak{p}^n = \mathfrak{q}$ y $\mathfrak{q}$ es un ideal principal.*

A.3. Extensiones enteras de anillos: propiedades de ascenso y descenso

Se van a enunciar una serie de definiciones y resultados para poder entender el lema de normalización de Noether.

DEFINICIÓN 12 (Extensión de anillos). *Sea R un anillo conmutativo. Una extensión de R es otro anillo R' que tiene a R como subanillo.*

DEFINICIÓN 13 (Extensión entera de anillos). *Dada una extensión de anillos $R \subseteq R'$, un elemento $x \in R'$ se dice entero sobre R si existe un polinomio mónico $p \in R[T]$ tal que $p(x) = 0$. Una extensión $R \subseteq R'$ se dice entera si todos los elementos de R' son enteros sobre R.*

OBSERVACIÓN A.3.1. En general en teoría de anillos se denomina extensión de un anillo A a todo morfismo de anillos con unidad $\varphi : A \longrightarrow B$. La imagen de A mediante φ es un subanillo de B. En esta situación diremos que un elemento de B es entero sobre A, si es entero sobre el subanillo imagen $\varphi(A)$.

DEFINICIÓN 14 (Extensión de ideales). *Sea $f : A \longrightarrow B$ un morfismo de anillos y $\mathfrak{a} \subseteq A$ un ideal de A. Llamaremos extensión del ideal $\mathfrak{a}$ al anillo B al ideal generado por $f(\mathfrak{a})$ en B:*

$$\mathfrak{a}^e := (f(\mathfrak{a})).$$

DEFINICIÓN 15 (Contracción de ideales). *Sea una extensión de anillos $R \subseteq R'$ y $\mathfrak{q} \subseteq R'$ un ideal. Se denominará contracción de $\mathfrak{q}$ al ideal $\mathfrak{q}^c = \mathfrak{q} \cap R$ del anillo R.*

PROPOSICIÓN A.3.2. *Sean una extensión de anillos $R \subseteq R'$. Se tienen las siguientes propiedades:*

i) Si la extensión es entera y $\mathfrak{b}$ es un ideal de R', entonces $R'/\mathfrak{b}$ es una extensión entera de $R/\mathfrak{b}^c$.

ii) Si $R' = R[\alpha_1, \ldots, \alpha_m]$ es un R-álgebra finitamente generada y $\{\alpha_1, \ldots, \alpha_m\}$ son enteros sobre R, entonces R' es entero sobre R.

DEFINICIÓN 16 (Clausura entera). *Sea una extensión de anillos $R \subseteq R'$. Los elementos de R' que son enteros sobre R forman un subanillo $\overline{R}$ de R' llamado clausura entera de R en R'.*

DEFINICIÓN 17 (Dominio normal). *Sea un dominio de integridad R. Se dice que es normal si la clausura entera $\overline{R}$ en su cuerpo de fracciones es $\overline{R} = R$.*

PROPOSICIÓN A.3.3. *Todo dominio de factorización única es un dominio normal.*

Ahora enuncio los teoremas Krull-Cohen-Seidenberg going-up y going-down

PROPOSICIÓN A.3.4. *Sea $R \subseteq R'$ una extensión entera de dominios de integridad. Entonces R' es un cuerpo si y solamente si R es un cuerpo. En particular, sea $\mathfrak{q}$ es un ideal primo de R', su contracción $\mathfrak{p} := \mathfrak{q}^c$ es maximal en R si y solamente si $\mathfrak{q}$ es maximal en R'.*

COROLLARIO A.3.5. *Sea $R \subseteq R'$ una extensión entera de anillos y $\varphi : Spec(R') \longrightarrow Spec(R)$ la aplicación continua dada por la contracción de ideales. Entonces:*

i) φ es suprayectiva.

ii) $\varphi(Spm(R')) \subseteq Spm(R)$ y a siguiente aplicación está bien definida y es suprayectiva:

$$\varphi_{Spm(R')} : Spm(R') \longrightarrow Spm(R).$$

COROLLARIO A.3.6. *Sea $\varphi : V \longrightarrow W$ un morfismo dominante de variedades algebraicas afines. Se tiene que si la extensión $\mathbb{K}[W] \subseteq \mathbb{K}[V]$ es entera, φ es suprayectiva.*

TEOREMA A.3.7 (Going-Up). *Sea $R \subseteq R'$ una extensión entera de anillos. Si tengo dos cadenas ascendentes de ideales primos:*

- *Una cadena ascendente de ideales primos de R:*

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n,$$

- *Una cadena ascendente de ideales primos de R':*

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m,$$

tal que $n > m$ y $\mathfrak{q}_i^c = \mathfrak{p}_i \ \forall i \in \{1, \ldots m\}$. Entonces existe una cadena ascendente de ideales primos de R' :

$$\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n,$$

tales que $\mathfrak{q}_i^c = \mathfrak{p}_i \ \forall i \in \{m+1, \ldots, n\}$.

Existe un teorema similar pero con las inclusiones en sentido inverso para dominios de integridad:

TEOREMA A.3.8 (Going-Down). *Sea $R \subseteq R'$ una extensión entera de dominios de integridad y R es un dominio normal. Si tengo dos cadenas descendentes de ideales primos:*

- *Una cadena descendente de ideales primos de R:*

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n,$$

- *Una cadena descendente de ideales primos de R':*

$$\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m,$$

tal que $n > m$ y $\mathfrak{q}_i^c = \mathfrak{p}_i \ \forall i \in \{1, \dots m\}$. Entonces existe una cadena descendente de ideales primos de R' :

$$\mathfrak{q}_m \supseteq \mathfrak{q}_{m+1} \supseteq \cdots \supseteq \mathfrak{q}_n,$$

tales que $\mathfrak{q}_i^c = \mathfrak{p}_i \ \forall i \in \{m+1, \dots, n\}$.

Gracias a los teoremas de ascenso y descenso se deduce el siguiente resultado:

COROLLARIO A.3.9. *Sea $R \subseteq R'$ una extensión entera de dominios de integridad y R es domino de factorización única. Entonces, se tiene:*

i) $\dim_{Krull}(R) = \dim_{Krull}(R')$
ii) Si $\mathfrak{q} \subseteq R'$ es primo y $\mathfrak{p} = \mathfrak{q}^c$ es una contracción a R, se tiene que:

$$ht(\mathfrak{p}) = ht(\mathfrak{q}),$$
$$coht(\mathfrak{p}) = coht(\mathfrak{q}).$$

A.4. Lema de Normalización de Noether y variaciones

DEFINICIÓN 18 (A-álgebra de tipo finito o finitamente generada y morfismo de tipo finito de anillos). *Sean A y B dos anillos y $f : A \longrightarrow B$ un morfismo. Se dice que B es una A-álgebra de tipo finito o finitamente generada y que f es un morfismo de tipo finito si existe un anillo de polinomios $A[X_1, \dots, X_n]$ sobre A y un epimorfismo de anillos:*

$$\varphi : A[X_1, \dots, X_n] \longrightarrow B,$$

tal que $\varphi|_A = f$.

PROPOSICIÓN A.4.1. *En el caso particular de que $A \subseteq B$, B será un A-álgebra de tipo finito si y solo si existe un ideal $\mathfrak{a}$ de un anillo de polinomios $A[X_1, \dots, X_n]$ tal que*

$$B \cong {A[X_1, \dots, X_n]}\Big/_{\mathfrak{a}}.$$

DEFINICIÓN 19 (Morfismo finito de anillos y A-álgebra finita). *Si $f : A \longrightarrow B$ es un morfismo de anillos, entonces tenemos inducida en B una estructura natural de A-módulo de modo obvio siguiente:*

$$\cdot_A : A \times B \longrightarrow B.$$
$$(a, b) \longmapsto f(a) \cdot b.$$

Se dice que f es un morfismo finito si B es un A-módulo (con la operación $\cdot_A$) finitamente generado, en cuyo caso B se dice que es un A-álgebra finita.

PROPOSICIÓN A.4.2. *Sea $A \subseteq B$ una extensión de anillos y sea $x \in B$. Se tiene que x es entero sobre A si y solo si existe una A-álgebra finita C tal que $A \subseteq C \subseteq B$ y $x \in C$.*

PROPOSICIÓN A.4.3. *Sea $A \subseteq B$ una extensión de anillos y B es un A-álgebra de tipo finito. Son equivalentes:*

i) B es un A-álgebra finita.
ii) $A \subseteq B$ es una extensión entera de anillos.

Se van a introducir los conceptos necesarios para entender el lema de normalización de Noether y así, como caso particular, llegar al Corolario A.4.9.

Definición 20 (Aplicación finita de variedades). *Sean X e Y dos variedades algebraicas afines y sea $f : X \longrightarrow Y$ una aplicación polinomial (o morfismo regular). Sea la aplicación entre los anillos de funciones polinomiales:*

$$f^* : K[Y] \longrightarrow K[X].$$
$$\varphi \longrightarrow \varphi \circ f.$$

Se dice que f es de tipo finito si f^* lo es como morfismo de anillos y que f es finito si f^* lo es.

Los siguientes resultados se encuentran en [**Sha, 1974**]:

Proposición A.4.4. *Sea $f : X \longrightarrow Y$ una aplicación finita entre variedades algebraicas afines. Se tiene:*

i) Sea $y \in Y$, su fibra $f^{-1}(y)$ es un número finito de elementos.
ii) f es sobreyectiva.
iii) f es cerrada.

Proposición A.4.5. *Sean X e Y dos variedades algebraicas afines y sea $f : X \longrightarrow Y$ una aplicación polinomial dominante. Entonces f^* es inyectiva y un monomorfismo de anillos. Por eso se suele denotar $f^*(\mathbb{K}[Y])$ por simplemente $\mathbb{K}[Y]$.*

Proposición A.4.6. *Sean X e Y dos variedades algebraicas afines K-definibles y sea $f : X \longrightarrow Y$ un morfismo. f será un isomorfismo si y solo si $f^* : K[Y] \longrightarrow K[X]$ es un isomorfismo de anillos.*

Proposición A.4.7. *Sea $f : X \longrightarrow Y$ una aplicación finita entre variedades algebraicas afines. Son equivalentes:*

i) $\mathbb{K}[X]$ es una $\mathbb{K}[Y]$-álgebra finita.
ii) $\mathbb{K}[Y] \subseteq \mathbb{K}[X]$ es una extensión entera de anillos.

Si además X es irreducible, entonces Y es irreducible y se tiene que

$$[\mathbb{K}(V) : \mathbb{K}(W)] < +\infty,$$

donde $\mathbb{K}(V)$ y $\mathbb{K}(W)$ son los cuerpos de fracciones de $\mathbb{K}[V]$ y $\mathbb{K}[W]$.

La versión algebraica del Lema de Normalización de Noether es la siguiente:

Teorema A.4.8 (Lema de Normalización de Noether). *Sea K un cuerpo de cardinal infinito y, como en Capítulos precedentes, sea $\mathbb{K}$ su clausura algebraica. Sea A una K-álgebra finitamente generada. Supongamos que*

$$A = K[X_1, \ldots, X_n] \Big/ \mathfrak{a},$$

donde $\mathfrak{a}$ es un ideal propio de $K[X_1, \ldots, X_n]$. Entonces, existe un abierto $\mathcal{U}$ en la topología de Zariski del espacio de matrices $\mathcal{U} \subseteq \mathscr{M}_n(\mathbb{K}) = \mathbb{A}^{n^2}(\mathbb{K})$, tal que se verifica la siguiente propiedad: Para cada matriz $B \in \mathcal{U}$, B es no singular (i.e. $\det(B) \neq 0$) y determina un cambio lineal de coordenadas en $\mathbb{A}^n(\mathbb{K})$ dado por la identidad siguiente:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = B \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

de tal modo que las formas lineales $\{Y_1, \ldots, Y_n\}$ verifican las siguientes propiedades:

i) Si $d = \dim(A)$ es la dimensión de Krull de la K-álgebra A, entonces $\{Y_1, \ldots, Y_d\}$ son algebraicamente independientes sobre $\mathbb{K}$. En particular, $\mathbb{K}[Y_1, \ldots, Y_d]$ es un anillo de polinomios en d variables.
ii) Si $B \in \mathscr{M}_n(\mathbb{K}) \cap \mathcal{U}$, la K-álgebra A es un $K[Y_1, \ldots, Y_d]$-módulo finitamente generado o, equivalentemente, la siguiente es una extensión entera de anillos:

$$K[Y_1, \ldots, Y_d] \hookrightarrow A.$$

iii) Si $A = \mathbb{K}[V]$ es el anillo de funciones polinomiales sobre una variedad algebraica afín equi-dimensional $V \subseteq \mathbb{A}^n(\mathbb{K})$, entonces la siguiente aplicación es un morfismo suprayectivo:

$$\Pi : V \longrightarrow \mathbb{A}^d(\mathbb{K}),$$
$$\underline{x} = (x_1, \ldots, x_n) \longmapsto (Y_1(\underline{x}), \ldots, Y_d(\underline{x})).$$

COROLLARIO A.4.9. *Para cualquier ideal no mezclado* $\mathfrak{a}$ *de* $K[X_1, \ldots, X_n]$ *se tiene:*

$$ht(\mathfrak{a}) + coht(\mathfrak{a}) = n.$$

El resultado es, en particular, cierto para ideales radicales, intersección de un número finito de primos todos de la misma altura.

La siguiente generalización del Teorema del Ideal Principal de Krull se puede encontrar en [**Ku, 1885**]

TEOREMA A.4.10 (Generalización del Teorema del Ideal Principal de Krull). *Sea* R *un anillo noetheriano,* $\mathfrak{a} \subseteq R$ *un ideal propio y* $\{f_1, \ldots, f_k\} \subseteq R$ *tales que* $\mathfrak{a} = (f_1, \ldots, f_k)$. *Entonces, para cualquier ideal primo* $\mathfrak{p}$ *minimal entre los que contienen al ideal* $\mathfrak{a}$ *se verifica* $ht(\mathfrak{p}) \leq k$. *Si, además,* $f_1, \ldots, f_k$ *es una sucesión regular sobre* R, *esto es, si se verifica:*

i) f_1 *no es divisor de cero en* R.

ii) Para cada $i, 2 \leq i \leq k$, f_i *no es divisor de cero en el anillo cociente*

$$R \Big/ (f_1, \ldots, f_{i-1}).$$

iii) $\mathfrak{a} = (f_1, \ldots, f_k) \neq (1)$ *es un ideal propio.*

Entonces todo ideal primo minimal sobre $\mathfrak{a}$ *tiene altura* k.

APÉNDICE B

Algunos Resultados Elementales de Geometría Algebraica

Índice

En este Apéndice revisaremos algunos de los resultados elementales en Geometría Algebraica afín que se usan a lo largo del Capítulo. Algunos son consecuencia de resultados estándar de Álgebra Conmutativa, otros recibirán un tratamiento más geométrico, aunque, en el fondo, casi todos ellos provienen directamente de estructuras algebraicas.
En ocasiones citaremos fuentes bibliográficas y en otras daremos alguna demostración más detallada.

B.1. Dimensión en variedades algebraicas: algunos resultados clásicos

Como ya se indicaba desde la Introducción, si $V \subseteq \mathbb{A}^m(\mathbb{K})$ es una variedad algebraica irreducible, el anillo $\mathbb{K}[V]$ es un dominio de integridad y $\mathbb{K}(V) = qf(\mathbb{K}[V])$ es su cuerpo de funciones racionales. Por ser $\mathbb{K}[V]$ una $\mathbb{K}$-álgebra finitamente generada, entonces el grado de trascendencia sobre $\mathbb{K}$ de $\mathbb{K}(V)$ es finito. Esto conduce a la definición clásica de dimensión siguiente:

DEFINICIÓN 21. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín.*

i) Si V is irreducible, llamaremos dimensión de V al grado de trascendencia de $\mathbb{K}(V)$ sobre $\mathbb{K}$:

$$\dim(V) := grtr_{\mathbb{K}}(\mathbb{K}(V)).$$

ii) Si V es reducible y admite una descomposición en componentes irreducibles de la forma siguiente:

$$V = V_1 \cup \cdots \cup V_s,$$

llamaremos dimensión de V al máximo de las dimensiones de sus componentes irreducibles, es decir,

$$\dim(V) := \max\{\dim(V_1), \ldots, \dim(V_s)\}.$$

El Lema de Normalización de Noether permite igualar esta noción clásica con las nociones de dimensión de Krull descritas en el Capítulo precedente (como se hace en el texto [**Ku, 1885**]).

PROPOSICIÓN B.1.1. *Sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín. Las siguientes expresiones definen la misma cantidad que llamaremos simplemente dimensión de V y denotaremos por* $\dim(V)$*:*

i) La dimensión de V, basada en el grado de trascendencia, como en la Definición 21.
ii) La dimensión de Krull de V como espacio topológico noetheriano con la topología de Zariski inducida por la de $\mathbb{A}^m(\mathbb{K})$.
iii) La dimensión de Krull del anillo $\mathbb{K}[V]$.
iv) La co-altura del ideal $I(V)$ en $\mathbb{K}[X_1, \ldots, X_m]$.

Por tanto, todos los resultados ya descritos en el Apéndice A se aplican apropiadamente a la dimensión de variedades algebraicas afines, con la apropiada transformación. Obviamente se tiene:

PROPOSICIÓN B.1.2. *Con las notaciones precedentes, sea $V \subseteq \mathbb{A}^m(\mathbb{K})$ una variedad algebraica afín. Son equivalentes:*

i) $\dim(V) = m-1$ *y todos sus componentes irreducibles tienen la misma dimensión (i.e. V es equi-dimensional).*

ii) Existe $f \in \mathbb{K}[X_1, \ldots, X_m] \setminus \mathbb{K}$ (un polinomio no nulo y no constante) tal que $V = V_{\mathbb{A}}(f)$.

DEMOSTRACIÓN. Para la primera implicación, supongamos que $\dim(V) = m-1$ y que todas sus componentes irreducibles tienen la misma dimensión . Sean $V_1, \ldots, V_r$ esas componentes irreducibles. Como $\dim(V_i) = m-1$, entonces, $I(V_i)$ es un ideal primo de coaltura $m-1$ en $\mathbb{K}[X_1, \ldots, X_m]$. Como $\mathbb{K}[X_1, \ldots, X_m]$ es catenario, $ht(I(V)) = 1$ para cada $i, 1 \leq i \leq r$. Como $\mathbb{K}[X_1, \ldots, X_m]$ es dominio de factorización única, todo ideal primo de altura 1 es principal. Por tanto, para cada $i, 1 \leq i \leq r$, existe $f_i \in \mathbb{K}[X_1, \ldots, X_m]$ tal que $I(V_i) = (f_i)$ y, obviamente, $V_i = V_{\mathbb{A}}(I(V_i)) = V_{\mathbb{A}}(f_i)$. Como V_i tiene dimensión 1 y $I(V_i)$ es ideal primo, no es posible que $f_i \in \mathbb{K}$. Finalmente, consideremos

$$f = \prod_{i=1}^{r} f_i \in \mathbb{K}[X_1, \ldots, X_m].$$

Como ningún $f_i \in \mathbb{K}$, tampoco es posible que $f \in \mathbb{K}$ por lo que $f \in \mathbb{K}[X_1, \ldots, X_m] \setminus \mathbb{K}$. Finalmente, como $f = \prod f_i$ tenemos

$$V_{\mathbb{A}}(f) = \bigcup_{i=1}^{r} V_{\mathbb{A}}(f_i) = \bigcup_{i=1}^{r} V_i = V.$$

Por otro lado, para la implicación inversa, consideremos el ideal $\mathfrak{a} = (f)$. Por el Teorema del Ideal Principal de Krull A.2.5, como $\mathbb{K}[X_1, \ldots, X_m]$ es un domino de integridad y $f \notin \mathbb{K}$, el ideal $\mathfrak{a}$ está generado por un elemento que no es divisor de cero en $\mathbb{K}[X_1, \ldots, X_m]$. Por tanto, todos los ideales primos minimales sobre $\mathfrak{a}$ tienen altura 1. Por el Teorema de Lasker-Noether, el número de tales primos minimales es finito. Sean $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ esos primos minimales. Entonces $\sqrt{\mathfrak{a}} = \bigcap_{i=1}^{r} \mathfrak{p}_i$, con lo que $V_{\mathbb{A}}(\mathfrak{p}_i)$ es una variedad algebraica irreducible de dimensión $m - ht(\mathfrak{p}_i)$ (porque $\mathbb{K}[X_1, \ldots, X_m]$ es catenario). En consecuencia:

- $\dim V_{\mathbb{A}}(\mathfrak{p}_i) = m-1$ para cada $i, 1 \leq i \leq r$.
- $\dim V_{\mathbb{A}}(\mathfrak{a}) = m-1$.

□

Una observación clásica que puede encontrarse en cualquier texto básico del Álgebra Conmutativa o Geometría Algebraica de los citados en la Bibliografía es la siguiente proposición:

PROPOSICIÓN B.1.3. *Sean $V \subseteq \mathbb{A}^n$ e $W \subseteq \mathbb{A}^m$ dos variedades algebraicas afines. Sea $V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^m$ su producto. Entonces se cumple:*

$$\dim_{Krull}(V \times W) = \dim_{Krull}(V) + \dim_{Krull}(W).$$

Por lo que respecta a uniones e intersecciones de variedades algebraicas, el comportamiento es dispar y tenemos los resultados siguientes:

PROPOSICIÓN B.1.4. *Dada $V = W_1 \cup \cdots \cup W_s$ una unión cualquiera de variedades algebraicas afines (no necesariamente irreducibles), se tiene:*

$$\dim(V) = \max\{\dim(W_1), \ldots, \dim(W_s)\}.$$

En lo que concierne a la intersección, más errática con variedades algebracias, el siguiente resultado se encuentra en cualquier texto básico como [**Ha, 1977**] o [**Sha, 1974**]:

TEOREMA B.1.5 (**Teorema de la dimensión de la intersección**). *Sean V, W variedades de dimensiones r, s en $\mathbb{A}^n_K$ con K cuerpo. Entonces cada componente irreducible Z de la variedad $V \cap W$ cumple:*

$$\dim Z \geq r + s - n.$$

El siguiente resultado se encuentra en [**Sha, 1974**]:

TEOREMA B.1.6 (**Dimensión de las Fibras**). *Sean $V \subseteq \mathbb{A}^m(\mathbb{K})$ y $W \subseteq \mathbb{A}^n(\mathbb{K})$ dos variedades algebraicas irreducibles. Sea $f : V \longrightarrow W$ un morfismo dominante. Se tiene:*

i) Si $y \in f(V)$, entonces la fibra $f^{-1}(\{y\})$ verifica:

$$\dim f^{-1}(\{y\}) \geq \dim(V) - \dim(W).$$

ii) Existe un abierto Zariski $U \subseteq W$ tal que para cada $y \in W$ la fibra $f^{-1}(\{y\})$ es no vacía y verifica:

$$\dim f^{-1}(\{y\}) = \dim(V) - \dim(W).$$

B.2. Intersección de variedades algebraicas: desigualdad de Bézout afín

En esta sección del Apéndice haremos una breve descripción de la teoría del grado de locamente cerrados afines (es decir, intersección de un abierto y un cerrado) en la topología de Zariski de $\mathbb{A}^n(\mathbb{K})$. El origen de estos resultados es el clásico [**He, 1983**]. Una fuente más reciente ha sido [**GMLMPS, 2020**] y también [**Pa,20a**].
Sea $V \subseteq \mathbb{A}^n(K)$ un conjunto localmente cerrado irreducible de dimensión de Krull r. Sea $\mathbb{A}^{nr} := \mathbb{A}^{nr}(K) = \mathscr{M}_{r\times n}$ el espacio de las matrices $r \times n$ con coordenadas en K. Sea la siguiente aplicación polinomial:

$$\Phi : \mathbb{A}^{nr} \times V \longrightarrow \mathbb{A}^{nr} \times \mathbb{A}^r.$$
$$(M, x) \longmapsto (M, Mx).$$

Proposición B.2.1. *Con las notaciones anteriores:*

i) El morfismo Φ es un morfismo dominante y la siguiente es una extensión de cuerpo finita y separable:

$$\Phi^* : K(\mathbb{A}^{rn} \times \mathbb{A}^r) \hookrightarrow K(\mathbb{A}^{rn} \times V).$$

ii) Para cada punto $(M, b) \in \mathbb{A}^{rn} \times \mathbb{A}^r$, si la fibra $\Phi^{-1}(\{(M, n)\})$ es finita, se tiene:

$$\sharp(\Phi^{-1}(\{(M, b)\})) \leq [K(\mathbb{A}^{rn} \times V) : K(\mathbb{A}^{rn} \times \mathbb{A}^r)].$$

iii) Existe un abierto Zariski $\mathcal{U} \subseteq \mathbb{A}^{rn} \times \mathbb{A}^r$ tal que para cada $(M, b) \in \mathcal{U}$ la fibra $\Phi^{-1}(\{(M, n)\})$ es finita y satisface:

$$\sharp(\Phi^{-1}(\{(M, b)\})) = [K(\mathbb{A}^{rn} \times V) : K(\mathbb{A}^{rn} \times \mathbb{A}^r)].$$

Gracias al Lema de Normalización de Noether A.4.8 y el resultado B.2.1 se tiene el siguiente corolario, que es una versión geométrica del Lema de Normalización de Noether:

Corollario B.2.2. *Sea K un cuerpo de cardinal infinito y sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica K-definible. Sea $GL(n, K) \subseteq K^{n^2}$ el abierto Zariski de las matrices $n \times n$ con coeficientes en K.*
Si V es irreducible (o equi-dimensional) existe un abierto Zariski $U \subseteq GL(n, K)$ en el que toda matriz $A \in U$ verifica:

i) Sea la aplicación lineal de cambio de coordenadas siguiente:

$$A : \mathbb{A}^n(\mathbb{K}) \longrightarrow \mathbb{A}^n(\mathbb{K}).$$
$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \longrightarrow A \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}.$$

Se tiene que $A(V) = \mathbb{A}^m(\mathbb{K}) \times \{0\}^{n-m}$, siendo $m = \dim(V)$.

ii) La restricción

$$A|_V : V \longrightarrow \mathbb{A}^m(\mathbb{K}),$$
$$(x_1, \ldots, x_n) \longmapsto (l_1(x_1, \ldots, x_n), \ldots, l_m(x_1, \ldots, x_n)),$$

es suprayectiva.

iii) La extensión de anillos

$$K[Y_1, \ldots Y_m] \longmapsto K[V],$$

es una extensión entera.

iv) Para cada $b = (b_1, \ldots, b_m) \in \mathbb{A}^m(\mathbb{K})$ el número de puntos en la fibra $(A_V)^{-1}(\{b\})$ es finito.

Sean $r, n \in \mathbb{N}$ dos enteros positivos, $r \leq n$. Sea $\mathbb{G}(n,r)$ el "Grasmaniano" de variedades afines lineales de codimensión como máximo r del espacio afín $\mathbb{A}^n(\mathbb{K})$. Sea la proyección natural:

$$\mathscr{G} : \mathbb{A}^{nr} \times \mathbb{A}^n \longrightarrow \mathbb{G}(n,r),$$
$$(M,b) \longmapsto \mathbb{G}(M,b) := \{x \in \mathbb{A}^n(\mathbb{K}) : Mx^t - b = 0\},$$

donde x^t es la transpuesta de $x = (x_1, \ldots, x_n)$. Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ un conjunto irreducible localmente cerrado de dimensión r y sea la clase:

$$\mathbb{G}(V) := \{L \in \mathbb{G}(n,r) : \sharp(V \cap L) < \infty\},$$

Proposición B.2.3. *Con las condiciones anteriores:*

i) La clase $\mathbb{G}(V)$ es no vacía y contiene un abierto Zariski de $\mathbb{G}(n,r)$
ii) El máximo $\max\{\sharp(L \cap V) : L \in \mathbb{G}(V)\}$ es finito.
iii) Existe un abierto Zariski $\mathcal{U} \subseteq \mathbb{G}(n,r)$ tal que para todo $L \in \mathcal{U}$ se tiene

$$\sharp(L \cap V) = \max\{\sharp(T \cap V) : T \in \mathbb{G}(V)\}.$$

Definición 22 (Grado de un subconjunto localmente cerrado). *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ un subconjunto irreducible localmente cerrado de dimensión de Krull r. Se define el grado de V como:*

$$\deg(V) := \max\{\sharp(L \cap V) : L \in \mathbb{G}(n,r), \sharp(L \cap V) < \infty\}.$$

Sea $W \in \mathbb{A}^n(\mathbb{K})$ un subconjunto localmente cerrado y sea $C_1, \ldots, C_s$ sus componentes irreducibles localmente cerradas. El grado de W se define como:

$$\deg(W) := \sum_{i=1}^{s} \deg(C_i).$$

Se resumen unas propiedades inmediatas:

Teorema B.2.4. *Con las condiciones anteriores, se cumple:*

i) Para cada subconjunto localmente cerrado $V \subseteq \mathbb{A}^n(\mathbb{K})$ se cumple:

$$\deg(V) = \deg(\overline{V}^z).$$

ii) El grado de un conjunto finito de puntos $C \subseteq \mathbb{A}^n(\mathbb{K})$ es igual a su cardinal:

$$\deg(C) = \sharp(C).$$

iii) El número de componentes irreducibles de un conjunto localmente cerrado está acotado por su grado.
iv) El grado de cualquier variedad afín lineal es 1.
v) El grado de conjuntos localmente cerrados es invariante por isomorfismos lineales o afines.
vi) Para cada polinomio no constante $f \in K[X_1, \ldots, X_n]$ el grado de la hipersuperficie $V_{\mathbb{A}^n(\mathbb{K})}(f)$ es como mucho el grado del polinomio $\deg f$ y $V_{\mathbb{A}^n(\mathbb{K})}(f) = \deg(f)$ si y solo si f es libre de cuadrados.

Lema B.2.5. *Sea $V \subseteq \mathbb{A}^n(K)$ un subconjunto localmente cerrado y $L \subseteq \mathbb{A}^n(K)$ una variedad afín lineal. Se cumple que:*

$$\deg(V \cap L) \leq \deg(V).$$

Proposición B.2.6. *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ un conjunto equidimensional localmente cerrado de dimensión r. Se tiene:*

$$\deg(V) = \max\{\sharp(L \cap V) : L \in \mathbb{G}(n,r), \sharp(L \cap V) < \infty\}.$$

De hecho, existe un abierto Zariski $\mathcal{U} \subseteq \mathbb{A}^{nr+r}$ tal que para todo $(M,b) \in \mathcal{U}$, se tiene:

$$\sharp(\mathbb{G}(M,b) \cap V) = \deg(V),$$

donde, como antes, $\mathbb{G}(M,b) := \{x \in \mathbb{A}^n(\mathbb{K}) : Mx^t = b\}$.

Proposición B.2.7. *Sea $\mathscr{L} : \mathbb{A}^n(K) \longrightarrow \mathbb{A}^m(K)$ una aplicación lineal y $V \subseteq \mathbb{A}^n(K)$ un conjunto localmente cerrado. Entonces, se tiene:*

$$\deg(\overline{\mathscr{L}(V)}^z) \leq \deg(V).$$

De hecho, si $\mathscr{L}(V)$ es localmente cerrado, se tiene:

$$\deg(\mathscr{L}(V)) \leq \deg(V).$$

PROPOSICIÓN B.2.8. *Sean $V \subseteq \mathbb{A}^n(\mathbb{K})$ y $W \subseteq \mathbb{A}^m$ dos conjuntos localmente cerrados. Sea $V \times W \subseteq \mathbb{A}^{n+m}$ su producto cartesiano, que también es localmente cerrado. Entonces se tiene:*

$$\deg(V \times W) = \deg(V)\deg(W).$$

El siguiente resultado se puede encontrar en [**He, 1983**](ver también [**To, 2020**]):

TEOREMA B.2.9 (**Desigualdad de Bézout para conjuntos localmente cerrados**). *Sean $V, W \subseteq \mathbb{A}^n(K)$ dos conjuntos localmente cerrados. Entonces se tiene:*

$$\deg(V \cap W) \leq \deg(V)\deg(W).$$

El siguiente resultado se encuentra en el [**Ha, 1977**]*:*

PROPOSICIÓN B.2.10. *Sea $X \subset \mathbb{A}^n(\mathbb{K})$ una variedad algebraica afín irreducible.* $\dim X = n-1$ *si y solo si existe $f \in K[X_1, \ldots, X_n]$ polinomio irreducible tal que $X = V_{\mathbb{A}^n(\mathbb{K})}(f)$*

TEOREMA B.2.11. *El anillo de polinomios $\mathbb{K}[X_1, \ldots, X_n]$ es un anillo de Cohen-Macaulay. En particular, dada una sucesión de polinomios $f_1, \ldots, f_k \in \mathbb{K}[X_1, \ldots, X_m]$ tales que la variedad que definen $V_{\mathbb{K}}(f_1, \ldots, f_k)$ tiene dimensión $n-k$, entonces todas sus componentes irreducibles tienen dimensión $n-k$ y es por tanto una variedad equi-dimensional.*

B.3. Espacio tangente de variedades algebraicas afines: Criterio del Jacobiano

DEFINICIÓN 23 (Multiplicidad de intersección). *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica afín y $a \in V$ un punto. Sea $v \in \mathbb{A}^n(\mathbb{K})$ un vector y $L = \{a + tv : t \in K\}$ la recta que pasa por a y tiene dirección v. Sea $\{f_1, \ldots, f_s\}$ un conjunto generador finito de $I_K(V)$ (que existe por el Hilbert Bassisatz). Definiremos la multiplicidad de intersección de la reta L con la variedad V en el punto $a \in V$ a la cantidad siguiente:*

$$m(V, L, a) := ord_0(gcd_{K[T]}(f_1(a + Tv), \ldots, f_s(a + Tv))),$$

donde $ord_0 : K[[T]] \to \mathbb{N}_+$ es la función orden sobre el anillo de series de potencias formales en una variable y $gcd_{K[T]}$ es el máximo común divisor en $K[T]$ de los polinomios univariados $f_1(a + Tv), \ldots, f(a + Tv) \in K[T]$.

PROPOSICIÓN B.3.1. *La multiplicidad de la intersección no depende del sistema generador escogido.*

DEMOSTRACIÓN. Sea V la variedad, $a \in V$ un punto y $v \in \mathbb{A}^n(\mathbb{K})$ un vector cualquiera. Sean dos sistemas generadores distintos de $I_K(V)$, $\mathcal{F} = \{f_1, \ldots, f_s\}$ y $\mathcal{G} = \{g_1, \ldots, g_r\}$ y sean $m_{\mathcal{F}}$ y $m_{\mathcal{G}}$ las multiplicidades calculadas mediante ambos sistemas respectivamente. Se va a demostrar que $gcd_{K[T]}(f_1(a + Tv), \ldots, f_s(a + Tv)) = gcd_{K[T]}(g_1(a + Tv), \ldots, g_r(a + Tv))$. Como $I_K(V) = (f_1, \ldots, f_s) = (g_1, \ldots, g_r)$ se tienen, para dos matrices $A \in m_{s\times r}(K[X_1, \ldots, X_n])$ $B \in m_{r\times s}(K[X_1, \ldots, X_n])$, las siguientes igualdades en $K[X_1, \ldots, X_n]$:

$$\begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & & \vdots \\ a_{s1} & \ldots & a_{sr} \end{pmatrix} \begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix}, \quad \begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} = \begin{pmatrix} b_{11} & \ldots & b_{1s} \\ \vdots & & \vdots \\ b_{r1} & \ldots & b_{rs} \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix},$$

y por lo tanto, reemplazando las variables $X_1, \ldots, X_n$ por las coordenadas de $a + Tv$ se tienen las siguientes igualdades en $K[T]$:

$$\begin{pmatrix} f_1(a + Tv) \\ \vdots \\ f_s(a + Tv) \end{pmatrix} = \begin{pmatrix} a_{11}(a + Tv) & \ldots & a_{1r}(a + Tv) \\ \vdots & & \vdots \\ a_{s1}(a + Tv) & \ldots & a_{sr}(a + Tv) \end{pmatrix} \begin{pmatrix} a_1(a + Tv) \\ \vdots \\ a_r(a + Tv) \end{pmatrix},$$

$$\begin{pmatrix} g_1(a + Tv) \\ \vdots \\ g_r(a + Tv) \end{pmatrix} = \begin{pmatrix} b_{11}(a + Tv) & \ldots & b_{1s}(a + Tv) \\ \vdots & & \vdots \\ b_{r1}(a + Tv) & \ldots & b_{rs}(a + Tv) \end{pmatrix} \begin{pmatrix} f_1(a + Tv) \\ \vdots \\ f_s(a + Tv) \end{pmatrix},$$

y por lo tanto se tiene la siguiente igualdad de ideales en $K[T]$:

$$(f_1(a + Tv), \ldots, f_s(a + Tv)) = (g_1(a + Tv), \ldots, g_r(a + Tv)).$$

Como $K[T]$ es dominio de ideales principales, los MCD coinciden y por tanto se tiene:

$$m_{\mathcal{F}} = gcd_{K[T]}(f_1(a + Tv), \ldots, f_s(a + Tv)) = gcd_{K[T]}(g_1(a + Tv), \ldots, g_r(a + Tv)) = m_{\mathcal{G}}.$$

□

DEFINICIÓN 24 (Recta y vector tangentes). *Una recta L es tangente a una variedad algebraica V en un punto $a \in V$ si la multiplicidad de la intersección es igual o mayor que 2 en a (i.e. si $m(V, L, a) \geq 2$). Un vector $v \in \mathbb{A}^n(\mathbb{K})$ se dice que es tangente en $a \in V$ si la recta $L_v := \{a + tv : t \in K\}$ es tangente en a.*

TEOREMA B.3.2. *Existe una inmersión natural (monomorfismo de K-álgebras) de $K[X_1, \ldots, X_n]$ en $K[[X_1 - a_1, \ldots, X_n - a_n]]$. A la representación de un elemento $f \in K[X_1, \ldots, X_n]$ como serie de potencias formales se la denomina serie de Taylor de f en a y se denota mediante:*

$$T_a f := \sum_{|\mu| \leq d} (T_a f)^{(\mu)} (X_1 - a_1)^{\mu_1} \ldots (X_n - a_n)^{\mu_n}.$$

donde $d = deg(f)$. Más aún, si $p = caract(K)$ es la característica del cuerpo y $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$ es un exponente tal que $p \nmid \mu_i!, 1 \leq i \leq n$, entonces

$$(T_a f^{(\mu)}) = \frac{1}{\mu_1! \ldots \mu_n!} \frac{\partial^{|\mu|} f}{\partial x_1^{\mu_1} \ldots \partial x_n^{\mu_n}}.$$

DEMOSTRACIÓN. Consideremos el siguiente conjunto de polinomios multivariados:

$$\mathscr{S}_n = \{f \in K[X_1, \ldots, X_n] : \exists d \in \mathbb{N} \wedge \exists \{c_\mu : |\mu| \leq d\} \subseteq K : f = \sum_{|\mu| \leq d} c_\mu (x_1 - a_1)^{\mu_1} \cdots (x_n - a_n)^{\mu_n}\}.$$

Probemos que $\mathscr{S}_n = K[X_1, \ldots, X_n]$. Dado que la inclusión $\subseteq$ es obvia, se demuestra $\supseteq$ por inducción en n.

Si $n = 1$, hay que demostrar que $K[X_1] \subseteq \mathscr{S}_1$. Se hace por inducción en el grado de los polinomios. Sea $f \in K[X_1] : deg(f) = 0$, es obvio que $f \in \mathscr{S}_1$. Sea $f \in K[X_1] : deg(f) = d \geq 1$. Por la división euclídea, $f = q(X_1 - a_1) + r$ con $q \in K[X_1], r = f(a_1)$ y como q tiene grado menor que d, por hipótesis de inducción se tiene que $q = \sum_{k \leq d-1} c_k (X_1 - a_1)^k$. Por tanto $f = \left(\sum_{k \leq d_1} c_k (x_1 - a_1)^k\right)(x_1 - a_1) + f(a_1)$ y por tanto $f \in \mathscr{S}_1$. Así pues, se tiene $K[X_1] \subseteq \mathscr{S}_1$.

Sea ahora $n \geq 2$. Como todo $f \in K[X_1, \ldots, X_n]$ es suma de productos monomios por constantes, si se demuestra que todo monomio de $K[X_1, \ldots, X_n]$ pertenece a $\mathscr{S}_n$ se tiene que todo polinomio también lo cumple. Sea un monomio $X_1^{\mu_1} \cdots X_n^{\mu_n}$, se tiene, por lo ya demostrado, que $X_1^{\mu_1} = \sum_{k \leq \mu_1} c_k (X_1 - a_1)^k$, y por hipótesis de inducción, que $X_2^{\mu_2} \ldots X_n^{\mu_n} = \sum_{|\theta| \leq \mu_2 + \cdots + \mu_n} d_\theta (X_2 - a_2)^{\theta_2} \ldots (X_n - a_n)^{\theta_n}$. Por tanto:

$$X_1^{\mu_1} \cdots X_n^{\mu_n} = \left(\sum_{k \leq \mu_1} c_k (X_1 - a_1)^k\right) \left(\sum_{|\theta| \leq \mu_1 + \cdots + \mu_n} d_\theta (X_2 - a_2)^{\theta_2} \ldots (X_n - a_n)^{\theta_n}\right).$$

Por lo tanto, multiplicando y agrupando la anterior expresión, se llega a que todo $X_1^{\mu_1} \cdots X_n^{\mu_n} \in \mathscr{S}_n$ y por tanto todo polinomio, y así se tiene $\mathscr{S}_n = K[X_1, \ldots, X_n]$.
Por otro lado, en realidad se tiene que $\mathscr{S}_n = K[X_1, \ldots, X_n] \cap K[[X_1 - a_1, \ldots, X_n - a_n]]$ y que es un K-espacio vectorial de dimensión finita. Por lo tanto, la inclusión será un monomorfismo de K-espacios vectoriales:

$$\begin{aligned} \Phi : \mathscr{S}_n &\longrightarrow K[X_1, \ldots, X_n]. \\ f &\longrightarrow f. \end{aligned}$$

Por lo visto anteriormente, es suprayectivo y, por tanto, tiene inversa

$$\begin{aligned} \Phi^{-1} : K[X_1, \ldots, X_n] &\longrightarrow \mathscr{S}_n \subseteq K[[X_1 - a_1, \ldots, X_n - a_n]]. \\ f &\longrightarrow \Phi^{-1}(f) := T_a f. \end{aligned}$$

Para la segunda afirmación, se definen las derivaciones formales con respecto a cada variable como las K-aplicaciones lineales definidas según:

$$\begin{aligned} \frac{\partial}{\partial X_i} : K[X_1, \ldots X_n] &\longrightarrow K[X_1, \ldots, X_n]. \\ (X_1^{\mu_1} \cdots X_n^{\mu_n}) &\longrightarrow \mu_i X_1^{\mu_1} \cdots X_{i-1}^{\mu_{i-1}} X_i^{\mu_i - 1} X_{i+1}^{\mu_{i+1}} \cdots X_n^{\mu_n}. \end{aligned}$$

Obsérvese que verifica la regla de Leibniz, que para todo par $f, g \in K[X_1, \dots X_n]$, $\frac{\partial}{\partial X_i}(f \cdot g) = f \cdot \frac{\partial g}{\partial X_i} + g \cdot \frac{\partial f}{\partial X_i}$.
Los operadores siguientes se definen de forma recursiva:

- Para cada i y para cada $\mu \in \mathbb{N}$, $\frac{\partial^\mu}{\partial X_i^\mu} = \frac{\partial}{\partial X_i} \circ \overset{\mu}{\cdots} \circ \frac{\partial}{\partial X_i}$ es la composición de μ veces la derivación $\frac{\partial}{\partial X_i}$
- Para cada $\mu = (\mu_i, \dots, \mu_n) \in \mathbb{N}^n$ se define $\frac{\partial^{|\mu|}}{\partial X_1^{\mu_1} \dots \partial X_n^{\mu_n}} = \frac{\partial^{\mu_1}}{\partial X_1^{\mu_1}} \circ \cdots \circ \frac{\partial^{\mu_1}}{\partial X_n^{\mu_n}}$. Debido a la definición de la aplicación lineal, el orden de las derivadas no influye.

Sea $f \in K[X_1, \dots, X_n], a \in \mathbb{A}^n(\mathbb{K})$, y su desarrollo de Taylor en a es $T_a f = \sum_{|\theta| \leq d} (c_\theta)(X_1 - a_1)^{\theta_1} \dots (X_n - a_n)^{\theta_n}$. Sea $\mu = (\mu_1, \dots, \mu_n) \in \mathbb{N}^n$. Se demuestra que:

$$\frac{\partial^{|\mu|} f}{\partial X_1^{\mu_1} \dots \partial X_n^{\mu_n}}(a) = \mu_1! \cdots \mu_n! \cdot c_\mu.$$

Se demuestra para los monomios $M_\theta = (X_1 - a_1)^{\theta_1} \cdots (X_n - a_n)^{\theta_n} \in K[[X_1 - a_1, \dots, X_n - a_n]]$ y por linealidad se tiene el resultado para un polinomio f cualquiera. Existen distintos casos:

i) $\exists j : \theta_j \leq \mu_j - 1$, entonces $\frac{\partial^{|\mu|} M_\theta}{\partial X_1^{\mu_1} \dots \partial X_n^{\mu_n}} = 0$ en $K[X_1, \dots, X_n]$

ii) $\exists \theta_j \geq \mu_j \forall j, 1 \leq j \leq n$, $\exists i : \theta_i > \mu_i$, entonces se tiene

$$\frac{\partial^{|\mu|} M_\theta}{\partial X_1^{\mu_1} \cdots \partial X_n^{\mu_n}} = c_\theta \prod_{i=1}^{n} \prod_{k=1}^{\mu_i} (\theta_i - k + 1) \prod_{l=1}^{n} (X_l - a_l)^{\theta_l - \mu_l},$$

por lo que si $\exists i : \theta_i > \mu_i$ implica que $(X_i - a_i) | \frac{\partial^{|\mu|} M_\theta}{\partial X^{\mu_1} \dots \partial X_n^{\mu_n}}$ en $K[X_1, \dots X_n]$, y por tanto $\frac{\partial^{|\mu|} M_\theta}{\partial X_1^{\mu_1} \dots \partial X_n^{\mu_n}}(a) = 0$

iii) Por último si $\theta = \mu$, se tiene precisamente

$$\frac{\partial^{|\mu|} M_\theta}{\partial X_1^{\mu_1} \dots \partial X_n^{\mu_n}} = \mu_1! \cdots \mu_n! \cdot c_\mu.$$

Se tiene que esta expresión se anula solamente si $c_\mu = 0$ o si la característica del cuerpo divide a algún $\mu_i!$.

□

Corollario B.3.3. *Sea $f \in K[X_1, \dots, X_n]$ y sea su desarrollo de Taylor $f = \sum_{|\mu| \leq d} c_\mu (X_1 - a_1)^{\mu_1} \cdots (X_n - a_n)^{\mu_n}$ Entonces se tiene:*

i) $c_{(0,\dots,0)} = f(a_1, \dots, a_n)$

ii) Para cada i, sea c_{l_i} el coeficiente del sumando $(X_i - a_i)$ en la expansión de Taylor. Entonces

$$c_{l_i} = \frac{\partial f}{\partial X_i}(a_1, \dots, a_n).$$

En particular, dado $v \in \mathbb{A}^n(\mathbb{K})$ y dada la recta $L = \{a + tv : v \in K\}$. Entonces son equivalentes:

i) $ord_0(f(a + Tv)) \geq 2$

ii) $f(a_1, \dots, a_n) = 0$ *y* $\langle \nabla_a f, v \rangle = \sum_{i=1}^n v_i \frac{\partial f}{\partial X_i}(a) = 0$, *donde* $\nabla_a f = (\frac{\partial f}{\partial X_1}(a), \dots, \frac{\partial f}{\partial X_n}(a))$ *es el gradiente de f en a.*

Proposición B.3.4 (Definición del espacio tangente a una variedad algebraica afín). *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica afín, $a \in V$ un punto, $\{f_1, \dots, f_s\}$ un sistema generador del ideal $I_K(V)$ y $v \in \mathbb{A}^n(\mathbb{K})$ un vector. Sea $L = \{a + tv : t \in K\}$ la recta definida por v pasando por a. Son equivalentes*

i) L es tangente a V en a.

ii) La multiplicidad de intersección satisface $m(V, L, a) \geq 2$

iii) El vector v es tangente a V en a.

iv) Se tiene la propiedad

$$Df(a) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

donde $v = (v_1, \ldots, v_n)$, $f = \{f_1, \ldots, f_s\}$ *y* $Df(a)$ *es la matriz con* s *filas y* n *columnas cuyas filas son los gradientes de los polinomios en la familia* $\{f_1, \ldots, f_s\}$, *es decir*

$$Df(a)\begin{pmatrix}\nabla_a f_1\\ \vdots \\ \nabla_a f_s\end{pmatrix} = \begin{pmatrix}\frac{\partial f_1}{\partial X_1}(a) & \ldots & \frac{\partial f_1}{\partial X_n}(a)\\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial X_1}(a) & \ldots & \frac{\partial f_s}{\partial X_n}(a)\end{pmatrix}.$$

Se define el espacio tangente a V *en* a *como el subespacio vectorial* $T_aV \subseteq K^n$ *formado por los vectores tangentes a* V *en* a *y que viene dado por la igualdad siguiente:*

$$T_aV = \{v \in K^n : Df(a)\begin{pmatrix}v_1\\ \vdots \\ v_n\end{pmatrix} = 0\} = \{v \in K^n : \nabla_a f_i v = 0, 1 \leq i \leq s\},$$

igualdad independiente del conjunto de generadores de $I_K(V)$ *escogido.*

Definición 25. *Sea* $V \subseteq \mathbb{A}^n(\mathbb{K})$ *una variedad algebraica afín y* $a \in V$ *un punto.*

i) Decimos que $a \in V$ *es un punto regular (o liso) si la dimensión del espacio tangente* T_aV *coincide con la dimensión de Krull de* V.

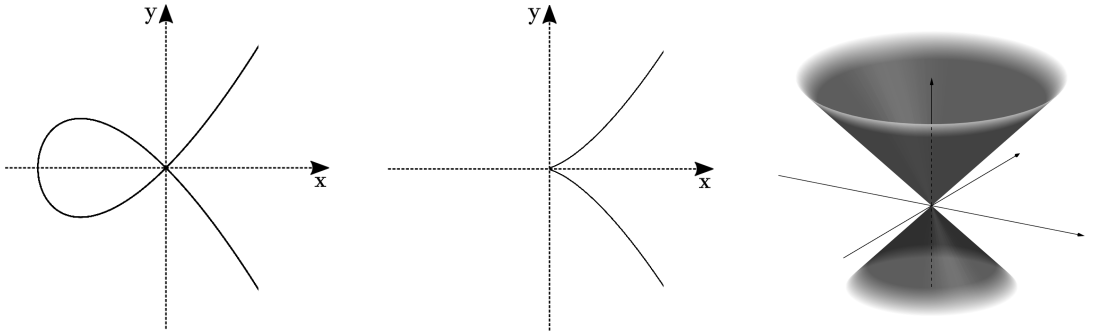
ii) Decimos que $a \in V$ *es un punto singular si* $\dim(T_aV) > \dim_{\text{Krull}}(V)$.

Ejemplo B.3.5. *En la Figura 1 se representan tres variedades con todos los puntos regulares salvo el origen.*

(A) $f = y^2 - x^2 - x^3$, $Df(x,y) = (-2x - 3x^2, 2y)$, *y en caso de ser* $x \neq 0$, $T_{(x,y)}V = \{\lambda\begin{pmatrix}3\\ -2\end{pmatrix} : \lambda \in \mathbb{C}\}$, *un espacio de dimensión 1, y por tanto* (x,y) *es un punto liso. Sin embargo, en el caso del* $(0,0)$, $Df(0,0) = (0,0)$, *y por tanto* $T_{(x,y)}V = \mathbb{C}^2$ *y entonces es un punto singular.*

(B) $f = y^2 - x^3$, $Df(x,y) = (-3x^2, 2y)$ *y un razonamiento similar al apartado anterior deduce que* $(0,0)$ *es el único punto singular.*

(C) $f = x^2 + y^2 - z^2$, $Df(x,y) = (2x, 2y, -2z)$ *y en este caso* $(0,0,0)$ *es el único punto singular.*



(A) $V_{\mathbb{A}}(y^2 - x^2 - x^3)$ (B) $V_{\mathbb{A}}(y^2 - x^3)$ (C) $V_{\mathbb{A}}(x^2 + y^2 - z^2)$

Figure 1. Proyección real de las variedades cuyo origen es un punto singular.

Con las notaciones precedentes, sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica afín irreducible, $a \in V$ un punto, y $K[V]$ el anillo de funciones polinomiales definidas en V. Sea $\mathfrak{n}_a = (X_1 - a_1, \ldots, X_n - a_n) = \{f \in K[X_1, \ldots, X_n] : f(a) = 0\}$ el ideal maximal de los polinomios en $K[X_1, \ldots, X_n]$ que se anulan en el punto a. Tendremos que $I_K(V)$ está contenido en $\mathfrak{n}_a$ y consideremos la localización en a de $K[X_1, \ldots, X_n]$, es decir, el anillo siguiente:

$$K[\mathbb{A}^n(\mathbb{K})]_a := K[X_1, \ldots, X_n]_{\mathfrak{n}_a}.$$

Los ideales primos de $K[\mathbb{A}^n(\mathbb{K})]_a$ están en biyección con los ideales primos de $K[X_1, \ldots, X_n]$ contenidos en $\mathfrak{n}_a$ según la Proposición A.1.5. En particular, $I_K(V)$ se relaciona con el ideal primo

$$I_K(V)_{\mathfrak{n}_a} := \{f/g : f \in I_K(V), g \notin \mathfrak{n}_a\} \in Spec(K[\mathbb{A}^n(\mathbb{K})]_a).$$

Sea ahora el anillo cociente siguiente:

$$K[V]_a := K[\mathbb{A}^n(\mathbb{K})]_a / I_K(V)_{\mathfrak{n}_a}.$$

Por otro lado, el ideal $\mathfrak{n}_a/I_K(V)$ es maximal en $K[V]$ porque, por el Segundo Teorema de Isomorfía, se tiene que el anillo cociente cumple:

$$K[V]\Big/\left(\mathfrak{n}_a\Big/I_K(V)\right) = \left(K[X_1,\dots,X_n]\Big/I_K(V)\right)\Big/\left(\mathfrak{n}_a\Big/I_K(V)\right) \cong K[X_1,\dots,X_n]\Big/\mathfrak{n}_a = K,$$

y por tanto es cuerpo.
Denotemos por $\mathfrak{m}_a = \mathfrak{n}_a / I_K(V) \in Spm(K[V])$ y podemos localizar $K[V]$ por $\mathfrak{m}_a$. Las propiedades de exactitud de la localización implican el siguiente isomorfismo:

$$K[V]_a \cong K[V]_{\mathfrak{m}_a}.$$

Denotemos también por $\mathfrak{m}_a$ a $\mathfrak{m}_a K[V]_{\mathfrak{m}_a}$ y sea $\mathfrak{m}_a^2$ su cuadrado.

DEFINICIÓN 26. *Al siguiente espacio vectorial se le denomina K-espacio vectorial de los diferenciales en a asociados a V.*

$$\mathfrak{m}_a\Big/\mathfrak{m}_a^2 = \mathfrak{m}_a K[V]_{\mathfrak{m}_a}\Big/\mathfrak{m}_a^2 K[V]_{\mathfrak{m}_a}.$$

Para entender la definición, se define la función de los diferenciales de un polinomio f en un punto $a \in \mathbb{A}^n(\mathbb{K})$:

$$d_a f := \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(X_i - a_i) \in K[X_1, \dots X_n].$$

Este polinomio de grado 1 se puede identificar con la función local definida sobre K^n por el gradiente:

$$\begin{aligned} d_a f : K^n &\longrightarrow K. \\ v &\longrightarrow \nabla_a f \cdot v = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a) \cdot v_i. \end{aligned}$$

Consideremos la aplicación siguiente:

$$\begin{aligned} d_a : K[X_1,\dots,X_n] &\longrightarrow \mathfrak{n}_a. \\ f &\longrightarrow d_a f. \end{aligned}$$

PROPOSICIÓN B.3.6. *La aplicación d_a es un morfismo de K-espacios vectoriales que verifica, además, la regla de Leibniz:*

$$d_a(fg) = f(a)d_a g + g(a)d_a g \in \mathfrak{n}_a. \tag{B.3.1}$$

Además, el núcleo de d_a está identificado por

$$\mathfrak{n}_a \cap \ker(d_a) = \mathfrak{n}_a^2 = \{f : f(a) = 0, \nabla_a f = (0,\dots,0)\}. \tag{B.3.2}$$

DEMOSTRACIÓN. Se cumple que $d_a(0) = 0$ y que $d_a(f+g) = \sum_{i=1}^n \frac{\partial(f+g)}{\partial X_i}(a)(X_i - a_i) = \sum_{i=1}^n \frac{\partial f}{\partial X_i}(a)(X_i - a_i) + \sum_{i=1}^n \frac{\partial g}{\partial X_i}(a)(X_i - a_i) = d_a(f) + d_a(g)$, así que es un morfismo de grupos, y evidentemente se cumple que $d_a(\lambda \cdot f) = \lambda \cdot d_a(f)$, por tanto se tiene que es un morfismo de K-espacios vectoriales.
Por otra parte, la igualdad B.3.1 se comprueba como un mero ejercicio de reescritura a partir de la definición.
Por último, la igualdad B.3.2 se demuestra por doble contenido. Por una parte se tiene que $\mathfrak{n}_a^2 \subseteq \mathfrak{n}_a$ y por otra, $\mathfrak{n}_a^2$ está generado por los productos de los generadores de $\mathfrak{n}_a$, por tanto, sus elementos serán combinación y producto de elementos tipo $(X_i - a_i)(X_i - a_j)$ con $i, j \in \{1,\dots,n\}$. Simplemente, a partir de B.3.1 se comprueba que $d_a((X_i - a_i)(X_i - a_j)) = 0$, y por tanto se concluye que $\mathfrak{n}_a^2 \subseteq \ker(d_a)$ y por tanto, se tiene el primer contenido.
Para el segundo, sea $f \in K[X_1,\dots,X_n]$ tal que $f \in \mathfrak{n}_a$. Por el desarrollo de Taylor de f en a:

$$f = f(a) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(X_i - a_i) + h,$$

con $h \in \mathfrak{n}_a^2$ dado que es combinación de elementos tipo $(X_1 - a_1)^{\mu_1} \cdots (X_n - a_n)^{\mu_n}$ con $\mu_1 + \cdots + \mu_n \geq 2$. Por tanto, $d_a f = 0$ si y solo si $\nabla_a f = 0$.

□

COROLLARIO B.3.7. *Sea $(K^n)^* = \mathrm{Hom}_K(K^n, K)$ el espacio dual de K^n. Tenemos el isomorfismo siguiente de K-espacios vectoriales:*

$$\begin{aligned} D_a : {\mathfrak{n}_a}\Big/{\mathfrak{n}_a^2} &\longrightarrow (K^n)^*. \\ f + \mathfrak{n}_a^2 &\longrightarrow d_a f. \end{aligned}$$

DEMOSTRACIÓN. Basta con ver que los duales de la base canónica de K^n están en la imagen de este morfismo de K-espacios vectoriales. De hecho, para $i = 1, X_1 + \mathfrak{n}_a^2 \in \mathfrak{n}_a / \mathfrak{n}_a^2, D_a(X_1 + \mathfrak{n}_a^2) = d_a(X_1)$ es la aplicación cuya imagen por $(1, 0, \ldots, 0) \in K^n$ es 1, pero para cualquier elemento $(0, \ldots, 1, \ldots) \in K^n$ su imagen es 0, es decir, es el dual del elemento $(1, 0, \ldots, 0)$ de la base canónica de K^n. El razonamiento es análogo para todo $i \in \{1, \ldots, n\}$. □

Sea ahora $V \subseteq \mathbb{A}^n(\mathbb{K})$ variedad algebraica afín irreducible y el ideal maximal $\mathfrak{m}_a K[V]_{\mathfrak{m}_a}$ citado anteriormente.

PROPOSICIÓN B.3.8. *El siguiente es un isomorfismo de K-espacios vectoriales:*

$$\begin{aligned} D_a|_{T_aV} : {\mathfrak{m}_a}\Big/{\mathfrak{m}_a^2} \cong {\mathfrak{m}_a K[V]_{\mathfrak{m}_a}}\Big/{\mathfrak{m}_a^2 K[V]_{\mathfrak{m}_a}} &\longrightarrow (T_aV)^*. \\ f + \mathfrak{m}_a^2 &\longrightarrow d_a f|_{T_aV}. \end{aligned}$$

DEMOSTRACIÓN. En primer lugar, veamos que es un morfismo, esto es, que está bien definido. Primero, por la definición del espacio tangente T_aV en B.3.4, se tiene que $\forall v \in T_aV, \forall f \in I_K(V), \nabla_a f \cdot v = 0$. Por tanto se tiene que $\mathfrak{n}_a^2 + I_K(V) \subseteq \ker(D_a|_{T_aV})$.
Segundo, nótese la siguiente igualdad:

$${\mathfrak{m}_a}\Big/{\mathfrak{m}_a^2} = {\mathfrak{n}_a}\Big/{I_K(V)}\Big/{(\mathfrak{n}_a^2 + I_K(V))}\Big/{I_K(V)} \cong {\mathfrak{n}_a}\Big/{\mathfrak{n}_a^2 + I_K(V)}.$$

Sean dos elementos $x, y \in \mathfrak{m}_a / \mathfrak{m}_a^2$, serán de la forma $x = g + \mathfrak{m}_a^2, y = h + \mathfrak{m}_a^2$ con $g, h \in \mathfrak{m}_a$. A su vez, estos elementos x, y tendrán, independientemente de sus representantes g y h, asociados dos elementos $x', y' \in \mathfrak{n}_a / (\mathfrak{n}_a^2 + I_K(V))$ de la forma $x' = g' + (\mathfrak{n}_a^2 + I_K(V)), y' = h' + (\mathfrak{n}_a^2 + I_K(V))$ con $g', h' \in \mathfrak{n}_a$. Se comprueba que la aplicación $D_a|_{T_aV}$ es independiente del representante de estos últimos, y así queda bien definida. Sea entonces $x' = g' + (\mathfrak{n}_a^2 + I_K(V)) = g'' + (\mathfrak{n}_a^2 + I_K(V))$, lo que implica que $g' - g'' \in \mathfrak{n}_a^2 + I_K(V)$. La imagen de x' será, por una parte $D_a|_{T_aV}(x') = d_a g'|_{T_aV}$, pero por otra $D_a|_{T_aV}(x') = d_a g''|_{T_aV}$, y solo será cierto si $d_a g'|_{T_aV} - d_a g''|_{T_aV} = d_a(g' - g'')|_{T_aV} = 0$, lo cual es cierto porque $g' - g'' \in \mathfrak{n}_a^2 + I_K(V) \subseteq \ker(D_a|_{T_aV})$.

Para ver que es epimorfismo, observemos que todo elemento de $(T_aV)^* = \hom_K(T_aV, K)$ es la restricción a T_aV de un elemento de K^*, por eso, por el Corolario B.3.7, si $L \in (T_aV)^*, \exists f \in \mathfrak{n}_a / \mathfrak{n}_a^2 : L = d_a f|_{T_aV}$ y por tanto $D_a : \mathfrak{n}_a / \mathfrak{n}_a^2 \longrightarrow (T_aV)^*$ es un epimorfismo de espacios vectoriales, y según las explicaciones anteriores, también lo es $D_a|_{T_aV}$.

Veamos que es monomorfismo. Así, sea $x = f' + \mathfrak{m}_a^2 \in \mathfrak{m}_a / \mathfrak{m}_a^2, x = f + (\mathfrak{n}_a^2 + I_K(V)) \in \mathfrak{n}_a / \mathfrak{n}_a^2 + I_K(V)$ tal que $D_a|_{T_aV}(x) = d_a f|_{T_aV} = 0$. Veamos que $x = 0$. Recordemos que $T_aV = \{v : \nabla_a f_i \cdot v = 0, 1 \leq i \leq s\}$ donde $I_K(V) = (f_1, \ldots, f_s)$. Entonces T_aV es el subespacio dado mediante

$$T_aV = \bigcap_{i=1}^{s} \ker(d_a f_i).$$

En particular, si L es una función lineal, $L \in (K^n)^*$ tal que $L|_{T_aV} = 0$, se tiene que L es una combinación lineal de las funciones lineales $\{d_a f_1, \ldots, d_a f_s\}$. Es decir, existen $\lambda_1, \ldots, \lambda_s \in K$ tales que

$$L = \lambda_1 d_a f_1 + \cdots + \lambda_s d_a f_s. \tag{B.3.3}$$

Como identidad en $(K^n)^*$.

Sea $L = d_a f$ y, por la Identidad B.3.3, existirán $\lambda_1, \dots, \lambda_s \in K$ tales que

$$d_a f = \lambda_1 d_a f_1 + \cdots + \lambda_s d_a f_s,$$

y ésta es una igualdad en $(K^n)^*$. Consideramos el polinomio $g = f - \lambda_1 f_1 + \cdots + \lambda_s f_s$. Observamos que, por linealidad, $d_a g = d_a f - \lambda_1 d_a f_1 \cdots - \lambda_s d_a f_s = 0$ en $(K^n)^*$. Por tanto, $g \in \ker(d_a)$. Como, además, $g(a) = f(a) - \lambda_1 f_1(a) \cdots - \lambda_s f_s(a) = 0$, tendremos que $g \in \mathfrak{n}_a \cap \ker(d_a)$. Por la proposición precedente, concluimos que $g \in \mathfrak{n}_a^2$ y por tanto

$$f = g + \lambda_1 f_1 + \cdots + \lambda_s f_s \in \mathfrak{n}_a^2 + I_K(V),$$

con lo que $x = 0$ y es un monomorfismo. □

Definición 27 (Anillo catenario). *Un anillo R se denomina catenario si para cualquier par de ideales primos tales que $\mathfrak{p} \subseteq \mathfrak{p}'$ de R se verifica que:*

$$ht\left(\mathfrak{p}' \Big/ \mathfrak{p}\right) = ht(\mathfrak{p}') - ht(\mathfrak{p}).$$

Corollario B.3.9. *(Criterio del Jacobiano) Sea K un cuerpo algebraicamente cerrado, $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible, $a \in V$. Con las notaciones precedentes, son equivalentes:*

i) $a \in V$ es liso (i.e. $\dim T_a V = \dim_{Krull}(V)$).

ii) Las siguientes dimensiones coinciden:

$$\dim_K \left(\mathfrak{m}_a \Big/ \mathfrak{m}_a\right) = \dim_{Krull}(V) = \dim_{Krull}(K[V]_a).$$

iii) El anillo $K[V]_a$ es un anillo local regular.

iv) El anillo graduado siguiente es un anillo de polinomios en d variables con coeficientes en K

$$G_{\mathfrak{m}_a K[V]_a}(K[V]_a),$$

siendo $d = \dim_{Krull}(V)$

v) Para cualquier sistema generador $\{f_1, \dots, f_s\}$ del ideal $I_K(V)$, el rango de la matriz jacobiana

$$D(f_1, \dots, f_s)(a) = \left(\frac{\partial f_i}{\partial X_j}(a)\right)_{\substack{1 \le i \le s \\ 1 \le j \le n}},$$

tiene rango $n - d$, con $d = \dim_{Krull}(V)$.

Demostración. La equivalencia entre *i)* y *ii)* se sigue porque $\mathfrak{m}_a / \mathfrak{m}_a^2 = (T_a V)^*$ y por tanto, por ser duales, ambos tienen la misma dimensión.

La equivalencia entre *ii)*, *iii)* y *iv)* se recoge en [**Ei, 1995**], y se sigue de las propiedades que caracterizan los anillo locales regulares, observando que, por ser $K[X_1, \dots, X_n]$ un anillo catenario se tiene:

$$\begin{aligned} d = \dim K[V]_a = \dim \left(K[X_1, \dots, X_n]_a \Big/ I_K(V) K[\mathbb{A}^n(\mathbb{K})]_a\right) = coht(I_K(V) K[\mathbb{A}^n(\mathbb{K})]_a) = \\ ht(\mathfrak{n}_{\mathfrak{a}}) - ht(I_K(V)) = n - (n - coht(I_K(V))) = n - n + coht(I_K(V)) = \\ coht(I_K(V)) - \dim_{Krull}(K[V]) = dim_{Krull}(V). \end{aligned}$$

La equivalencia de *i)* con *v)* se obtiene a partir de la definición de espacio tangente B.3.4 como núcleo de la aplicación definida mediante la matriz jacobiana $D(f_1, \dots, f_s)$. Por tanto, $\dim(T_a V) = \dim(\ker(D(f_1, \dots, f_s)(a))) = n - \operatorname{rank}(D(f_1, \dots, f_s)(a))$. □

Lema B.3.10. *El conjunto de puntos lisos de una variedad irreducible no es vacío.*

Demostración. Sea V la variedad irreducible, y sea $I_K(V) = (f_1, \dots f_k) \subseteq K[X_1, \dots X_n]$ su ideal asociado, que como es primo, cumple $\sqrt{I_K(V)} = I_K(V)$. Además, supongo que k es el menor entero que cumple lo anterior, y que $MCD(f_i, f_j) = 1\ \forall i, j \in \{1, \dots, k\}$, es decir, que es una sucesión regular. Entonces, precisamente, se tiene que $\dim(V) = n - k$.
Sea $D_{(i_1, \dots, i_k)}$ el determinante del menor $(i_1, \dots, i_k)$ de la matriz jacobiana. Sea $f_{(i_1, \dots, i_k)}$ un factor irreducible de $D_{(i_1, \dots, i_k)}$, que por ser irreducible, el ideal $(f_{(i_1, \dots, i_k)})$ es un ideal primo de altura 1.

Supongo que no existen puntos lisos, entonces, por B.3.9, $\forall a \in V$, la matriz $D(f_1, \dots, f_k)(a)$ tiene rango menor que $n - \dim(V) = k$, por tanto, todos los menores $k \times k$ se anularán en todo a y por tanto, $a \in V_{\mathbb{A}^n(\mathbb{K})}(D_{(i_1,\dots,i_k)})$, y por el Nullstellenstz se tiene:

$$I_K(V) = \sqrt{I_K(V)} \subseteq \bigcup_{i_1,\dots,i_k} \sqrt{(D_{(i_1,\dots,i_k)})} \subseteq \bigcup_{i_1,\dots,i_k} (f_{(i_1,\dots,i_k)}).$$

Si un ideal primo está contenido en la unión de ideales primos, debe estar contenido en al menos en uno de ellos, por tanto, $I_K(V) \subseteq (f_{(i_{10},\dots,i_{k0})})$ para algún $f_{(i_{10},\dots,i_{k0})}$. Si $k > 1$, como la altura de $I_K(V)$ es precisamente k, se tendría un ideal de altura k contenido en otro de altura 1, absurdo.
Si $k = 1$, puedo asumir que f_1 es irreducible, y entonces se tiene que f_1 y $\frac{\partial f}{\partial X_i}$ son primos entre sí, así que no puede ocurrir que $(f_1) \subseteq (f_i)$ para ningún i.

□

Proposición B.3.11. *Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible. El conjunto de puntos lisos es denso en V.*

Demostración. En primer lugar, el conjunto de los puntos lisos no es vacío por B.3.10. Sea $I_K(V) = (f_1, \dots, f_s)$, sea la matriz Jacobiana $D(f_1 \dots, f_s)(x) = \left(\frac{\partial f_i}{\partial X_j}(x)\right)_{\substack{1 \le i \le s \\ 1 \le j \le n}}$. Como el conjunto de puntos lisos no es vacío, $\exists a : \operatorname{rank} D(f_1 \dots, f_s)(a) = n - \dim_K V = r$. Sea $M(X_1, \dots, X_n)$ un menor $r \times r$ de $D(f_1 \dots, f_s)(x)$ con determinante $\det M(a) \neq 0$ y sean los conjuntos siguientes:

$$A = \{M(X_1, \dots, X_n) : M \text{ es menor de } D(f)(X_1, \dots, X_s), s \times s, r = s\},$$
$$B = \{N(X_1, \dots, X_n) : N \text{ es menor de } D(f)(X_1, \dots, X_s), s \times s, r < s\},$$
$$\widetilde{A} = \{\det M : M \in A\} \subseteq K[X_1, \dots, X_n],$$
$$\widetilde{B} = \{\det N : N \in B\} \subseteq K[X_1, \dots, X_n],$$

Se tiene que $\forall f \in \widetilde{B}, \forall a \in V, f(a) = 0$ porque si el punto a es liso, la matriz jacobiana tiene rango $r < s$, y por tanto, los menores de tamaño $s \times s$ se anulan en a, y si el punto a es singular, la dimensión del espacio tangente será mayor que la dimensión de V, y por la definición de espacio tangente, implica que la matriz jacobiana en a tendrá rango menor que en el caso anterior, es decir, menor que r. Por tanto, $\widetilde{B} \subseteq I_K(V)$. Además, debe existir $p \in \widetilde{A} : q \notin I_K(V)$, es decir, $\exists p \in \widetilde{A}, \exists a \in V : p(a) \neq 0$ porque el conjunto de puntos lisos no es vacío. Así pues, se tienen las siguientes implicaciones:

$$a \in V \text{ es singular} \Leftrightarrow q(a) = 0 \ \forall q \in \widetilde{B} \wedge p(a) = 0 \ \forall p \in \widetilde{A},$$

que implica que $\operatorname{Sing}(V) \subseteq V \cap \{a : p(a) = 0 \ \forall p \in \widetilde{A}\}$. Por tanto, se tiene que $\operatorname{Sing}(V) \subseteq V_{\mathbb{A}^n(\mathbb{K})}(I_K(V) + (p))$. Veamos que $\dim V_{\mathbb{A}^n(\mathbb{K})}(I_K(V) + (p)) \lneq \dim V$ y habremos acabado.
Por el teorema del ideal principal de Krull A.2.5, se tiene que, si $p \in \widetilde{A}, p \notin I_K(V)$, entonces se cumple que

$$\dim \left(K[X_1, \dots, X_n] \Big/ I_K(V) + (p) \right) = \dim K[V] - 1,$$

y por tanto $\operatorname{Sing}(V) \subseteq \dim V_{\mathbb{A}^n(\mathbb{K})}(I_K(V) + (p)) \lneq \dim V$, y como $V_{\mathbb{A}^n(\mathbb{K})}(I_K(V) + (p))$ es un cerrado de Zariski, entonces $\overline{\operatorname{Sing}(V)} \subseteq V_{\mathbb{A}^n(\mathbb{K})}(I_K(V) + (p))$, y por tanto, $\dim(\overline{\operatorname{Sing}(V)}) \lneq \dim(V)$. Como los abiertos son densos, $\overline{V \setminus \overline{\operatorname{Sing}(V)}} = V$, y por tanto, los puntos lisos son densos.

□

Bibliografía

[AM, 1969] M. F. Atigah, I. G. Macdonald, *"Introduction to Conmutative Algebra"*. Addison-Wesley Publishing Co., 1969 [1ª Edición en español, en E. Reverté 1980].

[Ar, 2006] E. Arrondo, *Another Elementary Proof of the Nullstellensatz*. Amer. Math. Monthly **13** (2006), 169-171.

[Bez, 1779] É. Bézout, *"Théorie générale des equations algebraiques"*. Paris, France, Ph.D. , 1779.

[Br, 1987] W. D. Brownawell, *Bounds for the degree in the Nullstellensatz*. Annals of Math. **126** (1987), 577-591.

[Ch, 1936] A. Church, *An unsolvable problem of elementary number theory*. Amer. J. Math. **58** (1936), 345-363.

[CGH, 1989] L. Caniglia, A. Galligo y J. Heintz *Borne simplement exponentielle pour les degrèes dans le théorème des zèros sur un corps de caractéristique quelconque* C.R. Acad. Sci. Paris, t. **307**, Série I (1988), 255-258.

[Ei, 1995] D. Eisenbud, *"Commutative algebra: with a view toward algebraic geometry"*, Springer Verlag, 1995.

[GJW, 2002] H.-L. Gan, J.-S. Jeang, N.-C. Wang, *An algebraic approach to the Banach-Stone theorem for separating linear bijections*. Tai. J. of Math. **6** (2002), 399-403.

[GHMP, 1995] M. Giusti, J. Heintz, J.E. Morais, Luis M. Pardo, *When polynomial equation systems can be solverd fast?*. In "Proc. AAECC-11", G. Cohen, M. Giusti, T. Mora (eds.) Lecture Notes in Comput. Sci. **948** (1995), 205-231.

[GHMP, 1997a] M. Giusti, J. Heintz, J.E. Morais, L. M. Pardo, *Straight-line programs in geometric elimination theory*. Journal of Pure and Applied Algebra **124** (1998), 101-146.

[GHHMMP, 1997b] M. Giusti, K. Hägele, J. Heintz, J. Morgenstern, J.L. Montaña, L. M. Pardo, *Lower bounds for diophantine approximations*. Journal of Pure and Applied Algebra **117** & **118** (1997), 277-317.

[GHMMP, 1998] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L. M. Pardo, *Straight-line programs in geometric elimination theory*. Journal of Pure and Applied Algebra **124** (1998), 101-146.

[GMLMPS, 2020] M. Giusti, J. Heintz, G. Lecerf, G. Matera, L. M. Pardo, P. Solernó, *"Résolution Géométrique"*. Libro en preparación, 2020.

[GJ, 1976] L. Gillman, M. Jerison, *"Rings of Continuous Functions"*. Springer-Verlag, New York, 1976.

[Gö, 1931] K. Gödel, *"Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I"*. Monatshefte für Mathematik und Physik **38** (1931), 173-198.

[Ha, 1977] R. Hartshorne, *"Algebraic geometry"*. Graduate Texts in Mathematics, Springer, 1977.

[He, 1983] J. Heintz, *"Definability and Fast Quantifier Elimination over Algebraically Closed Fields"*. Theoretical Computer Science **24** (1983), 239-277.

[He, 1996] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*. Math. Ann. **95** (1926), 736-788.

[Hi, 1890] D. Hilbert, *Über die Theorie der algebraischen Formen*. Math. Ann. **36** (1890), 473-534.

[Hi, 1893] D. Hilbert, *Ueber die vollen Invariantensysteme*. Math. Ann. **42** (1893), 313-373.

[HMPS, 2000] K. Hägele, J.E. Morais, M. Sombra, L. M. Pardo, *The intrinsic complexity of the Arithmetic Nullstellensatz*. J. of Pure and App. Algebra vol. **146**, (2000), 103-183.

[Je, 2001] Z. Jelonek, *Topological characterization of finite mappings*. Bull. Pol. Acad. Sci., Math **49** (2001), 375-379.

[Je, 2005] Z. Jelonek, *On the effective Nullstellensatz*. Inventiones mathematicae **162** (2005), 1-17.

[KrPa, 1996] T. Krick, L.M. Pardo, *A Computational Method for Diophantine Approximation*. In Algorithms in Algebraic Geometry and Applications, Proc. MEGA'94, Progress in Mathematics **143**, Birkh auser Verlag, (1996), 193-254.

[Kol, 1988] Z. Kollár, *Sharp Efective Nullstellensatz*. J. of A.M.S. **1** (1988), 963-975.

[Kol, 1999] Z. Kollár, *Effective Nullstellensatz for arbitrary ideals*. J. Eur. Math. Soc. (JEMS) **1** (1999), 313-337.

[KPS, 2001] T. Krick, L.M. Pardo, M. Sombra, *Sharp Estimates for the Arithmetic Nullstellensatz*. Duke Math. Journal **109** (2001), 521-598.

[Kl, 1936] S. C. Kelene, *λ-definability and recursiveness*. Dube Math. J. **2** (1936), 340-353.

[Kr, 1882] L. Kronecker, *Grundzüge Einer Arithmetischen Theorie Der Algebraischen Grössen*. J. reine angew. Math. **92** (1882), 1-122.

[Ku, 1885] E. Kunz, *"Introduction to Commutative Algebra and Algebraic Geometry"*. Birkhäuser, 1985.

[MaWü, 1971] D. W. Masser, G. Wüstholz, *Fields of large transcendence degree generated by values of elliptic functions*. Invent. Math. **72** (1971), 407-463.

[Mtj, 1970] Ju. V. Matijasevicz, *Enumerable sets are definable*. Soviet Math. Dolkl. **11.2** (1970), 354-358.

[Ma, 1980] H. Matsumura, *Commutative Algebra. (2nd. Edition)*", Benjamin/Cummings, 1980.

[Noe, 1921] E. Noether, *Idealtheorie in Ringbereichen*. Math. Ann. **83** (1921), 24-66.

[Pa, 1995] L. M. Pardo, *How lower and upper complexity bounds meet in elimination theory*. En "Proceding AAECC-11" C. Cohen, M. Giusti, T. Mora (eds), Lecture Notes in Comput. Sc. **948** (1995), 33-69.

[Pa,19] L. M. Pardo, *"Incidences; travaux en cours, "rendu tardif"; grèves sans préavis et perturbations dans l'ensemble de la ligne"*. Manuscrito no publicado, París, 2019.

[Pa,20a] L. M. Pardo, *"Notas para un curso Básico de Álgebra Conmutativa"*. Manuscrito, Univ. de Cantabira, 2020.

[Ra, 1929] G. Y. Rainich (pseudonym J.L. Rabinowitsch), *Zum Hilbertschen Nullstellensatz*. Math. Ann. **102** (1929), 520

[Ro, 1966] J. Robinson, *The undecidability of exponential diophantine equations*. En "Logic, Methodilogy and Philosophy of Science"; E.Nugel, P.Suppers, A.Tarski (eds.), Studies in Logic and the Foundations of Mathematics. **44** (1966), 12-13.

[Sha, 1974] I. R. Shafarevich, *"Basic Algebraic Geometry"*. Springer-Verlag, 1974.

[Som, 1999] M. Sombra, *A Sparse Effective Nullstellensatz*. Adv. in Appl. Math. **22** (1999), 271-295.

[Syl, 1853] J.J. Sylvester, *On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraical common measure*. Phil. Trans. of the Royal Soc. of London. **CXLIII** (1853), 407-548.

[To, 2020] T. Fernández, *"Una Deconstrucción de la Desigualdad de Bézout de* [**He, 1983**]*"*. Trabajo Fin de Grado de Matemáticas, Universidad de Cantabria, dirigido por Lus M. Pardo, 2020.

[Tu, 1937] A. Turing, *On Computable Numbers, with an application to the Entscheidungs Problem*. Proc. of the London Math. Soc. **42** (1936-37), 153-163.