
# Algunas Notas para un Curso Básico sobre Métodos Efectivos en Geometría Algebraica (MEGA)

Luis M. Pardo

# Índice general

Capítulo 1

# Introducción

Estas páginas tratan de la resolución por medios intrínseco-gométricos de sistemas de ecuaciones polinomiales. Adicionalmente, trata de mostrar la complejidad de tales algoritmos.
Las preguntas iniciales que uno debe hacerse para presentar un algoritmo y un problema son las siguientes:

- *¿ Qué se pretende?, ¿para qué propósitos?.*
- *Pre-condición:* Descripción de los objetos que van a ser tratados como INPUT.
- *Post-condición:* Que incluye la manera en que deseamos ver representados los OUPUTS de nuestro algoritmo.
- *Algoritmo:* La presentación habitual sería mediante un DISEÑO DESCENDENTE, empezando por lo general y estudiando, caso por caso, los subalgoritmos que componen el algoritmo.

Las páginas que siguen pretenden, en lo posible, seguir el esquema de responder a estas cuatro preguntas de manera lo menos alambicada posible. Las dificultades nacen de lo sofisticado de los objetos involucrados: variedades algebraicas. La segunda dificultad nace de lo sofisticado de las demostraciones de la correción de los algoritmos: se debe conocer un abundante material en Geometría Algebraica y Álgebra Conmutativa elementales.
Las motivaciones son varias. Resumiendo groseramente:

i) *Eliminación de Cuantificadores sobre Cuerpos Algebraicamente Cerrados:* Es un clásico asunto de los Fundamentos de la Matemática. Las Teorías de primer orden (cuantificadas) son indecidibles: no admiten algoritmo que verifique su verdad o falsedad, ni siquiera su demostrabilidad. Algunos casos particulares de Teorías de Primer Orden admiten discusiones particulares. Por ejemplo, la combinación de la obra de K. Gödel, con los trabajos de J. Robinson y la culminaciín de Y, Matjasievicz, responden negativamente al Problema X de Hilbert: La Teor'ıa de Primer Orden *Elementary Number Theory* es indecidible y es, incluso, indecidible si sólo admitimos cuantificadores eistenciales (un bloque de cuntificadores existenciales). En cambio, desde los trabajos de L. Kronecker, D. Hilbert o G. Hermann se conoce que la Teoría de Primer Orden sobre cuerpos algebraicamente cerrados ($\mathbb{C}$) admite eliminación de cuantificadores y es una teoría decidible. Desde la Obra de A. Tarski se sabe también que la Teoría de Primer Orden de Cuerpos Relmente Cerrados ($\mathbb{R}$) admite eliminación de cuantificadores y es decidible. Los temas de este curso afectan solamente al caso de cuerpos algebraicamente cerrados.

ii) *Complejidad Computacional:* Los algoritmos de eliminación de cuantificadores tienen una complejidad necesariamente doblemente exponencial ($2^{d^n}$) en el número de variables tanto en el caso algebraicamente cerrado como en el caso realmente cerrado. Ambos casos son conocidos. Por tanto, es necesario reflexionar dónde reside la dificultad del tratamiento de estos problemas. Por ello surge un subproblema más simple como objeto de estudio desde la perspectiva de la omplejidad computacional: *la decisión de fórmulas on un sólo bloque de cuantificadores existenciales.* Incluso, dentro de este modelo ya se

encuentran algunos de los problemas esenciales de la Matemática actual. Es una constatación evidente que se verifica la siguiente propiedad:
*Todo problema* **NP***-completo responde a una instancia particularmente simple del siguiente problema:*

PROBLEMA 1 (**Consistencia para una ecuación adicional**). *Sea $K$ un cuerpo primo ($K = \mathbb{F}_p \vee \mathbb{Q}$) y sean dados $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ una familia finita de polinomios con coeficientes en $K$. Sea $g \in K[X_1, \ldots, X_n]$ un polinomio adicional y supongamos que la variedad algebraica siguiente es no vacía:*

$$V(f_1, \ldots, f_s) := \{x \in \mathbb{K}^n \ : \ f_i(x) = 0,\ 1 \leq i \leq s\} \neq \emptyset,$$

*donde $\mathbb{K}$ es la clausura algebraica de $K$. Decidir si es o no cierta la afirmación siguiente:*

$$\exists x_1 \in \mathbb{K}, \ldots, \exists x_n \in \mathbb{K},\ f_i(x_1, \ldots, x_n) = 0,\ 1 \leq i \leq s,\ g(x_1, \ldots, x_n) = 0.$$

iii) *Aplicaciones en otros contextos:* Muchos problemas de otros contextos admiten una modelización mediante un conjunto finito de ecuaciones polinomiales. No es el objetivo del curso explorar esos contextos, pero se darán indicaciones de diversas lecturas en diversos ámbitos que van desde problemas de planificación de movimientos, a problemas de modelos de reacción en Química o problemas de Códigos, Criptología o Comunicaciones.

De lo dicho anteriormente se infiere que el objetivo del curso es tratar algoritmos que responden a preguntas como las propuestas y que nos concentramos en el caso de la eliminación de un bloque de cuantificadores existenciales como en el Problema 1. Analizando ese problema tenemos que descomponer los elementos definidos como Pre-condición y Post-condición:

i) *Pre-condición:* Los INPUTS son listas de polinomios multi-variados $f_1, \ldots, f_s, g$. Para representar los polinomios se pueden usar muy diversas formas de codificación. La más general es la codificación mediante *Esquemas de Evaluación* que podemos interpretar como "programas que evalúan esos polinomios". Por simplicidad podemos suponer que los inputs son una sub-clase de los polinomios de grado acotado por una cierta cantidad. Esta subclase se define mediante parametrizaciones de sus coeficientes. Incluso podemos ademitir que los polinomios son dados genéricamente: suponiendo que todos sus coeficientes son no nulos. Según el modelo de representación de los inputs que supongamos tendremos un comportamiento distinto de los algoritmos. Discutiremos diversas representaciones en su momento. Para el alumno iniciado en Álgebra Conmutativa se pude elegir la *codificación densa* que consiste en suponer que se representan todos los coeficientes para grado dado.

ii) *Post-condición:* En principio, parece que la respuesta a la pregunta del Problema 1 pertenece al conjunto $\{0, 1\}$ lo que no tiene muchas dificultades de ser expresado. Sin embargo, esta mera consideración no ayuda a comprender por qué estos problemas tienen alta complejidad. Por eso hay que "revisar" el modelo del problema. Dentro del problema de decisión se ocultan dos subproblemas que pueden ser tratados separadamente:

PROBLEMA 2 (**Problema de Resolución**). *Dada una lista de polinomios $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$, dar una descripción (una cantidad de información) explícita y re-usable del conjunto de soluciones no vacío $V(f_1, \ldots, f_s)$.*

PROBLEMA 3. **Problema de Eliminación***] Dada una lista de polinomios $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$, y dada una "resolución" del conjunto no vacío*

$$V(f_1,\ldots,f_s),\ \textit{decidir si un polinomio } g\in K[X_1,\ldots,X_n]\ \textit{adicional verifica:.}$$
$$\exists x_1\in\mathbb{K},\ldots,\exists x_n\in\mathbb{K},\ f_i(x_1,\ldots,x_n)=0,\ 1\leq i\leq s,\ g(x_1,\ldots,x_n)=0.$$

Nótese que los dos problemas últimos obligan a una fuerte interacción. Disponer de algoritmos que decidan para un $g$ adicional (Problema 3), obligan, de algún modo, a interpretar cómo se debe expresar la *"una descripción (una cantidad de información) explícita y re-usable del conjunto de soluciones"* (Problema 2) y, por tanto, condicionan la manera en que se describen las variedades algebraicas $V(f_1,\ldots,f_s)$. Aquí es necesaria una reflexión importante:
En los probelmas **NP**-completos, las soluciones $FV(f_1,\ldots,f_s)$ son, usualmente, fácilmente accesibles de modo individual, generando una ideología del tipo *"probar con cada uno de los posibles candidatos"*. La dificultad de la Conjetura de Cook se basa sustancialmente en discernir si ese proceso de "probar con cada uno de los posibles candidatos" es o no lo mejor que se puede hacer en términos de complejidad. Por tanto, desde la perspectiva de la mayoría de los problemas **NP**-completos el Problema 2 aparece oculto: no se necesita esta fase para probar con cada una de las soluciones, pero ¿sería posible buscar otra representación del conjunto de soluciones más eficiente que probar con cada objeto indepndientemente? y, lo que es más relevante, ¿En qué se diferencia el acceso fácil e inmediato a cada solución del caso de las ecuaciones polinomiales donde las soluciones vienen dadas "implícitamente"?. Del estudio del Problema 2 se obtendrá, con el tiempo, una mejor comprensión del fenómeno.
Por tanto, el problema subsiguientye consiste en determinar

PROBLEMA 4 (**Representación "explícita" de Variedades Algebraicas)**. *Definir un modelo de representación "explítica y re-usable" de las variedades algebraicas.*

Una buena parte del curso trata de este problema y usa y contiene lo poco (o mucho) que la Matemática ha desarrollado a lo largo de sus historia para definir el concepto. Trataremos los modelos siguientes:

i) *Representación Algebraica:* Con las ideas de Macaulay, Buchberger, Hironaka y las nociones de Bases de Gröbner, Se trata de representaciones basadas en BASES MONOMIALES que son especialmente significativas en el caso cero-dimensional. Al cabo de trata de representar la $K-$álgebra
$$K[X_1,\ldots,X_n]/\mathfrak{a},$$
donde $\mathfrak{a}$ es el ideal generado por los polinomios de la lista $(f_1,\ldots,f_s)$.
ii) *Representación Geométrica con bases monomiales:* De nuevo esencialmente " à la Macaulay", con bases monomiales pero para el anillo cociente:
$$K[X_1,\ldots,X_n]/\sqrt{\mathfrak{a}},$$
donde $\sqrt{\mathfrak{a}}$ es el radical del ideal. El sentido "geométrico" del radical se entiende, sobre todo, a partir del Nullstellensatz de Hilbert-Konecker. En realidad se suprimen multiplicidades y componentes inmersas que son uno de los grandes inconvenientes de la complejidad en el modelo anterior.
iii) *Representación Geométrica "à la Kronecker" en el caso cero-dimensional:* Se trata de definir un iromorfismo birregular (una aplicación biyectiva polinomial con inversa polinomial) de $V(f_1,\ldots,f_s)$ con un subjconjunto de $\mathbb{K}$. Todo el estudio se transforma en un estudio que transforma el trabajo con polinomios multivariados a un trabajo con polinomios univariados y todas las preguntas se simplifican.
iv) *Representación Geométrica mediante la forma de Cayley-Chow:* Se trata de representar la variedad $V(f_1,\ldots,f_s)$ mediante un polinomio multivariado único que contiene toda la inromación y del que se sabe que admiten representaciones cortas en relación con su grado (es fácil de evaluar).

v) *Representación Geométrica mediante ceros aproximados:* Sólo es aplicable en el caso $K = \mathbb{Q}$ y en el caso en que nuestros polinomios iniciales definan una variedad lisa cero-dimensional y su jacobiano no se anula en ninguno de sus ceros. Es decir, mismo número de ecuaciones que de variables, variedad no vacía y jacobiano de rango máximo en cada uno de sus ceros. En este caso, la variedad $V$ puede representarse mediante una variedad $W$ de cardinal posiblemente menor y un operador (típicamente el operador de Newton) $N_f$ de tal modo que para cada $\varepsilon > 0$, exuste $k$ tal que todos los puntos de la aplicación de $k$ iteraciones del operador sobre puntos de $W$ $N_f^k(W)$ están cerca de puntos de $V$. Si el cardinal de $W$ es estrictamente menor que el cardinal de $V$ es posible que hayamos perdido información sobre $V$ que sea, posiblemente, necesaria para decidir el Problema 3. Tomando $k := \log_2(\log_2(\varepsilon^{-1}))$ tenemos la *Teoría de los ceros aproximados de S. Smale y M. Shub.* Uno de los misterios más soprendentes de esta teoría es que con la sola presencia de uno de estos ceros aproximados en $\mathbb{Q}[i]^n$ suele ser suficiente para poder "reconstruir" toda la variedad.

vi) *Representación Geométrica "à la Kronecker" en el caso equi-dimensional:* Las variedades equi-dimensionales de dimensión positiva son birracionalmente equivalentes a hiper-superficies definidas por polinomios mónicos. Esta codificación pretende solamente representar ese isomorfismo birracional que se transmite de manera natural al álgebra $K[V]$ sólo en el caso de que $V$ sea una variedad intersección completa (i.e. dada por una secesión regular reducida).

vii) *Representación Geométrica mediante fibra de levantamiento en el caso intersección completa reducida:* En este caso, $\sqrt{\mathfrak{a}} = \mathfrak{a}$, el número de ecuaciones $s$ está liagado a la dimensión del conjunto de soluciones $\dim(V) = n - s$ y estamos en posición de Noether. Por ello, podemos representar $V$ mediante la fibra en un *punto no ramificado* y recuperar cualquier otra representación mediante el operador de Newton *No arquimediando* también entendido como *Teorema de la Función Implícita efectivo.*

viii) *Representación Geométrica mediante forma de Cayley-Chow en el caso equidimensional:* Es el clásico de la forma de Chow que involucra toda la información de una variedad en un sólo polinomio.

El objetio del curso trata de la interacción entre estas representaciones y cómo unos u otras permiten definir diversos tipos de algoritmos. Hay elementos más precisos en cada campo porque es necesarioa reflexionar detalles del tipo:

i) *¿Cómo se representan todos los polinomios que se han destacada en cada representación?.* Se ha comprobado que la forma más eficiente de representar los polinomios usados en las representaciones geométricas son los esquemas de evaluación.

ii) *¿Cómo se transfiere una información a la otra?* Se trata de discutir (y demostrar) que, por ejemplo, todas las presentaciones geométricas (diofánticas o polinomiales) son equivalentes entre sí: todas contienen la misma información sobre la variedad solución, aunque con distintas presentaciones.

iii) *¿Cómo se articulan estas representaciones para diseñar un algoritmo?* Se trata de definir un algoritmo incremental, que añade una ecuación a cada paso ("partido a partido") usando la transferencia entre representaciones y diversos algoritmos probabilistas de base. En esencia se incardinan las varias representaciones geométricas, incluyendo la elevación "sólo a una curva",

iv) *¿Cu'al es la complejidad de estos algoritmos?* La complejidad debe ser intrínseca, es decir, sólo depende de la Geometría de los objetos subyacentes calculados en cada una de las etapas. El algoritmo (o conjunto de algoritmos) que presentamos tiene la particularidad de que su complejidad es polinomial en la talla

del input, el número de variables y un parámetro intrínseco que se basa en el grado geométrico de los objetos involucrados.

Capítulo 2

# Una Prueba Elemental de Nullstellensatz de Hilbert

El objetivo de estas páginas es dar una demostración elemental del Nullstellensatz de Hilbert. Los contenidos de esta sección están inspirados en el trabajo de E. Arrondo [**Ar, 06**]. A partir de él, obtendremos un diccionario álgebra-geometría con el que podemos trabajar.

## 2.1. Una demostración elemental del Nullstellensatz de Hilbert: Parte I

**2.1.1. La Resultante y polinomios mónicos.** Comenzamos con la siguiente observación:

LEMA 2.1.1. *Sea $R$ un dominio de integridad y sea $g \in R[X]$ un polinomio mónico univariado en $R[X]$ (i.e. un polinomio cuyo coeficiente director es una unidad en el anillo $R$). Entonces, la $R-$álgebra cociente:*

$$A_g := R[X]/(g),$$

*es un $R-$módulo libre finitamente generado. Una base como $R-$módulo libre (la base monomial) viene dada por:*

$$\beta = \beta_g := \{\overline{1}, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1}\},$$

*donde $d := deg_X(g)$ es el grado de $g$ con respecto a la variable $X$ y $\overline{X}^k$ es la clase de restos $X^k + (g)$.*

DEMOSTRACIÓN. Es un sencillo ejercicio análogo al caso de polinomios. La única observación significativa es que al ser $g$ mónico tenemos garantizada la división euclídea por $g$. Es decir, para todo $f \in R[X]$ existen $q, r \in R[X]$ tales que:

- $f = qg + r$,
- $deg(r) \leq deg(g) - 1$.

Y, además, por ser $R$ dominio de integridad, el resto $r$ es único para cada $f$. Estas dos ideas bastan para concluir la afirmación. □

LEMA 2.1.2. *Sea $R$ un dominio de integridad, $g \in R[X]$ un polinomio mónico y sea $f \in R[X]$ un polinomio cualquiera. Consideremos la $R-$álgebra cociente $A_g$ del Lema anterior y el endomorfismo:*

$$\begin{array}{rccc} \eta_f : & A_g & \longrightarrow & A_g \\ & \overline{h} & \longmapsto & \overline{fh}, \end{array}$$

*donde $\overline{h}$ y $\overline{fh}$ son, respectivamente, las clases $h + (g)$ y $fh + (g)$. Entonces,*

i) *La matriz de $\eta_f$ en la base monomial $\beta$ descrita en el Lema anterior es $f(C(g))$, donde $C(g)$ es la matriz compañera de $g$, es decir,*

$$C(g) = \begin{pmatrix} 0 & 0 & 0 & \cdots & -u^{-1}a_0 \\ 1 & 0 & 0 & \cdots & -u^{-1}a_1 \\ 0 & 1 & 0 & \cdots & -u^{-1}a_2 \\ 0 & 0 & 1 & \cdots & -u^{-1}a_3 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -u^{-1}a_{d-1} \end{pmatrix} \in \mathcal{M}_d(R),$$

*donde* $g = uX^d + a_{n-1}X^{d-1} + \cdots + a_1X + a_0$, *siendo* $u \in R^*$ *unidad en* $R$.

ii) *El determinante* $Res_X(f,g) := det(f(C(g))) \in R$ *está en el ideal generado por* $(f,g)$ *en* $R[X]$ *(y se denomina la resultante de* $f$ *y* $g$ *con especto a la variable* $X$*). Es decir, existen* $a, b \in R[X]$ *tales que:*

$$Res_X(f,g) = af + bg \in R[X].$$

iii) *El endomorfismo* $\eta_f$ *es un isomorfismo de* $R-$*módulos libres si y solamente si* $Res_X(f,g) \in R^*$ *es una unidad de* $R$.

Demostración. ▪ Para la afirmación (2), utilizaremos el Teorema de Hamilton-Cayley para $R-$módulos libres finitamente generados. Denotemos mediante $\chi_f(T) \in R[T]$ el polinomio característico de $\eta_f$ con respecto a la base $\beta$. Por el Teorema de Hamilton-Cayley, el endomorfismo $\chi_f(\eta_f) = 0$ como endomorfismo de $A_g$. En particular, $\chi_f(\eta_f)(1) = 0 \in A_g$. Ahora, supongamos

$$\chi_g(T) := T^d + b_{d-1}T^{d-1} + \cdots + b_1T + b_0 \in R[T],$$

con $b_0 := \overline{\det(f(C(g)))} := \det(f(C(g))) + (g) \in R \subseteq A_g$ es la clase residual del elemento $\det(f(C(g)))$ módulo el ideal $(g)$ generado por $g$ en $R[X]$. Entonces, se tiene:

$$\chi_f(\eta_f)(1) = \eta_f^d(1) + b_{d-1}\eta_f^{d-1} + \cdots + b_1\eta_f(1) + b_0\overline{1} = 0,$$

o, lo que es lo mismo,

$$\chi_f(\eta_f)(1) = \overline{f}^d + b_{d-1}\overline{f}^{d-1} + \cdots + b_1\overline{f} + b_0\overline{1} = 0.$$

Dicho de otra manera, sea $h_i \in R[X]$ tal que $\overline{h_i} := h_i + (g) = b_i \in A_g$. Tenemos probado, sacando $\overline{f}$ factor común, que se verifica:

$$\overline{\det(f(C(g)))} + \overline{f}\left(\overline{f}^{d-1} + \sum_{i=1}^{d-1}\overline{h_i f}^{i-1}\right) = 0, \text{ en } A_g.$$

En otras palabras,

$$\overline{\det(f(C(g))) + f\left(f^{d-1} + \sum_{i=1}^{d-1} h_i f^{i-1}\right)} = 0, \text{ en } A_g.$$

Dicho de otra manera, definiendo $a := -\left(f^{d-1} + \sum_{i=1}^{d-1} h_i f^{i-1}\right) \in R[X]$, tenemos que

$$\det(f(C(g))) - af \in (g) \text{ en } R[X].$$

Luego existe $b \in R[X]$, tal que

$$\det(f(C(g))) = af + bg \in (f,g) \subseteq R[X].$$

□

Lema 2.1.3 (cf. [**Ar, 06**]). *Sea* $\mathfrak{a}$ *un ideal propio en* $K[X_1, \ldots, X_n]$, *donde* $K$ *es un cuerpo y sea* $\mathbb{K}$ *la clausura algebraica de* $K$. *Supongamos que* $n = 1$ *o* $n > 1$ *y se verifica:*

i) *Existe un polinomio* $g \in \mathfrak{a}$ *que es mónico con respecto a la variable* $X_n$,

ii) *El ideal contracción* $\mathfrak{b} := \mathfrak{a}^c = \mathfrak{a} \cap K[X_1, \ldots, X_{n-1}]$ *es propio y existe*

$$a := (a_1, \ldots, a_{n-1}) \in \mathbb{K}^{n-1},$$

*tal que* $h(a) = 0$ *para todo* $h \in \mathfrak{b}$.

*Entonces, existe* $a \in \mathbb{K}^n$ *tal que* $f(a) = 0$ *para todo* $f \in \mathfrak{a}$. *Es decir,* $V_{\mathbb{K}^n}(\mathfrak{a}) \neq \emptyset$.

DEMOSTRACIÓN. Para el caso $n = 1$, es obvio: Si $\mathfrak{a}$ es un ideal propio en $K[X]$, entonces es un ideal principal $\mathfrak{a} = (f)$ y $f$ no es cero ni unidad en $K[X_1]$. Por tanto, $f$ posee, al menos, una raíz $\alpha \in \mathbb{K}$ y, por tanto, $V_{\mathbb{K}}(\mathfrak{a}) \neq \emptyset$.
Para el caso $n = 2$, basta con observar que la propiedad ii) se verifica dado que $\mathfrak{b}$ es un ideal propio de $K[X_1]$ por ser $\mathfrak{a}$ propio. El resto del argumento es igual al caso general que sigue a continuación:
Para el caso $n > 1$, consideremos el ideal $\mathfrak{b} := \mathfrak{a}^c = \mathfrak{a} \cap K[X_1, \ldots, X_{n-1}]$. Como $\mathfrak{a}$ es un ideal propio en $K[X_1, \ldots, X_n]$, tenemos que $1 \notin \mathfrak{a}$, por tanto $1 \notin \mathfrak{b}$ y $\mathfrak{b}$ es un ideal propio de $K[X_1, \ldots, X_{n-1}]$ o $\mathfrak{b} = (0)$. En ambos casos, y asumiendo la hipótesis ii), existe

$$a := (a_1, \ldots, a_{n-1}) \in \mathbb{K}^{n-1},$$

tal que $h(a) = 0$ para todo $h \in \mathfrak{b}$. Consideremos ahora el siguiente conjunto:

$$\mathfrak{c} := \{f(a_1, \ldots, a_{n-1}, X_n) \in K[X] \ : \ f \in \mathfrak{a}\}.$$

Se trata, claramente, de un ideal en el anillo de polinomios univariados $K[X_n]$. Veamos que $\mathfrak{c} \subsetneq K[X_n]$, es decir, está estrictamente contenido en $K[X_n]$. Razonemos por reducción al absurdo y supongamos que $1 \in \mathfrak{c}$. Entonces, existe $f \in \mathfrak{a}$ tal que:

$$1 := f(a_1, \ldots, a_{n-1}, X_n).$$

De otro lado, sea $g \in \mathfrak{a}$ el polinomio mónico que existe en $\mathfrak{a}$ y que, por ser $\mathfrak{a}$ propio, es no unidad. Consideremos ahora el polinomio $h := Res_{X_n}(f, g) := \det(f(C(g))) \in K[X_1, \ldots, X_{n-1}]$. Consideremos el anillo $R := K[X_1, \ldots, X_{n-1}]$ y, por el Lema precedente, tenemos que $h$ está en el ideal generado por $f$ y $g$ en $R[X_n] = K[X_1, \ldots, X_n]$. Es decir,

$$h := Res_{X_n}(f, g) \in (f, g) \subseteq \mathfrak{a}.$$

Como $h \in K[X_1, \ldots, X_{n-1}]$, concluiremos que $h \in \mathfrak{b} = \mathfrak{a}^c$. De otro lado, obsérvese que $h$ es el determinante de la matriz obtenida reemplazando $X_n$ en $f$ por $C(g)$. Es decir, es el determinante de la matriz dada mediante

$$f(X_1, \ldots, X_{n-1}, C(g)(X_1, \ldots, X_{n-1})).$$

Más específicamente, tenemos

$$C(g)(X_1, \ldots, X_{n-1}) = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0(X_1, \ldots, X_{n-1}) \\ 1 & 0 & 0 & \cdots & -a_1(X_1, \ldots, X_{n-1}) \\ 0 & 1 & 0 & \cdots & -a_2(X_1, \ldots, X_{n-1}) \\ 0 & 0 & 1 & \cdots & -a_3(X_1, \ldots, X_{n-1}) \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{d-1}(X_1, \ldots, X_{n-1}) \end{pmatrix} \in \mathcal{M}_d(R),$$

donde

$$g = X_n^d + a_{n-1}(X_1, \ldots, X_{n-1})X_n^{d-1} + \cdots + a_1(X_1, \ldots, X_{n-1})X_n + a_0(X_1, \ldots, X_{n-1}).$$

Y si

$$f := b_t(X_1, \ldots, X_{n-1})X_n^t + \cdots + b_0(X_1, \ldots, X_{n-1}),$$

entonces

$$f(X_1, \ldots, X_{n-1}, C(g)(X_1, \ldots, X_{n-1})) := \sum_{i=0}^{t} b_i(X_1, \ldots, X_{n-1})C(g)(X_1, \ldots, X_{n-1})^i \in \mathcal{M}_d(K[X_1, \ldots, X_{n-1}]).$$

En particular, observemos que la matriz

$$f(a_1, \ldots, a_{n-1}, C(g)(a_1, \ldots, a_{n-1})) := \sum_{i=0}^{t} b_i(a_1, \ldots, a_{n-1})C(g)(a_1, \ldots, a_{n-1})^i \in \mathcal{M}_d(K),$$

es la matriz obtenida especializando las variables de $f(X_1,\ldots,X_{n-1},C(g)(X_1,\ldots,X_{n-1}))$ en las coordenadas de $a$. Tomando determinantes, tendremos que

$$Res_{X_n}(f,g)(a_1,\ldots,a_{n-1}) := \det(f(a_1,\ldots,a_{n-1},C(g)(a_1,\ldots,a_{n-1}))).$$

Ahora bien $f(a_1,\ldots,a_{n-1},X_n)=1$, con lo que

$$b_i(a_1,\ldots,a_{n-1})=0,\ \ 1\leq i\leq t,$$

y

$$b_0(a_1,\ldots,a_{n-1})=1.$$

Por tanto,

$$Res_{X_n}(f,g)(a_1,\ldots,a_{n-1})=\det(\sum_{i=0}^{t} b_i(a_1,\ldots,a_{n-1})C(g)(a_1,\ldots,a_{n-1})^i)=det(Id_d)=1.$$

Pero como $Res_{X_n}(f,g)\in\mathfrak{b}$, tendremos que $Res_{X_n}(f,g)(a_1,\ldots,a_{n-1})=0$ con lo que habremos llegado a contradicción.
En particular, tendremos que $\mathfrak{c}\subsetneq K[X_n]$ y existirá $z\in\mathbb{K}$ tal que $h(z)=0$ para todo $h\in\mathfrak{c}$. Pero, recordando la definición de $\mathfrak{c}$, tendremos que

$$f(a_1,\ldots,a_{n-1},z)=0,\ \ \forall f\in\mathfrak{a}.$$

Por tanto, $V_{\mathbb{K}^n}(\mathfrak{a})\neq\emptyset$ y haremos concluido la prueba del Lema. □

**2.1.2. El cálculo del Máximo común divisor: Nullstellensatz univariado.** Retomamos las notaciones de la Subsección 2.1.1 y de los Lemas 2.1.1 y 2.1.2 anteriores. Supongamos $K=R$ es un cuerpo, $g\in K[X]$ un polinomio univariado, consideremos el anillo cociente $A_g := K[X]/(g)$ y la base monomial

$$\beta_g := \{\overline{1},\overline{X},\overline{X}^2,\ldots,\overline{X}^{d-1}\},$$

donde $d := deg_X(g)$ es el grado de $g$ con respecto a la variable $X$ y $\overline{X}^k$ es la clase de restos $X^k+(g)$. Denotamos por $C(g)$ la matriz compañera de $g$. Para cada polinomio $f\in K[X]$, consideremos la homotecia:

$$\begin{array}{rccc}\eta_f: & A_g & \longrightarrow & A_g\\ & \overline{h} & \longmapsto & \overline{fh},\end{array}$$

donde $\overline{h}$ y $\overline{fh}$ son, respectivamente, las clases $h+(g)$ y $fh+(g)$. Como en la citada Subsección, la matriz de $\eta_f$ en la base $\beta_g$ es la matriz dada por la evaluación de $f$ en la matriz $g$. Denotaremos por $\mathbb{K}$ la clausura algebraica de $K$.

*2.1.2.1. Serie de Taylor.* Supongamos que un polinomio $h\in K[X]$ es dado y que $\zeta\in\mathbb{K}$ es un elemento de la clausura algebraica. Obviamente, la siguiente familia es una base de $\mathbb{K}[X]$ como espacio vectorial sobre $\mathbb{K}$:

$$\beta_\zeta := \{(X-\zeta)^k\ :\ k\in\mathbb{N}\}.$$

El polinomio $h$ de grado $m$ tiene una expasión finita en esa base $\beta_\zeta$, con lo que podemos suponer que se escribe:

$$h := \sum_{k=0}^{m} a_k(X-\zeta)^k.$$

Escribiremos $d^i_\zeta h := a_i\in\mathbb{K}$ y, en el caso de característica 0 se corresponde con la usual definición de derivada formal, i.e. si $caract(K)=0$,

$$d^i_\zeta h := \frac{1}{i!}h^{(i)}(\zeta).$$

Obviamente, independientemente de la característica, $d^0_\zeta h = h(\zeta)$. La expansión anterior de cada polinomio $h$ puede interpretarse en el anillo topológico $\mathbb{K}[[X-\zeta]]$, con la

métrica $(X-\zeta)-$ádica, aunque este asunto lo pospondremos hasta un capítulo posterior. por ahora nos vamos a conformar con introducir la noción de orden al nivel de $\mathbb{K}[X]$ del modo siguiente:

$$\begin{array}{rccl} ord_\zeta: & \mathbb{K}[X] & \longrightarrow & \mathbb{N} \\ & h & \longmapsto & ord_\zeta(h) := \min\{k \in \mathbb{N} \ : \ h \in \left((X-\zeta)^k\right)\}. \end{array}$$

Nótese que la función de orden en $\zeta$ se pude también caracterizar mediante el comportamiento de la expansión de Taylor de $h$:

$$ord_\zeta(h) := \min\{k \in \mathbb{N} \ : \ d_\zeta^k h \neq 0\}.$$

*2.1.2.2. Forma Canónica de Jordan.*

Proposición 2.1.4. *Sea $\zeta \in \mathbb{K}$ un elemento y consideremos el polinomio mónico $g = (X-\zeta)^n$. Consideremos el anillo cociente obtenido por extensión de escalares $\mathbb{K} \otimes_K A_g = \mathbb{K}[X]/(g)$. Se tiene:*

i) *La siguiente colección es una base de $\mathbb{K}[X]/(g)$ como $K-$espacio vectorial, a la que llamaremos base monomial en $\zeta$ de $\mathbb{K} \otimes_K A_g$:*

$$\mathbb{K} \otimes_K \beta_\zeta := \{1+(g), (X-\zeta)+(g), \ldots, (X-\zeta)^{d-1}+(g)\},$$

*donde $d = deg(g)$.*

ii) *La matriz en la base $\mathbb{K} \otimes_K \beta_\zeta$ de la homotecia $\eta_X$ es, justamente, la caja de Jordan de orden $d$ y valor "propio" $\zeta$. Es decir, la matriz $J(\zeta, d) \in \mathcal{M}_d(\mathbb{K})$ dada mediante:*

$$J(\zeta, n) := \begin{pmatrix} \zeta & 0 & 0 & \cdots & 0 & 0 \\ 1 & \zeta & 0 & \cdots & 0 & 0 \\ 0 & 1 & \zeta & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 & \zeta \end{pmatrix}.$$

*A la matriz $J(\zeta, d)$ se la denomina caja de Jordan de orden $d$ en honor del matemático C. Jordan* [1] .

iii) *Para cada $f \in K[X]$ la matriz de $\eta_f$ como endomorfismo de $\mathbb{K} \otimes_K A_g$ en la base $\mathbb{K} \otimes_K \beta_\zeta$ es $f(J(\zeta, d))$, que viene dada mediante:*

$$f(J(\zeta, d)) := \begin{pmatrix} d_\zeta^0 f & 0 & 0 & \cdots & 0 \\ d_\zeta^1 f & d_\zeta^0 f & 0 & \cdots & 0 \\ d_\zeta^2 f & d_\zeta^0 f & d_\zeta^0 f & \cdots & 0 \\ & \vdots & & \ddots & 0 \\ d_\zeta^{d-1} f & d_\zeta^{d-2} f & d_\zeta^{d-3} f & \cdots & d_\zeta^0 f \end{pmatrix}.$$

*En particular, observamos que*

$$\det\left(f(J(\zeta, d)\right) = f(\zeta)^d,$$

*y que*

$$rank\left(f(J(\zeta, d)\right) = d - \min\{d, ord_\zeta(f)\}.$$

Demostración. Basta con verificar el detalle de los enunciados que son bastante explícitos. □

[1] Camille Jordan introduce su forma canónica en su texto de 667 páginas *"Traité des substitutions et des équations algébriques"*. Gauthier-Villars, Paris, 1870. Este tratado es un estudio completo de la teoría de E. Galois, resolución de ecuaciones polinomiales univariadas, teoría de grupos y, en particular, contiene la forma canónica de Jordan (que lo hizo sólo para un cuerpo finito, llamados "cuerpos de Galois"). El texto, usado en la École Polytechnique, recibió en Premio Poncelet de la Academia de Ciencias de París.

La forma canónica de Jordan es una simple reescritura del Teorema Chino de los Restos, aplicado a la forma de Frobenius de un endomorfismo. Aquí lo onterpretaremos del modo siguiente.

PROPOSICIÓN 2.1.5 (**Forma de Jordan**). *Sea $g \in K[X]$ un polinomio mónico de grado $d$ y supongamos que existen $\zeta_1, \ldots, \zeta_r \in \mathbb{K}$, con $\zeta_i \neq \zeta_j$, y exponentes $m_i \in \mathbb{N}$, con $m_i \geq 1$, $1 \leq i \leq r$, tales que en $\mathbb{K}[X]$ se tiene:*

$$g(X) := \prod_{i=1}^{r} (X - \zeta_i)^{m_i}.$$

*Consideremos:*

- *Sea $\widetilde{\Phi} : \mathbb{K}[X]/(g) \longrightarrow \prod_{i=1}^{r} (\mathbb{K}[X]/(X-\zeta_i)^{m_i})$ el isomorfismo de anillos del Teorema Chino de los Restos. Entonces, $\widetilde{\Phi}$ es también un isomorfismo de $\mathbb{K}-$espacios vectoriales.*
- *En $\mathbb{K}[X]/(g)$ la base monomial $\beta := \{1+(g), X+(f), X^2+(f), \ldots, X^{d-1}+(g)\}$.*
- *En el espacio vectorial producto $\prod_{i=1}^{r} (\mathbb{K}[X]/(X-\zeta_i)^{m_i})$, la base $\Gamma$ inducida por las bases $\mathbb{K} \otimes_K \beta_{\zeta_i}$ en cada uno de los espacios vectoriales $\mathbb{K}[X]/(X-\zeta_i)^{m_i}$.*
- *Y sea $M_\Phi$ la matriz del isomorfismo $\widetilde{\Phi}$ en las bases $\beta$ y $\Gamma$.*

*Entonces, se tiene:*

$$C(g) := M_\Phi^{-1} \begin{pmatrix} J(\zeta_1, m_1) & 0 & \cdots & 0 \\ 0 & J(\zeta_2, m_2) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & J(\zeta_r, m_r) \end{pmatrix} M_\Phi.$$

*En paricular, $C(g)$ posee forma canónica de Jordan, ésta es única (salvo permutación de los bloques) y la matriz de cambio de base es la matriz del Teorema Chino de los Restos.*

DEMOSTRACIÓN. Es una simple verificación recordando el Teorema Chino de los Restos. Obsérvese que si $\zeta_i \neq \zeta_j$, entonces, $(X-\zeta_i)^k$ y $(X-\zeta_j)^s$ son co–maximales para $k, s \geq 1$. Por tanto, el hecho de ser $\widetilde{\Phi}$ un isomorfismo se sigue del Teorema Chino de los Restos. De otro lado, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} & \overset{\widetilde{\Phi}}{} & \\ \mathbb{K}[X]/(g) & \longrightarrow & \prod_{i=1}^{r} (\mathbb{K}[X]/(X-\zeta_i)^{m_i}) \\ \eta_X \quad \downarrow & & \downarrow \quad \prod_{i=1}^{r} \eta_X^{(i)} \\ \mathbb{K}[X]/(g) & \underset{\widetilde{\Phi}}{\longrightarrow} & \prod_{i=1}^{r} (\mathbb{K}[X]/(X-\zeta_i)^{m_i}) \end{array}$$

Este diagrama es conmutativo, donde $\prod_{i=1}^{r} \eta_X^{(i)}$ es el endomorfismo dado mediante el producto de los endomorfimos

$$\eta_X^{(i)} : \mathbb{K}[X]/(X-\zeta_i)^{m_i} \longrightarrow \mathbb{K}[X]/(X-\zeta_i)^{m_i}.$$

La conmutatividad del diagrama nos dice que

$$\eta_X = \widetilde{\Phi}^{-1} \circ \left( \prod_{i=1}^{r} \eta_X^{(i)} \right) \circ \widetilde{\Phi}.$$

□

COROLLARIO 2.1.6. *Sea $K$ un cuerpo y sean $f, g \in K[X]$ dos polinomios. Supongamos que $g$ es univariado y que admite una factorización en $\mathbb{K}[X]$ dada mediante:*

$$g := \prod_{i=1}^{r} (X - \zeta_i)^{m_i}.$$

*Entonces,*

i) *La resultante de $f$ y $g$ satisface:*

$$Res(f, g) := \det(f(C(g)) = \prod_{i=1}^{r} f(\zeta_i)^{m_i}.$$

*En particular, $f$ y $g$ poseen un cero común en $\mathbb{K}$ si y solamente si $Res(f, g) = 0$.*

ii) **Método de Barnett** *El grado del máximo común divisor de $f$ y $g$ es igual a la dimensión del núcleo de $\eta_f$, es decir,*

$$\deg(gcd(f, g)) = \dim_K \ker(\eta_f) = \dim_K \ker(f(C(g)) = deg(g) - rank(f(C(g)).$$

DEMOSTRACIÓN. Se trata solamente de seguir la Proposición precedente, usando el Teorema Chino de los restos. Para la afirmación i) basta eon observar que el determinante es un invariante por la raleación de semejanza. Luego

$$\det((f(C(g))) := \det\left( f\left( M_\Phi^{-1} \begin{pmatrix} J(\zeta_1, m_1) & 0 & \cdots & 0 \\ 0 & J(\zeta_2, m_2) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & J(\zeta_r, m_r) \end{pmatrix} M_\Phi \right) \right).$$

Es decir,

$$\det((f(C(g))) := \det \begin{pmatrix} f\left(J(\zeta_1, m_1)\right) & 0 & \cdots & 0 \\ 0 & f\left(J(\zeta_2, m_2)\right) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & (J(\zeta_r, m_r)) \end{pmatrix} = \prod_{i=1}^{r} \det\left(f\left(J(\zeta_i, m_i)\right)\right).$$

Y la afirmación se sigue por la forma de $f(J(\zeta_i, m_i))$ descrita anteriormente. De otro lado, tenemos el diagrama conmutativo siguiente, dado por el Teorema Chino de los Restos:

$$\begin{array}{ccc} & \widetilde{\Phi} & \\ \mathbb{K}[X]/(g) & \longrightarrow & \prod_{i=1}^{r} \left(\mathbb{K}[X]/(X - \zeta_i)^{m_i}\right) \\ \eta_f \quad \downarrow & & \downarrow \quad \prod_{i=1}^{r} \eta_f^{(i)} \\ \mathbb{K}[X]/(g) & \underset{\widetilde{\Phi}}{\longrightarrow} & \prod_{i=1}^{r} \left(\mathbb{K}[X]/(X - \zeta_i)^{m_i}\right) \end{array}$$

y la semejanza entre las matrices:

$$f(C(g)) := M_\Phi^{-1} \begin{pmatrix} f\left(J(\zeta_1, m_1)\right) & 0 & \cdots & 0 \\ 0 & f\left(J(\zeta_2, m_2)\right) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & f\left(J(\zeta_r, m_r)\right) \end{pmatrix} M_\Phi.$$

Por tanto, el núcleo de $\eta_f$ se descompone como la suma directa de los núcleos de las matrices en la suma diagonal anterior (dado que $M_\Phi$ es isomorfismo):

$$\ker(f(C(g)) = \bigoplus_{i=1}^{r} \ker\left(f\left(J(\zeta_i, m_i)\right)\right).$$

Luego,

$$\dim\left(\ker(f(C(g))\right) = \sum_{i=1}^{r} \dim\left(\ker\left(f\left(J(\zeta_i, m_i)\right)\right)\right) = \sum_{i=1}^{r} \text{mín}\{d, ord_{\zeta_i}(f)\}.$$

De otro lado, es obvio que si $h = gdc(f, g)$, entonces

$$h := \prod_{i=1}^{r} (X - \zeta_i)^{\text{mín}\{d, ord_{\zeta_i}(f)\}},$$

y la afirmación de Barnett se sigue de modo obvio. □

---

ALGORITMO 2.1.7 (**Cálculo del gcd en dimensión intrínseca**).
INPUT: *Dos polinomios $f, g \in K[X]$, siendo $g$ mónico.*
OUTPUT: *El polinomio $h = gcd(f, g) \in K[X]$.*

---

**initialize:** $M := C(g)$ *% la matriz compañera de $g$.*

**eval:** $N := f(M)$ *% la matriz de $\eta_f$ sobre $A_g$.*

**compute:** $\beta$ una base de $K_N := \ker(N)$

**compute:** la matriz $B$ de $\eta_X\ |_{K_N}$: $K_N \longrightarrow K_N$ en la base $\beta$. *% posible por ser $\eta_X-$invariante.*

**output:** $h(X) := \chi_B(X) := \det(XId - B)$ *% el polinomio característico de $B$.*

**end**

---

COROLLARIO 2.1.8. *El anterior algoritmo calcula el máximo común divisor de $f$ y $g$ y del número de operaciones aritméticas a realizar es del orden $O\left(\deg(f)\left(\deg(g)\right)^{\omega}\right)$, donde $\omega$ es el exponente del álgebra lineal. Nótese que el álgebra lineal implicada es del orden de* $\deg(g)$ *para operaciones Gaussianas y* $\deg(gcd(f, g))$ *para el cálculo de un polinomio característico.*

DEMOSTRACIÓN. Basta con seguir la descomposición del núcelo y probar la invarianza. ******* □

## 2.2. Un cambio de coordenadas útil

Usaremos la idea de Noether para poner nuestras variables en condición de extensión entera de anillos. Como antes, sea $K$ un cuerpo y sea $\mathbb{K}$ la clausura algebraica de $K$. Consideremos $(t_1, \ldots, t_{n-1}, 1) \in K^n$. Consideremos el siguiente cambio de variables:

$$\text{(2.2.1)}\qquad \begin{cases} Y_1 &= X_1 - t_1X_n, \\ Y_2 &= X_2 - t_2X_n, \\ &\vdots \\ Y_{n-1} &= X_{n-1} - t_{n-1}X_n, \\ Y_n &= X_n. \end{cases}$$

Consideremos el isomorfismo de $R-$álgebras dado por este cambio de coordenadas:

$$\text{(2.2.2)}\qquad \begin{array}{rccc} \varphi: & K[X_1,\ldots,X_n] & \longrightarrow & K[Y_1,\ldots,Y_n] \\ & f & \longmapsto & f(Y_1+t_1Y_n,\ldots,Y_{n-1}+t_{n-1}Y_n,Y_n). \end{array}$$

Lema 2.2.1. *Se verifican las siguientes propiedades:*

i) *Si $\mathfrak{a}\subseteq K[X_1,\ldots,X_n]$ es un ideal propio, entonces $\varphi(\mathfrak{a})$ es un ideal propio. Y recíprocamente.*

ii) *Consideremos la matriz triangular $P\in\mathcal{M}_n(K)$ dada mediante:*

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = P \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

*es decir, la matriz*

$$P := \begin{pmatrix} 1 & 0 & \cdots & 0 & -t_1 \\ 0 & 1 & \cdots & 0 & -t_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -t_{n-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

*La matriz inversa de la matriz $P$ es dada mediante:*

$$P^{-1} := \begin{pmatrix} 1 & 0 & \cdots & 0 & t_1 \\ 0 & 1 & \cdots & 0 & t_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & t_{n-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

iii) *Consideramos el isomorfismo de espacio vectoriales dado por $P$:*

$$\begin{array}{rccc} P: & \mathbb{K}^n & \longrightarrow & K^n \\ & \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto & \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \end{array}$$

*Entonces, para cada polinomio $f\in K[X_1,\ldots,X_n]$, $\varphi(f) := f\circ P^{-1}(Y_1,\ldots,Y_n)$. En particular, para cada ideal $\mathfrak{a}$ de $K[X_1,\ldots,X_n]$,*

$$V((\varphi(\mathfrak{a})) = P(V(\mathfrak{a})).$$

*En particular, $V(\mathfrak{a})\neq\emptyset$ si y solamente si $V(\varphi(\mathfrak{a}))\neq 0$.*

Demostración. Son todos ejercicios elementales.

□

Observación 2.2.2 (**Construcción a partir de las componentes homogéneas**). Consideremos el anillo $K[X_1,\ldots,X_n]$ y consideremos un polinomio cualquiera $f\in K[X_1,\ldots,X_n]$. Podemos descomponer $f$ es sus componentes homogéas de grado dado. Es decir, podemos escribir:

$$f := f_d(X_1,\ldots,X_n)+\cdots+f_0(X_1,\ldots,X_n),$$

donde $f_i \in K[X_1, \ldots, X_n]$ es un polinomio homogéneo de grado $d$, es decir,

$$f_i(X_1, \ldots, X_n) := \sum_{|\underline{\mu}|=d} a_{\underline{\mu}}^{(i)} X_1^{\mu_1} \cdots X_n^{\mu_n},$$

donde $\underline{\mu} = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$, $|\underline{\mu}| = \mu_1 + \cdots + \mu_n \in \mathbb{N}$, $a_{\underline{\mu}}^{(i)} \in K$. Además, esa descomposición es única. Supondremos que $f_d$ es un polinomio homogéneo.

Sea $\varphi : K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_n]$ el isomorfismo de $K-$álgebras descrito en la Sección precedente. Entonces, $\varphi$ respeta las componente homogéneas de los polinomios y tendremos que si $g = \varphi(f)$ admite una descomposición en componentes homogéneas del tipo:

$$g := g_d(X_1, \ldots, X_n) + \cdots + g_0(X_1, \ldots, X_n),$$

donde $g_i = \varphi(f_i)$. En particular, tendremos la siguiente igualdad:

$$g_i(Y_1, \ldots, Y_n) := \sum_{|\underline{\mu}|=d} a_{\underline{\mu}}^{(i)} (Y_1 + t_1 Y_n)^{\mu_1} \cdots (Y_{n-1} + t_{n-1} Y_n)^{\mu_{n-1}} Y_n^{\mu_n}.$$

LEMA 2.2.3. *Sean $f$ y $g$ como en la Observación precedente, entonces, existe un polinomio $h \in K[Y_1, \ldots, Y_n]$ tal que*

$$g = f_d(t_1, \ldots, t_{n-1}, 1) Y_n^d + h,$$

*y el grado de $h$ con respecto a la variable $Y_n$ es menor estricto que $d$.*

DEMOSTRACIÓN. Obvio por mera reescrittura. □

## 2.3. Tests de Nulidad para Polinomios.

Si bien antes hemos dicho que los esquemas de evaluación son una estructura de datos muy adecuada para tratar y manipular polinomios multivariados, hay una dificultad esencial para que sea tan precisa como la codificación densa o rala de polinomios. No es fácil decidir si dos códigos de dos esquemas de evaluación evalúan el mismo polinomio. Para resolverlo, tenemos dos opciones básicas :

i) INTERPOLAR OBTENIENDO TODOS LOS COEFICIENTES Y COMPARANDO A POSTERIORI. Esta no es una excelente idea, Por ejemplo, dadas dos formas de Cayley–Chow de dos variedades cero–dimensionales, interpolar para decidir si definen la misma variedad supone un esfuerzo considerablemente caro que nos lleva, usualmente, a una complejidad del orden $d^{n^2}$.

ii) DESARROLLAR TESTS DE NULIDAD PARA ESQUEMAS DE EVALUACIÓN. Se trata de algoritmos que evalúan los códigos dados en un número finito (y "pequeño") de puntos. Con los valores de esas "pocas" evaluaciones, tratamos de decidir si ambos esquemas de evaluación evalúan la misma función.

En esta Sección nos ocuparemos de estos Tests de Nulidad que pertenecen a tres tipos fundamentalmente :

i) *Los Tests de Zippel–Schwartz.* Se trata de seleccionar un conjunto fijo y, para cada polinomio, hay muchos puntos en los que no se anula. Se trata de un Test Probabilista que depende del polinomio y el esquema particular que tratamos. Fueron introducidos en los trabajos de J.T. Schwartz[2] y R. Zippel[3].

[2]J.T. Schwartz, *Fast Probabilistic Algorithms for Verification of Polynomial Identities.* J. of the ACM **27** (1980), 701–717.

[3]R. Zippel, *Interpolating Polynomials from their Values.* J. Symbol. Comput. **9** (1990), 375–403.

ii) *Los Cuestores o Correct Test Sequences.* Es un método alternativo al método de Zippel–Schwarzt. En ocasiones genera gran confusión entre los especialistas que no entienden la diferencia. El método de los cuestores es un método que no depende del polinomio particular que se discute sino de una clase de polinomios (y para ser más precisos de una familia uniracional). Por ejemplo, depende la clase de complejidad y es válido para toda ella. Fue introducido en el trabajo de J. Heintz y C.P. Schnorr [4] y refinado en el trabajo [**KrPa, 96**]. La versión que aquí se incluye es la versión refinada de [**KrPa, 96**].

iii) *Witness Theorem.* La existencia de un sólo punto donde un polinomio no se anula aparece ya en el trabajo de L. Kronecker y se conoce como "Esquema de Kronecker". En el caso de polinomios con coeficientes en $\mathbb{Z}$ el resultado aparece recogido, y atribuido a Kronecker, en el trabajo de J. Heintz y C.P. Schnorr de 1982, citado al pie. Posteriormente, S. Smale[5] redescubre el esquema de Kronecker para polinomios con coeficientes en un cuerpo de números y lo denomina "Witness Theorem" (véase también [**BCSS, 98**]. Sin embargo, las estimaciones de Smale y sus colaboradores eran muy groseras. Las estimaciones se mejoran en el trabajo [**CHMP, 01**].

Haremos la demostración del Test de Schwartz-Zippel y dejaremos los otros resultados para cuando tengamos una mejor fundamentación matemática.

**2.3.1. El Test de Schwartz–Zippel.** La clave del Test de Schwartz–Zippel es el siguiente enunciado :

LEMA 2.3.1. *Sea $f \in K[X_1, \ldots, X_n]$ un polinomio no nulo. Definamos recursivamente los siguientes polinomios :*

$$Q_1 := f \in k[X_1, \ldots, X_n],\ d_1 := deg_{X_1}(Q_1)$$

*Sea $Q_2 \in K[X_2, \ldots, X_n]$ el coeficiente de $X_1^{d_1}$ en $Q_1$. Para $i \leq 2$ definamos recursivamente :*

$$d_i := deg_{X_i} Q_i, Q_{i+1} \in K[X_{i+1}, \ldots, X_n]$$

*el coeficiente de $X_i^{d_i}$ in $Q_i$. Para $1 \leq i \leq n$ sea $I_i$ un subconjunto finito de $K$. Entonces, el número de ceros de $F$ in $I_1 \times \cdots \times I_n$ es a lo sumo*

$$\sharp(I_1 \times \cdots \times I_n)\left(\frac{d_1}{\sharp(I_1)} + \cdots + \frac{d_n}{\sharp(I_n)}\right)$$

DEMOSTRACIÓN. La prueba se sigue por inducción en $n$. En el caso $n = 1$ es obvio que un polinomio univariado de grado $d_1$ con coeficientes en un cuerpo no posee más de $d_1$ ceros en el cuerpo. La razón última es que $K[X]$ es un dominio de factorización única.
Consideremos ahora el caso $n > 1$. Consideremos el polinomio $Q_2 \in K[X_2, \ldots, X_n]$ que es el coeficiente director de $f$ con respecto a la variable $X_1$. Por construcción, la secuencia de polinomios $Q_2, \ldots, Q_n$ y de grados $d_2, \ldots, d_n$ es la misma comenzando por $Q_2$ o comenzando por $f$. Por tanto, podemos aplicar la hipótesis inductiva a $Q_2$ y tenemos que el número de elementos de $x = (x_2, \ldots, x_n) \in \prod_{i=2}^n I_i$ en los que $Q_2$ no se

[4] J. Heintz, C.P. Schnorr, *Testing Polynomials wich are easy to compute.* In Logic and Algorithmic (an International Symposium in honour of Ernst Specker), Monographie n. **30** de l'Enseignement Mathématique (1982), 237–254.

[5] L. Blum, F. Cucker, M. Shub, S. Smale, *Algebraic settings for the problem* **P**≠**NP***?*. In The mathematics of numerical analysis (Park City, UT, 1995), Amer. Math. Soc., Providence, 1996, 125–144.

anula es de cardinal mayor que:

$$\prod_{i=2}^{n} \sharp(I_i) - \prod_{i=2}^{n} \sharp(I_i) \left( \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right) = \prod_{i=2}^{n} \sharp(I_i) \left( 1 - \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right).$$

Para cada uno de los $x = (x_2, \ldots, x_n) \in \prod_{i=2}^{n} I_i$ en los que $Q_2(x) \neq 0$, el polinomio $f$ toma la forma:

$$f(X_1, x_2, \ldots, x_n) = Q_2(x) Y_1^{d_1} + h(X_1),$$

donde $h$ es un polinomio de grado a lo sumo $d_1 - 1$. En consecuencia, este polinomio univariado no se puede anular en, al menos, $\sharp(I_1) - d_1$ elementos de $I_1$. Y esto para cada $x$ con esas condiciones. Por tanto, $f$ no se anula en, al menos, el siguiente número de elementos de $\prod_{i=1}^{n} I_i$:

$$P := (\sharp(I_1) - d_1) \prod_{i=2}^{n} \sharp(I_i) \left( 1 - \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right).$$

Desarrollando este producto obtenemos

$$P := \sharp(I_1) \prod_{i=2}^{n} \sharp(I_i) \left( 1 - \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right) - d_1 \prod_{i=2}^{n} \sharp(I_i) \left( 1 - \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right).$$

Luego

$$P := \prod_{i=1}^{n} \sharp(I_i) - \prod_{i=1}^{n} \sharp(I_i) \left( \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right) - \frac{d_1}{\sharp(I_1)} \prod_{i=1}^{n} \sharp(I_i) + \frac{d_1}{\sharp(I_1)} \prod_{i=1}^{n} \sharp(I_i) \left( \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right).$$

Por tanto,

$$P \geq \prod_{i=1}^{n} \sharp(I_i) \left( 1 - \sum_{i=2}^{n} \frac{d_i}{\sharp(I_i)} \right) - \frac{d_1}{\sharp(I_1)} \prod_{i=1}^{n} \sharp(I_i) = \prod_{i=1}^{n} \sharp(I_i) \left( 1 - \sum_{i=1}^{n} \frac{d_i}{\sharp(I_i)} \right),$$

y se sigue el enunciado previsto. □

Tenemos la siguiente aplicación inmediata:

COROLLARIO 2.3.2. *Con las notaciones previas, sea $I$ un subconjunto finito de $K$ and $F \in K[X_1, \ldots, X_n]$ un polinomio de grado $d$. La probabilidad de que una elección aletaoria de un punto $x \in I^n$ sea un cero de $F$ es, a lo sumo :*

$$\frac{d}{\sharp(I)}$$

*En particular, si $\sharp(I) \geq 2d + 1$,la probabilidad de que una elección aletoria en $I^n$ de un valor no nulo de $F$ es, al menos, $1/2$.*

DEMOSTRACIÓN. Basta con usar el Lema precedente con $I = I_1 = \cdots = I_n$. □

Esto genera el siguiente algoritmo probablistia polinomial (**RP** o MonteCarlo) para detectar polinomios no nulos.

---

INPUT : El código de un esquema de evaluación bien paralelizable $\mathcal{G}$ en $n$ variables, que evalúa un polinomio de grado $d$.

**guess indeterministically**

$$x = (x_1, \ldots, x_n) \in \{-d, \ldots, 0, 1, \ldots, d\}$$

**Eval** $\mathcal{G}$ en $x$.
**if** $\mathcal{G}(x) \neq 0$, OUTPUT : "Es un polinomio no nulo",
  **else** OUTPUT : "Probablemente sea nulo",
**fi**

**end**

---

Para aumentar la "certeza" de que el polinomio probablemente sea el polinomio nulo, basta con repetir el proceso varias veces, observando que tras $k$ reiteraciones, si nos hubiera salido siempre nulo, el polinomio sería nulo con probabilidad al menos

$$1 - \frac{1}{2^k}.$$

COROLLARIO 2.3.3. *Con las anteriores notaciones, si existe un subconjunto $I$ de $K$ de, al menos, $2d$ elementos, entonces para todo polinomio $f \in K[X_1, \ldots, X_n]$ de grado a lo sumo $d$ existe $(t_1, \ldots, t_n) \in K^n$ tal que $f(t_1, \ldots, t_n) \neq 0$.*

DEMOSTRACIÓN. Consecuencia inmediata del resultado precedente. □

### 2.3.2. Cuestores.

DEFINICIÓN 1. *Dado un subconjunto (no necesariamente finito) $\mathcal{F} \subset K[X_1, \ldots, X_n]$ (que contiene al polinomio nulo) Diremos que un conjunto finito $\mathcal{Q} \subset \mathbb{K}^n$ es un questor (o una "Correct Test Sequence") para $\mathcal{F}$ si y sólo si para todo $F \in \mathcal{F}$ se tiene :*

$$P \mid_{\mathcal{Q}} = 0 \Longrightarrow P \equiv 0 \ .$$

El resultado depende fuertemente de la desigualdad de Bézoutque analizaremos posteriormente. El primer resultado significativo es el siguiente :

LEMA 2.3.4 ([**KrPa, 96**]). *Sea $O(L, \ell, n)$ el conjunto de todos los polinomios en $\mathbb{K}[X_1, \ldots, X_n]$ que se pueden evaluar mediante un esquema de evaluación de talla $L$ y profundidad $\ell$. Sea $W(L, \ell, n)$ la clausura Zariski de ese conjunto. Entonces, se verifica*

$$\deg W(L, \ell, n) \leq (2^{\ell+1} - 2)^{2L(L-(n+1))}.$$

TEOREMA 2.3.5 (Existencia de Conjuntos Cuestores). *Sea $K$ un cuerpo y sean $n, \ell, L \in \mathbb{N}$, $L \geq n + 1$. Sean*

$$u := (2^{\ell+1} - 2)\,(2^{\ell} + 1)^2 \qquad \text{and} \qquad t := 6\,(\ell L)^2.$$

*Supongamos que la característica de $K$ es mayor que $u$ o que la característica de $K$ es cero. Entonces, el conjunto $\{1, \ldots, u\}^n \subset K^n$ contiene al menos $u^{nt}\,(1 - u^{-\frac{t}{6}})$ conjuntos cuestores de longitud $t$ para $W(L, \ell, n)$. En particular, contiene al menos uno.*

Observe el lector que un elección aleatoria de un subconjunto cualquiera de $t$ elementos del conjunto $\{1, \ldots, u\}^n \subset K^n$ es un conjunto cuestor para $W(L, \ell, n)$ con probabilidad mayor que

$$(1 - u^{-\frac{t}{6}}) > 1/2.$$

Por tanto, el algoritmo del Tests de Zippel–Schwartz se transforma en un algoritmo **RP** mediante el siguiente esquema :

---

INPUT : El código de un esquema de evaluación bien paralelizable $\mathcal{G}$ en $n$ variables, que evalúa un polinomio de grado $d$. Supongamos que $\mathcal{G}$ es de talla $L$ y profundidad $\ell$.
**Compute** $u$ y $t$ (como en el Teorema anterior)
  **guess indeterministically** $\mathcal{Q} \subseteq \{1, \ldots, u\}^n$ de cardinal $t$.
  **Eval** $\mathcal{G}$ en $x$ para cada $x \in \mathcal{Q}$.
  **if** $\mathcal{G}(x) \neq 0$, para algún $x$ OUTPUT : "Es un polinomio no nulo",
    **else** OUTPUT : "Probablemente sea nulo",
  **fi**
**end**

---

En este caso, la probabilidad de no cometer errores es, al menos

$$(1 - u^{-\frac{t}{6}}).$$

**2.3.3. Witness Theorem.** Comencemos fijando la terminología con la siguiente Definición :

DEFINICIÓN 2. *Un testigo (Witness) para un polinomio $F \in K[X_1, \ldots, X_n]$ es un punto $\underline{\omega} \in K^n$ tal que si $F(\underline{\omega}) = 0$ implica $P = 0$.*

En otras palabras, un testigo es un punto $\underline{\omega} \in K^n$ fuera del conjunto de puntos $K-$racionales de la hipersuprficie $V(F)$ (si hubiera alguno). La manera de obtenerlo de modo explícito es el siguiente Teorema

TEOREMA 2.3.6 (Witness Theorem). *Sea $K$ un cuerpo de números, $F \in K[X_1, \ldots, X_n]$ un polinomio no nulo evaluable por un esquema de evaluación $\Gamma$ de talla $L$, profundidad $\ell$ y parámetros en $\mathcal{F} \subseteq K$. Sea $\omega_0 \in K$ tal que se verifica la siguiente desigualdad :*

$$ht(\omega_0) \geq \max\{\log 2, ht(\mathcal{F})\}.$$

*Sea $N \in \mathbb{N}$ un número natural tal que se verifica la siguiente desigualdad :*

$$\log N > \log(\ell + 1) + (\ell + 2)(\log 2)\,(\log\log(4L))\,.$$

*Definamos recursivamente la siguiente secuencia de números algebraicos (conocida como Esquema de Kronecker) :*

$$\omega_1 = \omega_0^N,$$

*y para cada $i$, $2 \leq i \leq n$, definamos*

$$\omega_i = \omega_{i-1}^N.$$

*Entonces, el punto $\underline{\omega} := (\omega_1, \ldots, \omega_n) \in K^n$ es un testigo para $F$ (i.e. $F(\underline{\omega}) \neq 0$).*

La demostración se sigue por un argumento inductivo, que usa fuertemente una Generalización de la Desigualdad de Liouville, descrito en [**CHMP, 01**].

COROLLARIO 2.3.7. *Sea $F \in K[X_1, \ldots, X_n]$un polinomio no nulo evaluable por un esquema de evaluación de talla $L$, profundidad $\ell$ y parámetros en $\mathcal{F} := \{x_1, \ldots, x_r\} \subseteq K$. Sea $\omega_{-1} \in K$ tal que*

$$ht(\omega_{-1}) := \max\{\log 2, ht(x_1), \ldots, ht(x_r)\}.$$

*Definamos $\omega_0 \in K$ como $\omega_0 := \omega_{-1}^{2L^2}$. Sea $N \in \mathbb{N}$ un número natural tal que*

$$\log N > \log(\ell + 1) + (\ell + 2)(\log 2)\,(\log\log(4L))\,.$$

*Definamos recursivamente la siguiente secuencia de números algebraicos (Esquema de Kronecker) :*

$$\omega_1 = \omega_0^N,$$

*y para cada $i$, $2 \leq i \leq n$, definamos $\omega_i = \omega_{i-1}^N$. Entonces, el punto $\underline{\omega} := (\omega_1, \ldots, \omega_n) \in K^n$ es un Testigo para $F$ (i.e. $F(\underline{\omega}) \neq 0$).*

OBSERVACIÓN 2.3.8.

i) El resultado nos da, codificado como un esquema de evaluación, un punto en el que no se anula el polinomio dado. Sin embargo, el tal Testigo es un punto que, en expansión binaria, resulta excesivo para poder manejarlo del modo adecuado. Por ello, el uso de métodos tipo Witness Theorem exigen poner un especial cuidado con el tamaño de los resultados intermedios o, en su defecto, usar Tests Probabilistas para números dados por esquemas de evaluación como los que se introducen en la Subsección 2.3.4 siguiente.

ii) El Caso Denso . Para la mayoría (genéricamente) de los polinomios $F \in K[X_1, \ldots, X_n]$ de grado $d$, el esquema de evaluación óptimo tiene talla

$$L = \binom{d+n}{n},$$

y profundidad $\ell = \log d + O(1)$. Los parámetros en este caso genérico son los coeficientes de $F$. El Teorema 2.3.6 anterior dice que existe una pequeña constante universal $c_2 > 1$, tal que la cota que debe verificar $N$ es simplemente la cota siguiente :

$$\log N > c_2 n \log^2 d.$$

iii) El caso Ralo (Sparse/Fewnomials). Supongamos que nuestro polinomio $F \in K[X_1, \ldots, X_n]$ tiene pocos términos no nulos. Supongamos que $F$ tiene grado a lo sumo $d$ y que a lo sumo $M$ de sus términos tienen coeficientes no nulos. Entre estos polinomios, el esquema de evaluación óptimo que los evalúa tiene talla del orden $L = c_3 M d$ (donde $c_3 > 0$ es una constante universal), y profundidad $\log_2 d + O(1)$. Entonces, el Teorema 2.3.6 anterior dice que existe una pequeña constante $c_3 > 1$, tal que la condición para definir $N$ en el esquema de Kronecker es la siguiente :

$$\log N > c_3 \log d \left(\log \log d + \log \log M\right).$$

**2.3.4. Tests de Nulidad para Números Dados por Esquemas de Evaluación.** Del mismo modo que los esquemas de evaluación pueden ser la buena estructura de datos para codificar polinomios que aparecen en Teoría de la Elminación, la misma estructura de datos se aplica a la representación de números enteros y racionales que aparecen como resultados de eliminación. Del mismo modo que ocurre con los polinomios, los esquemas de evaluación de números son muy adecuados para realizar operaciones aritméticas entre números codificados mediante esquemas. Sin embargo, los Tests de Igualdad (o Tests de Nulidad) son problemáticos. En este sentido, la operación correspondiente a la evaluación de un polinomio es la operación de evaluar un esquema de evaluación módulo una constante dada. La buena capacidad de adaptación de los esquemas de evaluación para estas propiedades hace que los Tests de Nulidad para esquemas de evaluación representando números pasen por los cálculos modulares. Los algoritmos esenciales en esta Sección vienen de los trabajos de O.H. Ibarra, S. Moran[6] y del trabajo de A. Schönhage [7]
El resultado esencial es el siguiente Teorema que aprovecha ampliamente del Teorema de Densidad de los Números Primos.

Teorema 2.3.9. *Existe un algoritmo probabilista que, en tiempo polinomial decide la nulidad de todo número entero evaluado por un esquema de evaluación.*

El resultado técnico esencial es el siguiente Lema.

Lema 2.3.10. *Sea $N$ un número entero no nulo tal que*

$$|N| \leq 2^{2n2^n}$$

*Etonces, para $n$ suficientemente grande, la probabilidad de que $N \neq 0$ mod $m$, para una elección aleatoria de $m \in \{1, \ldots, 2^{2n}\}$ es, al menos,*

$$\frac{1}{4n}$$

[6]O.H. Ibarra, S. Moran, *Equivalence of Straight–Line Programs.* J. of the ACM **30** (1983), 217–228.

[7]A. Schönhage, *On the power of random access machines.* In H. A. Maurer, ed., Proceedings of the 6th Colloquium on Automata, Languages and Programming, vol. **71** of LNCS, Springer, 1979, 520–529.

El algoritmo correspondiente se define del modo siguiente :

---

INPUT : $\Gamma$ el código de un esquema de evaluación de talla $L$ evaluando un número entero.
**Gess** un conjunto $D_L$ de $4L$ números enteros en el conjunto $\{1, \ldots, 2^{2L}\}$,
    **if** $\Gamma \neq 0 mod m$, para algún $m \in D_L$, OUTPUT : "El número es no nulo".
        **else** OUTPUT :"El número es probablemente nulo.
    **fi**
**end**

---

La probabilidad de error en este algoritmo es del orden

$$(1 - \frac{1}{4L})^{4L} < e^{-1} < 1/2,$$

donde $e$ es el número de Neper.

## 2.4. Una demostración elemental del Nullstellensatz de Hilbert: Parte II

La primera prueba del Nullstellensatz de Hilbert puede encontrarse en el trabajo de D. Hilbert[8] de 1893. Un poco antes, en 1882, L. Krnoecker [9] demuestra el miso resultado, aunque en un contexto y con una interpretación distintas.
Previamente al Teorema de los Ceros y, aunque no es necesario, vamos a recordar el Teorema de la Base de Hilbert, en la versión de Lasker o Neother. Dicho Teorema fue descrito por D. Hilbert[10] en 1890 y puede enunciarse como sigue.

TEOREMA 2.4.1 (**Hilbert's Basissatz**). *Si $K$ es un cuerpo (o un anillo noteheriano), el anillo $K[X_1, \ldots, X_n]$ es noetheriano. Es decir, todo ideal de $K[X_1, \ldots, X_n]$ es finitamente generado. En otras palabras, si $\mathfrak{a}$ es un ideal de $K[X_1, \ldots, X_n]$ exite un conjunto finito $\{f_1, \ldots, f_s\} \subseteq \mathfrak{a}$ tal que:*

$$\mathfrak{a} = (f_1, \ldots, f_s).$$

OBSERVACIÓN 2.4.2. El Teorema de la base de Hilbert puede escribirse de maneras diversas. Una maner didáctica de recordarle es la siguiente: Supongamos que nos dan un conjunto finito de elementos $\{f_1, \ldots, f_s\}$ en el anillo $K[X_1, \ldots, X_n]$. Entonces, el ideal $\mathfrak{a} = (f_1, \ldots, f_s)$ que generan se describe mediante:

$$\mathfrak{a} := \{g \in K[X_1, \ldots, X_n] \ : \ \exists g_1, \ldots, g_s \in K[X_1, \ldots, X_n], \ g = g_1 f_1 + \cdots + g_s f_s\}.$$

A las presentaciones de un elemento $g$ de un ideal $\mathfrak{a}$ como "combinación lineal" de los generadores, es decir, como:

$$g = g_1 f_1 + \cdots + g_s f_s,$$

se les suele denominar *Indetidad de Bézout*. Aunque, más normalmente, se suele aplicar al caso $g = 1$ cuando corresponda.

---

[8]D. Hilbert, *Über die vollen Invariantensysteme*. Mathematische Annalen **42** (1893), 313373.
[9]L. Kronecker, *Grundzüge einer arithmetischen theorie de algebraischen grössen*. J. reine angew. Math. **92** (1882) 1122.
[10]D. Hilbert, *Über theorie der Algebraischen Formen*. Math. Ann. **36** (1890), 473-534.

### 2.4.1. Nullstellensatz de Hilbert.

LEMA 2.4.3. *Sea $K$ un cuerpo y $f \in K[X_1, \ldots, X_n]$ un polinomio homogéneo no nulo. Entonces, para cada $i$, $1 \leq i \leq n$, el polinomio en una variable menos*

$$f(X_1, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n),$$

*es un polinomio no nulo.*

DEMOSTRACIÓN. Probaremos por inducción en $n$ que si $\mathbb{K}$ es una clausura algebraica de $K$, existe un punto $t = (t_1, \ldots, t_{n-1}) \in \mathbb{K}^n$ tal que $f(t_1, \ldots, t_{n-1}, 1) \neq 0$. El caso $n = 1$ es obvio. Probémoslo para el caso $i = n$ por simplicidad. Consideremos la expansión de $f$ con respecto a la variable $X_n$:

$$f = f_d(X_1, \ldots, X_{n-1})X_n^d + f_{d-1}(X_1, \ldots, X_{n-1})X_n^{d-1} + \cdots + f_0(X_1, \ldots, X_{n-1}),$$

donde $d$ es el grado de $f$ con respecto a la variable $X_n$ (es decir, $d$ es el mayor número natural $k$ tal que $X_n^k$ divide a algún término con coeficiente no nulo de la expansión monomial de $f$). En particular, $f_d \in K[X_1, \ldots, X_{n-1}]$ es un polinomio no nulo. Además, los distintos polinomios $f_i(X_1, \ldots, X_{n-1}) \in K[X_1, \ldots, X_{n-1}]$ son homogéneos de grado $\deg(f) - i$, donde $\deg(f)$ es el grado total del polinomio $f$ (para verificar ésto basta con observar que los $f_i$ se obtienen sacando factor común de los términos de la expansión monomial de $f$ divisibles por $X_n^i$).
Como $f_d$ es no nulo, por hipótesis inductiva, ha de existir un punto $t := (t_1, \ldots, t_{n-1}) \in \mathbb{K}^{n-1} \setminus \{0\}$ tal que $f_d(t_1, \ldots, t_{n-1}) \neq 0$. Ese punto puede existir por la simple aplicación de la hipótesis inductiva, aunque no nos preocupamos de quién es.
Consideremos el polinomio univariado:

$$f(t, X_n) := \sum_{i=0}^{d} f_i(t_1, \ldots, t_{n-1})X_n^i \in \mathbb{K}[X_n].$$

Como el coeficiente director ($f_d(t_1, \ldots, t_{n-1}) \neq 0$) de ese polinomio es no nulo, entonces, $f(t, X_n)$ es un polinomio no nulo en $\mathbb{K}[X_n]$. Consideremos ahora un punto $\lambda \in \mathbb{C} \setminus \{0\}$ un elemento no nulo. Entonces, tenemos la siguiente igualdad:

$$\lambda^{\deg(f)} f(t, \frac{1}{\lambda}) = \sum_{i=0}^{d} \lambda^{\deg(f)} f_i(t_1, \ldots, t_{n-1}) \left(\frac{1}{\lambda}\right)^i.$$

Por ser homogéneos tosos los polinomios involucrados, tendremos:

$$\lambda^{\deg(f)} f(t, \frac{1}{\lambda}) = \sum_{i=0}^{d} \lambda^{\deg(f)-i} f_i(t_1, \ldots, t_{n-1}) = \sum_{i=0}^{n} f_i(\lambda t_1, \ldots, \lambda t_{n-1}) = f(\lambda t_1, \ldots, \lambda t_{n-1}, 1).$$

Ahora, si el polinomio $f(X_1, \ldots, X_{n-1}, 1)$ fuera el polinomio nulo tendríamos:

$$\lambda^{\deg(f)} f(t, \frac{1}{\lambda}) = 0, \forall \lambda \in \mathbb{K} \setminus \{0\},$$

luego

$$f(t, \frac{1}{\lambda}) = 0, \forall \lambda \in \mathbb{K} \setminus \{0\},$$

o también

$$f(t, \lambda) = 0, \forall \lambda \in \mathbb{K} \setminus \{0\}.$$

Como $\mathbb{K}$ es un cuerpo infinito, esto sólo puede suceder si $f(t, X_n)$ es el polinomio idénticamente cero y habríamos llegado a contradicción. □

TEOREMA 2.4.4 (**Hilbert's Nullstellensatz**). *Sea $\mathfrak{a}$ un ideal en un anillo $K[X_1, \ldots, X_n]$, siendo $K$ un cuerpo infinito. Entonces, la variedad algebraica $V = V_{\mathbb{K}}(\mathfrak{a}) \subseteq \mathbb{K}^n$ verifica:*

$$V = \emptyset \iff 1 \in \mathfrak{a}.$$

DEMOSTRACIÓN. Hay una implicación obvia: si $1 \in \mathfrak{a}$, es decir $\mathfrak{a} = K[X_1, \ldots, X_n]$, es obvio que $V_{\mathbb{K}}(\mathfrak{a}) = \emptyset$.
Para la otra implicación haremos inducción en $n$, usando el Corolario 2.3.3 anterior. El caso $n = 1$ es obvio.
Supongamos que el resultado es cierto para todo ideal propio en todo ideal de un anillo de polinomios involucrando a los sumo $n-1$ variavles (esto es, en todo anillo del tipo $K[Y_1, \ldots, Y_r]$, con $r \leq n-1$).
Por hipótesis, $\mathfrak{a}$ es un ideal propio en $K[X_1, \ldots, X_n]$. Como $K$ es infinito, podemos encontrar un elemento $f \in \mathfrak{a}$ de grado $d$ no nulo y un subconjunto $I$ de $K$ de cardinal $2d+1$. Siguiendo la descomposición descrita en la Observación 2.2.2, sea $f_d(X_1, \ldots, X_n)$ su parte homogénea de grado $d$ y no nula. Supongamos, sin pérdida de la generalidad, que $f(X_1, \ldots, X_{n-1}, 1) \neq 0$. Por tanto, existe $(t_1, \ldots, t_{n-1}) \in I^{n-1}$, tal que

$$f(t_1, \ldots, t_{n-1}, 1) \neq 0.$$

Consideremos ahora el isomorfismo descrito en la Sección 2.2 (es decir, el isomorfismo de la Ecuación 2.2.2):

$$\begin{array}{rccc} \varphi: & K[X_1, \ldots, X_n] & \longrightarrow & K[Y_1, \ldots, Y_n] \\ & f & \longmapsto & f(Y_1 + t_1 Y_n, \ldots, Y_{n-1} + t_{n-1} Y_n, Y_n). \end{array} \tag{2.4.1}$$

Entonces, por el apartado i) del Lema 2.2.1, como $\mathfrak{a}$ es un ideal propio, también lo es el ideal $\mathfrak{b} := \varphi(\mathfrak{a})$. Pero $g := \varphi(f)$ es, tras este cambio de variables un polinomio mónico no nulo en $\mathfrak{b}$. Adicionalmente, consideremos el ideal

$$\mathfrak{c} := \mathfrak{b}^c := \mathfrak{b} \cap K[Y_1, \ldots, Y_{n-1}].$$

Como $\mathfrak{b}$ es propio, también lo es $\mathfrak{c}$. Y, por hipótesis inductiva, $V_{\mathbb{K}^{n-1}}(\mathfrak{c}) \neq \emptyset$.
Podemos aplicar el Lema 2.1.3 (se satisfacen las dos condiciones i) y ii)) a $\mathfrak{b}$ y concluir que $V_{\mathbb{K}}(\mathfrak{b}) \neq \emptyset$ es no vacío. Usando el apartado iii) del Lema 2.2.1, tendremos que $V_{\mathbb{K}}(\mathfrak{a}) \neq \emptyset$ es no vacío. □

### 2.4.2. Nullstellensatz de Hilbert: Cuerpos finitos.

TEOREMA 2.4.5 (**Hilbert's Nullstellensatz: cuerpos finitos**). *Sea $\mathfrak{a}$ un ideal en un anillo $K[X_1, \ldots, X_n]$, siendo $K$ un cuerpo finito. Supongamos que $\mathfrak{a}$ posee un elemento no nulo y no unidad de grado $d \geq 1$. Supongamos que el cardinal de $K$ verifica: $\sharp(K) \geq 2d+1$. Entonces, la variedad algebraica $V = V_{\mathbb{K}}(\mathfrak{a}) \subseteq \mathbb{K}^n$ verifica:*

$$V = \emptyset \Longleftrightarrow 1 \in \mathfrak{a}.$$

DEMOSTRACIÓN. El resultado se sigue de una demostración idéntica a la anterior. Nótese que el punto crítico es que el número de elementos del cuerpo sea suficientemente grande. □

OBSERVACIÓN 2.4.6. En las utilizaciones algorítmicas del Nullstellensatz sobre cuerpos finitos, si el cuerpo inicial $K$ sobre el que se trabaja no tiene suficientemente elementos se suelen usar extensiones finitas de $K$ que tienen un cardinal suficientemente grande con respecto a los grados de los polinomios involucrados. Una forma de entender estas construcciones son las siguientes.

*2.4.2.1. Un recordatorio sobre Cuerpos Finitos.* Unas palabras para recordar los cuerpos finitos y cómo podemos extenderlos.

TEOREMA 2.4.7. *Todo cuerpo finito $F$ de cardinal $p^m$ y característica $p$ es el menor cuerpo que contiene a $\mathbb{Z}/p\mathbb{Z}$ y a todas las raíces de la ecuación*

$$X^{p^m} - X = 0.$$

*De hecho, los elementos de $F$ son justamente las raíces de esa ecuación.*

DEFINICIÓN 3. *Sea $F$ un cuerpo finito de cardinal $q = p^m$ y sea $n$ un número entero coprimo con $q$. Llamaremos raíz primitiva $n-$ésima de la unidad a todo elemento $\theta$ de $F$ tal que las siguientes sean las $n$ raíces distintas de la unidad :*

$$\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}.$$

En el caso en que $n$ es coprimo con $q$ las raíces $n-$ésimas primitivas de la unidad sobre $F$ tienen un comportamiento próximo al caso de característica 0; aunque con matices y diferencias que es necesario destacar.

DEFINICIÓN 4. *Sea $F$ un cuerpo finito de cardinal $q = p^m$ y sea $n$ un número natural no nulo coprimo con $q$. La siguiente función racional es un polinomio en $F[X]$ llamado polinomio ciclotómico de grado $n$ :*

$$f_n(X) := \prod_{d|n} \left(X^{n/d} - 1\right)^{\mu(d)},$$

*donde $\mu$ es la función de Möbius. La funcin de Möbius fue introducida como el discriminante en Teoría de Números. Viene definida del modo siguiente : Sea $n \in \mathbb{N}$ un número natural. Definimos $\mu(n)$, mediante :*

$$\mu(n) := \begin{cases} 0 & \text{si } n \text{ posee algún factor irreducible múltiple} \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ con } p_i \text{ primo, } gcd(p_i, p_j) = 1 \\ 1 & \text{si } n = 1 \end{cases}$$

*En suma, $\mu(n) = 0$ si y solamente si posee factores irreducibles múltiples. Esto permite identificar las propiedades de la función de Möbius con las propiedades del discriminante de un polinomio. Sin embargo, la función de Möbius no se sabe calcular sin conocer la factorización (lo que hace de ella una función difícil de evaluar) y tiene propiedades muy significativas como la famosa "Fórmula de Inversión de Möbius"(véase el texto descrito en el pie de página [11] para más información).*

Obsérvese que el cálculo de polinomio ciclotómico $f_n$ puede hacerse fácilmente a partir de la factorización de $n$ (en tiempo $O(\sqrt{n}log_2^2 n)$) y de todos sus divisores (tiempo $O(\sqrt{n}log_2^2 n)$).
Una raíz $n-$ésima de la unidad sobre $F$ es un elemento $\theta$ tal que $\theta^n = 1$ y las potencias $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ son todas las raíces $n-$ésimas de la unidad sobre $F$ y son todos distintos. Para calcularlas y poder trabajar con ellas, es necesario hacer uso del siguiente :

LEMA 2.4.8. *Sea $F$ un cuerpo finito de cardinal $q = p^m$ y sea $n$ un número natural no nulo coprimo con $q$. Sea $(\mathbb{Z}/n\mathbb{Z})^*$ el grupo multiplicativo de las clases de restos módulo $n$. Sea $r$ el orden de $q$ como elemento de $(\mathbb{Z}/n\mathbb{Z})^*$. Entonces, el polinomio ciclotómico $f_n$ factoriza en $F[X]$ como un producto de $\frac{\varphi(n)}{r}$ polinomios irreducibles de grado $r$ cada uno de ellos, siendo $\varphi$ la función de Euler.*

La función de Euler : Se define mediante $\phi(1) = 1$ y para $n \geq 2$ del modo siguiente :

$$\varphi(m) := \sharp\{a \in \mathbb{N} \ : \ 1 \leq a \leq m-1, mcd(a, m) = 1\}.$$

Se trata de probar que $\phi(m)$ coincide con el número de elementos del grupo de las unidades en $(\mathbb{Z}/m\mathbb{Z})^*$. En particular, $\mathbb{Z}/m\mathbb{Z}$ es un cuerpo si y solamente si $\varphi(m) = m-1$.
Otras propiedades de la funcin de Euler :

i) La funcin de Euler es multiplicativa, esto es, si $mcd(p, q) = 1$, entonces $\varphi(pq) = \varphi(q)\varphi(q)$.

[11] El texto clásico de Teoría de Números G. H. Hardy and E. M. Wright, *"An Introduction to the Theory of Numbers"*. Oxford at the Clarendon Press, 1938. Este texto contiene la fórmula de inversion de Möbius como su Teorema 270.

ii) Se tiene :

$$\sum_{m|n} \varphi(m) = n$$

Las raíces primitivas $n-$ésimas de la unidad sobre $F$ son las raíces de uno de esos factores.
Para detectar las raíces primitivas de la unidad, factoricemos $f_n$ usando uno cualquiera de los algoritmos de factorización de polinomios univariados sobre cuerpos finitos. Por ejemplo, el método descrito por E. Berlekamp y que puede resumirse en el siguiente enunciado:

TEOREMA 2.4.9 ([**Be, 70**]). *Sea $p \in \mathbb{N}$ un número primo. Sea $\mathbb{F}_p$ el cuerpo primo de $p$ elementos. Entonces, existe una máquina de Turing $M$ determinista tal que realiza la siguiente tarea :*
*dado $f \in \mathbb{F}_p[T]$ un polinomio mónico, sin factores múltiples y de grado $d$, $M$ calcula los factores irreducibles de $f$ en $\mathbb{F}_p[T]$. El tiempo de cálculo de tal máquina de Turing es polinomial en $p$ y $d$, i.e.*

$$p^{O(1)} d^{O(1)}$$

A partir de esa factorización, sea $g_n$ uno de esos factores y definamos el cuerpo

$$F' := F(\theta) = F[Y]/(g_n(Y)).$$

Se tiene :

LEMA 2.4.10. *La clase de $Y$ módulo $g_n$ (esto es, $\theta \in F'$) es una raíz primitiva $n-$ésima de la unidad sobre $F$.*

Con ello tenemos una descripción de cualquier cuerpo.

### 2.4.3. Nullstellensatz: Identidad de Bézout.

TEOREMA 2.4.11 (**Hilbert's Nullstellensatz: Identidad de Bézout**). *Sea $\{f_1, \ldots, f_s\}$ un conjunto finito de elementos de $K[X_1, \ldots, X_n]$ no todos nulos y ninugno unidad, siendo $K$ un cuerpo. Sea $d$ el máximo de os grados de los polinomios $f_1, \ldots, f_s$.Sea $V \subseteq \mathbb{K}^n$ la variedad algebraica $V = V_{\mathbb{K}}(f_1, \ldots, f_s) \subseteq \mathbb{K}^n$ de los ceros comunes de estos polinomios. Supongamos que el cardinal de $K$ satisface: $\sharp(K) \geq 2d + 1$. En tonces son equivalente:*

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

*y $\exists g_1, \ldots, g_s \in K[X_1, \ldots, X_n]$, tales que:*

$$1 = g_1 f_1 + \cdots + g_s f_s.$$

DEMOSTRACIÓN. Simplemente notar que si $\mathfrak{a}$ es el ideal que generan los polinomios $\{f_1, \ldots, f_s\}$, el ideal es propio si y solamente si $V(\mathfrak{a}) = V(f_1, \ldots, f_s) \neq \emptyset$. El resto es reescritura. □

*2.4.3.1. La Teoría de Primer Orden sobre los Complejos admite Eliminación de Cuantificadores.* Una de las aplicaciones obvias del Nullstellensatz en la forma de identidad de Bézout es la de permitir la eliminación de cuantificadores existenciales en la Teoría de Primer Orden sobre los Complejos, por ejemplo, y sobre todo cuerpo de característica cero. Analicemos un poco esa formulación, sin entrar en profundidad en los detalles. Por simplicidad supongamos $K = \mathbb{Q}$ y $\mathbb{K} = \mathbb{C}$ que, aunque no es la clausura algebraica de $\mathbb{Q}$ admite la misma formulación.
Consideremos todas las expresiones que se pueden escribir usando los siguientes elementos y sus combinaciones naturales (definen un lenguaje regular):

- Un conjunto numerable de variables $\{X_n : n \in \mathbb{N}\}$,
- Un conjunto de constantes $\{0, 1, -1\}$,

- Operaciones usuales de la teoría de anillos $(\{+,-,\dot{\}})$ y la inversión sobre las constantes no nulas $\{^{-1}\}$.
- Condiciones de signo $\{=0\}$.
- Operadores booleanos $\{\vee,\wedge,\neg\}$.
- Cuantificadores que afectan a elementos de $\mathbb{K}$: $\{\forall,\exists\}$.

Unas pocas observaciones:

i) Las constantes son los objetos que puedo construir usando $\{-1,0,1\}$ y las operaciones elementales de cuerpo $\{+,-,\dot{\}}$. Luego se trata de los número naturales $\mathbb{Z}$.

ii) Si admito la inversión de constantes no nulas $(\{^{-1}\})$ tengo el cuerpo de los racionales $\mathbb{Q}$.

iii) Las funciones se obtienen mezclando constantes (en $\mathbb{Q}$), variables y las operaciones de anillo $\{+,-,\dot{\}}$, son los polinomios en un número finito de variables $\mathbb{Q}[X_0,\ldots,X_n]$.

iv) Las fórmulas atómicas son, expresiones de la forma $f(X_0,\ldots,X_n)=0$, con $f\in\mathbb{Q}[X_0,\ldots,X_n]$ un polinomio en un número finito de variables. Usualmente, de admiten como fórmulas atómicas las negaciones de las anteriores, es decir, $\neg(f(X_0,\ldots,X_n)=0)$ o, equivalentemente, $f(X_0,\ldots,X_n)\neq 0$.

v) Se admiten coombinaciones booleanas de fórmulas atómicas. Se pede probar que todas se pueden escribir como:

$$\bigvee_{i=1}^{n}\left(\bigwedge_{j=1}^{k}(f_{i,j}=0)\right)\bigwedge\left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}\neq 0)\right).$$

Una de las primeras observaciones casi inmediatas es que se puede suponer que todas las fórmulas son estudiables en forma pre-nexa, es decir, con los cuantifidaores por delante. Suponiendo que $f_{i,j},h_{i,j}\in K[X_0,\ldots,X_n]$, una fórmula se primer orden en el lenguaje de cuerpos algebracaente cerrados en forma pre-nexa es una fórmula del tipo:

$$Q_1X_{i_1},\ldots,Q_rX_{i_r},\ \bigvee_{i=1}^{n}\left(\bigwedge_{j=1}^{k}(f_{i,j}=0)\right)\bigwedge\left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}\neq 0)\right),$$

donde $Q_i\in\{\forall,\exists\}$ son cuantificadores. Si los cuantificadores son todos del tipo $Q_i\in\{\exists\}$, decimos que es una fórmula existencial o que sólo involucra un bloque de cuantificadores existenciales.

La **Semántica** de esas fórmulas consiste en indeiticador las fórmulas con subconjuntos de $\mathbb{K}^n$, donde $\mathbb{K}$ es algebraicamente cerrado.. Unas ideas son:

i) Así, un átomo, $f(X_0,\ldots,X_n)=0$ se identifica con el conjunto algebraico

$$V(f):=\{x=(x_0,\ldots,x_n)\in\mathbb{K}^{n+1}\ :\ f(x)=0\}.$$

ii) Una fórmula del tipo:

$$\left(\bigwedge_{j=1}^{k}(f_{i,j}(X_0,\ldots,X_n)=0)\right),$$

se identifica con la variedad algebraica (atmbién llamado cerrado en la topología de Zariski) $V(\mathfrak{a})$ donde $\mathfrak{a}$ es el ideal generado por $f_{i,1},\ldots,f_{i,m}$. Es decir, con

$$V(f_{i,1},\ldots,f_{i,m})=\{x\in\mathbb{K}^{n+1}\ :\ \left(\bigwedge_{j=1}^{k}(f_{i,j}(x)=0)\right)\}.$$

De hecho, el Teorema de la Base indica que todo $V(\mathfrak{a})$, para cualquier ideal $\mathfrak{a}$ de $K[X_0,\ldots,X_n]$ se puede escribir mediante una fórmula de este tipo.

iii) Una negación de un átomo $f(X_0,\ldots,X_n)\neq 0$ se identifica con el complementario de un conjunto algebraico dado por una sola ecuación:

$$V(f)^c := \{x=(x_0,\ldots,x_n)\in\mathbb{K}^{n+1} \ : \ f(x)\neq 0\}.$$

Se llaman abiertos de la sub-base de la toplogía de Zariski.

iv) Las fórmulas del tipo:

$$\left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}(X_0,\ldots,X_n)\neq 0)\right),$$

definen los conjuntos que forman la base de abiertos de la topología de Zariski.

$$\{x\in\mathbb{K}^{n+1} \ : \ \left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}(x)\neq 0)\right)\}.$$

Por culpa de la condición noetheriana (Teorema de la Base de Hilbert) todos los abiertos de la toplogía de Zarsikis serán uniones finitas de abiertos de la base.

v) Las fórmulas del tipo:

$$\left(\bigwedge_{j=1}^{k}(f_{i,j}=0)\right)\bigwedge\left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}\neq 0)\right)$$

definen conjuntos que son intersección de un abierto y un cerrado en la topología de Zariski.

$$\{x\in\mathbb{K}^{n+1} \ : \ \left(\bigwedge_{j=1}^{k}(f_{i,j}=0)\right)\bigwedge\left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}\neq 0)\right)\}.$$

Se llaman, obviamente, *localmente cerrados* en la topología de Zariski.

vi) Las uniones finitas de localmente cerrados se denominan *constructibles* de la toplogía de Zariski y, obviamente, son dados por fórmulas de la forma:

$$\bigvee_{i=1}^{n}\left(\bigwedge_{j=1}^{k}(f_{i,j}=0)\right)\bigwedge\left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}\neq 0)\right)$$

TEOREMA 2.4.12 (**Teorema Fundamental de la Teoría de la Eliminación**). *Sea $C\subseteq\mathbb{K}^{n+1}$ un conjunto constructible y sea $\pi:\mathbb{K}^{n+1}\longrightarrow\mathbb{K}^r$ una proyección. Entonces, $\pi(C)\subseteq\mathbb{K}^{n+1}$ es también constructible.*

En otras palabras, sea $C\subseteq\mathbb{K}^{n+1}$ un conjunto constructible dado por una fórmula $\Phi(X_0,\ldots,X_n)$ sin cuantificadores. Sea $\pi:\mathbb{K}^{n+1}\longrightarrow\mathbb{K}^r$ la proyección dada mediante:

$$\begin{array}{rccc}\pi: & \mathbb{K}^{n+1} & \longrightarrow & \mathbb{K}^r \\ & (x_0,\ldots,x_n) & \longmapsto & (x_{n-r+1},\ldots,x_n).\end{array}$$

La proyección $\pi(C)$ es el conjunto dado por la fórmula

$$\exists X_{n-r+1}\in\mathbb{K},\ldots,\exists X_n\in\mathbb{K},\ \ \Phi(X_0,\ldots,X_n).$$

El Teorema afirma que existe una fórmula de primer orden libre de cuantificadores $\Psi$ de la forma

$$\Psi(X_0,\ldots,X_{n-r}) := \bigvee_{i=1}^{n}\left(\bigwedge_{j=1}^{k}(f_{i,j}(X_0,\ldots,X_{n-r})=0)\right)\bigwedge\left(\bigwedge_{\ell=1}^{t}(g_{i,\ell}(X_0,\ldots,X_{n-r})\neq 0)\right),$$

tal que

$$\pi(C) := \{x \in \mathbb{K}^{n-r+1} \ : \ \Psi(x_0, \ldots, x_{n-r})\}.$$

Por tanto, toda fórmula con cuantificadores existencias es equivalente a una fórmula sin cuantificadores (se dice *libre de cuantificadores*). Como los constructibles son cerrados por complementación y $\forall$ se interpreta mediante $\neg\,(\exists\neg(...))$, podemos concluir.

TEOREMA 2.4.13. *Toda fórmula de primer orden del lenguajde de cuerpos algebraicamente cerrados es semánticamente equivalente a una fórmula libre de cuantificadores. Luego la teoría es completa. Además es decidible, es decir, existe un algoritmo que elimina los cuantificadores de la fórmula cuantificada.*

*2.4.3.2. Uso del Nullstellensatz Efectivo en la eliminación de un bloque de cuantificadores existenciales.* Una de las estrategias antiguas más habituales para eliminar un bloque de cuantificadores existenciales es el uso del llamado Nullstellensatz Efectivo. Fué comenzado por la alumna de D. Hilbert G. Hermann en su trabajo de 1926 [**He, 26**]. Básicamente, este enunciado puedes darse como sigue:

TEOREMA 2.4.14 (**Nullstellensatz Efectivo**, [**He, 26**]). *Existe una función* $D : \mathbb{N}^3 \longrightarrow \mathbb{R}_+$ *que verifica las popiedades siguientes:*
*Sea* $\{f_1, \ldots, f_s\}$ *un conjunto finito de elementos de* $K[X_1, \ldots, X_n]$. *Sea* $d$ *el máximo de os grados de los polinomios* $f_1, \ldots, f_s$. *Sea* $V \subseteq \mathbb{K}^n$ *la variedad algebraica* $V = V_{\mathbb{K}}(f_1, \ldots, f_s) \subseteq \mathbb{K}^n$ *de los ceros comunes de estos polinomios. Supongamos que el cardinal de* $K$ *satisface:* $\sharp(K) \geq 2d + 1$. *Entonces son equivalente:*

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

*y* $\exists g_1, \ldots, g_s \in K[X_1, \ldots, X_n]$, *tales que:*

$$deg(g_i) \leq D(d, n, s),$$

*Y*

$$1 = g_1 f_1 + dotsg_s f_s.$$

*Además,* $D(d, n, s)$ *puede elegirse satisfaciendo:*

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

La demostración es más sutil que la descrita para el Nullstellensatz porque es constructiva: se trata de dar descripciones de los polinomios que surgen en el Nullstellensatz en función de los datos $f_1, \ldots, f_s$. Las cotas iniciales de G. Hermann fueron sucesivamente reducidas por la colaboración de diversos autores y el paso de casi un centenar de aos. Se pueden destacar las siguientes:

i) D.W. Masser, G. Wusholtz (cf. [**MaWü, 71**]) : $D(d, n, s) \leq d^{2^n} s$.
ii) D.W. Brownawell (cf. [**Br, 87**]), L. Caniglia, A. Galligo, J. Heintz (cf. [**CGH, 88**]), J. Kollár (cf. [**Kl, 88**]) :$D(d, n, 2) \leq \text{máx}\{3, d\}^n$.
iii) Otras variantes con distintos métodos de cálculo se puede obtener en [**KrPa, 96**], [**HMPS, 00**], [**KPS, 01**] y sus referencias.

Este procedimiento da, por ejemplo, un procedimiento para decidir si un sistema de ecuaciones polinomiales posee una solución en una clausura algebraica sin conocer las soluciones ni calcularlas. El ejemplo más simple es el siguiente procedimiento:

---

INPUT: Una lista de polinomios $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ con coeficientes en el cuerpo $K$.

OUTPUT: Una respuesta SÍ o NO a la fórumla de primer orden:

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

---

Concepto del procedimiento:

**Introducir** un juego de variables

$$\mathfrak{Z} := \bigcup_{i=1}^{s} \{Z_{\underline{\mu}}^{(i)} \ : \ \underline{\mu} \in \mathbb{N}^n, \ |\underline{\mu}| \leq D(d,n,s)\}.$$

**Introducir** la lista de polinomios genéricos $\{G_i(\mathfrak{Z}, X_1, \ldots, X_n) \ : \ 1 \leq i \leq s\}$ dados mediante:

$$G_i(\mathfrak{Z}, X_1, \ldots, X_n) := \sum_{|\underline{\mu}| \leq D(d,n,s)} Z_{\underline{\mu}}^{(i)} X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

**Escribir** La identidad de Bézout:

$$1 = G_1(\mathfrak{Z}, X_1, \ldots, X_n) f_1(X_1, \ldots, X_n) + \cdots + G_s(\mathfrak{Z}, X_1, \ldots, X_n) f_s(X_1, \ldots, X_n). \tag{2.4.2}$$

Observación: Se trata de una igualdad entre dos polinomios de grados acotados por $D(d,n,s)+d$. Por tanto, es un sistema de ecuaciones lineales. Para verificarlo, introduzcamos un poco más de notación. Como todos los polinomios $f_1, \ldots, f_s$ tiene grado acotado por $d$, podemos suponer que existen constantes

$$\bigcup_{i=1}^{s} \{a_{\underline{\mu}}^{(i)} \ : \ \underline{\mu} \in \mathbb{N}^n, \ |\underline{\mu}| \leq d\},$$

de tal modo que:

$$f_i := \sum_{|\underline{\mu}| \leq d} a_{\underline{\mu}}^{(i)} X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Los coeficientes del producto $G_1 f_i$ se pueden escribir como sigue:

$$G_i(\mathfrak{Z}, X_1, \ldots, X_n) f_i(X_1, \ldots, X_n) := \sum_{|\underline{\theta}| \leq D(d,n,s)+d} L_{\underline{\theta}}^{(i)}(\mathfrak{Z}) X_1^{\theta_1} \cdots X_n^{\theta_n},$$

donde $L_{\underline{\theta}}^{(i)}(\mathfrak{Z})$ es la aplicación lineal (en las variables $\{Z_{\underline{\mu}}^{(i)}\}$ dada mediante:

$$L_{\underline{\theta}}^{(i)}(\mathfrak{Z}) := \sum_{\substack{\underline{\tau} + \underline{\mu} = \underline{\theta}, \\ |\underline{\tau}| \leq D(d,n,s), |\underline{\mu}| \leq d}} a_{\underline{\mu}}^{(i)} Z_{\underline{\tau}}^{(i)}.$$

Finalmente, tenemos la aplicación lineal:

$$L_{\underline{\theta}}(\mathfrak{Z}) := L_{\underline{\theta}}^{(1)}(\mathfrak{Z}) + \cdots + L_{\underline{\theta}}^{(s)}(\mathfrak{Z}).$$

Esto nos permite escribir el polinomio:

$$G_1(\mathfrak{Z}, X_1, \ldots, X_n) f_1 + \cdots + G_s(\mathfrak{Z}, X_1, \ldots, X_n) f_s = \sum_{|\underline{\theta}| \leq D(d,n,s)} L_{\underline{\theta}}(\mathfrak{Z}) X_1^{\theta_1} \cdots X_n^{\theta_n}.$$

Por tanto, la ecuación (2.4.2) es equivalente al siguiente sistema de ecuaciones lineales en las variables en la colección $\mathfrak{Z}$ siguientes:

$$\begin{cases} L_{\underline{\theta}}(\mathfrak{Z}) = 0, & \text{si } \underline{\theta} \neq (0, \ldots, 0) \\ L_{\underline{\theta}}(\mathfrak{Z}) = 1, & \text{si } \underline{\theta} = (0, \ldots, 0) \end{cases} \tag{2.4.3}$$

Lema 2.4.15. *Las siguientes propiedades son equivalentes:*

i) *Los polinomios $f_1, \ldots, f_s$ posee una solución común en $\mathbb{K}^n$, es decir, la fórmula:*

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

ii) *No existen valores en $K$ de la forma*

$$\zeta := (z_{\underline{\tau}}^{(i)} \ : \ 1 \leq i \leq s, |\underline{\tau}| \leq D(d,n,s)) \in K^{N(d,n,s)},$$

*donde $N(d,n,s)$ son los índices de las variables en la lista $\mathfrak{Z}$. Tales que*

$$1 = g_1 f_1 + \cdots ` + g_s f_s,$$

*donde*

$$g_i := G_i(\zeta, X_1, \ldots, X_n) \in K[X_1, \ldots, X_n].$$

iii) *El sistema de ecuaciones lineales (2.4.3) en las variables $\mathfrak{Z}$ con coeficientes en $K$ es incompatible.*

Demostración. La equivalencia entre i) y ii) es el Nullstellensatz de G. Hermann. La equivalencia entre ii) y iii) es mera re-escritura de la identidad de Bézout como sistema de ecuaciones lineales. En el cao univariado, el sistema es el famosos sistema asociado a la matriz de Sylvester. □

**Output:** YES si y solamente si el sistema de ecuaciones lineales (2.4.3) es un sistema de ecuaciones lineales incompatible.

---

Teorema 2.4.16. *Sea $K$ un cuerpo computable de característica distinta de 2 y sea $\mathbb{K}$ un cuerpo algebraicamente cerrado que le contiene. Existe un algoritmo que realiza la tera siguiente:*
*Dados como inputs polinomios $\{f_1, \ldots, f_s\} \in K[X_1, \ldots, X_n]$, el algoritmo decide si*

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

*El tiempo de ejecución del algoritmo está acotado por un procedimiento que realiza un número de operaciones en $K$ acotado por:*

$$O\left(\left(s\binom{\text{máx}\{3,d\}^n + d + n}{n}\right)^{\omega}\right) \leq O(s^{\omega}\, \text{máx}\{3,d\}^{\omega n^2} + d^{\omega n}),$$

*donde $\omega \leq 2{,}7$.*

Demostración. Se trata simplemente de decidir si el sistema de ecuaciones lineales (2.4.3) es o no compatible. Para el caso de caracterítica distinta de 2 podemos aplicar la cota de Bronawell–Caniglia-Galligo-Heintz-Kollár y tendremos

$$D(d,n,s) \leq \text{máx}\{3,d\}^n.$$

Ahora bien, el sistema de ecuaciones lineales (2.4.3) tiene:

- El número de variables involucradas es el número de variables en $\mathfrak{Z}$, es decir,

$$s\binom{D(d,n,s)+n}{n} \leq s\binom{\text{máx}\{3,d\}^n + n}{n},$$

  para el caso que nos ocupa es el número de coeficientes estudiado en la Parte 1 del curso para una listra de $s$ polinomios en $n$ variables de grados acotados por $D(d,n,)$.
- El número de ecuaciones en el sistema de ecuaciones lineales (2.4.3) es el número de coeficientes en $n$ variables de un polinomo de grado acotado por $D(d,n,s)+d \leq \text{máx}\{3,d\}^n + d$.

Finalmente, el exponente $\omega \leq 2{,}7$ es el exponente (menor estricto que 3) conocido desde los trabajos de V. Strassen (cf. [**St, 69**]) tal que permite decidir si un sistema de $n$ ecuaciones lineales en $m$ variables es compatible en tiempo $O(\text{máx}\{n,m\}^{\omega})$. □

COROLLARIO 2.4.17. *Existe un algoritmo que permite realizar la tarea siguiente: Dada una secuencia de polinomios* $f_1, \ldots, f_s, g_1, \ldots, g_t \in K[Y_1, \ldots, Y_m, X_1, \ldots, X_n]$, *hallar una fórmula libre de cuantificadores con coeficientes en* $K$ *y en las variables* $\{Y_1, \ldots, Y_m\}$

$$\Psi(Y_1, \ldots, Y_m),$$

*equivalente a la fórmula*
(2.4.4)

$$\exists X_1 \in \mathbb{K}, \ldots, \exists X_n \in \mathbb{K}, \left( \bigwedge_{j=1}^{s} (f_j(Y_1, \ldots, Y_m, X_1, \ldots, X_n) = 0) \right) \bigwedge \left( \bigwedge_{\ell=1}^{t} (g_\ell(Y_1, \ldots, Y_m, X_1, \ldots, X_n) \neq 0) \right).$$

*En particular, la teoría de primer orden sobre cuerpos algebraicamente cerrados es decidible y completa y admite algoritmos de eliminación de cuantificadores.*

DEMOSTRACIÓN. La única idea es reescribir la fórmula (2.4.4) como una fórmula del tipo del Nullstellensatz, usando el truco siguiente: añadamos una variable $Z_\ell$ para $1 \leq \ell \leq t$, de tal modo que se observa que la fórmula siguiente:

$$(\exists X_1 \in \mathbb{K}, \ldots, \exists X_n \in \mathbb{K},\ g_\ell(Y_1, \ldots, Y_m, X_1, \ldots, X_n) \neq 0),$$

es equivalente a la fórmula

$$(\exists Z_\ell \in \mathbb{K}, \exists X_1 \in \mathbb{K}, \ldots, \exists X_n \in \mathbb{K},\ Z_\ell g_\ell(Y_1, \ldots, Y_m, X_1, \ldots, X_n) - 1 = 0).$$

Una vez puesta nuestra fórmula en la forma del Nullstellensatz del Teorema precedente, hacemos crecer el cuerpo considerando $L = K(Y_1, \ldots, Y_m)$. Escribimos la correspondiente ecuación lineal (2.4.3) cuya matriz tiene coordenadas en $L$. De hecho, las coordenadas están en $K[Y_1, \ldots, Y_m]$. Ahora, el sistema es incompatible si y solamente si ciertos menores de la matriz de coeficientes del sistema de ecuaciones lineales (2.4.3) son nulos o no. La fórmula $\Psi(Y_1, \ldots, Y_m)$ son combinaciones booleanas de condiciones de signo sobre los menores de esa matriz. Esos menores son polinomios en $K[Y_1, \ldots, Y_m]$[12]. En particular, acabamos de denostrar el Teorema Fundamental de la Eliminación usando el Nullstellensatz y Álgebra Lineal Elemental. El resto se sigue de modo obvio. □

OBSERVACIÓN 2.4.18 (**Críticas a este Procedimiento**). Este procedimiento es el que subyace a los intentos de mejorar los Nullstellensatz Efectivos que fueron moda a finales de los años 80 y principios de los 90, pero que siguen siendo considerados resultados de élite en Matemáticas. Sin embargo, el método no es nada bueno porque la conpmplejidad ni siquiera es simplemente exponencial: está en $O(d^{\omega n^2})$. Veremos, si es posible a lo largo del curso, que se puede decidir en tiempo $O(d^{(\omega+1)n})$ con una complejidad que necesariamente están en $\Omega(d^n)$ (al menos para algoritmos universales). Por tanto, no es recomendable usar este procedimiento por más que sea el más accesible e inmediato de entender.

**2.4.4. Nullstellensatz: Maximales.** Esta versión del Nullstellensatz (totalmente equivalente a las anteriores) tiene sus reminiscencias en el Teorema del Resto, consecuencia inmediara de la división Euclídea. En España, por tradiciones incomprensibles, se suele llamar Teorema de Ruffini al Teorema del Resto. En realidad, están confundiendo el "Método de Ruffini" (que sí es un método para dividir por $(X - a)$) y es

[12]Note el alumno que se trata de los menores que, rudimentariamente, le salían en los lejanos cursos de secundaria en los que se discutía si un sistema de ecuaciones lineales con parámetros era compatbile o no.

debido a Ruffini[13]. En cambio, en el mundo anglosajón ese método de Ruffini es conocido como el "Horner's method" y se basa en un trabajo de Horner[14]. Una descripción de ese conocimiento puede verse en [**Ca, 11**]. Recientemente, en la campaña de enaltecimiento del nuevo imperio global, se ha descubierto, cómo no, que, en realidad, el "Método de Ruffini" era ya conocido por el matemático chino Qin Jiushao[15] en el siglo XIII. En todo caso, el método es tan obvio que darle un nombre carece de interés: es el "método" que a cualquiera se le ocurre. Lo que no sí es evidente es que el Teorema de Resto es antecesor de todos ellos, es consecuencia de la existencia de división euclídea y se remonta, cuando menos, al siglo III a. de C y a los *Elementos* de Euclides.
Haremos la discusión suponiendo que $K = \mathbb{K}$ es un cuerpo algebraicamente cerrado. De todos modos, la restriccón es innecesaria siempre que se consideren adecuandamente los ideales en el anillo de polinomios cuyo cuerpo de coeficientes es el cuerpo base. La hipótesis simplemente simplifica la exposición de los hechos.

Observación 2.4.19 (**Ideales maximales asociados a puntos**). Hay un tipo particular de ideales. Supongamos $\zeta := (z_1, \ldots, z_n) \in \mathbb{K}^n$ un punto en el espacio afín. Definimos el siguiente conjunto en el anillo $K[X_1, \ldots, X_n]$:

$$\mathfrak{m}_\zeta := \{f \in K[X_1, \ldots, X_n] \ : \ f(\zeta) = 0\}.$$

Se trata claramente de un ideal en $K[X_1, \ldots, X_n]$ y es un ideal maximal. Además, si $K = \mathbb{K}$, se tiene claramente que el cociente:

$$K[X_1, \ldots, X_n]/\mathfrak{m}_\zeta \cong K.$$

Se puede probar, además, que este ideal maximal tiene el siguiente cojunto de generadores:

$$\mathfrak{m}_\zeta := (X_1 - z_1, \ldots, X_n - z_n).$$

Como notación, denotaremos como $Spm(R)$ al conjunto de todos los ideales maximales de un anillo $R$.

Teorema 2.4.20 (**Hilbert's Nullstellensatz: maximales**). *Sea $K = \mathbb{K}$ un cuerpo algebraicamente cerrado. La siguiente es una biyección entre conjuntos no vacíos:*

$$\begin{array}{rccc} \mathfrak{m}: & \mathbb{K}^n & \longrightarrow & Spm(\mathbb{K}[X_1, \ldots, X_n]) \\ & \zeta & \longmapsto & \mathfrak{m}_\zeta \end{array} \tag{2.4.5}$$

Demostración. De hecho, se tiene la equivalencia entre las siguientes tres afirmaciones:

i) El cuerpo $K$ es algebraicamente cerrado, esto es, $K = \mathbb{K}$,
ii) La aplicación $\mathfrak{m}$ anterior es una biyección entre $K^n$ y $Spm(K[X_1, \ldots, X_n])$,
iii) Se verifica el Nullstellensatz de Hilbert en $K[X_1, \ldots, X_n]$ en la forma siguiente: Para cada ideal $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$, existe $\zeta \in K^n$ tal que $f(\zeta) = 0$, $\forall f \in \mathfrak{a}$, si y solamente si $1 \notin \mathfrak{a}$.

Probar que si no se verifica i), no se verifica iii) es evidente. Si un cuerpo no es algebraicamente cerrado, siempre hay un polinomio univariado e irreducible que no posee raíces en $K$ (el ejemplo $f = X^2 + 1 \in \mathbb{R}[X]$ es clásico). Ese polinomio define un ideal propio $\mathfrak{a} = (f)$ (con $1 \notin \mathfrak{a}$) y no posee ninguna solución en $K^1$. Por tanto, iii)$\Longrightarrow$ i).

[13] P. Ruffini, *Sopra la determinazione delle radici nelle equazioni numeriche di qualunque grado*. Memoria del Dottor Paolo Ruffini, pubblico professore di matematica sublime in Modena, uno dei quaranta délia società italiana delle scienze ec. Coronata dalla società medesima. In Modena, MDOCCIV. Presso la società tipografica. Con Approvazione, 1804.

[14] W. G. Horner, Horner, William George (July 1819). *A new method of solving numerical equations of all orders, by continuous approximation*. Philosophical Transactions (Royal Society of London), July 1819,. 308335.

[15] Qin Jiushao, *Shu Shu Jiu Zhang (Tratado Matemático en Nueve Secciones)*, 1247.

La implicación i) $\Longrightarrow$ iii) es simplemente el Teorema 2.4.4, dado que todo cuerpo algebraicamente cerrado es de cardinal infinito.
De otro lado, ii) $\Longrightarrow$ iii). La razón es obviamente la siguiente. En la equivalente de iii) sólo hay una implicación, la otra es obvia. La implicación es la siguiente:

$$1 \notin \mathfrak{a}, \implies \exists \zeta \in K^n, \ \ f(\zeta) = 0, \ \forall f \in \mathfrak{a}.$$

Pero si $1 \notin \mathfrak{a}$, entonces, hay un ideal maximal $\mathfrak{n}$ de $K[X_1, \ldots, X_n]$ que contiene al ideal $\mathfrak{a}$ (i.e.$\mathfrak{a} \subseteq \mathfrak{n}$). Pero, por ii), todos los tales maximales son de la forma $\mathfrak{n} = \mathfrak{m}_\zeta$, con $\zeta \in K^n$. En conclusión, existe $\zeta \in K^n$ tal que $\mathfrak{a} \subseteq \mathfrak{m}_\zeta$. Esto es lo mismo que escribir $f(\zeta) = 0$, $\forall f \in \mathfrak{a}$ y tendremos la implicación relevante de iii).
Finalmente, iii) $\Longrightarrow$ ii). Si $\mathfrak{n}$ es un ideal maximal, entonces $1 \notin \mathfrak{n}$ luego, por iii), existe $\zeta \in K^n$ tal que $f(\zeta) = 0$, $\forall f \in \mathfrak{n}$. Esto es lo mismo que decir $\mathfrak{n} \subseteq \mathfrak{m}_\zeta$. Como $\mathfrak{n}$ es maximal, entonces $\mathfrak{n} = \mathfrak{m}_\zeta$ y $\mathfrak{m}$ es suprayectiva. La inyectividad se sigue del hecho de que dos puntos disntintos de $K^n$ definen distintos maximales $\mathfrak{m}_{\zeta_1} \neq \mathfrak{m}_{\zeta_1}$. □

Observación 2.4.21. Una variación clásica de esta verisón del Nullstellensatz es el famoso Teorema de Banach-Stone-Cech-Gelfand-Kolmogorov (y algún otro autor que, probablemente, descubirón un resultado análogo por el camino). Una demostración del mismo pude consultarse en [**GiJe, 76**]. No inistermoes aquí en su historia, pero este resultado afirma lo siguiente:

Teorema 2.4.22 (**Banach-Stone-Cech-Gelfand-Kolmogorov)**. *Si $X$ es un espacio topológico compacto, entonces $X$ es homemorfo al espectro maximal de $\mathcal{C}^0(X)$.*

**2.4.5. Nullstellensatz: Rabinowitsch.** El "Truco de Rabinowitsch" es el método descrito por George Yuri Rainich, bajo el peudónimo de J. J. Raboniwtsch, en su trabajo [**Rb, 29**]. El resultado es una identificación entre los ideales del anillo de polinomios que son radicales y las variedades algebriacas. Es consecuencia inmediata del Nullstellensatz y vamos a tratar de recuperarlo.

Definición 5. *El radical de un ideal $\mathfrak{a}$ de un anillo $R$ se define mediante la siguiente igualdad:*

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

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

Se podría hacer un estudio de propiedades del radical de un ideal, pero nos limitaremos a reflejar una propiedad como la siguiente:

Proposición 2.4.23. *Si $\mathfrak{a}$ es un ideal de un anillo $R$, su radical es la intersección de todos los primos que le contienen, es decir,*

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

*donde $Spec(R)$ es el conjunto de todos los ideales primos de $R$.*

Teorema 2.4.24 (**Nullstellensatz: Rabinowitsch trick)**. *Sea $K$ un cuerpo infinito y $\mathbb{K}$ un cuerpo algebraicamente cerrado que le contiene. Consideremos los conjuntos siguientes:*

$$\mathcal{R}ad_K := \{\mathfrak{a} \subseteq K[X_1, \ldots, X_n] \ : \ \mathfrak{a} \text{ es ideal}, \sqrt{\mathfrak{a}} = \mathfrak{a}\}.$$
$$\mathcal{C}l_K := \{V_{\mathbb{K}}(\mathfrak{b}) \ : \ \mathfrak{a} \text{ es ideal de } K[X_1, \ldots, X_n]\}.$$

*La siguiente aplicación es una biyección:*

$$\begin{array}{rccc} V_{\mathbb{K}}: & \mathcal{R}ad_K & \longrightarrow & \mathcal{C}l_K \\ & \mathfrak{b} & \longmapsto & V_{\mathbb{K}}(\mathfrak{b}) \end{array}$$

*La aplicación inversa es dada mediante:*

$$\begin{array}{rccc} I_{\mathbb{K}}: & \mathcal{C}l_K & \longrightarrow & \mathcal{R}ad_K \\ & V & \longmapsto & I_{\mathbb{K}}(V) := \{f \in K[X_1, \ldots, X_n] \ : \ f(\zeta) = 0, \ \forall \zeta \in V\}. \end{array}$$

*Dicho de otra manera, para cada ideal* $\mathfrak{b}$ *de* $K[X_1, \ldots, X_n]$ *se verifica*

$$I_{\mathbb{K}}(V_{\mathbb{K}}(\mathfrak{b})) = \sqrt{\mathfrak{b}},$$

*mientras*

$$V_{\mathbb{K}}(I_{\mathbb{K}}(V)) = V, \forall V \in \mathcal{C}l_{\mathbb{K}}.$$

DEMOSTRACIÓN. En realidad sólo hay que probar que para cada ideal $\mathfrak{b}$ de $K[X_1, \ldots, X_n]$ se verifica

$$I_{\mathbb{K}}(V_{\mathbb{K}}(\mathfrak{b})) = \sqrt{\mathfrak{b}}.$$

Y, dado que tenemos que $K[X_1, \ldots, X_n]$ es noetheriano, basta con que probemos que dado un conjunto finito de elementos $\{f_1, \ldots, f_s\}$ en $K[X_1, \ldots, X_n]$, y dado un elemento adicional $f \in K[X_1, \ldots, X_n]$, si $f$ se anula sobre $V_{\mathbb{K}}(f_1, \ldots, f_s)$, entonces, existen $m \in \mathbb{N}$ y existen $g_1, \ldots, g_s \in K[X_1, \ldots, X_n]$ verificando:

$$f^m := g_1 f_1 + \cdots + g_2 f_2.$$

En realidad, técnicamente, el Truco de Rabinowirsch consiste en trabajar en la localización $K[X_1, \ldots, X_n]_f$, pero, para no introducir más lenguaje sofisticado en el curso, lo haremos sin hablar de esa localización.
Para hacerlo de esta manera clásica, introduzcamos una nueva variable $X_{n+1}$ y trabajemos en el anillo de polinomios $K[X_1, \ldots, X_n, X_{n+1}]$. En este anillo de polinomios consideremos el ideal $\mathfrak{b}'$ generado por los siguientes polinomios:

$$\mathfrak{b}' := (f_1, \ldots, f_s, X_{n+1} f - 1).$$

Dado que $f$ se anula en todos los puntos en los que se anulan simultáneamente $f_1, \ldots, f_s$, entonces

$$V_{\mathbb{K}}(\mathfrak{b}') \subseteq \mathbb{K}^{n+1},$$

es el conjunto vacío, esto es, $V_{\mathbb{K}}(\mathfrak{b}') = \emptyset$. Podemos aplicar el Nullstellensatz básico (Teorema 2.4.4 anterior) y concluiremos que existen $g_1, \ldots, g_s, g_{s+1}$ en $K[X_1, \ldots, X_{n+1}]$ tales que

$$1 = g_1 f_1 + \cdots + g_2 f_2 + g_{s+1}(X_{n+1} f - 1).$$

Ahora reemplazamos la variable $X_{n+1}$ por $\frac{1}{f}$ en la expresión anterior, observando que $f_1, \ldots, f_s$ no contienen esa variable, y obtendremos:

$$1 := \left( \sum_{i=1}^{s} g_i(X_1, \ldots, X_n, \frac{1}{f}) f_i(X_1, \ldots, X_n) \right) + g_{s+1}(X_1, \ldots, X_n, \frac{1}{f})(\frac{1}{f} f - 1).$$

Es decir, obtenemos la siguiente igualdad (en $K[X_1, \ldots, X_n]_f$):

$$1 := \left( \sum_{i=1}^{s} g_i(X_1, \ldots, X_n, \frac{1}{f}) f_i(X_1, \ldots, X_n) \right). \tag{2.4.6}$$

Sea $m$ una cota superior de los grados de los $g_i$'s con respecto a la variable $X_{n+1}$. Entonces, es una mera comprobación el verificar que:

$$h_i(X_1, \ldots, X_n) = f^m g_i(X_1, \ldots, X_n, \frac{1}{f}) \in K[X_1, \ldots, X_n].$$

Por tanto, multiplicando por $f^m$ a la identidad (**??**) obtendremos:

$$f^m := \left( \sum_{i=1}^{s} h_i(X_1, \ldots, X_n) f_i(X_1, \ldots, X_n) \right) \in \mathfrak{b}.$$

Por tanto, $f \in \sqrt{\mathfrak{b}}$ y tenemos la afirmación buscada. □

COROLLARIO 2.4.25. *Si $K = \mathbb{K}$ es un cuerpo algebraicamente cerrado, el radical y el radical de Jacobson de todo ideal en $K[X_1, \ldots, X_n]$ coinciden, es decir, para cada ideal $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$ se tiene:*

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{m} \in Spm(K[X_1, \ldots, X_n]) \ : \ \mathfrak{m} \supseteq \mathfrak{a}\}.$$

DEMOSTRACIÓN. Un contenido es evidente ($\subseteq$), para el otro, supogamos que $f$ está en todos los ideales maximales que contienen a $\mathfrak{a}$. Pero los maximales en $K[X_1, \ldots, X_n]$ están asociados a puntos. Entonces, si $\zeta \in V_{\mathbb{K}}(\mathfrak{a})$, entonces $\mathfrak{m}_\zeta \supseteq \mathfrak{a}$ y, por tanto, $f \in \mathfrak{m}_\zeta$. Luego $f(\zeta) = 0$. Por la versión anterior del Nullstellensatz, concluimos que $f \in \sqrt{\mathfrak{b}}$ y la afirmación queda demostrada. □

OBSERVACIÓN 2.4.26. El Truco de Rabinowitsch, que no es sino una variante del Nullstellensatz, permite introducir un **Diccionario Álgebra-Geometría** que permitirá traducir indistintamente los objetos geométriocs a objetos descriptibles mediante polinomios y recíprocamente. Éste es el principio de la Geometría Algebraica y tendrá su influencia en el posterior desarrollo de la Geometría a lo largo de la segunda mitad del siglo XX y princpios del XXI. Por lo que a nosotros respecta, nos quedaremos con que esa identificación existe y la usaremos cuando convenga.

Capítulo 3

# El Concepto de Solución

El concepto de solución de un sistema de ecuaciones polinomiales no puede tener una definición matemática precisa sino, más bien, una metadefinición basada en la experiencia histórica. Una pesuo-definición sería la siguiente. Consideremos un sistema de ecuaciones polinomiales:

$$\left\{\begin{array}{rcl} f_1(X_1,\ldots,X_n) & = & 0,\\ f_2(X_1,\ldots,X_n) & = & 0,\\ & \vdots & \\ f_s(X_1,\ldots,X_n) & = & 0, \end{array}\right. \tag{3.0.1}$$

donde $f_1,\ldots,f_s \in K[X_1,\ldots,X_n]$.

Definición 6 (**Pseudo-Definición**). *La resolución de un sistema de ecuaciones polinomiales multivariadas compo (3.0.1) consiste en una cantidad suficiente de información para responder a preguntas relativas al conjunto de las soluciones de esas ecuaciones, capaz de responder a preguntas relativas a ese conjunto.*

Obviamente, esto no puede ser una definición correcta en el contexto matemático y necesita de algunas precisiones más. Como afirmaba S. Lang en su teto clásico [**Lng, 72**], el objeto de la Geometría Algebraica consiste en *"...la resolución de sistemas de ecuaciones polinomiales multivariadas..."*. Lang no era "moderno" en su afirmación: simplemente retomaba la tradición clásica de geómetras de la talla de L. Kroncker, M.S. Macaulay, O. Zariski o S. Abhyankar, por citar unos nombres. Sin embargo, esto tampoco ayuda. De una parte, la Geometría Algebraica estudia los objetos geométricos así definidos y, con el tiempo, el objeto de estudio se impuso a su manipulación, por lo que no simpre contiene la la referencia a "resolución". De otro lado, el estudio de esos métodos es la fuente y la razón de un curso de Métodos Efectivos en Geometría Algebraica. En 15 horas y sin una formación preliminar medio seria en Geometría algebraica y Álgebra Conmutativa, sin embargo, es imposible dar una introducción seria al campo. A pesar de ello, vamos a hacer un esfuerzo en exponer esos elementos.
Por simplificar, comencemos exponiendo dos preguntas básicas que uno puede enunciar con respecto a las ecuaciones descritas en (3.0.1) anteriores.

Problema 5 (**Problema de Satisfactibilidad**). *Decidir si el sistema de ecuaciones (3.0.1) posee alguna solución en $K^n$.*

Observación 3.0.1. Este problema se satisfactibilidad tiene variantes que hay que discutir con cuidado:

i) Si la pregunta se hace en el caso $K = \mathbb{Q}$, el Teorema de Gödel-Turing-Robinson-Matijasievich nos dice que esa pregunta es algorítmicamente indecidible para polinomios cualesquiera. Con ello estamos diciendo simplemente que no hay algoritmo, ergo no hay método, ergo no haya nada que estudiar en este curso.
ii) Si el cuerpo $K$ es un cuerpo finito, la pregunta no es sino una verisión polinomial del problema **SAT** del que ya sabemos que es **NP**-completo y se trata de la *Conjetura de Cook*. De hecho, si el cardinal de $K$ crece, la pregunta es una

generalización más sofisticada que la mera conjetura de Cook y se trataría de un problema central en Teoría de Números.

iii) Si el cuerpo es la clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ y si sabemos, por algún método externo, que el conjunto $V_{\overline{\mathbb{Q}}}(f_1, \ldots, f_s)$ es una variedad abeliana (i.e. es un grupo, además de una variedad algebraica, con alguna operación abeliana, entonces el problema se denomina la *Conjetura de Birch y Swinerton-Dyers*.

iv) Si el cuerpo $K = \mathbb{R}$, entonces se trata del *Principio de Tarski* y es el objeto de estudio de la Geometría Algebraica Real Efectiva.

Nótese que, en esta afirmación hemos contemplado el 33 % de las Matemáticas más importantes del siglo XXI, según el Instituto Clay y el Millenium Prize[1] . Debemos decir que, en este curso, no contemplamos el caso real $K = \mathbb{R}$.

PROBLEMA 6 (**Problema de Consistencia**). *Sea $K$ cuerpo y $\mathbb{K}$ un cuerpo algebraicamente cerrado que contiene a $K$. Se trata de decidir si el sistema (3.0.1) posee soluciones en $\mathbb{K}^n$.*

OBSERVACIÓN 3.0.2. Este problema de consistencia hace referencia al Nullstellensatz del que ya hemos hablado en el Capítulo anterior. No necesairiamente usaremos el Nullstellensatz para resolver el Problema de Consistencia, pero, al menos, sabemos que siempre es tratable algorítmicamente.

PROBLEMA 7 (**Problema de Resolución**). *De nuevo sea $\mathbb{K}$ un cuerpo algebraicamente cerrado que contiene a $K$. Sabiendo, por algún medio externo, que el conjunto de soluciones del sistema (3.0.1) posee soluciones en $\mathbb{K}^n$, dar una descripción "usable" de ese conjunto de soluciones.*

En este Capítulo nos ocuparemos, sobre todo del Problema de Resolución.

## 3.1. El caso cero-dimensional

Consideremos el ideal $\mathfrak{a}$ generado por las ecuaciones $\{f_1, \ldots, f_s\}$ en $K[X_1, \ldots, X_n]$. Y nos ocupamos de pensar en el anillo cociente

$$R := K[X_1, \ldots, X_n]/\mathfrak{a}.$$

Retomamos una serie de ideas básicas de E. Artin sobre este tipo de anillos, antes de proseguir.

PROPOSICIÓN 3.1.1 (**Anillos de Artin**). *sea $R$ un anillo. Las dos propiedades siguientes son equivalentes:*

i) *Toda cadena descendente de ideales se estabiliza, es decir, dada una cadena descendente de ideales de $R$:*

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_m \supseteq \cdots,$$

*existe $m \in \mathbb{N}$ tal que $\mathfrak{a}_n = \mathfrak{a}_m$, $\forall n \geq m$.*

ii) *Todo conjunto no vacío de ideales de $R$ posee elemento minimal.*

*Los anillos que satisfacen cualquiera de estas dos propiedades equivalentes se llaman anillos de Artin o artinianos.*

DEMOSTRACIÓN. Acudir a cualquier texto básico de Álgebra Conmutativa cono [**AtMc, 69**]. □

Los anillos de Artin poseen algunas propiedades interesantes que podemos resumir. De nuevo, para una demostración se puede acudir a cualquier texto básico de Álgebra Conmutativa para no iniciados como el [**AtMc, 69**].

[1] Consultar http://www.claymath.org/millennium-problems

PROPOSICIÓN 3.1.2. *Si $R$ es un anillo de Artin, el ideal $(0)$ es un producto finito de ideales maximales. Es decir, existen ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ y enteros positivos $n_1, \ldots, n_2 \in \mathbb{N}$ tales que*

$$(0) = \mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_s^{n_s}.$$

TEOREMA 3.1.3 (**Teorema de Akizuki**). *Un anillo $R$ es artiniano si y solamente si se verifican las dos propiedades siguientes:*

i) *$R$ es noetheriano, es decir, todo ideal de $R$ es finitamente generado.*
ii) *Todo ideal $\mathfrak{p}$ primo en $R$ es maximal.*

Vamos a extraer un sencillo Corolario sobre la estructura de los anillos artinianos a través del Teorema Chino de los Restos. Recordemos este enunciado:

TEOREMA 3.1.4 (**Teorema Chino de los Restos**). *Sea $R$ un anillo y sea $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ una familia finita de ideales de $R$. Supongamos que estos ideales son dos a dos comaximales, es decir,*

$$\forall i, j,\ i \neq j\ \mathfrak{a}_i + \mathfrak{a}_j = R.$$

*Entonces, el siguiente es un isomorfismo de anillos:*

$$\begin{array}{rccc} \varphi: & R/\mathfrak{a} & \longrightarrow & \prod_{i=1}^{s} (R/\mathfrak{a}_i) \\ & x + \mathfrak{a} & \longmapsto & (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_s), \end{array}$$

*donde*

$$\mathfrak{a} = \bigcap_{i=1}^{s} \mathfrak{a}_i = \prod_{i=1}^{s} \mathfrak{a}_i.$$

De nuevo el resultado es un clásico y una demostración puede seguirse en cualquier clásico de Álgebra Conmutativa como [**AtMc, 69**]. Una conclusión casi inmediata es la siguiente:

COROLLARIO 3.1.5 (**Teorema de Estructura de anillos locales de Artin**). *Todo anillo de Artin es isomorfo a un producto de anillos locales de Artin. En particular, si*

$$(0) = \mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_s^{n_s}.$$

*es una descomposición del ideal $(0)$ de $R$ como producto de ideales maximales, el siguiente es un isomorfismo de anillos:*

$$\begin{array}{rccc} \varphi: & R/\mathfrak{a} & \longrightarrow & \prod_{i=1}^{s} (R/\mathfrak{m}_i^{n_i}) \\ & x + \mathfrak{a} & \longmapsto & (x + \mathfrak{m}_1^{n_1}, \ldots, \mathfrak{m}_s^{n_s}), \end{array}$$

DEMOSTRACIÓN. Es evidente a partir de las discusiones precendentes. □

Vamos a ver lo que significa el concepto de anillos de Artin en nuestro contexto:

DEFINICIÓN 7 (**Ideales Cero-dimensionales**). *Sea $K$ un cuerpo, $\mathbb{K}$ su calusura algebraica, $\mathfrak{a}$ un ideal en $K[X_1, \ldots, X_n]$ y $V_{\mathbb{K}}(\mathfrak{a})$ el conjunto de sus soluciones en $\mathbb{K}^n$. Decimos que $\mathfrak{a}$ es cero-dimensional si $V_{\mathbb{K}}(\mathfrak{a})$ es un conjunto finito.*
*Un conjunto finito de ecuaciones (como las descritas en (3.0.1)) se dice cero-dimensional si posee un número finito de soluciones o, equivalentemente, si el ideal $\mathfrak{a}$ que generan es cero-dimensional.*

El siguiente enunciado caracteriza los ideales y los sistemas de ecuaciones cero-dimensionales:

TEOREMA 3.1.6. *Sea $K$ un cuerpo, $\mathbb{K}$ un cuerpo algebraicamente cerrado que contiene a $K$, $\{f_1, \ldots, f_s\}$ un conjunto finito de polinomios en $K[X_1, \ldots, X_n]$. Sea $\mathfrak{a}$ el ideal gebnerado por $\{f_1, \ldots, f_s\}$ en $K[X_1, \ldots, X_n]$ y $\mathfrak{a}^e$ el ideal que generan en $\mathbb{K}[X_1, \ldots, X_n]$. Sea $V_{\mathbb{K}}(\mathfrak{a})$ el conjunto de soluciones del sistema de ecuaciones (3.0.1) en $\mathbb{K}$'n. Son equivalentes:*

i) *El sistema de ecuaciones (3.0.1) asociado a $\{f_1, \ldots, f_s\}$ es cero-dimensional.*

ii) *El ideal* $\mathfrak{a}$ *es cero-dimensional en* $K[X_1, \ldots, X_n]$.
iii) *El ideal* $\mathfrak{a}^e$ *es cero-dimensional en* $\mathbb{K}[X_1, \ldots, X_n]$.
iv) *El radical* $\sqrt{\mathfrak{a}}$ *es intersección finita de maximales de* $K[X_1, \ldots, X_n]$.
v) *El radical* $\sqrt{\mathfrak{a}}^e$ *es intersección finita de maximales de* $\mathbb{K}[X_1, \ldots, X_n]$.
vi) *El anillo* $K[X_1, \ldots, X_n]/\mathfrak{a}$ *es un anillo de Artin.*
vii) *El anillo* $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}^e$ *es un anillo de Artin.*
viii) *El anillo* $K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}$ *es un anillo de Artin.*
ix) *El anillo* $\mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}^e$ *es un anillo de Artin.*
x) *El anillo* $K[X_1, \ldots, X_n]/\mathfrak{a}$ *es un* $K-$*espacio vectorial de dimensión finita.*
xi) *El anillo* $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}^e$ *es un* $\mathbb{K}-$*espacio vectorial de dimensión finita.*
xii) *El anillo* $K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}$ *es un* $K-$*espacio vectorial de dimensión finita.*
xiii) *El anillo* $\mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}^e$ *es un* $\mathbb{K}-$*espacio vectorial de dimensión finita.*

De nuevo dejamos la demostración para el [**AtMc, 69**], combinando con el Nullstellensatz de Hilbert que hemos discutido en el Capítulo precedente. Pasemoa a describir algún detalle de lo que significan estos resultados.
En primer lugar, supongamos que $V = V_{\mathbb{K}}(\mathfrak{a}) = V_{\mathbb{K}}(\mathfrak{a}^e)$ es el conjunto dado por los elementos siguientes:

$$V := \{\zeta_1, \ldots, \zeta_{\mathscr{D}}\},$$

donde $\mathscr{D} = \sharp(V)$ es el cardinal del conjunto de soluciones. Se denomina grado de $V$ y se representa mediante $deg(V) = \mathscr{D}$. Escribamos $R$ para el anillo $K[X_1, \ldots, X_n]/\mathfrak{a}$ y escribiremos $\mathbb{K} \otimes_K R$ para $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}^e$. Finalmente, escribamos

$$R_{\text{red}} := K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}},$$

y

$$(\mathbb{K} \otimes_K R)_{\text{red}} := \mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}^e.$$

Proposición 3.1.7. *Se dan las siguientes desigualdades e igualdades:*

i) *Las dimensiones de los espacios vectoriales satisfacen:*

$$\dim_K(R) = \dim_{\mathbb{K}}(\mathbb{K} \otimes_K R) \geq \mathscr{D}.$$

*Además, como* $R \subseteq \mathbb{K} \otimes_K R$, *una base de* $R$ *como* $K-$*espacio vectorial es base de* $\mathbb{K} \otimes_K R$ *como* $\mathbb{K}-$*espacio vectorial.*
ii) *Las dimensiones de los espaciones vectoriales satisfacen:*

$$\dim_K(R_{\text{red}}) = \dim_{\mathbb{K}}\left((\mathbb{K} \otimes_K R)_{\text{red}}\right) = \mathscr{D}.$$

*Además, como* $R_{\text{red}} \subseteq (\mathbb{K} \otimes_K R)_{\text{red}}$, *una base de* $R_{\text{red}}$ *como* $K-$*espacio vectorial es base de* $(\mathbb{K} \otimes_K R)_{\text{red}}$ *como* $\mathbb{K}-$*espacio vectorial.*

Demostración. La idea clave del asunto es el Teorema Chino de los Restos, junto al Teorema de Akizuki y el Nullstellensatz. Comencemos con el caso de los anillos sobre $\mathbb{K}$. Como $\mathbb{K} \otimes_K R$ es zero-dimensional, esto es, artiniano, podemos usar el Teorema Chino de los Restos y concluir que hay un número finito de ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ y enteros positivos $n_1, \ldots, n_s \in \mathbb{N}$ tales que

$$\mathfrak{a}^e := \prod_{i=1}^{s} \mathfrak{m}_i^{n_i},$$

y, además, un isomorfismo de anillos:

$$\varphi : \quad \mathbb{K} \otimes_K R = \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}^e \quad \longrightarrow \quad \prod_{i=1}^{s} \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_i^{n_i}$$

Pero, además, el Nullstellensatz nos dice cómo son los ideales maximales de $\mathbb{K}[X_1, \ldots, X_n]$. Son todos de la forma $\mathfrak{m}_\zeta := (X_1 - z_1, \ldots, X_n - z_n)$, donde $\zeta := (z_1, \ldots, z_n) \in \mathbb{K}^n$. Pero,

además, si $\zeta \in V_{\mathbb{K}}(\mathfrak{a})$ entonces $\mathfrak{m}_\zeta \supseteq \mathfrak{a}$ y recíprocamente. Luego los ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ y los ceros en $V_{\mathbb{K}}(\mathfrak{a})$ están indenticados. Es decir,

$$\{\mathfrak{m}_1, \ldots, \mathfrak{m}_s\} = \{\mathfrak{m}_{\zeta_1}, \ldots, \mathfrak{m}_{\zeta_{\mathscr{D}}}\}.$$

Por tanto, uno puede concluir que

$$\mathfrak{a}^e := \prod_{i=}^{\mathscr{D}} \mathfrak{m}_{\zeta_i}^{n_i},$$

y

$$\mathbb{K} \otimes_K R \cong \prod_{i=1}^{\mathscr{D}} \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_{\zeta_i}^{n_i}.$$

Viendo que $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_{\zeta_i}^{n_i}$ es un $\mathbb{K}-$espacio vectorial de dimensión al menos 1 tenemos la desigualdad:

$$\dim_{\mathbb{K}}(\mathbb{K} \otimes_K R) \geq \mathscr{D}.$$

De hecho, hemos entendido mejor que existe una ligazón entre el anillo $\mathbb{K} \otimes_K R$ y las soluciones del sistema de ecuaciones. Al exponente $n_i$ se le puede denominar la multiplicidad de $\zeta_i$ como solución del sistema de ecuaciones que define el ideal $\mathfrak{a}$.
Para estudiar $R$ y la relación entre $R$ y $\mathbb{K} \otimes_K R$, recordemos un sencillo detalle. El conjunto de todos los monomios es una base de $K[X_1, \ldots, X_n]$. por su parte $\mathfrak{a}$ es un subespacio vectorial y claramente, por ser $R$ de dimensión finita, existe una base de $R$ dada por las clases de equivalencia de un conjunto finito de monomios, es decir, existe $J \subseteq \mathbb{N}^n$ tal que:

$$\beta := \{X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a} \ : \ \underline{\mu} = (\mu_1, \ldots, \mu_n) \in J\},$$

sería una base de $R := K[X_1, \ldots, X_n]/\mathfrak{a}$. Es (relativamente) fácil ver que estos mismos monomios definen una base de $\mathbb{K} \otimes R$ mediante

$$\mathbb{K} \otimes \beta := \{X_1^{\mu_1} \cdots X_n^{\mu_n} + \mathfrak{a}^e \ : \ \underline{\mu} = (\mu_1, \ldots, \mu_n) \in J\}.$$

Con ello tenemos la igualdad entre las dimensiones como espacios vectoriales (aunque con respecto a diferentes cuerpos):

$$\dim_K(R) = \dim_{\mathbb{K}}(\mathbb{K} \otimes_K R).$$

Para la otra igualdad bastará con que observemos que "tomar radicales" significa quitar exponentes y, por tanto, tendríamos algo como:

$$\mathfrak{a}^e := \prod_{i=}^{\mathscr{D}} \mathfrak{m}_{\zeta_i}^{n_i} \Longrightarrow \mathfrak{a}^e := \prod_{i=}^{\mathscr{D}} \mathfrak{m}_{\zeta_i}.$$

En particular, el Teorema Chino de los Restos implicará un ispmorfismo de anillos que es isomorfismo de espacios vectoriales (sobre $\mathbb{K}$) del tipo siguiente:

$$(\mathbb{K} \otimes_K R)_{\text{red}} \cong \prod_{i=1}^{\mathscr{D}} \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_{\zeta_i}.$$

Recordemos, además, que los maximales de la forma $\mathfrak{m}_\zeta$ tienen la propiedad de dar isomorfismos de anillos (y, por tanto, de $\mathbb{K}-$espacios vectoriales) del tipo

$$\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_\zeta \cong \mathbb{K}.$$

Por tanto,

$$(\mathbb{K} \otimes_K R)_{\text{red}} \cong \prod_{i=1}^{\mathscr{D}} \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_{\zeta_i} \cong \mathbb{K}^{\mathscr{D}},$$

y tenemos la primera igualdad de dimensiones. Usando de nuevo las bases monomiales, probaremos que

$$\dim_K(R_{\text{red}}) = \dim_{\mathbb{K}}(\mathbb{K} \otimes_K R)_{\text{red}} = \mathscr{D},$$

y se conluye el enunciado. □

Observación 3.1.8. Lo importante en este enunciado no es solamente las igualdades entre las dimensiones, sino, también, cómo son sus descomposiciones y cómo son los isomorfismos.

## 3.2. Solución en el caso cero-dimensional

Usaremos las tres nociones siguientes:

Definición 8 (**Solución simbólico-algebraica**). *Sea $K$ un cuerpo y $\mathbb{K}$ un cuerpo algebraicamente cerrado que le contiene. Dado un conjunto finito de ecuaciones $\{f_1, \ldots, f_s\} \subseteq K[X_1, \ldots, X_n]$ definiendo un sistema cero-dimensional. Una solución simbólico-algebraica del sistema (3.0.1) asociado a $\{f_1, \ldots, f_s\}$ es una descripción de los anillos cocientes:*

$$K[X_1, \ldots, X_n]/\mathfrak{a}, \;\; \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}^e.$$

Definición 9 (**Solución algebro-geométrica (o intrínseca)**). *Sea $K$ un cuerpo y $\mathbb{K}$ un cuerpo algebraicamente cerrado que le contiene. Dado un conjunto finito de ecuaciones $\{f_1, \ldots, f_s\} \subseteq K[X_1, \ldots, X_n]$ definiendo un sistema cero-dimensional. Una solución intrínseca del sistema (3.0.1) asociado a $\{f_1, \ldots, f_s\}$ es una descripción de los anillos cocientes:*

$$K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}, \;\; \mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}^e.$$

Definición 10 (**Solución numérica**). *Sea $\mathbb{Q} \subseteq K$ un cuerpo y $\mathbb{K} = \mathbb{C}$ el cuerpo de los co,plejos. Dado un conjunto finito de ecuaciones $\{f_1, \ldots, f_s\} \subseteq K[X_1, \ldots, X_n]$ definiendo un sistema cero-dimensional. Una solución numérica del sistema (3.0.1) asociado a $\{f_1, \ldots, f_s\}$ es una descripción de algunos puntos $\{z_1, \ldots, z_s\} \subseteq \mathbb{C}^n$ que "aproximan" la variedad $V_{\mathbb{C}}(\mathfrak{a})$.*

El objetivo del resto del Capítulo consiste en reflexionar cóono se pueden hacer esas descripciones y qué relaciones hay entre ellas. Así, estudiaremos:

i) Mediante Bases de Gröbner–Hironaka.
ii) Descripción "à la Macaulay".
iii) Descipricón " à la Kronecker".
iv) Descripción mediante la forma de Cayley-Chow.
v) Descripción a través de ceros aproximados ("à la Shub-Smale").

## 3.3. Descripción Simbólico-algebraica: caso cero-dimensional

Tomemos un ideal cero-dimensional $\mathfrak{a}$ del anillo de polinomios $K[X_1, \ldots, X_n]$ y analizamos la doble naturaleza del anillo cociente:

$$R := K[X_1, \ldots, X_n]/\mathfrak{a}.$$

Este anillo contiene dos ingredientes:

i) Su naturaleza de espacio vectorial de dimensión finita sobre $K$.
ii) Su naturaleza de anillo.

Definición 11 (**Homotecia definida por un elemento**). *Con las notaciones anteriores, sea $g \in K[X_1, \ldots, X_n]$ un polinomio adicional. Se denomina homotecia de razón $g$ al endomorfismo de $K-$espacios vectoriales:*

$$\begin{array}{rccc} \eta_g : & R & \longrightarrow & R \\ & h + \mathfrak{a} & \longmapsto & gh + \mathfrak{a}. \end{array}$$

Las propiedades elementales de estas homotecias son las siguientes:

PROPOSICIÓN 3.3.1. *Con las notaciones anteriores, sean $g_1, g_1 \in K[X_1, \ldots, X_n]$ y sea $\beta$ una base de $R$ como $K-$espacio vectorial y supongamos que el primer elemento de la base $\beta$ es el elemento $1 + \mathfrak{a}$. Se tiene:*

i) $\eta_{g_1} \circ \eta_{g_2} = \eta_{g_2} \circ \eta_{g_1} = \eta_{g_1 g_2} = \eta_{g_2 g_1}$.
ii) $\eta_1 = Id_R$.
iii) $\eta_{g_1} \circ \eta_{g_2} = \eta_{g_1+g_2}$.
iv) *Sean $\eta_{X_1}, \ldots, \eta_{X_n}$ las hotecias definidas por los elementos $X_1, \ldots, X_n \in K[X_1, \ldots, X_n]$. Entonces, para todo $g \in K[X_1, \ldots, X_n]$ se tiene:*
$$\eta_g := g(\eta_{X_1}, \ldots, \eta_{X_n}).$$
v) *Denotemos por $M_g$ la matriz del endomorfismo $\eta_g$ en la base $\beta$. Entonces, la primera columna de la matriz $M_g$ con las coordenadas de $g$ en la base $\beta$.*
vi) *Las matrices verifican las siguientes propiedades obvias:*
$$M_{g_1} + M_{g_2} = M_{g_2} + M_{g_1} = M_{g_1+g_2}.$$
$$M_{g_1} M_{g_2} = M_{g_2} M_{g_1} = M_{g_1 g 2}.$$
$$M_g = 0 \Longleftrightarrow g \in \mathfrak{a}.$$
vii) $M_g = g(M_{X_1}, \ldots, M_{X_n})$.
viii) *Los valores propios de la matriz $M_g$ son los valores*
$$\{g(\zeta_1), \ldots, g(\zeta_{\mathscr{D}})\},$$
*donde $V(\mathfrak{a}) = \{\zeta_1, \ldots, \zeta_{\mathscr{D}}\}$.*
ix) *El determinante de la matriz $M_g$ verifica:*
$$det(M_g) := \prod_{\zeta \in V_{\mathbb{K}}(\mathfrak{a})} g(\zeta)^{N_\zeta},$$
*donde $N_\zeta \in \mathbb{N}$ es una cantidad que depende de la mutiplicidad de $\zeta$ con respecto al ideal cero-dimensional $\mathfrak{a}$.*

DEMOSTRACIÓN. Es un ejercicio de mera comprobación. □

DEFINICIÓN 12 (**Resolución simbólico-algebraica "à la Macaulay"**). *Dado un ideal cero-dimensional $\mathfrak{a}$ en $K[X_1, \ldots, X_n]$ llamaremos resolución simbólico-algebraica "à la Macaulay" del ideal $\mathfrak{a}$ a la siguiente información:*

i) *Una base $\beta$ del anillo cociente $K[X_1, \ldots, X_n]/\mathfrak{a}$ como $K-$espacio vectorial finitamente generado y tal que su primer elemento es $1 + \mathfrak{a}$.*
ii) *Las matrices $M_{X_1}, \ldots, M_{X_n}$ de las homotecias $\eta_{X_1}, \ldots, \eta_{X_n}$ en la base $\beta$ anterior. A dichas matrices se las denomina* los tensores de multiplicación *del anillo cociente $K[X_1, \ldots, X_n]/\mathfrak{a}$.*

OBSERVACIÓN 3.3.2. Es importante observar que, en el apartado i), estamos hablando de una base de $R := K[X_1, \ldots, X_n]/\mathfrak{a}$ y no de una base de $\mathbb{K} \otimes_K R := \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}^e$. La razón es la siguiente. De una parte, el enunciado precedente Teorema 3.1.6 nos dice que las bases de $R$ como $K-$pesacio vectorial son también base de $\mathbb{K} \otimes_K R$ como $\mathbb{K}-$espacio vectorial. Con lo que calculando unas tenemos algunas de las otras. De otra parte, usualmente, el cuerpo $K$ es un cuerpo computable como, por ejemplo, los cuerpos primos o locs cuerpos finitos. Es decir, podemos pensar que $K := \mathbb{Q}$ o $K := \mathbb{F}_q$, con $q = p^n$, $p \in \mathbb{N}$ primo. De otro lado, $\mathbb{K}$ es un cuerpo algebraicamente cerrado que contiene a $K$ (no siempre la clausura algebraica). La clausura algebraica de $K$ es computable (no lo demostraremos), pero, en otros casos, $\mathbb{K}$ puede ser directamente un cuerpo no computable. El ejemplo más simple sería suponer $K = \mathbb{Q}$ y $\mathbb{K} = \mathbb{C}$. En este caso, manejar un espacio finitamente generado sobre $\mathbb{C}$ es directamente no computable, salvo porque podemos manejar sus propiedades a través de la base de $R$ como $\mathbb{Q}-$espacio

vectorial y sabemos que también es base de $\mathbb{C}\otimes_{\mathbb{Q}} R$ como $\mathbb{C}-$espacio vectorial. Lo mismo se puede decir del manejor de las matrices $M_g$ que pueden ser vistas sobre $K$, pero sus valores prpios, su forma canónica de Jordan podría leerse sobre $\mathbb{K}$ y eso es importante a la hora de obtener información sin necesidad de calcularla de manera explícita.

Dos preguntas básicas a partir de esta noción de solución son ¿cómo se puede usar? y ¿cómo se calcula?. Aquí vamos a analizar cómo se usan y en le Sección siguiente daremos un algoritmo para ver cómo se pueden calcular en algún caso, en el que la base $\beta$ es una base monomial (i.e. formada por las clases módulo $\mathfrak{a}$ de algunos de los monomios).

**3.3.1. Problema de Pertenencia al ideal.** Dado un ideal cero-dimensional $\mathfrak{a}$ en $K[X_1,\dots,X_n]$ y un polinomio adicional $g \in K[X_1,\dots,X_n]$ queremos decidir si $g \in \mathfrak{a}$. Para ello, observamos que son equivalentes:

i) $g \in \mathfrak{a}$,
ii) La matrzi $M_g = 0$,
iii) La primera columna de la matriz $M_g$ es cero.

---

Input:

- La lista $\beta$, $M_{X_1},\dots,M_{X_n}$ dada por la base y los tensores del anillo cociente $K[X_1,\dots,X_n]/\mathfrak{a}$.
- Un nuevo polinomio $g \in K[X_2,\dots,X_n]$.

**Eval** $g(M_{X_1},\dots,M_{X_n}) = M_g$
Output: **Aceptar** sii la primera columna de $M_g$ es indénticamente cero.

---

**3.3.2. Problema de Pertenencia al radical del ideal.** Dado un ideal cero-dimensional $\mathfrak{a}$ en $K[X_1,\dots,X_n]$ y un polinomio adicional $g \in K[X_1,\dots,X_n]$ queremos decidir si $g \in \sqrt{\mathfrak{a}}$. Para ello, observamos que son equivalentes:

i) $g \in \sqrt{\mathfrak{a}}$,
ii) La matriz $M_g = 0$ es nilpotente,
iii) El polinomio mínimo de $M_g$ es del tipo $T^k$.
iv) El polinomio característico de $M_d$ es $T^D$, donde $D = \dim(K[X_1,\dots,X_n]/\mathfrak{a})$.

---

Input:

- La lista $\beta$, $M_{X_1},\dots,M_{X_n}$ dada por la base y los tensores del anillo cociente $K[X_1,\dots,X_n]/\mathfrak{a}$.
- Un nuevo polinomio $g \in K[X_2,\dots,X_n]$.

**Eval** $g(M_{X_1},\dots,M_{X_n}) = M_g$
**Hallar** el polinomio característico

$$\chi_g(T) = \det(TId_D - M_g) \in K[T].$$

Output: **Aceptar** sii $\chi_g(T) = T^D$.

---

**3.3.3. Problema de Consistencia (una ecuación adicional).** Dado un ideal cero-dimensional $\mathfrak{a}$ en $K[X_1,\ldots,X_n]$ y un polinomio adicional $g \in K[X_1,\ldots,X_n]$ queremos decidir si

$$\exists \zeta \in \mathbb{K}^n,\ \ \zeta \in V_{\mathbb{K}}(\mathfrak{a}) \wedge g(\zeta) = 0.$$

Para ello, observamos que son equivalentes:

i) $\exists \zeta \in \mathbb{K}^n,\ \ \zeta \in V_{\mathbb{K}}(\mathfrak{a}) \wedge g(\zeta) = 0$,
ii) La matriz $M_g = 0$ posee un valor propio nulo.
iii) $\det(M_g) = 0$.

---

INPUT:

- La lista $\beta$, $M_{X_1},\ldots,M_{X_n}$ dada por la base y los tensores del anillo cociente $K[X_1,\ldots,X_n]/\mathfrak{a}$.
- Un nuevo polinomio $g \in K[X_2,\ldots,X_n]$.

**Eval** $g(M_{X_1},\ldots,M_{X_n}) = M_g$
**Hallar** $\det(M_g) \in K$.
OUTPUT: **Aceptar** sii $\det(M_g) = 0$.

---

OBSERVACIÓN 3.3.3 (**Ventajas e inconvenientes**). La única ventaja obvia es que el tipo de preguntas (y otras similares) se pueden responder de manera natural usando un poco de álgebra lineal. La desventaja es la dimensón posiblemente elevada del espacio vectorial $D$, que nos obliga a trabajar con matrices de altísima dimensión.

## 3.4. Bases de Gröbner

Los métodos de bases de Gröbner pertenecen a la clase de *métodos de reescritura*: Los métodos puramente sintácticos, también llamados de reescritura, son los métodos más sencillos de comprender y de implementar y es por éso que son los más difundidos. Desgraciadamente son también los más ineficaces, teniendo un comportamiento intratable y generando bloqueos en los ordenadores donde se ejecutan estos algoritmos.
Por otro lado, son los métodos más implementados en los paquetes de software simbólico y no requieren altos contenidos de matemáticas para ser entendidos.
Las referencia básicas será el [**CoLiOS, 97**] y, si se quiere, el capítulo que dedican J. von zur Gathen y J. Gerhard en su libro [**vzGGe, 99**]. El texto más completo para entender las bases de Gröbner, es el excelente libro [**BeWe, 93**]. Un texto de gran interés es el manuscrito de M. Lejeune–Jalabert, [**Le, 84**] donde se explican bien las nociones de base estándard y base de Gröbner. Se da una buena demostración del Teorema de Bézout en el caso intersección completa proyectiva.

**3.4.1. Ordenes Monomiales.** La motivación principal de la introducción de bases de Gröbner es la ausencia de un algoritmo de división euclídea en el anillo de polinomios muiltivariados con coeficientes en un cuerpo $K[X_1,\ldots,X_n]$. En particular, los ideales de este anillo de polinomios no son principales y tampoco disponemos de un algoritmo de Euclides para el cálculo del máximo común divisor[2]. La observación

[2]Mejor dicho, disponemos del algoritmo de división (siempre que el divisor sea un polinomio mónico con respecto a una de las variables), y de la noción de máximo común divisor (por el Lema de Gauss, $K[X_1,\ldots,X_n]$ es un dominio de factorización única) pero ni la una ni el otro tienen las buenas propiedades que tenían en el caso univariado.

fundamental de H. Hironaka[3] en este contexto es que :*La división euclídea funciona por disponer* $\mathbb{N}$ *de un buen orden compatible con el producto de polinomios.* Esta observación permitirá extender la división euclídea (de una manera menos perfecta) al anillo de polinomios en varias variables $K[X_1, \ldots, X_n]$. Lo haremos del modo siguiente :
Dado $\underline{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ denotaremos el MONOMIO de multigrado $\underline{\alpha}$ en las variables $X_1, \ldots, X_n$ al elemento

$$\underline{X}^{\alpha} := X_1^{\alpha_1} \cdots X_n^{\alpha_n}.$$

Llamaremos GRADO del monomio $\underline{X}^{\underline{\alpha}}$ al número natural :

$$|\underline{\alpha}| := \alpha_1 + \cdots + \alpha_n \in \mathbb{N}^n.$$

El conjunto de los monomios define una base de $K[X_1, \ldots, X_n]$ como $K-$espacio vectorial.
Dado un polinomio $f \in K[X_1, \ldots, X_n]$ existen un subconjunto finito no vacío $I \subseteq \mathbb{N}^n$ tal que :

$$f = \sum_{\underline{\alpha} \in I} a_{\underline{\alpha}} \underline{X}^{\underline{\alpha}},$$

donde $a_{\underline{\alpha}} \in K$. Los elementos de la forma $a_{\underline{\alpha}} \underline{X}^{\underline{\alpha}}$, con $a_{\underline{\alpha}} \in K \setminus \{0\}$ se denominan TÉRMINOS del polinomio $f$. El elemento $\underline{\alpha}$ se denomina EXPONENTE del término $a_{\underline{\alpha}} \underline{X}^{\underline{\alpha}}$. Ténicamente, esta representación de polinomios como combinación lineal de monomios se enomina REPRESENTACIÓN DENSA DE LOS POLINOMIOS.

*3.4.1.1. La Noción de Orden Monomial.* Por lo anterior, tenemos identificado $\mathbb{N}^n$ con los monomios en las variables $X_1, \ldots, X_n$. Además, la operación suma $+$ sobre $\mathbb{N}^n$ está identificada con la operación producto de monomios. Por tanto, podemos estudiar relaciones de orden sobre el conjunto de monomios en $K[X_1, \ldots, X_n]$ mediante las relaciones de orden sobre el monoide conmutativo $(\mathbb{N}^n, +)$. Las relaciones de orden buscadas han de ser compatibles con la operación del monoide. Esto es lo que se destaca en la siguiente noción :

DEFINICIÓN 13. *Una relación de orden* $\leq$ *en* $\mathbb{N}^n$ *se denomina un orden monomial si sevrifica las siguientes propiedades :*

i) *La relación* $\leq$ *es un buen orden en* $\mathbb{N}^n$*, ésto es, todo subconjunto no vacío de* $\mathbb{N}^n$ *posee mínimo.*
ii) *Dados* $\underline{\alpha}, \underline{\beta}, \underline{\gamma} \in \mathbb{N}^n$*, se tiene :*

$$Si \ \ \underline{\alpha} \leq \underline{\beta}, \quad entonces \ \ \underline{\alpha} + \underline{\gamma} \leq \underline{\beta} + \underline{\gamma}.$$

iii) *El elemento* $\underline{0} := (0, \ldots, 0)$ *es el mínimo de* $\mathbb{N}^n$*.*

Obsérvese que la propiedad *ii*) es la compatibilidad del orden con el producto de monomios.

*3.4.1.2. Los ejemplos clásicos de órdenes monomiales.*

- EL ORDEN DE $\mathbb{N}$ : Es el orden usual asociado a los algoritmos de división euclídea en $K[X]$.
- LEXICOGRÁFICO : Es el orden dado por el orden lexicográfico. Viene dado en los términos siguientes : Dados $\underline{\alpha} := (\alpha_1, \ldots, \alpha_n), \underline{\beta} := (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, diremos $\underline{\alpha} \leq_{plex} \underline{\beta}$ si y solamente si se verifica la siguiente propiedad : existe $j \in \{1, \ldots, n\}$, tal que

$$\alpha_i = \beta_i, \ \ \forall i, 1 \leq i \leq j-1, \quad \alpha_j \leq \beta_j.$$

[3]De hecho, el introductor de las bases de Gröbner fue Hironaka en su famoso trabajo de 1964 que la valió la medalla Fields sobre resolución de singularidades. H. Hironaka llamó a estas bases "bases standard" y demostró el Teorema de División que veremos más adelante. El algoritmo de cálculo de bases standard (o de Gröbner) es debido a B. Buchberger. El trabajo al que hacemos referencia en realidad son dos artículos aparecidos en el Annals : H. Hironaka, *Resoluction of Singularities of an Algebraic Variety over a Field of Characteristic Zero.* Annals of Math. **79** (1964), I : 109–203, II : 205–326.

- Graduado Lexicográfico : Consiste en añadir el grado al orden *plex*. Con las anteriores notaciones, diremos que $\underline{\alpha} \leq_{grlex} \underline{\beta}$ si y solamente si se verifica : o bien $|\underline{\alpha}| < |\underline{\beta}|$ o bien $|\underline{\alpha}| = |\underline{\beta}|$ y $\underline{\alpha} \leq_{plex} \underline{\beta}$.
- Graduado reverso lexocográfico [4] : Con las mismas notaciones diremos que que $\underline{\alpha} \leq_{revgrlex} \underline{\beta}$ si y solamente si se verifica : o bien $|\underline{\alpha}| < |\underline{\beta}|$ o bien o bien $|\underline{\alpha}| = |\underline{\beta}|$ y existe $j \in \{1, \ldots, n\}$ tal que $\alpha_i = \beta_i$ para todo $i$ tal que $j+1 \leq i \leq n$ y $\alpha_j \leq \beta_j$.

Antes de concluir, introduzcamos un poco más de notación sobre la representación densa de polinomios $f \in \mathbb{K}[X_1, \ldots, X_n]$. Supongamos fijado un orden monomial $\leq$ sobre $\mathbb{N}^n$ :

i) Grado de $f$ : $deg(f)$ es el máximo de los grados de sus términos.
ii) Multigrado de $f$ : $md(f)$ es el máximo de los multigrados de los términos de $f$ para el orden monomial $\leq$ fijado.
iii) Término director de $f$ : $LT(f)$ es el término de $f$ cuyo multigrado coindice con el multigrado de $f$
iv) Coeficiente director de $f$ : $LC(f)$ es el coeficiente del $LT(f)$.

**3.4.2. División de Hironaka.** Es el resultado crucial para entender las bases de Gröbner. En principio, petende ser un análogo a la división euclídea. Veremos después dónde se encuentran las diferencias y cómo podemos diseñar algoritmos que arreglen las dificultades subyacentes. Supongamos que disponemos de un orden monomial $\leq$ sobre $\mathbb{N}^n$ ya fijado en esta Subsección.
Comenzamos definiendo el escalón asociado a un exponente monomial $\underline{\alpha} \in \mathbb{N}$. Se define mediante :

$$E(\underline{\alpha}) := \underline{\alpha} + \mathbb{N}^n = \{\underline{\alpha} + \underline{\beta} \ : \ \underline{\beta} \in \mathbb{N}^n\}.$$

Obsérvese que el escalón $E(\underline{\alpha})$ es el conjunto de multigrados de todos los monomios que son divisibles por $\underline{X}^{\underline{\alpha}}$.
El resultado principal se expresa mediante el siguiente enuniciado conocido como División de Hironaka :

Teorema 3.4.1 (División de Hironaka). *El siguiente Algoritmo realiza la tarea siguiente :*
*Dados $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$, y dado $g \in K[X_1, \ldots, X_n]$. Supongamos*

$$\underline{\alpha}_i := md(f_i), \quad 1 \leq i \leq r.$$

*Definamos los conjuntos de multigrados :*

$$\begin{aligned}
\Delta_1 &:= E(\underline{\alpha}_1), \\
\Delta_2 &:= E(\underline{\alpha}_2) \setminus \Delta_1, \\
\Delta_3 &:= E(\underline{\alpha}_3) \setminus (\Delta_1 \bigcup \Delta_2), \\
&\vdots \\
\Delta_r &:= E(\underline{\alpha}_r) \setminus \left( \bigcup_{i=1}^{r-1} \Delta_i \right), \\
\overline{\Delta} &:= \mathbb{N}^n \setminus \left( \bigcup_{i=1}^{r} \Delta_i \right).
\end{aligned}$$

[4] No se trata de un orden obtenible mediante los anteriores y una permutación de las variables. Debe señalarse que, a pesar de lo extraño de su definición, suele ser el orden que mejor se comporta en la ejecución del algoritmo de cálculo de bases de Gröbner. No se sabe muy bien el porqué de este fenómeno con este particular orden monomial.

*El algoritmo anterior genera polinomios* $g_1, \ldots, g_r, h \in K[X_1, \ldots, X_n]$ *tales que se satisfacen las siguientes propiedades :*

i) *Para cada* $i$, $1 \leq i \leq r$, *los términos del polinomio* $g_i$ *tienen multigrado en* $\Delta_i$,
ii) *Los términos del polinomio* $h$ *tienen multigrado en* $\overline{\Delta}$,
iii) *Se verifica la siguiente igualdad :*

$$g := g_1 f_1 + \cdots + g_r f_r + h.$$

iv) *Los polinomios* $g_1, \ldots, g_r$ *verificando las anteriores propiedades son únicos y se denominan cocientes de la divissón de Hironaka.*
v) *El polinomio* $h$ *es único y se denomina resto de la división de Hironaka.*

El algoritmo al que hace referencia este enunciado es el siguiente :

---

INPUT : $f_1, \ldots, f_r, g \in K[X_1, \ldots, X_r]$.
$g_1 := 0, \ldots, g_r := 0, h := 0$
$p := g$
**while** $p \neq 0$ **do**
  i:=1
  div:=FALSO
    **while** $i \leq r$ y div:=FALSO **do**
      **if** $LT(f_i)$ divide a $LT(p)$ **then**
        $g_i := g_i + LT(p)LT(f_i)^{-1}$,
        $p := p - LT(p)LT(f_i)^{-1} f_i$
        div:=TRUE
      **else**
        $h := h + LT(p)$
        $p := p - LT(p)$
      **fi**
    **od**
**od**
OUTPUT : $g_1, \ldots, g_r, h$

---

Dada una lista $F := [f_1, \ldots, f_r]$ de polinomios y dado $g \in K[X_1, \ldots, X_n]$ al resto de la división de Hironaka de $g$ por $F$ se le denota $NormF(g, F)$ y se le denomina también Forma Normal de $g$ con respecto a $F$. Observe el lector que, conociendo los conjuntos $\Delta_1, \ldots, \Delta_r, \overline{\Delta}$ el anterior algoritmo consiste simplemente en resolver un sistema de ecuaciones lineales.

**3.4.3. Cálculo de Bases de Gröbner.** Volviendo al contexto histórico, si bien H. Hironaka introdujo las bases standard de un ideal, en 1965 y de modo independiente, B. Buchberger introduce las bases de Gröbner en su tesis [5]. El nombre de bases de Gröbner es en honor del director de tesis de B. Buchberger (W. Gröbner). Sin embargo, lo importante en el trabajo de B. Buchberger no es quién introdujo las bases de Gröbner

[5]B. Buchberger. *"Ein Algoritmus zum Auffinden der Basiselemente des Restklassenringes nach einen nulldimensionallen Polynomideal"*. Tesis Doctoral, Universidad Leopold–Franzens, Innsbruck (1965). Posteriomente publicó varios trabajos, un tanto minimalistas sobre su algoritmo. Nótese que trata el caso cero –dimensional solamente, aunque luego se extendió al caso general de manera obvia. Sus trabajos iniciales sobre el tema están mal publicados y no muy bien redactados. Habrá que esperar a su trabajo de 1985 para que B. Buchberger reescriba lo que quiso decir en su tesis. para entonces, una gran cantidad de científicos de todo el mundo, esencialmente provenientes del mundo de la Teoría de las Singularidades, habían caído sobre el tema y habían aportado su grano de arena. El trabajo de Buchberger de 1985 es el trabajo "Gröbner Basis : An Algorithmic Method in Polynomial Ideal theory". En *Multimdimensional Systems Theory , Mathematics and its Applications* **6**, Reidel (1985) 184–232.

(asunto éste que ha levantado más de una ampolla) sino que *B. Buchberger es el primero que muestra un algoritmo de cálculo de bases de Gröbner de un ideal* a partir de un sistema de generadores dado. Este es el mérito esencial de B. Buchberger.
El problema principal que tratan de resolver las bases de Gröbner es el siguiente :

*3.4.3.1. Problema de Pertenecia a un Ideal. Dado un ideal* $(f_1, \ldots, f_r)$ *por sus generadores y dado* $g \in K[X_1, \ldots, X_n]$ *decidir si* $g \in (f_1, \ldots, f_r)$.
Retomemos el algoritmo de Euclides para el caso univariado $n = 1$ y tratemos de observar cómo el algoritmo de Euclides justamente resuelve ese Problema en el caso univariado.

- Si el ideal es dado por un sólo generador $f_1$ basta con hallar el resto de la división euclídea de $g$ por $f_1$. El polinomio $g$ está en $(f_1)$ si y solamente si ese resto es 0.
- Si el ideal es dado por varios generadores $(f_1, \ldots, f_r)$ existe un generador especial del mismo ideal : *el máximo común divisor de* $f_1, \ldots f_r$. Sea $h$ ése máximo común divisor. Entonces, $(f_1, \ldots, f_r) = (h)$ y decidir si $g$ está en $(f_1, \ldots, f_r)$ se reduce al caso de un sólo polinomio mediante el algoritmo de Euclides.

En el caso multivariado las cosas no son tan sencillas :

i) Los ideales de $K[X_1, \ldots, X_n]$ son finitamente generados, pero no siempre (de hecho casi nunca) son principales.
ii) Existe una noción de máximo común divisor en $K[X_1, \ldots, X_n]$ por ser este anillo un dominio de factorización única (Lema de Gauss) pero este máximo común divisor no tiene las mismas buenas propiedades que en el caso univariado.

Por tanto, dado $(f_1, \ldots, f_r)$ se trata de buscar un sistema de generadores del mismo ideal $(g_1, \ldots, g_s) = (f_1, \ldots, f_r)$ que tengan las buenas propiedades del máximo común divisor en el caso univariado. Esto son las *bases de Gröbner*. Supongamos, desde ahora, que tenemos fijado un orden monomial $\leq$ en $\mathbb{N}^n$.

DEFINICIÓN 14. *Sea* $I := (f_1, \ldots, f_r)$ *un ideal de* $K[X_1, \ldots, X_n]$. *Una base de Gröbner para* $I$ *es todo subconjunto finito* $G := \{g_1, \ldots, g_s\}$ *verificando las siguientes propiedades :*

i) $(g_1, \ldots, g_s) = (f_1, \ldots, f_r)$ *y,*
ii) *Para todo polinomio* $g \in K[X_1, \ldots, X_n]$ *se tiene* $g \in I$ *si y solamente si*

$$NormF(g, G) = 0,$$

*donde* $NormF(g, G)$ *es el resto de la división de Hironaka de* $g$ *por el conjunto* $G$.

Obsérvese que la segunda propiedad (afirmación *ii*)) hace de una base de Gröbner algo muy próximo al máximo común divisor (con las debidas precauciones). No todo sistema generador de un ideal es base de Gröbner, así que el esfuerzo último consiste en desarrollar algoritmos tales que dado un ideal por sus generadores, podamos calcular una base de Gröbner del ideal. Exactamento éso es lo que hace el ALGORITMO DE B. BUCHBERGER que describimos a continuación.
Comencemos por definir el $S-$polinomio de dos polinomios dados : Sean $f, g \in K[X_1, \ldots, X_n]$ y supongamos

$$md(f) := \underline{\alpha} := (\alpha_1, \ldots, \alpha_n),$$
$$md(g) := \underline{\beta} := (\beta_1, \ldots, \beta_n),$$

llamaremos el mínimo común múltiplo de $\underline{\alpha}$ y $\underline{\beta}$ al elemento

$$LCM(\underline{\alpha}, \underline{\beta}) := \underline{\gamma} := (\gamma_1, \ldots, \gamma_n),$$

donde :

$$\gamma_i := max\{\alpha_i, \beta_i\}, \;\; 1 \leq i \leq n.$$

Nótese que $\underline{X}^{\underline{\gamma}}$ es justamente el mínimo común múltiplo de los monomios $\underline{X}^{\underline{\alpha}}$ y $\underline{X}^{\underline{\beta}}$. Por tanto, los términos directores de $f$ y $g$ dividen a $\underline{X}^{\underline{\gamma}}$. Con ello tiene sentido definir el $S-$polinomio de $f$ y $g$ mediante :

$$S(f,g) := \frac{\underline{X}^{\underline{\gamma}}}{LT(f)} f - \frac{\underline{X}^{\underline{\gamma}}}{LT(g)} g.$$

La propiedad fundamental del $S-$polinomio es que el multigrado de $S(f,g)$ es estrictamente menor que el multigrado de $\underline{X}^{\underline{\gamma}}$ con lo que se gana "algo" al calcularlo. Con esta sencilla idea como instrumento, B. Buchberger introduce el siguiente algoritmo que no es sino una versión de la eliminación Gaussiana con matrices de un tamaño desmesurado.

Teorema 3.4.2 (Buchberger). *El siguiente algoritmo calcula una base de Gröbner del ideal* $(f_1, \ldots, f_r)$.

---

Input : $F := [f_1, \ldots, f_r]$ (una lista de polinomio que generan el ideal $I$).
$G := F$
**while** $G' \neq G$ **do**
    $G' := G$
    Para cada par $(f,g)$ en $G'$ hacer
    $S := NormF(S(f,g), G')$.
        **if** $S \neq 0$ **then** $G := G \bigcup \{S\}$ (añadir $S$ a $G$)
        **else** siguiente par.
        **fi**
**od**
Output : $G$

---

Habitualmente, las bases de Gröbner contienen una información desmesuradamente grande y conducen a polinomios de un tamaño tal que bloquean las computadoras. Discutiremos este aspecto más adelante. De todas formas, ha habido algunos intentos de buscar una unicidad de las bases de Gröbner imponiendo la condición de reduciblidad. Veamos cómo hacerlo.

Definición 15. *Una base de Gröbner* $G := \{g_1, \ldots, g_s\}$ *de un ideal se denomina reducida si verifica :*

$$\forall i, \; 1 \leq i \leq s, \; NormF(g_i, G \setminus \{g_i\}) = g_i.$$

El algoritmo obvio permite transformar una base de Gröbner de un ideal en una base de Gröbner reducida. Además se tiene la propiedad siguiente :

Teorema 3.4.3. *Para un orden monomial fijado, todo ideal posee una única base de Gröbner reducida.*

**3.4.4. Aplicaciones de las bases de Gröbner.** Sería el tipo de preguntas que se puede calcular mediante bases de Gröbner. Por ejemplo,

*3.4.4.1. El Problema de Pertenencia a un Ideal.* Dado un ideal por sus generadores $(f_1, \ldots, f_r)$ , dado un polinomio $g \in K[X_1, \ldots, X_n]$, elijamos un orden monomial $\leq$ en $\mathbb{N}^n$. Hallemos una base de Gröbner $G$ de ese ideal se tiene :

$g$ pertenece al ideal $(f_1, \ldots, f_r)$ si y solamente si $NormF(g, G) = 0$.

*3.4.4.2. El problema de Consistencia.* Recuperamos el Nullstellensatz de Hilbert para resolver el Problema de Consistencia :

TEOREMA 3.4.4. *Dados $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ el sistema de ecuaciones polinomiales*

$$\left\{ \begin{array}{rcl} f_1(X_1, \ldots, X_n) & = & 0 \\ \vdots & \vdots & \vdots \\ f_s(X_1, \ldots, X_n) & = & 0 \end{array} \right. \tag{3.4.1}$$

*posee solución $(x_1, \ldots, x_n) \in \mathbb{K}^n$ si y solamente si para un orden monomial cualquiera, la base de Gröbner reducida del ideal es $\{1\}$.*

*3.4.4.3. El Problema de Pertenencia al Radical.* Esencialmente se trata de una reducción al Problema de Consistencia a través del "truco" de J.L. Rabinowitz. Insistimos en la idea:

LEMA 3.4.5 (J.L. Rabinowitz, 1930). *Sea $F := [f_1, \ldots, f_s] \in K[X_1, \ldots, X_n]^s$ una sucesión de polinomios. Sea $g \in K[X_1, \ldots, X_n]$ un polinomio adicional y sea $V(F) \subseteq \mathbb{K}^n$ el conjunto de ceros en $\mathbb{K}^n$ de los polinomios en la familia $F$. Sea $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ el ideal generado por los polinomios que aperecen en $F$. Son equivalentes :*

i) $g \in \sqrt{\mathfrak{a}}$,
ii) $g(x) = 0$, *para todo* $x \in V(F)$,
iii) *Dada una nueva variable $Y$ y dado el ideal*

$$\mathfrak{b} := \mathfrak{a} + (Yg - 1) \subseteq K[X_1, \ldots, X_n, Y],$$

*el ideal $\mathfrak{b}$ es el ideal trivial.*

El enunciado indica claramente cómo debe diseñarse el algoritmo que resuelva este problema.

*3.4.4.4. Resolución en el Caso Cero–dimensional.* Recuperamos aquí el análisis de los problemas de resolución de ecuaciones polinomiales en el caso cero–dimensional descritos en el Capítulo **??**.

LEMA 3.4.6. *Sea dado un sistema de ecuaciones polinomiales $F := [f_1, \ldots, f_s] \in K[X_1, \ldots, X_n]^s$ que genera un ideal $\mathfrak{a}$. Sea $V(F) \subseteq \mathbb{K}^n$ el conjunto de sus ceros comunes. Sea $G := \{g_1, \ldots, g_r\}$ una base de Gröbner de $\mathfrak{a}$ con respecto a ese ideal y sea*

$$EXP(\mathfrak{a}) := \left( \bigcup_{i=1}^{r} EXP(g_i) + \mathbb{N}^n \right).$$

*Entonces, el conjunto de los monomios :*

$$\Gamma := \{\underline{X}^{\underline{\gamma}} \ : \ \underline{\gamma} \in \mathbb{N}^n \setminus EXP(\mathfrak{a})\},$$

*es una base del cociente*

$$K[X_1, \ldots, X_n]/\mathfrak{a},$$

*como $K-$espacio vectorial. En particular, $V(F)$ es cero–dimensional si y solamente si $\mathbb{N}^n \setminus EXP(\mathfrak{a})$ es un conjunto finito.*

TEOREMA 3.4.7. *Con las condiciones del Lemma anterior, si $V(F)$ es cero–dimensional, para cada polinomio $g \in K[X_1, \ldots, X_n]$, la matriz del endomorfismo $\eta_g$ en la base monomial definida por la base de Gröbner de $\mathfrak{a}$ Tiene por columna $i-$ésima las coordenadas en la base $\Gamma$ de los polinomios*

$$NormF(g\underline{X}^{\underline{\gamma}}, G),$$

*donde $\underline{X}^{\underline{\gamma}}$ es el $i-$ésimo monomio de la base monomial $\Gamma$.*

El resto de los análisis puede hacerse mediante lo discutido en la sección precedente.

*3.4.4.5. Cálculo de la Calusura Zariski de la Proyección.* Retomemos el Teorema Fundamental de la Teor'ıa de la Eliinación, usando la noción de contracción de un ideal.

TEOREMA 3.4.8 (Teorema Fundamental de la Teoría de la Eliminación). *Sea* $\mathfrak{a}$ *un ideal de* $K[X_1, \ldots, X_n]$ *y sea* $V(\mathfrak{a}) \subseteq \mathbb{K}^n$ *el conjunto algebraico que define. Sea* $\mathfrak{a}^c$ *el ideal contracción de* $\mathfrak{a}$ *al anillo de polinomios*

$$\mathfrak{a}^c := \mathfrak{a} \cap K[X_1, \ldots, X_r].$$

*Sea* $\pi : \mathbb{K}^n \longrightarrow \mathbb{K}^r$ *la proyección dada mediante :*

$$\pi(x_1, \ldots, x_n) := (x_1, \ldots, x_r).$$

*Entonces, la clausura Zariski de* $\pi(V(\mathfrak{a}))$ *es, justamente,* $V(\mathfrak{a}^c)$*. Más aún, si* $\mathfrak{a}$ *es un ideal homogéneo, se tiene la igualdad* $\pi(V(\mathfrak{a})) = V(\mathfrak{a}^c)$*.*

TEOREMA 3.4.9. *Sea* $\mathfrak{a}$ *un ideal de* $K[X_1, \ldots, X_n]$ *y sea* $V(\mathfrak{a}) \subseteq \mathbb{K}^n$ *el conjunto algebraico que define. Sea* $G$ *una base de Gröbner de* $\mathfrak{a}$ *con respecto a un orden monomial tal que* $X_1 > X_2 > \cdots > X_n$*. Sea* $\mathfrak{a}^c$ *el ideal contracción*

$$\mathfrak{a}^c := \mathfrak{a} \cap K[X_{k+1}, \ldots, X_n].$$

*Entonces,* $G^c := G \cap K[X_{k+1}, \ldots, X_n]$ *es una base de Gröbner de* $\mathfrak{a}^c$ *para el orden monomial inducido en* $K[X_{k+1}, \ldots, X_n]$ *por el orden monomial de* $K[X_1, \ldots, X_n]$*.*

Los algoritmos para el cálculo de la clausura Zariski de la imagen de un conjunto algebraico por una aplicación polinomial se siguen de manera obvia, como el cálculo de la clausura Zariski de la proyección del grafo de una aplicación polinomial.

**3.4.5. Complejidad de las bases de Gröbner.** Por lo visto en las Secciones anteriores, las bases de Gröbner tienen dos propiedades esenciales que justifican su "popularidad" entre los programadores :

i) Las bases de Gröbner disponen de un algoritmo de construcción de sencillo aspecto (i.e. cualquier programador con un bajo nivel de conocimiento en Algebra puede tratar de programarlas).
ii) Las bases de Gröbner preservan mucho de la ideología subyacente al pensamiento de D. Hilbert, E. Noether y W. Krull (i.e. al Algebra Conmutativa) por lo que, fácilmente, se adaptan a sus aplicaciones en Geometría Algebraica.

Esta popularidad de las bases de Gröbner ha hecho que sean el método de eliminación más difundido en el universo de la enseñanza del Algebra Conmutativa y que permanezcan como un ingrediente de aspecto teórico muy reconocido. Sin embargo, pocos son los casos de aplicación donde verdaderamente se usan las bases de Gröbner. La razón hay que buscarla en problemas de eficacia o complejidad. En este sentido, un resultado de E. Mayr y A. Meyer de 1982[6] supuso un duro golpe que marca tanto el zénit como el declive de las bases de Gröbner por sus aplicaciones.
Ya se venía observando una cierta dificultad en la ejecución de los algoritmos basados en bases de Gröbner una vez implementados : típicamente acababan consumiendo toda la memoria del ordenador y pocas veces daban respuestas a los problemas planteados. Este fenómeno se verá fácilmente en la práctica sobre bases de Gröbner propuesta.
Dejaremos simplemente constancia de los resultados principales de Mayr y Meyer
El primer dato relevante, es la construcción de un famoso ejemplo de sistema de Thue para semi–grupos abelianos que permite deducir lo siguiente con respecto al Problema de División :

[6]E. Mayr and A. Meyer, *The complexity of the word problem for commutative semigroups.* Advances in Math. **46** (1982), 305–329. Véase también el trabajo posterior de E. Mayr, *Membership in Polynomial Ideals over* $\mathbb{Q}$ *Is Exponential Space Complete.* In Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (STACS'89) (1989), 400–406.

TEOREMA 3.4.10. *Dados $k, d \in \mathbb{N}, d \geq 5, n := 10k$, existen $P_1, \ldots, P_{n+1}$ polinomios en $\mathbb{Z}[X_1, \ldots, X_n]$ tales que $deg(P_i) \leq d$, $X_1 - X_n$ está en el ideal $(P_1, \ldots, P_{n+1})$ y tales que si*

$$X_1 - X_n := \sum_{i=1}^{n+1} g_i P_i,$$

*entonces*

$$max\{deg(g_i)\} \geq (d-2)^{2^{k-1}}.$$

*En particular, cualquier algoritmo que resuelva el problema de División requiere tiempo doblemente exponencial en el número de variables.*

Sobre la base de este ejemplo se hicieron varios desarrollos posteriores. Por ejemplo, el siguiente es un resultado de E. Mayr :

TEOREMA 3.4.11. *El Problema de Palabra de Semi–grupos conmutativos es equivalente al Problema de Pertenencia a un ideal y ambos son* **EXPSPACE***–completos.*
*En otras palabras, el espacio necesario para calcular una base de Gröbner es expo–polinomial y esta cota no se puede mejorar.*

Varios autores trabajaron aún más las reflexiones de A. Meyer y E. Mayr. Entre ellos cabe citar a D. Bayer y M. Stillman[7], M. Demazure[8] y C.K. Yap[9]
El trabajo de C.K. Yap nos permitirá cconcluir el siguiente resultado :

TEOREMA 3.4.12. *Existen algoritmos que calculan bases de Gröbner en tiempo doblemente exponencial en el número de variables. Pero también existen ejemplos de ideales en los que toda base de Gröbner contiene al menos un polinomio de grado doblemente exponencial en el número de variables. Por lo tanto, la cota de tiempo no puede mejorarse.*

Este defecto notable hace de las bases de Gröbner un procedimiento de casi nula utilidad. Si acaso, en el caso cero–dimensional, usando algoritmos alternativos (véase la propuesta de D. Lazard en [10]) se podrían obtener bases de Gröbner en tiempo $d^{n^2}$. Este es el algoritmo subyacente a los trabajos de programación de J.C. Faugére conocidos como **GB** y **FGB**.
Por último debe señalarse que, a pesar de los graves inconvenientes de la utilización de bases de Gröbner, quedan muchos investigadores de la comunidad científica internacional apegados al sueño de comprenderlas e investigando por ver si consiguen resolver su dificultades. De otro lado, la sencillez de la noción y de los algoritmos subyacentes hace que exista un apego a la noción y que siga programándose en las librerías de software como Maple, MAGMA, MACALAY o Cocoa.

---

[7] D. Bayer, M. Stillman, *On the complexity of computing syzygies.* J. of Symb. Comput. **6** (1988), 135–147.

[8] M. Demazure, *Le monoïde de Mayr y Meyer.* Notes informelles de Calcul Formel, École Polytechnique ,1984.

[9] Chee K. Yap, *A New Lower Bound Construction for Commutative Thue Systems with Applications.* J. of Symb. Comput. **12** (1991) 1–27.

[10] D. Lazard, *Résolution des systèmes d'équations algébriques*, Theor. Comp. Sci. **15** (1981), 77–110.

Capítulo 4

# Resolución algebro-geométrica en el caso cero-dimensional

## 4.1. Unos pocos Ejemplos para Reflexionar

Retomamos la resolución discutida en el Capítulo precedente con varios ejemplos. Todos ellos son dados a partir de ecuaciones cuadráticas.

Ejemplo 4.1.1 (**La multiplicidad aumenta la dimensión)**. Consideremos el sistema de ecuaciones definido por las ecuaciones

$$X_1^2 = 0, \ldots, X_n^2 = 0.$$

El ideal que generan esos polinomios sería el ideal $\mathfrak{a} := (X_1^2, \ldots, X_n^2)$ y la dimensión del anillo cociente es $2^n$:

$$\mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{a}.$$

La base son las clases módulo $\mathfrak{a}$ de los monomios siguientes:

$$\beta := \{X_1^{\varepsilon_1} \cdots X_n^{\varepsilon_n} + \mathfrak{a} \ : \ \underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n\}.$$

Estgo hace que, de momento, las matrices involucradas para tratar preguntas sobre una nueva ecuación $g$ (es decir, las matrices $M_g$) tengan un tamaño $2^n \times 2^n$. Sin embargo, es obvio (en este caso) que el sistema sólo tiene una solución. Incluso tenemos una forma de expresarlo a través del radical del ideal. Es claro que

$$\sqrt{\mathfrak{a}} = (X_1, \ldots, X_n),$$

y

$$\mathbb{Q}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}} = \mathbb{Q},$$

y una base como $\mathbb{Q}-$espacio vectorial sería

$$\beta := \{1 + \sqrt{\mathfrak{a}}\}.$$

Es cierto que, trabajando en este espacio perdemos la capacidad de respuesta a algunas de las preguntas naturales: no podemos responder al Problema de Pertenencia al Ideal $\mathfrak{a}$ porque le hemos perdido por el camino. Pero el Problema de Pertenencia al Ideal es propio del deseo de manejar el ideal aundo, en realidad, el realidad ligado a la Geometría no es el ideal $\mathfrak{a}$ sino el ideal $\sqrt{\mathfrak{a}}$ y, además, resulta que salidmos ganando dado que la dimensión involucrada, al menos en este caso, es más pequeña.

Ejemplo 4.1.2 (**Los Problemas NP-completos son instancias particulares)**. Esta es la razón que muestra la relevancia de estudiar el caso cero-dimensional y el problema de consistencia que surge al añadir una nueva ecuación. Todos los problemas **NP**–completos son instancias particulares de este mismo problema. Comencemos considerando una variante del *Knapsack* del modo siguiente. Consideremos el sistema de ecuaciones polinomiales siguiente

$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0.$$

Y el ideal $\mathfrak{a} := (X_1^2 - X_1, \ldots, X_n^2 - X_n)$ en $\mathbb{Q}[X_1, \ldots, X_n]$. Este ideal es radical, es decir

$$\sqrt{\mathfrak{a}} = \mathfrak{a} = (X_1^2 - X_1, \ldots, X_n^2 - X_n).$$

La base como $\mathbb{Q}-$espacio vectorial del cociente

$$R_{\text{red}} = R = \mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{a} = \mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{a},$$

es la misma que en el ejemplo precedente:

$$\beta := \{X_1^{\varepsilon_1} \cdots X_n^{\varepsilon_n} + \mathfrak{a} \ : \ \underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n\}.$$

El anillo cociente reducido tiene, por tanto, dimensión $2^n$. Lo que cambian son las matrices de los tensores. En el caso precedente, las matrices $M_{X_i}$ eran nilpotentes

$$M_{X_i}^2 = 0,$$

con lo que su polinomio mínimo (el de todas ellas) es $T^2$ y su forma canónica de Jordan es una suma diagonal de $2^{n-1}$ cajas de Jordan $2 \times 2$ del tipo siguiente:

$$J(0,2) := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

En el caso actual, las matrices de los tensores $M_{X_i}$ tienen como polinomio mínimo al polinomio $T^2 - T = T(T-1)$. Son, por tanto matrices diagonalizables y su forma canónica de Jordan es una suma diagonal de $2^{n-1}$ cajas $2 \times 2$ del tipo siguiente:

$$J := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Lo que obviamente cambia es la posición de estas cajas. Esta diferencia entre los tensores muestra la diferencia natural entre este ejemplo y el precedente.
Consideremos ahora una nueva ecuación. Por ejemplo, una ecuación lineal con coeficientes en $\mathbb{Z}$:

$$g := m_1 X_1 + \cdots + m_n X_n - k.$$

Nos preguntamos sobre el problema de consistencia de $g$ sobre el conjunto de soluciones $V_{\mathbb{C}}(\mathfrak{a})$. En este ejemplo jugamos con ventaja, dado que conocemos ese conjunto de soluciones. Esto no suceredr'an en general y la dificultad estará justamente en *determinarlos sin poder escribirlos* (noción que clarificaremos más adelante). En este sencillo caso, sabemos que

$$V_{\mathbb{C}}(\mathfrak{a}) = \{0,1\}^n \subseteq \mathbb{C}^n.$$

El Teorema Chino de los restos nos garantizará que la matriz $M_g$ es diagonalizable (cuando se considera sobre $(\mathbb{C} \otimes_{\mathbb{Q}} R)_{\text{red}}$ y que sus valores propios son, precisamente los valores $g(\zeta)$ con $\zeta \in V_{\mathbb{C}}(\mathfrak{a})$. Es decir, $M_g$ en el caso reducido es semejante a una matriz de la forma:

$$M_g \approx \begin{pmatrix} g(\zeta_1) & 0 & 0 & \cdots & 0 \\ 0 & g(\zeta_2) & 0 & \cdots & 0 \\ 0 & 0 & g(\zeta_3) & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & g(\zeta_{\mathscr{D}}) \end{pmatrix},$$

donde $\approx$ indica semejanza de matrices,

$$V_{\mathbb{C}}(\mathfrak{a}) := \{\zeta_1, \ldots, \zeta_{\mathscr{D}}\},$$

y $\mathscr{D} = deg(V_{\mathbb{C}}(\mathfrak{a}))$. Por tanto, en el caso actual, podemos describir fácilmente tanto el polinomio característico como el determinante de nuestra matrix $M_g$ del modo siguiente:

$$\chi_g(T) := \prod_{\underline{\varepsilon} \in \{0,1\}^n} \left(T - (m_1\varepsilon_1 + \cdots + m_n\varepsilon_n - k)\right).$$

Por su parte, del determinante viene dao por:

$$\det(M_g) := \prod_{\zeta \in V_{\mathbb{C}}(\mathfrak{a})} g(\zeta) = \prod_{\underline{\varepsilon} \in \{0,1\}^n} \left(m_1\varepsilon_1 + \cdots + m_n\varepsilon_n - k\right).$$

En particular, tenemos la equivalencia entre los tres casos siguientes:

i) *Problema de Consistencia:*

$$\exists \zeta \in \mathbb{C}^n, \ \ \zeta \in V_{\mathbb{C}}(\mathfrak{a}) \wedge g(\zeta) = 0.$$

ii) $\det(M_g) = 0$
iii) *Knapsack:*

$$\exists S \subseteq \{1, \ldots, n\},\ \sum_{i \in S} m_i = k.$$

Esto demuestra que el Knapsack es una instancia particular de un Problema de Consistencia.

Podemos ver otros ejemplos, como el problema de 3−Colorabilidad. Recordemos que se trata de

Problema 8 (**3COLOR**). *Se trata del lenguaje formado por los grafos no orientados $G := (V, E)$ que son tres-coloreables, esto es, tales que se pueden asignar colores (etiquetas $\{1, 2, 3\}$) de tal modo que dos vértices vecinos no posean el mismo color.*

Este problema es equivalente a la existencia de solución de un sistema de ecuaciones polinomiales dado del modo siguiente

$$X_1^3 - 1 = 0, \ldots, X_n^3 - 1 = 0,$$

que definen la variedad cero-dimensional asociada a los tres colores $\{1, \omega, \omega^2\}$ que son las tres raices cúbicas de la unidad. El ideal $\mathfrak{a}$ pasa a ser

$$\mathfrak{a} := (X_1^2 - 1, \ldots, X_n^2 - 1).$$

En este caso, el ideal $\mathfrak{a}$ vuelve a ser radical y

$$V_{\mathbb{C}}(\mathfrak{a}) := \{1, \omega, \omega^2\}^n,$$

El grafo $(V, E)$ es 3-coloreable si y solamente si se da el siguiente *Problema de Consistencia*:

$$\exists \zeta \in \mathbb{C}^n,\ \zeta \in V_{\mathbb{C}}(\mathfrak{a}) \wedge \left[X_i^2 + X_i X_j + X_j^2 = 0, \forall (i, j) \in E\right].$$

Aquí ya no sólo hay una ecuación adicional sino varias y habría que buscar una estretagia para añadir una sola $g$ (asociada al grafo) que nos permita discutir el problema como en el caso del Knapsack o bien generar un algoritmo incremental añadiendo una a una cada una de las ecuaciones que aparecen asociadas a las aristas $E$ y que siguen dando ideales cero-dimensionales.
Una manera de añadir una sola ecuación consiste en añadir un nuevo conjunto de variables $\{T_{i,j} \ :\ (i, j) \in E\}$. Y añadimos esas variables al cuerpo de coeficientes de modo que tenemos un nuevo cuerpo

$$L := K(T_{i,j} \ :\ (i, j) \in E).$$

Y miramos una clausura algebraica Ł de $L$. Consideramos la extensión $\mathfrak{a}^e$ del ideal $\mathfrak{a}$ al anillo $L[X_1, \ldots, X_n]$. Sigue siendo un ideal radical, seguimos estando en una situación cero-dimensional y podemos considerar un nuevo polinomio $g \in L[X_1, \ldots, X_n]$ dado mediante:

$$g_= \sum_{(i,j) \in E} T_{i,j}(X_i^2 + X_i X_j + X_j^2).$$

La matriz $M_g$ sobre $L \otimes_K R_{\text{red}} := L[X_1, \ldots, X_n]/\mathfrak{a}^e$, con coordenadas en $L$, se obtiene de manera simple a partir de las matrices $M_{X_1}, \ldots, M_{X_n}$ originales (es decir en $K[X_1, \ldots, X_n]/\mathfrak{a}$ del modo siguiente:

$$M_g := \sum_{(i,j) \in E} T_{i,j} \left(M_{X_i}^2 + M_{X_i} M_{X_j} + M_{X_j}^2\right).$$

Ahora podemos calcular el determinante de esta matriz (que es un polinomio en $K[T_{i,j} : (i,j) \in E]$:

$$D_G(T_{i,j}) := \det(M_g) = \det\left(\sum_{(i,j)\in E} T_{i,j}\left(M_{X_i}^2 + M_{X_i}M_{X_j} + M_{X_j}^2\right)\right) \in K[T_{i,j} \ : \ (i,j) \in E].$$

Ahora se tiene la siguiente equivalencia:

i) El grafo $G := (V, E)$ es 3-colorable.
ii) El polinomio $D_G(T_{i,j})$ es idénticamente cero.

Nótese que, en este caso, podemos utilizar los tests de nulidad de polinomios (descritos en el Capítulo precedente) para decidir la $3COLOR$ y que sólo hemos añadido una ecuación aunque, aparentemente, hemos añadido muchas variables.

Como última reflexión sobre los problemas **NP**-completos debemos decir que no solamente se tratan con coeficientes en $\mathbb{Q}$ y soluciones en $\mathbb{C}$. Podríamos planteranos otros cuerpos como, por ejemplo, los cuerpos finitos. De hecho, podemos pensar en el cuerpo $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ Sea $\mathbb{K}_2$ la clausura algebraica de $\mathbb{F}_2$. Para ello, consideremos, de nuevo, el sistema de ecuaciones:

$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0.$$

Y el ideal $\mathfrak{a} := (X_1^2 - X_1, \ldots, X_n^2 - X_n)$ en $\mathbb{F}_2[X_1, \ldots, X_n]$. Este ideal es radical, es decir

$$\sqrt{\mathfrak{a}} = \mathfrak{a} = (X_1^2 - X_1, \ldots, X_n^2 - X_n).$$

La base como $\mathbb{F}_2-$espacio vectorial del cociente

$$R_{\text{red}} = R = \mathbb{F}_2[X_1, \ldots, X_n]/\mathfrak{a} = \mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{a},$$

es la misma que en el ejemplo precedente:

$$\beta := \{X_1^{\varepsilon_1} \cdots X_n^{\varepsilon_n} + \mathfrak{a} \ : \ \underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n\}.$$

El anillo cociente reducido tiene, por tanto, dimensión $2^n$. El conjunto de soluciones vuelve a ser el mismo:

$$V_{\mathbb{K}_2}(\mathfrak{a}) = \{0,1\}^n \subseteq \mathbb{K}_2^n.$$

Ahora consideremos el problema 3SAT del que sabemos que es un problema **NP**-completo. Una instancia del problema tiene la forma

$$\Phi(X_1, \ldots, X_n) := \bigwedge_{i=1}^{2} C_i(X_{i_1}, X_{i_2}, X_{i_3}),$$

siendo $C_i$ una $3-$cláusula. Es obvio que toda $3-$clásula se puede transformar en un polinomio en tres variables de grado a lo más 3 $p_i(X_{i_1}, X_{i_2}, X_{i_3})$ de tal modo que:

$$C_i(\varepsilon_{i_1}, \varepsilon_{i_2}, \varepsilon_{i_3}) = 1 \Longleftrightarrow p_i(\varepsilon_{i_1}, \varepsilon_{i_2}, \varepsilon_{i_3}) = 1,$$

donde la primera identidad es una identidad a valores booleanos y la segunda indetidad es una igualdad aritmética sobre el cuerpo $\mathbb{F}_2$ o sobre su clausura algebraica $\mathbb{K}_2$. Del mismo modo, podemos considerar $\Phi(X_1, \ldots, X_n)$ que es una fórmula booleana en forma normal conjuntiva y podemos considerar el polinomio:

$$g(X_1, \ldots, X_n) := \prod_{i=1}^{2} \left(p_i(X_{i_1}, X_{i_2}, X_{i_3}) - 1\right).$$

Se tiene la siguiente equivaolencia:

i) *Problema de Consistencia:*

$$\exists \zeta \in \mathbb{K}_2^n, \ \zeta \in V_{\mathbb{K}_2}(\mathfrak{a}) \wedge g(\zeta) = 0.$$

ii) $\det(M_g) = 0$.

iii) *3SAT:*

$$\exists \underline{\varepsilon} \in \{V, F\}^n,\ \Phi(\varepsilon_1, \ldots, \varepsilon_n) = V.$$

Ejemplo 4.1.3 (**Pueden parecer NP-completos y no serlo)**. Retomamos el mismo ejemplo de base del Ejemplo precdente. Consideremos el sistema de ecuaciones polinomiales siguiente

$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0.$$

Y el ideal $\mathfrak{a} := (X_1^2 - X_1, \ldots, X_n^2 - X_n)$ en $\mathbb{Q}[X_1, \ldots, X_n]$. Este ideal es radical, es decir

$$\sqrt{\mathfrak{a}} = \mathfrak{a} = (X_1^2 - X_1, \ldots, X_n^2 - X_n).$$

La base como $\mathbb{Q}-$espacio vectorial del cociente

$$R_{\text{red}} = R = \mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{a} = \mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{a},$$

es la misma que en el ejemplo precedente:

$$\beta := \{X_1^{\varepsilon_1} \cdots X_n^{\varepsilon_n} + \mathfrak{a} \ :\ \underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0, 1\}^n\}.$$

El anillo cociente reducido tiene, por tanto, dimensión $2^n$. Y consideramos una ecuación adicional como la siguiente:

$$g := 2^{n-1} X_1 + \cdots + 2X_{n-1} + X_n - k.$$

Nótese que es muy similar al Knapsack anterior, pero aquí se tiene la equivalencia:

i) *Problema de Consistencia:*

$$\exists \zeta \in \mathbb{C}^n,\ \ \zeta \in V_{\mathbb{C}}(\mathfrak{a}) \wedge g(\zeta) = 0.$$

ii) $\det(M_g) = 0$

iii) La expansión binaria de $k$ tiene longitud $\leq n$.

Obviamente, la afirmación iii) se resuelve simplemente mirando la expansión binaria de $k$ y el uso de las matrices de dimensión $2^n \times 2^n$ parece excesivo. Sin embargo, no se dispone de un mecanismo eficiente para discernir entre un caso como éste y los casos del ejemplo anterior. Esta es una dificultad que está fuertemente ligada al hecho de no concer "a priori" las solciones de las ecuaciones y que, a posteriori, tenemos la dificultad de decidir si hemos eprdido el tiempo trabajando más de lo necesario. Incluso el determinar si hemos perdido el tiempo no parece algo obvio.

Ejemplo 4.1.4 (**Los aspectos diofánticos también juegan)**. El siguiente ejemplo muestra que los aspectos diofánticos, en especial el crecimiento de las alturas de los objetos involucrados en la resolución (y, por tanto, su talla bit) también juegan un papel en el proceso de resolución. Tomenos el siguiente ejemplo de sistema de ecuaciones:

$$X_1^2 - h = 0, X_2 - X_1^2 = 0, X_3 - X_2^2 = 0, \ldots, X_n - X_{n-1}^2 = 0.$$

En este caso, el ideal es el dado por $\mathfrak{a} := (X_1^2 - h, X_2 - X_1^2, \ldots, X_n - X_{n-1}^2)$ es un ideal radical en $\mathbb{Q}[X_1, \ldots, X_n]$. La dimensión del cociente es fácil de determinar:

$$\dim_{\mathbb{Q}} \left(\mathbb{Q}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}\right) = 1,$$

y la base es también sencilla:

$$\beta := \{1 + \mathfrak{a}\}.$$

Además, hay una única solución:

$$V_{\mathbb{C}}(\mathfrak{a}) := \{(h, h^2, h^4, \ldots, h^{2^{n-1}})\}.$$

La dificultad aquí es el orden de grandeza (o pequeñez) de esta única solución (lo que, en términos de Teoría de Números se llama altura). Así, por ejemplo, el único valor propio de la matriz $M_g$ (que es diagobalizable y $1 \times 1$ tiene la forma:

$$g(h, h^2, h^4, \ldots, h^{2^{n-1}}).$$

Determinar el Problema de Consistencia de $g$ sobre $\mathfrak{a}$ consiste en hallar el valor anterior. Obsérvense los casos siguientes:

i) Tomando $h = 1$, es fácil verificar si $g(1, 1, \ldots, 1) = 0$ siempre que $g$ sea un polinomio "sencillo".
ii) Tomando $h = 2$, verificar si
$$f(2, 2^2, \ldots, 2^{2^{n-1}}) = 0,$$
nos obliga a trabajar con números enteros de talla exponencial en el número de variables.
iii) Tomando $h = 1/2$, serificar si
$$f(\frac{1}{2}, \frac{1}{2^2}, \ldots, \frac{1}{2^{2^{n-1}}}) = 0,$$
nos obliga a trabajar con números racionales de talle exponencial.

De una parte, los tests de nulidad de números enteros descritos en el Capítulo precedente podrían usarse en situaciones como esta. Pero, de nuevo, no sabemos si estamos o no en una situación así hasta que no hemos resuelto y, para entonces, ya habríamos dedicado un tiempo excesivo y no queda claro que podamos siempre determinar que estamos en una situación así. Alguien podría argumentar que tarbajando en base 2 permite trabajar confortablemente con $2^{2^{n-1}}$, pero nótese que $h$ podría ser 3 y entonces nos enfrentamos a $3^{2^{n-1}}$ cuya expensión binaria no es tan simple como la de $2^{2^{n-1}}$ y, como antes, no sabemos "a priori" si vamos a tener que usar base 2 o base 3.

Ejemplo 4.1.5 (**El Conteo de las soluciones)**. Se trata de los problemas del tipo $\sharp\mathbf{P}$ introducidos por L.G. Valiant[1] en su tgrabajo de 1979. Se trata, esencialmente de contar soluciones. En nuestro caso, el problema podría diseñarse del modo siguiente: Dado un ideal $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ cero-dimensional y dado un polinomio adicional $g \in K[X_1, \ldots, X_n]$, hallar el número de soluciones de $V_{\mathbb{K}}(\mathfrak{a})$ que están en la hipersuperficie $V_{\mathbb{K}}(g)$. Es decir, hallar el número:
$$\sharp\{\zeta \in \mathbb{K}^n \ : \ \zeta \in V_{\mathbb{K}}(\mathfrak{a}) \wedge g(\zeta) = 0\}.$$
Claramente tenemos que $\mathbf{NP} \subseteq \sharp\mathbf{P}$, pero nadie sabe si ambas clases de complejidad coinciden. En el caso de la resolución simbólico-geométrica, el cáulo del número de soluciones se enfrenta a la dificultad de manejar las mutiplicidades que ocultan el verdadero valor del número. Por ejemplo, si consideramos las ecuaciones
$$X_1^2 = 0, \ldots, X_n^2 = 0,$$
y consideramos el ideal $\mathfrak{a}$ que generan y la matriz $M_g$ en alguna base de $R$, s
'olo tendremos dos posibles respuestas: o bien, $M_g = 0$ y en ese caso respondemos $2^n$ o bien $M_g \neq 0$ y, en ese caso, la matriz $M_g$ tiene rango $2^n$ y respondemos 0 a la pregunta de Valiant.
Esto se resuelve directamente con el uso del álgebra reducida en todos los casos. Ya hemos dicho antes que si tomamos $R_{\text{red}} := K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}$ y $(\mathbb{K} \otimes_K R)_{\text{red}}$ la matriz $M_g$ es diagonalizable sobre $\mathbb{K}$ y toma la forma:
$$M_g \approx \begin{pmatrix} g(\zeta_1) & 0 & 0 & \cdots & 0 \\ 0 & g(\zeta_2) & 0 & \cdots & 0 \\ 0 & 0 & g(\zeta_3) & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & g(\zeta_{\mathscr{D}}) \end{pmatrix},$$

[1] L.G. Valiant, *The Complexity of Computing the Permanent.* Theoretical Computer Science **8** (1979), 189201.

donde $\approx$ indica semejanza de matrices,

$$V_{\mathbb{C}}(\mathfrak{a}) := \{\zeta_1, \ldots, \zeta_{\mathscr{D}}\},$$

Claramente se obtiene la equivakencia entre las afirmaciones siguientes:

i) *Problema de Conteo de soluciones:* Hallar $M \in \mathbb{N}$, con $0 \leq M \leq \mathscr{D}$, tal que:

$$M := \sharp\{\zeta \in \mathbb{K}^n \ : \ \zeta \in V_{\mathbb{K}}(\mathfrak{a}) \wedge g(\zeta) = 0\}.$$

ii) Hallar el rango $R$ de $M_g$ y se tiene:

$$M := \mathscr{D} - R.$$

Ejemplo 4.1.6 (**La dificultad del cálculo del radical con bases de Gröbner)**. Uno pensaría directamente en usar técnicas de reescritura, como las bases de Gröbner, para trabajar directamente con los radicales de los ideales en lugar de los ideales "per se". Un trabajo clásico de P. Gianni, B. Trager y G. Zacharias [2] permite calcular las bases de Gröbner del radical de un ideal. De nuevo la complejidad se va a doblemente exponencial, especialmente por la presencia de componentes inmersas, y surge la dificultad de usar directamente este tipo de algoritmos.

## 4.2. Solución "à la Macaulay" intrínseca

Comencemos remozando un poco las notaciones. Así tenemos un cuerpo $K$ un cuerpo algebraicamente $\mathbb{K}$ que le contiene, un ideal $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ (finitamente generado por estar en el caso noetheriano), y $\sqrt{\mathfrak{a}}$ su radical y $\sqrt{\mathfrak{a}^e}$ el radical de su extensión a $\mathbb{K}[X_1, \ldots, X_n]$.

Definición 16 (**Funciones Polinomiales)**. *Sea $V = V_{\mathbb{K}}(\mathfrak{a}) \subseteq \mathbb{K}^n$ la variedad algebraica definida por los polinomios en $\mathfrak{a}$. Llamaremos función polinomial (o regular) sobre $V$ a toda aplicación $f : V \longrightarrow \mathbb{K}$ tal que existe un polinomio $p \in K[X_1, \ldots, X_n]$ tal que:*

$$p \mid_V = f.$$

Proposición 4.2.1. *El conjunto de las funciones polinomiales forma un anillo con las operaciones suma y producto de funciones. Dicho anillo se denotará mediante $K[V]$. Además, se verifica que, con las notaciones anteriores, se tiene:*

$$K[V] := K[X_1, \ldots, X_n]/I_K(V) = K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}.$$

*Denotaremos mediante $\mathbb{K}[V]$ al anillo de las funciones polinomiales con coeficientes en $\mathbb{K}$ que se anulan sobre $V$ y se tiene también:*

$$\mathbb{K}[V] := \mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}^e}.$$

Demostración. Es consecuencia inmediata del uso del Nullstellensatz. □

Definición 17 (**Aplicaciones Polinomiales)**. *Sean $V \subseteq \mathbb{K}^n$ y $W \subseteq \mathbb{K}^m$ dos conjuntos algebraicos definibles sobre $K$. Una aplicación polinomial $K-$definible es una aplicación*

$$f : V \longrightarrow W,$$

*tal que existen $f_1, \ldots, f_m \in K[V]$ tales que:*

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

*Se llaman isomorfismos regulares (o se dice que $V$ y $W$ son birregularmente isomorfos sobre $K$) si existe una aplicación polinomial $f : V \longrightarrow W$ biyectiva tal que su inversa $f^{-1} : W \longrightarrow V$ es también polinomial.*

[2] Véase el trabajo en tiempo doblemente exponencial debido a P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals.* J. Symbolic Comput. **6** (1988), 149–167.

Algunas propiedades sencillas de verificar son las que se resumen en el siguiente enunciado:

PROPOSICIÓN 4.2.2 (**Propiedades Básicas de las aplicaciones polinomiales (y I)**). *Con las notaciones, anteriores, sean $V \subseteq \mathbb{K}^n$ y $W \subseteq \mathbb{K}^m$ dos variedades algebraica y $f : V \longrightarrow W$, una aplicación polinomial $K-$ definible entre ellas. Entonces podemos definir un morfismo de $K-$álgebras (i.e. morfismo de anillos que es la identidad sobre $K$):*

$$\begin{array}{rccc} f^* : & K[W] & \longrightarrow & K[V] \\ & h & \longmapsto & f^*(h) := h \circ f. \end{array}$$

*Entonces, se verifica $(f \circ g)^* = g^* \circ f^*$, $(Id_V)^* = Id_{K[V]}$. En particular, si $f$ es un isomorfismo birregular, entonces $K[V]$ y $K[W]$ son isomorfos como $K-$álgebras.*

DEMOSTRACIÓN. Un pesado ejercicio de verificación. □

PROPOSICIÓN 4.2.3 (**Propiedades Básicas de las aplicaciones polinomiales (y II)**). *Con las notaciones, anteriores, sean $V \subseteq \mathbb{K}^n$ y $W \subseteq \mathbb{K}^m$ dos variedades algebraica y sea*

$$\varphi : K[W] \longrightarrow K[V],$$

*un morfismo de anillos de tal modo que*

$$\varphi \mid_K = Id_K.$$

*Definamos las aplicación del modo siguiente. Para cada $i$, $1 \leq j \leq m$, consideremos la función polinomial*

$$f_i := \varphi(Y_i + I_K(W)) \in K[V].$$

*Definamos la aplicación polinomial siguiente:*

$$\begin{array}{rccc} \varphi_* : & V & \longrightarrow & W \\ & x & \longmapsto & (f_1(x), \ldots, f_m(x)). \end{array}$$

*Entonces, la aplicación polinomial $\varphi_*$ está bien definida y verifica $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$, $(Id_{K[V]})^* = Id_V$. En particular, si $\varphi$ es un isomorfismo birregular, entonces $V$ y $W$ son birregularmente isomorfos sobre $K$.*

DEMOSTRACIÓN. Un pesado ejercicio de verificación. □

OBSERVACIÓN 4.2.4. En términos clásicos diríamos que las categorías de variedades $K-$definibles y las $K-$álgebras finitamente generadas y reducidas son cateforías naturalmente equivalentes. Pero dejaremos ese lenguaje por el momento.

Un par de observaciones elementales serían las siguientes.

DEFINICIÓN 18. *Una variedad algebraica $K-$definible $V \subseteq \mathbb{K}^n$ se denomina irreducible si no se puede escribir como unión de dos variedades algebraicas $K-$definibles propias y distintas entre sí. En otro caso, se dice que es reducible.*

PROPOSICIÓN 4.2.5. *Toda variedad algebraica $K-$definible es descomponible como unión finita de irreducibles.*

DEMOSTRACIÓN. Es una consecuencia (casi inmediata) de la noetherianidad de $K[X_1, \ldots, X_n]$. Pero la omtimos en este curso. □

PROPOSICIÓN 4.2.6. *Las siguientes propiedades son equivalentes para una variedad algebraica $K-$definible $V \subseteq \mathbb{K}^n$:*

i) *$V$ es irreducible.*
ii) *El ideal $I_K(V)$ es primo, es decir, satisface:*

$$\forall f, g \in K[X_1, \ldots, X_n],\ fg \in I_K(V) \Longrightarrow [f \in I_K(V)] \vee [g \in I_K(V)].$$

iii) *La $K-$álgebra $K[V]$ es un dominio de integridad (es decir, no posee divisores de cero no nulos).*

DEMOSTRACIÓN. Es un sencillo ejercicio, muy recomendable. □

DEFINICIÓN 19 (**Topología de Zariski)**. *Dado un cuerpo $K$ y un cuerpo algebraicamente cerrado $\mathbb{K}$ que le contiene. Llamamos topología de Zariski en $\mathbb{K}^n$ de $K-$definibles a la única toplogía cuyo conjunto de cerrados es el siguiente:*

$$\mathcal{F} := \{V \subseteq \mathbb{K}^n \ : \ \exists \mathfrak{a} \subseteq K[X_1, \ldots, X_n], \text{ ideal}, V = V_{\mathbb{K}}(\mathfrak{a})\}.$$

*Se llama clausura Zariski de $F$ al menor cerrado Zariski $K-$definible que contiene al subconjunto $F$ de $\mathbb{K}^n$ (i.e. el menor conjunto algebraico $K-$definible que contiene a $F$). Lo denotaremos mediante $\overline{F}^Z$.*

DEFINICIÓN 20 (**Aplicaciones dominantes)**. *Una aplicación polinomial $K-$definible $f : V \longrightarrow W$ se dice dominante (o de rango denso) si $\overline{f(V)}^Z = W$.*

PROPOSICIÓN 4.2.7. *Una aplicación polinomial $K-$definible $f : V \longrightarrow W$ es dominante si y solamente si el morfismo de $K-$álgebras asociado $f^* : K[W] \longrightarrow K[V]$ es inyectivo.*

DEMOSTRACIÓN. Mero ejericio. □

PROPOSICIÓN 4.2.8. *Dada aplicación polinomial $K-$definible $f : V \longrightarrow W$ dominante. Si $V$ es irreducible, entonces $W$ es irreducible.*

DEMOSTRACIÓN. Baste con observar que si $K[V]$ es dominio de integridad, también lo son sus subanillos y, en particular $f^*(K[W])$ que es una $K-$álgebra isomorfa a $K[W]$ porque $f^*$ es inyectiva. □

**4.2.1. Solución "à la Macaulay" intrínseca en el caso cero-dimensional.** Supongamos ahora que $K$ es cuerpo, $\mathbb{K}$ es algebraicamente cerrado que contiene a $K$. Consideremos un sistema de ecuaciones polinomiales:

$$\left\{ \begin{array}{rcl} f_1(X_1, \ldots, X_n) & = & 0, \\ f_2(X_1, \ldots, X_n) & = & 0, \\ & \vdots & \\ f_s(X_1, \ldots, X_n) & = & 0, \end{array} \right. \tag{4.2.1}$$

donde $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$. Sea $\mathfrak{a}$ e ideal en $K[X_1, \ldots, X_n]$ generado por $f_1, \ldots, f_s$ y $V = V_{\mathbb{K}}(\mathfrak{a}) \subseteq \mathbb{K}^n$ la variedad que define. Supongamos que $\mathfrak{a}$ es cero-dimensional (o, equivalentemente, que $V$ es un conjunto finito).

DEFINICIÓN 21 (**Solución Intrínseca "à la Macaulay")**. *Con las notaciones anteriores, una solución al sistema de ecuaciones polinomiales (4.2.1) consiste en dar una descripción "à la Macaulay" de $K[V]$, esto es,*

i) *Una base $\beta$ de $K[V]$ como $K-$espacio vectorial, tal que $1 \in \beta$, donde $1$ es la función polinomial unidad.*
ii) *Las matrices de los tensores $M_{X_1}, \ldots, M_{X_n}$ en esa base.*

OBSERVACIÓN 4.2.9 (**De las bases de Gröbner a la resolución à la Macaulay intrínseca)**. Supongamos que tenemos un ideal $\mathfrak{a}$ en $K[X_1, \ldots, X_n]$ y tenemos una base de Gröbner reducida del radical $\sqrt{\mathfrak{a}}$ dada por una colección de polinomios:

$$G := \{f_1, \ldots, f_s\}.$$

Supongamos que tenemos un orden $\leq$ en $\mathbb{N}^n$ y consideremos los términos:

$$a_i X_1^{\mu_1} \cdots X_n^{\mu_n} = LT(f_i).$$

Consideremos el conjunto de todos los exponentes de todos los elementos del ideal $\sqrt{\mathfrak{a}}$, es decir:

$$Exp(\sqrt{\mathfrak{a}}) := \{\mu \in \mathbb{N}^n \ : \ \exists g \in \sqrt{\mathfrak{a}}, y \exists a \in K, a \neq 0, LT(g) = aX^\mu\}.$$

Entonces, la propiedad clave con las bases de Gröbner es que

$$Exp(\sqrt{\mathfrak{a}}) = \bigcup_{i=1}^{s} \mu_i + \mathbb{N}^n.$$

La base del anillo cociente (llamada base monomial) a la que se hace referencia en el enunciado de Macaulay es

$$\beta := \{X_1^{\mu_1} \cdots X_n^{\mu_n} + \sqrt{\mathfrak{a}} \ : \ (\mu_1, \ldots, \mu_n) \notin Exp(\sqrt{\mathfrak{a}})\}.$$

Y es obviamente calculable a partir de la base de Gröbner $G$ (los autores clásicos lo llaman la "escalera" del ideal). Escribamos $M := \sharp(\beta)$ la dimensión del espacio vectorial en el que estamos trabajando.

Los elementos de esa base se pueden ordenar (son linealmente independientes y sólo dependen de su combinatoria) mediante el orden $\leq$ que es un orden total. Ahora consideremos la variable $X_i$ y consideremos un elementos que ocupa el lugar $k$, con $1 \leq k \leq M$. Supongamos que ese $k-$ésimo elemento es

$$X_1^{\mu_1} \cdots X_n^{\mu_n} + \sqrt{\mathfrak{a}}.$$

Consideremos ahora el polinomio

$$X_i \left(X_1^{\mu_1} \cdots X_n^{\mu_n}\right) = X_1^{\mu_1} \cdots X_i^{\mu_i+1} \cdots X_n.$$

Y consideremos la forma normal de este polinomio con respecto a la base $G$, es decir:

$$h := NF(X_1^{\mu_1} \cdots X_i^{\mu_i+1} \cdots X_n, G).$$

Esto de la forma normal no es otra cosa que el resto de la división de Hironaka y, por la propia definición de la División de Hironaka) $h$ es combinación lineal de los elementos de la base $\beta$:

$$h := \sum_{\mu \notin Exp(\sqrt{\mathfrak{a}})} b_\mu X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Pues bien, los elementos de la columna $k-$ésima de la matriz del tensor $M_{X_i}$ es la lista de coeficientes de este polinomio $(b_\mu \ : \ \mu \notin Exp(\sqrt{\mathfrak{a}}))$ escritos con el orden dado por el orden monomial $\leq$.

Proposición 4.2.10. *La solución "à la Macaulay" de una variedad cero-dimensional, es calculable a partir de una base de Gröbner del radical del ideal que hemos usado para definir la variedad.*

Demostración. Es lo que se muestra en la Observación precendente. □

Observación 4.2.11. Pero ya hemos indicado que, a priori, es caro hallar la base del Gröbner del radical de un ideal, así que esta vía no va a ser la buena. Veamos qué nos aporta la solución "à la Macaulay" para poder avanzar.

La propiedad fundamental para trabajar con $K[V]$ en lugar de trabajar con las componentes algebraicas, se resumen en la siguiente Proposición:

Proposición 4.2.12 (**Propiedades de la Resolución intrínseca**). *Con las notaciones precedentes se tienen las siguientes propiedades:*

i) *La dimensión de $K[V]$ como $K-$espacio vectorial es igual al grado de $V$. De hecho,*
$$\dim_K(K[V]) = \dim_{\mathbb{K}}(\mathbb{K}[V]) = \deg(V) = \mathscr{D}.$$
ii) *Si $\beta \subseteq K[V]$ es una base de $K[V]$ como $K-$espacio vectorial, entonces $\beta$ también es base de $\mathbb{K}[V]$ como $\mathbb{K}-$espacio vectorial.*

iii) *Si $\beta$ es base de $K[V]$ y, simultánemanete, de $\mathbb{K}[V]$, as matrices $M_{X_i}$ de los tensores en la base $\beta$ son las mismas en $K[V]$ y en $\mathbb{K}[V]$.*

iv) *Si $g \in K[X_1, \ldots, X_n]$ es un polinomio adicional, la matriz $M_g$ en la base $\beta$ es la dada mediante:*

$$M_g := g(M_{X_1}, \ldots, M_{X_n}).$$

v) *La matriz $M_g$ es una matriz diagonalizable sobre $\mathbb{K}$ y su forma canónica de Jordan es la siguiente:*

$$M_g \approx \begin{pmatrix} g(\zeta_1) & 0 & 0 & \cdots & 0 \\ 0 & g(\zeta_2) & 0 & \cdots & 0 \\ 0 & 0 & g(\zeta_3) & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & g(\zeta_{\mathscr{D}}) \end{pmatrix},$$

*donde $\approx$ indica semejanza de matrices,*

$$V = V_{\mathbb{K}}(\mathfrak{a}) := \{\zeta_1, \ldots, \zeta_{\mathscr{D}}\},$$

*y $\mathscr{D} = deg(V_{\mathbb{K}}(\mathfrak{a}))$.*

Demostración. Las primeras afirmaciones no son nuevas. Es la afirmación sobre el hecho de la diagonalización de $M_g$ y su forma diagonal la que tiene interés y aporta novedad con respecto a lo dicho en el caso sombólico-algebraico. La razón es la siguiente: Supongamos $\zeta \in \mathbb{K}^n$ un punto y el morfismo de anillos dado por la evaluación en $\zeta$ siguiente:

$$\begin{array}{rccc} eval_\zeta: & \mathbb{K}[X_1, \ldots, X_n] & \longrightarrow & \mathbb{K} \\ & f & \longmapsto & f(\zeta). \end{array}$$

El núcleo de ese morfismo de $\mathbb{K}-$álgebras es justamente el ideal

$$\mathfrak{m}_\zeta := \{f \in \mathbb{K}[X_1, \ldots, X_n] \ : \ eval_\zeta(f) = f(\zeta) =\}.$$

Por tanto, el isomorfismo del Primer Teorema de Isomorfía es el dado por la siguiente identificación:

$$\begin{array}{rccc} \varphi_\zeta: & \mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_\zeta & \longrightarrow & \mathbb{K} \\ & f + \mathfrak{m}_\zeta & \longmapsto & f(\zeta). \end{array}$$

Ahora observemos que si $\mathfrak{a}$ es el ideal de $K[X_1, \ldots, X_n]$ que define $V$, tenemos que

$$\sqrt{\mathfrak{a}} = \bigcap_{\zeta \in V} \mathfrak{m}_\zeta,$$

y podemos aplicar el isomorfismo del Teorema Chino de los Restos:

$$\begin{array}{rccc} \psi: & \mathbb{K}[V] := \mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}} & \longrightarrow & \prod_{\zeta \in V} (\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{m}_\zeta) \\ & f + \sqrt{\mathfrak{a}} & \longmapsto & (f + \mathfrak{m}_\zeta \ : \ \zeta \in V). \end{array}$$

Es decir, visto el isomorfismo de la Ecuación (4.2.1) anterior, podemos considerar este isomorfismo de la forma siguiente:

$$\begin{array}{rccc} \psi: & \mathbb{K}[V] := \mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}} & \longrightarrow & \prod_{\zeta \in V} \mathbb{K} \\ & f + \sqrt{\mathfrak{a}} & \longmapsto & (f(\zeta) \ : \ \zeta \in V). \end{array}$$

De hecho, si $V = \{\zeta_1, \ldots, \zeta_{\mathscr{D}}\}$, con $\mathscr{D} = \deg(V)$, podemos tambiés escribir ese isomorfismo mediante:

$$\begin{array}{rccc} \psi: & \mathbb{K}[V] := \mathbb{K}[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}} & \longrightarrow & \mathbb{K}^{\mathscr{D}} \\ & f + \sqrt{\mathfrak{a}} & \longmapsto & (f(\zeta_1), \ldots, f(\zeta_{\mathscr{D}}). \end{array}$$

Ahora, si tomamos $g \in K[X_1, \ldots, X_n]$ podemos considerar el siguiente diagrama conmutativo asociado al endomorfismo $\eta_g$:

$$\begin{array}{ccccc} & & \eta_g & & \\ & \mathbb{K}[V] & \longrightarrow & \mathbb{K}[V] & \\ \psi & \downarrow & \circlearrowleft & \downarrow & \psi \\ & \mathbb{K}^{\mathscr{D}} & \longrightarrow & \mathbb{K}^{\mathscr{D}} & \\ & & \tau_g & & \end{array}$$

Como $\eta_g = \psi^{-1} \circ \tau_g \circ \psi$, tenemos que $\psi$ representa un cambio de base y $\eta_g$ y $\tau_g$ son semejantes. Ahora la matriz $M_g$ de $\eta_g$ en cualquier base de $\mathbb{K}[V]$ como $\mathbb{K}-$espacio vectorial, será semejante a la matriz de $\tau_g$. Todo lo que queda es ver cuál es la forma de $\tau_g$ para que ese diagrama conmute y se observa fácilmente que ese endomorfismo toma la forma siguiente:

$$\begin{array}{rccc} \tau_g : & \mathbb{K}^{\mathscr{D}} & \longrightarrow & \mathbb{K}^{\mathscr{D}} \\ & (x_1, \ldots, x_{\mathscr{D}}) & \longmapsto & (g(\zeta_1)x_1, \ldots, g(\zeta_{\mathscr{D}})x_{\mathscr{D}}) \end{array}$$

con lo que su matriz es la matriz diagonal y, por tanto, tenemos la semajanza declarada en el enunicado del Teorema entre $M_g$ y la matriz diagonal correspondiente.

$$M_g := g(M_{X_1}, \ldots, M_{X_n}).$$

La matriz $M_g$ es una matriz diagonalizable sobre $\mathbb{K}$ y su forma canónica de Jordan es la siguiente:

$$M_g \approx \begin{pmatrix} g(\zeta_1) & 0 & 0 & \cdots & 0 \\ 0 & g(\zeta_2) & 0 & \cdots & 0 \\ 0 & 0 & g(\zeta_3) & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & g(\zeta_{\mathscr{D}}) \end{pmatrix}.$$

□

*4.2.1.1. El Problema de Consistencia.* Obviamente se resuelve mediante un simple cálculo del determinante:

$$[\exists \zeta \in \mathbb{K}^n, \zeta \in V_{\mathbb{K}}(\mathfrak{a}) \wedge g(\zeta) = 0] \Leftrightarrow \det(M_g) = 0.$$

Lo que incluye a todos los problemas **NP**-completos.

*4.2.1.2. El Conteo del número de soluciones.* Obviamente se resuelve mediante un simple cálculo del rango:

$$M = \sharp\{\zeta \in \mathbb{K}^n \ : \ \zeta \in V_{\mathbb{K}}(\mathfrak{a}) \wedge g(\zeta) = 0\} \Leftrightarrow [M + rank(M_g) = \mathscr{D}].$$

Lo que incluye a todos los problemas $\sharp$**P**-completos.

Observación 4.2.13. La conclusión es que todas estas preguntas se responden con Álgebra Lineal en tiempo $O(\mathscr{D}^\omega)$ con lo que se debe plantear:

i) Averiguar quién es $\mathscr{D}$,
ii) Diseñar un algoritmo que calcule una resolución intrínseca "à la Macaulay".

Lo primero lo vamos a ver en la Sección siguiente con un poco de Teoría de la Intersección. Lo segundo requerirá dar unas vueltas más.

## 4.3. Teoría de la Intersección : Desigualdad de Bézout.

uno de los elementos claves para entender la resolución "à la Macaulay" intrínseca es entender quién es $\mathscr{D}$ que es la dimensión de $K[V]$ y, por tanto, el tamaño del álgebra lineal que se maneja para los algoritmos y las aplicaciones subsiguientes ya descritas. Este cardinal $\mathscr{D}$ es un objeto de fuerte significación geométrica y, en esta Sección, vamos a resumir algunas de sus propiedades fundamentales.

Uno de los resultados cruciales en la Teoría de la Intersección de conjuntos algebraicos es el teorema conocido como Desigualdad de Bézout. El caso bivariado fue demostrado

por E. Bézout[3] en su trabajo de 1764. Desde entonces, varios autores han intentado una presentación completa del resultado que mide el número de puntos en la intersección de dos variedades algebraicas. A finales de los años 70 y principios de los años 80, tres autores establecieron Desigualdades de Bézout, viniendo de tres ambientes dispares y con técnicas y métodos bien distintos.

i) J. Heintz[4] en su trabajo, tardíamente publicado, de 1983 establece una Desigualdad de Bézout para el caso de conjuntos algebraicos afines. Será ésta la aproximación que seguiremos en estas páginas.
ii) W. Vogel[5] en su trabajo de 1984. Se trata de una desigualdad de Bézout para conjuntos algebraicos proyectivos usando intensamente el polinomio de Hilbert–Samuel.
iii) W. Fulton[6] desarrolla en 1984 una Igualdad de Bézout basándose en el uso de la Teoría de Divisores.

**4.3.1. Rudimentos de Dimensión de Variedades Algebraicas.** Para un conjunto algebraico irreducible $V \subseteq \mathbb{K}^n$, denotemos por $\mathbb{K}(V)$ el cuerpo de funciones racionales definidas en $V$. Una diferencia relevante entre el estudio de las variedades algebraicas y el estudio de las variedades fines lineales (dadas por ecuaciones de grado 1) es la dificultad de controlar la interacción entre número de variables y dimensión. Haremos una sucinta introducción a la noción de dimensión aquí y, dado que no precisamos las pruebas, dejamos para la Sección 6.4 próxima el detalle de su análisis.

Definición 22 (**Dimensión de un Conjunto Algebraico**). *Sea $K$ un cuerpo, $\mathbb{K}$ una clausura algebraica que contiene a $K$, $\mathfrak{a}$ un ideal en $K[X_1, \ldots, X_n]$ y $V = V_{\mathbb{K}}(\mathfrak{a})$ un cerrado Zariski. Lo haremos en dos fases:*

i) *Si $V = \emptyset$ diremos que* $\dim(V) = -1$.
ii) *Si $V$ es irreducible, llamaremos dimensión de Krull (o simplemente dimensión) del conjunto $V$ al máximo de las longitudes de $\ell$ de cadenas finitas*

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_\ell = V,$$

*donde $V_i$ es cerrado irreducible y $K-$definible y lo llamaremos* $\dim(V)$.
iii) *si $V$ es reducible y admite un descomposición en irreducibles*

$$V = W_1 \cup W_2 \cup \cdots \cup W_s,$$

*donde $W_i$ es irreducible, llamamos dimensión de $V$ al máximo:*

$$\dim(V) := \text{máx}\{\dim(W_i) \ : \ 1 \leq i \leq 2\}.$$

*Una variedad algebraica $V$ se dice equidimensional si todas sus componentes irreducibles tienen la misma dimensión.*

Observación 4.3.1. Nótese que el Problema de Consistencia es un problema de cálculo de la dimensión de un algebraico, porque:

$$V \neq \emptyset \Longleftrightarrow \dim(V) \geq 0.$$

[3]E. Bézout, *Recherches su le degré des équations résultants de l'évanouisement des inconnnues*. Histoires de l'Academie Royale des Sciences (1764), 288–338.

[4]J. Heintz, *Fast quantifier elimination over algebraically closed fields*. Theoret. Comp. Sci. **24** (1983), 239–277.

[5] W. Vogel, *"Lectures on Results on Bézout's Theorem"*. (notes by D.P. Patil). Tata Institue of Fundamental research, Springer, 1984.

[6]W. Fulton, *"Intersection Theory"*. Ergebnisse der Mathematik **3**, Springer, 2 edition, 1984.

Un resultado esencial en la Teoría de la dimensión es el Teorema del Ideal Principal de W. Krull[7] (Krull Haputidealsatz) que aquídaremos en una versión simplificada.

TEOREMA 4.3.2 (**Krull's Hauptidealsatz**). *Sea $V \subseteq \mathbb{K}^n$ una variedad algebraica equi-dimensional. Sea $f \in K[X_1, \ldots, X_n]$ una nueva ecuación. Entonces, se tiene:*

i) *La clase en $K[V]$ de $f$ $(f+I(V))$ es un divisor de cero en $K[V]$, si y solamente si se verifica:*
$$\dim\left(V \cap V_{\mathbb{K}}(f)\right) = \dim(V).$$
*Además, en este caso, o bien $V \cap V_{\mathbb{K}}(f) = \emptyset$ o bien $V \cap V_{\mathbb{K}}(f)$ deja de ser equi-dimensional y tiene componentes de dimensión igual a la dimensión de $V$ y otras de dimensión igual a $\dim(V) - 1$.*

ii) *La clase en $K[V]$ de $f$ $(f + I(V))$ no es un divisor de cero en $K[V]$, si y solamente si se verifica una de las dos propiedades siguientes:*
   a) *$V \cap V_{\mathbb{K}}(I) = \emptyset$ o,*
   b) *$V \cap V_{\mathbb{K}}(I) \neq \emptyset$ y, en este caso, es equi-dimensional y todas las componentes irreducibles de $V \cap V_{\mathbb{K}}(I)$ tienen dimensión igual $\dim(V) - 1$.*

En realidad ambos epígrafes son el mismo, pero lo dejaremos para un estudio posterior.

COROLLARIO 4.3.3 (**Teorema de la Altura de Krull**). *Con las mismas notaciones, dada una colección de funciones polinomiales $f_1, \ldots, f_m \in K[V]$, entonces, la intersección*
$$V \cap V_{\mathbb{K}}(f_1, \ldots, f_m),$$
*verifica que o bien es vacía, o bien tiene dimensión mayor o igual que $\dim(V) - m$.*

Un resultado no trivial, pero esperable, es el siguiente:

TEOREMA 4.3.4 (**Dimensión de un espacio afín**). *Con las notaciones precedentes, se tiene:*
$$\dim(\mathbb{K}^n) = n.$$
*Además, todos los subconjuntos algebraicos contenidos en $\mathbb{K}^n$ tienen dimensión menor que $n$.*

DEMOSTRACIÓN. *Sketch* La parte fácil es mostrar que, efectivamente, hay una cadena de longitud $n$ de algebraicos $K-$definibles en $\mathbb{K}$:
$$V_{\mathbb{K}}(X_1, \ldots, X_n) \subsetneq V_{\mathbb{K}}(X_2, X_3, \ldots, X_n) \subsetneq \cdots \subsetneq V_{\mathbb{K}}(X_n) \subsetneq \mathbb{K}^n.$$
Esto demuestra que hay una cadena de longitud $n$, peor hay que hacer un esfuerzo adicional para mostrar que no hay cadenas de irreducibles de longitud mayor que $n$. Lo dejamos para más adelante.

□

EJEMPLO 4.3.5 (**Algunos Ejemplos** ). A partir de estos dos resultados ya podemos mostrar algunos ejemplos básicos de dimensiones de conjuntos algebraicos:

[7] W. Krull estudió en Götingen bajo la dirección de F. Klein y E. Noether. Si bien F. Klein influyó en la comprensión de la matemática en un sentido amplio, E. Noether dejó en W. Krull todo un programa de trabajo que ella misma no pudo concluir por el advenimiento de los nazis al poder en Alemania. En su trabajo W. Krull,*Primidealketten in allgemeinen Ringbereichten.* S.–B. Heildelberg Akad. Wiss. **7** (1928), introdujo la noción de dimensión de un anillo noetheriano, lo que le permitió alcanzar el enunciado del Teorema del Ideal Principal, dando un fuerte espaldarazo a las ideas de su maestra E. Noether sobre la algebrización de la geometría. Posteriormente influirá a geómetras como C. Chevalley y O. Zariski quienes, a a su vez, continuarían la obra de W. Krull. Entre sus obras, debe destacarse este trabajo de 1928, su trabajo sobre los anillos asociados a variedades algebraicas de 1938 (en el que introduce los anillos locales regulares) y, sobre todo, su influyente libro [**Kr, 35**]. Es a este texto y a su autor a quienes debemos la transformación del conjunto de resultados de P. Gordan, D. Hilbert y E. Noether, y sus respectivas escuelas, sobre Teoría de Invariantes en una nueva rama del conocimiento matemático hoy conocida como Algebra Conmutativa.

i) La dimensión de un conjunto finito de puntos de $\mathbb{K}^n$ es 0 (de ahí el término cero-dimensional).
ii) La dimensión de una variedad afín lineal coincide con la dimensión que usualmente se da en los cursos de Álgebria Lineal. Es decir, supongamos que $V$ es un algebraico $K-$definible en $\mathbb{K}^n$ dado por un sistema de ecuaciones lineales:
$$AX = B.$$
Entonces, la dimensión como conjunto algebraico es $-1$.
iii) La dimensión de una hipersuperficie (i.e. $V = V_{\mathbb{K}}(f)$, con $f \in K[X_1, \ldots, X_n]$ y $f$ no unidad) es siempre $n-1$. De hecho, todos los algebraicos de dimensión $n-1$ son hipersuperficies. Nótese que eso no ocurre en el caso $\mathbb{K} = \mathbb{R}$, pero, en este curso, estamos en el caso algebraicamente cerrado y no en el caso real cerrado.

Un resultado relevante, del que daremos una interpretación simplificada y dedicada solamente al caso geométrico, es el famosos Teorema de la Pureza de Macaulay, descrubierto por F.S. Macaulay en [**Mc, 16**] y extendido,en 1946, por I.S. Cohen[8] al caso de anillos de series de potencias formales. Un enunciado puede ser el siguiente:

Teorema 4.3.6 (**Teorema de la Pureza de Macaulay**). *El anillo de polinomios $K[X_1, \ldots, X_n]$ es un anillo de Cohen-Macaulay. En particular, dada una sucesión de polinomios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ tales que la variedad que definen $V := V_{\mathbb{K}}(f_1, \ldots, f_m)$ tiene dimensión $n - m$, entonces todas sus componentes irreducibles tienen dimensión $n - m$ (i.e. no posee componentes "inmersas") y es una variedad equi-dimensional.*

Definición 23 (**Variedades Intersección completa**). *Llamaremos intersección completa (conjuntista) todas las variedades $V \subseteq \mathbb{K}^n$ tales que existen polinomios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ verificando*
$$V := V_{\mathbb{K}}(f_1, \ldots, f_m),$$
*y*
$$\dim(V) = n - m.$$

Es decir, son intersección completa, aquellas variedades en las que es posible encontrar un número de ecuaciones que determinan la dimensión y, en virtud del Teorema de la Pureza de Macaulay, todas sus componentes irreducibles tienen la buena dimensión.
Una generalización interesante del Teorema del Ideal Principal de Krull pasa por la noción de sucesión regular.

Definición 24 (**Sucesión Regular**). *Sea $R$ un anillo, una sucesión $a_1, \ldots, a_s \in R$ se dice sucesión regular si se verifica:*

i) *El ideal $(a_1, \ldots, a_s) \neq (1)$ es un ideal propio en $R$.*
ii) *$f_i$ no es divisor de cero en el anillo cociente $R/(f_1, \ldots, f_{i-1})$.*

*Si, además, todos los ideales $\mathfrak{a}_i := (a_1, \ldots, a_i)$ son ideales radicales (incluyendo $\mathfrak{a}_0 = (0)$ en $R$), entonces se dice que es una sucesión regular reducida.*

Teorema 4.3.7. *Con las anteriores notaciones, sea $V$ una variedad algebraica $K-$definible en $\mathbb{K}^n$ y sean $f_1, \ldots, f_m \mathbb{K}[V]$ una sucesión regular de funciones polinomiales. Entonces, la variedad*
$$W := V \cap V_{\mathbb{K}}(f_1, \ldots, f_m)$$
*tiene dimensión igual a $\dim(V) - m$. Más aún, si $K[V]$ es Cohen-Macaulay (por ejemplo, si $I(V)$ está generado por una sucesión regular), entonces todas las componentes*

[8] I.S. Cohen, *On the structure and ideal theory of complete local rings*. Transactions of the Amer. Math. Soc. **59** (1946), 54106.

*irreducibles de $W$ tienen dimensión igual a $\dim(V)-m$. Además, si $f_1,\ldots,f_m$ son una sucesión regular reducida, $K[W]$ es Cohen-Macaulay.*

De este Teorema nos quedamos solamente con sus significado geométrico y dejamos un poco de lado la interpretación de la condición "ser Cohen-Macaulay". Para el estudio de anillos de Cohen-Macaulay es muy recomendable el texto [**BH, 93**], pero con estas ideas nos basta por ahora.

Observación 4.3.8 (**Sobre las longitudes de las sucesiones regulares)**. El Teorema precedente, junto con las ideas de Krull y Macaulay, nos indica el límite de las longitudes de las succeciones regulares en $K[X_1,\ldots,X_n]$. Dada una sucesión regular $f_1,\ldots,f_m\in K[X_1,\ldots,X_n]$ las variedades intermedias $V_i := V_{\mathbb{K}}(f_1,\ldots,f_i)$, $1\leq i\leq m$, satisfacen todas el Teorema de Krull y el teorema de la Pureza de Macaulay, con lo que

$$\dim(V_i) = n-i.$$

Por tanto, necesariamente $m\leq n$. Más aún, dada una sucesión de ecuaciones $f_1,\ldots,f_m\in K[X_1,\ldots,X_n]$ (con, posiblemente, $m\geq n$) y tales que para cada $i$, $f_i$ no es divisor de cero en el anillo

$$K[X_1,\ldots,X_n]/(f_1,\ldots,f_{i+1}),$$

Entonces las variedades $V_i := V_{\mathbb{K}}(f_1,\ldots,f_i)$ satisfacen las propiedades siguientes:

i) Si $1\leq i\leq n$, $V_i$ es o bien vacío o una variedad equidimensional de dimensión $n-i$.
ii) Si $i=n+1$, entonces $V_i = V_{n+1}$ es necesriamente vacío.
iii) Si $i\geq n+2$, entonces es imposible que $f_i$ no sea divisor de cero en el anillo cociente $K[X_1,\ldots,X_n]/(f_1\ldots,f_{i-1})$ porque $(f_1,\ldots,f_{i-1}) = K[X_1,\ldots,X_n]$.

**4.3.2. La desigualdad de Bézout geométrica.** El resultado esencial para alcanzar la desigualdad de Bézout es la siguiente Proposición. Para demostrarla, un buen uso del Teorema de Ideal Principal de Krull, de la Normalización de Noether y, sobre todo, del Teorema de la dimensión de la Fibra son los ingredientes necesarios.

Proposición 4.3.9. *Sea $V\subseteq\mathbb{K}^n$ un conjunto algebraico irreducible de dimensión $m$ y sea $\varphi : V\longrightarrow\mathbb{K}^m$ un morfismo dominante (i.e. $\varphi(V)$ es Zariski–denso en $\mathbb{K}^m$). La extensión de cuerpos*

$$\mathbb{K}(\mathbb{K}^m)\subseteq\mathbb{K}(V),$$

*es una extensión finita de cuerpos. Además, si tal extensión es separabale, se tiene :*

i) *Para cada $y\in\mathbb{K}^m$, la fibra $\varphi^{-1}(y)$ es finita y se verifica :*

$$\sharp\varphi^{-1}(y)\leq[\mathbb{K}(V) : \mathbb{K}(\mathbb{K}^m)].$$

ii) *Existe un abierto Zariski no vacío $U\subseteq\mathbb{K}^m$ tal que para cada $y\in U$ se verifica la siguiente igualdad :*

$$\sharp\varphi^{-1}(y) = [\mathbb{K}(V) : \mathbb{K}(\mathbb{K}^m)].$$

Sea $V\subseteq\mathbb{K}^n$ un conjunto algebraico irreducible de dimensión $r$. Sea $\mathbb{K}^{rn}$ el espacio de las matrices $r\times n$ con coeficientes en $\mathbb{K}$. Definamos el morfismo :

$$\varphi : \mathbb{K}^{rn}\times V\longrightarrow\mathbb{K}^{rn}\times\mathbb{K}^r$$

dado mediante :

$$\varphi(A,x) := (A,Ax),$$

donde $Ax$ es el efecto de multiplicar la matriz $A$ por el punto $x$. Entonces, se tiene :

Proposición 4.3.10. *Con las anteriores notaciones, se tiene :*

i) *El morfismo $\varphi$ es un morfismo dominante,*
ii) *La extensión de cuerpos $\mathbb{K}(\mathbb{K}^{rn}\times\mathbb{K}^r)\subseteq\mathbb{K}(\mathbb{K}^{rn}\times V)$ es finita y separable.*

iii) *Existe un abierto Zariski $O$ de $\mathbb{K}^{rn}$ tal que la restricción de $\varphi$ a $O \times V$ es un morfismo finito.*

DEFINICIÓN 25. *Sea $V \subseteq \mathbb{K}^n$ un conjunto algebraico irreducible, supongamos $dim(V) = r$. Llamaremos grado (geométrico) de $V$ a la cantidad expresada mediante la siguiente igualdad :*
(4.3.1)

$$\begin{aligned} deg(V) &:= [\mathbb{K}(K^{rn} \times V) \ : \ \mathbb{K}(\mathbb{K}^{rn} \times \mathbb{K}^r)] \\ &= sup\{\sharp(V \cap L) \ : \ L \subseteq \mathbb{K}^n \text{ es una variedad afín lineal de dimensión } n-r\} \end{aligned}$$

*Si $V \subseteq \mathbb{K}^n$ es un conjunto algebraico, llamaremos grado de $V$ a la suma de los grados de las componentes irreducibles de $V$.*

Observar que el grado de un conjunto finito de puntos es el número de puntos o que el grado de una variedad afín lineal es 1 son consecuencias inmediatas de la definición. Un resultado importante en el análisis de la noción de grado geométrico es el siguiente :

LEMA 4.3.11. *Sea $\varphi \ : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ una aplicación afín lineal y sea $V \subseteq \mathbb{K}^n$ un conjunto algebraico. entonces, el grado de la clausura Zariski de la imagen $deg(\overline{\varphi(V)}^Z)$ está acotado por el grado de $V$.*

Un resultado clave que concluye la esencia de la prueba de esta demostración de la Desigualdad de Bézout es el siguiente :

TEOREMA 4.3.12. *Sea $V \subseteq \mathbb{K}^n$ y $W \subseteq \mathbb{K}^m$ dos conjuntos algebraicos afines. Entonces,*

$$deg(V \times W) = deg(V) \cdot deg(W).$$

Combinando el Lema y el Teorema anteriores, tenemos la deseada Desigualdad de Bézout :

TEOREMA 4.3.13 (Desigualdad de Bézout). *Sea $V$ y $W$ dos subconjuntos algebraicos afines de $\mathbb{K}^n$. Entonces,*

$$deg(V \cap W) \leq deg(V) \cdot deg(W).$$

Algunas consecuencias importantes de este enunciado, que van a ser usadas con posterioridad, son las siguientes.

**4.3.3. Grado de Intersecciones Completas.** Retomamos lo dicho sobre las ideas de Krull, Macaulay y Cohen relacionando el número de ecuaciones con la dimensión. Uno de los resultados más inmediatos es el diguiente:

COROLLARIO 4.3.14. *Sea $K$ un cuerpo, $\mathbb{K}$ su clausura algebraica y $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ una colección de polinomios y $V = V_{\mathbb{K}}(f_1, \ldots, f_m)$. Supongamos que $V \neq \emptyset$. Entonces, se tiene:*

$$\deg(V_{\mathbb{K}}(f_1, \ldots, f_m)) \leq \prod_{i=1}^{m} \deg(f_i),$$

*donde* $\deg(f_i)$ *es el grado total de $i$.*
*Más aún, si $f_1, \ldots, f_m$ forman una sucesión regular, se tiene:*

$$\deg(V_{\mathbb{K}}(f_1, \ldots, f_k)) \leq \prod_{i=1}^{k} \deg(f_i), \ \ y \ \ \dim(V) = n - k.$$

DEMOSTRACIÓN. Consecuencia inmediata de los Teoremas de Krull, Macaulay y de la desigualdad de Bézout. □

NOTACIÓN 4.3.15 (**Listas de ecuaciones de grados fijados**). retomemos las notaciones usadas en la primera parte del curso, aunque trataremos solamente el caso afín. Para un entero $d \in \mathbb{N}$, denotemos mediante

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

Dado $m \in \mathbb{N}$, consideremos una lista de grados $(d) := (d_1, \ldots, d_m)$ y definamos

$$\mathcal{P}_{(d)}^{(m)}(X_1, \ldots, X_n) := \prod_{i=1}^{m} P_d(X_1, \ldots, X_n).$$

En ocasiones supondremos que $n$ es el número de variables en cuestión, y no las exhibiremos para no recargar demasiado la notación, dándolas por sobre-entendidas. En ese caso escribiremos simplemente $\mathcal{P}_{(d)}^{(m)}$. Puede parecer que la notación con el exponente $^{(m)}$ es excesiva dado que $m$ ya está contemplado en la lista $(d)$. Sin embargo, la vamos a guardar provisionalmente para poder usarla a conveniencia. Nótese que $\mathcal{P}_{(d)}^{(m)}(X_1, \ldots, X_n)$ es un espacio vectorial de dimensión finita sobre $K$ y que, en particular, podemos identificar

$$\mathcal{P}_{(d)}^{(m)} \cong K^{N_{(d)}},$$

donde

$$N_{(d)} = \sum_{i=1}^{m} \frac{d_i + n}{n}.$$

COROLLARIO 4.3.16. *Con las notaciones anteriores, si $m \leq n$, existe un conjunto algebraico $K-$definible $\Sigma_{(d)} \subsetneq \mathbb{K}^{N_{(d)}}$ tal que*

$$\forall f := (f_1, \ldots, f_m) \in \left(\mathbb{K}^{N_{(d)}} \setminus \Sigma_{(d)}\right) \cup K^{N_{(d)}}\Big),$$

*se tiene:*

i) *Si $1 \leq i \leq n$, $f_1, \ldots, f_i$ son una sucesión regular reducida. En particular, el ideal que genera es radical y se tiene, además, que:*

$$\dim(V_{\mathbb{K}}(f_1, \ldots, f_i) = n - i, \ \ \deg(V_{\mathbb{K}}(f_1, \ldots, f_i)) = \prod_{k=1}^{i} \deg(f_k) = \prod_{k=1}^{i} d_k.$$

ii) *Si $n + 1 \leq i \leq m$. $V_K(f_1, |ldots, f_i) = \emptyset$.*

OBSERVACIÓN 4.3.17. Algunos autores, y sobre todo en la Parte 1 de esta curso, insisten en llamar a la cantidad

$$\mathscr{D} := \prod_{i=1}^{n} d_i,$$

el número de Bézout de un sistema dado por ecuaciones $f_1, \ldots, f_n$. La razón son los resultados que acabo de enunciar y que son debidos a Krull, Macaulay, Heintz, Vogel etc.... El último Corolario indica, además, que si tratamos con un sistema de $n$ ecuaciones con $n$ variables y de grados dados por una lista $(d) = (d_1, \ldots, d_n)$ la esperanza (en el sentido Estadístico) de la dimensión $\mathscr{D}$ de la $K-$álgebra donde hay que hacer Álgebra Lineal (y, por tanto, el tamaño de las matrices) es el número de Bézout.

$$\mathscr{D} := \prod_{i=1}^{n} d_i.$$

Un resultado que aparece en [**He, 83**] y que está fuertemente inspirado en ideas de Kronecker es el siguiente:

TEOREMA 4.3.18. *Sea* $\{f_1, \ldots, f_s\} \subseteq K[X_1, \ldots, X_n]$ *un conjunto de ecuaciones polinomiales que generan un ideal* $\mathfrak{a}$ *en* $K[X_1, \ldots, X_n]$. *Supongamos* $deg(f_i) \leq d$. *Sea* $V_{\mathbb{K}}(\mathfrak{a}) \subseteq \mathbb{K}^n$ *el conjunto algebraico que definen y supongamos que es equidimensional y de dimensión* $r$. *Entonces,*

$$deg(V(\mathfrak{a})) \leq d^{n-r}.$$

DEMOSTRACIÓN. Se trata de construir una cadena de polinomios $\{g_1, \ldots, g_r\}$ en $\mathfrak{a}$, dados como combinaciones lineales de los polinomios de la familia $\{f_1, \ldots, f_s\}$ de tal modo que cada nueva ecuación haga caer en uno la dimensión de tal modo que las componentes irreducibles de $V_{\mathbb{K}}(\mathfrak{a})$ estén entre las componentes irreducibles de $V_{\mathbb{K}}(g_1, \ldots, g_r)$. Además, los grados de $g_1, \ldots, g_r$ no serán mayores que el máximo de los grados de los $f_i$ y se produce:

$$\deg(V_{\mathbb{K}}(\mathfrak{a})) \leq \deg(V_{\mathbb{K}}(g_1, \ldots, g_r)) \leq \prod_{i=1}^{r} \deg(g_i) \leq d^{n-r}.$$

□

**4.3.4. Grado de la Imagen.** Este primer resultado es crucial para desarrollar la técnica de los Questores (Correct Test Sequences) en la Sección 2.3 :

TEOREMA 4.3.19. *Sea* $V \subseteq \mathbb{K}^n$ *un conjunto algebraico y sea*

$$\varphi \ : V \subseteq \mathbb{K}^n \longrightarrow \mathbb{K}^N$$

*un morfismo regular. Supongamos que*

$$\varphi := (\varphi_1, \ldots, \varphi_N),$$

*donde* $\varphi_1, \ldots, \varphi_N \in \mathbb{K}[Z_1, \ldots, Z_n]$ *son polinomios de grado a lo sumo* $d$.
*Sea* $W \subseteq \mathbb{K}^N$ *la clausura Zariski de* $Im\ \varphi$. *Entonces, se verifica la siguiente desigualdad :*

$$deg(W) \leq deg(V) d^{dim(V)}.$$

## 4.4. Solución "à la Kronecker" del caso cero-dimensional

El uso del elemento primitivo ha sido redescubierto múultiples veces a lo largo de la historia de la Teoría de la Eliminación. Así, por ejemplo, la Resolvente de Lagrange (cf. [**Lgr, 1771**]) no es sino un ejemplo particular de uso del Elemento Primitivo. Es también patente que la nocién subyace al trabajo de L. Kronecker [**Krn, 1882**] e, incluso, a la noción de forma de Chow (que discutiremos más adelante). Se pueden encontrar referencias en B.L. van der Waerden [**Wae, 49**] (bajo la forma de U-resultante) y autores anteriores como F.S. Macaulay ([**Mc, 16**]) y J. König ([**Kö, 1903**]). En el contexto del la Geometría Algebraica Efectiva del presente siglo (i.e. con posterioridad a los años 70) es comúnmente citado el trabajo de H. Kobayashi, S. Moritsugu y R.W. Hogan [**KMH, 89**], con la denominación *Shape Lemma*. Sin embargo, no me seríaa nada difícil citar apariciones de la noción en R. Narasimhan, entre los antecesores, o los autores más "modernos" como J. Canny, J. Renegar, B. Mourain, F. Rouillier.... Seguiremos la presentación de [**Pa, 95**] y antecesores. Trabajaremos en cuerpos $K$ perfectos (por ejemplo, cuerpos finitos o cuerpos de característica cero). Supondremos que son de cardinal "suficientemente grande" (o aplicaremos lo discutido en el Capítulo 2, en la Subsección 2.4.2)

LEMA 4.4.1. *Sea* $K$ *un cuerpo prefecto de cardinal suficientemente grande y* $\mathbb{K}$ *un cuerpo algebraicamente cerrado q1ue le contiene. Sean* $\{\zeta_1, \ldots, \zeta_{\mathscr{D}}\} \subseteq \mathbb{K}^n$ *un conjunto de* $\mathscr{D}$ *puntos ditintos en* $\mathbb{K}$.. *Entonces, existe una función lineal*

$$\begin{array}{rccc} u: & \mathbb{K}^n & \longrightarrow & \mathbb{K}^n \\ & x & \longmapsto & u(x) := u_1 x_1 + \cdots + u_n X_n, \end{array}$$

*tal que*

$$u(\zeta_i) \neq u(\zeta_j), \forall i \neq j,$$

*siendo* $(u_1, \ldots, u_n)$*. De hecho, basta con que el cardinal de* $K$ *satisfaga la desigualdad:*

$$\sharp(K) \geq \mathscr{D}(\mathscr{D}-1)+1.$$

Demostración. Basta con considerar el polinomio siguiente:

$$\chi(U_1, \ldots, U_n) := \prod_{i<j}\left(\sum_{k=1}^{n} U_k(\zeta_{i,k}-\zeta_{j,k})\right) \in K[X_1, \ldots, X_n],$$

donde

$$\zeta_i := (\zeta_{i,1}, \ldots, \zeta_{i,n}) \in \mathbb{K}^n.$$

Este es un polinomio no nulo dado que hemos supuesto que los $\zeta_i$'s son todos distintos, luego es un polinomio no nulo. Es un polinomio de grado $\frac{\mathscr{D}(\mathscr{D}-1)}{2}$. Luego, usando los resultados descritos en la Subsección 2.3.1, podemos garabtizar que si $\sharp(K) \geq \mathscr{D}(\mathscr{D}-1)+1$, entonces, existe $u := (u_1, \ldots, u_n) \in K^n$ tal que $\chi_(u) \neq 0$. Lo que queda por observar es que si $\chi(u) \neq 0$, la función lineal que define "separa" todos los elementos del conjunto $\{\zeta_1, \ldots, \zeta_{\mathscr{D}}\} \subseteq \mathbb{K}^n$. □

Definición 26 (**Elemento separante**). *Con las notaciones anteriores, dado un conjunto finito* $V := \{\zeta_1, \ldots, \zeta_{\mathscr{D}}\} \subseteq \mathbb{K}^n$*, se llama elemento separante (o elemento primitivo) para* $V$ $K-$*definible a todo polinomio* $g \in K[X_1, \ldots, X_n]$ *tal que*

$$g(\zeta_i) \neq g(\zeta_j),\ \forall i \neq j.$$

El Lema precedente prueba que si $K$ posee suficientemente muchos elementos, un onjunto finito posee elementos separantes $K-$definibles e, inlcuosl podemos suponer que son lineales.

Definición 27 (**Solución "à la Kronecker": caso cero-dimensional**). *Sea* $K$ *un cuerpo perfecto con suficientes elementos,* $\mathbb{K}$ *una extensión algebraica,* $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ *un ideal cero-dimensional y* $V = V_{\mathbb{K}}(\mathfrak{a}) \subseteq \mathbb{K}^n$ *el conjunto de sus soluciones. Supongamos* $\mathscr{D} := \deg(V)$*. Una solución à la Kronecker de* $\mathfrak{a}$ *es la lista dada por la siguiente información:*

i) *Una forma lineal* $u := u_1X_1 + \cdots + u_nX_n \in K[X_1, \ldots, X_n]$ *que es separante sobre* $K$*.*
ii) *Un polinomio univariado* $\chi_u(T) \in K[T]$ *dado mediante*

$$\chi_u(T) := \prod_{i=1}^{\mathscr{D}}(T-u(\zeta_i)).$$

iii) *Una lista de polinomios univariados* $v_1, \ldots, v_n \in K[T]$ *y una constante no nula* $\rho \in K$ *tal que*

$$\rho\zeta_{i,k} - v_k(u(\zeta_i)) = 0,\ \forall i, 1 \leq i \leq \mathscr{D}, 1 \leq k \leq n.$$

*Al polinomio* $\chi_u(T)$ *se le denomina polinomio eliminante de* $u$ *sobre* $V$ *y a los polinomios* $v_i(T)$ *se les llama parametrizaciones, mientras que la constante no nule* $\rho$ *se llamará discriminante asociado a la forma separante* $u$*.*

Teorema 4.4.2. *Todo ideal cero-dimensional sobre cuerpos* $K$ *perfecto (con suficientes elementos) posee solución a la Kronecker. Además, toda solución "à la Kronecker" es un tipo particular de solución "à la Macaulay". De hecho, dada una lista* $\{u, \chi_u(T), \rho, v_1(T), \ldots v_n(T)\}$ *como en la definición anterior tenemos, siendo* $u = u_1X_1 + \cdots + u_nX_n \in K[X_1, \ldots, X_n]$*:*

i) *La siguiente es una base de* $K[V]$ *como* $K-$*espacio vectorial:*

$$\beta_u := \{1+I(V), u+I(V), u^2+I(V), \ldots, u^{\mathscr{D}-1}+I(V)\}.$$

ii) *La matriz de la homotecia $\eta_u$ definida por $u$ en esa base es la matriz compañera $M_u = C(\chi_u)$ de $\chi_u$.*
iii) *Las matrices de los tensores vienen dadas por:*

$$M_{X_i} = \rho^{-1} v_i(M_u).$$

*Y tenemos, obviamente, una solución "à la Macaulay".*

Demostración. Ya hemos visto la existencia de una forma separante, luego también existe $\chi_u(T)$. Es "sencillo" recordar un "poco" de Teoría de Galois para observar que $\chi_u(T) \in K[T]$. Pero si la Teoría de Galois no fuera satissfactoria, consideremos la matriz $M_u$ asociada a la homotecia $\eta_u : K[V] \longrightarrow K[V]$. Es calro que la matriz

$$M_u := u_1 M_{X_1} + \cdots + u_n M_{X_n} \in \mathcal{M}_{\mathscr{D}}(K),$$

es una matriz con coordenadas en $K$. Luego su polinomio caracetrístico tiene sus coeficientes en $K$. Pero los vaolores propios de la matriz $M_u$ eran $\{u(\zeta_1), \ldots, u(\zeta_{\mathscr{D}})\}$, luego tenemos:

$$\det(TId_{\mathscr{D}} - M_u) = \prod_{i=1}^{\mathscr{D}} (T - u(\zeta_i)) \in K[T].$$

Pero este polinomio característico es, justamente, $\chi_u(T)$. Lo inquietante es que tengamos, además, un isomorfismo de $K-$álgebras. Para ello, consideremos $W \subseteq \mathbb{K}$, el conjunto dado mediante:

$$W := \{z \in \mathbb{K} \ : \ \chi_u(z) = 0\} \subseteq \mathbb{K}.$$

Es una variedad algebraica, tenemos que

$$u : V \longrightarrow W$$

es una aplicación polinomial suprayectiva, luego dominante, luego

$$u^* : K[W] \longrightarrow K[V],$$

es un morfismo inyectivo de $K-$álgebras. Además, es claro que

$$K[W] := K[T]/(\chi_u(T)).$$

La razón es que, por construcción, $\chi_u(T)$ es un polinomio libre de cuadrados (no posee factores múltiples) luego el ideal que genera es radical y, por el Nullstellensatz, $I_K(W) := (\chi_u(T))$. Además, es fácil ver que la dimensión de $K[W]$ como espacio vectorial es $\mathscr{D} = \deg(\chi_u(T))$.
Luego $u^*(K[W])$ es un subespacio vectorial de $K[V]$ de dimensión $\mathscr{D}$, pero ya sabemos que la dimensión de $K[V]$ como $K-$espacio vectoral es $\mathscr{D}$, luego

$$u^*(K[W]) = K[V],$$

y $u^*$ es un isomorfismo de $K-$álgebras. Pero, esto significa que cada variable $X_i$ verifica que

$$X_i + I(V) = u^*(v_i + (\chi_u(T))).$$

Luego, esto significa que

$$X_i - v_i(u_1 X_1 + \cdots + u_n X_n) \in I_K(V).$$

y tenemos la existencia de las parametrizacions y sus propiedades. Hemos hecho el asunro con $\rho = 1$. Veremos después qué significa $\rho$.
De hecho, lo que acabamos de probar confirma las afirmaciones descritas en las afirmaciones i) y ii) del enunciado. □

OBSERVACIÓN 4.4.3. En términos geométricos, una solución a la Kronecker en el caso cero-dimensional es, en realidad un isomorfismo birregular con una variedad propio en $\mathbb{K}$ (i.e. en el espacio afín de dimensión 1 sobre $\mathbb{K}$). La variedad con la que hacemos que $V$ sea isomorfo birregularmente, es justamente en conjunto de ceros en $\mathbb{K}$ de $\chi_u(T)$. y tenemos un isomorfismo birregular

$$\begin{array}{rccc} u: & V & \longrightarrow & V_{\mathbb{K}}(\chi_u) \\ & \zeta & \longmapsto & u(\zeta), \end{array}$$

La transformación inversa de este isomorfismo birregular es la dada por las parametrizaciones:

$$\begin{array}{rccc} u^{-1}: & V_{\mathbb{K}}(\chi_u) & \longrightarrow & V \\ & u & \longmapsto & (\rho^1 v_1(u), \ldots, \rho^{-1} v_n(u)). \end{array}$$

**4.4.1. De cualquier solución "à la Macaulay" a una solución "à la Kronecker": algoritmos.** Si bien toda solución "à la Kronecker" define una solución "à la Macauley", el recíproco require un poco de reflexión. La razón es simple: en princpio, no tenemos acceso a las "verdaderas" soluciones, luego no parece posible que podamos construir la información de $\chi_u$ sin conocer los $\zeta_i$'s. Este es el juego que queremos jugar. Comencemos con la siguiente observación clásica del Álgebra Lineal:

LEMA 4.4.4. *Sea $K$ un cuerpo perfecto y sea $M \in \mathcal{M}_m(K)$ la matriz de un endomorfismo. Supongamos que $M$ es diagonalizable en la clausura algebraica de $K$. Entonces, el polinomio mínimo de $M$ viene dado por la siguiente propiedad:*
*Sea $\chi(T) \in K[T]$ el polinomio característico de $M$:*

$$\chi(T) := \det(TId_m - M) \in K[T],$$

*Sea $\chi'(T) \in K[T]$ la derivada de $\chi(T)$ con respecto a la variable $T$. Sea $h(T) \in K[T]$ el máximo común divisor de $\chi(T)$ y $\chi'(T)$, i.e.*

$$h := gcd(\chi, \chi').$$

*Entonces, el polinomio mínimo de $M$ es el polinomio dado mediante:*

$$m_M(T) := \frac{\chi(T)}{h}.$$

*Más aún, la matriz $M$ es diagonalizable y todos sus valores propios son distintos dos a dos si y solamente si $m_M = \chi(T)$ o, equivalentemente, si y solamente si el discriminante de $\chi(T)$ es no nulo. Recordemos que el discriminante de un polinomio es dado mediante:*

$$disc_T(\chi) := \det(\chi'(C(\chi))),$$

*donde $C(\chi)$ es la matriz compañera de $\chi$.*

DEMOSTRACIÓN. Recordad vuestros cursos de Álgebra Lineal que, se supone, fueron muy profundos. □

*4.4.1.1. Interpolación de Lagrange.* De otro lado, recodemos el método de interpolación de Lagrange. Este método nos dice que si disponemos de una familia de pares de elementos en un cuerpo $\{(a_i, b_i) : 1 \leq i \leq m\}$, con la condición $a_i \neq a_j$, $\forall i \neq j$. Entonces exite un polinomio $p \in K[T]$ verificando:

$$p(a_i) = b_i, \ \ \forall i, \ 1 \leq i \leq m.$$

De hecho, el polinomio se puede definir mediante la siguiente famosa fórmula de Lagrange:

$$p(T) := \sum_{i=1}^{m} b_i \frac{\prod_{j \neq i}(T - a_j)}{\prod_{j \neq i}(a_i - a_j)} \in K[T].$$

De hecho, observamos que podemos considerar el polinomio

$$h(T) := \prod_{i=1}^{m}(T - a_i).$$

El discriminante de ese polinomio tiene que ver con el elemento del cuerpo $\rho \in K$ dado mediante:

$$\rho := \prod_{i<j}(a_i - a_j),$$

y, de hecho,

$$h'(T) := \sum_{i=1}^{m}\prod_{j\neq i}(T - a_i),$$

luego el discriminante

$$disc_T(h) := \det(h'(C(h)) = \prod_{i=1}^{m}\prod_{j\neq i}(a_i - a_j) = \rho^2.$$

Lo que sí podemos concluir es que existe un polinomio $p \in K[T]$ de grado menor que $m-1$ satisfaciendo

$$p(a_i) = b_i.$$

Con esta información inicial tenemos el siguiente resultado:

TEOREMA 4.4.5. *Existe un algoritmo probabilista tal que, en un número de operaciones en $K$ polinomial en*

$$\mathscr{D}, n$$

*realiza la siguiente tarea:*
*Dada una resolución "à la Macaulay" de un ideal cero-dimensional $\mathfrak{a}$, el algoritmo devuelve una resolución "à la Kronecker" del mismo ideal.*

DEMOSTRACIÓN. El algoritmo es simple por todo lo visto hasta ahora.

---

INPUT: La solución "à la Macaulay":

$$(\beta, \{M_{X_1}, \ldots, M_{X_n}\}).$$

**Hallar el polinomio** $\chi(U_1, \ldots, U_n, T) \in K[U_1, \ldots, U_n, T]$ dado mediante:

$$\chi(U_1, \ldots, U_n, T) := \det(TId_{\mathscr{D}} - (U_1M_{X_1} + \cdots + U_nM_{X_n}) \in K[U_1, \ldots, U_n, T].$$

**Hallar el discriminante** de ese polinomio:

$$D(U_1, \ldots, U_n) := \det(\frac{\partial\chi}{\partial T}(U_1, \ldots, U_n, C(\chi)) \in K[U_1, \ldots, U_n],$$

donde $C(\chi)$ es la matriz compañera de $\chi$ con respecto a la variable $T$. **Test de Nulidad de Polinomios:** Usar cualquier test de nulidad de polinomios para hallar un punto $u := (u_1, \ldots, u_n) \in K^n$ tal que

$$D(u_1, \ldots, u_n) \neq 0.$$

**Hallar matriz**

$$M_u := u_1M_{X_1} + \cdots + u_nM_{X_n}.$$

y su polinomio característico $\chi_u \in K[T]$.
**Resolver los sistemas de ecuaciones lineales:** para cada $k$, $1 \leq k \leq n$, hallar las soluciones

$$\{t_{i,k} \ : \ 1 \leq k \leq n, 0 \leq i \leq \mathscr{D} - 1\}.$$

los sistemas de ecuaciones lineales siguientes

$$M_{X_k} := \sum_{i=0}^{\mathscr{D}-1} T_{i,k} C(\chi_u)^i, \tag{4.4.1}$$

donde $C(\chi_u)$ es la matriz compañera de $\chi_u(T)$.
OUTPUT:

- El punto $u = (u_1, \ldots, u_n) \in K^n$
- El polinomio $\chi_u(T)$ dado por sus coeficientes.
- La lista de polinomios:

$$v_k(T) := \sum_{i=0}^{\mathscr{D}-1} t_{i,k} T^i \in K[T], \;\; 1 \leq k \leq n.$$

---

Para el análisis de complejidad debemos hacer algunas precisiones:

i) El discriminante $D(U_1, \ldots, U_n)$ es un polinomio de grado $\mathscr{D}(\mathscr{D}-1)$ en $n$ variables. Si lo intentáramos escribir por sus coeficientes tendríamos un problema porque el número de sus coeficientes es enorme:

$$\binom{\mathscr{D}+n}{n} \approx \mathscr{D}^n.$$

Sin embargo, *para hallar $u$ no necesitamos nunca escribir el discriminante* $D(U_1, \ldots, U_n)$. Esta es la razón de usar Tests Probabilistas de Nulidad de Polinomios. Lo que necesitamos es poder evaluar $D(u_1, \ldots, u_n)$ para puntos $(u_1, \ldots, u_n) \in I^n$ si $I$ es el conjuntod definido por el Teste de Zippel-Schwartz. Es más elegante usar, por eejmplo, los cuestores, pero no entro en ese detalle ténico por ahora. Y para hallar $D(u_1, \ldots, u_n)$ en una elección aleatoria de $u \in I^n$, no necesitamos escribir $D(U_1, \ldots, U_n)$ sino evaluar los determinantes de matrices con coordenadas en $K$ y de tamaño $\mathscr{D}^2$ que se indican en el algoritmo.... Luego se puede hacer en tiempo

$$n^{O(1)} \mathscr{D}^{\omega}.$$

Más adelante explicaremos este curioso fenómeno como la representación de polinomios mediante esquemas de evaluación (o *straight–line programs* o SLP's).

ii) Las ecuaciones lineales a resolver en las identidades (4.4.1) son $n$ sistemas de ecuaciones lineales, cada una de las cuales tiene $\mathscr{D}^2$ ecuaciones (una por coordenada de las matrices involucradas) en $\mathscr{D}$ variables. Esto require algunas matizaciones.
   - *La primera es que todos esos sistemas en ((4.4.1)) son compatibles*, es decir, sabemos que poseen solución siempre. Así que, aunque el sistema sea muy sobredeterminado, el sistema es siempre compatible.
   - *La segunda es que todas las matrices involucradas son matrices de homotecias $\eta_g$ de polinomios $g$* y sabemos que las homotecias $\eta_g$ al escribir sus matrices en una base $\beta$ que tiene a la clase de 1 como primer elemento de la base, están totalmente determinadas por la primera columna. Así que, en realidad, los que hay que hacer es:
     Para cada $i$, $0 \leq i \leq \mathscr{D}-1$,
     **Hallar** $C_{i,k} \in K^{\mathscr{D}}$ la primera columna de la matriz $C(\chi_u)^i$.
     **Hallar** la primer columna $C_k \in K^{\mathscr{D}}$ de la matriz $M_{X_k}$.

**Resolver los $n$ sistemas de ecuaciones lineales con $\mathscr{D}$ variables y el mismo número de ecuaciones:**

$$C_k := \sum_{i=0}^{\mathscr{D}-1} T_{i,k} C_{i,k}.$$

En suma, nunca hacemos nada que no sea Álgebra Lineal en dimensión $\mathscr{D}$ y todo eso se hace en tiempo $\mathscr{D}^\omega$. Como mucho en $\mathscr{D}^{\omega+1}$ (por las potencias) y $n^{O(1)}\mathscr{D}^{\omega+1}$ por tratar de ser generoso con la complejidad. □

## 4.5. Solución mediante Forma de Cayley-Chow del caso cero-dimensional

Con lo discutido anteriormente, ya podemos devolver la definición de resolución vasada en la $\mathcal{U}-$resultante de van der Waerden que también se denomina polinomio eliminante of forma de Cayley-Chow para el caso de ideales cero-dimensionales.

Definición 28 (**Solución mediante la Forma de Cayley-Chow)**. *Dado un cuerpo perfecto $K$ y una estención $\mathbb{K}$ algebraicamente cerrada de $K$. Sea $\mathfrak{a}$ un ideal cero-dimensional en $K[X_1,\ldots,X_n]$ y sea $V := V_{\mathbb{K}}(\mathfrak{a})$ la variedad $K-$definible que define. Una solución mediante forma de Cayley-Chow de las ecuaciones en $\mathfrak{a}$ es un polinomio multi-variado en el anillo $K[U_1,\ldots,U_n,T]$ dado mediante:*

$$\chi_{\mathcal{U}}(U_1,\ldots,U_n,T) := \prod_{\zeta=(\zeta_1,\ldots,\zeta_n)\in V} (T - (U_1\zeta_1 + \cdots + U_n\zeta_n)) \in K[U_1,\ldots,U_n,T].$$

El polinomio eliminante (o forma de Cayley-Chow) en el caso cero-dimensional es un polinomio homogéneo en $n+1$ variables, mónico con respecto a la variable $T$ y de grado total $\mathscr{D} = \deg(V)$. Sin embargo, como ya hemos inidcado, no lo vamos a representar mediante sus coeficientes, sino mediante esquemas de evaluación. Ya discutimos después esa representación y, por el momento, admitimos que podemos representarle mediante una información de tamaño polinomial en $\mathscr{D}$.

Observación 4.5.1 (**De la solución "à la Macualy" a la solución a la Cayley–Chow)**. Debe señalarse que, aunque la forma de Cayley-Chow tiene la forma descrita en la Definición precedente, i.e.,

$$\chi_{\mathcal{U}}(T) := \prod_{\zeta=(\zeta_1,\ldots,\zeta_n)\in V} (T - (U_1\zeta_1 + \cdots + U_n\zeta_n)),$$

en realidad NUNCA tenemos acceso a las soluciones $\zeta \in V$ de modo directo, sino que, en la mayoría de los casos tenemos acceso a $\chi_{\mathcal{U}}$ sin tener acceso a los $\zeta$. Esto es más evidente si partimos de una resolución "à la Macaulay" con tensores $M_{X_1},\ldots,M_{X_n}$. En ese caso, la forma de Cayley-Chow sience dada por:

$$\chi_{\mathcal{U}}(U_1,\ldots,U_n,T) = \det\left(U_1M_{X_1} + \cdots + U_nM_{X_n}\right) \in K[U_1,\ldots,U_n,T].$$

Sabemos que $\chi_{\mathcal{U}}$ tiene la forma adecuada, pero no concemos individualmente las soluciones.
Es claro que podemos obtener la forma de Cayley-Chow a partir de una solución "à la Macaulay" y que podemos representar ese polinomio con la información necesaria para escribir un determinante que, usando métodos adecuados, à la Berkowizc-Mulmuley, por ejemplo, son programas que se pueden escribir usando $\mathscr{D}^{\omega+1}$ operaciones aritméticas.

La parte "difícil" es recuperar la información "à la Macaulay" (o "à la Kronecker") a partir de la forma de Cayley-Chow. Comencemos definiendo ciertos polinomios derivados de la forma de Cayley-Chow: Sea $\chi_{\mathcal{U}}(T)$ una forma de Cayley-Chow de una variedad $V$ cero-dimensional como en la Definición anterior. Consideremos los polinomios siguientes:

i) La derivada con respeto a $T$:

$$\chi'_{\mathcal{U}}(U_1,\ldots,U_n,T) := \frac{\partial \chi_{\mathcal{U}}(T)}{\partial T}(U_1,\ldots,U_n,T) \in K[U_1,\ldots,U_n,T].$$

ii) Las derivadas parciales con respecto a las otras variables:

$$Q_i(U_1,\ldots,U_n,T) := \frac{\partial \chi_{\mathcal{U}}(T)}{\partial U_i}(U_1,\ldots,U_n,T) \in K[U_1,\ldots,U_n,T].$$

iii) El discriminante:

$$D(U_1,\ldots,U_n) := Res_T(\chi_{\mathcal{U}}(T),\chi'_{\mathcal{U}}(T)) := \det\left(\chi'_{\mathcal{U}}\left(U_1,\ldots,U_n,C\left(\chi_{\mathcal{U}}\right)\right)\right).$$

Se trata de un polinomio en $D(U_1,\ldots,U_n) \in K[U_1,\ldots,U_n]$.

Si nos fijamos en el Lema 2.1.2 del Capítulo 2 tenemos la siguiente propiedad, usando como anillo $R := K[U_1,\ldots,U_n]$:

COROLLARIO 4.5.2. *Con las notaciones anteriores, existen polinomios*

$$a, b \in K[U_1,\ldots,U_n,T]$$

*tales que*

$$D(U_1,\ldots,U_n) := a(U_1,\ldots,U_n,T)\chi_{\mathcal{U}} + b(U_1,\ldots,U_n,T)\chi'_{\mathcal{U}}.$$

*Además, en Lema 2.1.2 se expone quienes son los polinomios $a$ y $b$.*

Introduzcamos las siguientes notaciones:

i) Tenemos un ideal cero-dimensional $\mathfrak{a}$ en $K[X_1,\ldots,X_n]$.

ii) La variedad $V := V\mathbb{K}(\mathfrak{a})$ tiene grado $\mathscr{D}$, la dimensión de $K[V]$, como $K-$espacio vectorial, es $\mathscr{D}$ y los elementos de $V$ se representan mediante:

$$V := \{\zeta_1,\ldots,\zeta_{\mathscr{D}}\},$$

con $\zeta_i := (\zeta_{i,1},\ldots,\zeta_{i,n}) \in \mathbb{K}^n$

iii) Consideremos las proyecciones canónicas:

$$\begin{array}{rccc} \pi_i: & \mathbb{K}^n & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & x_i. \end{array}$$

iv) Para cada $\zeta := (\zeta_1,\ldots,\zeta_n) \in \mathbb{K}^n$, escribamos $\mathcal{U}(\zeta)$ para representar el punto

$$\mathcal{U}(\zeta) := U_1\zeta_1 + \cdots + U_n\zeta_n \in \mathbb{K}[U_1,\ldots,U_n].$$

PROPOSICIÓN 4.5.3. *Con las anteriores notaciones, se verifican las siguientes propiedades en $\mathbb{K}[U_1,\ldots,U_n]$:*

i) *El discriminante verifica:*

$$D(U_1,\ldots,U_n) := \prod_{\zeta\in V}\chi'_{\mathcal{U}}\left(\mathcal{U}(\zeta)\right) = \prod_{i=1}^{\mathscr{D}}\chi'_{\mathcal{U}}\left(\mathcal{U}(\zeta_i)\right) = \prod_{i=1}^{\mathscr{D}}\left(\prod_{j\neq i}\left(\mathcal{U}(\zeta_i-\zeta_j)\right)\right.\left.\right).$$

ii) *Las demás derivadas verifican, para cada $\zeta \in V$:*

$$\frac{\partial \chi_{\mathcal{U}}}{\partial U_i}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) = \pi_i(\zeta)\frac{\partial \chi_{\mathcal{U}}}{\partial T}(U_1,\ldots,U_n,\mathcal{U}(\zeta)).$$

DEMOSTRACIÓN. Es una mera comprobación a partir de las definiciones de las distintas funciones. □

PROPOSICIÓN 4.5.4. *Con las notaciones anteriores, sea $u := (u_1,\ldots,u_n) \in K^n$ un punto en el espacio afín sobre $K$ de tal modo que*

$$D(u_1,\ldots,u_n) \neq 0.$$

*Denotemos también por $u : \mathbb{K}^n \longrightarrow \mathbb{K}$ la aplicación lineal definida por $u$ mediante:*

$$u(X_1,\ldots,X_n) := u_1X_1 + \cdots + u_nX_N \in K[X_1,\ldots,X_n].$$

*Se verifica:*

i) *La forma lineal $u \in K[X_1, \ldots, X_n]$ es una forma separante para $V$.*

ii) *El polinomio eliminante $\chi_u(T) \in K[T]$ de la forma lineal $u$ verifica:*

$$\chi_u(T) = \chi_{\mathcal{U}}(u_1, \ldots, u_n, T) \in K[T].$$

iii) *Se verifica la siguiente propiedad:*

$$q_i(u(X_1, \ldots, X_n)) = X_i R(u(X_1, \ldots, X_n)) \in \sqrt{\mathfrak{a}} = I_K(V),$$

*donde*

$$q_i(T) := \frac{\partial \chi_{\mathcal{U}}}{\partial U_i}(u_1, \ldots, u_n, T) \in K[T],$$

*y*

$$q_i(u(X_1, \ldots, X_n)) \in K[X_1, \ldots, X_n],$$

*mientras que:*

$$R(T) := \chi'_u(T) = \frac{\partial \chi_{\mathcal{U}}}{\partial T}(u_1, \ldots, u_n, T) \in K[T]),$$

*y*

$$R(u(X_1, \ldots, X_n)) = \frac{\partial \chi_{\mathcal{U}}}{\partial T}(u_1, \ldots, u_n, u(X_1, \ldots, X_n)) \in K[X_1, \ldots, X_n]).$$

Demostración. Las primeras dos afirmaciones son obvias a partir de las definiciones de los polinomios involucrados. Para la afirmación iii) obsérvese que la Proposición prcedente nos dice que para toda lista de variables $\{U_1, \ldots, U_n\}$ y para todo $\zeta \in \zeta$ se tiene:

$$\frac{\partial \chi_{\mathcal{U}}}{\partial U_i}(U_1, \ldots, U_n, \mathcal{U}(\zeta)) = \pi_i(\zeta) \frac{\partial \chi_{\mathcal{U}}}{\partial T}(U_1, \ldots, U_n, \mathcal{U}(\zeta)).$$

Por tanto, se tiene también,

$$q_i(u(\zeta)) - \pi_i(\zeta) R(u(\zeta)) = 0,$$

para todo $\zeta \in V$. Si escribo el polinomio

$$h(X_1, \ldots, X_n) := q_i(u(X_1, \ldots, X_n)) = X_i R(u(X_1, \ldots, X_n)) \in K[X_1, \ldots, X_n],$$

verifica que

$$h(\zeta) = q_i(u(\zeta)) - \pi_i(\zeta) R(u(\zeta)) = 0, \ \forall \zeta \in V.$$

Por tanto

$$h(X_1, \ldots, X_n) \in I_K(V) = \sqrt{\mathfrak{a}},$$

usando el Nullstellensatz. Y tenemos probada la afirmación iii) y el enunciado. □

Observación 4.5.5 (**Solución mediante isomorfismo birracional)**. La anterior Proposición nos da una representación de $V$ mediante un siomorfismo birracional con una subvariedad de dimensión cero de $\mathbb{K}$. El isomorfismo birracional viene dado por considerar $W \subseteq \mathbb{K}$ dado mediante:

$$W := \{z \in \mathbb{K} \ : \ \chi_u(z) = 0\}.$$

El isomorfismo birracional viene dado mediante las dos aplicaciones (una inversa de la otra siguientes:

$$\begin{array}{rccc} u: & V & \longrightarrow & W \\ & \zeta & \longrightarrow & u(\zeta) := u_1\zeta_1 + \cdots + u_n\zeta_n. \end{array}$$

Y su inversa es dada mediante:

$$\begin{array}{rccc} u^{-1}: & W & \longrightarrow & V \\ & z & \longrightarrow & u^{-1}(z) := \left(\frac{q_1(z)}{R(z)}, \ldots, \frac{q_n(z)}{R(z)}\right) \end{array}$$

De hecho, el único punto importante es la buena definición de $u^{-1}$ pero esto está garantizado por la condición $D(u_1, \ldots, u_n) \neq 0$. Como $D(u_1, \ldots, u_n)$ es el discriminante

de $\chi_u(T)$ y como $R(T)$ es la derivada de $\chi_u(T)$, entonces, no hay cero de $\chi_u(T)$ en el que se anule en $\chi'_u(T)$, es decir, $\chi'_u(z) \neq 0$ para todo $z \in W$, garantizando que $u^{-1}$ está bien definido sobre $W$. Algunos autores prefieren la terminología *Resolución Racional Univariada* o RUR (como, por ejemplo, en la Tesis de F. Rouillier[9] y sus trabajos y referencias de ese período.) a una representación de $V$ mediante isomorfismo birracional.

COROLLARIO 4.5.6 (**Resolución "à la Kronecker" desde la Forma de Cayley-Chow**). *Con las notaciones anteriores, sea $u := (u_1, \ldots, u_n) \in K^n$ un punto en el espacio afín sobre $K$ de tal modo que*

$$D(u_1, \ldots, u_n) \neq 0.$$

*Denotemos también por $u : \mathbb{K}^n \longrightarrow \mathbb{K}$ la aplicación lineal definida por $u$ mediante:*

$$u(X_1, \ldots, X_n) := u_1 X_1 + \cdots + u_n X_N \in K[X_1, \ldots, X_n].$$

*La siguiente información nos da una resolución "à la Kronecker" de la variedad cero-dimensional $V$:*

i) *La forma lineal $u \in K[X_1, \ldots, X_n]$ es una forma separante para $V$.*
ii) *El polinomio eliminante $\chi_u(T) \in K[T]$ de la forma lineal $u$ verifica:*

$$\chi_u(T) = \chi_{\mathcal{U}}(u_1, \ldots, u_n, T) \in K[T].$$

iii) *El discriminante $\rho \in K \setminus \{0\}$ viene dado mediante la siguiente identidad:*

$$\rho := D(u_1, \ldots, u_n)$$

iv) *Las parametrizaciones vienen dadas mediante las siguientes propiedades: Sean $A, B \in K[U_1, \ldots, U_n, T]$ tales que*

$$D(U_1, \ldots, U_n) = A\chi_{\mathcal{U}} + B\chi'_{\mathcal{U}}.$$

*Para cada $i$, $1 \leq i \leq n$ consideremos los polinomios:*

$$Q_i(U_1, \ldots, U_n, T) := \frac{\partial \chi_{\mathcal{U}}}{\partial U_i}(U_1, \ldots, U_n, T) \in K[U_1, \ldots, U_n, T],$$

*y sus especializaciones:*

$$q_i(u_1, \ldots, u_n, T) \in K[T].$$

*Definamos*

$$V_i(U_1, \ldots, U_n, T) := rem_T(B \cdot Q_i, \chi_{\mathcal{U}}),$$

*donde $rem_T$ quiere decir cálculo del resto para una división univariada (con respecto a la variable $T$) con divisor $\chi_{\mathcal{U}}(T)$, que es mónico con respecto a la variable $T$. Entonces, una parametrización de $V$ viene dada mediante:*

$$v_i(T) := V_i(u_1, \ldots, u_n, T) \in K[T],$$

*y*

$$\rho X_i - v_i(u(X_1, \ldots, X_n)) \in \sqrt{\mathfrak{a}}.$$

DEMOSTRACIÓN. Las propiedades i) y ii) se siguen de la Proposición anterior. La propiedad iii) necesita un poco más de reflexión. De una parte, la Proposición precedente nos dice que para cada $\zeta = (\zeta_1, \ldots, \zeta_n) \in V$ se tiene:

$$\frac{\partial \chi_{\mathcal{U}}}{\partial U_i}(U_1, \ldots, U_n, \mathcal{U}(\zeta)) = \pi_i(\zeta) \frac{\partial \chi_{\mathcal{U}}}{\partial T}(U_1, \ldots, U_n, \mathcal{U}(\zeta)).$$

Especializando las variables $U_i$ en las constantes $u_i$ obtenemos que tambié es cierto:

$$\frac{\partial \chi_{\mathcal{U}}}{\partial U_i}(u_1, \ldots, u_n, u(\zeta)) = \pi_i(\zeta) \frac{\partial \chi_{\mathcal{U}}}{\partial T}(u_1, \ldots, u_n, u(\zeta)).$$

[9] F. Rouillier, *"Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux"*. Thèse, Université de Rennes I, 1996.

De otro lado, tenemos que se tiene

$$D(U_1,\ldots,U_n) = A\chi_{\mathcal{U}} + B\chi'_{\mathcal{U}}.$$

Multiplicando for $B$ tenemos que para todo $\zeta \in V$, y recuperando las notaciones del enunciado, tenemos la siguiente igualdad en $\mathbb{K}[U_1,\ldots,U_n,T]$:

(4.5.1)
$$B(U_1,\ldots,U_n,\mathcal{U}(\zeta))Q_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) = \pi_i(\zeta)B(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi'_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)).$$

Pero, además,

$$\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) = 0, \forall \zeta \in V.$$

Pero, además,

$$A\cdot\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) = 0, \forall \zeta \in V.$$

Por tanto, desde la Ecuación (4.5.1) anterior, concluimos que $\forall \zeta \in V$ se tiene:
(4.5.2)
$$B(U_1,\ldots,U_n,\mathcal{U}(\zeta))Q_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + \pi_i(\zeta)A(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) =$$

$$= \pi_i(\zeta)B(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi'_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + \pi_i(\zeta)A(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)).$$

Pero, tenemos que:

$$\pi_i(\zeta)D(U_1,\ldots,U_n) =$$

$$= \pi_i(\zeta)B(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi'_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + \pi_i(\zeta)A(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)).$$

Luego la Ecuación (4.5.2) se convierte en la siguiente para todo $\zeta \in V$:

(4.5.3)
$$B(U_1,\ldots,U_n,\mathcal{U}(\zeta))Q_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + \pi_i(\zeta)A(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) =$$

$$= \pi_i(\zeta)D(U_1,\ldots,U_n).$$

De otro lado, haciendo divisón con respecto a la variable $T$ en $K[U_1,\ldots,U_n,T]$ y aprovechando que $\chi_{\mathcal{U}}$ es mónico con respecto a $T$, existirán $R_i, V_i \in K[U_1,\ldots,U_n,T]$ tales que

$$B(U_1,\ldots,U_n,T)Q_i(U_1,\ldots,U_n,T) = R_i\chi_{\mathcal{U}}(U_1,\ldots,U_n,T) + V_i(U_1,\ldots,U_n,T),$$

El polinomio $V_i$, cuyo grado en $T$ es menor estricto que el grado en $T$ de $\chi_{\mathcal{U}}$ es lo que hemos llamado el $rem_T$ en el enunciado. Entonces, para cada $\zeta \in V$ tendremos:

$$B(U_1,\ldots,U_n,\mathcal{U}(\zeta))Q_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + \pi_i(\zeta)A(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) =$$
$$V_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + H(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)),$$

donde

$$H(U_1,\ldots,U_n,\mathcal{U}(\zeta)) = \left(R_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + \pi_i(\zeta)A(U_1,\ldots,U_n,\mathcal{U}(\zeta))\right).$$

Pero, como $\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) = 0$, para cada $\zeta \in V$, concluimos:

$$B(U_1,\ldots,U_n,\mathcal{U}(\zeta))Q_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) + \pi_i(\zeta)A(U_1,\ldots,U_n,\mathcal{U}(\zeta))\chi_{\mathcal{U}}(U_1,\ldots,U_n,\mathcal{U}(\zeta)) =$$
$$V_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)).$$

Esto último nos lleva a transformar la Ecuación (4.5.3) queda transformada en la siguiente para todo $\zeta \in V$:

$$V_i(U_1,\ldots,U_n,\mathcal{U}(\zeta)) = \pi_i(\zeta)D(U_1,\ldots,U_n). \tag{4.5.4}$$

Especializando las variables $U_i$'s en constantes $u_i$'s obtendremos:

$$V_i(u_1,\ldots,u_n,u(\zeta)) - \pi_i(\zeta)D(u_1,\ldots,u_n) = v_i(u(\zeta)) - \rho\pi_i(\zeta) = 0,\ \forall \zeta \in V. \tag{4.5.5}$$

Ahora, si consideramos el polinomio

$$h(X_1,\dots,X_n) = v_i(u_1X_1+\cdots+u_nX_n) - \rho X_i \in K[X_1,\dots,X_n],$$

tenemos que

$$h(\zeta) = v_i(u(\zeta)) - \rho\pi_i(\zeta) = 0, \forall \zeta \in V.$$

Y esto significa que $v_1,\dots,v_n$ son las parametrizaciones a la Kronecker y que $\rho$ es el discriminete. Adicionalmente, tenemos el isomorfismo birregular entre $V$ y $W := \{z \in \mathbb{K} \,:\, \chi_u(z) = 0\} \subseteq \mathbb{K}$:

$$\begin{array}{rccc} u: & V & \longrightarrow & W \\ & \zeta & \longrightarrow & u(\zeta) := u_1\zeta_1+\cdots+u_n\zeta_n. \end{array}$$

Y su inversa es dada mediante:

$$\begin{array}{rccc} u^{-1}: & W & \longrightarrow & V \\ & z & \longrightarrow & u^{-1}(z) := \left(\rho^{-1}v_1(z),\dots,\rho^{-1}v_n(z)\right). \end{array}$$

□

Estas dos Proposiciones nos llevan a conluir el siguiente enunciado:

Teorema 4.5.7 (**De la forma de Cayley-Chow a la solución "à la Kronecker"**). *Existe un algoritmo probabilista que realiza la taerea siguiente:*
*Sea $K$ un cuerpo perfecto, $\mathbb{K}$ un algebraicamente cerrado que contiene a $K$, $\mathfrak{a}$ un ideal cero-dimensional en $K[X_1,\dots,X_n]$, $V := V\mathbb{K}(\mathfrak{a})$ la variedad cero dimensional definida por $\mathfrak{a}$. Entonces, el algoritmo computa, tomando como* Input *una forma de Cayley-Chow de $V$, una solución "à la Kronecker" de $V$.*
*El tiempo de ejecución del algoritmo es, en operaciones sobre el cuerpo base $K$, polinomial en $n$ y $\mathscr{D}$, donde $\mathscr{D} = \deg(V)$.*

Demostración. Es esencialmente lo descrito en las Proposiciones precendentes, pero lo expresamos en forma de algoritmo:

---

Input: La forma de Cayley-Chow:

$$\chi_{\mathcal{U}}(U_1,\dots,U_n,T) \in K[U_1,\dots,U_n,T].$$

**Hallar Las derivadas parciales y el discriminante:**

- La derivada con respeto a $T$:

$$\chi'_{\mathcal{U}}(U_1,\dots,U_n,T) := \frac{\partial\chi_{\mathcal{U}}(T)}{\partial T}(U_1,\dots,U_n,T) \in K[U_1,\dots,U_n,T].$$

- Las derivadas parciales con respecto a las otras variables:

$$Q_i(U_1,\dots,U_n,T) := \frac{\partial\chi_{\mathcal{U}}(T)}{\partial U_i}(U_1,\dots,U_n,T) \in K[U_1,\dots,U_n,T].$$

- El discriminante genérico:

$$D(U_1,\dots,U_n) := \det(q_i(U_1,\dots,U_n,C(\chi_{\mathcal{U}}))) \in K[U_1,\dots,U_n],$$

  donde $C(\chi_{\mathcal{U}})$ es la matriz compañera de $\chi_{\mathcal{U}}$ con respecto a la variable $T$.

**Hallar los coeficientes de la identidad de Bézout** del Discriminante. Es decir, polinomios $A, B \in K[U_1,\dots,U_n,T]$ tales que:

$$D(U_1,\dots,U_n) = A\chi_{\mathcal{U}} + B\chi'_{\mathcal{U}}.$$

**Hallar el resto de la división por $\chi_{\mathcal{U}}$:**

$$V_i(U_1,\dots,U_n,T) := rem_T(B\cdot Q_i, \chi_{\mathcal{U}}),$$

**Aplicar Tests de Nulidad de polinomios para hallar:** $u \in \mathbb{K}^n$ tal que:

$$D(u_1,\dots,u_n) = 0.$$

OUTPUT: La información siguiente:

- La forma separante $u := u_1X_1 + \cdots + u_nX_n$.
- El plinomio mínimo de la forma separante:
$$\chi_u(T) := \chi_{\mathcal{U}}(u_1, \ldots, u_n, T) \in K[T].$$
- Las parametrizaciones:
$$v_i(T) := V_i(u_1, \ldots, u_n, T).$$
- El discriminante:
$$\rho := D(u_1, \ldots, u_n) \in K \setminus \{0\}.$$

---

Este algoritmo realiza la tarea indicada y, en sus cálculos, todo lo que hace es Álgebra Lineal en dimensión $\mathscr{D}$, aunque a veces, en $K(U_1, \ldots, U_n)$ (pero éso, mediante SLP's, es manejable en tiempo polinomial en $\mathscr{D}$ y $n$). □

## 4.6. Objetivo del Curso: Algoritmos Intrínsecos

El objetivo de esta segunda parte del curso sería probar que se verifica el siguiente resultado:

TEOREMA 4.6.1. *Existe un algoritmo probabilista (MonteCarlo) que realiza la siguiente tarea:*
*Sea $K$ un cuerpo perfecto, $\mathbb{K}$ un algebraicamente cerrado que contiene a $K$, $\mathfrak{a}$ un ideal cero-dimensional en $K[X_1, \ldots, X_n]$, $V := V_{\mathbb{K}}(\mathfrak{a})$ la variedad cero dimensional definida por $\mathfrak{a}$. Supongamos que existe una sucesión regular reducida*
$$f_1, \ldots, f_n \in K[X_1, \ldots, X_n],$$
*que genera el ideal $\mathfrak{a}$ (i.e. $\mathfrak{a} = (f_1, \ldots, f_n)$).*
*Entonces, el algoritmo computa, tomando como* INPUT *$f_1, \ldots, f_n$, una solución "à la Kronecker" de $V$.*
*El tiempo de ejecución del algoritmo es, en operaciones sobre el cuerpo base $K$, polinomial en $n$ y $\mathscr{D}$ y $L$, donde $\mathscr{D} = \deg(V) = \prod_{i=1}^{n} \deg(f_i)$ y $L$ es la talla de la representación de los polinomios $f_1, \ldots, f_n$ en cualquier representación razonable elegida.*

La demostración ocupará bastantes Capítulos de cuanto sigue y necesitaremos avanzar en la comprensión de la naturaleza de los objetos geométricos involucrados.

Capítulo 5

# Soluciones mediante ceros aproximados

## 5.1. Bases $L^3-$ reducidas.

### 5.1.1. Retículos en $\mathbb{R}^n$.

Definición 29. *Llamaremos retículo a todo $\mathbb{Z}-$módulo libre de rango n contenido en $\mathbb{R}^n$ y tal que contiene una base de $\mathbb{R}^n$ como espacio vetorial.*

Observación 5.1.1. Obsérvese que la condición de que contiene una base del propio $\mathbb{R}^n$ no es evitable. Un submódulo libre de rango 2 en $\mathbb{R}^2$ es el dado por $\langle(\sqrt{2},0),(\sqrt{3},0)\rangle$. De otro lado la condición rango $n$ sí puede ser evitada si imponemos la frase : un retículo es el $\mathbb{Z}-$módulo libre generado por una base de $\mathbb{R}^n$.

Definición 30. *Dado un retículo $L \subseteq \mathbb{R}^n$ y una base del mismo $v_1,\ldots,v_n$, llamaremos volumen del retículo al volumen del paralelepípedo determinado por esta base, i.e.*

$$vol(L) := \mid det(B) \mid$$

*donde $B \in \mathcal{M}_n(\mathbb{R})$ es la matriz cuyas columnas son los vectores de la base $v_1,\ldots,v_n$.*

Observación 5.1.2. Como los cambios de base en módulos libres se hacen mediante determinantes de valor absoluto 1, esta noción no depende de la base elegida.

Llamaremos discriminante de una base $\{v_1,\ldots,v_n\}$ de $\mathbb{R}^n$ al determinante de la matriz de Wishart asociada a la matriz de coordenadas de los vectores de esa base, esto es:

$$d := \det \begin{pmatrix} \langle v_1,v_1\rangle & \cdots & \langle v_1,v_n\rangle \\ \vdots & \ddots & \vdots \\ \langle v_n,v_1\rangle & \cdots & \langle v_n,v_n\rangle \end{pmatrix}$$

Claramente se tiene

Proposición 5.1.3. *Sea $L$ un retículo de $\mathbb{R}^n$ y sea $v_1,\ldots,v_n$ una base de $L$, entonces el dsicriminante es el cuadrado del volumen, i.e.*

$$vol(L)^2 = det\left((\langle v_i,v_j\rangle)_{1\leq i,j\leq n}\right)$$

Definición 31. *Un subretículo de un retículo $L$ es simplemente un retículo en $\mathbb{R}^n$ contenido en $L$.*

Una bonita propiedad que relaciona el volumen con el gurpo cociente nos muestra que :

Proposición 5.1.4. *dados $L_1 \subseteq L_2$ dos retículos en $\mathbb{R}^n$ se tiene*

$$\sharp(L_2/L_1) = \frac{vol(L_1)}{vol(L_2)}$$

**5.1.2. Bases Reducidas.** Sea $L \subseteq \mathbb{R}^n$ un retículo y $v_1,\ldots,v_n$ una base de $L$. Denotaremos mediante $v_1^*,\ldots,v_n^*$ la base (de $\mathbb{R}^n$) obtenida aplicando el proceso de ortogonalización de Gram–Schmidt a la base $v_1,\ldots,v_n$, i.e.

$$\begin{cases} v_1^* & := & v_1 & \\ v_2^* & := & v_2 - \mu_{2,1}v_1^*, & \mu_{2,1} := \frac{\langle v_2,v_1^*\rangle}{\langle v_1^*,v_1^*\rangle} \\ & \vdots & & \vdots \\ v_i^* & := & v_i - \sum_{j=1}^{i-1}\mu_{i,j}v_j^*, & \mu_{i,j} := \frac{\langle v_i,v_j^*\rangle}{\langle v_j^*,v_j^*\rangle} \end{cases}$$

DEFINICIÓN 32. *Una base $v_1, \ldots, v_n$ de un retículo $L$ se denomina reducida si, con las notaciones anteriores, se tiene :*

$$| \mu_{i,j} | \leq \frac{1}{2}$$

$$||v_i^* + \mu_{i,i-1} v_{i-1}^*||^2 \geq \frac{3}{4} ||v_{i-1}^*||^2$$

Estas exóticas propiedades se canalizan desde la siguiente :

PROPOSICIÓN 5.1.5. *En las notaciones anteriores, sea $v_1, \ldots, v_n$ una base reducida de un retículo $L \subseteq \mathbb{R}^n$. Sean $v_1^*, \ldots, v_n^*$ los vectores obtenidos tras aplicar Gram-Schmidt a esta base. Entonces,*

i) $||v_i^*||^2 \leq ||v_i||^2 \leq 2^{i-1} ||v_i^*||^2$,
ii) $vol(L) \leq \prod_{i=1}^n ||v_i|| \leq 2^{\frac{n(n-1)}{4}} vol(L)$,
iii) $||v_j||^2 \leq 2^{i-1} ||v_i^*||^2$, *para* $1 \leq j \leq i \leq n$.
iv) $||v_1|| \leq 2^{\frac{n-1}{4}} vol(L)^{\frac{1}{n}}$.

DEMOSTRACIÓN. Para la tercera de las afirmaciones, baste observar que :

$$||v_i^*||^2 \geq \frac{1}{2^{i-1}} ||v_1^*||^2 = ||v_1||^2$$

con lo que

$$2^{\frac{n(n-1)}{4}} vol(L)^2 = \prod_{i=1}^n 2^{i-1} ||v_i^*||^2 \geq \prod_{i=1}^n ||v_1||^2$$

Tomando raices $2n-$ésimas a ambos lados tenemos la desigualdad buscada. □

OBSERVACIÓN 5.1.6. La primera de las desigualdades de *ii*) hace referencia a la famosa desigualdad de Hadamard y no necesita la condición de reducida para probarse.
En cuanto a la segunda desigualdad de *ii*) es una de las etapas de un enunciado del texto de Cassels [**Ca, 71**], ch. VIII. Nos falta probar la existencia de bases reducidas.

Veamos algunas consecuencias de esta Proposición (que se relacionan con las ideas de Minkowski sobre bases minimales)

PROPOSICIÓN 5.1.7. *Sea $L$ un retículo y sea $v_1, \ldots, v_n$ una base reducida. Entonces, para cada $x \in L, x \neq 0$, se tiene :*

$$||v_1||^2 \leq 2^{n-1} ||x||^2$$

DEMOSTRACIÓN. Este resultado se sigue observando la relación que hay entre las coordenadas de cada elemento $x \in L$ en función de la base del retículo y de la base obtenida por Gram–Schmidt, es decir :

$$x = \sum_{i=1}^n r_i^* v_i^* = \sum_{i=1}^n r_i v_i$$

entonces, por la ortogonalidad se sigue que :

$$||x||^2 := \sum_{i=1}^n r_i^2 ||v_i^*||^2$$

Ahora bien, las coordenadas se relacionan mediante :

$$\begin{pmatrix} 1 & \mu_{2,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \cdots & \mu_{n,2} \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & \mu_{n,n-1} \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} r_1^* \\ \vdots \\ r_n^* \end{pmatrix}.$$

Por lo tanto, si $k$ es el máximo índice tal que $r_k \neq 0$ tendremos que $r_k = r_k^* \in \mathbb{Z}$. Finalmente concluimos

$$||x||^2 \geq (r_k^*)^2||v_k^*||^2 \geq ||v_k^*||^2$$

Usando la última de las cotas de la Proposición anterior se sigue el resultado. □

De modo análogo se tiene la siguiente Proposición que es simplemente una extensión via inducción.

PROPOSICIÓN 5.1.8. *Sea $L$ un retículo y sea $v_1, \ldots, v_n$ una base reducida. Sean $x_1, \ldots, x_t \in L$ elementos linelamente independientes. Entonces, para $1 \leq i \leq t$ se tiene*

$$||v_i||^2 \leq 2^{n-1} max\{||x_i||^2 : \ 1 \leq i \leq t\}$$

### 5.1.3. Un algoritmo de Cálculo de las Bases $L^3-$reducidas.

DEFINICIÓN 33. *Sea $v_1, \ldots, v_n$ una base de un retículo $L$ en $\mathbb{R}^n$. Definiremos el volumen determinado por los menores diagonales del modo siguiente :*

$$d_k := det\left((\langle v_i, v_j\rangle)_{1\leq i,j\leq k}\right)$$

$$D := \prod_{i=1}^{n-1} d_k$$

Una simple observación nos recuerda que el proceso de ortogonalización de Gram-Schmidt es inductivo y depende del orden; pero es incremental, con lo cual se tiene :

PROPOSICIÓN 5.1.9. *Con las anteriores notaciones, sean $v_1^*, \ldots, v_n^*$ los vectores obtenidos aplicando Gram–Schmidt a la base del retículo $L$ dada. Entonces,*

$$d_k := \prod_{i=1}^{k} ||v_i^*||^2$$

Para el diseño del proceso $L^3$ bastará con que tengamos en cuenta el efecto sobre $D$ y $d_k$ de ciertos cambios de base en el retículo.

PROPOSICIÓN 5.1.10. *Sean $v_1, \ldots, v_n$ una base ordenada de un retículo $L$ de $\mathbb{R}^n$. Sean $d_k$ y $D$ los volúmenes de los menores principales, i.e.*

$$d_k := det\left((\langle v_i, v_j\rangle)_{1\leq i,j\leq k}\right)$$

$$D := \prod_{i=1}^{n-1} d_k$$

*y sean*

$$\mu_{i,j} := \frac{\langle v_i, v_j^*\rangle}{\langle v_j^*, v_j^*\rangle}$$

*con $1 \leq i < j \leq n$, las constantes que aparecen en el proceso de ortogonalización de Gram–Schmidt.*
*Sea $r \in \mathbb{Z}$ y consideremos una nueva base del retículo $w_1, \ldots, w_n \in L$ dada mediante :*

$$w_i := v_i, \quad i \neq k$$

$$w_k := v_k - rv_l, \quad \text{para algún } l \ \ 1 \leq l < k$$

*Sean $\overline{d_k}$ y $\overline{D}$ los volúmenes de los menores principales determinados por la nueva base, i.e.*

$$\overline{d_k} := det\left((\langle w_i, w_j\rangle)_{1\leq i,j\leq k}\right)$$

$$\overline{D} := \prod_{i=1}^{n-1} \overline{d_k}$$

*y sean*

$$\overline{\mu_{i,j}} := \frac{\langle w_i, w_j^* \rangle}{w_j^*, w_j^* \rangle}$$

*las constantes que aparecen el el proceso de ortogonalización de Gram–Schmidt aplicado a la nueva base.*
*Entonces, se producen las siguientes variaciones :*

$$\begin{gathered} \overline{d_k} = d_k, \quad \overline{D} = D \\ \overline{\mu_{k,j}} = \mu_{k,j}, \quad l\langle j \leq k-1 \\ \overline{\mu_{k,l}} = \mu_{k,l} - r \end{gathered}$$

La otra operación posible de cambio de base en un retículo viene dada por la operación cambio de orden de los elementos de una base. Esta operación se utilizará solamente en un caso excepcional :

PROPOSICIÓN 5.1.11. *Sean $v_1, \ldots, v_n$ una base ordenada de un retículo $L$ de $\mathbb{R}^n$. Sean $d_k$ y $D$ los volúmenes de los menores principales. Supongamos que la base obtenida tras el proceso de ortogonalización de Gram–Schmidt verifica :*

$$||v_k^* + \mu_{k,k-1} v_{k-1}^*||^2 < \frac{3}{4}||v_{k-1}^*||^2$$

*Consideremos una nueva base del retículo $w_1, \ldots, w_n \in L$ dada mediante :*

$$w_i := v_i, \quad i \neq k, k-1$$

$$w_k := v_{k-1}, \quad w_{k-1} := v_k$$

*Sean $\overline{d_k}$ y $\overline{D}$ los volúmenes de los menores principales determinados por la nueva base, $\overline{\mu_{i,j}}$ las constantes que aparecen el el proceso de ortogonalización de Gram–Schmidt aplicado a la nueva base. Entonces, se tiene :*

i) $\overline{d_i} = d_i$ *para todo* $i \neq k-1$,
ii) $\overline{d_{k-1}} \leq \frac{3}{4} d_{k-1}$,
iii) $\overline{D} \leq \frac{3}{4} D$.

Con estas dos operaciones elementales estamos en condiciones de definir un procedimiento que calcula bases reducidas de retículos del modo siguiente :

---

SUBALGORITMO GRAM–SCHMIDT($\beta$) :
INPUT : Una base $v_1, \ldots, v_n \in \mathbb{Z}^n$ de un retículo $L \subset \mathbb{R}^n$.
OUTPUT :

*La base de la ortogonalización de Gram-Schmidt :

$$\beta^* := (v_1^*, \ldots, v_n^*) \in (\mathbb{Q}^n)^n$$

* Las constantes del proceso :

$$\mu_{i,j} := \frac{\langle v_i, v_j^* \rangle}{\langle v_j^*, v_j^* \rangle}$$

---

PROCEDIMIENTO DE CÁLCULO DE BASES $L^3-$REDUCIDAS
INPUT : Una base $v_1, \ldots, v_n \in \mathbb{Z}^n$ de un retículo $L \subset \mathbb{R}^n$.
OUTPUT : Una base reducida $w_1, \ldots, w_n \in \mathbb{Z}^n$ del mismo retículo $L$.

---

*Inicializar :*
$\beta := (v_1, \ldots, v_n) \in (\mathbb{Z}^n)^n$,
$k := 2$.
*while* $k < n+1$ *do* $L^3(\beta, k)$
*output* $\beta$
*end*

---

PROCEDIMIENTO $L^3(\beta, k)$ :
INPUT :
* Una base $\beta := (v_1, \ldots, v_n) \in \mathbb{Z}^n$ de un retículo $L \subset \mathbb{R}^n$,
* $k \leq n$.
OUTPUT :
* Una base $\beta := (w_1, \ldots, w_n) \in \mathbb{Z}^n$ del mismo retículo $L$.
* $k \leq n+1$,

---

*Input* $\beta$, $k$
* $Gram - Schmidt(\beta)$
* Hallar el número entero $r$ más próximo a $\mu_{k,k-1}$, i.e.

$$r \in \mathbb{Z}, |\mu_{k,k-1} - r| < \frac{1}{2}$$

* $w_i := v_i$, $i \neq k$,
* $w_k := v_k - rv_{k-1}$,
* $\beta := (w_1, \ldots, w_n)$
* $Gram - Schmidt(\beta)$
*if*

$$||v_k^* + \mu_{k,k-1}v_{k-1}^*||^2 < \frac{3}{4}||v_{k-1}^*||^2$$

*then*
* $w_i := v_i, \quad i \neq k, k-1$
* $w_k := v_{k-1}, \quad w_{k-1} := v_k$
* $\beta := (w_1, \ldots, w_n)$,
* $k := max\{k-1, 2\}$,

*else*
* $l := k-2$,
*while* $l \geq 1$ *do*
* Hallar el número entero $r \in \mathbb{Z}$ más próximo a $\mu_{k,l}$
* $w_i := v_i, \quad i \neq k$,
* $w_k := v_k - rv_l$
* $\beta := (w_1, \ldots, w_n)$
* Gram–Schmidt($\beta$),
* $l := l - 1$,
*endwhile*
* $k := k+1$

*endif*
*output* $\beta$, $k$.
*end*

---

TEOREMA 5.1.12 ([**L$^3$, 82**]). *El anterior procedimiento $L^3$ calcula entiempo polinomial bases reducidas para cualquier retículo $L \subseteq \mathbb{R}^n$ dado a través de una base en $\mathbb{R}^n$.*

Demostración. El enunciado así expuesto tiene una formulación más técnica como la siguiente :
Existe una constante universal $c > 0$ tal que el anterior algoritmo $L^3$ calcula una base reducida del retículo $L$, dado por una base $\beta = (v_1, \ldots, v_n) \in (\mathbb{Z}^n)^n$, en tiempo del mismo orden que $(nh)^c$, donde

$$h := max\{log_s|v_{i,j}| \ : \ 1 \leq i, j \leq n\}$$

siendo $v_I = (v_{i,1}, \ldots, v_{i,n})$.
La clave de la demostración consiste en el análisis de las ejecuciones de $L^3(\beta, k)$. En otra palabras, tras $t$ aplicaciones del procedimiento $L^3(\beta, k)$, tenemos una sucesión :

$$\{(\beta_i, k_i) \ : \ 1 \leq i \leq t\}$$

donde $\beta_i$ es una base del retículo $L$ y $1 \leq k_i \leq n + 1$, verificándose :

$$\beta_0 := \beta, \ k_0 := 2$$

$$L^3(\beta_i, k_i) := (\beta_{i+1}, k_{i+1})$$

En particular, se tendrán dos tipos de modificaciones de los índices $k_i$ :

- *Avances :* cuando $k_{i+1} = k_i + 1$,
- *Retrocesos :* cuando $k_{i+1} = max\{k_i - 1, 2\}$.

Sean $a$ el número de avances y $r$ el número de retrocesos. Tendremos :

$$a + r = t, \ a - r + 2 \leq n + 1$$

Finalmente, se $D_i$ el producto de los determinantes de la diagonal principal de la matriz asociada a la base $\beta_i$. Por cada retroceso, este valor disminuye en $(3/4)$ con lo cual, podemos concluir :

$$D_t \leq (3/4)^r D_0$$

Dado que $D_0$ es un número entero, y que los $D_i$ son también números enteros positivos, tendremos :

$$0 \leq D_t \leq (3/4)^r D_0$$

En particular el número de retrocesos posibles está acotado por $2log_2 D_0$. Sea $t \geq 4log_2 D_0 + n - 1$. En ese caso, el número de avances tendrá que ser al menos $a \geq 2log_2 D_0 + n - 1$. Pero $k_t \geq a - r + 2 = n + 1$, en cuyo caso la máquina ha de detenerse tras $t$ iteraciones del proceso. Luego *se trata de un algoritmo que para en todas las entradas.*

□

## 5.2. Aplicación a la Factorización de Polinomios.

Esta fase final consiste en relacionar factorización y bases reducidas. Ya estaba iniciada en el trabajo de A.K. Lenstra[1], que es el motor de los resultados de $L^3$.
Consideraremos las siguientes condiciones :

i) Sea $f \in \mathbb{Z}[X]$ un polinomio primitivo, $d = deg(f)$, libre de cuadrados.
ii) Sea $p$ un número primo tal que
   *a)* $\overline{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ es un polinomio libre de cuadrados[2] ,
   *b)* $deg(\overline{f}) = deg(f)$, esto es, el coeficiente director de $f$ es no nulo módulo $p$.
iii) Sea $h \in \mathbb{Z}[X]$ un polinomio mónico de grado $\ell \rangle 0$, verificando las propiedades siguientes :
   - $\overline{h} \mid \overline{f}$ en $\mathbb{Z}/p\mathbb{Z}[X]$.
   - $\overline{h} \mid \overline{f}$ en $\mathbb{Z}/p^k\mathbb{Z}[X]$.

[1] A. K. Lenstra. "Lattices and Factorization of Polynomials". Report IW 190, 81. Amsterdam Mathematisch Centrum (1981).

[2] Nótese que, entonces, es también libre de cuadrados en $\mathbb{Z}/p^k\mathbb{Z}[X]$ para cualquier $k \geq 1$ : es una cuestión de manejo del discriminante.

- $\overline{h}$ es irreducible en $\mathbb{F}_p[X]$.

PROPOSICIÓN 5.2.1. *En las anteriores hipótesis, existe un único factor (salvo signo) $h_0$ irreducible de $f$ en $\mathbb{Z}[X]$ tal que*

$$\overline{h} \mid \overline{h_0}$$

*en $\mathbb{F}_p[X]$.*

DEMOSTRACIÓN. Como $\overline{h}$ es irreducible en $\mathbb{F}_p[X]$ es claro que divide a algún factor irreducible de $\overline{f}$; pero como este polinomio es libre de cuadrados (en $\mathbb{F}_p[X]$), no puede dividir a ningún otro. □

Definamos el siguiente retículo :

$$L_m(h) := \{g \in \mathbb{Z}[X] \ : \ deg(g) \leq m, \ \ \overline{h} \mid \overline{g} \ \text{ en } \ \mathbb{Z}/p^k\mathbb{Z}[X]\}$$

Entonces, se tiene el siguiente :

TEOREMA 5.2.2 ([L³, 82]). *Con las anteriores notaciones e hipótesis, sea dada una base $L^3-$reducida del retículo $L_m(h)$ : $b_1, \ldots, b_{m+1}$.*
*Si*

$$p^{k\ell} > 2^{\frac{dm}{2}} 2^{dm} ||f||^{m+d}$$

*se tiene*

$$h_0 \in L_m(h) \Leftrightarrow ||b_1|| < \left(\frac{p^{k\ell}}{||f||^m}\right)^{\frac{1}{d}}$$

*Más aún, sea $t \in \{1, \ldots, m+1\}$ el índice máximo tal que :*

$$||b_j|| < \left(\frac{p^{kl}}{||f||^m}\right)^{1/d} \tag{5.2.1}$$

*Entonces,*

$$h_0 = mcd(b_1, \ldots, b_t)$$

Para la demostración, veamos diversos resultados intermedios. Para comenzar, obsérvense las siguientes propiedades relativas al retículo $L_m(h)$

- Una base de $L_m(h)$ como $\mathbb{Z}-$módulo y, por ende, como retículo es la dada por el siguiente conjunto :

  $$\{X^i h \ : \ 0 \leq i \leq m - \ell\} \cup \{p^k X^j \ : \ 0 \leq j \leq \ell - 1\}.$$

- tiene volumen independiente de $m$ :

  $$vol(L_m(h)) = p^{k\ell}$$

  La razón es simple : $h$ ha sido elegido mónico y basta con considerar la base descrita anteriormente.
- Para cualquier base reducida $b_1, \ldots, b_{m+1}$ se tiene :

  $$||b_1|| \leq 2^{\frac{d-1}{4}} vol(L_m(h))^{\frac{1}{d}} \leq 2^{\frac{d-1}{4}} p^{\frac{k\ell}{d}}$$

Comenzamos con la siguiente observación :

PROPOSICIÓN 5.2.3. *En las hipótesis y notaciones anteriores, para cada divisor $g$ de $f$, las siguientes propiedades son equivalentes :*

i) $\overline{h} \mid \overline{g}$ *en* $\mathbb{F}_p[X]$.
ii) $\overline{h} \mid \overline{g}$ *en* $\mathbb{Z}/p^k\mathbb{Z}[X]$.
iii) $h_0$ *divide a* $g$ *en* $\mathbb{Z}[X]$.

DEMOSTRACIÓN. Como $g$ es un divisor de $f$ y $f$ es libre de cuadrados (por serlo $\overline{f}$) $g$ es un producto de factores irreducibles y primitivos de $f$. Ahora la disquisición está en que $h_0$ divida o no divida a $g$. Si $h_0$ no divide a $g$, malamente puede ocurrir que $\overline{h}$ divida a $\overline{g}$ en $\mathbb{F}_p[X]$, pues esta condición caracteriza completamente a $h_0$. Luego si $\overline{h} \mid \overline{g}$, automáticamente, $h_0 \mid g$ en $\mathbb{Z}[X]$. Tenemos $i) \Rightarrow iii)$. Las condiciones $iii) \Rightarrow i)$ y $ii) \Rightarrow i)$ se verifican obviamente.
Nos queda $i) \Rightarrow ii)$. Sea $f_1 \in \mathbb{Z}[X]$ el polinomio dado por $f/g$. Puesto que $\overline{f}$ no posee factores múltiples, $\overline{h}$ y $\overline{f_1}$ son comaximales en $\mathbb{F}_p[X]$. Sean $\lambda, \mu, \nu \in \mathbb{Z}[X]$ tales que :

$$\lambda h + \mu f_1 = 1 - p\nu$$

igualdad que se verifica en $\mathbb{Z}[X]$. Ahora multipliquemos a ambos lados por $g$ y la suma $1 + p\nu + \cdots + p^{k-1}\nu^{k-1}$. Obtendremos :

$$g(1 + p\nu + \cdots + p^{k-1}\nu^{k-1})(\lambda h + \mu f_1) = (1 - p^k\nu^k)g$$

Luego, la siguiente igualdad se da en $\mathbb{Z}[X]$ :

$$\Big(g(1 + p\nu + \cdots + p^{k-1}\nu^{k-1})\lambda h + (1 + p\nu + \cdots + p^{k-1}\nu^{k-1})\mu f\Big) + p^k\nu^k g = g$$

Tomando clases módulo $p^k$ tendremos una igualdad similar válida en $\mathbb{Z}/p^k\mathbb{Z}[X]$; pero como $\overline{h}$ divide a $\overline{f}$ en $\mathbb{Z}/p^k\mathbb{Z}[X]$ obtendremos la igualdad :

$$\overline{\Big(g(1 + p\nu + \cdots + p^{k-1}\nu^{k-1})\lambda + (1 + p\nu + \cdots + p^{k-1}\nu^{k-1})\mu(\frac{\overline{f}}{\overline{h}}\Big)\overline{h} = \overline{g}}$$

□

La detección de tales factores $g$ de $f$ divisibles por $h_0$ y, por lo tanto, de una posible cota para el grado de $h_0$ viene de la mano de la siguiente propiedad métrica :

PROPOSICIÓN 5.2.4. *En las anteriores notaciones e hipótesis, supongamos $b \in L_m(h)$ tal que :*

$$||f||^m||b||^d < p^{k\ell}$$

*Entonces, $b$ es divisible por $h_0$ en $\mathbb{Z}[X]$. En particular, $mcd(f, b) \neq 1$*

DEMOSTRACIÓN. Supongamos que $b \neq 0$. Sea $g = mcd(b, f)$. Adicionalmente, supongamos :

- $e = deg(g)$,
- $m' = deg(b) \leq m$.

Consideremos el siguiente módulo :

$$M := \{\lambda f + \mu b \ : \ \lambda, \mu \in \mathbb{Z}[X], deg(\lambda) < m' - e, deg(\mu) < d - e\}$$

Sea $\mathbb{Z}[X]_{m'+d-e-1}$ el $\mathbb{Z}-$módulo de todos los polinomios de grado acotado por $m' + d - e - 1$. Claramente, tenemos que $M$ es un submódulo de $\mathbb{Z}[X]_{m'+d-e-1}$.
Consideremos la siguiente proyeccin :

$$\pi \ : \mathbb{Z}[X]_{m'+d-e-1} \longrightarrow \mathbb{Z}[X]_{m'+d-e-1}/\mathbb{Z}\langle 1, X, \ldots, X^{e-1}\rangle \equiv \mathbb{Z}^{m'+d-2e} \subseteq \mathbb{R}^{m'+d-2e}.$$

$$q \longmapsto [q],$$

donde

$$q := a_{m'+d-e-1}X^{m'+d-e-1} + \cdots + a_0 \longmapsto [q] := a_{m'+d-e-1}X^{m'+d-e-1} + \cdots + a_eX^e.$$

Consideramos $\pi(M) \subseteq \mathbb{Z}^{m'+d-2e}$. Como primera observación, *el siguiente conjunto constituye una base de $\pi(M)$ :*

$$\{X^i[f] \ : \ 0 \leq i < m' - e\} \cup \{X^j[b] \ : \ 0 \leq j < d - e\}.$$

Para demostrar este resultado, baste con observar que si $\nu \in M$ y $\pi(\nu) \in \pi(M)$, se tiene, obviamente que $[\nu]$ es combinacin $\mathbb{Z}-$lineal de estos parmetros. Para ver que es libre, supongamos :

$$\lambda[f] + \mu[b] = 0 \Rightarrow q := \lambda f + \mu b \in \mathbb{Z}[X]_{e-1}.$$

Por tanto, como el grado del mximo comn divisor de $f$ y $b$ es $e$, concluimos $q = 0$. Por tanto,

$$\lambda f + \mu b = 0.$$

Dado que $g$ es el mximo comn divisor de $f$ y $b$, se tendr :

$$\lambda(\frac{f}{g}) = -\mu(\frac{b}{g}).$$

Por tanto,

$$\frac{b}{g} \mid \lambda.$$

Pero,

$$deg(\lambda) < m' - e = deg(\frac{b}{g}).$$

Con lo que llegamos a contradicción salvo que $\lambda = 0$. Adicionalmente, $\mu = 0$ y habremos terminado. Tenemos que $\pi(M)$ es un retículo en $\mathbb{R}^{m'+d-2e}$. Usando la desigualdad de Hadamard :

$$vol(\pi(M)) \leq \prod_{i=0}^{m'-e-1} \|X^i[f]\| \prod_{i=0}^{d-e-1} \|X^i[b]\| \leq \|f\|^m \|b\|^d < p^{k\ell}.$$

De otro lado, supongamos que $gcd(f, b) = 1$. Entonces, se tiene $e = 0$ y $\overline{h}$ divide a $\overline{f}$ en $\mathbb{Z}/p^k\mathbb{Z}[X]$ y a $\overline{b}$ en $\mathbb{Z}/p^k\mathbb{Z}[X]$ (pues $b \in L_m(h)$). Por tanto,

$$\pi(M) = M \subseteq L_m(h).$$

En particular,

$$vol(M) = vol(\pi(M)) \geq vol(L_m(h)) = p^{k\ell}.$$

Con lo que hemos llegado a contradicción. Como $e > 1$ y $\overline{h} \mid \overline{b}$, tendremos $\overline{h} \mid \overline{g}$ y $g$ es un divisor de $f$. Luego $h_0$ divide a $g$ y, por ende, a $b$ y habremos terminado.

□

Proposición 5.2.5. *Sean $p, k, f, d, h, \ell$ con las notaciones usadas a lo largo de esta Subsección y con análogas propiedades. Sea $h_0$ el factor irreducible de $f$ asociado a $h$, $m$ y $L_{\ell,m}$ como en la Proposición anterior. Supongamos que $b_1, \ldots, b_{m+1}$ es una base reducida de $L_{\ell,m}$ y que se verifica la siguiente desigualdad :*

$$p^{k\ell} > 2^{dm/2} 2^{dm} ||f||^{m+d}$$

*Entonces, tenemos $deg(h_0) \leq m$ si y solamente si :*

$$|| b_1 || < \left(\frac{p^{k\ell}}{|| f ||^m}\right)^{\frac{1}{d}}$$

Demostración. Dada la desigualdad :

$$|| b_1 || < \left(\frac{p^{k\ell}}{|| f ||^m}\right)^{\frac{1}{d}}$$

podemos concluir

$$|| b_1 ||^d || f ||^m < p^{k\ell}$$

luego la condición es suficiente en vista de la Proposición anterior. Es decir, $h_0$ divide a $b_1$ y $deg(b_1) \leq m$.

Para la otra implicación, usaremos acotaciones para los factores de polinomios como consecuencia de la medida de Mahler, de la igualdad de Jensen y de la desigualdad de Landau. Así, suponiendo que $deg(h_0) \leq m$, tenemos que $h_0 \in L_{\ell,m}$ y

$$|| \, h_0 \, || \leq 2^m \, || \, f \, ||$$

Ahora, recordemos de la Proposición 5.1.7,que :

$$|| \, b_1 \, || \leq 2^{\frac{m+1-1}{4}} \, || \, h_0 \, || \leq 2^{m/2} 2^m \, || \, f \, ||$$

Entonces,

$$||b_1||^d ||f||^m \leq 2^{dm/2} 2^{dm} \, || \, f \, ||^{m+d} \leq p^{k\ell}$$

Lo que termina la demostración. □

Observación 5.2.6. Como consecuencia de esta Proposición tenemos ya demostrada la primera de las afirmaciones del Teorema 5.2.2. Veamos cómo se alcanza la segunda.

Proposición 5.2.7. *Con las notaciones e hipótesis de toda esta Subsección, si, además de la desigualdad de la Proposición anterior, se verifica que existe un índice* $j \in \{1, 2, \ldots, m+1\}$ *para el cual*

$$|| \, b_j \, || < \left( \frac{p^{kl}}{|| \, f \, ||^m} \right)^{1/d} \tag{5.2.2}$$

*Sea* $t$ *el mayor de tales valores* $j$*. Entonces,*

- $deg(h_0) = m + 1 - t$,
- $h_0 = mcd(b_1, \ldots, b_t)$.

*Y la desigualdad 5.2.2 se verifica para todo* $j, 1 \leq j \leq t$.

Demostración. Sea

$$\mathcal{J} := \{j \in \{1, \ldots, m+1\} \ : \ (5{,}2{,}2) \quad \text{es válida}\}$$

Sabemos de la Proposición 5.2.4 que $h_0$ divide a $b_j$ para cada $j \in \mathcal{J}$. Luego, si escribimos $h_1 := \gcd\{b_j \ : \ j \in \mathcal{J}\}$ , entonces, $h_0$ divide a $h_1$. Cada $b_j$ posee grado menor que $m$, luego está en el $\mathbb{Z}-$módulo

$$\mathbb{Z}h_1 + \mathbb{Z}h_1 X + \cdots + \mathbb{Z}h_1 X^{m-deg(h_1)}$$

Como los $b_j$ son linealmente independientes, concluimos :

$$\sharp\mathcal{J} \leq m + 1 - deg(h_1)$$

De otra parte, la cota de los factores de $f$ nos produce :

$$|| \, h_0 X^i \, || = || \, h_0 \, || \leq 2^m \, || \, f \, ||$$

Para $i = 0, \ldots, m - deg(h_0)$, tenemos $h_0 X^i \in L_{\ell,m}$, luego,

$$|| \, b_j \, || \leq 2^{m/2} 2^m \, || \, f \, || \Rightarrow ||b_j||^d ||f||^m \leq p^{k\ell}$$

para $1 \leq j \leq m + 1 - deg(h_0)$. De donde concluimos,

$$\{1, 2, \ldots, m + 1 - deg(h_0)\} \subseteq \mathcal{J}$$

Veamos que esta inclusión es una igualdad. Puesto que $deg(h_0) \leq deg(h_1)$, se tiene

$$m + 1 - deg(h_0) \geq m + 1 - deg(h_1)$$

Pero acabamos de probar que

$$m + 1 - deg(h_1) \geq m + 1 - deg(h_0)$$

con lo que se da la igualdad de cardinales y, por tanto, la igualdad entre los dos conjuntos anteriores. Como $h_0$ es primitivo, nos queda el prurito de probar que $h_1$ también lo es. Para ello, veamos que cada $b_j$ es primitivo. Pero si no lo fueran, y $c_j$ fuera el contenido

de cada $b_j$, tendríamos que $h_0$ divide a $b_j/c_j$, que estaría en $L_{\ell,m}$ y $b_j$ está en una base de $L_{\ell,m}$. Necesariamente, $c_j = 1$, los $b_j$ son primitivos y $h_1$ también lo es. □

OBSERVACIÓN 5.2.8. En el trabajo original [**L$^3$, 82**], no se considera la hipótesis $\overline{f}$ libre de cuadrados, sino que se sustituye por $(\overline{h})^2$ no divide a $\overline{f}$ en $\mathbb{F}_p[X]$. Claramente, esta segunda disquisición es menos exigente; aunque todo resulta muy parejo (siempre hay que buscar un buen primo).

## 5.3. Equivalencia Computacional entre las diferentes formas de solución

**5.3.1. De los ceros aproximados a la resolución a la Kronecker.** Los conceptos de esta Subsección son herencia de la equivalencia demostrada en [**CHMP, 01**]. En la Subsección 5.1.3 se exhibe el algoritmo de Lenstra–Lenstra–Lovasz para el cálculo de bases $L^3-$reducidas de retículos. Al mismo tiempo, dado un retículo $\Lambda \subseteq \mathbb{R}^n$ y una base reducida $\beta := \{v_1, \ldots, v_n\}$. El primer elemento $v_1$ verifica las siguientes propiedades descritas en la Subsección 5.1 :

$$\|v_1\| \leq 2^{\frac{n-1}{4}} vol(\Lambda)^{1/n}.$$

$$\|v_1\|^2 \leq 2^{n-1}\|x\|^2, \quad \forall x \in \Lambda.$$

En lo que sigue usaremos estas desigualdades para desarrollar un algoritmo (debido al trabajo de R. Kannan, A. K. Lenstra, y L. Lovasz citado al pie [3]) que transforma aproximaciones diofánticas en polinomios mínimos.
Para comenzar supongamos que $\zeta \in \mathbb{C}$ es un número complejo y sea $\overline{\zeta} \in \mathbb{Q}[i]$ una aproximación de $\zeta$ Supongamos que $\deg(\zeta) \leq m$ (grado de su polinomio mínimo sobre $\mathbb{Q}$). Sea $c > 0$ un nmero real y consideremos el retículo $\Lambda(\overline{\zeta}), c) \subseteq \mathbb{R}^{m+1}$ generado por las filas de la siguiente matriz :

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & c.Re((\overline{\zeta})^0) & c.Im((\overline{\zeta})^0) \\ 0 & 1 & 0 & \cdots & c.Re((\overline{\zeta})^1) & c.Im((\overline{\zeta})^1) \\ 0 & 0 & 1 & \cdots & c.Re((\overline{\zeta})^2) & c.Im((\overline{\zeta})^2) \\ \vdots & \ddots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c.Re((\overline{\zeta})^m) & c.Im((\overline{\zeta})^m) \end{pmatrix},$$

donde $Re(\cdot)$ representa parte real e $Im(\cdot)$ parte imaginaria del número complejo considerado. Podemos introducir los polinomios de grado menor que $m$ con coeficientes enteros como algunos de los elementos de este retículo del modo siguiente : Dado $g := a_0 + a_1 X + \cdots + a_m X^m \in \mathbb{Z}[X]$, definamos :

$$\overline{g} := \sum_{i=0}^{m} a_i b_i \in \Lambda(\overline{\alpha}, c),$$

donde $b_0, \ldots, b_m$ son las filas de la matriz anterior. Se observa que la norma del vector $\overline{g} \in \mathbb{R}^{m+1}$ satisface :

$$\|\overline{g}\| = \|g\|^2 + c^2 |g(\overline{\zeta})|,$$

donde $\|g\|$ es la norma del polinomio $g$ en el sentido descrito en la Subsección precendente. El siguiente paso es una consecuencia de los Nullstellensätze Aritméticos, aunque aplicados al caso univariado. Para entender el fenómeno pueden seguirse [**KPS, 01**], [**HMPS, 00**] o [**KrPa, 96**].

[3] R. Kannan, A. K. Lenstra, and L. Lovasz, *Polynomial factorization and non-randomness of bits of algebraic and some transcendental numbers.* In *Proceedings of the 16th Ann. ACM Symposium on Theory of Computing (Washington, D.C.)*, 1984, 191–200.

PROPOSICIÓN 5.3.1. *Sea $\zeta \in \mathbb{C}$ un número complejo algebraico sobre los racionales. Sea $h \in \mathbb{Z}[X]$ su polinomio mínimo y supongamos que del grado de $h$ es a lo sumo $m$, $m \geq 2$. Sea $g \in \mathbb{Z}[X]$ otro polinomio tal que $g(\zeta) \neq 0$. Entonces,*

$$|g(\zeta)| \geq (\|h\| + \|g\|)^{4-3m}.$$

En otras palabras, $|g(\zeta)|$ no puede ser arbitrariamente pequeño. Utilizando las acotaciones de las dos Proposiciones anteriores, se concluye el siguiente resultado :

TEOREMA 5.3.2. *Sea $\zeta \in \mathbb{C}$ un número complejo algebraico sobre los racionales. Sea $h \in \mathbb{Z}[X]$ su polinomio mínimo. Supongamos $M := wt(\zeta)$ y $m := \deg(\zeta)$ respectivamente el peso y el grado de $h$. Sea $\overline{\zeta} \in \mathbb{Q}[i]$ un racional de Gauss tal que se verifican las siguientes propiedades :*

$$|\zeta - \overline{\zeta}| \leq \frac{1}{2^{2d^2+3d+4dlog_2 M}},$$

$$|\overline{\zeta}| \leq |\zeta|.$$

*Definamos la constante $c$ mediante :*

$$c := 2^{\frac{3}{2d^2+2d-1}} M^{3d}.$$

*Sea $\Lambda(\overline{\zeta}; c)$ el retículo antes definido. Finalmente, sea $g \in \mathbb{Z}[X]$ un polinomio con coeficientes enteros tal que $g(\zeta) \neq 0$. Se tiene :*

$$|\overline{h}|^2 \leq 2M^2,$$

$$|\overline{g}|^2 > 2^m \left(2M^2\right).$$

*En particular, dado que $\overline{h} \in \Lambda(\overline{\zeta}, c)$, el primer elemento de una base reducida de $\Lambda(\overline{\zeta}, c)$ ha de ser $\overline{h}$.*

Obviamente este resultado tiene varias aplicaciones razonables :

i) **Cálculo del Polinomio Mínimo de un Número Algebraico a Partir de un Cero Aproximado.** Si disponemos de un cero aproximado $z \in \mathbb{Q}[i]$ de un polinomio $f$, aplicando el operador de Newton $N_f$ varias veces, podemos garantizar que el resultado $\overline{\zeta} := N_f^k(z)$ de $k$ aplicaciones verifica las hipótesis del Teorema anterior. Aplicando el algoritmo de cálculo de bases reducidas descrito en la Subsección 5.1 recuperaremos el polinomio mínimo de la raíz que tratamos de aproximar. El procedimiento `minpoly (r,d)` calcula el polinomio mínimo de un número algebraico próximo a $r$ y de grado menor que $d$.

ii) **Factorización de un Polinomio por Métodos Numéricos.** Se trata de usar los métodos numéricos para factorizar en $\mathbb{Q}[X]$. El proceso aplicará el método de homotopía descrito en la Sección anterior para localizar algún cero aproximado asociado a alguna raíz $\zeta$ del polinomio dado $f \in \mathbb{Q}[X]$. Con el método anterior, hallaríamos el polinomio mínimo $h$ de $\zeta$ que será un factor irreducible de $f$. El proceso continúa con $f := f/h$ hasta que $f$ se convierte en constante. El procedimiento es también de complejidad polinomial.

### 5.3.2. De la resolución Numérica a la Resolución a la Kronecker.

LEMA 5.3.3. *Sea $K$ un cuerpo algebraicamente cerrado y sean $p(X) \in K[X]$ y $q(Y) \in K[Y]$ dos polinomios libres de cuedrados. Entonces, el ideal $\mathfrak{a} := (p, q)$ en $K[X, Y]$ es un ideal radical.*

DEMOSTRACIÓN. Obvio. □

*5.3.2.1. Hipótesis para la Resolución Numérica.*

i) Supongamos dado un ideal cero dimensional $\mathfrak{a} \subseteq \mathbb{Q}[X_1, \ldots, X_n]$ dado por una sucesión regular reducida:

$$\mathfrak{a} := (f_1, \ldots, f_n).$$

ii) Supongamos que somos capaces de hallar ceros aproximados de $f = (f_1, \ldots, f_n)$ asociados a ceros de $V_{\mathbb{C}}(\mathfrak{a})$, con la condición siguiente:

$$V_{\mathbb{C}}(\mathfrak{a}) := \{\zeta_1, \ldots, \zeta_{\mathcal{D}}\},$$
$$\mathcal{S} := \{z_1, \ldots, z_{\mathcal{D}}\} \subseteq \mathbb{Q}[i],$$

de tal modo que

$$||z_i - \zeta_i|| \leq \frac{3 - \sqrt{7}}{2\gamma(f, \zeta_i)}.$$

Usando el operador de Newton $N_f$ podemos hallar aproximaciones $Z_1, \ldots, Z_{\mathcal{D}} \in \mathbb{Q}[i]$ tales que

$$||Z_i - \zeta_i|| \leq \frac{1}{H},$$

para un $H$ a determinar.

*5.3.2.2. Los polinomios mínimos de las proyecciones.* Elijamos $\underline{\lambda} := (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ un punto con coordenadas enteras y definamos:

$$U_i := \sum_{j \neq i} \lambda_j X_j \in \mathbb{Q}[X_1, \ldots, X_n]$$

Nótese que

$$||U_k(Z_i) - U_k(\zeta_i)|| \leq \frac{||\underline{\lambda}||_2}{H},$$

Denotemos por $\pi_k : \mathbb{C}^n \longrightarrow \mathbb{C}$ la proyección sobre la coordenada $k-$ésima. Entonces, tenemos

$$||\pi_k(Z_i) - \pi_k(\zeta_i)|| \leq \frac{1}{H}.$$

Elijamos $H$ suficientemente grande para que se verifiquen las hipótesis el algoritmo $KL^2$.

Aplicando $KL^2$ a cada $U_k(Z_i)$ y cada $\pi_j(Z_i)$, y recombinando los resultados, dispondremos de la siguiente información:

i) Una lista de polinomios $p_1, \ldots, p_n \in \mathbb{Q}[T]$ libres de cuadrados, tales que

$$p_k(U_k(\zeta_i)) = 0,\ 1 \leq i \leq \mathcal{D}.$$

ii) Una lista de polinomios $q_1, \ldots, q_n \in \mathbb{Q}[T]$ libres de cuadrados, tales que

$$q_k(\pi_k(\zeta_i)) = 0,\ 1 \leq i \leq \mathcal{D}.$$

Para cada $k$, $1 \leq k \leq n$ consideremos el ideal $\mathfrak{a}_k := (p_k(T_k), q_k(X_k)) \subseteq \mathbb{Q}[T_k, X_k]$, donde $T_k$ es una nueva variable. Consideremos los morfismos de anillos:

$$\varphi_k : \mathbb{Q}[T_k, X_k] \hookrightarrow \mathbb{Q}[X_1, \ldots, X_n],$$

dado mediante $\varphi(X_k) = X_k$ y $\varphi_k(T_k) = U_k$. Se tiene:

PROPOSICIÓN 5.3.4. *Con las anteriores notaciones, se tienen las siguientes propiedades:*

i) *Los morfismos $\varphi_k$ son monomorfismos de anillos.*
ii) *Los ideales $\mathfrak{a}_k$ están contenidos en las contracciones del ideal $\mathfrak{a}$ a cada uno de los anillos $\mathbb{Q}[X_1, \ldots, X_n]$.*
iii) *Dada la lista $\underline{\lambda} := (\lambda_1, \ldots, \lambda_n)$ si, para cada $k$, $1 \leq k \leq n$, $T_k + \lambda_k X_k$ es un elemento primitivo para el cociente $\mathbb{Q}[T_k, X_k]/\mathfrak{a}_k$, entonces la forma lineal $U := \lambda_1 X_1 + \cdots + \lambda_n X_n = \varphi_k(T_k + \lambda_k X_k)$ es un elemento primitivo para el cociente $\mathbb{Q}[X_1, \ldots, X_n]/\mathfrak{a}$.*

iv) *Supongamos que la forma lineal $U$ anterior es elemento primitivo para $\mathbb{Q}[T_k, X_k]/\mathfrak{a}_k$ para cada $k$, $1 \leq k \leq n$. Para cada $k$, $1 \leq k \leq n$, sea $m_k$ el polinomio mínimo de $T_k + \lambda_k X_k$ en $\mathbb{Q}[T_k, X_k]/\mathfrak{a}_k$. Sea $P(T) \in \mathbb{C}[T]$ el máximo común divisor de $m_1, \ldots, m_k$. Entonces, $P(U(X_1, \ldots, X_n)) \in \mathfrak{a}$.*

v) *Con las mismas hipótesis del item anterior, existen polynomios $W_k(T) \in \mathbb{C}[T]$ tales que $X_k - W_k(T_k + \lambda_k X_k)) \in \mathfrak{a}_k$, para cada $k$, $1 \leq k \leq n$. En particular,*

$$X_k - W_k(U(X_1, \ldots, X_n)) \in \mathfrak{a},\ 1 \leq k \leq n.$$

Demostración. Probemos cada afirmación separadamente.

i) La primera afirmación es obvia.

ii) En primer lugar nótese que, con nuestras hipótesis, $\mathfrak{a}$ es un ideal radical. Además, el polinomio $p_k(U_k(X_1, \ldots, X_n)) \in \mathbb{Q}[X_1, \ldots, X_n]$ se anula en $V_{\mathbb{C}^n}(\mathfrak{a})$. Por tanto, $p_k \in \mathfrak{a}$ por el Nullstellensatz. Lo mismo sucede con los polinomios $q_k(X_k)$. Por tanto,

$$\mathfrak{a}_k \subseteq \mathfrak{a}^c.$$

iii) Consideremos $V_k := \varphi_k(V(\mathfrak{a})) \subseteq \mathbb{C}^2$. Más aún, consideremos $V(\mathfrak{a}_k)$ y se tiene $V_k \subseteq V(\mathfrak{a}_k)$. Además, consideremos la aplicación $\rho_k : \mathbb{C}^2 \longrightarrow \mathbb{C}$ dada mediante:

$$\rho_k(t_k, x_k) = t_k + \lambda_k(x_k).$$

Nótese que para cada $\zeta = (\zeta^{(1)}, \ldots, \zeta^{(n)}) \in V(\mathfrak{a})$,

$$\rho_k(\varphi_k(\zeta)) = U(\zeta) = \sum_{i=1}^{n} \lambda_i \zeta^{(i)} \in \mathbb{C}.$$

Por tanto, si $T_k + \lambda_k X_k$ es primitivo módulo $\mathfrak{a}_k$ es porque toma valores diferentes para cualesquiera valores en $V(\mathfrak{a}_k)$. En particular, dados dos puntos $\zeta, \zeta' \in V(\mathfrak{a})$, con $\zeta \neq \zeta'$, debe haber un $k$, $1 \leq k \leq n$ tal que $\varphi_k(\zeta) \neq \varphi_k(\zeta')$. Esto es así porque si $\zeta := (\zeta_1, \ldots, \zeta_n)$ y $\zeta' := (\zeta'_1, \ldots, \zeta'_n)$, con $\zeta \neq \zeta'$, debe haber una coordenada $k$ tal que $\zeta_k \neq \zeta'_k$, con lo que $\varphi_k(\zeta) \neq \varphi_k(\zeta'_k)$. Entonces, $\rho_k(\varphi_k(\zeta)) \neq \rho_k(\varphi_k(\zeta'_k))$ y, por tanto, $U(\zeta) \neq U(\zeta')$ y $U$ es primitivo módulo $\mathfrak{a}$ (porque $\mathfrak{a}$ es radial).

iv) Es evidente que $m_k(U(X_1, \ldots, X_n)) = m_k(\varphi_k(T_k + \lambda_k X_k)) = \varphi_k(m_k) \in \mathfrak{a}_k \subseteq \mathfrak{a}^c := \varphi_k^{-1}(\mathfrak{a})$ y que $m_k(U(X_1, \ldots, X_n)) \in \mathfrak{a}$. Por tanto, si $P(T)$ es el máximo común divisor de $m_1, \ldots, m_k$, tenemos que $P(U(X_1, \ldots, X_n))$ es un elemento del ideal $\mathfrak{a}$.

v) La existencia de los polinomios $W_k$ tales que $X_k - W_k(T_k + \lambda_k X_k)) \in \mathfrak{a}_k$ es consecuencia inmediata de ser $U$ elementos primitivo módulo $\mathfrak{a}_k$ y de ser $\mathfrak{a}_k$ un ideal radical. El resto se sigue de observar que $\varphi_k(X_k - W_k(T_k + \lambda_k X_k)) = X_k - W_k(U(X_1, \ldots, X_n)) \in \mathfrak{a}$.

□

Consideremos ahora el ideal $\mathfrak{b} \subseteq \mathfrak{a}$ dado mediante:

$$\mathfrak{b} := (P(U(\underline{X})), X_1 - W_1(U(\underline{X})), \ldots, X_n - W_n(U(\underline{X}))) \subseteq \mathbb{Q}[X_1, \ldots, X_n],$$

donde

$$\underline{X} = (X_1, \ldots, X_n).$$

El ideal $\mathfrak{b}$ define un ideal cero-dimensional contenido en el ideal $\mathfrak{a}$. Ahora consideremos los polinomios univariados

$$F_k(T) := f_k(W_1(T), \ldots, W_n(T)),\ 1 \leq k \leq n.$$

Proposición 5.3.5. *Sea $p(T) := gcd(F_1, \ldots, f_n) \in \mathbb{Q}[T]$. Definamos, $v_k := rem(W_k(T), p(T))$ el resto de la división de $W_k$ por $p(T)$. Entonces,*

$$\mathfrak{a} = (p(U(\underline{X})), X_1 - v_1(\underline{X}), \ldots, X_n - v_n(\underline{X})).$$

DEMOSTRACIÓN. Basta con probar la igualdad de $\mathfrak{a}/\mathfrak{b}$. Para eso, basta con escribir los elementos módulo $\mathfrak{b}$ y $F_i + \mathfrak{b} = f_i + \mathfrak{b}$. El resto es evidente.

□

Capítulo 6

# El Concepto de Dimensión

Este material es obtenidble en [**AtMc, 69**], [**Ma, 80**], [**Ma, 89**] y, para el Lema de Normalización de Noether[1], seguiremos la prueba que da [**Ku, 85**].

## 6.1. Extensiones Enteras de Anillos

Definición 34. *Dada una extensión de anillos $R \subseteq R'$, un elemento $x \in R'$ se dice entero sobre $R$ si verifica una ecuación polinomial mónica con coeficientes en $R$. Una extensión $R \subseteq R'$ se dice entera si todos los elementos de $R'$ son enteros sobre $R$.*

Proposición 6.1.1. *Las siguientes propiedades son equivalentes para una extensión de anillos $R \subseteq R'$:*

- *Un elemento $x \in R'$ es entero sobre $R$.*
- *La $R-$álgebra $R[x]$ es un $R-$módulo finitamente generado.*
- *La $R-$álgebra $R[x]$ está contenido en un subanillo $B$ de $R'$ tal que $B$ es un $R-$módulo finitamente generado.*
- *Existe un $R[x]-$módulo fiel $M$ que es de generación finita como $R-$módulo.*

Corollario 6.1.2 (Clausura Entera). *Dada una extensión entera de anillos $R \subseteq R'$, los elementos de $R'$ que son enteros sobre $R$ forman un subanillo $\bar{R}$ de $R'$ llamado clausura entera de $R$ en $R'$.*

Corollario 6.1.3 (Transitividad). *Dadas extensiones de anillos $R \subseteq R' \subseteq R''$, si $R'$ es enetro sobre $R$ y $R''$ es entero sobre $R'$, entonces $R''$ es entero sobre $R$. En particular, la clausura entera de $R$ en $R'$ es íntegramente cerrado en $R'$.*

Proposición 6.1.4. *Dada una extensión entera de anillos $R \subseteq R'$. Se tiene:*

- *Si $\mathfrak{b}$ es un ideal de $R'$, entonces, $R'/\mathfrak{b}$ es enetro sobre $R/\mathfrak{b}^c$.*
- *Si $S$ es un subconjunto multiplicativamente cerrado de $R$, entonces $S^{-1}R'$ es entero sobre $S^{-1}R$.*

## 6.2. Going–Up y Going–Down

Aunque normalmente se les asigna a I.S. Cohen y A. Seidenberg, parece que W. Krull también los conocía con lo que podrían llamarse los teoremas KCS o Krull–Cohen–Seidenberg.

### 6.2.1. Going–Up.

La clave es la siguiente Proposición.

Proposición 6.2.1. *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, si $\mathfrak{q}$ 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 6.2.2. *Sea $R \subseteq R'$ una extensión entera de anillos. Entonces, no hay relación de inclusión propia entre ideales primos de $R'$ que se contraen sobre el mismo idela primo de $R$.*

[1] E. Noether, "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl und Funktionenkrpern". *Math. Ann.* , **96** (1927) pp. 26-61.

COROLLARIO 6.2.3. *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:*

- *$\varphi$ es suprayectiva*
- *$\varphi(Spm(R')) \subseteq Spm(R)$ y la siguiente aplicación está bien definida y es suprayectiva:*

$$\varphi_{Spm(R')} : Spm(R') \longrightarrow Spm(R).$$

Podemos incluir también una interpretación geométrica.

COROLLARIO 6.2.4. *Sea $\varphi : V \longrightarrow W$ un morfismo de conjuntos algebraicos dominante (i.e. $\varphi^* : \mathbb{K}[W] \longrightarrow \mathbb{K}[V]$ es inyectiva). Entonces, si la extensión $\mathbb{K}[W] \subseteq \mathbb{K}[V]$ es entera, $\varphi$ es suprayectiva.*

TEOREMA 6.2.5 (Going–Up). *Sea $R \subseteq R'$ una extensión entera de anillos. Sean dadas:*

- *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 $R'$:*

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m,$$

*De tal modo que $n > m$ y $\mathfrak{q}_i^c = \mathfrak{p}_i$, para cada $i$, $1 \leq i \leq m$. Entonces, existe una cadena ascendente de ideales primos de $R'$:*

$$\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \mathfrak{q}_{m+2} \subseteq \cdots \subseteq \mathfrak{q}_n,$$

*tales que $\mathfrak{q}_i^c = \mathfrak{p}_i$ para cada $i$, $m+1 \leq i \leq n$.*

### 6.2.2. Going–Down.

PROPOSICIÓN 6.2.6. *Sea $R \subseteq R'$ una extensión de anillos, $\bar{R}$ la clausura entera de $R$ en $R'$ y $S$ un sistema multiplicativamente cerrado de $R$. Entonces, $S^{-1}\bar{R}$ es la clausura entera de $S^{-1}R$ en $S^{-1}R'$.*

DEFINICIÓN 35 (Dominios normales). *Un dominio $R$ se dice normal o íntegramente cerrado si es íntegramente cerrado en su cuerpo de fracciones.*

PROPOSICIÓN 6.2.7. *La condición "normalidad" es una propiedad local.*

Tras algún esfuerzo probaremos:

TEOREMA 6.2.8 (Going–Down). *Sea $R \subseteq R'$ una extensión entera de dominios de integridad, siendo $R$ un dominio normal. Sean dadas:*

- *Una cadena desscendente 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 $R'$:*

$$\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m,$$

*De tal modo que $n > m$ y $\mathfrak{q}_i^c = \mathfrak{p}_i$, para cada $i$, $1 \leq i \leq m$. Entonces, existe una cadena descendente de ideales primos de $R'$:*

$$\mathfrak{q}_m \supseteq \mathfrak{q}_{m+1} \supseteq \mathfrak{q}_{m+2} \supseteq \cdots \supseteq \mathfrak{q}_n,$$

*tales que $\mathfrak{q}_i^c = \mathfrak{p}_i$ para cada $i$, $m+1 \leq i \leq n$.*

## 6.3. Condición de cadena ascendente para submódulos e ideales

Una versión más suave el Axioma de Zorn, conocido como el *Axioma de Elección Dependiente*.

DEFINICIÓN 36 (**Axioma de Elección Dependiente**). *Sea $X$ un conjunto no vacío y $R \subseteq X \times X$ una relación. Supongamos que $R$ satisface la siguiente propiedad:*

$$\forall a \in X, \ \exists b \in X, \ aRb.$$

*Entonces, existe una sucesión $\{x_n \ : \ n \in \mathbb{N}\} \subseteq X$ de tal modo que $x_n R x_{n+1}$, $\forall n \in \mathbb{N}$.*

PROPOSICIÓN 6.3.1 (**Módulo Noetheriano**). *Sea $R$ un anillo y $M$ un $R-$módulo. Las siguientes propiedades son equivalentes:*

i) *Todo submódulo de $M$ es finitamente generado.*
ii) *Los submódulos de $M$ satisfacen las "condición de cadena ascendente", es decir, dada una cadena ascendente de submódulos de $M$:*

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_m \subseteq \cdots ,$$

*entonces existe un entero $n \in \mathbb{N}$ a partir del cual la cadena se estabiliza, es decir, $N_m = N_n$, $\forall m \geq n$.*
iii) *Todo conjunto no vacío de submódulos de $M$ posee elemento maximal para la inclusión.*

DEMOSTRACIÓN.

- (1) $\Rightarrow$ (2): Nótese que si tenemos una cadena ascendente:

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_m \subseteq \cdots ,$$

la unión $N := \bigcup_{i \in \mathbb{N}} N_i \subseteq M$ es también un submódulo de $M$ y, por (1), será finitamente generado. Una colección finita $\{n_1, \ldots, n_r\}$ de generadores de $N$ debe pertenecer a algún submódulo $N_n$ de $M$ (simplemente porque todo subconjunto finito de naturales posee elemento maximal). Entonces, $N = N_n$ y $N_m = N_n$, $\forall m \geq n$.

- (2) $\Rightarrow$ (3): Aquí usaremos el *Axioma de Elección Dependiente* del modo siguiente. Sea $X$ un subconjunto no vacío de submódulos de $M$ y supongamos que no posee elemento maximal. Entonces, verifica que

$$\forall N \in X, \ \exists N \in X, \ N \subsetneq N'.$$

Tomando $R = \subsetneq$ como la relación sobre $X$, concluiremos que existe una cadena ascendente:

$$N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_m \subsetneq \cdots ,$$

contradiciendo (2).

- (3) $\Rightarrow$ (1): Sea $N$ un submódulo de $M$. Consideremos el conjunto $X_N$ formado por todos los submódulos $L$ de $N$ que son finitamente generados. Como (0) es submódulo, finitamente generado, y $(0) \subseteq N$, entonces $(0) \in X \neq \emptyset$. Por tanto, $X$ posee una elemento maximal para la inclusión. Sea $N_0$ ese elemento maximal. Tenemos que $N_0 \subseteq N$. Si $N_0 = N$ habremos concluido. Supongamos, por tanto, que $N_0 \subsetneq N$. Entonces, existe $n \in N \setminus N_0$ y consideremos el submódulo $N_1 := N_0 + \langle n \rangle \subseteq N$. Claramente $N_1 \in X$ y $N_0 \subsetneq N_1$, con lo que llegaríamos a contradicción.

□

OBSERVACIÓN 6.3.2. Usualmente la prueba de la equivalencia entre estas tres propiedades (esencialmente la prueba de (2) $\Rightarrow$ (3) o, equivalentemente, la prueba de (2) $\rightarrow$ (1) se hace sin mostrar la relevancia del Axioma de Elección Dependiente. Este aspecto fue destacado por W. Hodges, en su trabajo:

W. Hodges, *Six impossible rings*, J. Algebra **31** (1974), 218-244.
Este trabajo ha generado bastante controversia y nuestra elección simplifica por la ví de elegir un Axioma más débil.

Idénticamente a la anterior Proposición, como todo anillo es $R-$módulo sobre sí mismo y sus submódulos son sus ideales, tenemos el correspondiente enunciado para anillos:

PROPOSICIÓN 6.3.3 (**Anillo Noetheriano**). *Sea $R$ un anillo. Las siguientes propiedades son equivalentes:*

i) *Todo ideal de $R$ es finitamente generado.*
ii) *Los ideales de $R$ satisfacen las "condición de cadena ascendente", es decir, dada una cadena ascendente de ideales de $R$:*

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \subseteq \cdots,$$

*entonces existe un entero $n \in \mathbb{N}$ a partir del cual la cadena se estabiliza, es decir, $\mathfrak{a}_m = \mathfrak{a}_n$, $\forall m \geq n$.*
iii) *Todo conjunto no vacío de ideales de $R$ posee elemento maximal para la inclusión.*

*En particular, todo anillo que satisface una cualquiera de esas propiedades equivalentes posee al menos un ideal maximal.*

PROPOSICIÓN 6.3.4 (**Espacio Topológico noetheriano**). *Sea $(X, \mathcal{T})$ un espacio topológico. Las siguientes propiedades son equivalentes:*

i) *Los cerrados verifican la condición de cadena descendente, es decir. dada una cadena descendente de cerrados:*

$$X_0 \supseteq X_1 \supseteq X_2 \supseteq \cdots \supseteq X_n \supseteq \cdots,$$

*entonces la cadena se estabiliza, es decir, existe $m \in \mathbb{N}$ tal que para todo $n \geq m$, se tiene $X_n = X_m$.*
ii) *Todo conjunto no vacío de cerrados de $(X, \mathcal{T})$ posee elemento minimal.*
iii) *Todo subconjunto $Y \subseteq X$ con la toplogía inducida con $\mathcal{T}$ es compacto.*

DEMOSTRACIÓN. La equivalencia ente i) y ii) se obtiene de modo análogo al caso de módulos y anillos. Es el mismo tipo de artumento basado en el Axioma de Elección Dependiente. Para la compacidad, usaremos los siguientes argumentos:

- *ii) $\Longrightarrow$ iii):* Sea $Y$ un subconjunto de $X$ y supongamos dado un cubrimiento de $Y$ por abiertos en $Y$. Podemos suponer que ese cubrimiento viene dado por una familia $\{A_i \ : \ i \in J\}$ de abiertos de $X$ de tal modo que

$$Y \subseteq \bigcup_{j \in J} A_J.$$

Consideremos el siguiente conjunto de cerrados en $X$:

$$\mathcal{F} := \{\bigcap_{i \in I}(X \setminus A_i) \ : \ I \subseteq J, \ I \text{ es finito}\}.$$

Es claro que $\mathcal{F}$ es no vacío y, por tanto, posee un elemento minimal. Sea $I \subseteq J$ un subconjunto finito tal que $\cap_{i \in I}(X \setminus A_i)$ es minimal en $\mathcal{F}$. Es claro que, entonces, el siguiente es un elemento maximal entre las uniones finitas de abiertos de la familia $\{A_i \ : \ i \in J\}$:

$$A := \bigcup_{i \in I} A_i.$$

Supongamos ahora que $Y \not\subseteq A$. Esto significa que existe $y \in Y$ tal que $Y \notin A$. Pero, entonces, existe $j \in J$ tal que $y \in A_j$ y considero la familia finita

$$\left(\bigcup_{i\in I} A_i\right) \bigcup A_j \supseteq \left(\bigcup_{i\in I} A_i\right) = A.$$

Por la maximalidad de $A$, tendremos que

$$\left(\bigcup_{i\in I} A_i\right) \bigcup A_j = \left(\bigcup_{i\in I} A_i\right) = A,$$

contradiciendo el hecho supuesto de que $y \notin A$. Luego $Y \subseteq A$ y existe un subcubirmiento finito de $Y$ formado por elementos de $\{A_j \ : \ j \in J\}$, lo que confirma la compacidad de $Y$.

- *iii)* $\Longrightarrow$ *i):* Consideremos una cadena descendente de cerrados:

$$X_0 \supseteq X_1 \supseteq X_2 \supseteq \cdots \supseteq X_n \subseteq \cdots,$$

Que genera una cadena ascendente de abiertos:

$$(X \setminus X_0) \subseteq (X \setminus X_1) \subseteq (X \setminus X_2) \subseteq \cdots \subseteq (X \setminus X_n) \subseteq \cdots,$$

Definamos $Y$ mediante la union de todos ellos:

$$Y := \bigcup_{i\in\mathbb{N}} (X \setminus X_i).$$

Como $Y$ es compacto, posee un subcubrmiento finito, que podemos suponer de la forma:

$$Y = \bigcup_{i=0}^{n} (X \setminus X_i).$$

Entonces, claramente se tiene $X_m = X_n$, para todo $m \geq n$ y la cadena de estabiliza.

□

Definición 37. *Se tienen las nociones siguientes:*

i) *Un $R-$módulo $M$ se llama noetheriano si satisface una cualquiera de las propiedades equivalentes descritas en la Proposición 6.3.1 anterior.*
ii) *Un anillo $R$ se llama noetheriano si es noetheriano como módulo sobre sí mismo, esto es, si satisface una cualquiera de las propiedades equivalentes descritas en la Proposición 6.3.3 anterior.*
iii) *Un espacio topológico $(X, \mathcal{T})$ se llama noetheriano si verifica una cualquiera de las propiedades descritas en la Proposición 6.3.4 anterior.*

Ejemplo 6.3.5. Algunos ejemplos elementales e inmediatos:

- Los cuerpos son, obviamente, anillos noetherianos.
- Los dominios de ideales principales son anillos noetherianos (todos sus ideales son finitamente generados).
- Los espacios vectoriales son finitamente generados si y solamente si son neotherianos (todos sus subespacios son finitamente generados).
- Los grupos abelianos libres finitamente generados son noetherianos: sus submódulos son libres de torsión (y, por tanto, libres) y finitamente generados
- Submódulos de módulos noetherianos son noetherianos porque los submódulos de un submódulo son submódulos del módulo original.
- Cocientes de módulos noetherianos son noetherianos: para verlo basta con usar la propiedad (3) de la Proposición 6.3.1: Recuérdese que los submódulos de un cociente $M/N$ están biyectados con los submódulos de $M$ que contienen a $N$ y que esa biyección preserva la inclusión.

- Cocientes de anillos noetherianos son también noetherianos.

Pero necesitamos de mecanismos adicionales para mostrar ejemplos más aleborados de anillos y módulos noetherianos.

EJEMPLO 6.3.6. Si $R$ es un anillo noetheriano, tanto $Spec(R)$ como $Spem(R)$ son espacios topológicos noetherianos. El recíproco no es, en general, cierto, como prueba el siguiente ejemplo:

$$R := \mathbb{C}[X_i \ : \ i \in \mathbb{N}]/\mathfrak{a},$$

donde $\mathfrak{a}$ es el ideal generado por $(X_n^2 \ : \ n \in \mathbb{N})$. Claramente, $Spec(R)$ ee, en este caso, un sólo punto y es neotheriano, mientras que $R$ no es un nanillo noetheriano.

### 6.3.1. El Teorema de la Base de Hilbert.

PROPOSICIÓN 6.3.7. *Dada una sucesión exacta corta de $R-$módulos:*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0,$$

*entonces, $M$ es noetheriano si y solamente si $M'$ y $M''$ son noetherianos.*

DEMOSTRACIÓN. Es claro que si $M$ es noetheriano, $M'$ también lo es dado que es isomorfo a un submódulo de $M$. De otro lado, $M''$ es isomorfo a un cociente de $M$ por un submódulo (de heho, $M'' \cong M/M'$). Por tanto, sólo hay que probar la otra implicación.
Comencemos tomando un submódulo $N$ de $M$ y sea $g(N)$ submódulo de $M''$. Como $M''$ es noetheriano, entonces, existen $n_1, \ldots, n_p \in N$ tales que $g(n_1), \ldots, g(n_p)$ generan $g(N)$ como submódulo de $M''$. De otro lado, $f^{-1}(N)$ es un submódulo de $M'$. Como $M'$ es noetheriano, posee un conjunto finito $m_{p+1}, \ldots, m_s$ de generadores y considero $n_{p+1} = f(m_{p+1}), \ldots, n_s := f(m_s)$ elementos de $N$. Probemos que el conjunto $X := \{n_1, \ldots, n_p, n_{p+1}, \ldots, n_s\}$ genera $N$ como submódulo de $M$. Para ello, consideremos un elemento $n \in N$ y el submódulo $N_X \subseteq N$ generado por $X$. Tenemos que $g(n) \in g(N)$ y, por tanto, existen $x_1, \ldots, x_p \in R$ tales que

$$g(n) = x_1 g(n_1) + \cdots + x_p g(n_p).$$

En particular, tendremos que $g(n - (x_1 n_1 + \cdots + x_p n_p)) = 0$, lo que significa que $n - (x_1 n_1 + \cdots + x_p n_p) \in Keg(g) = Im(f)$. Pero $n - (x_1 n_1 + \cdots + x_p n_p) \in N$, luego existe $y \in f^{-1}(N)$ tal que $f(y) = n - (x_1 n_1 + \cdots + x_p n_p)$. Pero $m_{p+1}, \ldots, m_s$ generan $f^{-1}(N)$. Por tanto, existen $x_{p+1}, \ldots, x_s \in R$ tales que $y = x_{p+1} m_{p+1} + \cdots + x_s m_s$. Esto último implica que

$$n - (x_1 n_1 + \cdots + x_p n_p) = x_{p+1} f(m_{p+1}) + \cdots + x_s f(m_s).$$

Esto último también se resscribe:

$$n = x_1 n_1 + \cdots + x_p n_p + x_{p+1} n_{p+1} + \cdots + x_s n_s,$$

y queda probado que $n \in N_X$, con lo que $N = N_X$ y $M$ es noetheriano. □

PROPOSICIÓN 6.3.8. *Si $R$ es un anillo noetheriano, entonces un $R-$módulo es noetheriano si y solamente si es finitamente generado como $R-$módulo.*

DEMOSTRACIÓN. Es claro que si $M$ es un $R-$módulo noetheriano es finitamente generado (todos sus submódulos lo son). Por tanto, sólo hay que probar el recíproco.
Así, sea $M$ un $R-$módulo finitamente generado, suponiendo que $R$ es noetheriano. Supongamos que $M$ es generado por $n$ elementos. Probaremos, por inducción en $n$, que $M$ es un $R-$módulo noetheriano.

Para el caso $n = 1$, si $M$ está generado por un sólo elemento, entonces $M$ es isomorfo como $R-$módulo a un cociente $R/\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal de $R$. Entonces, aplicando la anterior proposición, habremos concluido que $M$ es un $R-$módulo noetheriano a través de la sucesión exacta:

$$0 \longrightarrow \mathfrak{a} \longrightarrow R \longrightarrow R/\mathfrak{a} \longrightarrow 0.$$

Supongamos que el resultado es cierto para toso los $R-$módulos que se pueden generar con a lo sumo $n-1$ elementos. Sea $\{m_1, \ldots, m_n\}$ un conjunto de elementos de $M$ que lo generan como $R-$módulo. Consideremos el submódulo $M'$ de $M$ generado por $\{m_1, \ldots, M_{n-1}\}$. Por hipótesis inductiva, $M'$ es noetheriano. Pero, además podemos considerar la sucesión exacta corta siguiente:

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M/M' \longrightarrow 0,$$

donde $i$ es la inclusión canónica y $\pi$ es la proyección canónica. Además, es fácil observar que $M/M''$ está generado, como $R-$módulo, por la clase $\{x_n + M'\}$. Aplicando el caso $n = 1$ tenemos que $M/M'$ es también noetheriano y, finalmente, aplicando la Proposición 6.3.7 concluiremos que $M$ ha de ser noetheriano también. □

Proposición 6.3.9. *Sea $S$ un sistema multiplicativo de un anillo $R$. Si $R$ es neotheriano, también es neotheriano su localización $S^{-1}R$. En particular, para cada ideal primo $\mathfrak{p} \in Spec(R)$ se un anillo noetheriano, la localización $R_{\mathfrak{p}}$ es anillo local noetheriano.*

Demostración. Basta con recordar la relación entre los ideales de $S^{-1}R$ y los ideales de $R$ que no intersecan $S$. Así, si $\mathfrak{q}$ es un ideal de $S^{-1}R$, su contracción $\mathfrak{q}^c \subseteq R$ es un ideal de $R$ y es finitamente generado cuando $R$ es neotheriano. Si $\mathfrak{q}$ está generado por $\{x_1, \ldots, x_r\}$, entonces $\mathfrak{q}$ estará generado por $\{x_1/1, \ldots, x_r/1\}$ y será finitamente generado. □

Teorema 6.3.10 (**Hilbert Basissatz**). *Si $R$ es un anillo noetheriano, entonces $R[X]$ también es un anillo noetheriano.*

Demostración. Para probar este Teorema tomemos un ideal $\mathfrak{a}$ en $R[X]$ y consideremos el conjunto $\mathfrak{b} \subseteq A$ siguiente:
Un elemento $a \in R$ están en $\mathfrak{b}$ si y solamente si existe un polinomio $f := a_n X. + a_{n-1}X^{n-1} + \cdots + a_o \in \mathfrak{a}$ tal que $a_n = a$. Es decir, el conjunto formado por todos los coeficientes dorectores de elementos en $\mathfrak{a}$. Es fácil comprobar que $\mathfrak{b}$ es un ideal de $R$ y, por ser $R$ noetheriano, es finitamente generado. Consideremos $\{a_1, \ldots, a_p\}$ un conjunto finito de generadores de $\mathfrak{b}$. Supongamos $f_1, \ldots, f_p \in \mathfrak{a}$ tales que el coeficiente director de $f_i$ es $a_i$. Es decir, para cada $i$, $1 \leq i \leq p$ se tiene:

$$f_i := a_i X^{n_i} + h_i,$$

con $deg(h_i) \leq n_i$. Sea $N := \text{máx}\{n_1, \ldots, n_p\}$ el máximo de esos grados y consideremos la intersección $\mathfrak{a}_N := \mathfrak{a} \cap R[X]_N$, donde $R[X]_N$ son los polinomios en $R[X]$ de grado a lo sumo $N$. Claramente, $R[X]_N$ es un $R-$módulo finitamente generado y, por tanto, noetheriano. Además, $\mathfrak{a} \cap R[X]_N$ es un submódulo de $R[X]_N$, luego es finitamente generado. Consideremos $\{g_1, \ldots, g_s\}$ un conjunto de generadores de $\mathfrak{a} \cap R[X]_N$ como $R-$módulo. Entonces, el conjunto:

$$F := \{f_1, \ldots, f_p\} \cup \{g_1, \ldots, g_2\},$$

generan $\mathfrak{a}$ como ideal en $R[X]$. Denotemos por $(F)$ el ideal generador por $F$. Supongamos que existe $h \in \mathfrak{a}$ un elemento que no está en el ideal $(F)$. Supongamos, además,

que $h$ es de grado mínimo con esa propiedad. Si $deg(h) \leq N$, entonces $h \in \mathfrak{a} \cap R[X]_N$, luego han de existir constantes $\lambda_1, \ldots, \lambda_s \in R$ de tal modo que:

$$h = \lambda_1 g_1 + \cdots + \lambda_s g_s \in (F).$$

Por tanto, $deg(h) > N$. De otro lado, supongamos

$$h := b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0,$$

siendo $m$ el mínimo de los grados de los polinomios $h \in \mathfrak{a} \setminus (F)$. Es claro que $b_m \in \mathfrak{b}$ por lo que han de existir $\theta_1, \ldots, \theta_p \in R$ tales que

$$b_m = \theta_1 a_1 + \cdots + \theta_p a_p.$$

Ahora consideremos el polinomio:

$$h_1 := h - \sum_{i=1}^{p} \theta_i X^{m-n_i} f_i.$$

Es claro que el polinomio $h_1 \in \mathfrak{a}$. De otro lado, $h_1 \notin (F)$ pues, si $h_1 \in (F)$, entonces, $h \in (F)$ y llegaríamos a contradicción. Pero, además, es claro que el coeficiente de grado $m$ de $h_1$ es dado por:

$$b_m - (\theta_1 a_1 + \cdots + \theta_p a_p) = 0.$$

En otras palabras, $deg(h_1) \leq m - 1$, contradiciendo la minimalidad de $m$. Por tanto, no puede existir ningún $h \in \mathfrak{a} \setminus (F)$ y $\mathfrak{a} = (F)$, concluyendo que $\mathfrak{a}$ es finitamente generado. □

Corollario 6.3.11. *Si $R$ es un anillo noetheriano, también lo es el anillo de polinomios en un número finito de variables $R[X_1, \ldots, X_n]$. En particular, si $R$ es noetheriano tambin lo es toda $R-$ álgebra finitamente generada, esto es, todo anillo $B$ de la forma $R[X_1, \ldots, X_n]/\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal de $R[X_1, \ldots, X_n]$.*

Demostración. Obvio por inducción. □

Ejemplo 6.3.12.

- Todos los anillos de polinomios con coeficientes en un cuerpo $K[X_1, \ldots, X_n]$ son noetherianos. También lo son los cocientes $K[X_1, \ldots, X_n]/\mathfrak{a}$ que se denominan *$K-$álgebras finitamente generadas.*
- Todos los anillos de polinomios con coeficientes en dominios de ideales principales son noetherianos.
- No son noetherianos los anillos de polinomios en una cantidad infinita de variables $K[X_n \ : \ n \in \mathbb{N}]$.
- Todos los $K[V]$ , cuando $V \subseteq \mathbb{K}^n$ es una variedad algebraica afín, son anillos noetherianos.
- Todas las localizaciones de anillos de polinomios $K[X_1, \ldots, X_n]_{\mathfrak{p}}$, por ideales primos $\mathfrak{p} \in Spec(K[X_1, \ldots, X_n])$ son anillos noetherianos. Los mismo con las localizaciones $K[V]_{\mathfrak{p}}$, que también son noetherianos.

Obviamente son noetherianos todos los módulos finitamente generados sobre esos anillos.

Ejemplo 6.3.13. Como consecuencia del Teorema de la Base, todo espacio afín $\mathbb{K}^n$ con la toplogía de Zariski es noetheriano como espacio topológico. Y también lo son los cerrados Zariski $V \subseteq \mathbb{K}^n$ con la topología de Zariski inducida.

Ejemplo 6.3.14. Una de las conscuencias inmediatas del Teorema de la Base de Hilbert es que toda variedad algebraica es intersección de un número finito de hipersuperficies. En particualr, Si $V \subseteq \mathbb{K}^n$ es una variedad algebraica (un cerrado Zariski) dado mediante $V(\mathfrak{a})$, siendo $\mathfrak{a}$ un ideal en $k[X_1, \ldots, X_n]$, entonces $\mathfrak{a}$ es finitamente generado y se tiene $\mathfrak{a} = (f_1, \ldots, f_s)$ para un número finito de elementos $f_1, \ldots, f_s \in \mathfrak{a}$. Esto obviamente implica $V(\mathfrak{a}) = V(f_1, \ldots, f_s)$ y, por tanto:

$$V = V(\mathfrak{a}) = \bigcap_{i=1}^{s} V(f_i).$$

## 6.4. Dimensión en Anillos Noetherianos

Comencemos con una sencilla propiedad de los espacios topológicos neotherianos. Las nociones son esencialmente debidas a W. Krull[2]

Definición 38 (**Cerrado irreducible**). *Sea $(X, \mathcal{T})$ un espacio topológico, un cerrado $C$ de $X$ se dice irreducible si no se puede descomponer como unión de cerrados propios, es decirm si verifica*

$$C = V \bigcup W, \;\; V, W \in \mathcal{T}^c \Longrightarrow [C = V] \vee [C = W].$$

*Los cerrados que no son irreducibles se denominan reducibles.*

Proposición 6.4.1. *Sea $(X, \mathcal{T})$ un espacio toplógico noetheriano. Entonces todo cerrado posee una descomposicón única como unión finita de irreducibles. A los irreducibles que aparecen en esa descomposición se les denomina componenets irreducibles.*

Demostración. Se trata de usar, de modo evidente, la noción de Noetheriano. Consideremos el conjunto

$$\mathcal{F} := \{V \subseteq X \;:\; V \text{ es cerrado y no es unión finita de irreducibles}\}.$$

Suponganos, por reducción al absurdo, que este conjunto sea no vacío. Entonces posee un elemento minimal que denotaremos por $V$. Es claro que, como $V \in \mathcal{F}$, $V$ no puede ser irreducible (porque sería unión finita de irreducible), luego es reducible y existen $W_1, W_2$ dos cerrados tales que $W_i \subsetneq V$ y

$$V = W_1 \cup W_2.$$

Como $V$ es minimal en $\mathcal{F}$ concluiremos que $W_i \notin \mathcal{F}$, luego, por ser cerrados, han de ser unión finita de irreducibles. Pero, entonces, $V$ lo es también contradiciendo su minimalidad en $\mathcal{F}$ y permitiéndonos concluir que $\mathcal{F} = \emptyset$. Usando la minimalidad de todas las desomposiciones finitas podemos encontrar un mínimo y la unicidad. □

Proposición 6.4.2. *Sea $K$ un cuerpo $\mathbb{K}$ un cuerpo algebraicamente cerrado que le contiene. Un conjunto algebraico $K-$definible $V \subseteq \mathbb{K}^n$ es irreducible si y solamente si su ideal $I_K(V)$ es primo en $K[X_1, \ldots, X_n]$.*

[2]W. Krull estudió en Götingen bajo la dirección de F. Klein y E. Noether. Si bien F. Klein influyó en la comprensión de la matemática en un sentido amplio, E. Noether dejó en W. Krull todo un programa de trabajo que ella misma no pudo concluir por el advenimiento de los nazis al poder en Alemania. En su trabajo W. Krull *"Primidealketten in allgemeinen Ringbereichten"*. S.–B. Heildelberg Akad. Wiss. **7** (1928), introdujo la noción de dimensión de un anillo noetheriano, lo que le permitió alcanzar el enunciado del Teorema del Ideal Principal. Posteriormente influirá a geómetras como C. Chevalley y O. Zariski quienes, a a su vez, continuarían la obra de W. Krull. Entre sus obras, debe destacarse este trabajo de 1928, su trabajo sobre los anillos asociados a variedades algebraicas de 1938 (en el que introduce los anillos locales regulares) y, sobre todo, su texto W. Krull, *"Idealtheorie"*. Springer, 1935. Es a este texto y a su autor a quienes debemos la transformación del conjunto de resultados de P. Gordan, D. Hilbert y E. Noether, y sus respectivas escuelas, sobre Teoría de Invariantes en una nueva rama del conocimiento matemático hoy conocida como Álgebra Conmutativa.

Demostración. Es obvio y no necesita el Nullstellensatz. Sí necesita una cierta condición de separabilidad por polinomios. Así, si $I_K(V)$ es primo y si $V = W_1 \cup W_2$, entonces, existen $f \in I_K(W_1)$ y $g \in I_K(W_2)$ tales que

$$f\,|_{W_2} \neq 0, \quad g\,|_{W_1} \neq 0.$$

Simplementre porque $W_1 \neq W_2$. Pero $fg \in I_K(V)$ mientras que $f, g \notin I_K(V)$, contradiciendo la primalidad de $I_K(V)$.
Para el recíproco, si $fg \in I_K(V)$ y $V$ es irreducible, definamos

$$W_1 := V \cap V(f), \quad W_2 := V \cap V(g).$$

Tendremos $V = W_1 \cup W_2$ y, por ser $V$ irreducible, $V = W_1$ o $V = W_2$, lo que es equivalente a decir $f \in I_K(V)$ o $g \in I_K(V)$, lo que implica la primalidad de $I_K(V)$. □

Proposición 6.4.3. *En un anillo noetheriano $R$, todo ideal radical es una intersección finita de ideales primos, llamadas componentes primas del ideal.*

Demostración. Dado que todo ideal radical es intersección de primos, el argumento es el mismo de siempre usando la condición noetheriana. □

Observación 6.4.4. El anterior resultado entronca con el clásico Teorema de Lasker-Noether sobre desomposición primaria de ideales en anillo noteherianos que obviaremos por falta de tiempo.

**6.4.1. Dimensión de Krull en espacios topológicos noetherianos.** La noción de dimensión que vamos a desarrollar en esta parte del curso es una noción bien adapatada a los espacios topológicos neotherianos y basada en una noción intuitivamente muy simple, como son las cadenas de irreducibles. Ya nos hemos enfrentado a un ejemplo de esta noción : los anillos artinianos tiene un espacio topológico noethereiano de dimensión 0 y finito.

Definición 39. *Sea $(X, \mathcal{T})$ un espacio topológico noetheriano. Llamaremos dimensión de Krull de $X$ al máximo de las longitudses de cadenas de irreudcibles de $X$, es decir el máximo de los números naturales $n \in \mathbb{N}$ tales que existen :*

$$\emptyset \subsetneq V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n \subseteq X$$

*donde $V_0, \ldots, V_n$ son cerrados irreducibles de $X$.*

Ejemplo 6.4.5.
- Para un conjunto algebraico $V \subseteq K^n$, su dimensión de Krull es el máximo de las longitudes de cadenas de conjuntos algebraicos irreducibles contenidos en $V$.
- Lo mismo podemos decir de la dimensión de los conjuntos algebraicos proyectivos.
- Como primera observación concerniente a estos tres casos, si $K$ es un cuerpo infinito, la dimensión de un cerrado en las topologías de Zariski $K^n$ y $\mathbb{P}_n(K)$ de un cerrado 0 si y solamente si están formados por un conjunto finito de puntos.
- Dado un cerrado $V \subseteq Spec(A)$, llamaremos dimensión de Krull de $V$ al máximo de las longitudes de cadenas de irreducibles contenidos en $V$. En esta caso, podemos encontrar cerrados de dimensión 1 formados por un conjunto finitio de puntos.

Definición 40. *Llamaremos dimensión de Krull de un anillo $A$ a la dimensión de Krull de $Spec(A)$.*

Ejemplo 6.4.6. Los anillos artinianos tienen dimensión 0. Los conjuntos finitos de puntos de $K^n$ tienen dimensión de Krull 0.

DEFINICIÓN 41. *Sea $A$ un anillo y $\mathfrak{p}$ un ideal primo de $A$.*

i) *Llamaremos altura de $\mathfrak{p}$ al máximo de las longitudes de cadenas de ideales primos de $A$ contenidas en $\mathfrak{p}$, esto es, el máximo de los números naturales $n \in \mathbb{N}$ tales que exite :*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subseteq \mathfrak{p}$$

*donde $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ son ideales primos de $A$. Lo denotaremos por $ht(\mathfrak{p})$.*

ii) *Llamaremos coaltura de $\mathfrak{p}$ al máximo de las longitudes de cadenas de ideales primos de $A$ que contienen a $\mathfrak{p}$, esto es, el máximo de los números naturales $n \in \mathbb{N}$ tales que exite :*

$$\mathfrak{p} \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

*donde $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ son ideales primos de $A$. Lo denotaremos por $coht(\mathfrak{p})$.*

PROPOSICIÓN 6.4.7. *Sea $A$ un anillo. Sea tiene :*

i)

$$dim_{Krull}(A) = max\{ht(\mathfrak{p}) \ : \ \mathfrak{p} \in Spec(A)\} = max\{coht(\mathfrak{m}) \ : \ \mathfrak{m} \in Spm(A)\}$$

ii)

$$dim_{Krull}(A) = max\{coht(\mathfrak{p}) \ : \ \mathfrak{p} \in Spec(A)\}$$

iii) *Si $A$ es noetheriano,*

$$dim_{Krull}(A) = max\{coht(\mathfrak{p}) \ : \ \mathfrak{p} \in Ass(A)\}$$

DEMOSTRACIÓN. Para las dos primeras afirmaciones baste con observar la biyección existente entre los irreducibles de $Spec(A)$ y los ideales primos de $A$. La tercera, el caso noetheriano, se sigue del hecho de que los ideales primos minimales de $A$ están entre los ideales primos asociados a $A$. □

DEFINICIÓN 42. *Sea $\mathfrak{a}$ un ideal de un anillo $A$.*

i) *Llamaremos altura del ideal $\mathfrak{a}$ al ínfimo de las alturas de los ideales primos que contienen a $\mathfrak{a}$. Lo denotaremos por $ht(\mathfrak{a})$.*

ii) *Llamaremos coaltura del ideal $\mathfrak{a}$ al máximo de las coalturas de los ideales primos que contienen al ideal $\mathfrak{a}$. Lo denotaremos por $coht(\mathfrak{a})$.*

*En ocasiones a la altura se la denomina codimensión, mientras a la coaltura de la denomina dimensión del ideal.*

PROPOSICIÓN 6.4.8. *Sea $A$ un anillo, $\mathfrak{a}$ un ideal de $A$, $\mathfrak{p}$ un ideal primo de $A$.*

i)

$$dim_{Krull}(A/\mathfrak{a}) = coht(\mathfrak{a})$$

ii)

$$dim_{Krull}(A_{\mathfrak{p}}) = ht(\mathfrak{p})$$

iii)

$$ht(\mathfrak{a}) + coht(\mathfrak{a}) \leq dim_{Krull}(A)$$

DEMOSTRACIÓN. Las dos primeras afirmaciones son obvias para el conocimiento actual de los alumnos. En ucanto a la tercera, es fácil probarla para los ideales primos de $A$. Para un ideal cualquiera $\mathfrak{a}$, si $coht(\mathfrak{a}) = coht(\mathfrak{p})$ y $\mathfrak{p}$ es un primo que contiene a $\mathfrak{a}$, entonces, $\mathfrak{p}$ es minimal sobre $\mathfrak{a}$. De otro lado, $ht(\mathfrak{a})$ es elínfimo de las alturas de los primos minimales conteniendo al ideal $\mathfrak{a}$. □

DEFINICIÓN 43. *Sea $M$ un $A-$módulo. Llamaremos dimensión de Krull de $M$ a la dimensión del espacio topológico asociado a $M$ : $Supp(M)$, es decir,*

$$dim_{Krull}(M) = dim_{Krull}(Supp(M))$$

PROPOSICIÓN 6.4.9. *Si $A$ es un anillo noetheriano y $M$ es un $A-$módulo finitamente generado, se tiene :*

$$dim_{Krull}(M) = dim_{Krull}(A/Ann(M)) = coht(Ann(M))$$

DEMOSTRACIÓN. Obvio □

EJEMPLO 6.4.10.
- Si $K$ es un cuerpo algebraicamente cerrado y $V \subseteq K^n$ es un conjunto algebraico, se tiene :

$$dim_{Krull}(V) = dim_{Krull}(K[V]) = coht(I(V))$$

- Obsérvese que en cuerpos finitos, la dimensión de todo conjunto algebraico $V \subseteq K^n$ es 0, mientras los ideales pueden tener diversas alturas (cf. Problemas).
- Los dominions de ideales principales son anillos noetherianos cuya dimensión de Krull es igual a 1. El recíproco no es cierto. Baste copnsiderar el anillo $\mathbb{C}[X,Y]/(X^2+Y^2)$ que es un anillo noetehriano de dimensión de Krull igual a 1, pero el maximal definido por las clases de $X, Y$ no es rpincipal.
- Los anillos de valoración discreta y los dominios de Dedekind son de dimensión de Krull 1.

Es interesante observar el buen comportamiento de la dimensión de Krull con extensiones enteras de anillos. Eso es lo que vamos a ver en el siguiente :

TEOREMA 6.4.11. *Sea $A \subseteq B$ una extensión entera de anillos, entonces :*

$$dim_{Krull}(A) = dim_{Krull}(B)$$

DEMOSTRACIÓN. Usaremos las propiedades elementales demostradas en nuestro estudio de los teoremas del Ascenso y del Descenso. En primer lugar, la operación de contracción define una aplicación suprayectiva entre $Spec(B)$ y $Spec(A)$, que transforma ideales maximales de $B$ en ideales maximales de $A$. Recordemos también que no hay inclusión estricta entre los ideales primos de $B$ que se contraen sobre el mismo ideal primo de $A$. Así, consideremos una cadena de ideales primos de $B$ :

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

y sean $\mathfrak{p}_i := P_i \cap A$, sus contracciones en $A$. Por la propiedad sobre la inclusión estricta, $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$. Y tendremos

$$dim_{Krull}(B) \leq dim_{Krull}(A)$$

Recíprocamente, consideremos una cadena de ideales primos de $A$ :

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

Existirá $P_0$ un ideal primo de $B$ que se contrae sobre $\mathfrak{p}_0$. Aplicando el teorema del Ascenso, construiremos unos ideales primos $P_i$ de $B$ tales que $P_i$ se contrae sobre $\mathfrak{p}_i$ y la siguientees una cedna de ideales primos de $B$ :

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

luego

$$dim_{Krull}(A) \leq dim_{Krull}(B)$$

y hemos terminado la prueba. □

Podemos observar también la relación entre las nociones de dimensión que afectan a los conjuntos algebraicos proyectivos y sus partes afines. Para ello disponemos del siguiente :

TEOREMA 6.4.12 (Dimensión en $\mathbb{P}_n(K)$). *Sea $V \subseteq \mathbb{P}_n(K)$ un conjunto algebraico proyectivo, sin componentes en el hiperplano del infinito.*

i) *La dimensión de $V$ es igual a la dimensión de su cono propyectante menos uno, es decir :*

$$dim_{Krull}(V) = dim_{Krull}(\pi^{-1}(V)) - 1$$

ii) *Si $V$ no posee componentes en el hiperplano del infinito, sea $V \cap K^n$ la parte afín de $V$, entonces,*

$$dim_{Krull}(V) = dim_{Krull}(V \cap K^n)$$

iii) *Si $W \subseteq K^n$ es un conjunto algebraico afín, sea $\overline{W} \subseteq \mathbb{P}_n(K)$ su clausura proyectiva. Entonces,*

$$dim_{Krull}(V) = dim_{Krull}(W)$$

iv) *$V$ tiene dimensión de Krull 0 si y solamente si consta de un número finito de puntos.*

Demostración. Recordando que $\pi : K^{n+1} \setminus \{(0,\dots,0)\} \hookleftarrow \mathbb{P}_n(K)$ transforma conjuntos algebraicos en algebraicos, □

Proposición 6.4.13. *Sea $V \subseteq \mathbb{P}_n(K)$ un conjunto algebraico proyectivo, $K$ algebraicamente cerrado y $\mathfrak{m} := (X_0,\dots,X_n)$ ideal maximal de $K[X_0,\dots,X_n]$. Denotemos por $\overline{\mathfrak{m}} := \mathfrak{m}/\mathbb{I}(V)$ que es un ideal maximal del anillo graduado $K[V]$. Entonces,*

$$dim_{Krull}(V) + 1 \text{ ( en } \mathbb{P}_n(K) \text{ )} \geq ht(\overline{\mathfrak{m}}) \text{ ( en } K[V])$$

Demostración. Tenemos una biyección entre los conjuntos algebraicos irreducibles no vacíos contenidos en $V$ y los ideales primos homogéneos de $K[X_0,\dots,X_n]$ que contienen a $\mathbb{I}(V)$ y definen una variedad no vacía en $\mathbb{P}_n(K)$, luego se trata de probar que $ht(\overline{\mathfrak{m}})$ coincide con el máximo de las longitudes de cadenas de ideales primos homogéneos que definen una variedad no vacía en $\mathbb{P}_n(K)$ :

$$\mathbb{I}(V) \subseteq \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

La desigualdad es obvia, pues todo ideal primo homogéneo está contenido en $\mathfrak{m}$, basta con considerar la cadena :

$$\mathbb{I}(V) \subseteq \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r \subseteq \mathfrak{m}$$

Como $V_{\mathbb{P}_n(K)}(\mathfrak{p}_r) \neq \emptyset$, el último es un contenido estricto. □

Una curiosa propiedad de los anillos noetherianos relaciona factorialidad y altura de los ideales primos minimales sobre un ideal principal. Pero insistiremos en esa idea a la luz del Teorema del Ideal Principal de Krull. Por el momento veremos :

Lema 6.4.14. *Si $A$ es un dominio noetheriano y $f, g \in A \setminus \{0\}$, $f$ no unidad en $A$, entonces existe y es finito el número dado por :*

$$max\{n \in \mathbb{N} \,:\, f^n \mid g\}$$

Demostración. Si $f$ no divide a $g$ ese máximo es 0 y no hay nada que probar. En caso contrario, podríamos construir una cadena infinita creciente estrictamente de naturales positivos $k_n \in \mathbb{N}$, $n \in \mathbb{N}$ tales que $f^{k_n} \mid g$. Así las cosas, se $h_n \in A$ tal que $h_n f^{k_n} = g$ y tenemos la siguiente cadena ascendente de ideales de $A$ :

$$(h_0) \subseteq (h_1) \subseteq \cdots \subseteq (h_n) \subseteq \cdots$$

Para verlo, baste ver que $h_n$ es divisible por $h_{n+1}$.

$$g = h_n f^{k_n} = h_{n+1} f^{k_{n+1}} = h_{n+1} f^{k_{n+1}-k_n} f^{k_n}$$

Por ser $A$ dominio, $f \neq 0$ y $g \neq 0$, concluimos :

$$h_n = h_{n+1} f^{k_{n+1}-k_n}$$

Ahora la cadena ha de estabilizarse, luego :

$$h_{n+1} = u_{n+1}h_n$$

con lo cual, obtendremos

$$h_n = h_{n+1}f^{k_{n+1}-k_n} = u_{n+1}f^{k_{n+1}-k_n}h_n$$

De nuevo la condición de dominio de $A$ implicaría que $f$ es una unidad y habremos llegado a contradicción . □

LEMA 6.4.15. *Si $A$ es un dominio noetheriano, todo ideal primo, principal distinto de* $(0)$*, tiene altura* 1*.*

DEMOSTRACIÓN. Supongamos $\mathfrak{p} = (f)$ un ideal primo y principal de un dominio noetheriano $A$. Sea $\mathfrak{p}' \subseteq \mathfrak{p}$ un ideal primo estrictamemnte contenido en $\mathfrak{p}$. Supongamos que $\mathfrak{p}'$ no es el ideal $(0)$ de $A$ y sea $g \in \mathfrak{p}'$ un elemento no nulo de $\mathfrak{p}'$. Dado que $f$ no es unidad de $A$ y $f \neq 0$, sea $n$ la máxima potencia de $f$ que divide a $g$. Claramente $n \leq 1$ y tendremos :

$$g := hf^n$$

donde $h \notin \mathfrak{p}$. Ahora, si $f \notin \mathfrak{p}'$, concluiríamos $h \in \mathfrak{p}' \subseteq \mathfrak{p}$, $f$ divide a $h$ y tenemos una contradicción. □

LEMA 6.4.16. *Si $A$ es un dominion 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.*

DEMOSTRACIÓN. Supongamos que $\mathfrak{p} = (f)$, hallemos la mínima potencia de $f$ que se encuentra en $\mathfrak{q}$ : $f^r \in \mathfrak{q}$. Es claro que $\mathfrak{p}^r = (f^r) \subseteq \mathfrak{q}$, pero veamos el recíproco : Si $g \in \mathfrak{q}$, sea $n$ la máxima potencia de $f$ que divide a $g$. Entonces, $g = hf^n$ y $h \notin \mathfrak{p}$. Entonces, por ser $\mathfrak{q}$ primario, $f^n \in \mathfrak{q}$, luego $n \geq r$ y $g \in (f^r) = \mathfrak{p}^r$. □

PROPOSICIÓN 6.4.17. *Un dominio noetheriano $A$ es un dominio de factorización única si y solamente si los ideales primos asociados a un ideal principal son también principales.*

DEMOSTRACIÓN. Supongamos que $A$ es un D.F.U. y sea $(f)$ un ideal principal. Entonces, existen elemntos primos distintos $f_1, \ldots, f_n \in A$ tales que :

$$f := f_1^{k_1} \cdots f_n^{k_n} \qquad (*)$$

Obsérvese que

$$(f_1^{k_1}) \cdots (f_n^{k_n}) = (f_1^{k_1}) \cap \cdots \cap (f_n^{k_n})$$

Para verlo baste hacer inducción en $n$. Si $n = 1$, no hay nada que probar. Para el caso $n \geq 2$, sea $g \in (f_1^{k_1}) \cap \cdots \cap (f_n^{k_n})$ y sea $k$ l máxima potencia de $f_1$ que divide a $g$ . Entonces, $k \geq k_1$ y supongamos $g = hf^k$. Claramente $f$ no divide a $h$ y $f^k$ no es un elemento de $(f_i)$ para $2 \leq i \leq n$. Por lo tanto, siendo $(f_i^{k_i})$ un ideal primario, $h \in (f_i^{k_i})$, $2 \leq i \leq n$. Aplicando la hipótesis inductiva habremos terminado.
Por lo tanto, la identidad $(*)$ nos ofrece una descomposición primaria del ideal $(f)$ con primos asociados $(f_1), \ldots, (f_n)$. Como son todos distintos, la descomposición primaria es irredundante y los ideales primos asociados a $A/(f)$ son justamente los de esta lista. Para ver el recíproco, sea $f \in A$ un elemento no nulo y no unidad. Sea

$$(f) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

una descomposición primaria irredundante del ideal $(f)$ de $A$, donde $\mathfrak{q}_i$ es $\mathfrak{p}_i-$primario. En consecuencia, $\mathfrak{p}_i = (f_i)$ donde $f_i$ es primo e irreducible de $A$. En particular, $\mathfrak{q}_i := (f_i^{k_i})$ y tendremos, usando un argumento similar al del apartado anterior, que :

$$(f) := (f_1^{k_1} \cdots f_n^{k_n})$$

Luego existe una unidad $u \in A$ tal que :

$$f = uf_1^{k_1} \cdots f_n^{k_n}$$

La unicida de la factorización se seguirá de la unicidad de las descomposiciones primarias en anillos noetherianos, con escaso esfuerzo adicional. □

### 6.4.2. El Polinomio de Hilbert-Samuel.

DEFINICIÓN 44. *Sea $f : \mathbb{N} \longrightarrow \mathbb{Q}$ una aplicación. Diremos que $f$ es una aplicación polinomial si existen $n_0 \in \mathbb{N}$ y $q \in \mathbb{Q}[T]$ tales que :*

$$f(n) = q(n), \ \ \forall n \geq n_0$$

PROPOSICIÓN 6.4.18. *Si $f : \mathbb{N} \longrightarrow \mathbb{Q}$ es una aplicación polinomial, existe un único polinomio $q \in \mathbb{Q}[T]$ que coincida con $f$ salvo en un número finito de puntos. Así, podemos hablar del coeficiente director de $f$ y del grado de $f$ como el coeficiente director y el grado del polinomio asociado.*

DEMOSTRACIÓN. Baste notar que dos polinomios de $\mathbb{Q}[T]$ no pueden tener un número inifinito de raíces comunes en $\mathbb{N}$. □

NOTACIÓN 6.4.19.

- Si el polinomio asociado a una función polinomial es el polinomio nulo, diremos que el grado de la función polinomial es $-1$. Si es una constante no nule, diremos que el grado de $f$ es 0.
- Sea $f : \mathbb{N} \longrightarrow \mathbb{Q}$ una aplicación cualquiera. Por inducción en $r$, definiremos las aplicaciones incremento siguientes :

$$\Delta^0(f) := f$$

$$\Delta^r(f) := \Delta^{r-1} f(n+1) - \Delta^{r-1} f(n)$$

LEMA 6.4.20. *Sea $f : \mathbb{N} \longrightarrow \mathbb{Q}$ una aplicación. Entonces, $f$ es un aplicación polinomial de grado $d$ si sy solamente si $\Delta f : \mathbb{N} \longrightarrow \mathbb{Q}$ es una función polinomial de grado $d-1$. Además, el coeficiente director de $f$ es el coeficiente director de $\Delta f$ dividido por $d$.*

DEMOSTRACIÓN.

- Es casi obvio, si $q \in \mathbb{Q}[T]$ es el polinomio asociado a $f$, el polinomio asociado a $\Delta f$ es el polinomio dado por :

$$q'(T) := q(T+1) - q(T) \in \mathbb{Q}[T]$$

que tiene claramente grado $d-1$ y su coeficiente director es dado por la siguiente regla de cálculo : Si $q(T) := \sum_{i=0}^{d} a_k T^k$,

$$q'(T) := \sum_{k=0}^{d} a_k((T+1)^k - T^k) = da_d T^{d-1} + g(T)$$

donde $g$ es un polinomio de grado a lo más $d-2$.

- Es la parte más importante de la prueba y la que nos dará argumentos inductivos más adelante. Supongamops $h \in \mathbb{Q}[T]$ una función polinomial de grado $d-1$ coincidiendo con $\Delta f$. Hagamos inducción en $deg(h)$.
  - Si $deg(h) = 0$, entonces, $\Delta f$ es una constante. Supongamos $c \in \mathbb{Q}$ tal que $\Delta f(n) = c$ para $n \geq n_0$. Tenemos la siguiente relación :

$$f(n+1) = f(n) + c, \ \forall n \geq n_0$$

En este caso, sea $a := f(n_0)$ y se tiene :

$$f(n) := c(n - n_0) + a$$

- Supuesto probado para el caso $deg(h) \geq r-1$, veamos qué sucede con el caso $deg(h) = r$ : Sea

$$h(t) := a_r T^r + \cdots + a_0$$

y tenemos la siguiente relación para $n \geq n_0$ :

$$\Delta f(n) = f(n+1) - f(n) = \frac{a_r}{r+1}\left[(n+1)^{r+1} - n^{r+1} + g(n)\right]$$

donde $g \in \mathbb{Q}[T]$ es un polinomio de grado menor o igual que $r-1$. Definamos ahora la aplicación polinomial :

$$f^*(n) := f(n) - \frac{a_{r+1}}{r+1}$$

Observamos que

$$\Delta f^* = f^*(n+1) - f^*(n) = g(n)$$

Aplicando la hipótesis inductiva podremos concluir que $f^*$ es una aplicación polinomial de grado $r$ y, por su definición, también $f$ ha de ser una aplicación polinomial (de grado $r+1$ en este caso). Las relaciones entre los coeficientes directores son obvias.

□

*6.4.2.1.* **Algunas Hipótesis.**

- Sea $A := \oplus_n A_n$ un anillo graduado. Supongamos que el anillo $A_0$ es un anillo artiniano y que existan elementos $x_1, \ldots, x_r \in A_1$ generando $A$ como $A_0-$álgebra. Por lo visto en la Sección **??** el anillo $A$ es noetheriano.
- En las mismas condiciones, sea $M := \oplus_n M_n$ un $A-$módulo graduado finitamente generado. Por ser $A$ noetheriano, $M$ es también noetheriano y cada subgrupo $M_n$ es un $A_0-$módulo finitamente generado. Como $A_0$ es artiniano, cada $M_n$ es un $A_0-$módulo artiniano y, por ende, de longitud finita. Tiene sentido, pues, considerar :

$$\ell_{A_0}(M_n)$$

PROPOSICIÓN 6.4.21 (Polinomio de Hilbert). *Bajo las hipótesis anteriormente descritas, la siguiente función $\chi(M,-)$, dada por :*

$$\chi(M,-)\mathbb{N} \longrightarrow \mathbb{N}$$

$$\chi(M,n) := \ell_{A_0}(M_n)$$

*es una aplicación polinomial de grado menor o igual que $r-1$ (recordemos que $r$ es el número tal que $x_1, \ldots, x_r \in A_1$, generan $A$ como $A_0-$álgebra).*

DEMOSTRACIÓN. Haremos la demostración por inducción en $r$.

- $r = 0$ : En este caso $A = A_0$. Ahora, dado un conjunto finito $S$ de generadores homogéneos de $M$ como $A_0-$módulo, sea :

$$n_0 := max\{deg(s) \ : \ s \in S\}$$

Claramente, $M_n = (0)$ para $n \geq n_0$ y se tiene $\chi(M,n) = 0$, para $n \geq n_0$.

- $r \geq 1$ : Supongamos que el resultado es cierto para todos los módulos graduados finitamente generados sobre anillos graduados noetherianos, verificando las hipótesis anteriores, cuyos generadores en $A_1$ como $A_0-$módulos son menos de $r-1$. Consideremos el siguiente morfismo graduado de grado 1 entre $A-$módulos :

$$(x_r)_M \ : M \longrightarrow M$$

dado por $(x_r)_M(m) := x_r m$. Ahora, $x_r M_n \subseteq M_{n+1}$ nos permite considerar las restricciones a $M_n$ de ese morfismo y obtener morfismos de $A_0-$módulos

$$\varphi_n := x_r \mid_{M_n} : M_n \longrightarrow M_{n+1}$$

la cual nos permite construir la siguiente sucesión exacta de $A_0-$módulos :

$$0 \longrightarrow K_n \longrightarrow M_n \longrightarrow M_{n+1} \longrightarrow C_{n+1} \longrightarrow 0$$

donde $K_n := Ker(\varphi_n)$, y

$$C_{n+1} := M_{n+1}/Im(\varphi_n)$$

Definamos :

$$K := Ker(x_r)_M := \bigoplus_n K_n, \quad C := \bigoplus_{n \geq -1} (M_{n+1})/Im(\varphi_n) = M/Im(x_r)_M = CoKer(x_r)_M$$

Tanto $K$ como $C$ son dos $A-$módulos noetherianos y se verifican las hipótesis anteriores a la Proposición, luego podemos considerar $\chi(K,-)$ y $\chi(C,-)$, observando la siguiente relación :

$$\Delta\chi(M,-) := \chi(C, n+1) - \chi(K, n)$$

Ahora bien, tanto $C$ como $K$ son $A'-$módulos, cuando $A'$ es el módulo graduado $A/(x_r)$, con la graduación cociente (que tiene sentido por ser $x_r$ un elemento homogéneo de grado 1). Ahora observamos que $x_r \in Ann_A(K)$ y $x_r \in Ann_A(C)$, luego sus estructuras como $A-$módulos u su estructura como $A'-$módulos coinciden. Lo mismo se puede decir de las graduaciones y observamos que $A'$ está generado como $A_0-$álgebra por las clases módulo $(x_r)$ definidas por $\{x_1, \ldots, x_{r-1}\}$. Podemos aplicar la hipótesis inductiva y $\chi(K,-)$ y $\chi(C,-)$ son aplicaciones polinomiales de grado menor o igual que $r-2$. Retomando el Lema previo, $\chi(M,-)$ será una aplicación polinomial de grado a lo más $r-1$.

□

Definición 45. *A la función $\chi(M,-)$ se la denomina función de Hilbert de $M$. Al polinomio en $\mathbb{Q}[T]$ coincidente con $\chi(M,-)$ se le denomina polinomio de Hilbert y se le denota también por $\chi(M,-)$. Al grado de $\chi(M,-)$ se le denomina dimensión de Hilbert de $M$ y a su coeficiente director se le denomina grado de $M$. Al número natural $n_0$ tal que la función polinomial coincide con el polinomio se le denomina "regularidad de la función de Hilbert" de $M$.*

Ejemplo 6.4.22. ▪ Sea $V \subseteq \mathbb{P}_n(K)$ un conjunto algebraico proyectivo. Consideremos $I(V)$ que es un ideal homogéneo de $K[X_0, \ldots, X_n]$ y consideremos el anillo graduado cociente :

$$K[V] := K[X_0, \ldots, X_n]/I_K(V)$$

Este es un anillo graduado, noetheriano, cuyos elementos homogéneos de grado 0 son justamente los elementos del cuerpo $K$. Si denotamos por $\mathfrak{h}_n(V)$ los elementos homogéneos de grado $n$ en $I(V)$, tendremos que la función de Hilbert de $K[V]$ viene dada por :

$$\chi(K[V], m) := dim H_m(X_0, \ldots, X_n) - dim \mathfrak{h}_m(V)$$

para cualquier $m \in \mathbb{N}$, donde la dimensión se refiere a la dimensión como $K-$espacio vectorial. En particular, observamos que el grado de $\chi(K[V],-)$ está acotado por $n$ y es una función polinomial. Así, el grado de la función de Hilbert de $\mathbb{P}_n(K)$ es justamente $n$ y el grado de la función de Hilbert de $\emptyset$ es justamente $-1$. Llamaremos dimensión del Hilbert de $V$ al grado de ese

polinomio de Hilbert de $K[V]$. Y llamaremos grado proyectivo de $V$ al valor dado por :

- Si $a_0$ es el coeficiente director de $\chi(K[V], -)$.
- Y si $d$ es el grado de $\chi(K[V], -)$,

El grado de $V$ es dado por :

$$a_0 d!$$

Volveremos más adelante sobre estas nociones.

- Demos un método para calcular la función de Hilbert de este anillo :
  - Sean $\{g_1, \ldots, g_s\}$ polinomios homogéneos, $deg(g_i) = m_i$, generando $I(V)$.
  - Para $m \geq max\{m_1, \ldots, m_s\}$, se observa que un polinomio homogéneo de grado $m$, $f \in K[X_+0, \ldots, X_n]$, está en $\mathfrak{h}_m(V)$ si y solamente si existen polinomios homogéneos $h_i$ de grado $m - m_i$ tales que

$$f = \sum_{i=1}^{s} h_i g_i$$

  - El procedimiento será como sigue :
    - Considerar todos los monomios

$$\beta := \{X^\mu \ : \ \mu \in \mathbb{N}^{n+1}, \mid \mu \mid \leq m\}$$

      como base de $H_m(X_0, \ldots, X_n)$.
    - Considerar todos los monomios de la forma :

$$\{X^\mu g_i \ : \mid \mu \mid = m - m_i\}$$

      por sus coordenadas en la base $\beta$.
    - Sea $A$ la matriz cuyas filas son los vectores de la anterior colección. Entonces, el rango de $A$ es la dimensión de $\mathfrak{h}_m(V)$ y podemos calcular la función de Hilbert de $K[V]$ por ser conocido

$$dim H_m(X_0, \ldots, X_n) = \binom{m+n}{n}$$

- Consideremos ahora $(A, \mathfrak{m})$ un anillo local noetheriano. Llamaremos "ideal de definición" de $A$ a todo ideal $\mathfrak{q}$ tal que $\sqrt{\mathfrak{q}} = \mathfrak{m}$, es decir, tal que existe $n \in \mathbb{N}$, $n \geq 1$ tal que :

$$\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$$

Sea ahora $M$ un $A-$módulo finitamente generado y consideremos tanto en $A$ como en $M$ la filtración $\mathfrak{q}-$ádica, definida por el ideal $\mathfrak{q}$, así como los graduados (anillos y módulo) asociados :

$$G_\mathfrak{q}(A) := \bigoplus_{n \in \mathbb{N}} \mathfrak{q}^n / \mathfrak{q}^{n+1}, \quad G_\mathfrak{q}(M) := \bigoplus_{n \in \mathbb{N}} \mathfrak{q}^n M / \mathfrak{q}^{n+1} M$$

Por ser $\mathfrak{q}$ un ideal de definición de $A$ y $A$ un anillo local de maximal $\mathfrak{m}$, el único maximal de $A/\mathfrak{q}$ es $\mathfrak{m}/\mathfrak{q}$, por lo que éste anillo es artiniano. Además, las clases módulo $\mathfrak{q}^2$ de los elementos de $\mathfrak{q}$ generan $G_\mathfrak{q}(A)$ como $A/\mathfrak{q}-$álgebra. Dado que $\mathfrak{q}$ es finitamente generado, las clases defnidas por los generadores de $\mathfrak{q}$ en $\mathfrak{q}/\mathfrak{q}^2$, generan $G_\mathfrak{q}(A)$ como $A/\mathfrak{q}-$álgebra. Además, $G_\mathfrak{q}(M)$ es un $G_\mathfrak{q}(A)-$módulo finitamente generado.

PROPOSICIÓN 6.4.23. *Si $(A, \mathfrak{m})$ es un anillo local noetheriano, $\mathfrak{q}$ un ideal de definición de $A$ y $M$ un $A-$módulo finitamente gereando, las funciones $\chi(G_\mathfrak{q}(M), -)$ y $\chi(G_\mathfrak{q}(A), -)$ son Aplicaciones polinomiales y su grado está cotado por $r - 1$, donde $r$ es el mínimo de los cardinales de conjuntos generadores de $\mathfrak{q}$ como ideal de $A$.*

Demostración. La prueba ha sido desarrollada en la discusión del ejemplo anterior. □

Ejemplo 6.4.24. Bajo las hipótesis del apartado *ii)* del ejemplo anterior, observemos que

$$Supp(M/\mathfrak{q}^n M) = \{\mathfrak{m}\}$$

como $A-$módulo. Claramente, pues $\mathfrak{q}^n$ tiene que estar contenido en $Ann_A(M)$, luego $\mathfrak{m}$ es el único ideal primo de $A$ que contiene a $\mathfrak{q}^n$. Dicho de otra manera, $M/\mathfrak{q}^n M$ es un $A-$módulo finitamente generado y su soporte está formado solamente por ideales maximales de $A$. Por el Teorema de Akizuki para módulos, deducimos que $M/\mathfrak{q}^n M$ es un $A-$módulo de longitud finita y podemos considerar :

$$\ell_A(M/\mathfrak{q}^n M) < +\infty$$

Proposición 6.4.25 (**Polinomio de P. Samuel**). *En las condiciones de los ejemplos anteriores, definamos la función de Samuel de $M$ :*

$$P_{\mathfrak{q}}(M, -) : \mathbb{N} \longrightarrow \mathbb{N}$$

*dada por :*

$$P_{\mathfrak{q}}(M, n) := \ell_A(M/\mathfrak{q}^n M)$$

*Entonces, $P_{\mathfrak{q}}(M, -)$ es una función polinomial cuyo grado está acotado por el mínimo de los cardinales de los conjuntos generadores de $\mathfrak{q}$. Además se tiene la siguiente relación :*

$$\Delta P_{\mathfrak{q}}(M, n) = \chi(G_{\mathfrak{q}}(M), n)$$

Demostración. Consideremos la siguiente sucesión exacta corta de $A/\mathfrak{q}-$módulos :

$$0 \longrightarrow \mathfrak{q}^n M/\mathfrak{q}^{n+1} M \longrightarrow M/\mathfrak{q}^{n+1} M \longrightarrow M/\mathfrak{q}^n M \longrightarrow 0$$

donde el último morfismo es la proyección canónica. Se trata de una sucesión exacta corta de $A-$módulos de longitud finita puesto que $Supp(\mathfrak{q}^n M/\mathfrak{q}^{n+1} M) = \{\mathfrak{m}\}$ es el único maximal de $A$. Tenemos la siguiente relación entre las respectivas longitudes :

$$\ell_A(M/\mathfrak{q}^{n+1} M) - \ell_A(M/\mathfrak{q}^n M) = \ell_A(\mathfrak{q}^n M/\mathfrak{q}^{n+1} M)$$

Ahora,

$$\mathfrak{q} \subseteq Ann_A(\mathfrak{q}^n M/\mathfrak{q}^{n+1} M)$$

luego la estructura de $A-$módulo y la de $A/\mathfrak{q}-$módulo en $\mathfrak{q}^n M/\mathfrak{q}^{n+1} M$ coinciden. Tambi'en lo hará la longitud (que sólo depende de los respectivos submódulos). Podremos concluir así :

$$\Delta P_{\mathfrak{q}}(M, n) := P_{\mathfrak{q}}(M, n+1) - P_{\mathfrak{q}}(M, n) = \chi(G_{\mathfrak{q}}(M), n)$$

y tenemos el resultado apetecido. □

Nos queda por observar que el grado del polinomio de Samuel no depende del ideal de definición elegido. Eso nos lo garantiza la siguiente :

Proposición 6.4.26. *Sea $(A, \mathfrak{m})$ un anillo local noetheriano, $\mathfrak{q}$ un ideal de definición de $A$ y $M$ un $A-$módulo finitamente generado. Entonces, los grados de los polinomios de Samuel $P_{\mathfrak{q}}(M, -)$ y $P_{\mathfrak{q}}(M, -)$ coinciden. En particular, el grado del polinomio de Samuel no depende el ideal de definición elegido. Llamaremos dimensión de Samuel de $M$ al grado de su polinomio de Samuel con respecto a cualquier ideal de definición de $(A, \mathfrak{m})$.*

Demostración. Sea $m \in \mathbb{N}$ tal que $\mathfrak{m}^n \subseteq \mathfrak{q}\mathfrak{m}$. Para cada $n \in \mathbb{N}$ tenemos :

$$\mathfrak{m}^{nm} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$$

con lo que podemos considerar los siguientes epimorfismos de $A-$módulos :

$$M/\mathfrak{m}^n M \longrightarrow M/\mathfrak{q}^n M$$
$$M/\mathfrak{m}^{nm} M \longrightarrow M/\mathfrak{q}^n M$$

Por lo tanto, tendremos :

$$\ell_A(M/\mathfrak{m}^n M)\ell_A(M/\mathfrak{q}^n M) \leq \ell_A(M/\mathfrak{m}^{nm} M)$$

Lo que se transforma en la siguiente relación entre funciones de Samuel :

$$P_{\mathfrak{m}}(M,n) \leq P_{\mathfrak{q}}(M,n) \leq P_{\mathfrak{m}}(M,nm)$$

Dado que tanto $P_{\mathfrak{m}}(M,-)$ como $P_{\mathfrak{q}}(M,-)$ son funciones polinomiales, la anterior relación implica una relación de igualdad de grado. □

Observación 6.4.27. Los coeficientes directores de los polinomios de Samuel son posiotivos, pues $M/\mathfrak{q}^n M = (0) \Rightarrow M = (0)$ por el Lema de Nakayama. Luego, salvo en ese caso, $P_{\mathfrak{q}}(M,n) \geq 0$, De otro lado, si $d = deg(P_{\mathfrak{q}}(M,T)) = deg(P_{\mathfrak{m}}(M,T))$ sea $a_d$ el coeficiente director de $P_{\mathfrak{q}}(M,T)$ mientras $b_d$ es el coeficiente director de $P_{\mathfrak{m}}(M,T)$. Ambos son números racionales positivos y verificarán la relación :

$$b_d \leq a_d \leq b_d m^d$$

donde $m$ es tal que $\mathfrak{m}^m \subseteq \mathfrak{q} \subseteq \mathfrak{m}$.

Un instrumento técnico de gran utilidad en lo que sigue es la siguiente Proposición que relaciona los polinomios de Samuel y las sucesiones exactas cortas :

Proposición 6.4.28. *Sea $(A,\mathfrak{m})$ un anillo local noetheriano, $\mathfrak{q}$ un ideal de definición de $A$ y la sucesión exacta corta de $A-$módulos finitamente generados :*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

*Entonces, existe una aplicación polinomial $R : \mathbb{N} \longrightarrow \mathbb{Q}$, cuyo grado es estrictamente menor que el grado de $P_{\mathfrak{q}}(M,T)$, siendo el coeficiente director de $R$ no negativo, y verificándose :*

$$P_{\mathfrak{q}}(M',n) + P_{\mathfrak{q}}(M'',n) = P_{\mathfrak{q}}(M,n) + R(n), \ \ \forall n \in \mathbb{N}$$

Demostración. A partir de nuestra sucesión exacta corta, podemos obtener la siguiente :

$$0 \longrightarrow M'/(M' \cap \mathfrak{q}^n M) \longrightarrow M/\mathfrak{q}^n M \longrightarrow M''/\mathfrak{q}^n M'' \longrightarrow 0$$

que es también una sucesión exacta corta de $A-$módulos de longitud finita. Tendremos la siguiente relación :

$$\ell_A\left(M/\mathfrak{q}^n M\right) = \ell_A(M''/\mathfrak{q}^n M'') + \ell_A(M'/(M' \cap \mathfrak{q}^n M)\big) \qquad (*)$$

Denotemos por $M'_n := M' \cap \mathfrak{q}^n M$, submódulo de $M'$ y tendremos una filtración en $M'$ definida por la filtración $\mathfrak{q}-$ádica de $M$. Por el Lema de Artin-Rees, existirá un $n_0 \in \mathbb{N}$ tal que

$$\mathfrak{q}M'_n = M'_{n+1}, \quad \forall n \geq n_0$$

En particualr, para cada $n \in \mathbb{N}$, tendremos :

$$\mathfrak{q}^{n_0+n} M' \subseteq M'_{n+n_0} = \mathfrak{q}^n M'_{n_0} \subseteq \mathfrak{q}^n M'$$

lo que supone en términos de longitudes :

$$\ell_A(M'/\mathfrak{q}^n M') \leq \ell_A(M'/M'_{n+n_0}) \leq \ell(M'/\mathfrak{q}^{n+n_0} M') \qquad (**)$$

En otras notaciones :

$$P_{\mathfrak{q}}(M', n) \leq \ell_A(M'/M'_{n+n_0}) \leq P_{\mathfrak{q}}(M', n + n_0)$$

Resulta claro que tanto $P_{\mathfrak{q}}(M, -)$ como $\ell_A(M'/M'_n)$ son aplicaciones polinomiales. La primera por el resultado de Samuel y la segunda por la identidad descrita en $(*)$. La relación $(**)$ nos garanetiza que ambas funciones polinomiales poseen el mismo grado y el mismo coeficiente director. Podemos considerar $R : \mathbb{N} \longrightarrow \mathbb{Q}$ dada por :

$$R(n) := P_{\mathfrak{q}}(M, n) - \ell_A(M'/M'_n)$$

Por la relación $(**)$ deducimos también que $R$ es positiva a partir de $n_0$, luego su coeficiente director es un número no negativo. Finalmente, es claro de la relación $(*)$ que $R$ verifica las propiedades requeridas :

$$P_{\mathfrak{q}}(M', n) + P_{\mathfrak{q}}(M'', n) = P_{\mathfrak{q}}(M, n) + R(n), \quad \forall n \in \mathbb{N}$$

□

Definición 46. *Llamaremos dimensión de Samuel ( o de Hilbert-Samuel) de un $A-$módulo $M$ verifiucando las propiedades anteriormente descritas al grado de $P_{\mathfrak{q}}(M, T)$, para cualquier ideal de definición $\mathfrak{q}$ de $(A, \mathfrak{m})$.*

Corollario 6.4.29. *Sea $(A, \mathfrak{m})$ un anillo local noetheriano, $\mathfrak{q}$ un idela de definición de $A$, $M$ un $A-$módulo finitamente generado y $N$ un submódulo de $M$. Entonces,*

$$dim_{Hilbert-Samuel}(N) \leq dim_{Hilbert-Samuel}(M)$$

$$dim_{Hilbert-Samuel}(M/N) \leq dim_{Hilbert-Samuel}(M)$$

Demostración. Baste tomar la sucesión exacta corta :

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

yaplicar la Proposición anterior. Entonces,

$$P_{\mathfrak{q}}(N, n) + P_{\mathfrak{q}}(M/N, n) = P_{\mathfrak{q}}(M, n) + R(n)$$

dado que el grado de $R$ es menor estricto que el grado de $P_{\mathfrak{q}}(M, -)$, y que la función de Samuel es positiva, tendremos que los coeficientes directores de $P_{\mathfrak{q}}(N, -)$ y $P_{\mathfrak{q}}(M/N, -)$ son números positivos y los grados no son mayores que el grados de $P_{\mathfrak{q}}(M, -)$ □

Un bonita manera de ver el comportamiento del polinomio de Samuel, será la dada por la siguiente argumentación :

Proposición 6.4.30. *Sea $(A, \mathfrak{m})$ un anillo local noetheriano. Sea $K := A/\mathfrak{m}$ el cuerpo cociente, por se $\mathfrak{m}$ un ideal maximal. Ahora observamos que para $\{x_1, \ldots, x_r\} \subseteq \mathfrak{m}$ son equivalentes :*

- *Las clases $\{x_1 + \mathfrak{m}^2, \ldots, x_r + \mathfrak{m}^2\}$ son una base del $K-$espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$.*
- *$\{x_1, \ldots, x_r\}$ son un sistema generador de cardinal minimal del ideal $\mathfrak{m}$.*

Demostración. Para demostrar este resultado, baste observar que, gracias al Lema de Nakayama, si $\{x_1 + \mathfrak{m}^2, \ldots, x_r + \mathfrak{m}^2\}$ generan $\mathfrak{m}/\mathfrak{m}^2$ como $K-$espacio vectorial, también lo generan como $A-$módulo, luego generan $\mathfrak{m}$ como ideal de $A$. Si hubiera un sistema generador de $\mathfrak{m}$ como ideal con menos de $r$ elementos, sus clases módulo $\mathfrak{m}^2$ generarían $\mathfrak{m}/\mathfrak{m}^2$ como espacio vectorial, contraviniendo la hipótesis de que $r$ es la dimensión de tal esopacio. Recíprocamente, si $\{x_1, \ldots, x_r\}$ son de cardinal minimal generando $\mathfrak{m}$ como ideal, sus clases son un sistema generador del espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$. Si no fueran una base, un subconjunto propio suyo también generaría ese espacio vectorial y, levantando con Nakayama, generaría $\mathfrak{m}$ como ideal, contradiciendo la minimalidad de $r$. □

Esta afirmación sobre $\mathfrak{m}/\mathfrak{m}^2$ tiene su interés en el siguiente :

COROLLARIO 6.4.31. *En las notaciones anteriores, sea $(A, \mathfrak{m})$ un anillo local noetheriano y $r$ el mínimo de los cardinales de los generadores de $\mathfrak{m}$ como ideal de $A$. Entonces, $P_{\mathfrak{m}}(A, T)$ tiene grado $r$ si y sólo si $G_{\mathfrak{m}}(A)$ es un anillo de polinomios en $r$ variables con coeficientes en el cuerpo $K := A/\mathfrak{m}$.*

DEMOSTRACIÓN. Sean $\{x_1, \ldots, x_r\}$ un conjunto de cardinal minimal de generadores de $\mathfrak{m}$ como ideal de $A$. Definamos el epimorfismo de $K-$álgebras graduadas de grado 0 :

$$\varphi \ : K[X_1, \ldots, X_r] \longrightarrow G_{\mathfrak{m}}(A)$$

donde $\varphi(X_i) = x_i$, $1 \leq i \leq r$. El grado del polinomio de Samuel es $r$ si y solamente si $\varphi$ es un isomorfismo. Para verlo, baste con tomar $\mathfrak{a} := Ker(\varphi)$ ideal de $K[X_1, \ldots, X_r]$. Tomemos los respectivos polinomios de Hilbert, para lo cual consideramos la sucesión exacta corta :

$$0 \longrightarrow \mathfrak{a} \cap H_m(X_1, \ldots, X_r) \longrightarrow H_m(X_1, \ldots, X_r) \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow 0$$

Como $\mathfrak{a}$ es un ideal homogéneo de $K[X_1, \ldots, X_r]$, $\mathfrak{a}_m := \mathfrak{a} \cap H_m(X_1, \ldots, X_r)$ son los polinomios homogéneos de grado $m$ en $\mathbb{I}$. dado que una de las implicaciones es evidente, supongamos que el grado del polinomio de Hilbert es $r-1$. A partir de la sucesión exacta anterior, tendremos la siguiente relación :

$$\chi(G_{\mathfrak{m}}(A), n) = \binom{n+r-1}{r-1} - \ell_A(\mathfrak{a}_n)$$

Sea ahora $f \in \mathfrak{a}_d$ un elemento homogéneo no nulo de grado $d$. Para cada número natural $n \in \mathbb{N}$, se tiene $fH_n(T_1, \ldots, T_r) \subseteq \mathbb{I}_{n+d}$. Como $K[T_1, \ldots, T_r]$ es un dominio de integridad, $f$ no es divisor de cero y la homotecia definida por $f$ es inyectiva, luego

$$dim_K(fH_n(T_1, \ldots, T_r)) = dim_K(H_n(T_1, \ldots, T_r)$$

En particular, concluimos la siguiente relación entre longitudes :

$$\ell_K(\mathfrak{a}_{n+1}) \geq \ell_K(fH_n(T_1, \ldots, T_r))\ell_K(H_n(T_1, \ldots, T_r) \geq \ell_K(\mathfrak{a}_n)$$

Tendremos que los polinomios de Hilbert de $K[T_1, \ldots, T_r]$ e $\mathfrak{a}$ son aplicaciones polinomiales del mismo grado y mismo coeficiente director. De la igualdad $(*)$ deduciríamos $deg(\chi(G_{\mathfrak{m}}(A), -) < r - 1$. □

COROLLARIO 6.4.32. *En las mismas hipótesis anteriores, para cualquier ideal de definición $\mathfrak{q}$ de $A$, $deg(P_{\mathfrak{q}}(A, -)) = r$ si y solamente si $G_{\mathfrak{m}}(A)$ es un anillo de polinomios en $r$ variables.*

**6.4.3. Teorema de la Dimensión Local.** El objetivo de esta Sección es demostrar el Teorema de dimensión local para anillos locales noetherianos y módulos finitamente generados sobre estos anillos. Así como algunas de sus consecuencias más inmediatas. Además de la dimensión de Krull en anillo y módulos, disponemos de las siguientes nociones de dimensión :

DEFINICIÓN 47. *Dado $(A, \mathfrak{m})$ un anillo local noetheriano y $M \neq (0)$ un $A-$módulo finitamente generado, llamaremos dimensión de Chevalley de $M$, y lo denotaremos por $dim_{Chevalley}(M)$, al mínimo de los números naturales $m \in \mathbb{N}$ tales que :*

$$\exists a_1, \ldots, a_m \in \mathfrak{m} \ \text{ tales que } \ \ell_A\left(M/(a_1, \ldots, a_m)M\right) < +\infty$$

*Si $M = (0)$ diremos $dim_{Chevalley}(M) = -1$.*

Nótese que tal mínimo siempre existe : el cardinal mínimo de generadores de $\mathfrak{m}$ es una cota superior porque $M/\mathfrak{m}M$ es un $A/\mathfrak{m}-$espacio vectorial de dimensión finita.

TEOREMA 6.4.33 (de la Dimensión). *Si $(A, \mathfrak{m})$ es un anillo local noetheriano y $M$ es un $A-$módulo fintamente generado, se tiene :*

$$dim_{Krull}(M) = dim_{Hilbert-Samuel}(M) = dim_{Chevalley}(M) < +\infty$$

*Y a partir de ahora utiulizaremos solamente la palabra dimensión para designar una cualquiera de las cantidades citadas.*

Dividiremos la prueba en varias partes :

LEMA 6.4.34. *En las condiciones del Teorema*

i) $dim_{Hilbert-Samuel}(M) < +\infty$.
ii) $dim_{Chevalley}(M) < +\infty$.

DEMOSTRACIÓN. Obsérvese que el grado del polinomio de Samuel $P_{\mathfrak{m}}(M, -)$ está siempre acotado por el cardinal de un conjunto de generadores de $\mathfrak{m}$. En cuanto al segundo apartado lo hemos discutido previamente. □

LEMA 6.4.35. *En las anteriores condiciones :*

$$dim_{Krull}(M) \leq dim_{Hilbert-Samuel}(M)$$

DEMOSTRACIÓN. Primero probaremos la afirmación para anillo locales noetherianos y después para módulos.
En primer lugar, observemos que si $dim_{H-S}(A) = -1$, entonces $A/\mathfrak{m}^n = (0)$ para algún $n \in \mathbb{N}$. Aplicando el Lema de Nakayama $A = (0)$ luego $dim_{Krull}(A) = -1$.
Vamos a probar la siguiente afirmación por inducción en $r$ : Para cualquier cadena de ideales primos de $A$ :

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \cdots \mathfrak{p}_r,\ \mathfrak{p}_0 \text{ minimal} \Rightarrow \leq dim_{H-S}(A)$$

Puesto que $A/\mathfrak{p}_0 \neq (0)$, es claro que $dim_{H-S}(A)$ no puede ser $-1$, por lo discutido anteriormente, luego se verifica el caso $r = 0$.
Supongamos, como hipótesis inductiva que la afirmación es cierta para cualquier cadena de longitud menor que $r-1$. Supongamos $a \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Sea $\mathfrak{p}' \in Spec(A)$ un ideal primo minimal entre los ideales que contienen a $\mathfrak{p}_0 + (a)$ (su existencia está garantizada por la condición de noetherianidad de $A$). Consideremos el anillo $A' := A/\mathfrak{p}$ y la cadena de primos :

$$\mathfrak{p}' \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

tendremos $r-1 \leq dim_{Krull}(A')$. Como $\mathfrak{p}'$ es minimal sobre $\mathfrak{p}_0+(a)$ también es asociado, con lo que tenemos un monomorfismo de $A-$módulos :

$$0 \longrightarrow A/\mathfrak{p}' \hookleftarrow A/(\mathfrak{p}_0 + (a))$$

por lo tanto, $dim_{H-S}(A') \leq dim_{H-S}(A/(\mathfrak{p}_0 + (a))$.
Consideremos la sucesión exacta corta definida por la homotecia $a_{A/\mathfrak{p}_0}$ :

$$0 \longrightarrow A/\mathfrak{p}_0 \longrightarrow A/\mathfrak{p}_0 \longrightarrow A/(\mathfrak{p}_0 + (a))$$

Existirá una función polinomial $R : \mathbb{N} \longrightarrow \mathbb{N}$ de grado menor que el grado de la función de Samuel de $A/\mathfrak{p}_0$ y de coeficiente director positivo tal que :

$$P_{\mathfrak{m}}(A/\mathfrak{p}_0, n) + P_{\mathfrak{m}}(A/(\mathfrak{p}_0 + (a)), n) = P_{\mathfrak{m}}(A/\mathfrak{p}_0, n) + R(n)$$

Luego :

$$dim_{H-S}(A/\mathfrak{p}_0) = deg(P_{\mathfrak{m}}(A/\mathfrak{p}_0, n) \geq P_{\mathfrak{m}}(A/\mathfrak{p}_0 + (a)) + 1 \geq r$$

Finalmente, dado $\mathfrak{p}_0 \in Ass(A)$ minimal existe un monomorfismo $A/\mathfrak{p}_0 \mathfrak{m} on o A$, con lo cual

$$dim_{H-S}(A/\mathfrak{p}_0) \leq dim_{H-S}(A)$$

y hemos terminado con los anillos.
Por otro lado, si $M$ es un $A-$módulo finitamente generado,

$$dim_{Krull}(M) = dim_{Krull}(A/Ann(M))$$

Si $\mathfrak{p} \in Supp(M)$ es un primo asociado a $M$, tenemos :

$$0 \longrightarrow A/\mathfrak{p} \hookleftarrow M$$

con lo cual $dim_{H-S}(M) \geq dim_{H-S}(A/\mathfrak{p})$. Dado que $Ass(M)$ contiene a los pirmos minimales sobre $Ann(M)$ y aplicando el caso de anillo,s habremos terminado. □

Corollario 6.4.36. *Se tiene:*

i) *Todo anillo local noetheriano tiene dimensión de Krull finita.*
ii) *Todo ideal primo de un anillo noetheraino tiene altura finita.*
iii) *Mismo para módulos.*

Lema 6.4.37. *Sea $A$ un anillo noetheriano y $M$ un $A-$módulo finitamente generado. Entonces, para cada ideal $\mathfrak{a}$ de $A$ se tiene :*

$$Ann(M/\mathfrak{a}M) \subseteq \sqrt{\mathfrak{a} + Ann(M)}$$

Demostración. Este resultado se prueba fácilmente usando la propiedad :

$$M/\mathfrak{a}M = A/\mathfrak{a} \bigotimes_A M$$

y el comportamiento del soporte con respecto al producto tensorial. Una demostración alternativa es la siguiente :
Dado $\lambda \in Ann(M/\mathbb{I}M)$, y $\{m_1, \ldots, m_r\}$ un sistema generador de $M$ como $A-$módulo, para cada $m \in M$ se tiene :

$$\exists b_{1,i}, \ldots, b_{r,i} \in \mathfrak{a}, \quad \lambda m_i := \sum_{j=1}^{r} b_{j,i} m_j$$

Sea

$$B := \begin{pmatrix} b_{1,1} & \cdots & b_{1,r} \\ \vdots & & \vdots \\ b_{r,1} & & b_{r,r} \end{pmatrix}.$$

la matriz $r \times r$ con coeficientes en $A$ y consideremos

$$f := det(\lambda Id_r - B) = \lambda^r + h$$

donde $h \in \mathfrak{a}$, es un polinomio sin término independiente. Consideremos la aplicación lineal :

$$(\lambda Id_r - B) : A^r \longrightarrow A^r$$

y observemos que para cada $x_1, \ldots, x_r \in A$, si

$$(\lambda Id_r - B) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix}$$

se tiene :

$$z_1 m_1 + \cdots + z_r m_r = 0$$

La razón es la siguiente :

$$z_i := \lambda x_i - \sum_{j=1}^{r} b_{i,j} x_j$$

Luego,

$$\sum_{i=1}^{r} z_i m_i = x_1(\sum_{i=1}^{r} \lambda m_1 - \sum_{i=1}^{r} b_{i,1} m_i) + \cdots + x_r(\sum_{i=1}^{r} \lambda m_r - \sum_{i=1}^{r} b_{i,r} m_i) = 0$$

En particular, usando la transpuesta de la adjunta :

$$^t Adj(\lambda Id_r - B)(\lambda Id_r - B) = det(\lambda Id_r - B) Id_r$$

Luego,

$$det(\lambda Id_r - B) m_i = 0,\ 1 \leq i \leq r$$

y $det(\lambda Id_r - B) = \lambda^r + h \in Ann(M)$. □

LEMA 6.4.38. *En las hipótesis del Teorema de la Dimensión :*

$$dim_{Hilbert-Samuel}(M) \leq dim_{Chevalley}(M)$$

DEMOSTRACIÓN. Si la dimensión de Chevalley de $M$ es $-1$ es porque $M = (0)$ y su dimensión de Hilbert-Samuel también es $-1$. Podemos suponer $s = dim_{Chevalley}(M) \geq 0$ y consideremos : $a_1, \ldots, a_s \in A$ tales que :

$$\ell_A(M/(a_1, \ldots, a_s)M) < +\infty$$

Entonces, el $A-$módulo $M/(a_1, \ldots, a_s)M$ es artiniano y su soporte tiene que ser $\{\mathfrak{m}\}$. Pero $Ann(M/(a_1, \ldots, a_s)M) \subseteq \sqrt{(a_1, \ldots, a_s) + Ann(M)}$. En particular, este ideal $\mathfrak{a} := (a_1, \ldots, a_s) + Ann(M)$ es un ideal de definición de $A$. La razón es simple, el único ideal primo que puede contener a este ideal es $\mathfrak{m}$.
Ahora observemos que la estructura de $A-$módulo en $M$ y la estructura de $A/Ann(M)-$módulo coinciden. Denotesmo por $\overline{A} := A/Ann(M)$ y $\overline{\mathfrak{a}} := (a_1, \ldots, a_s) + Ann(M)/Ann(M)$. También concluiremos que $\overline{\mathfrak{a}}$ es un ideal de definición de $\overline{A}$.
Más aún, se tiene la siguiente igualdad entre longitudes :

$$\ell_{\overline{A}}(M/\overline{\mathfrak{a}}M) = \ell_A(M/\mathfrak{a}M)$$

Como $\overline{\mathfrak{a}}$ está generado por $s$ elementos, el grado del polinomio de Samuel $P_{\overline{\mathfrak{a}}}(M, -)$ está acotado por $s$. En particular, lo estará también $P_{\mathfrak{a}}(M, -)$ y por ende la dimensión de Chevalley de $M$. □

LEMA 6.4.39. *En las condiciones del Teorema de la Dimensión,*

$$dim_{Chevalley}(M) \leq dim_{Krull}(M)$$

DEMOSTRACIÓN. Lo haremos por inducción en la dimensión de Krull de $M$, que es finita por lo probado en 6.4.35.
Si la dimensión de Krull de $M$ es $-1$ es porque $M = (0)$ y su dimensión de Chevalley es también $-1$.

$$dim_{Krull}(M) = -1 \Leftrightarrow Ann(M) = A \Leftrightarrow M = (0)$$

Si la dimensión de Krull de $M$ es 0, $Supp(M) = Ass(M) = \{\mathfrak{m}\}$ y $M$ es artiniano, con lo que la dimensión de Chevalley es también 0 y hemos terminado.
Supongamos ahora que la dimensión de Krull es estrictamente positiva y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in Spec(A)$ los ideales primos asociados a $M$ tales que :

$$dim_{Krull}(M) = coht(\mathfrak{p}_i)$$

mientras que si $\mathfrak{p} \neq \mathfrak{p}_i$, $dim_{Krull}(M) > coht(\mathfrak{p}_i)$ (la finitud queda garantizada por la noetherianidad). Tenemos que $\mathfrak{p}_i \neq \mathfrak{m}$ luego existe $a \in \mathfrak{m}$ que no es divisor de cero de $M$, luego no están en la unión de los primos asociados a $M$ y

$$a \notin \bigcup_{i=1}^{s} \mathfrak{p}_i$$

Sea $M' := M/aM$. Tenemos que la dimensión de Krull de $M'$ es estrictamente menor que le dimensión de Krull de $M$, luego coincide con la dimensión de Chevalley de $M'$. Baste notar que la dimensión de Chevalley de $M$ está acotada por la dimensión de Chevalley de $M' + 1$ para concluir la prueba :
Así, si $\{a_1, \ldots, a_s\}$ son tales que $M''/(a_1, \ldots, a_s)M'$ es artiniano, es claro que $\{a_1, \ldots, a_s, a\}$ verifican que :

$$M/(a_1, \ldots, a_s, a)M \text{ es artiniano}$$

□

Queda así demostrado el Teorema de la Dimensión y podemos pasar a algunas aplicaciones inmediatas.

Corollario 6.4.40 (Teorema del Ideal Principal de Krull). *Sea $A$ un anillo noetheriano, $\mathfrak{a} := (a_1, \ldots, a_r) \subsetneq A$ un ideal generado por $r$ elementos. Entonces, cualquier ideal primo minimal conteniendo al ideal $\mathfrak{a}$ tiene altura menor o igual a $r$. Luego $ht(\mathfrak{a}) \leq r$.*
*En particular, si $\mathfrak{a} \subsetneq A$ es principal, $\mathfrak{a} = (a_1)$ y $a_1$ no es divisor de cero en $A$, todo ideal primo minimal conteniendo a $\mathfrak{a}$ tiene altura* 1*.*

Demostración. La primera observación obvia es la siguiente :

$$ht(\mathfrak{p}) := dim(A_{\mathfrak{p}})$$

para cualquier primo del anillo $A$. Sea, pues, $\mathfrak{p}$ un primo minimal sobre $\mathfrak{a}$, entonces, $\mathfrak{a}A_{\mathfrak{p}}$ es un ideal de definición del anillo local noetheriano $(A_{\mathfrak{p}}, \mathfrak{p}A_{\mathfrak{p}})$. Si $\mathfrak{a}$ está generado por $r$ elementos, es claro que $ht(\mathfrak{p}) \leq r$.
De otro lado, si $\mathfrak{a}$ es principal y $\mathfrak{p}$ es un ideal que contiene a $\mathfrak{a}$ y tiene altura 0, entonces, $\mathfrak{p}$ es un ideal minimal de $A$, con lo que es asociado y el generador de $\mathfrak{a}$ es un divisor de cero de $A$ por estar en $\mathfrak{p}$. □

Corollario 6.4.41. *Sea $A$ un dominion noetheriano. Entonces, $A$ es un dominio de factorización única si y solamente si todo ideal primo de altura* 1 *es principal.*

Comenzaremos con un pequeño Lema :

Lema 6.4.42. *Sea $A$ un dominio noetheriano. Entonces, si todo ideal de altura* 1 *es principal, los ideales primos asociados a un ideal principal son minimales.*

Demostración. Sea $\mathfrak{a} := (f)$ un ideal principal propio de $A$. Consideremos una descomposición primaria de $\mathfrak{a}$ :

$$\mathfrak{a} := \bigcup_{i=1}^{r} \mathfrak{q}_i$$

donde $\mathfrak{q}_i$ es $\mathfrak{p}_i-$primario. Supongamos que $\mathfrak{p}_i := (f_i)$, con $1 \leq i \leq s \leq r$. Sea $\alpha_i$ la máxima potencia de $f_i$ que divide a $f$. Consideremos la cadena :

$$F_1 := \frac{f}{f_1^{\alpha_1}} \notin \mathfrak{p}_1$$

$$F_i := \frac{F_{i-1}}{f_i^{\alpha_i}} \notin \bigcup_{k=1}^{i} \mathfrak{p}_k$$

Esta cadena tiene sentido porque estamos en un dominio : $f = F_1 f_1^{\alpha_1}$, como $f \in \mathfrak{p}_i$ y $f_1^{\alpha_1} \notin \mathfrak{p}_i$, entonces $F_1 \in \mathfrak{p}_i$, $1 \leq i \leq s$. Consideremos entonces, $F_s$. Es claro que $F_s \mid f$, mientras $F_s \in \mathfrak{p}_{s+1} \cap \cdots \mathfrak{p}_r$. Aplicando el Teorema del Ideal Principal de Krull, todo ideal primo minimal sobre $F_s$ es de altura 1, luego es principal. Sea $\mathfrak{p} = (g)$ uno de esos minimales sobre $F_s$. Entonces, $g \mid F_s \mid f$, pero $g \notin \mathfrak{p}_i$, $1 \leq i \leq s$ (si perteneciera a alguno de tales $\mathfrak{p}_i$, también $F_s$ pertenecería, llegando a contradicción). Luego $\mathfrak{p}$ es un

ideal primo de altura 1 que contiene a $\mathfrak{a}$ y no es $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ (ni los contiene). Se trata pues, de un ideal minimal sobre $\mathfrak{a}$ y ha de estar asociado. Por lo tanto, es igual a algún $\mathfrak{p}_j$, con $s+1 \leq j \leq r$, contradiciendo la hipótesis de que estos ideales tienen altura mayor estricto que 1. □

*Demostración del Corolario :* si $A$ es un D.F.U. ya hemos visto que todos los primos minimales sobre un ideal principal han de ser principales, como el Teorema de Krull nos dice que son de altura 1, hemos acabado. Recíprocamente, si todo ideal de altura 1 es principal, todo asociado es minimal (Lema de arriba) y todo asociado a un ideal principal es principal, con lo que tenemos el enunciado. □

Definición 48. *Llamaremos sucesión regular en un anillo $A$ a toda cadena de elementos de $A$, $f_1, \ldots, f_r \in A$, tal que :*

- *$f_i$ no es divisor de cero en $A/(f_1, \ldots, f_{i-1})$.*
- *$(f_1, \ldots, f_r) \subsetneq A$.*

Corollario 6.4.43. *Si $A$ es noetheriano y $f_1, \ldots, f_r$ es una sucesión regular de $A$, $ht(f_1, \ldots, f_r) = r$ y todo ideal primo minimal sobre $\mathfrak{a} = (f_1, \ldots, f_r)$ tiene altura $r$.*

Demostración. Baste aplicar el Teorema de Krull por inducción en $r$. Es claro que $ht(\mathfrak{a}) \leq r$ y que $ht((f_1) = 1$ en $A$ y todo ideal primo minimal sobre $(f_1)$ tiene altura 1.
Para el caso $r$, sea $\mathfrak{p}$ un ideal primo minimal sobre $(f_1, \ldots, f_r)$. Sabemos que $ht(\mathfrak{p}) \leq r$ y $\mathfrak{p}$ no es minimal sobre $(f_1, \ldots, f_{r-1})$ porque $f_r \in \mathfrak{p}$ y $f_r$ no es divisor de cero módulo $(f_1, \ldots, f_{r-1})$. Entonces, existe un primo minimal $\mathfrak{p}'$ sobre $(f_1, \ldots, f_{r-1})$ tal que :

$$(f_1, \ldots, f_{r-1}) \subseteq \mathfrak{p}' \subsetneq \mathfrak{p}$$

Luego $ht(\mathfrak{p}) > ht(\mathfrak{p}') = r - 1$. □

Definición 49. *Sea $(A, \mathfrak{m})$ un anillo local noetheriano de dimensión $d$. Llamaremos sistema de parámetros de $A$ a toda colección, $a_1, \ldots, a_d$ de elementos de $A$ generando un ideal de definición de $A$.*

Proposición 6.4.44. *Si $(A, \mathfrak{m})$ es un anillo local noetheriano y $\{a_1, \ldots, a_d\}$ es un sistema de parámetros de $A$, se tiene :*

$$dim A/(a_1, \ldots, a_i) = d - i$$

Demostración. Consideremos $A' := A/\mathfrak{a}_i$, $\mathfrak{a}_i := (a_1, \ldots, a_i)$. Claramente $dim A' \leq d-i$ pues $\{a_{i+1}+\mathfrak{a}_i, \ldots, a_d+\mathfrak{a}_i\}$ generan un ideal de definición de $A'$. Recíprocamente, si $b_1, \ldots, b_p \in A$ son tales que sus clases $b_j + \mathfrak{a}_i$ generan un ideal de definición de $A/\mathfrak{a}_i$, entonces, $\{a_1, \ldots, a_i, b_1, \ldots, b_p\}$ generan un ideal de definición de $A$ y $dim(A) \leq i+p$. □

## 6.5. Dimensión en $K-$álgebras: Normalización de Noether y álgebras Cohen-Macaulay

**6.5.1. El Lema de Normalización de Noether.** Según algunas fuentes, el Lema de Normalización de E. Noether[3] también puede ser debido a D. Hilbert quien ya había demostrado un resultado análogo en el contexto de álgebras de invariantes en su trabajo de 1893[4]. La formulación actual, sin embargo, es enteramente debida a Noether. Aquí seguiremos la demostración de [**Ku, 85**], p. 51 y siguientes.

[3] E. Noether, "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl und Funktionenkrpern". *Math. Ann.* , **96** (1927) pp. 26-61.

[4] D. Hilbert. "Über die vollen Invariantensysteme". *Math. Annalen* **42** (1893) 313–373.

TEOREMA 6.5.1 (**Lema de Normalización de E. Noether**). *Sea $A$ una $K-$álgebra finitamente generada sobre un cuerpo y sea $\mathfrak{a} \subseteq A$ un ideal propio. Entonces, existen elementos $Y_1, \ldots, Y_d \in A$ y existe $s \leq d$ tales que :*

i) $\{Y_1, \ldots, Y_d\}$ *son algebraicamente independientes sobre* $K$.
ii) $A$ *es un* $K[Y_1, \ldots, Y_d]-$*módulo finitamente generado.*
iii) $\mathfrak{a} \bigcap K[Y_1, \ldots, Y_d] = (Y_{s+1}, \ldots, Y_d)$.

*Más aún, si $K$ es un cuerpo consuficientes elementos y $A := K[x_1, \ldots, x_n]$ es una $K$álgebra finitamente generada, podemos suponer que los elementos $Y_i$ son combinaciones lineales de los elementos $\{x_1, \ldots, x_n\}$.*

Haremos la demostración en diversas etapas, marcadas por Lemas.
El enunciado y la prueba lo he tomado, con matices, de [**?**].

LEMA 6.5.2. *Sean $p_1, \ldots, p_m \in K[T]$, $caract(K) = 0$ polinomios univariados cualesquiera que supondremos de grado a lo más $d$. Entonces, existe $k \in \{0, 1, \ldots, \binom{m}{2}d\}$ tal que*

$$p_i(k) \neq p_j(k), \ \ \forall i \neq j$$

DEMOSTRACIÓN. Definamos el polinomio univariado no nulo :

$$\prod_{i<j}(p_i - p_j) \in K[T]$$

Este polinomio tiene grado a lo más $\binom{m}{2}d$ y claramente no puede anularse en el conjunto citado. En caso contrario, aplicando un argumento obvio sobre interpolación, este polinomio sería un polinomio idénticamente nulo. □

Obsérvese que si la característica del cuerpo es distinta de cero, bastará con tomar un conjunto cualquiera con el mismo cardinal.

LEMA 6.5.3. *Sea $F \in K[X_1, \ldots, X_n]$ un polinomio no nulo de grado a lo más $d$ y sean $\{\alpha_0, \ldots, \alpha_d\} \subseteq K$ elementos distintos del cuerpo $K$. Entonces, existe $\underline{\alpha} \in \{\alpha_0, \ldots, \alpha_d\}^n$ tal que :*

$$F(\underline{\alpha}) \neq 0$$

LEMA 6.5.4. *Un polinomio homogéneo no nulo de $K[X_1, \ldots, X_n]$ no puede anularse en ningún abierto afín de $K^n$.*

LEMA 6.5.5. *Sea $F$ un polinomio no constante en $K[X_1, \ldots, X_n]$ un polinomio no constante.*

- *a) : Mediante una sustitución de la forma :*

$$X_i := Y_i + X_n^{r_i}, \quad (1 \leq i \leq n-1)$$

*para adecuados $r_i \in \mathbb{N}$, el polinomio $F$ se transforma en un polinomio de la forma :*

$$aX_n^m + \rho_1 X_n^{m-1} + \cdots + \rho_m$$

*donde $a \in K \setminus \{0\}$, $\rho_i \in K[Y_1, \ldots, Y_{n-1}]$, $1 \leq i \leq m$. los $r_i$ verifican la cota*

$$r_i \leq (\frac{N}{2}(n-1))^i$$

*donde $N$ es el número de monomios de coeficiente no nulo de $F$.*

- *b) : Si $K$ es un cuerpo infinito, entonces el mismo resultado puede ser obtenido por medio de una sustitución del tipo :*

$$X_i := Y_i + a_i X_n$$

*para adecuados $a_i \in K$.*

DEMOSTRACIÓN.

- $a$) : Supongamos :

$$F := \sum_{\nu \in \mathbb{N}^n} a_\nu X_1^{\nu_1} \cdots X_n^{\nu_n}$$

Para cada $\nu \in \mathbb{N}^n$ tal que $a_\nu \neq 0$, definamos

$$p_\nu(T) := \nu_n + \nu_1 T + \nu_2 T^2 + \cdots + \nu_{n-1} T^{n-1} \in \mathbb{Z}[T]$$

Se trata de polinomios distintos cuando es distinto el índice $\nu$ a que hacen referencia. En este sentido existirá un cierto $k$ de valor absoluto a lo más $\binom{N}{2}(n-1)$ tal que :

$$p_\nu(k) \neq p_{\nu'}(k), \quad \forall \nu \neq \nu'$$

Ahora definamos $r_i := k^i$ y las variables :

$$Y_i := X_i - X_n^{r_i}, \quad 1 \leq i \leq n-1$$

Tendremos la siguiente transformación para $F$ :

$$F(X_1, \ldots, X_n) := \sum_{\nu \in \mathbb{N}^n} a_\nu (Y_1 + X_n^{r_1})^{\nu_1} \cdots (Y_{n-1} + X_n^{r_{n-1}})^{\nu_{n-1}} X_n^{\nu_n}$$

De esta manera el polinomio $F$ toma la forma :

$$F(Y_1, \ldots, Y_{n-1}, X_n) := a_\mu X_i^{p_\mu(k)} + G_\mu(Y_1, \ldots, Y_{n-1}, X_n)$$

donde $p_\mu(k)$ es el máximo de los $p_\nu(k)$, con lo cual el gradoi en $X_n$ de $G_\mu$ es estrictamente menor que $p_\nu(k)$ y $F$ tiene la forma apetecida.

- $b$) : Supongamos de nuevo :

$$F := \sum_{\nu \in \mathbb{N}^n} a_\nu X_1^{\nu_1} \cdots X_n^{\nu_n}$$

y escribamos :

$$Y_i := X_i - a_i X_n, \quad 1 \leq i \leq n-1$$

Escribamos $F := F_0 + \cdots + F_d$ la descomposición de $F$ en componentes homogéneas en $K[X_1, \ldots, X_n]$, donde $d$ es el grado total de $F$ y $F_d \neq 0$. Con el cambio buscado, tomemos :

$$F := \sum -\nu \in \mathbb{N}^n a_\nu (Y_1 + a_1 X_n)^{\nu_1} \cdots (Y_{n-1} + a_{n-1} X_n)^{\nu_{n-1}} X_n^{\nu_n}$$

Entonces,

$$F := F_d(a_1, \ldots, a_{n-1}, 1) X_n^d + G_{d-1}(Y_1, \ldots, Y_{n-1}, X_n)$$

donde $G_{d-1}$ es un polinomio de grado a lo más $d-1$ en $X_n$. Como $F_d$ es un polinomio homogéneo no se anula en el abierto Zariski de $K^n$ dado por : $\{X_n \neq 0\}$. Luego $F_d(T_1, \ldots, T_{n-1}, 1)$ es un polinomio no nulo y podremos encontrar un punto $(a_1, \ldots, a_{n-1}) \in K^{n-1}$ verificando la inecuación $F_d(a_1, \ldots, a_{n-1}, 1) \neq 0$. Ese punto verificará las propiedades prescritas.

□

*Demostración del Lema de Normalización de Noether.–*

- Caso 1 : *Supongamos que $A := K[X_1, \ldots, X_n]$ es un anillo de polinomios con coeficientes en un cuerpo $K$ y el ideal $\mathfrak{a} = (F)$ es un ideal principal.*
- Bastará con que apliquemos el Lema previo. Hagamos el cambio de coordenadas

$$(X_1, \ldots, X_n) \longrightarrow (Y_1, \ldots, Y_{n-1}, X_n)$$

correspondiente bien al caso $a$) o al caso $b$) del Lema. Describamos el caso $b$) por su belleza. Entonces, el polinomio :

$$G(Y_1, \ldots, Y_{n-1}, X_n) := F(Y_1 + a_1 X_n, \ldots, Y_{n-1} + a_{n-1} X_{n-1}, X_n)$$

que es un polinomio mónico en $X_n$. Definamos $Y_n := F$ y tendremos :

$$K[Y_1, \ldots, Y_n] \hookrightarrow K[X_1, \ldots, X_n]$$

es una extensión entera de anillos. Es claro que $X_n$ verifica una ecuación de dependencia entera sobre el anillo $K[Y_1, \ldots, Y_n]$ :

$$G(Y_1, \ldots, Y_{n-1}, X_n) - Y_n = 0$$

Por lo demás tenemos la cadena de extensiones :

$$K[Y_1, \ldots, Y_n] \hookrightarrow K[Y_1, \ldots, Y_{n-1}, X_n] \hookrightarrow K[X_1, \ldots, X_n]$$

Siendo todas ellas enteras, el tercer anillo es entero sobre el primero y, por ende, finitamente generado como módulo. Ahora, al ser $\{X_1, \ldots, X_n\}$ algebraicamente independientes sobre $K$, tambien lo son $\{Y_1, \ldots, Y_n\}$, por estar ante una extensión entera (luego algebraica). De otro lado, $\mathfrak{a} \cap K[Y_1, \ldots, Y_n] \supseteq (Y_n)$. Pero si $H(Y_1, \ldots, Y_n) \in \mathfrak{a} \cap K[Y_1, \ldots, Y_n)$, tendremos :

$$H = H'F$$

en $K[X_1, \ldots, X_n]$. Como $H'$ es entero sobre $K[Y_1, \ldots, Y_n]$ verificará una ecuación de dependencia entera :

$$(H')^d + a_{d-1}(H')^{d-1} + \cdots + a_0 = 0$$

Como los $a_i \in K[Y_1, \ldots, Y_n]$ podemos multiplicar esa ecuación por $F^d$ y obtendremos :

$$H^d + a_{d-1}Y_nH^{d-1} + \cdots + a_0Y_n^d = 0$$

de donde se deduce que $Y_n \mid H$ en $K[Y_1, \ldots, Y_n]$.

- Caso 2 : *Supongamos que $A := K[X_1, \ldots, X_n]$ es un anillo de polinomios y el ideal $\mathfrak{a}$ es un ideal cualquiera de $A$.*
- Hagamos inducción en el número de variables $n$. Para $n = 1$, o bien $\mathfrak{a} = (0)$ o bien $\mathfrak{a}$ es un ideal principal y basta con retrotraerse al caso anterior para no tener nada más que hacer. Supongamos $n \geq 1$ y consideremos el caso que que $\mathfrak{a}$ no es un ideal principal. Si $\mathfrak{a}$ es principal o nulo no hay nada que hacer. Supongamos $\mathfrak{a} \neq (0)$ y sea $F \in \mathfrak{a}$, $F \neq 0$, Sea $\mathfrak{b} = (F) \subseteq \mathfrak{a}$ y apliquemos el caso $n = 1$ : Existirán $\{Y_1, \ldots, Y_n\}$ tales que :

$$K[Y_1, \ldots, Y_n] \hookrightarrow K[X_1, \ldots, X_n]$$

es una extensión entera de anillos. Además $\mathfrak{b} \cap K[Y_1, \ldots, Y_n] = (Y_n)$. Sea $\mathfrak{a}^c$ la contracción de $\mathfrak{a}$ a $K[Y_1, \ldots, Y_n]$ y sea $\overline{\mathfrak{a}} := \mathfrak{a}^c/(Y_n)$ que es un ideal de $K[Y_1, \ldots, Y_n]/(Y_n) = K[Y_1, \ldots, Y_{n-1}]$. Estamos en condiciones de aplicar la hipótesis inductiva y existirán : $\{Y_1', \ldots, Y_{n-1}'\}$ tales que :

$$K[Y_1', \ldots, Y_{n-1}'] \hookrightarrow K[Y_1, \ldots, Y_{n-1}]$$

es una extensión entera de anillos, siendo :

$$\overline{\mathfrak{a}} \cap K[Y_1', \ldots, Y_{n-1}'] = (Y_{s+1}', \ldots, Y_{n-1}')$$

Tomando $\{Y_1', \ldots, Y_{n-1}', Y_n\}$ tenemos la colección buscada y es fácil probar que se verifican las propiedades requeridas.

- Caso 3 : *Caso general.*
- Baste notar que si $A$ es una $K-$álgebra finitamente generada tiene la forma :

$$A = K[X_1, \ldots, X_n]/\mathfrak{b}$$

donde $\mathfrak{b}$ es un ideal de $K[X_1, \ldots, X_n]$ mientras $\mathfrak{a}$ tiene la forma $\tilde{\mathfrak{a}}/\mathfrak{b}$, siendo $\tilde{\mathfrak{a}}$ un ideal de $K[X_1, \ldots, X_n]$ que contiene a $\mathfrak{b}$. Aplicando el caso 2 a $\mathfrak{b}$ existirán $\{Y_1, \ldots, Y_n\}$ tales que :

$$K[Y_1, \ldots, Y_n] \hookrightarrow K[X_1, \ldots, X_n]$$

es una extensión entera de anillos, mientras

$$\mathfrak{b} \cap K[Y_1, \ldots, Y_n] = (Y_{r+1}, \ldots, Y_n)$$

Como las extensiones enteras se portan bien al tomar cocientes, la siguiente es una extensión enetra de anillos :

$$K[Y_1, \ldots, Y_r] = K[Y_1, \ldots, Y_n]/\mathfrak{b} \hookrightarrow A$$

Consideremos el ideal contracción $\mathfrak{a}^c$ dado mediante :

$$\mathfrak{a}^c := \tilde{\mathfrak{a}} \cap K[Y_1, \ldots, Y_r] := \mathfrak{a} \cap (K[Y_1, \ldots, Y_n]/\mathfrak{b})$$

Apliquemos de nuevo el caso 2 a $\mathfrak{a}^c$ y obtengamos : $\{Y_1', \ldots, Y_r'\}$ tales que :

$$K[Y_1', \ldots, Y_r'] \hookrightarrow K[Y_1, \ldots, Y_r] \hookrightarrow A$$

son extensiones enteras de anillos y, además :

$$\mathfrak{a} \cap K[Y_1', \ldots, Y_r'] = \mathfrak{a}^c \cap K[Y_1', \ldots, Y_r'] = (Y_{s+1}', \ldots, Y_r')$$

□

Este sencillo Lema tiene muchas consecuencias relevantes, algunas de las cuales pasaremos a analizar :

COROLLARIO 6.5.6. *Sea $K$ un cuerpo infinito, $\mathfrak{a}$ ideal homogéneo de $K[X_0, \ldots, X_n]$ entonces, existen $\{Y_0, \ldots, Y_n\}$ polinomios homogéneos, tales que :*

i) *$K[Y_0, \ldots, Y_n] \hookrightarrow K[X_0, \ldots, X_n]$ es una extensión entera de anillos.*
ii) *$\mathfrak{a} \cap K[Y_0, \ldots, Y_n] = (Y_{r+1}, \ldots, Y_n)$.*
iii) *La extensión de anillos :*

$$K[Y_0, \ldots, Y_r] \hookrightarrow K[X_0, \ldots, X_n]/\mathfrak{a}$$

*es entera y es un morfismo de anillos graduados de grado 0.*

DEMOSTRACIÓN. Se trata de la misma demostración, usando cambios lineales de coordenadas y siguiendo la misma estrategia del Lema de Normalización de Noether, pero tomando homogéneos a cada etapa. □

Hagamos ahora un recordatorio de algunos resultados concernientes a extensiones enteras de anillos :

LEMA 6.5.7. *Si $A \hookrightarrow B$ es una extensión entera de anillosse tiene :*

i) *Si $B$ es un cuerpo, $A$ es un cuerpo.*
ii) *Los ideales maximales de $B$ se contraen sobre ideales maximales de $A$.*
iii) *No hay relación de inclusión estricta entre los ideales primos de $B$ que se contraen sobre el mismo ideal primo de $A$.*
iv) *$f^* : Spec(B) \longrightarrow Spec(A)$ es suprayectiva.*

COROLLARIO 6.5.8. *Sea $A \hookrightarrow B$ un extensión entera de anillos. Entonces,*

i)

$$dim_{Krull}(A) = dim_{Krull}(B)$$

.

ii) *Para cualquier ideal primo $P$ de $B$, $coht(P) = coht(P \cap A)$.*

DEMOSTRACIÓN. Sea

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

una cadena de ideales primos de $B$. Sean $\mathfrak{p}_i := P_i \cap A$ y tenemos una cadena de ideales primos de $A$ dada por :

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

La razón profunda de la permanencia de loes contenidos estrictos es la propiedad *iii)* del Lema previo. Con lo cual $dim_{Krull}(A) \geq dim_{Krull}(B)$.

Para el otro contenido, utilizaremos la Propiedad del Ascenso que verifica toda extensión entera de anillos. Así, consideremos una cadena de ideales primos de $A$ :

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

y sea $P_0$ un ideal primo de $B$ que se contrae sobre $\mathfrak{p}_0$. Por el Teorema del Ascenso, tendremos una cadena de ideales primos de $B$ :

$$P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n$$

donde $P_i \cap A = \mathfrak{p}_i$. Los contenidos estrictos abajo significan contenidos estrictos arriba (obvio) y esta cadena tiene longitud $n$, con lo que queda terminada la prueba. □

Corollario 6.5.9. *Sea $A \hookrightarrow B$ una extensión entera de anillos y supongamos que $A$ es un anillo normal. Entonces, para cada ideal primo $P$ de $B$ se tiene : $ht(P) = ht(P \cap P)$.*

Demostración. De hecho, esta propiedad se verifica cuando se verifica la propiedad del Descenso. Así, tomemos una cadena de ideales primos de $B$ contenidos en $P$ :

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$$

Por no haber inclusión estricta entre los ideales primos de $B$ que se contraen sobre el mismo ideal primo de $A$, si $\mathfrak{p}_i := P_i \cap A$, tenemos una cadena de contenidos estrictos :

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = P \cap A$$

De otro lado, sea $\mathfrak{p} := P \cap A$ y consideremos una cadena de ideales primos de $A$ contenidos en $\mathfrak{p}$ :

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

Como $P$ se contraen sobre $\mathfrak{p}$, aplicando el Teorema del Descenso, tendremos

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$$

tales que $P_i \cap A = \mathfrak{p}_i$ y habremos terminado la prueba. □

Observación 6.5.10. La anterior propiedad se verifica también para cualquier ideal $\mathfrak{a}$ de $B$. Para verlo, sea $\mathfrak{b} := \mathfrak{a} \cap A$. Para cada ideal primo $P$ que contiene a $\mathfrak{a}$ se tiene $P \cap A$ contiene a $\mathfrak{b}$ y $ht(P) = ht(P \cap A)$. Con ello se prueba :

$$ht(\mathfrak{a}) := min\{ht(P) \ : \ P \supseteq \mathfrak{a}\} \geq min\{ht(\mathfrak{p}) \ : \ \mathfrak{p} \supseteq \mathfrak{b}\}$$

De otro lado, dado $\mathfrak{p} \supseteq \mathfrak{b}$ un ideal primo, por ser la extensión de anillos :

$$A/\mathfrak{b} \hookrightarrow A/\mathfrak{a}$$

entera, existirá un ideal primo $P \supseteq \mathfrak{a}$ de $B$ tal que $P \cap A = \mathfrak{p}$, luego

$$ht(\mathfrak{b}) \geq ht(\mathfrak{a})$$

y habremos terminado.

Proposición 6.5.11. *Sea $K$ un cuerpo,*

$$dim_{Krull}(K[X_1, \ldots, X_n]) = n$$

*Además, $ht(X_1, \ldots, X_i) = i$, $1 \leq i \leq n$.*

Demostración. Es claro que tenemos la siguiente cadena de ideales primos de $K[X_1, \ldots, X_n]$ :

$$(0) \subsetneq (X_1) \subsetneq \cdots \subsetneq (X_1, \ldots, X_n)$$

con ello tenemos ya probado,

$$dim_{Krull}(K[X_1, \ldots, X_n]) \geq n$$

Además, por ser los ideales $(X_1, \ldots, X_i)$ primos y la sucesión $X_1, \ldots, X_i$ regular, tenemos las propiedades de la altura.
Para la otra desigualdad, haremos inducción en $n$. En el caso $n = 1$ todo ideal de $K[X]$ es principal, luego todo primo distinto de (0) tiene altura 1 y habremos terminado. Para dimensión superior, supongamos una cadena de ideales primos :

$$(0) = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n+1}$$

Apliquemos el Lema de Normalización de Noether y tendremos $\{T_1, \ldots, T_n\}$ algebraicamente independientes sobre $K$ tales que :

$$K[T_1, \ldots, T_n] \hookrightarrow K[X_1, \ldots, X_n]$$

es una extensión entera de anillos y $\mathfrak{p}_1 \cap K[T_1, \ldots, T_n] = (T_{r+1}, \ldots, T_n)$ Podremos construir la siguiente cadena de ideales primos de $K[T_1, \ldots, T_r]$, $r \leq n-1$ :

$$(0) \subsetneq P_2 \subsetneq \cdots \subsetneq P_{n+1}$$

donde $P_i$ es la contracción a $K[T_1, \ldots, T_{n-1}]$ de $\mathfrak{p}_i/\mathfrak{p}_1$. Los contenidos estrictos se siguen por ser la siguiente una extensión entera de anillos :

$$K[T_1, \ldots, T_{n-1}] = K[T_1, \ldots, T_{n-1}, T_n]/\mathfrak{p}_1^c \hookrightarrow K[X_1, \ldots, X_n]$$

Aplicando la hipótesis inductiva habremos llegado a contradicción. □

Corollario 6.5.12. *Sea $K$ un cuerpo,*

i) *Si $\mathfrak{p}$ es un ideal primo de $K[X_1, \ldots, X_n]$,*

$$coht(\mathfrak{p}) := dim_{Krull}(K[X_1, \ldots, X_n]/\mathfrak{p}) = grtr_K(q.f.(K[X_1, \ldots, X_n]/\mathfrak{p}))$$

ii) *Si $V \subseteq K^n$ es un conjunto algebraico irreducible :*

$$coht(I(V)) = dim_{Krull}(K[V]) = grtr_K(K(V))$$

Demostración. Usando el Lema de Normalización de Noether, es claro que si $\{T_1, \ldots, T_r\}$ son tales que :

$$K[T_1, \ldots, T_r] \hookrightarrow K[X_1, \ldots, X_n]$$

son algebraicamente independientes sobre $K$, entonces, $r = n$. Además si $\mathfrak{p} \cap K[T_1, \ldots, T_n] = (T_{s+1}, \ldots, T_n)$, tenemos la siguiente cadena de extensiones enteras de anillos :

$$K[T_1, \ldots, T_s] = K[T_1, \ldots, T_n]/\mathfrak{p} \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{p}$$

Se trata de extensiones algebraicas entre los respectivos cuerpos de fracciones, luego el grado de trascendencia del último es $s$; pero $s$ es también la dimensión de Krull de los dos primeros. Por ser la extensión entera, también $s$ es la dimensión de Krull del último y habremos terminado. □

Corollario 6.5.13. *Sea $\mathfrak{p}$ un ideal primo de $K[X_1, \ldots, X_n]$, entonces*

$$ht(\mathfrak{p}) + coht(\mathfrak{p}) = n$$

*En particular, todos los ideales maximales de $K[X_1, \ldots, X_n]$ tienen altura $n$. En cambio, el único ideal primo de coaltura $n$ de $K[X_1, \ldots, X_n]$ es el ideal* (0).

Demostración. Apliquemos el Lema de Normalización de Noether y sean $\{T_1, \ldots, T_n\}$ algebraicamente independientes sobre $K$ tales que :

$$K[T_1, \ldots, T_n] \hookrightarrow K[X_1, \ldots, X_n]$$

es entera. Tenemos que $\mathfrak{p} \cap K[T_1, \ldots, T_n] = (T_{s+1}, \ldots, T_n)$. Claramente, $s = coht(\mathfrak{p})$. Además, podemos aplicar el Teorema del Descenso para concluir que :

$$ht(\mathfrak{p}) = ht(\mathfrak{p} \cap K[T_1, \ldots, T_n]) = n - s$$

El caso de los maximales queda descrito por ser los maximales los primos de coaltura 0. El otro caso es igual por ser (0) de altura 0. □

COROLLARIO 6.5.14. *Si $V \subseteq \mathbb{K}^n$ es un conjunto algebraico, exiten $d \in \mathbb{N}$ y existe una aplicación lineal $\varphi : \mathbb{K}^n \longrightarrow \mathbb{K}^d$ tal que:*

- *$\varphi\,|_V : V \longrightarrow \mathbb{K}^d$ es suprayectiva,*
- *Para cada $y \in \mathbb{K}^d$, la fibra $\varphi^{-1}(y)$ es finita.*

COROLLARIO 6.5.15. *Para cualquier ideal $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$ se tiene :*

$$ht(\mathfrak{a}) + coht(\mathfrak{a}) = n$$

DEMOSTRACIÓN. Para demostrarlo, se $\mathfrak{p}$ un ideal primo minimal sobre $\mathfrak{a}$ tal que $coht(\mathfrak{p}) = coht(\mathfrak{a})$. Hallemos una normalización de Noether :

$$K[T_1, \ldots, T_n] \hookrightarrow K[X_1, \ldots, X_n]$$

tal que $\mathfrak{a} \cap K[T_1, \ldots, T_n] = (T_{s+1}, \ldots, T_n)$. Entonces, $s = coht(\mathfrak{a}) = coht(\mathfrak{p})$. Por el Corolario anterior, $n - s = ht(\mathfrak{p}) \leq ht(\mathfrak{a})$. Luego $ht(\mathfrak{a}) + coht(\mathfrak{a}) \geq n$. Como la otra desigualdad se da siempre, tenemos el resultado. □

COROLLARIO 6.5.16. *Toda $K-$ágebra finitamente generada tiene dimensión finita, todo ideal primo suyo tiene altura y coaltura finitas y acotadas pr la dimensión de $A$.*

OBSERVACIÓN 6.5.17. La propiedad enunciada en el anterior Corolario no es extensible a cualesquiera anillos noetherianos, aunque sí es extensible a los anillos locales noetherianos.

Una propiedad importante es la de respetar los cocientes mediante las alturas.

DEFINICIÓN 50. *Un anillo $A$ se denomina catenario si para cualesquiera dos ideales primos $\mathfrak{p} \subseteq \mathfrak{p}'$ de $A$, se verifica :*

$$ht(\mathfrak{p}'/\mathfrak{p}) = ht(\mathfrak{p}') - ht(\mathfrak{p})$$

COROLLARIO 6.5.18. *Los anillos de polinomios $K[X_1, \ldots, X_n]$ son catenarios. Más aún, para cualesquiera dos ideales primos $\mathfrak{p} \subseteq \mathfrak{p}'$ se tiene :*

$$ht(\mathfrak{p}'/\mathfrak{p}) = ht(\mathfrak{p}') - ht(\mathfrak{p}) = coht(\mathfrak{p}) - coht(\mathfrak{p}')$$

DEMOSTRACIÓN. Basta con hacerlo para anillos de polinomios. Hallemos una normalización de Noether de $K[X_1, \ldots, X_n]$ con respecto al ideal $\mathfrak{p}$, es decir $\{T_1, \ldots, T_n\}$ tales que :

$$K[T_1, \ldots, T_n] \hookrightarrow K[X_1, \ldots, X_n]$$

donde $\mathfrak{p} \cap K[T_1, \ldots, T_n] = (T_{s+1}, \ldots, T_n)$. Se tiene que $s = coht(\mathfrak{p})$ y $n - s = ht(\mathfrak{p})$. Sea $\overline{\mathfrak{p}'}$ el ideal primo $\mathfrak{p}'/\mathfrak{p}$ y sea $\overline{\mathfrak{p}'}^c$ su contración a $K[T_1, \ldots, T_s]$. Claramente,

$$coht(\overline{\mathfrak{p}'}^c) + ht(\overline{\mathfrak{p}'}^c) = s$$

Pero

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

Por lo tanto,

$$ht(\mathfrak{p}'/\mathfrak{p}) = ht(\overline{\mathfrak{p}'}^c) = s - coht(\mathfrak{p}') = coht(\mathfrak{p}) - coht(\mathfrak{p}') = (n - ht(\mathfrak{p})) - (n - ht(\mathfrak{p}')) = ht(\mathfrak{p}') - ht(\mathfrak{p})$$

□

COROLLARIO 6.5.19. *Sean $f_1, \ldots, f_r$ una sucesión regular de $K[X_1, \ldots, X_n]$. Entonces, si $K$ es algebraicamente cerrado se tiene :*

$$dim_{Krull}(V(f_1, \ldots, f_r)) = n - r$$

DEMOSTRACIÓN. Baste notar que $ht(f_1, \ldots, f_r) = r$ y la identificación entre los ideales radicales de $K[X_1, \ldots, X_n]$ y los conjuntos algebraicos. □

Para los conjuntos algebraicos proyectivos tenemos una situación relativamente distinta :

LEMA 6.5.20. *Sea $A = K[X_0, \ldots, X_n]$ anillo graduado con la graduación usual. Sea $\mathfrak{m} := (X_0, \ldots, X_n)$ ideal maximal en $A$, y sea $\mathfrak{m}' := \mathfrak{m}A_{\mathfrak{m}}$ el único ideal maximal de $A_{\mathfrak{m}}$. Entonces,*

$$G_{\mathfrak{m}'}(A_{\mathfrak{m}}) = K[X_0, \ldots, X_n]$$

DEMOSTRACIÓN. Obsérvese que

$$\mathfrak{m}^m/\mathfrak{m}^{m+1} := H_m(X_0, \ldots, X_n)$$

Por la definición de la operación en el graduado, bastará con que probemos que los siguientes son espacio vectoriales isomorfos sobre $K = A/\mathfrak{m}$ :

$$\mathfrak{m}'^m/\mathfrak{m}'^{m+1} \cong H_m(X_0, \ldots, X_n)$$

Es claro que tenemos un monomorfismo :

$$\varphi : H_m(X_0, \ldots, X_n) \hookrightarrow \mathfrak{m}'^m/\mathfrak{m}'^{m+1}$$

dado por $\varphi(F) := F/1 + \mathfrak{m}'^{m+1}$. Supongamos, ahora $p/q + \mathfrak{m}'^{n+1} \in \mathfrak{m}'^m/\mathfrak{m}'^{m+1}$, un elemento cualquiera.
Podemos suponer que $p \in H_m(X_0, \ldots, X_n)$, (descomponiento $p/q$ en sumas donde los numeradores son homogéneos, todo lo que pase de grado $n+1$ se va). Ahora $q = a_0 + h$, con $a_0 \in K$ y $h \in \mathfrak{m}$, podemos concluir :

$$a_0 p - qp = -(hp) \in \mathfrak{m}^{n+1} \subseteq \mathfrak{m}'^{n+1}$$

con lo que $\varphi(a_0 p) = p/q + \mathfrak{m}'^{n+1}$ y $\varphi$ es un isomorfismo. □

LEMA 6.5.21. *Sea $A = K[X_0, \ldots, X_n]$ anillo graduado con la graduación usual. Sea $\mathfrak{m} := (X_0, \ldots, X_n)$ ideal maximal en $A$ e $\mathfrak{a}$ un ideal homogéneo de $A$. Sean $\overline{\mathfrak{m}} := \mathfrak{m}/\mathfrak{a}$ ideal maximal del anillo graduado $A/\mathfrak{a}$. Entonces, los siguientes anillos son isomorfos :*

$$G_{\overline{\mathfrak{m}}(A/\mathfrak{a})_{\overline{\mathfrak{m}}}}((A/\mathfrak{a})_{\overline{\mathfrak{m}}}) = A/\mathfrak{a}$$

DEMOSTRACIÓN. Sigue los mismos pasos que la prueba anterior. □

COROLLARIO 6.5.22. *Sea $\mathfrak{a}$ un ideal homogéneo en $A := K[X_0, \ldots, X_n]$. Sea $\mathfrak{m} := (X_0, \ldots, X_n)$ ideal maximal de $A$ y sea $\overline{\mathfrak{m}} := \mathfrak{m}/\mathfrak{a}$ ideal maximal de $A/\mathfrak{a}$. Entonces,*

$$deg(\chi(G(A/\mathfrak{a}, -) = degP_{\overline{\mathfrak{m}}}((A/\mathfrak{a})_{\overline{\mathfrak{m}}}, -) - 1 = dim_{Krull}((A/\mathfrak{a})_{\mathfrak{m}})) - 1$$

*En particular, para cualquier conjunto algebraico proyectivo, $V \subseteq ¶_n(K)$ se tiene :*

$$deg(\chi(K[V], -) = dimK[V]_{\overline{\mathfrak{m}}} - 1$$

*donde $\overline{\mathfrak{m}} := \mathfrak{m}/I(V)$.*

DEMOSTRACIÓN. Usando el Teorema de la dimensión y los isomorfismos destacados en los apartados anteriores tenemos claramente el Corolario. □

COROLLARIO 6.5.23 (**Dimensión de la Intersección**). *Sean $\mathfrak{p}_1$ y $\mathfrak{p}_2$ dos ideales primos en un anillo de polinomios $R = K[X_1, \ldots, X_n]$ sobre un cuerpo $K$. Supongamos $dim(R/\mathfrak{p}_1) = r$, $dim(R/\mathfrak{p}_2) = s$. Entonces, para cualquier ideal primo $\mathfrak{q}$ minimal sobre $\mathfrak{p}_1 + \mathfrak{p}_2$ se tiene :*

$$dim(R/\mathfrak{q}) \geq r + s - n$$

Demostración. Consideremos un nuevo conjunto de variables $\{Y_1, \ldots, Y_n\}$ y el ideal $\mathfrak{p}_2'$ en el anillo $K[Y_1, \ldots, Y_n]$ obtenido simplemente cambiando las variables. Definamos finalmente

$$R' := K[X_1, \ldots, X_n Y_1, \ldots, Y_n]$$

En este anillo consideramos el ideal $I := \mathfrak{p}_1 + \mathfrak{p}_2'$ y el ideal $D$ generado por $(X_1 - Y_1, \ldots, X_n - Y_n)$ que corresponde a la diagonal. Obsérvese el isomorfismo de anillos entre $R'/D$ y $R$.
Ahora, tomemos normalizacioones de Noether de $K[X_1, \ldots, X_n]/\mathfrak{p}_1$ y $K[Y_1, \ldots, Y_n]/\mathfrak{p}_2'$, tendremos una normalizacion de Noether de $R'/I$ y facilmente se concluye

$$dim(R'/I) := dim(R/\mathfrak{p}_1) + dim(R/\mathfrak{p}_2)$$

Ahora, sea $\mathfrak{q}$ un primo minimal de $R$ sobre $\mathfrak{p}_1 + \mathfrak{p}_2$. Por el isomorfismo, podemos identificarlo con un ideal primo $Q$ de $R'/D$ que contiene a $I + D/D$. Más aún, se respetan las condiciones de minimalidad y coaltura. En particular, $Q/I$ es un ideal primo minimal sobre $D$ en $R'/I$. Por estar generado $D + I/D$ por las clases de sus $n$ generadores, obtenemos $ht(Q/I) \leq n$ (Krull).
De otro lado, $R'/I + D$ es isomorfo a $R/\mathfrak{p}_1 + \mathfrak{p}_2$, luego,

$$dim(R/\mathfrak{q}) := dim((R'/I)/(Q/I)) = dim(R'/I) - ht(Q/I) \geq r + s - n$$

□

Corollario 6.5.24. *Sea $K$ un cuerpo algebraicamente cerrado $V, W \subseteq K^n$ dos conjuntos algebraicos irreducibles. Entonces,*

$$dim(V \cap W) \geq dim(V) + dim(W) - n$$

**6.5.2. Grado y Normalización de Noether.** Aunque aún no hemos hablado del caso de dimensión positiva, veremos más adelante la relevancia de la Normalización de Noether (ya hemos visto algo en nuestra prueba del Nullstellensatz) y, en ese contexto, será útil valorar el resultado siguiente:

Teorema 6.5.25. *Sea $F := [f_1, \ldots, f_s] \in K[X_1, \ldots, X_n]^s$ un sistema de ecuaciones polinomiales generando un ideal $\mathfrak{a}$. Sea $V(F) \subseteq \mathbb{K}^n$ el conjunto algebraico que definen y supongamos que es equidimensional (i.e. todas sus componentes tienen la misma dimensión). Sea $K[Y_1, \ldots, Y_r]$ una normalización de Noether de $K[X_1, \ldots, X_n]/\mathfrak{a}$. Supongamos que $Y_1, \ldots, Y_r$ son combinaciones lineales de las variables $X_1, \ldots, X_n$. Sea $g \in K[X_1, \ldots, X_n]$ un polinomio adicional. Se tiene :*

i) *La siguiente es una extensión entera de anillos :*

$$K[Y_1, \ldots, Y_r] \hookrightarrow K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}.$$

ii) *La imagen del morfismo $G$ siguiente es una hipersuperficie de $\mathbb{K}^{r+1}$, donde*

$$G \ : V \longrightarrow \mathbb{K}^{r+1}$$

*donde*

$$G(x_1, \ldots, x_n) := (Y_1(x_1, \ldots, x_n), \ldots, Y_r(x_1, \ldots, x_n), g(x_1, \ldots, x_n)).$$

iii) *El grado de la hipersuperficie $G(V)$ está acotado por $deg(V) \cdot deg(g)$.*

iv) *El polinomio mínimo mónico de la dependencia entera de $g + \sqrt{\mathfrak{a}} \in K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}$ sobre $K[Y_1, \ldots, Y_r]$ está acotado por $deg(V) \cdot deg(g)$ y, de hecho, coincide con el polinomio mínimo de la hipersuperficie $G(V)$.*

*Más aún, si $V(F)$ es irreducible se tiene :*

$$\left[q.f.\left(K[X_1, \ldots, X_n]/\sqrt{\mathfrak{a}}\right) \ : \ K(Y_1, \ldots, Y_r)\right] \leq deg(V(F)),$$

*donde $q.f.$ significa cuerpo de fracciones.*

Capítulo 7

# El Teorema de la Función Implícita : Fibras de Levantamiento.

## 7.1. Introducción

El Teorema de la Función Implícita ha sido una de las piezas fundamentales de la Historia de la Matemática. La parametrización local de variedades alrededor de puntos donde el jacobiano no se anula comienza con I. Newton en 1771. El algoritmo que Newton había pensado para aproximar raíces de polinomios univariados era adaptable a la aproximación local de curvas mediante funciones racionales y su expansión en series de potencias formales. Ciertamente Newton vislumbra las series de potencias que luego serán extendidas por B. Taylor[1]. Parece que Taylor asigna el descubrimiento de las series de potencias formales a Newton en la frase *"Sir Isaac Newton's series"*. Sin embargo, las series "de Taylor" parecen remontarse a J. Wallis[2], quien las introdujo para el cálculo de la integral de la función $(1-x^2)^{1/2}$. Parece, también, que otros matemáticos como J. Gregory, G.W. Leibniz, Johann Bernoulli y A. de Moivre habían descubierto ya variantes de las series de potencias o series "de Taylor".
La aportación fundamental de Newton es doble : de una parte permite representar funciones implícitas a través de su expansión en series de potencias formales. De otra parte, ofrece un algoritmo de aproximación de estas series de potencias formales. Tenemos así un Teorema de la Función Implícita con funciones dadas mediante series de las que Newton desconoce la convergencia. Parece también que no se preocupó excesivamente de este problema.
De hecho, debemos esperar a K. Weirstrass para disponer de una Teoría completa de las Funciones Analíticas. Debido a sus problemas de salud, Weierstrass no escribió siempre y del modo más completo las ideas subyacentes a sus investigaciones. Los primeros estudios sobre funciones analíticas datan de su trabajo de 1854[3]. No será hasta 1861 que Weierstrass obtendrá el primer ejemplo de función real continua no diferenciable. Esto supuso un vuelco considerable en la fundamentación del Análisis que, hasta Weierstrass, tenía mucho de intuicionista. Las aportaciones fundamentales de K. Weierstrass tuvieron siempre la forma de cursos semestrales impartidos en la Universidad de Berlín (hoy Humboldt Universität). Dichos cursos fueron recogidos por muchos de sus alumnos en forma de textos (como, por ejemplo, las notas tomadas por W. Killing de los cursos impartidos en 1868 o las notas tomadas por A. Hurwirtcz de los cursos de Weierstrass en 1878). Es destacable, por la influencia que tiene en este Capítulo, el curso de 1863/64 sobre la *"Teoría General de las Funciones Analíticas"*.
En lo concerniente a este Capítulo nos interesarán sustancialmente los Teoremas de División y Preparación[4] que discutiremos en el caso de anillos de series de potencias formales.

---

[1] B. Taylor. *" Methodus incrementorum directa et inversa"*. (1715)

[2] J. Wallis. *"Arithmetica infinitorum"*. (1656)

[3] En este trabajo Weierstrass explora la descripción de las funciones abelianas mediante series de potencias formales : K. Weierstras. "Zur Theorie der Abelschen Functionen". *J. für Reine und Angew. Math.* (1854).

[4] K. Weierstrass. "Zur Theorie der eindeutigen analytischen Functionen". *Berl. Abh.* (1876) 11-60.

Posteriormente, estos trabajos iniciales de Newton se diversifican en varios frentes. De una parte, un esfuerzo por demostrar el Teorema de la Función Implícita y la convergencia de las series resultantes; pero preservando el carácter iterativo del método de Newton puede encontrarse en J. Liouville[5]. A la sazón, A. Cauchy, predecesor de Liouville en la École Polytechnique, había dado ya una demostración del Teorema de la Función Implícita de tipo existencial, basándose en los desarrollos hechos para demostrar la existencia y unicidad de solución de Ecuaciones Diferenciales Ordinarias (Teorema de Cauchy–Peano–Lipschitz)[6].

De otro lado, V. Puisseux, ha continuado los trabajos de Cauchy, obteniendo las nociones de polo y puntos de ramificación, así como las series de potencias formales con exponente fraccionario (Series de Puisseux) y ha extendido el algoritmo original de Newton para la representación local de curvas alrededor de puntos singulares.

Finalmente, K. Hensel reinterpreta las ideas de K. Weierstrass sobre series de potencias formales introduciendo y desarrollando los número p-ádicos y la correspondiente interpretación del algoritmo de Newton.

Este Capítulo está dedicado a hacer una relectura, en el lenguaje actual, de la historia de estos resultados. Ciertamente, como en el caso de Newton, no haremos mucho caso a la cuestión de la convergencia y nos instalaremos en el confortable anillo local regular de las series de potencias formales en un punto. Comenzaremos con una somera descripción de las propiedades del completado de anillos locales Noetherianos para la filtración $\mathfrak{m}-$ádica (Sección 7.3) siguiendo una combinación del [**ZaSa, 60**] y del [**Ma, 80**].

Posteriormente (Sección 7.4 ) se demuestran los Teoremas de División y Preparación que pueden encontrarse en cualquiera de los textos clásicos de Funciones Holomorfas en Varias Variables Complejas como [**GuRo, 65**], [**Nar, 68**]. Aunque esos enunciados también se encuentran en [**ZaSa, 60**], he elegido la versión del más reciente [**Ka$^2$, 83**].

En el camino (Sección 7.5) nos dedicaremos a la noción de anillo local regular y a exponer el Criterio del Jacobiano. La noción genérica de anillo local regular es debida al alumno de E. Noether W. Krull[7]. Incluimos una demostración del Teorema de Estructura para anillos locales equi–característicos, como el prensentado por el alumno de O. Zariski I.S. Cohen[8]. La demostración propuesta para este resultado que propongo seguir es la expuesta en [**ZaSa, 60**]. Juntando este Teorema de I.S. Cohen con los Teoremas de Weierstrass tenemos una versión débil como resolución del Problema de Serre.

A partir de esta Sección ya pasamos a la Demostración del Teorema de la Función Implícita (Sección 7.6). En esta Sección daremos dos variantes del Lema de Newton–Hensel. De una parte, la versión del Lema de Hensel propuesta en [**ZaSa, 60**] y la no menos destacable influencia del texto de P. Ribenboim[9]. La demostración de [**ZaSa, 60**] consiste en mostrar un algoritmo de convergencia lineal para la norma no–arquimediana definida por la filtración $\mathfrak{m}-$ádica (en la Subsección 7.6.1). Posteriormente, ofreceremos una demostración no ya del Lema de Hensel sino del Teorema de la Función Implícita usando el operador de Newton multivariado (en la Subsección 7.6.2) y demostrando que tiene una convergencia cuadrática para la norma no–arquimediana.

---

[5]Véase el comentario histórico hecho por M. Demazure en su texto *"Catastrophes et Bifurcations"* Ellipses (1989).

[6]Véase una descripción de los sucesos históricos en el excelente texto de ecuaciones diferenciales E.L. Ince. *"Ordinary Differential Equations"*. Dover (1956).

[7]Véanse los trabajos

- W. Krull. "Dimensionen in Stellensringen". *J. reine angew. Math.***179** (1938) 204–26.
- W. Krull. *"Idealtheorie"*. Springer (1935).

[8]I.S. Cohen. "On the Structure and Ideal Theory of Complete Local Rings". *Trans. AMS* **59** (1946) 54–106.

[9]P. Ribenboim. "Equivalent forms of Hensel's Lemma". *Expo. Math.* **3** (1985) 3–24.

## 7.2. Anillos y módulos topológicos : filtraciones y completados

El propósito es comenzar con el [**Po, 66**] y continuar, más adelante, con el modelo del discurso del Capítulo final de [**ZaSa, 60**].

DEFINICIÓN 51. *Llamaremos anillo topológico a todo anillo $A$ dotado de una topología $\mathcal{T}$ tal que las siguientes son aplicaciones continuas :*

i) $- : A \times A \longrightarrow A, \quad -(a,b) := a - b$
ii) $\cdot : A \times A \longrightarrow A, \quad \cdot(a,b) := a \cdot b.$

*donde $A \times A$ está dotado de la topología producto.*

Tras unos pocos ejemplos clásicos :

DEFINICIÓN 52. *Sea $(A, \mathcal{T})$ un anillo topológico, $M$ un $A-$módulo y $\mathcal{T}'$ una topología sobre $M$. Diremos que $M$ es un $A-$módulo topológico si las siguientes son aplicaciones continuas :*

i) $- : M \times M \longrightarrow M, \quad -(m,n) := m - n$
ii) $\cdot : A \times M \longrightarrow M, \quad \cdot(a,m) := a \cdot m.$

*donde $A \times M$ está dotado con la topología producto.*

PROPOSICIÓN 7.2.1. *Sean $(A, \mathcal{T})$ un anillo topológico y $(M, \mathcal{T}')$ un $A-$módulo topológico. Entonces para $x \in A$ y $m \in M$, se tiene :*

i) *la traslación $t_x : A \longrightarrow A$, dada por $t_x(a) := a + x$, es un homeomorfismo.*
ii) *la traslación $t_m : M \longrightarrow M$, dada por $t_m(n) := m + n$, es un homeomorfismo.*

Obsérvese que, como en el caso de los espacios vectoriales topológicos, si $\mathcal{U}_0$ es una base de entornos de $0 \in A$, donde $(A, \mathcal{T})$ es un anillo topológico. Entonces, la clase :

$$x + \mathcal{U}_0 := \{t_x(U) \ : \ U \in \mathcal{U}_0\}$$

es una base de entornos de $x \in A$.
Análogamente ocurrirá cuando tratemos de $A-$módulos topológicos.
La conclusión de esta observación es que para determinar una topología en un anillo o en un módulo, nos basta con determinar una base de entornos del 0 para esa topología. Las propiedades adicionales que tal base de entornos debe verificar se describen en la siguiente Proposición tomada del texto clásico de grupos topológicos de [**Po, 66**].

PROPOSICIÓN 7.2.2. *Sea $A$ un anillo cualquiera y consideremos una colección de subconjuntos de $A$, $\Sigma \subseteq \mathcal{P}(A)$ verificando :*

i) *La intersección de dos elementos cualesquiera de $\Sigma$ contiene a algún elemento de $\Sigma$.*
ii) *Si $U \in \Sigma$, existe $W \in \Sigma$ tal que :*

$$W - W := \{x - y \ : \ x, y \in W\} \subseteq U, \quad W^2 := \{xy \ : \ x, y \in W\} \subseteq U$$

iii) *Si $U \in \Sigma$, $x \in U, y \in A$, existe $W \in \sigma$ tal que :*

$$t_x(W) \subseteq U, \quad yW := \{y \cdot a \ : \ a \in W\} \subseteq U$$

*Entonces, existe una única topología $\mathcal{T}$ sobre $A$ tal que $(A, \mathcal{T})$ es un anillo topológico y $\Sigma$ es una base de entornos abiertos de $0 \in A$.*

PROPOSICIÓN 7.2.3. *Sea $(A, \mathcal{T})$ un anillo topológico y $\Sigma$ una base de entornos abiertos de $0 \in A$. Entonces, $\Sigma$ verifica las propiedades i), ii) y iii) de la Proposición anterior.*

Análogos resultados se pueden obtener para módulos topológicos (cf. [**Po, 66**]).

PROPOSICIÓN 7.2.4. *Sea $(A, \mathcal{T})$ un anillo topológico y $(M, \mathcal{T}')$ un $A-$módulo topológico con respecto a la topología $\mathcal{T}$ sobre $A$. Las siguientes afirmaciones son equivalentes :*

i) *$(M, \mathcal{T}')$ es un espacio topológico de Hausdorff.*

ii) *El conjunto* $\{0\}$ *es un cerrado.*
iii) *Si* $\Sigma'$ *es una base de entornos abiertos de* $0 \in M$*, se tiene :*

$$\{0\} = \bigcap_{U \in \Sigma'} U$$

No vamos a ocupar este curso en un amplio estudio de los anillos topológicos. El alumno puede seguir, si quiere, el texto [**Po, 66**]. Nos centraremos en las filtraciones.

DEFINICIÓN 53. i) *Sea* $A$ *un anillo. Llamaremos filtración sobre* $A$ *a toda colección* $\Sigma$*, cadena descendente de ideales :*

$$\Sigma := \{A = \mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \cdots\}$$

*verificando* $\mathfrak{a}_n \cdot \mathfrak{a}_m \subseteq \mathfrak{a}_{n+m}$, $\forall n, m \in \mathbb{N}$*. Diremos que* $(A, \Sigma)$ *es un anillo filtrado.*

ii) *Sea* $(A, \Sigma)$ *un anillo filtrado y* $M$ *un* $A-$*módulo. Una filtración sobre* $M$ *compatible con la filtración* $\Sigma = \{\mathfrak{a}_n : n \in \mathbb{N}\}$ *de* $A$*, a toda cadena descendente de submódulos de* $M$ *:*

$$\Sigma' := \{M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n \supseteq \cdots\}$$

*tal que* $\mathfrak{a}_n \cdot N_m \subseteq N_{n+m}$, $\forall n, m \in \mathbb{N}$*.*

PROPOSICIÓN 7.2.5. i) *Si* $(A, \Sigma)$ *es un anillo filtrado, la filtración* $\Sigma$ *verifica las propiedades de la Proposición 7.2.2 anterior y existe una única topología sobre* $A$ *para la cual* $\Sigma$ *es una base de entornos abiertos de* $0 \in A$*. A esa topología se la denomina topología asociada a la filtración* $\Sigma$*.*

ii) *Un análogo resultado se tiene para módulos con filtraciones.*

PROPOSICIÓN 7.2.6. *Sea* $(A, \Sigma)$ *es un anillo filtrado, y* $(M, \Sigma')$ *es un* $A-$*módulo filtrado, con una filtración* $\Sigma'$ *compatible con la filtración* $\Sigma$ *de* $A$*. Supongamos*

$$\Sigma := \{A = \mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \cdots\}$$

$$\Sigma' := \{M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n \supseteq \cdots\}$$

*Entonces, para cada* $S \subseteq A$ *y cada* $N \subseteq M$*, las clausuras de* $S$ *y* $N$ *para las respectivas topologías vienen dadas por :*

$$\overline{S} = \bigcap_{n \in \mathbb{N}} (S + \mathfrak{a}_n)$$

$$\overline{N} = \bigcap_{n \in \mathbb{N}} (N + N_n)$$

COROLLARIO 7.2.7. *Con las mismas notaciones de la Proposición anterior, sea* $\mathfrak{a}$ *un ideal de* $A$ *y* $N$ *un submódulo de* $M$*. Entonces,*

i)

$$\overline{\mathfrak{a}} = \bigcap_{n \in \mathbb{N}} (\mathfrak{a} + \mathfrak{a}_n)$$

ii) *Si* $\mathfrak{a}$ *es abierto en* $A$*, entonces es cerrado.*
iii)

$$\overline{N} = \bigcap_{n \in \mathbb{N}} (N + N_n)$$

iv) *Si* $N$ *es abierto en* $M$*, entonces es cerrado.*

COROLLARIO 7.2.8. *Sea* $(A, \Sigma)$ *es un anillo filtrado, y* $(M, \Sigma')$ *es un* $A-$*módulo filtrado, con una filtración* $\Sigma'$ *compatible con la filtración* $\Sigma$ *de* $A$*. Supongamos :*

$$\Sigma' := \{M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n \supseteq \cdots\}$$

*Entonces, $M$ con la topología asociada a la filtración $\Sigma'$ es de Hausdorff si y solamente si :*

$$\{0\} = \bigcap_{n\in\mathbb{N}} N_n$$

Seguiremos con la condición de metrizabilidad, que se basará en este Corolario, y que trataremos de seguir a través del Capítulo de Algebra Local del texto [**ZaSa, 60**]. Más adelante recuperaremos la condición de Hausdorff a través del Teorema de la Intersección de Krull.

TEOREMA 7.2.9. *Sea $(A,\Sigma)$ es un anillo filtrado, y $(M,\Sigma')$ es un $A-$módulo filtrado, con una filtración $\Sigma'$ compatible con la filtración $\Sigma$ de $A$. Supongamos*

$$\Sigma' := \{M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n \supseteq \cdots\}$$

*Si $M$ es Hausdorff con la topología asociada a la filtración $\Sigma'$, entonces es metrizable con la métrica :*

$$d_M(x,y) := e^{-k}$$

*donde $x-y \in N_k, x-y \notin N_{k+1}$. En particular, si $\overline{B_M}(0,e^{-n})$ es la bola cerrada de centro $0 \in M$ y radio $e^{-n}$ para la métrica $d_M$, esta bola coincide con el submódulo $N_n$.*

Recordemos que todo espacio métrico posee un completado. Podemos hacer aquí la construcción del completado de un $A-$módulo filtrado cuya topología es de Hausdorff. Recordemos de los cursos elementales de topología la siguiente propiedad :

TEOREMA 7.2.10 (Completado de un espacio métrico). *Sea $(X,d)$ un espacio métrico. Entonces, existe un espacio métrico completo $(X^*,d^*)$ y una función $i : X \longrightarrow X^*$ continua, verificando :*

i) *$i$ es una isometría entre $X$ y una parte densa de $X^*$.*
ii) *Dada $\varphi : X \longrightarrow Y$ una función uniformemente contínua, donde $(Y,d')$ es un espacio métrico completo, existe una única función continua $\psi : X^* \longrightarrow Y$ tal que $\psi \circ i = \varphi$.*

*De otro lado, cualquier otro espacio métrico completo que verifique estas dos propiedades es homeomorfo (e isométrico) a $(X^*,d^*)$.*
*A cualquier espacio métrico $(X^*,d^*)$ y aplicación $i : X \longrightarrow X^*$ verificando estas propiedades se le denomina completado del espacio métrico $(X,d)$.*

Observando que la suma y el producto son funciones uniformemente continuas, se pueden extender las respectivas estructuras de anillo y módulo al completado. Esto es,

PROPOSICIÓN 7.2.11. *Sea $(A,\Sigma)$ es un anillo filtrado, y $(M,\Sigma')$ es un $A-$módulo filtrado de Hausdorff, con una filtración $\Sigma'$ compatible con la filtración $\Sigma$ de $A$. Sea $M^*$ es el completado de $M$ para la métrica definida por la filtración $\Sigma'$. Entonces, $M^*$ posee una estructura de $A-$módulo filtrado de Hausdorff, es decir, es un $A-$módulo filtrado con la filtración dada por :*

$$\Sigma^* := \{M^* \supseteq \overline{N_1} \supseteq \cdots \supseteq \overline{N_n} \supseteq \cdots\}$$

*donde $\overline{N_i}$ es la clausura de $N_i$ en $M^*$, y la topología definida por esa filtración en $M^*$ es la topología de $M^*$ como completado del espacio métrico $(M,d_M)$.*

Lo mismo se puede decir del anillo y su completado $A^*$.
Las filtraciones y las graduaciones en anillos y módulos son elementos interrelacionados de manera fuerte. Para verlo, introduzcamos los siguientes ejemplos :

EJEMPLO 7.2.12. ▪ Sea $A$ un anillo $\Sigma := \{A = \mathfrak{a}_0 \supseteq \cdots \mathfrak{a}_n \supseteq \cdots\}$ una filtración sobre $A$. Podemos definir el grupo abeliano

$$G_\Sigma(A) := \oplus_{n\in\mathbb{N}}(\mathfrak{a}_n/\mathfrak{a}_{n+1})$$

Al grupo abeliano $G_\Sigma(A)$ le podemos dotar de una estructura de anillo, extendiendo la operación producto

$$\cdot : G_\Sigma(A) \times G_\Sigma(A) \longrightarrow G_\Sigma(A)$$

sobre los elementos "homogéneos" de la manera natural. Con esta definición, $G_\Sigma(A)$ es un anillo graduado que llamaremos anillo graduado asociado a la filtración $\Sigma$ sobre $A$.

- Sea $(A, \Sigma)$ un anillo filtrado y $(M, \Sigma')$ un $A-$módulo filtrado con una filtración compatible con la filtración $\Sigma$ de $A$. De la manera natural se construye $G_{\Sigma'}(M)$ y se le dota de una estructura de $G_\Sigma(A)-$módulo, que llamaremos módulo asociado a la filtración $\Sigma'$ sobre $M$.

DEFINICIÓN 54. *Sea $(A, \Sigma)$ un anillo filtrado y $(M, \Sigma')$ un $A-$módulo filtrado con una filtración compatible con $\Sigma$. Dados $x \in A$, $m \in M$, llamaremos parte inicial de $x$ y de $m$ a los elementos :*

$$G_\Sigma(x) = x + \mathfrak{a}_{n+1} \in G_\Sigma(A), \quad \textit{donde } n = \nu_\Sigma(x)$$

$$G_{\Sigma'}(m) = m + N_{n+1} \in G_\Sigma(M), \quad \textit{donde } n = \nu_{\mathfrak{a}}(m)$$

*o bien $G_\Sigma(x) = 0$ y $G_{\Sigma'}(m) = 0$, cuando $\nu_\Sigma(x) = +\infty$ y $\nu_{\Sigma'}(m) = +\infty$*

LEMA 7.2.13. *En las notaciones anteriores, dados $a, b \in A$, son equivalentes :*

i) $\nu_\Sigma(ab) > \nu_\Sigma(a) + \nu_\Sigma(b)$.
ii) $ab \in \mathfrak{a}_{\nu_\Sigma(a)+\nu_\Sigma(b)+1}$.
iii) $G_\Sigma(a)G_\Sigma(b) = 0$ *en* $G_\Sigma(A)$.

*Donde $\nu_\Sigma$ es la función de orden asociada a la filtración $\Sigma$.*

**7.2.1. Graduaciones y filtraciones $\mathfrak{a}-$ádicas.** Uno de los ejemplos esenciales de filtraciones en anillos y módulos es el definido por las potencias de un ideal.

DEFINICIÓN 55. *Sea $A$ un anillo, $M$ un $A-$módulo y $\mathfrak{a}$ un ideal de $A$. Llamaremos filtración $\mathfrak{a}-$ádica sobre $A$ y sobre $M$ a las filtraciones definidas por los conjuntos :*

$$\Sigma_{\mathfrak{a}}(A) := \{A = \mathfrak{a}^0 \supseteq \mathfrak{a}^1 \supseteq \mathfrak{a}^2 \supseteq \cdots\}$$

$$\Sigma_{\mathfrak{a}}(M) := \{M = \mathfrak{a}^0 M \supseteq \mathfrak{a}^1 M \supseteq \mathfrak{a}^2 M \supseteq \cdots\}$$

EJEMPLO 7.2.14.

- Dado el anillo de polinomios $A := K[X_0, \ldots, X_n]$ y el ideal maximal $\mathfrak{m} := (X_0, X_1, \ldots, X_n)$, la filtración $\mathfrak{m}-$ádica en $A$ es la dada por las potencias del ideal $\mathfrak{m}$, es decir, por los ideales $\mathfrak{m}^n$ formados por los polinomios tales que la multiplicidad de $(0, \ldots, 0)$ es, al menos, $n$.
- Dado el anillo $\mathbb{Z}$ y un elemento primo $p \in \mathbb{Z}$, la filtración $p-$ádica es la filtración asociada a las potencias del ideal primo $(p)$ de $\mathbb{Z}$.

DEFINICIÓN 56. *Sea $A$ un anillo, $M$ un $A-$módulo y $\mathfrak{a}$ un ideal de $A$. Llamaremos anillo graduado asociado a la filtración $\mathfrak{a}-$ádica, $G_{\mathfrak{a}}(A)$, en $A$ y el $G_{\mathfrak{a}}(A)-$módulo asociado a la filtración $\mathfrak{a}-$ádica en $M$ a los siguientes anillo y módulo graduados :*

$$G_{\mathfrak{a}}(A) := \oplus_{n\in\mathbb{N}}(\mathfrak{a}^n/\mathfrak{a}^{n+1})$$

$$G_{\mathfrak{a}}(M) := \oplus_{n\in\mathbb{N}}(\mathfrak{a}^n M/\mathfrak{a}^{n+1}M)$$

*con las operaciones pertinentes.*

NOTACIÓN 7.2.15. Denotaremos por $\nu_{\mathfrak{a}}$ tanto a la función de orden definida por la filtración $\mathfrak{a}-$ádica en $A$ como en $M$, declarando en cada caso a cuál nos referimos. De la misma manera denotaremos la parte inicial de un elemento $x \in A$ o $m \in M$, siendo :

$$G_{\mathfrak{a}}(x) = x + \mathfrak{a}^{n+1} \in \mathfrak{a}^n/\mathfrak{a}^{n+1}, \quad \text{donde } n = \nu_{\mathfrak{a}}(x)$$

$$G_{\mathfrak{a}}(m) = m + \mathfrak{a}^{n+1}M \in \mathfrak{a}^n M/\mathfrak{a}^{n+1}M, \quad \text{donde } n = \nu_{\mathfrak{a}}(m)$$

Las filtraciones y graduaciones $\mathfrak{a}-$ádicas permiten obtener propiedades del anillo a partir del anillo graduado asociado. Así, tenemos :

LEMA 7.2.16. *Sea $A$ un anillo, $\mathfrak{a}$ un ideal de $A$, y sea $M$ un $A-$módulo.*

i) *Si $A$ es noetheriano, también lo es $G_{\mathfrak{a}}(A)$.*
ii) *Si $A$ es Hausdorff (i.e. $\cap_{n\in\mathbb{N}}\mathfrak{a}^n = (0)$), entonces,*

$$G_{\mathfrak{a}}(A) \text{ es un dominio} \Rightarrow A \text{ es un dominio}$$

*En este caso, $\nu_{\mathfrak{a}}(ab) = \nu_{\mathfrak{a}}(a) + \nu_{\mathfrak{a}}(b)$, para cada $a, b \in A$.*
iii) *Si $A$ es noetheriano y $M$ es un $A-$módulo finitamente generado, $G_{\mathfrak{a}}(M)$ es un $G_{\mathfrak{a}}(A)-$módulo noetheriano.*
iv) *En las anteriores condiciones, cada $\mathfrak{a}^n M/\mathfrak{a}^{n+1}M$ es un $A/\mathfrak{a}-$módulo noetheriano y finitamente generado.*

También condiciones más técnicas como la de ser normal un anillo se trasladan bien del graduado al anillo total en ciertas condiciones :

PROPOSICIÓN 7.2.17. *Sea $A$ un anillo noetheriano, $\mathfrak{a}$ un ideal de $A$. Supongamos que todo ideal principal de $A$ es cerrado para la topología $\mathfrak{a}-$ádica. Entonces,*

$$G_{\mathfrak{a}}(A) \text{ normal } \Rightarrow A \text{ normal}$$

**Construcción** Como siempre, sea $A$ un anillo, $M$ un $A-$módulo, $N$ un submódulo de $M$ e $\mathfrak{a}$ un ideal de $A$. Tratamos de relacionar los anillos graduados correspondientes a las filtraciones $\mathfrak{a}-$ádicas en $M$ y $M/N$. Para ello, consideremos la proyección canónica :

$$\pi : M \longrightarrow M/N$$

Observamos que $\pi(\mathfrak{a}^n M) = \mathfrak{a}^n(M/N)$. Para cada $n \in \mathbb{N}$, consideremos el morfismo de $A-$módulos :

$$\varphi_n : \mathfrak{a}^n M + N \longrightarrow \mathfrak{a}^n(M/N)$$

dado por $\varphi_n(m) := m + N$. Este morfismo de $A-$módulos induce :

PROPOSICIÓN 7.2.18. *En las notaciones anteriores :*

$$G_{\mathfrak{a}}(M/N) \cong \oplus_{n\in\mathbb{N}} \left(\mathfrak{a}^n M + N/\mathfrak{a}^{n+1}M + N\right)$$

Consideremos ahora el morfismo de $G_{\mathfrak{a}}(A)-$módulos dado mediante :

$$\varphi : G_{\mathfrak{a}}(M) \longrightarrow G_{\mathfrak{a}}(M/N)$$

definido por :

$$\varphi(a + \mathfrak{a}^{n+1}M \in \mathfrak{a}^n M/\mathfrak{a}^{n+1}M) := a + \mathfrak{a}^{n+1}M + N \in \mathfrak{a}^n M + N/\mathfrak{a}^{n+1}M + N$$

Es fácil ver que se trata de un epimorfismo graduado de grado cero de $G_{\mathfrak{a}}(A)-$módulos. El núcleo será un submódulo homogéneo cuyos elementos homogéneos de grado $n$ viene dados por :

$$\left(((\mathfrak{a}^n M) \cap (\mathfrak{a}^{n+1}M + n))/(\mathfrak{a}^{n+1}M)\right)$$

Tenemos así la sucesión exacta corta de $A-$módulos :

$$0 \to ((\mathfrak{a}^n M) \cap (\mathfrak{a}^{n+1}M + N))/(\mathfrak{a}^{n+1}M) \to \mathfrak{a}^n M/\mathfrak{a}^{n+1}M \to \mathfrak{a}^n M + N/\mathfrak{a}^{n+1}M + N \to 0$$

Lo que induce una sucesión exacta corta de $G_{\mathfrak{a}}(A)-$módulos graduados :

$$0 \longrightarrow \oplus_{n\in\mathbb{N}} \left((\mathfrak{a}^n M \cap (\mathfrak{a}^{n+1}M + N))/\mathfrak{a}^{n+1}M\right) \longrightarrow G_{\mathfrak{a}}(M) \longrightarrow G_{\mathfrak{a}}(M/N) \longrightarrow 0$$

DEFINICIÓN 57. *Sea $A$ un anillo, $\mathfrak{a}$ un ideal de $A$, $M$ un $A-$módulo y $N$ un submódulo de $M$. Llamaremos submódulo director de $N$ al submódulo del $G_{\mathfrak{a}}(A)-$módulo $G_{\mathfrak{a}}(M)$ generado por :*

$$\oplus_{n\in\mathbb{N}} \left((\mathfrak{a}^n M) \cap (\mathfrak{a}^{n+1}M + N)/(\mathfrak{a}^{n+1}M)\right)$$

Obsérvese que el submódulo director de $M$ es el propio $G_{\mathfrak{a}}(M)$.

LEMA 7.2.19. *Sea $A$ un anillo, $\mathfrak{a}$ un ideal de $A$, $M$ un $A-$módulo y $N$ un submódulo de $M$. Entonces, el submódulo director de $N$ está generado por las formas iniciales de los elementos de $N$*

Estos resultados nos preparan para los dos primeros enunciados esenciales de esta Sección.

**7.2.2. El Lema de Artin–Rees y el Teorema de la Intersección de Krull.** Si bien el resultado conocido como Lema de Artin–Rees (fue probado independientemente por E. Artin y D. Rees [10]) tiene el aspecto de un sencillo Lema técnico, sus consecuencias (tanto para la demostración del Teorema de la Dimensión Local como para el Teorema de la Intersección de Krull) serán esenciales. En esta Subsección trataremos de la demostración de tal resultado técnico y lo aplicaremos a la demostración del Teorema de la Intersección de Krull. Por su parte, el Teorema de la Intersección, que se sigue del Lema de Artin–Ress y del Lema de Nakayama, tiene muy interesantes consecuencias en términos de la estructura topológica de los anillos con la filtración $\mathfrak{a}-$ádica.
La idea del Lema de Artin–Rees se expresa diciendo que para filtraciones en módulos compatibles con la filtración $\mathfrak{a}-$ádica, la topología inducida por la filtración y por la filtración $\mathfrak{a}-$ádica coinciden. Vemos la terminología.

DEFINICIÓN 58. *Sea $(A,\Sigma)$ un anillo filtrado y $(M,\Sigma')$ un $A-$módulo filtrado. Sea $\mathfrak{a}$ un ideal de $A$. Supongamos :*

$$\Sigma' := \{M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots\}$$

*Diremos :*

i) *La filtración $\Sigma'$ es compatible con la filtración $\mathfrak{a}-$ádica sobre $A$ si $\mathfrak{a}M_n \subseteq M_{n+1}$, para cada $n \in \mathbb{N}$.*
ii) *La filtración $\Sigma'$ es estable para la filtración $\mathfrak{a}-$ádica sobre $A$ si existe $n_0 \in \mathbb{N}$ tal que $\mathfrak{a}M_n = M_{n+1}$, para cada $n \geq n_0$.*

Nótese que la condición de ser compatible significa solamente que $(M,\Sigma')$ es un $A-$módulo filtrado, cuando en $A$ se considera la filtración $\mathfrak{a}-$ádica.
La filtración $\mathfrak{a}-$ádica en $M$ es un vivo ejemplo de filtración estable.

TEOREMA 7.2.20 (Lema de Artin-Rees). *Sea $A$ un anillo noetheriano, $\mathfrak{a}$ un ideal de $A$ y $M$ un $A-$módulo finitamente generado. Sea $N$ un submódulo de $M$.*
*Entonces, para toda filtración $\mathfrak{a}-$estable sobre $M$, la filtración inducida sobre $N$ es estable con respecto al ideal $\mathfrak{a}$ de $A$.*

COROLLARIO 7.2.21. *Sea $A$ un anillo noetheriano, $\mathfrak{a}$ un ideal de $A$, $M$ un $A-$módulo finitamente generado y $N$ un submódulo de $M$. Entonces, existe $n_0 \in \mathbb{N}$ tal que :*

$$\forall n \geq n_0,\ \mathfrak{a}(\mathfrak{a}^n M \cap N) = \mathfrak{a}^{n+1} M \cap N$$

Combinando el Lema de Nakayama con el Lema de Artin–Rees obtenemos el siguiente resultado relevante.

TEOREMA 7.2.22 (El Teorema de la Intersección de W. Krull). *Sea $A$ un anillo noetheriano, $\mathfrak{a}$ un ideal de $A$, $M$ un $A-$módulo finitamente generado*

i) *Si $N := \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n M$, $\mathfrak{a}N = N$.*
ii) *Si $\mathfrak{a}$ está contenido en el radical de Jacobson de $A$,*

$$\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n M = (0)$$

[10] D. Rees. "Two classical theorems of ideal theory". *Proc. Cambridge Philos. Soc.* **52** (1956), 155–157.

*y la topología definida por la filtración $\mathfrak{a}-$ádica sobre $M$ es Hausdorff y metrizable.*

iii) *Si $A$ es un dominio noetheriano, para cada ideal $\mathfrak{a}$ de $A$ se tiene :*

$$\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = (0)$$

*y la topología $\mathfrak{a}-$ádica sobre $A$ es Hausdorff y metrizable.*

COROLLARIO 7.2.23. *Si $(A, \mathfrak{m})$ es un anillo local noetheriano, las topologías $\mathfrak{q}-$ádicas definidas por cualquier ideal propio de $A$ en cualquier $A-$módulo finitamente generado son Hausdorff y, por ende, metrizables.*

PROPOSICIÓN 7.2.24. *Si $A$ es un anillo noetheriano y $\mathfrak{a}$ es un ideal contenido en el radical de Jacobson de $A$ :*

$$G_{\mathfrak{a}}(A) \text{ normal } \Rightarrow A \text{ normal}$$

El recíproco no es cierto. Ver [**Ma, 89**], p.119.

## 7.3. Propiedades del Completado : Anillos de Zariski.

Recordamos la construcción del completado de un anillo noetheriano con respecto a las filtraciones $\mathfrak{a}-$ádicas, hecho en las Subsecciones 7.2 y 7.2.1. Retomamos aquellos temas y hacemos algunas disquisiciones adicionales. Las referencias básicas serán los textos [**Ra** *et al.*, **75**], [**Ma, 80**], [**Ma, 89**] y [**ZaSa, 60**].

PROPOSICIÓN 7.3.1. *Sea $A$ un anillo noeteheriano, sea $\mathfrak{a}$ un ideal contenido en el radical de Jacobson de $A$,sea $M$ un $A-$módulo finitamente generado. Sea $A^*$ y $M^*$ los completados de $A$ y $M$ para las respectivas filtraciones $\mathfrak{a}-$ádicas. entonces, $M^*$ es el $A^*-$módulo generado por $M$.*[11]

COROLLARIO 7.3.2. *Sea $B$ un anillo y sea $A$ un subanillo de $B$, tal que $B$ es un $A-$módulo finitamente generado. Supongamos que $A$ es noetheriano y sea $\mathfrak{a}$ un ideal de $A$. Entonces, la topología de $B$ como $A-$módulo y la topología $\mathfrak{a}B-$ádica coinciden. En particular, la inclusión $A \hookrightarrow B$ induce una inclusión $A^* \hookrightarrow B^*$.*

Tenemos toda una serie de conclusiones técnicas, de gran utilidad en las argumentaciones futuras, como las siguientes :

COROLLARIO 7.3.3. *Sea $A$ un anillo noetheriano, $\mathfrak{a}$ un ideal de $A$, $M$ un $A-$módulo finitamente generado. Supongamos que tanto $A$ como $M$ son Hausdorff para sus respectivas topologías $\mathfrak{a}-$ádicas. Entonces :*

i) *La clausura de todo submódulo $N$ de $M$ en $M^*$ viene dada por el submódulo de $M^*$ generado por $N$ (i.e. $A^*N$). Más aún, $N$ es cerrado en $M$ si y solamente si $N = A^*N \cap M$.*

ii) *Las topologías de los completados $A^*$ y $M^*$ son sus respectivas topologías $\mathfrak{a}A^*-$ádicas.*

iii) *El completado del cociente $M/N$ para todo submódulo cerrado $N$ de $M$ viene dado por $M^*/A^*N$.*

iv) *Los anillos graduados $G_{\mathfrak{a}}(A)$ y $G_{\mathfrak{a}A^*}(A^*)$ son isomorfos como anillos graduados, por tanto, también se tiene :*

$$A/\mathfrak{a} \cong A^*/\mathfrak{a}A^*,$$

*isomorfismo como anillos y son isomorfimos de $A/\mathfrak{a}-$módulos los siguientes :*

$$\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \mathfrak{a}^n A^*/\mathfrak{a}^{n+1}A^*.$$

*Lo mismo sucede con los módulos finitamente generados.*

[11] En las notaciones de [**ZaSa, 60**], escribiríamos $M^* = A^*M$. Sin embargo, en las notaciones más apropiadas de [**Ma, 80**] escribiríamos $M^* = A^* \otimes_A M$. El enunciado se puede dar de ambas maneras.

Un importante resultado técnico es el siguiente :

TEOREMA 7.3.4. *Sea $A$ un anillo noetheriano, $\mathfrak{a}$ un ideal propio de $A$, $M$ un $A-$módulo y $N$ un submódulo de $M$. Supongamos que $A$ y $M$ son espacios de Hausdorff para las respectivas topologías $\mathfrak{a}-$ádicas y supongamos, además, que $A$ es completo.*
*Sean $\{x_1, \ldots, x_n\}$ una colección finita de elementos de $N$ tales que sus formas iniciales generan el submódulo director de $N$ en $G_{\mathfrak{a}}(M)$ como $G_{\mathfrak{a}}(A)-$módulo. Entonces, $\{x_1, \ldots, x_n\}$ generan $N$ como submódulo de $M$.*

El resultado puede verse en [**ZaSa, 60**].
La siguiente es una caracterización del tipo de anillos completos que más utilizaremos en estas páginas y que se denominan anillos de Zariski.

DEFINICIÓN 59. *Un anillo noetheriano $A$ se dice anillo de Zariski con respecto a un ideal propio $\mathfrak{a}$ de $A$ si para todo ideal propio $\mathfrak{b}$ de $A$, se tiene que $\mathfrak{b}$ es cerrado en $A$ para la topología definida por la filtración $\mathfrak{a}-$ádica.*

La siguiente caracterización puede verse en [**Ma, 80**] :

TEOREMA 7.3.5. *Sea $A$ un anillo noetheriano y $\mathfrak{a}$ un ideal propio de $A$. Son equivalentes :*

i) *El ideal $\mathfrak{a}$ está contenido en el radivcal de Jacobson de $A$,*
ii) *$1 - a$ es unidad de $A$ para todo $a \in \mathfrak{a}$,*
iii) *Si $M$ es un $A-$módulo finitamente generado y $\mathfrak{a}M = 0$, entonces, $M = 0$,*
iv) *Si $M$ es un $A-$módulo finitamente generado, la topología $\mathfrak{a}-$ádica sobre $M$ es Hausdorff,*
v) *Para todo $A-$módulo finitamente generado, todo submódulo $N$ de $M$ es cerrado para la topología $\mathfrak{a}-$ádica sobre $M$,*
vi) *$A$ es un anillo de Zariski con respecto al ideal $\mathfrak{a}$:*

Una caracterización más que puede verse en [**Ma, 80**] :

PROPOSICIÓN 7.3.6. *Sea $A$ un anillo noetheriano y $\mathfrak{a}$ un ideal propio de $A$. Entonces, $A$ es un anillo de Zariski si y solamente si su completado $A^*$ con respecto a la topología definida por la filtración $\mathfrak{a}-$ádica es fielmente plano sobre $A$.*

Como Corolario obtenemos

COROLLARIO 7.3.7. *El completado de todo anillo semi–local (respectivamente local) noetheriano con respecto a su radical de Jacobson es un anillo semi–local (resp. local) noetheriano de la misma dimensión.*

## 7.4. Los Teoremas de División y Preparación de Weierstrass.

En su esfuerzo por fundamentar el análisis complejo a partir de las series de potencias convergentes, K. Weierstrass impartió varios cursos basados en su trabajo de 1876 [12]. Los resultados que más han trascendido, conocidos como Teoremas de División y Preparación, son los resultados de los que nos ocuparemos en esta Sección. Para ello, recordaremos al alumno los elementos básicos del anillo de potencias formales. Comenzaremos introduciendo los anillos de series de potencias formales con coeficientes en un anillo $A$. Obtendremos como primer resultado el siguiente, que puede consultarse en [**Ma, 80**] :

PROPOSICIÓN 7.4.1. *Sea $A$ un anillo conmutativo con unidad. Entonces, $A[[X_1, \ldots, X_n]]$ es el completado de $A[X_1, \ldots, X_n]$ con respecto a la topología definida por la filtración $\mathfrak{a}-$ádica, donde*

$$\mathfrak{a} := (X_1, \ldots, X_n).$$

[12] K. Weierstrass. "Zur Theorie der eindeutigen analytischen Functionen". *Berl. Abh.* (1876) 11-60.

En particular, concluimos :

COROLLARIO 7.4.2. *Con las anteriores notaciones :*

i) *Si $A$ es noetheriano, $A[[X_1, \ldots, X_n]]$ es noetheriano.*
ii) *Si $A$ es un dominio, $A[[X_1, \ldots, X_n]]$ es un dominio.*
iii) *Si $A$ es normal, entonces $A[[X_1, \ldots, X_n]]$ es normal.*
iv) *Si $A$ es un anillo local, $A[[X_1, \ldots, X_n]]$ es un anillo local cuyo maximal está generado por el maximal de $A$ y las variables $X_1, \ldots, X_n$.*

Para la factorialidad necesitaremos dos clásicos resultados de K. Weierstrass conocidos como los Teoremas de Divisón y Preparación. Puede seguirse en cualquier texto clásico de Varias Variables Complejas o de Geometría Analítica como los textos [**GuRo, 65**], [**Nar, 68**] o [**Ka$^2$, 83**]. También se encuentran en [**ZaSa, 60**]. Seguiré esencialmente el texto de Kaup y Kaup.

DEFINICIÓN 60. *Una serie de potencias formales $\sigma \in K[[X_1, \ldots, X_n, Y]$ se denomina distinguida en $Y$ de orden $b$ si*

$$\sigma(0, \ldots, 0, Y) = Y^b e,$$

*para alguna unidad $e \in K[[Y]]$.*
*Sea denomina polinomio de Weierstsrass de grado $b$ a toda serie $\sigma \in K[[X_1, \ldots, X_n, Y]]$ de la forma :*

$$\sigma := Y^b + \sum_{k=0}^{b-1} a_k Y^k,$$

*donde $A_k \in K[[X_1, \ldots, X_n]]$.*

TEOREMA 7.4.3 (Teorema Preparatorio de Weierstrass). *Sea $\sigma \in K[[X_1, \ldots, X_n, Y]]$ una serie de potencias formales distinguida en $Y$ de orden $b$, entonces, existe un polinomio de Weierstrass $\omega \in K[[X_1, \ldots, X_n]][Y]$ de grado $b$ y una unidad $e \in K[[X_1, \ldots, X_n]]^*$ tales que*

$$\sigma = e\omega.$$

*Más aún, si $K = \mathbb{C}$ y $\sigma$ es una serie convergente, también es convergente $\omega$.*

TEOREMA 7.4.4 (Teorema de División de Weierstrass). *Si $\sigma \in K[[X_1, \ldots, X_n, Y]]$ es una serie distinguida de orden $b$, entonces, la aplicación :*

$$K[[X_1, \ldots, X_n, Y]] \cdot \sigma \oplus K[[X_1, \ldots, X_n]][Y]_{b-1} \longrightarrow K[[X_1, \ldots, X_n, Y]],$$

*dada mediante :*

$$(q \cdot \sigma, r) \longmapsto q \cdot \sigma + r,$$

*es un isomorfismo de $K[[X_1, \ldots, X_n]]-$módulos. En otras palabras, para toda serie de potencias formales $F \in K[[X_1, \ldots, X_n, Y]]$, existen series únicas $q \in K[[X_1, \ldots, X_n, Y]]$ y un polinomio distinguido de grado a lo sumo $b-1$ tales que*

$$F = q\sigma + r.$$

Los Corolarios más relevantes a este enunciado son, obviamente,

COROLLARIO 7.4.5. *El anillo de series de potencias formales $K[[X_1, \ldots, X_n]]$ es un dominio de factorización única, normal, local y noetheriano de dimensión $n$.*

## 7.5. Anillos Locales Regulares.

El concepto de anillo local regular fue introducido por W. Krull[13] en su trabajo de 1938, tratando de responder a una pregunta que él mismo había introducido en su texto de 1935[14].

DEFINICIÓN 61. *Diremos que un anillo local noetheriano $(A, \mathfrak{m})$ es un anillo local regular si su ideal maximal está generado por un sistema de parámetros. Esto es, si $dim(A) = d$ y existen $x_1, \ldots, x_d \in \mathfrak{m}$ tales que*

$$(x_1, \ldots, x_d) = \mathfrak{m}.$$

*A tales conjuntos se les denomina sistemas regulares de parámetros.*

Son anillos locales regulares los anillos de series de potencias formales o los localizados del anillo de polinomios con coeficientes en un cuerpo (cf. [**Ma, 80**], Capítulo 7, pp.126–127, por ejemplo).

TEOREMA 7.5.1. *Sea $(A, \mathfrak{m})$ un anillo local noetheriano de dimensión $d$. Son equivalentes :*

i) *$A$ es un anillo local regular,*
ii) *El anillo graduado $G_{\mathfrak{m}}(A)$ es un anillo de polinomios en $d$ variables con coeficientes en $A/\mathfrak{m}$,*
iii) *El $A/\mathfrak{m}-$espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ tiene dimensión $d$.*

La demostración, muy elemental, puede seguirse en [**Ra** *et al.*, **75**].

COROLLARIO 7.5.2. *Un anillo local noetheriano $(A, \mathfrak{m})$ es local regular si y solamente si su completado $A^*$ es local regular.*
*Además, dado que $G_{\mathfrak{m}}(A)$ es un anillo normal, todo anillo local regular es un anillo normal.*

PROPOSICIÓN 7.5.3. *Sea $(A, \mathfrak{m})$ un anillo local regular de dimensión $d$ y sean $a_1, \ldots, a_j$ una colección de $j$ elementos de $A$. Son equivalentes :*

i) *$\{a_1, \ldots, a_j\}$ es parte de un sistema regular de parámetros de $A$,*
ii) *Las clases $a_1 + \mathfrak{m}^2, \ldots, a_j + \mathfrak{m}^2$ son $A/\mathfrak{m}-$linealmenmte independientes en $\mathfrak{m}/\mathfrak{m}^2$,*
iii) *$A/(a_1, \ldots, a_j)$ es un anillo local regular de dimenjsión $d - j$.*

*En particular, para cada ideal primo $\mathfrak{p}$ de $A$, $A/\mathfrak{p}$ es local regular de dimensión $d - r$ si y solamente si $\mathfrak{p}$ está generado por $r$ elementos de $A$ que forman parte de un sistema regular de parámetros de $A$.*

### 7.5.1. Criterio del Jacobiano.

Seguiré básicamente la introducción de [**Shf, 74**], aunque no es inapropiada la presentada en [**Hrt, 77**].
Sea $V \subseteq \mathbb{K}^n$ un conjunto algebraico, $P \in V$ un punto, $f_1, \ldots, f_s$ un conjunto de generadores de $I(V)$ en $\mathbb{K}[X_1, \ldots, X_n]$.

DEFINICIÓN 62. *Una recta $\{P+tv \ : \ t \in \mathbb{K}\} \subseteq \mathbb{K}^n$ pasando por el punto $P$ se denomina tangente a $V$ en $P$, si se verifica que el siguiente polinomio univariado :*

$$f(T) := gdc(f_1(P + Tv), \ldots, f_s(P + Tv)) \in \mathbb{K}[T],$$

*tiene en $t = 0$ una raíz de multiplicidad mayor que 1.*

Sea $\mathfrak{m}_P$ el ideal maximal de $\mathbb{K}[X_1, \ldots, X_n]$ asociado al punto $P$. Sea $\mathbb{K}[X_1, \ldots, X_n]_P$ la localización de $\mathbb{K}[X_1, \ldots, X_n]$ en el maximal $\mathfrak{m}_P$ (que es un anillo local regular de dimensión $n$). Obsérvese que

$$\mathbb{K}[X_1 - \alpha_1, \ldots, X_n - \alpha_n] \cong G_{\mathfrak{m}_P}(\mathbb{K}[X_1, \ldots, X_n]),$$

[13] W. Krull. "Dimensionen in Stellensringen". *J. reine angew. Math.***179** (1938) 204–26
[14] W. Krull. *"Idealtheorie"*. Springer (1935)

donde $P = (\alpha_1, \ldots, \alpha_n)$. Para cada $G \in \mathbb{K}[X_1, \ldots, X_n]$ denotemos por $d_P(G)$ la diferencial de $G$ en $P$, ésto es, la componente homogénea de grado 1 de $G$ como elemento de $G_{\mathfrak{m}_P}(\mathbb{K}[X_1, \ldots, X_n])$.

LEMA 7.5.4. *Con las anteriores notaciones, una recta $\{P + tv \ : \ t \in \mathbb{K}\}$ es tangente a $V$ en $P$ si y solamente si $d_P(f_i)(v) = 0$, $1 \leq i \leq s$.*

Denotemos por $T_PV$ el espacio tangente a $V$ en $P$ y sea $D(f_1, \ldots, f_s)_P$ la matriz jacobiana en $P$ de un sistema generador de $I(V)$. Se tiene :

$$T_PV := \{v \in \mathbb{K}^n \ : \ D(f_1, \ldots, f_s)_P(v) = 0\}.$$

Más aún, sea $\overline{\mathfrak{m}}_P$ el ideal maximal de $\mathbb{K}[V]$ asociado al punto $P$ y consideremos

$$d_P \ : \overline{\mathfrak{m}}_P/\overline{\mathfrak{m}}_P^2 \longrightarrow (T_PV)^*.$$

la aplicación inducida por $d_P$. Entonces, se tiene :

PROPOSICIÓN 7.5.5. *La aplicación $d_P$ define un isomorfismo de $\mathbb{K}-$espacios vectoriales.*

DEFINICIÓN 63. *Con las anteriores notaciones, diremos que un punto $P \in V$ es un punto regular o un punto simple si y solamente si*

$$dim T_PV = dim(V).$$

*En caso contrario diremos que $P$ es un punto singular de $V$.*

Obsérvese que la condición $dim T_PV \geq dim V$ se satisface siempre.

TEOREMA 7.5.6 (Criterio del Jacobiano). *Sea $V \subseteq \mathbb{K}^n$ un conjuto algebraico, supongamos $I(V) = (f_1, \ldots, f_s)$ y sea $D(f_1, \ldots, f_s)$ la matriz jacobiana definida por un sistema generador de $I(V)$. Sea $P \in V$ un punto y $\overline{\mathfrak{m}}_P$ el maximal de $\mathbb{K}[V]$ asociado al punto $P$. Son equivalentes :*

i) *$P \in V$ es un punto simple,*
ii) *el anillo local noetheriano $\mathbb{K}[V]_{\overline{\mathfrak{m}}_P}$ es un anillo local regular de dimensión igual a la dimensión de $V$.*
iii) *el rango de la matriz jacobiana en $P$ es $n - dim(V)$, i.e.*

$$rang(D(f_1, \ldots, f_s)_P) = n - dim(V).$$

Observe el lector que la condición de ser simple es análoga a las hipótesis del Teorema de la Función Implícita en el que insistiremos más adelante. Por ahora, es conveniente señalar al alumno las implicaciones geométricas de esta propiedad.
En particular, conviene señalar que el conjunto de puntos singulares es un subconjunto algebraico propio de $V$ y que la condición de ser un punto liso es una condición genérica en $V$.

**7.5.2. Teorema de Estructura de Cohen.** De haber dispuesto de tiempo para poder diseñar un buen curso de Algebra Conmutativa, contando con una buena base de Algebra Homológica, habría desarrollado las demostraciones de los Teoremas de J.P. Serre[15] o el Teorema de M. Auslander y D.A. Buchsbaum[16]. Ambos resultados suponen respuestas a dos preguntas formuladas por W. Krull en 1938. Sin embargo, no es éste

[15] *Todo anillo local noetheriano es regular si y solamente si es de dimensión global finita y su dimensión global coincide con su dimensión de Krull.* Demostrado por J.P. Serre en "Sur la Dimension Homologique des Anneaux et des Modules Noetheriens". En *Proc. Int. Symp. Alg. Number Theory, Tokyo* (1956) 175–189.

[16] *Todo anillo local regular es un dominio de factorización única* en M. Auslander, S.A. Buchsbaum. "Unique Factorisation in Regular Local Rings". *Proc. Nat. Acad. Sci. US* **45** (195) 733–764. Este resultado es, sin embargo, consecuencia de las investigaciones de ambos en torno a la dimensión homológica de anillos en M. Auslander y D.A. Buchsbaum. "Homological Dimension in Local Rings". *Trans. AMS* **85** (1957) 390–405.

el propósito del curso por lo que nos conformaremos con el Teorema del alumno de O. Zariski I.S. Cohen[17].
El teorema de I.S. Cohen se lee del modo siguiente en [**ZaSa, 60**], según los propios autores, siguiendo una demostración debida a A. Geddes :

TEOREMA 7.5.7. *Si $A$ es un anillo local regular completo y equicaracterístico, entonces, $A$ contiene un cuerpo de representantes, ésto es, existe un subcuerpo $K$ de $A$ tal que $K$ es isomorfo a $A/\mathfrak{m}$.*

La conclusión de este Teorema se lee del modo siguiente :

COROLLARIO 7.5.8 (Teorema de Estructura de I.S. Cohen). *Todo anillo local regular equicaracterístico y completo es un anillo de series de potencias formales.*

En vista de los Teoremas de División y Preparación de Weierstrass, todo anillo local regular completo y equicaracterístico es un dominio de factorización única. Y, siguiendo el [**ZaSa, 60**], será cierto para todo anillo local regular equicaracterístico.

## 7.6. Teorema de la Función Implícita.

En esta Sección se demuestra la presentación clásico (la de [**ZaSa, 60**], por ejemplo) del Lema de Hensel. Así mismo se presenta el algoritmo de convergencia cuadrática para calcular buenas aproximaciones de las funciones implícitas a través del operador de Newton Multivariado.

**7.6.1. El Lema de Hensel.** Sea trata de una versión univariada del Teorema de la Función Implícita. K. Hensel desarrolló sus ideas a partir del método de K. Weierstrass de 1897 sobre la aproximación de series de potencias formales algebraicas. Así introdujo los números p–ádicos. Hoy asignamos a Hensel lo que, en buena medida, corresponde a ambos. Su incidencia en factorización de polinomios lo hace esencial. Podría darse como consecuencia de los resultados que expondremos más adelante (Sección 7.6.2) pero un cierto regusto clásico y la belleza del resultado hacen atractivo escribirlo aquí separadamente.
Hagamos notar que, con las convenientes hipótesis adicionales, el Lema de Hensel puede implicar (y de hecho implica) el Teorema de la Función Implícita multivariado.
La versión que hemos elegido es básicamente la prueba que aparece en el texto de O. Zariski y P. Samuel (cf. [**ZaSa, 60**]) el cual, con el paso de los años gana en valor ante mis ojos. Hay un bonito trabajo de P. Ribenboim[18] donde el lector podrá encontrar disquisiciones históricas y formulaciones equivalentes del mismo Lema de Hensel. Otras referencias que muestran la relevancia del resultado pueden ser el [**Bo, 67**], [**Nag, 75**] o [**Ray, 78**], aunque en estos casos la presentación es mucho más exquisita que la expuesta en estas páginas.
No es menos interesante la presentación hecha en [**PoZa, 89**] o [**Kob, 77**], este último para el caso $p-$ádico.

LEMA 7.6.1 (Lema Bilineal). *Sea $(A, \mathfrak{m})$ un anillo local noetheriano y completo para la topología $\mathfrak{m}-$ádica. Sean $E, E'$ y $F$ tres $A-$módulos finitamente generados. Supongamos que la topología $\mathfrak{m}-$ádica en todos ellos es Hausdorff. Sea $f : E \times E' \longrightarrow F$ una aplicación bilineal y sea :*

$$\overline{f} : E/\mathfrak{m}E \times E'/\mathfrak{m}E' \longrightarrow F/\mathfrak{m}F$$

*la aplicación bilineal obtenida tensorizando con $A/\mathfrak{m}$.*
*Sea $y \in F$, $\alpha \in E$ y $\alpha' \in E'$ tales que :*

[17] I.S. Cohen. "On the Structure and Ideal Theory of Complete Local Rings". *Trans. AMS* **59** (1946) 54–106.
[18] P. Ribenboim. "Equivalent forms of Hensel's Lemma". *Expo. Math.* **3** (1985) 3–24.

- $\overline{f}(\alpha + \mathfrak{m}E, \alpha' + \mathfrak{m}E') = y + \mathfrak{m}F \in F\mathfrak{m}F$.
- $\overline{f}(\alpha, E'/\mathfrak{m}E') + \overline{f}(E/\mathfrak{m}E, \alpha') = F/\mathfrak{m}F$.

*Entonces, existen* $a \in E$ *y* $a' \in E'$ *tales que :*

i) $a + \mathfrak{m}E = \alpha + \mathfrak{m}E$, $a' + \mathfrak{m}E' = \alpha' + \mathfrak{m}E'$.
ii) $f(a, a') = y$ *en* $F$.

Este Lema Bilineal se demuestra mediante un algoritmo iterativo de construcción de los elementos $a$ y $a'$. Se trata de un algoritmo de convergencia lineal que será mejorado más adelante. Con este Lema Bilineal, el Lema de Hensel resulta muy sencillo de probar. Para un anillo local $(A, \mathfrak{m})$ y un polinomio $f \in A[X]$ denotaremos por $\overline{f}$ el polinomio de $A/\mathfrak{m}[X]$ dado tomando clases módulo $\mathfrak{m}$ de los coeficientes de $f$.

LEMA 7.6.2 (Lema de Hensel). *Sea* $(A, \mathfrak{m})$ *un anillo local noetheriano y completo para la topología* $\mathfrak{m}-$*ádica. Sea* $f \in A[X]$ *un polinomio univariado de grado* $d$ *cuyo coeficiente director es una unidad en* $A$.
*Sean* $\alpha(X), \alpha'(X) \in A[X]$ *polinomios de grados respectivos* $r$ *y* $d - r$ *tales que :*

- $\overline{f} = \overline{\alpha}\overline{\alpha'}$ *en* $A/\mathfrak{m}[X]$,
- $m.c.d.(\overline{\alpha}, \overline{\alpha'}) = 1$ *en* $A/\mathfrak{m}[X]$.

*Entonces, exsiten polinomios* $a, a' \in A[X]$ *de grados respectivos* $r$ *y* $d - r$ *tales que :*

- $f = aa'$ *en* $A[X]$,
- $\overline{a} = \overline{\alpha}, \overline{a'} = \overline{\alpha'}$ *en* $A/\mathfrak{m}[X]$.

La formulación en términos de la función implícita es la clásica y la obvia; pero es preferible pasar ahora a la versión generalizada del operador de Newton.

**7.6.2. El Operador de Newton No–Arquimediano.** Consideraremos la siguiente situación :

- $(A, \mathfrak{m})$ es un anillo local noetheriano y completo, $\mathfrak{m}$ es su único ideal maximal.
- $\mid a \mid \in \mathbb{R}$ es la norma (valor absoluto) del elemento $a \in A$ para la topología definida por la filtración $\mathfrak{m}-$ádica en $A$.
- $\nu : A \longrightarrow \mathbb{N}$ es la valoración (función de orden) asociada a la filtración $\mathfrak{m}-$ádica. Recordemos que existe una constante $e \in \mathbb{R}$, $e > 1$ tal que :

$$\mid a \mid = \frac{1}{e^{\nu(a)}}$$

- $f_1, \ldots, f_n \in A[X_1, \ldots, X_n]$ una sucesión de polinomios.

Escribamos $F := (f_1, \ldots, f_n)$ y, por simplificar la notación $\underline{X} = (X_1, \ldots, X_n)$.
Para cada elemento $a \in A$ denotemos por $\overline{a} := a + \mathfrak{m} \in A/\mathfrak{m}$ la clase que define en el cuerpo cociente $A/\mathfrak{m}$. Observemos que las unidades de $A$ se caracterizan por la propiedad $\overline{a} \neq 0$. Para cada polinomio $f \in A[X_1, \ldots, X_n]$ denotaremos por $\overline{f}$ el polinomio en $A/\mathfrak{m}[X_1, \ldots, X_n]$ obtenido tomando clases módulo $\mathfrak{m}$ de los coeficientes de $f$.
Con la topología producto, $A^n$ es un espacio métrico completo. Denotaremos por $|| \, . \, ||$ la extensión a $A^n$ de la norma sobre $A$, usando la norma del máximo.
Consideremos la matriz jacobiana (en el módulo de matrices $n \times n$ con coeficientes en $A[X_1, \ldots, X_n]$) asociada a la sucesión $F$ de polinomios :

$$D(F)_{\underline{X}} := \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial X_1} & \cdots & \frac{\partial f_n}{\partial X_n} \end{pmatrix} \tag{7.6.1}$$

Supongamos que existe un punto $\underline{a} = (a_1, \ldots, a_n) \in A^n$ verificando las siguiente hipótesis (que permanecerán inalteradas a lo largo de todo lo que sigue) :

- $\overline{f_i(a_1,\ldots,a_n)} = \overline{f}_i(\overline{a_1},\ldots,\overline{a_n}) = 0$ en $A/\mathfrak{m}$, para $1 \leq i \leq n$.
- El determinante de la matriz jacobiana no se anula en $A/\mathfrak{m}$, es decir :

$$\overline{det\left((D(F))_{\underline{a}}\right)} \neq 0 \quad \text{en} \quad A/\mathfrak{m}$$

En particular, $det\left((D(F))_{\underline{a}}\right)$ es una unidad del anillo local noetheriano $(A,\mathfrak{m})$. (Insisto en esta idea porque la matriz $D(F)_{\underline{a}}$ es por tanto una matriz inversible en $\mathcal{M}_n(A)$). Más aún, para cualquier $\underline{\xi} := (\xi_1,\ldots,\xi_n) \in A^n$ si

$$\overline{\xi}_j = \overline{a}_j \ \ , 1 \leq j \leq n, \ \text{ en } \ A/\mathfrak{m}$$

la matrix $D(F)_{\overline{\underline{\xi}}}$ también es inversible como matriz en $\mathcal{M}_n(A)$.
Pasamos a definir el operador de Newton en $n$ variables :

$$N_F(X_1,\ldots,X_n) := \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - D(F)^{-1}_{\underline{X}} \begin{pmatrix} f_1(\underline{X}) \\ \vdots \\ f_n(\underline{X}) \end{pmatrix} \tag{7.6.2}$$

LEMA 7.6.3. *Sea $\underline{\xi} = (\xi_1,\ldots,\xi_n) \in A^n$ tal que :*

- *$min\{\nu\left(f_i(\underline{\xi})\right) \ : \ 1 \leq i \leq n\} \geq N$*
- *$\overline{\xi}_j = \overline{a}_j$ en $A/\mathfrak{m}$, para $1 \leq j \leq n$.*

*y consideremos el punto $\underline{\sigma} := (\sigma_1,\ldots,\sigma_n) \in A^n$ dado por*

$$\begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix} = N_F(\underline{\xi})$$

*Entonces,*

$$min\{\nu\left(f_i(\underline{\sigma})\right) \ : \ 1 \leq i \leq n\} \geq 2N$$

LEMA 7.6.4. *Sea $(A,\mathfrak{m})$ un anillo local noetheriano, $F \in A[X_1,\ldots,X_n]$ un polinomio homogéneo de grado $m$ y sean $(h_1,\ldots,h_n) \in A^n$ tales que $h_j \in \mathfrak{m}^N$. Entonces,*

$$F(h_1,\ldots,h_n) \in \mathfrak{m}^{mN}$$

LEMA 7.6.5. *En las hipótesis anteriores, sea $\underline{\xi} = (\xi_1,\ldots,\xi_n) \in A^n$ y supongamos $D(F)_{\underline{\xi}}$ inversible en $\mathcal{M}_n(A)$. Sea $\underline{\sigma} = (\sigma_1,\ldots,\sigma_n) \in A^n$. Entonces,*

$$min\{\nu(\xi_j - \sigma_j) \ : \ 1 \leq j \leq n\} = min\{\nu(f_j(\underline{\xi}) - f_j(\underline{\sigma})) \ : \ 1 \leq j \leq n\}$$

TEOREMA 7.6.6 (Newton). *En las hipótesis de esta subsección, existen $(\sigma_1,\ldots,\sigma_n) \in A^n$ tales que*

$$f_j(\sigma_1,\ldots,\sigma_n) = 0$$

*Además, definiendo recursivamente*

$$\begin{pmatrix} \sigma_1^{(1)} \\ \vdots \\ \sigma_n^{(1)} \end{pmatrix} = N_F(a_1,\ldots,a_n)$$

*y*

$$\begin{pmatrix} \sigma_1^{(k)} \\ \vdots \\ \sigma_n^{(k)} \end{pmatrix} = N_F(\sigma_1^{(k-1)},\cdots,\sigma_N^{(k-1)})$$

*se tiene*

$$\mid \sigma_j - \sigma_j^{(k)} \mid \leq \frac{1}{2^{2^k}}$$

Los ámbitos de aplicación más corrientes de este enunciado son los casos del completado de $\mathbb{Z}_{p\mathbb{Z}}$, donde $p$ es un número primo (i.e. los enteros $p-$ádicos) y el Teorema de la Función Implícita propiamente dicho. Obsérvese que de la existencia de solución en los respectivos cocientes es condición suficiente para la existencia de solución en el anillo y la convergencia cuadrática queda ya garantizada.
El mecanismo habitual de manipulación de las sucesivas iteraciones del operador de Newton, tal y como ha sido introducido en esta Sección, es a través de un esquema de evaluación con divisiones. Utilizando Vermediung von Divisionen (véase Subsección **??**) podremos evitar las divisiones en la forma siguiente :
Sea $R$ un anillo de polinomios sobre $K$, sea $\mathcal{K}$ su cuerpo de fracciones y sean $F := [f_1, \ldots, f_n] \in R[X_1, \ldots, X_n]^n$ polinomios de grado a lo más $d$. Supongamos que los polinomios $f_1, \ldots, f_n$ vienen dados por un esquema de evaluación sin divisiones $\beta$ de talla $L$ y profundidad no escalar $\ell$. Supongamos que la matriz jacobiana

$$D(F) := D(f_1, \ldots, f_n) := \left(\frac{\partial f_i}{\partial X_j}\right)_{1 \leq i,j \leq n}$$

asociada al sistema $F$ es regular. Consideramos el operador de Newton– Hensel definido por:

$$N_F(X_1, \ldots, X_n) := \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - D(F)^{-1} \begin{pmatrix} f_1(X_1, \ldots, X_n) \\ \vdots \\ f_n(X_1, \ldots, X_n) \end{pmatrix}. \tag{7.6.3}$$

Este operador define $n$ funciones racionales de $\mathcal{K}(X_1, \ldots, X_n)$ y lo mismo es válido para el resultado correspondiente a la iteración $k$ veces del mismo operados, $N_F^k \in \mathcal{K}(X_1, \ldots, X_n)^n$. Por lo tanto, para cualquier número natural, $k \in \mathbb{N}$, existen polinomios $g_1^{(k)}, \ldots, g_n^{(k)}$ y $h^{(k)} \in \mathcal{K}[X_1, \ldots, X_n]$ tales que

$$N_f^k = \left(\frac{g_1^{(k)}}{h^{(k)}}, \ldots, \frac{g_n^{(k)}}{h^{(k)}}\right) \in \mathcal{K}(X_1, \ldots, X_n)^n.$$

El lema que sigue muestra la existencia de un esquema de evaluación que calcula tales polinomios sin utilizar divisiones.

LEMA 7.6.7. *Consideremos las mismas notaciones e hipótesis que antes. Entonces, existe un esquema de evaluación en $R[X_1, \ldots, X_n]$ de talla $O(kd^2n^7L)$ y profundidad no escalar $O((log_2 n + \ell)k)$ que, utilizando los mismos parámetros que $\beta$, computa los numeradores $g_1^{(k)}, \ldots, g_n^{(k)}$ y un denominador (distinto de cero) $h^{(k)}$ para $N_F^k$.*

Capítulo 8

# Un Algoritmo de Resolución de Naturaleza Intrínseca

## 8.1. Introducción

A la vista de los resultados de Mayr y Meyer, expuestos en el Capítulo 3, es claro y notorio, para la Comunidad Científica de Algebra Computacional, que las bases de Gröbner no son la respuesta a los problemas de resolución de sistemas de ecuaciones polinomiales multivariadas. Una complejidad doblemente exponencial en el número de variables y un consumo de espacio expo–polinomial suponen que los algoritmos de bases de Gröbner no van a funcionar tal cual en la práctica. Algunas reducciones fueron propuestas por D. Lazard[1] y sus continuadores. Estos resultados venían a significar que, obviamente, las bases de Gröbner no eran la respuesta a numerosos problemas con dimensión positiva del conjunto de soluciones; pero, eventualmente, se podría hacer un esfuerzo notable en algunos casos particulares. Así, por ejemplo, en el caso de dimensión cero afín, se podría bajar la complejidad secuencial hasta una complejidad del orden $d^{O(n^2)}$ (rebajada recientemente hasta $(nd)^{O(n)}$), con un consumo de espacio del mismo orden.

De otro lado, algunos de los investigadores que más alegremente se habían lanzado a trabajar con bases de Gröbner (la lista de nombres es larga) se fueron dando cuenta de que sus investigaciones precedentes corrían el riesgo de desaparecer. También se dieron cuenta, y ésto es inevitable, de que debían mantener la llama de las investigaciones en ese campo. Por dar una visión positiva del asunto, supongamos que han creído siempre que sus investigaciones sobre bases de Gröbner podían llegar a romper la barrera. Sea cual sea la razón, se hizo caso omiso a los comentarios de los especialistas en Complejidad y se continuó con la práctica y la implementación de las bases de Gröbner (entre otras cosas, porque son fáciles de implementar para un programador no muy experto en Matemáticas).

Unos pocos investigadores se desmarcaron de esta línea de investigación y se iniciaron trabajos sobre propuestas alternativas. Una de ellas, la que ha alcanzado los límites más furctíferos del asunto, es la que se trata de exponer en este Capítulo.

Las primeras modificaciones de los algoritmos de Eliminación, se basaban en abandonar toda suerte de esfuerzos sobre las bases monomiales y las bases de Gröbner. Comenzaron con los estudios de complejidad del Nullstellensatz Efectivo que, al menos, podían resolver el problema de Consistencia de sistemas de Ecuaciones Polinomiales Multivaridas. Los estudios sobre el Nullstellensatz Efectivo de finales de los años 80 y su evolución hasta la actualidad se han discutido en la Subsección 2.4.3.2. Estos resultados suponían un avance significativo con respecto a las bases de Gröbner. La complejidad en tiempo era del tipo $d^{O(n^2)}$ independientemente de la dimensión; pero el espacio se habría reducido a polinomial.

A principios de los años 90 surge un nuevo avance significativo. Renunciando a las bases monomiales y utilizando técnicas de deformación homotópica brutales (en el caso $0-$dimensional proyectivo) la colaboración de M. Giusti, J. Heintz y L.M. Pardo[2] y el trabajo [**KrPa, 96**] introdujeron una nueva filosofía para la resolución de ecuaciones

[1] D. Lazard. "Résolution des systèmes d'équations algébriques", *Theor. Comp. Sci.* **15** (1981) 77–110.

[2] Véanse los trabajos

polinomiales multivariadas. A partir de entonces, los polinomios multivariados se codificarían mediante esquemas de evaluación. Esto suponía unas ciertas dificultades e incovenientes. La primera de la dificultades era demostrar que, efectivamente, los polinomios que surgen en la resolución de sistemas de ecuaciones polinomiales multivariadas tienen grado alto ($d^{O(n)}$) pero se pueden codificar mediante un esquema de evaluación de tamaño similar al grado. Una vez observada (y demostrada) tal cosa, había que desarrollar todo un concepto nuevo de algorítmo en el que objetos del estilo de la división de Hironaka eran reemplazados por técnicas menos simples y más ingeniosas. *Un considerable esfuerzo se hizo para demostrar, en el trabajo* [**KrPa, 96**], *un Teorema crucial que asevera que se pueden resolver ecuaciones polinomiales multivariadas en tiempo* $d^{O(n)}$ *y espacio polinomial*. También en ese trabajo se demuestra que se puede resolver el problema de Consistencia, construir las identidades del Nullstellensazt Efectivo y, adicionalmente, demostrar cotas hiper–finas sobre el Nullstellensatz Aritmético del mismo orden de grandeza. Esto supuso un cambio cuantitativo y cualitativo de profundidad y, al mismo tiempo, suponía una nueva frontera no siempre bien recibida por quienes, como antes indiqué deseaban permanecer en el inamovible mundo de las bases de Gröbner.

Sin embargo, estos algoritmos no eran suficientemente buenos. Tenían varios defectos conceptuales (excesiva dependencia de parámetros extrínsecos al problema (sintácticos)) y, sobre todo, eran generalistas e inacapaces de adaptarse a las particularidades especiales del sistema concreto dado. A partir de mi conferencia plenaria en AAECC–11 ([**Pa, 95**]) y del trabajo [**Pa** *et al.*, **1995a**] se cambia completamente el perfil de la algorítmica simbólica para la resolución de sistemas de ecuaciones polinomiales multivariadas. Se introduce, por vez primera, un número de condicionamiento del Algebra Computacional y la Geometría Algebraica Efectiva y se exhibe, tras varios avances técnicos que culminaron en el trabajo [**Pa** *et al.*, **1997b**], un algoritmo simbólico cuyo tiempo depende polinomialmente de un parámetro intrínseco (el *Grado Geométrico del Sistema*) tanto en dimensión cero como en dimensión positiva (al menos para variedades equidimensionales). El algoritmo fue programado y ha demostrado su eficacia, incluso en versiones muy primitivas, de modo experimental. Lo que se propone en este Capítulo es ofrecer una versión "light" y un tanto naïve de este algoritmo.

Debe señalarse que este algoritmo es el mejor algoritmo posible (como se ha demostrado en mis trabajos[3]) y que deben explorarse alternativas con la esperanza de encontrar un mejor comportamiento en promedio.

El Capítulo comienza con la Sección 8.2 dedicada a informar a los alumnos de la existencia del Teorema de Quillen–Suslin. Desgraciadamente, como ya ocurriera en el Capítulo precedente con los Teoremas de Auslander–Buchsbaum y Serre, no es posible impartir una demostración completa de este enunciado (ni siquiera a la manera de [**Ku, 85**]) en un curso tan limitado como éste. Es, sin embargo, conveniente que los alumnos sepan

---

- Luis M. Pardo (con N. Fitchas, M. Giusti, F. Smietanski),*Sur la complexité du théorème des zéros*. In *Approximation and Optimization in the Caribbean II, Proceedings of the Second International Conference on Approximation and Optimization*, La Habana, 1993, M. Florenzano et al., eds., Approximation and Optimization, Peter Lang Verlag, Frankfurt, 1995, 274–329.
- M. Giusti, J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, In *Proc. Computational Algebraic Geometry and Commutative Algebra, Cortona, Symposia Matematica* **XXXIV**, 1993, 216–256.

[3]Véanse los trabajos :

- Luis M. Pardo, *Universal Elimination requires Exponential running Time (Extended Abstract)*. In Actas *EACA'2000*, Barcelona, A. Montes, ed., 2000 25–51.
- Luis M. Pardo (con D. Castro, M. Giusti, J. Heintz, G. Matera), *The Hardness of Polynomial Equation Solving*. Found. of Computational Mathematics **3** (2003), 347-420.

de su existencia y de las consecuencias sobre la existencia de bases para módulos libres dados a través de normalizaciones de Noether de anillos de Cohen–Macaulay. Esto genera un concepto de solución (a la Macaulay) que es ineficiente pero ya apunta maneras interesantes. Así, en las Secciones 8.3, 8.4 y 8.5 se establecen algunos ingredientes fundamentales como el concepto de Polinomio Eliminante módulo un ideal intersección completa, sus propiedades básicas y su manejo algorítmico eficiente. Estamos ya en concidiones de dar el salto a la Sección 8.6 en la que se define un segundo concepto de solución basado en la descrición de una variedad equi–dimensional a través de un isomorfismo birracional que usa una Normalización de Noether. Se estudian los algoritmos básicos de manipulación de dicho concepto y se insiste en la forma de Cayley–Chow con respecto a una normalización de Noether en la Sección **??** como segundo concepto de solución, estableciendo los algoritmos eficientes que relacionan ambos conceptos. Finalmente, en la Sección 8.8 se introduce un Cuarto y último concepto de solución que, a través del operador de Newton descrito en el Capítulo 7, se muestra como equivalente algorítmicamente a los anteriores. Debe señalarse que todos estos algoritmos de equivalencia usan fuertemente los algoritmos de base descritos en el Capítulo **??** anterior. La Sección 8.9 muestra cuáles son los algoritmos básicos para proceder a eliminar una nueva ecuación de manera eficaz y cómo hallar los ingredientes nuevos de un nuevo ideal (se trata del paso de iteración del algoritmo). Finalmente, la Sección 8.10 está dedicada a establacer el algoritmo propuesto así como su complejidad. Debe señalarse que se trata de un algoritmo de deformación homotópica (al estilo del del análisis numérico) y que su complejidad es óptima e inevitable en tanto que algoritmo universal.

## 8.2. El concepto de Solución a partir del Teorema de Quillen–Suslin.

A partir de ahora supondremos que el cuerpo $K$ es un cuerpo de característica cero[4]. Un elemento relevante en la construcción del Algoritmo es la respuesta de D. Quillen[5] y A. Suslin[6] a una Conjetura de J.P. Serre[7]. El enunciado principal se interpreta en los términos siguientes :

TEOREMA 8.2.1 (Quillen–Suslin). *Sea $A$ un dominio de ideales principales. Todo módulo proyectivo sobre el anillo de polinomios $A[X_1, \ldots, X_n]$ es un módulo libre.*

Una presentación didáctica de este resultado puede seguirse en el texto [**Ku, 85**]. El resultado podría ser el objetivo de un buen curso de "Algebra Conmutativa", pero la incultura es madre del atrevimiento y de la limitación intelectual propia de tiempos en los que conocer se diferencia de saber por ser esta última sinónimo impocible de saber hacer que es la demostración palpable del fin del pensamiento humano. Se trata del siguiente enunciado equivalente :

COROLLARIO 8.2.2. *Sea $K$ un cuerpo. Todo $K[X_1, \ldots, X_n]-$módulo localmente libre es libre.*

El ejemplo más relevante de $K[X_1, \ldots, X_n]-$módulo libre que voy a considerar en estas páginas requiere es el caso de un anillo de restos módulo un ideal intersección completa. De nuevo, voy a incluir solamente un poco de terminología y algunos enunciados esenciales, conformándome con ellos para el propósito de este curso. La siguiente definición es la extensión de un relevante resultado obtenido por F.S. Macaulay [8] sobre los ideales

[4]Aunque los resultados y técnicas son aplicables a cualquier cuerpo perfecto con suficientes elementos.

[5]D. Quillen. "Projective Modules over polynomial Rings". *Invetn. Math.* **36** (1976) 436–437.

[6]A. Sulin. "Projective Modules over Polynomial Rings". *Dokl. Akad. Nauk. S.S.S.R.* **26** (1976) (en ruso).

[7]J.P. Serre. "Sur les Modules Projectifs".Sém. Dubreil–Pisot 1960/61.

[8]F.S. Macaulay. *The Algebraic Theory of Modular Systems"*. Cambridge tracts in math. and Math. Physics, Cambridge University Press (1916). A

intersección completa en anillos de polinomios. Dicho resultado fue extendido al caso de anillos locales regulares por el alumno de O. Zariski I.S. Cohen[9] en su trabajo de 1946. Una buena descripción de las ideas puede seguirse en la Sección 17 de [**Ma, 89**].

DEFINICIÓN 64. *Un anillo Noetheriano $R$ se dice Cohen–Macaulay si verifica la condición de la pureza, es decir, si todo ideal de altura $r$ de $R$ generado por $r$ elementos no posee primos asociados inmersos.*

El resultado de Macaulay se puede reller en los términos siguientes :

TEOREMA 8.2.3 (Macaulay, 1916). *Si $A$ es un anillo de Cohen–Macaulay, también lo es $A[X_1, \ldots, X_n]$.*

Un resultado clarificador sobre la naturaleza de los ejemplos de anillos de Cohen–Macaulay que necesitamos es el siguiente enunciado que se puede encontrar en el trabajo de I. Armendariz y P. Solernó[10] de 1995.

LEMA 8.2.4. *Sea $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ un ideal sin primos inmersos de altura $n - r$. Sea*

$$K[Y_1, \ldots, Y_r] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a},$$

*una normalización de Noether. Son equivalentes :*

i) *el anillo $K[X_1, \ldots, X_n]/\mathfrak{a}$ es Cohen–Macaulay.*
ii) *el $K[Y_1, \ldots, Y_n]-$módulo $K[X_1, \ldots, X_n]/\mathfrak{a}$ es localmente libre y, por ende, libre como consecuencia del Teorema de Quillen–Suslin.*

Este resultado se complementa con el siguiente enunciado que, con un argumento inductivo, puede seguirse en el trabajo de M. Giusti, J. Heintz y J. Sabia[11] de 1993.

PROPOSICIÓN 8.2.5. *Sea $\mathfrak{a} = (f_1, \ldots, f_s)$ un ideal tal que $V(\mathfrak{a})$ es una variedad equidimensional de dimensión $n - s$. Sea*

$$K[Y_1, \ldots, Y_{n-s}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a},$$

*una normalización de Noether. Entonces, $K[X_1, \ldots, X_n]/\mathfrak{a}$ es un $K[Y_1, \ldots, Y_{n-s}]-$módulo localmente libre.*

A partir de estos resultados podemos introducir la noción de solución en el caso intersección completa, en los términos siguientes :

DEFINICIÓN 65 (**Solución en el Caso Intersección Completa**). *Sea dada una sucesión secante de ecuaciones polinomiales $F := [f_1, \ldots, f_r] \in K[X_1, \ldots, X_n]^r$ (ésto es, la variedad $V(F) \subseteq \mathbb{K}^n$ es una variedad algebraica de dimensión $n - r$). Sea $\mathfrak{a}$ el ideal generado por $F$. Llamaremos solución del sistema de ecuaciones polinomiales definido por $F$ a la información siguiente :*

i) *Una normalización de Noether de $K[X_1, \ldots, X_n]/\mathfrak{a}$, ésto es, elementos $Y_1, \ldots, Y_{n-r}$ tales que la siguiente es una extensión entera de anillos :*

$$K[Y_1, \ldots, Y_{n-r}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a}.$$

ii) *Una base $\beta$ de $K[X_1, \ldots, X_n]/\mathfrak{a}$ como $K[Y_1, \ldots, Y_{n-r}]-$mólulo libre.*
iii) *Las matrices en la base $\beta$ de los tensores de multiplicación $M_{X_1}, \ldots, M_{X_n}$.*

---

[9] I.S. Cohen. "On the Structure and Ideal Theory of Complete Local Rings". *Trans. AMS* **59** (1946) 54–106.

[10] I. Armendáriz and P. Solernó. "On the computation of the radical of polynomial complete intersection ideals". In *Applied Algebra, Algebraic Algorithms and Error Corecting Codes, Proc. AAECC-11. LNCS* **948** (1995) 106–119.

[11] M. Giusti and J. Heintz and J. Sabia. "On the Efficiency of effective Nullstellensätze". *Comput. Complexity* **3** (1993) 56–95.

Este concepto de solución es un concepto muy adecuado que permitiría reconstruir sistemáticamente muchas de las reflexiones hechas en el Capítulo 3 sobre los conceptos de solución y eliminación. Sin embargo, este concepto se enfrenta a una drástica dificultad (muy difícil de soslayar) : no se conoce ningún algoritmo eficiente para calcular bases de módulos libres, ni siquiera en el caso intersección completa. Los resultados más avanzados han sido obtenidos sólo recientemente por P. Solernó y sus colaboradores (véase la tesis de I. Almeida[12] del año 2001). Los mejores algoritmos conocidos para el caso intersección completa remontan a una complejidad del orden $d^{n^4}$, donde $d$ es el máximo de los grados de los polinomios en $F$ y $n$ es el número de variables. En la Sección siguiente veremos cómo evitar esta dificultad, mejorando sustancialmente las cotas de complejidad conocidas, aunque renunciando al cálculo de la base como módulo libre.

## 8.3. El Caso Intersección Completa Reducida.

Comenzaremos con algunas reflexiones menores sobre el caso intersección completa reducida. Para empezar sea $\mathfrak{a}$ un ideal de $K[X_1, \ldots, X_n]$. Diremos que *las variables* $X_1, \ldots, X_n$ *están en posición de Noether con respecto al ideal* $\mathfrak{a}$ si $ht(\mathfrak{a}) = r$ y la siguiente es una extensión entera de anillos :

$$K[X_1, \ldots, X_{n-r}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a}.$$

El siguiente Lema nos da un instrumento de gran utilidad para caracterizar ideales radicales :

LEMA 8.3.1. *Sea* $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ *un ideal no mezclado (i.e. todos sus primos asociados tienen la misma altura). Entonces,* $\mathfrak{a}$ *es radical si, y sólo si, para todo idel primo minimal* $\mathfrak{p}$ *de* $\mathfrak{a}$ *se tiene*

$$\mathfrak{a} \cdot K[X_1, \ldots, X_n]_{\mathfrak{p}} = \mathfrak{p} \cdot K[X_1, \ldots, X_n]_{\mathfrak{p}}.$$

Combinando este Lema con el uso del Criterio del Jacobiano (expuesto en la Subsección 7.5.1) y el Teorema de la Pureza de Macaulay, nos permite concluir la siguiente caracterización de los ideales radicales

PROPOSICIÓN 8.3.2. *Sea* $f_1, \ldots, f_s$ *una sucesión regular de polinomios en* $K[X_1, \ldots, X_n]$. *Supongamos que las variables están en posición de Noether con respecto al ideal* $\mathfrak{a} := (f_1, \ldots, f_s)$, *es decir, la extensión de anillos*

$$A = K[X_1, \ldots, X_{n-s}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a} = B,$$

*es entera. Sea* $D(F)$ *la matriz jacobiana dada por*

$$D(F) = \left(\frac{\partial f_i}{\partial X_j}\right)_{1 \leq i \leq s \,,\, n-s+1 \leq j \leq n}$$

*y sea* $J(F) \in K[X_1, \ldots, X_n]$ *su determinante. Entonces, el ideal* $\mathfrak{a}$ *es radical si, y sólo si,* $J(F)$ *es no divisor de cero en* $B$.

Dado que el rango de los módulos libres se conserva por localización y haciendo buen uso del Lema de Nakayama combinado con el Teorema de los Ceros de Hilbert, podemos concluir el siguiente resultado :

PROPOSICIÓN 8.3.3. *Sea* $F := [f_1, \ldots, f_s] \in K[X_1, \ldots, X_n]^s$ *una sucesión de polinomios tales que el ideal* $\mathfrak{a}$ *que generan es un ideal de altura* $s$. *Supongamos que* $\mathfrak{a}$ *es un ideal radical y sea* $V(F) \subseteq \mathbb{K}^n$ *el conjunto de soluciones comunes a los polinomios en* $F$. *Supongamos que las variables* $X_1, \ldots, X_n$ *están en posición de Noether con respecto*

[12] I. Almeida. *" Aspectos Algorítmicos para el Cálculo de Bases de Módulos sobre Anillos de Polinomios"*. Tesis, Universidad de Buenos Aires (2001), dirigida por P. Solernó.

*a la variedad $V(F)$. Esto es, supongamos que la siguiente es una extensión entera de anillos :*

$$A = K[X_1, \ldots, X_{n-s}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a} = B.$$

*Entonces,*

i) *$B$ es un $A-$módulo libre de rango acotado por $deg(V(F))$.*

ii) *Sea $P := (p_1, \ldots, p_{n-s}) \in \mathbb{K}^{n-s}$. Sea $V_P(F) \subseteq \mathbb{K}^n$ la fibra definida mediante :*

$$V_P(F) := \{x \in V(F) \ : \ x_i = p_i, \ 1 \leq i \leq n-r\}.$$

*Sea $B(P)$ la $\mathbb{K}-$álgebra $0-$dimensional definida mediante :*

$$B(P) := \mathbb{K}[V_P(F)].$$

*Para genéricamente muchos (i.e. salvo un conjunto algebraico) $P \in \mathbb{K}^{n-s}$ se verifica la siguiente igualdad :*

$$deg(V_P(F)) = rank_A B = dim_{\mathbb{K}} B(P).$$

*Los puntos $P \in \mathbb{K}^{n-s}$ tales que se verifica la igualdad ii) anterior se denominan puntos no ramificados con respecto a la normalización de Noether elegida.*

## 8.4. Polinomio Eliminante.

En esta Sección vamos a fijar el concepto de Polinomio Eliminante que nos conducirá a una primera alternativa a la noción de solución planteada por el Teorema de Quillen–Suslin (véase la Sección 8.2 anterior). Supondremos las siguientes hipótesis :

i) $F := [f_1, \ldots, f_s]$ es una sucesión de polinomios en $K[X_1, \ldots, X_n]$ que definen un ideal intersección completa reducida $\mathfrak{a}(F) \subseteq K[X_1, \ldots, X_n]$. Es decir, el ideal $\mathfrak{a}(F)$ es un ideal radical y todos sus primos asociados son minimales y de altura $s$. Así mismo, definen un conjunto algebraico equidimensional $V(F) \subseteq \mathbb{K}^n$.

ii) Las variables están en posición de Noether con respecto a la variedad $V(F)$, ésto es, la siguiente es una extensión entera de anillos :

$$A = K[X_1, \ldots, X_{n-r}] \hookrightarrow B = K[X_1, \ldots, X_n]/\mathfrak{a}(F).$$

Por lo expuesto en Secciones anteriores, $B$ es un $A-$módulo libre y el rango de $B$ como $A-$módulo libre está acotado por el grado geométrico de $V(F)$, ésto es,

$$rank_A B \leq deg(V(F)).$$

A partir de aquí, sea $C$ el cuerpo de fracciones de $A$ y sea $B' := C \otimes_A B$ la localización de $B$ por el cuerpo de fracciones de $A$. Se tiene :

Proposición 8.4.1. *Con las anteriores notaciones, $B' := C \otimes_A B$ es una $C-$álgebra cero–dimensional y la dimensión de $B'$ como $C-$espacio vectorial coincide con el rango de $B$ como $A-$módulo libre. Esto es,*

$$dim_C C \otimes_A B = rank_A B \leq deg(V(F)).$$

Sea $g \in K[X_1, \ldots, X_n]$ un polinomio adicional y consideremos la homotecia definida por $g$

$$\eta_g \ : B \longrightarrow B,$$

dada mediante :

$$\eta_g(h) := \overline{gh}.$$

También podemos considerar la extensión de escalares de esta homotecia :

$$Id_C \otimes_A \eta_g \ : C \otimes_A B \longrightarrow C \otimes_A B,$$

definida del mismo modo. Se tiene :

PROPOSICIÓN 8.4.2. *Toda matriz de $\eta_g$ sobre una base cualquiera de $B$ como $A-$módulo libre y toda matriz de $Id_C \otimes \eta_g$ sobre una base de $B'$ como $C-$espacio vectorial son matrices semejantes. En particular, son diagonalizables y tienen el mismo polinomio mínimo y característico. Tanto el polinomio mínimo como el característico de $\eta_g$ son polinomios mónicos en el monoide $K[X_1,\ldots,X_{n-r}][T]_{mon}$.*

A partir de ahora, usaré la notación $\eta_g$ para denotar indistintamente a $\eta_g$ o a su extensión $Id_C \otimes_A \eta_g$, señalando, en los casos en que sea necesario, a cuál de los dos endomorfismos me refiero.
A partir del polinomio $g$ podemos considerar el morfismo regular :

$$G\ : V(F) \subseteq \mathbb{K}^n \longrightarrow \mathbb{K}^{n-s+1},$$

dado mediante :

$$G(x_1,\ldots,x_n) := (x_1,\ldots,x_{n-r}, g(x_1,\ldots,x_n)).$$

PROPOSICIÓN 8.4.3. *La imagen del morfismo $G$ anterior es una hipersuperficie $H_g$ de $\mathbb{K}^{n-s+1}$. Además, el polinomio mínimo de esa hipersuperficie coincide con el polinomio mínimo del endomorfismo $\eta_g$. A dicho polinomio mínimo, que denotaremos por $m_g$ se le denominará Polinomio Eliminante de $g$ con respecto a la variedad $V(F)$ y a la Normalización de Noether Fijada.*

El siguiente enunciado establece algunas propiedades adicionales del polinomio eliminante :

TEOREMA 8.4.4 (Polinomio Eliminante). *Con las anteriores notaciones, se tiene :*

i) *Por la Desigualdad de Bézout vista en la Sección 4.3, se tiene :*

$$deg(G(V(F)) = deg(m_g) \leq deg(V(F))deg(g).$$

ii) *El polinomio $g$ es un divisor de cero en $B$ si y solamente si el término independiente de $m_g$ con respecto a $T$ (i.e. el polinomio $a_0 := m_g(X_1,\ldots,X_{n-s},0) \in K[X_1,\ldots,X_{n-s}]$) es nulo.*

iii) *La intersección $V(F)\cap V(g) \subseteq \mathbb{K}^n$ verifica una y sólo una de las propiedades siguientes :*
   a) *$V(F)\cap V(g) \subseteq \mathbb{K}^n$ es una variedad de dimensión $n-s$ (o, equivalentemente, el término independiente de $m_g$ con respecto a $T$ es nulo o, también de modo equivalente, $g$ es un divisor de cero en $g$)*
   b) *$V(F)\cap V(g) \subseteq \mathbb{K}^n$ es una variedad de dimensión $n-s-1$ (o, equivalentemente, el término independiente de $m_g$ con respecto a $T$ es un polinomio en $K[X_1,\ldots,X_{n-s}]\setminus K$ no nulo y no constante).*
   c) *$V(F)\cap V(g) \subseteq \mathbb{K}^n$ es vacío (o, equivalentemente, el término independiente de $m_g$ es una constante no nula).*

Las siguientes dos Proposiciones son consecuencia (más o menos directa) de los Teoremas de Bertini expuestos por J.P. Jouanolou en su texto [**Jou, 83**].

PROPOSICIÓN 8.4.5. *Sean $f_1,\ldots,f_s$ polinomios en $K[X_1,\ldots,X_n]$ que generan el ideal trivial. Sea $g_1,\ldots,g_t$ $(t<n)$ una sucesión regular $K[X_1,\ldots,X_n]$ tal que el ideal $\mathfrak{a} = (g_1,\ldots,g_t)$ es radical en $K[X_1,\ldots,X_n]$. Sean $T_1,\ldots,T_s$ nuevas variables y sea $g$ el polinomio*

$$g = T_1f_1 + \cdots + T_sf_s.$$

*Si $F := K(T_1,\ldots,T_s)$, se tiene*

- *$g$ no es divisor de cero en $F[X_1,\ldots,X_n]/(g_1,\ldots,g_t)$,*
- *y*
  - *o bien $(g_1,\ldots,g_t,g)$ es el ideal trivial de $F[X_1,\ldots,X_n]$,*

- *o bien* $(g_1, \ldots, g_t, g)$ *es un ideal radical* $F[X_1, \ldots, X_n]/(g_1, \ldots, g_t)$.

De manera análoga se tiene :

PROPOSICIÓN 8.4.6. *Sean* $f_1, \ldots, f_s$ *polinomios en* $K[X_1, \ldots, X_n]$ *tales que el ideal* $\mathfrak{a}$ *que generan es un ideal de altura* $s$. *Sean* $g_1, \ldots, g_t$ $(t < s-2)$ *una sucesión regular* $K[X_1, \ldots, X_n]$ *tal que el ideal* $\mathfrak{b} = (g_1, \ldots, g_t)$ *es radical en* $K[X_1, \ldots, X_n]$. *Supongamos que los polinomios* $g_1, \ldots, g_t$ *han sido obtenidos como combinaciones lineales de los polinomios* $f_1, \ldots, f_s$. *Sean* $T_1, \ldots, T_s$ *nuevas variables y sea* $g$ *el polinomio*

$$g = T_1 f_1 + \cdots + T_s f_s.$$

*Si* $F := K(T_1, \ldots, T_s)$, *se tiene*

- $g$ *no es divisor de cero en* $F[X_1, \ldots, X_n]/(g_1, \ldots, g_t)$,
- *y* $(g_1, \ldots, g_t, g)$ *es un ideal radical en* $F[X_1, \ldots, X_n]/(g_1, \ldots, g_t)$.

## 8.5. Unos Pocos Algoritmos Instrumentales.

El anterior Teorema 8.4.4 indica que algunas preguntas importantes se pueden responder a partir del conocimiento del polinomio mínimo $m_g$ antes descrito. En esta Sección fijaré los conceptos de tales algoritmos instrumentales. Supondré que se tienen las siguientes hipótesis (que, por otra parte, son las mismas que he supuesto en la Sección previa) :
*Sea* $F := [f_1, \ldots, f_s] \in K[X_1, \ldots, X_n]^s$ *una sucesión de polinomios tales que el ideal* $\mathfrak{a}$ *que generan es un ideal de altura* $s$. *Supongamos que* $\mathfrak{a}$ *es un ideal radical y sea* $V(F) \subseteq \mathbb{K}^n$ *el conjunto de soluciones comunes a los polinomios en* $F$. *Supongamos que las variables* $X_1, \ldots, X_n$ *están en posición de Noether con respecto a la variedad* $V(F)$. *Esto es, supongamos que la siguiente es una extensión entera de anillos :*

$$A = K[X_1, \ldots, X_{n-s}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a} = B.$$

Se usarán masivamente los Tests Probabilistas descritos en la Sección 2.3 del Capítulo **??**

**8.5.1. Un Algoritmo para la Normalización de Noether Iterada.** Supongamos que disponemos de la siguiente información :
INPUT :

- La lista de polinomios $F$, verificando las anteriores hipótesis.
- Un polinomio adicional $g \in K[X_1, \ldots, X_n]$ del cual conocemos un esquema de evaluación bien paralelizable que evalúa el polinomio $m_g$. Supongamos que $V(F) \cap V(g)$ es no vacío.

Queremos decidir esencialmente dos cosas :
OUTPUT :

- Una respuesta "NEGATIVO" si $g$ es divisor de cero en $B$,
- Una matriz $A \in GL(n, K) \subset \mathcal{M}_n(K)$ regular tal que las variables obtenidas por el cambio lineal de coordenadas :

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = A \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

verifican que la siguiente es una extensión entera de anillos :

$$K[Y_1, \ldots, Y_{n-s-1}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a} + (g).$$

LEMA 8.5.1. *Sea* $a_0 := m_g(X_1, \ldots, X_{n-s}, 0) \in K[X_1, \ldots, X_{n-s}]$ *el término independiente de* $m_g$ *con respecto a* $T$. *Con las anteriores notaciones, sea* $B \in \mathcal{M}_{n-s}(K)$ *una matriz regular tal que el cambio de coordenadas*

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_{n-s} \end{pmatrix} = A \begin{pmatrix} X_1 \\ \vdots \\ X_{n-s} \end{pmatrix}$$

*hace de* $a_0$ *un polinomio mónico con respecto a* $Y_{n-s}$. *Entonces, la matriz* $A$ *dada mediante :*

$$A := \begin{pmatrix} B & 0 \\ 0 & Id_s \end{pmatrix},$$

*responde a los requerimientos del algoritmo anterior.*

El cálculo de la matriz $B$ como una matriz triangular a partir de un punto $(\lambda_1, \ldots, \lambda_{n-s-1}, 1)$ que no anula la componente homogénea de mayor grado de $a_0$ es un argumento clásico de demostración del Lema de Normalización de Noether.
Para el cálculo de un esquema de evaluación que evalúe la componente homogénea de mayor grado de $a_0$, baste observar que se trata del algoritmo subyacente a la prueba del Vermeidung von Divisionen (cf. [**St, 73**]).
Finalmente, todo se reduce a aplicar Tests de Nulidad probabilísticos al estilo de los presentados en la Sección 2.3.

**8.5.2. Un Algoritmo para el Problema de Consistencia.** Supongamos que disponemos de la siguiente información :
INPUT :

- La lista de polinomios $F$, verificando las anteriores hipótesis.
- Un polinomio adicional $g \in K[X_1, \ldots, X_n]$ del cual conocemos un esquema de evaluación bien paralelizable que evalúa el polinomio $m_g$. Supongamos que $V(F) \cap V(g)$ es no vacío.

Queremos decidir esencialmente dos cosas :
OUTPUT :

- Una respuesta "NEGATIVO" si $g$ es divisor de cero en $B$,
- Una respuesta "VACÍO", si $V(F) \cap V(g) = \emptyset$,
- Una respuesta "CAE LA DIMENSIÓN en UNO" si estamos en las condiciones de la Subsección anterior.

El algoritmo trivialmente se reduce a testar si $a_0 := m_g(X_1, \ldots, X_{n-s}, 0) \in K[X_1, \ldots, X_{n-s}]$ es una constante o no y, si es una constante, decidir si es la constante nula o no. Por tanto, se usan dos veces los Tests de Nulidad descritos en la Sección 2.3 :

i) Primero testamos si $a_0$ es un polinomio nulo o no.
ii) Después testamos si es nulo el polinomio $A_0 \in K[X_1, \ldots, X_{n-s}, Y_1, \ldots, Y_{n-s}]$ dado mediante :

$$A_0 := a_0(X_1, \ldots, X_{n-s}) - a_0(Y_1, \ldots, Y_{n-s}).$$

## 8.6. Segundo Concepto de Solución : Isomorfismo Birracional.

De nuevo consideramos las condiciones de la Sección 8.4 anterior.

i) $F := [f_1, \ldots, f_s]$ es una sucesión de polinomios en $K[X_1, \ldots, X_n]$ que definen un ideal intersección completa reducida $\mathfrak{a}(F) \subseteq K[X_1, \ldots, X_n]$. Así mismo, definen un conjunto algebraico equidimensional $V(F) \subseteq \mathbb{K}^n$.
ii) Las variables están en posición de Noether con respecto a la variedad $V(F)$, ésto es, la siguiente es una extensión entera de anillos :

$$A = K[X_1, \ldots, X_{n-r}] \hookrightarrow B = K[X_1, \ldots, X_n]/\mathfrak{a}(F).$$

Por lo expuesto en Secciones anteriores, $B$ es un $A-$módulo libre y el rango de $B$ como $A-$módulo libre está acotado por el grado geométrico de $V(F)$, ésto es,

$$rank_A B \leq deg(V(F)).$$

Sea $g$ un polinomio adicional, $G$ el morfismo regular definido a través de $g$ y la normalización de Noether como en la Sección 8.4. Sea $H_g \subseteq \mathbb{K}^{n-s+1}$ la hipersuperficie dada como $G(V(F))$ y sea $m_g$ el polinomio mínimo de esa hipersuperficie que, al mismo tiempo, es el polinomio mínimo del endomorfismo $\eta_g$.

Definición 66. *Con las anteriores notaciones, el polinomio $g$ se dice Elemento Primitivo con respecto a la variedad $V(G)$ y la Normalización de Nother fijada si $G$ define un isomorfismo birracional entre $V(G)$ y la hipersuperficie $H_g$.*

El siguiente enunciado nos ofrece una caracterización de la condición de elemento primitivo :

Proposición 8.6.1 (Elemento Primitivo). *Con las anteriores notaciones, las siguiente condiciones equivalentes caracterizan el hecho de ser Elemento primitivo :*

i) *$g$ es un Elemento Primitivo con respecto a $V(F)$ y la Normalización de Noether fijada.*
ii) *$g$ es un Elemento Primitivo para todas las componentes irreducibles de $V(G)$ que identifica las componentes irreducibles de $V(G)$ y las componente irreducibles de $H_g$.*
iii) *El Polinomio Característico $\chi_g$ de $\eta_g$ es libre de cuadrados.*
iv) *El Polinomio mínimo y el polinomio característico de $\eta_g$ coinciden, ésto es*

$$m_g = \chi_g.$$

v) *Si $D := rank_A B = dim_C B'$, la siguiente es una base de $B'$ como espacio vectorial :*

$$\{1, g, g^2, \ldots, g^{D-1}\}.$$

Los Elementos Primitivos permiten ofrecer una descripción del álgebra cero–dimensional $B'$ en los términos siguientes : Dado un polinomio $g \in K[X_1, \ldots, X_n]$ que sea Elemento Primitivo con respecto a $V(G)$ y dado su polinomio mínimo $m_g$ disponemos de la siguiente información :

- El grado del Polinomio Mínimo es la dimensión de $B'$ como $C-$espacio vectorial.
- Disponemos de una base de $B'$ como $C-$espacio vectorial.
- Tenemos la matriz de la homotecia $\eta_g : B' \longrightarrow B'$ con respecto a esa base : $C(m_g)$ es la matriz compañera del polinomio mínimo.

Adicionalmente, tenemos la siguiente Proposición :

Proposición 8.6.2. *Con las anteriores notaciones, si $g$ es un elemento primitivo con respecto a $V(G)$ y la Normalización de Noether dada se tiene : Para cada $i$, $n-s+1 \leq i \leq n$, existen :*

i) *Un Polinomio no nulo $\rho \in K[X_1, \ldots, X_{n-s}]$ de grado acotado por $deg(V(F))^2 deg(g)$,*
ii) *Polinomios $v_i(X_1, \ldots, X_{n-2}, T) \in K[X_1, \ldots, X_{n-s}, T]$ tales que*
   - *$deg_T v_i \leq deg_T m_g$,*
   - *$deg(v_i) \leq (deg(V(G))deg(g))^3$,*

*De tal modo que para cada $x \in V(G)$ se verifica :*

$$\rho(x)x_i - v_i(x_1, \ldots, x_{n-2}, g) = 0.$$

*Estas funciones racionales se denominan parametrizaciones asociadas al elemento primitivo.*

Obsérvense las siguientes dos propiedades fundamentales :

PROPOSICIÓN 8.6.3. *Con las notaciones e hipótesis anteriores, la inversa del isomorfismo birracional* $G : V(G) \longrightarrow H_g$ *es dada por :*

$$G^{-1}(y) := (y_1, \ldots, y_{n-s}, \rho^{-1}(y_1, \ldots, y_{n-s})v_{n-s+1}(y), \ldots, \rho^{-1}(y_1, \ldots, y_{n-s})v_n(y)),$$

*para todo* $y \in H_g$.

PROPOSICIÓN 8.6.4. *Con las notaciones e hipótesis anteriores, sea* $\mathfrak{a}(F)^e$ *la extensión de* $\mathfrak{a}(F)$ *al álbera cero–dimensional* $B'$. *La siguiente es una igualdad de ideales en* $B'$ *:*

$$\mathfrak{a}(F)^e = (m_g(x_1, \ldots, x_{n-s}, g), \rho^{-1}v_{n-s+1}(x_1, \ldots, x_{n-s}, g), \ldots, \rho^{-1}v_n(x_1, \ldots, x_{n-s}, g))).$$

DEFINICIÓN 67 (Solución a la Kronecker o el Isomorfismo Birracional). . *Sea* $F := [f_1, \ldots, f_s]$ *una sucesión de polinomios que generan un ideal* $(F)$ *intersección completa reducida. Llamaremos solución a la Kronecker de* $F$ *a la siguiente información :*

i) *Un cambio de coordenadas que pone las variables en posición de Noether con respecto a la variedad* $V(F)$,
ii) *Un polinomio* $g$ *que define un isomorfismo birracional* $G$ *con respecto a esa posición de Noether.*
iii) *La información relativa a una descripción completa de ese isomorfismo birracional :*
   a) *El polinomio mínimo de la hipersuperficie* $H_g$ *birracionalmente isomorfa a* $V(G)$ *(ésto es, el polinomio mínimo de* $\eta_g$*),*
   b) *Las parametrizaciones (ésto es, la descripción de* $G^{-1}$*).*

Obsérvese que la información de una resolución a la Kronecker, mediante un isomorfismo birracional, contiene una descripción de la $C-$álgebra $B'$ en el sentido expuesto en el Capítulo 3. Es decir, se dispone de la siguiente información :

i) La normalización de Noether :

$$A = K[X_1, \ldots, X_{n-r}] \hookrightarrow B = K[X_1, \ldots, X_n]/\mathfrak{a}(F).$$

ii) Una base de $B'$ como espacio vectorial :

$$\{1, g, g^2, \ldots, g^{D-1}\},$$

donde $D$ es el grado del polinomio mínimo $m_g$.
iii) La matriz de la homotecia $\eta_g$ en esa base :

$$M_g := C(m_g),$$

es la matriz compañera de $m_g$.
iv) Las matrices en esa base de los tensores de multiplicación $\eta_{X_i} : B' \longrightarrow B'$ :

$$M_{X_i} := \rho^{-1}v_i(X_1, \ldots, X_{n-s}, M_g).$$

**8.6.1. Cálculo del Polinomio Eliminante y Algoritmos Instrumentales.** De nuevo usaremos las estrategias propuestas en el Capítulo 3, aunque usando la estructura de datos esquema de evaluación : Dada una descripción de $V(G)$ mediante un isomorfismo birracional ("a la Kronecker") y dado un nuevo polinomio $h \in K[X_1, \ldots, X_n]$, la matriz de la homotecia definida por $h$ viene dada por la siguiente identidad :

$$M_h := h(X_1, \ldots, X_{n-s}, M_{X_{n-s+1}}, \ldots, M_{X_n}).$$

Est matriz corresponde a un endomorfismo diagonalizable (estamos en el caso reducido) y, por tanto, su polinomio mínimo es el polinomio característico libre de cuadrados. Concluimos

PROPOSICIÓN 8.6.5. *Con las anteriores notaciones, dada una descripción de $V(G)$ "a la Kronecker" y dado un polinomio adicional $h$, podemos calcular el Polinomio Eliminante de $h$ con respecto a $V(G)$ en tiempo polinomial en la codificación de $h$, el grado de $V(G)$ y el grado del Elemento Primitivo $g$. El tal polinomio Eliminante es descrito como la lista de sus coeficientes en $K[X_1, \ldots, X_{n-s}]$ y estos coeficientes son dados mediante esquemas de evaluación.*

El método esencial es el uso del algoritmo de Berkowicz (véase [**Bkw, 84**]) dando como salida la descripción de los coeficientes del polinomio característico $\chi_h$ como el propio esquema de evaluación de Berkowicz y no como polinomios en forma densa. A partir del polinomio $\chi_g$ basta con quitar los factores múltiples usando la estrategia obvia a través de la matriz de van der Monde.
A partir de estas reflexiones, disponemos de algoritmos que permiten resolver problemas como los siguientes :

i) DECIDIR SI UN POLINOMIO ADICIONAL ES TAMBIÉN ELEMENTO PRIMITIVO. Basta con calcular el polinomio característico de $M_h$ y el mínimo y compararlos usando un Test de Nulidad (no olvidemos que están dados como esquemas de evaluación) de los descritos en la Sección 2.3. Obviamente, el Test es probabilista pero muy eficiente.

ii) CONSISTENCIA : DECIDIR SI UN POLINOMIO ADICIONAL SE ANULA EN ALGÚN PUNTO DE LA VARIEDAD $V(G)$. Basta con que el término independiente del Polinomio Eliminante no sea una constante. De nuevo usamos Tests Probailistas de los descritos en la Sección 2.3 anterior.

iii) DECIDIR SI UN NUEVO POLINOMIO ES DIVISOR DE CERO O NO. Basta con que el término independiente del polinomio mínimo sea no nulo. De nuevo, Tests Probabilistas al estilo de la Sección 2.3.

iv) TÉCNICAS A LA BERTINI. Se trata de las técnicas descritas en las Proposiciones 8.4.5 y 8.4.5 de la Sección 8.4. A partir del polinomio eliminante de una combinación lineal genérica, usando Tests de Nulidad al estilo de los descritos en la Sección 2.3 se puyeden hallar combinaciones lineales particulares que verifican cualquiera de las condiciones genéricas descritas en las dos Proposiciones relativas a los Teoremas de Bertini.

v) LOS ALGORITMOS INSTRUMENTALES DESCRITOS EN LA SECCIÓN ANTERIOR. En la Sección 8.5 anterior se describen unos algoritmos instrumentales a través del concepto de solución basado en el Teorema de Quillen– Suslin. El lector observará que se trata de algoritmos que usan como principal información coeficientes del Polinomio Eliminante calculados a partir de una base del módulo. Dado que el polinomio eliminante es también calculable a partir de la matriz coordenada con respecto a una base del álgebra obtenida mediante extensión de escalares y que esta matriz está fácilmente disponible a partir de una solución a la Kronecker, tenemos todos los medios para realizar estos algoritmos en el mismo orden de complejidad.

## 8.7. Tercer Concepto de Solución : Polinomio de Cayley–Chow.

Como hemos observado anteriormente, el grado del polinomio $g$ usado como elemento primitivo puede interferir con las complejidades. En esta Sección observaremos que, dado que estamos sobre un cuerpo perfecto y un ideal radical (caso separable) y si suponemos que el cuerpo tiene "suficientes elementos" (para poder aplicar los Tests de Nulidad de la Sección 2.3) podemos mostrar ejemplos particulares de elementos primitivos que son formas lineales.

DEFINICIÓN 68. *Con las notaciones de la Sección anterior, llamaremos polinomio de Cayley–Chow de la variedad $V(F)$ con respecto a una normalización de Noether dada,*

*al polinomio eliminante de la forma lineal genérica*

$$\mathcal{U} := T_{n-2+1}X_{n-s+1} + \cdots + T_nX_n.$$

*8.7.0.1. Cálculo del Polinomio de Cayley–Chow. Dada una descripción "a la Kronecker" de la variedad $V(F)$, podemos calcular el polinomio de Chow en tiempo polinomial en el tamaño de esa descripción. El Polinomio de Chow será dado en codificación mixta. Es decir, como la lista de los coeficientes con respecto a una variable de eliminación distinguida $T$ y los coeficientes (polinomios en $K[X_1, \ldots, X_{n-s}, T_{n-s+1}, \ldots, T_n]$) como esquemas de evaluación. La codificación del Polinomio de Chow es también polinomial en la talla de la descripción "a la Kronecker" de $V(F)$ y el grado geométrico de la variedad $V(F)$ como consecuencia del siguiente resultado.*

Proposición 8.7.1. *Con las anteriores notaciones, el polinomio de Chow es un polinomio en $K[X_1, \ldots, X_{n-s}, T_{n-s+1}, \ldots, T_n][T]$, mónico con respecto a la variable $T$, de grado acotado en cada grupo de variables por $deg(V(F))$, libre de cuadrados.*

Proposición 8.7.2. *Sea $D \in K[X_1, \ldots, X_{n-s}, T_{n-s+1}, \ldots, T_n]$ el discriminante del polinomio de Chow con respecto a la variable $T$. Sea $\underline{\lambda} := (\lambda_{n-s+1}, \ldots, \lambda_n) \in K^s$ un punto cualquiera tal que el polinomio :*

$$D(X_1, \ldots, X_{n-s}, \lambda_{n-s+1}, \ldots, \lambda_n) \in K[X_1, \ldots, X_{n-s}],$$

*sea un polinomio no nulo. Entonces, la forma lineal :*

$$u := \lambda_{n-s+1}X_{n-s+1} + \cdots \lambda_nX_n \in K[X_1, \ldots, X_n],$$

*es un elemento primitivo de $V(F)$ con respecto a la Normalización de Noether fijada.*

Estos resultados nos permiten anunciar la equivalencia entre la codificación "a la Kronecker" y el uso del Polinomio de Chow para codificar variedades intersección completa reducidas.

Definición 69 (Solución a la Cayley–Chow). *Con las notaciones e hipótesis de las Secciones anteriores, llamaremos solución a la Cayley–Chow del sistema de ecuaciones polinomiales definido por $F$ a la información siguiente :*

i) *Una lista de variables en posición de Noether con respecto a la variedad $V(F)$,*
ii) *El polinomio de Cayley–Chow de $V(F)$ con respecto a esa Normalización de Noether.*

Teorema 8.7.3. *Las codificaciones de variedades intersección completa reducida a la Kronecker y a la Cayley–Chow son computacionalmente equivalentes. Esto es,*

i) *Existe un algoritmo probabilista tal que dada una resolución a la Kronecker de $V(F)$ permite calcular una resolución a la Cayley–Chow en tiempo polinomial en*
$$deg(V(F))L,$$
*donde $deg(V(F)$ es el grado geométrico de $V(F)$ y $L$ es la talla de la codificación a la Kronecker.*
ii) *Existe un algoritmo probabilista tal que dada una resolución a la Cayley–Chow de $V(F)$ permite calcular una resolución a la Kronecker en tiempo polinomial en*
$$deg(V(F))L,$$
*donde $deg(V(F)$ es el grado geométrico de $V(F)$ y $L$ es la talla de la codificación a la Cayley–Chow.*

Obviamente ambos algoritmos utilizan los Tests de Nulidad descritos en la Sección 2.3 y estos Tests son los únicos elementos probabilistas que intervienen. Así mismo, los algoritmos de paso se basan fuertemente en los algoritmos descritos en el Capítulo 3 para el caso de dimensión cero. De hecho, observe el lector que todo lo expuesto no es

sino una relectura de lo hecho en el caso cero–dimensional, dado que hemos restringido nuestras disquisiciones al álgebra cero–dimensional $B'$.

## 8.8. Cuarto Concepto de Solución : Fibras de Levantamiento.

Como se observó en [**Pa, 95**] y [**Pa** *et al.*, **1995a**], la utilización de las resoluciones a la Kronecker o a la Cayley–Chow, combinadas por la codificación mediante esquema de evaluación, podrían permitir acelerar los procesos de resolución de ecuaciones polinomiales multivariadas. Sin embargo, estos procesos hacían intervenir una recursión de interpolaciones que modifica la complejidad de los algoritmos, aumentándolos en una exponencial. La solución a esta dificultad se obtuvo mediante una técnica basada en una reducción al caso cero–dimensional y un proceso de deformación homotópica. Para entender este proceso, se introdujeron en al Capítulo 7 las Fibras de Levantamiento. Retomemos esa terminología.

Definición 70. *Sea $V(F) \subseteq \mathbb{K}^n$ un conjunto algebraico intersección completa, donde $F := [f_1, \ldots, f_s]$ es una lista de polinomios que genera un ideal radical $\mathfrak{a}(F)$ en $K[X_1, \ldots, X_n]$ de altura $s$. Supongamos que las variables están en posición de Noether con especto a la variedad $V(F)$, ésto es, supongamos que la siguiente es una extención entera de anillos :*

$$A := K[X_1, \ldots, X_{n-s}] \hookrightarrow B := K[X_1, \ldots, X_n]/\mathfrak{a}(F).$$

*Un punto $P \in K^{n-s}$ se denomina un punto de levantamiento de $V(F)$, si se tiene que :*

i) *La variedad obtenida como la intersección :*

$$V_P(F) := V(F) \cap (\{P\} \times \mathbb{K}^s),$$

*es una variedad lisa de grado igual a $rank_A B$*

ii) *El determinante de la matriz jacobiana*

$$D_P(F) := \left(\frac{\partial f_i}{\partial X_j}(P, X_{n-s+1}, \ldots, X_n)\right)_{1 \leq i \leq, n-s+1 \leq j \leq n},$$

*no es un divisor de cero en $K[V_P(F)]$.*

*La variedad $V_P(F)$ se denomina Fibra de Levantamiento.*

Observe el Lector que las hipótesis expuestas nos permiten hacer uso del Lema de Hensel descrito en el Capítulo 7.

### 8.8.1. Cálculo de Fibras de Levantamiento desde la Solución a la Kronecker.

La siguiente Proposición nos permitirá obtener fibras de levantamiento a partir de una descripción a la Kronecker de la variedad intersección completa reducida $V(F)$.

Proposición 8.8.1. *Con las notaciones anteriores, supongamos dada la siguiente información :*

i) *La Normalización de Noether :*

$$A := K[X_1, \ldots, X_{n-s}] \hookrightarrow B := K[X_1, \ldots, X_n]/\mathfrak{a}(F).$$

ii) *Un elemento primitivo dado como una forma lineal $u := \lambda_{n-2+1} X_1 + \cdots + \lambda_n X_n \in K[X_1, \ldots, X_n]$.*

iii) *El Polinomio Eliminante $m_u \in K[X_1, \ldots, X_{n-s}, T]$ del elemento primitivo. Sea $\mu \in K[X_1, \ldots, X_{n-s}]$ el discriminante de $m_g$.*

iv) *El Polinomio no nulo $\rho \in K[X_1, \ldots, X_{n-s}]$ y los polinomios $v_i \in K[X_1, \ldots, X_{n-s}, T]$ tal que $\rho^{-1} v_{n-s+1}, \ldots, \rho^{-1} v_n$ definen las parametrizaciones.*

v) *El determinante* $Det_F \in K[X_1, \ldots, X_n]$ *de la matriz jacobiana*

$$\left(\frac{\partial f_i}{\partial X_j}(X_1, \ldots, X_n)\right)_{1 \leq i \leq, n-s+1 \leq j \leq n}.$$

*Sea* $\Delta \in K[X_1, \ldots, X_{n-s}]$ *el término independiente del Polinomio Eliminante de* $Det_F$ *con respecto a* $V(F)$ *y la Normalización de Noether fijada.*

*Sea* $P := (p_1, \ldots, p_{n-s}) \in K^{n-s}$ *un punto tal que se verifican las siguientes propiedadees :*

$$\mu(P) \neq 0, \rho(P) \neq 0, \Delta(P) \neq 0. \tag{8.8.1}$$

*Entonces,* $P$ *es un punto de levantamiento de* $V(F)$ *y se verifica además :*

- *La forma lineal* $u := \lambda_{n-2+1}X_1 + \cdots + \lambda_n X_n \in K[X_{n-s+1}, \ldots, X_n]$ *es un elemento primitivo de la* $K-$*álgebra cero–dimensional* $K[V_P(F)]$.
- *El Polinomio* $m_{u,P} \in K[T]$ *dado mediante :*

$$m_{u,P} := m_u(p_1, \ldots, p_{n-s}, T) \in K[T],$$

*es un polinomio libre de cuadrados y es el polinomio mínimo de* $u$ *en* $K[V_P(F)]$.
- *Los polinomios* $v_{i,P} \in K[T]$ *dados mediante :*

$$v_{i,P} := \rho^{-1}(p_1, \ldots, p_{n-s}) v_{n-s+1}(p_1, \ldots, p_{n-s}, T) \in K[T],$$

*son las parametrizaciones de la variedad* $V_P(F)$ *con respecto al elemento primitivo* $u$.
- *El determinante de la matriz jacobiana*

$$D_P(F) := \left(\frac{\partial f_i}{\partial X_j}(P, X_{n-s+1}, \ldots, X_n)\right)_{1 \leq i \leq, n-s+1 \leq j \leq n},$$

*no es un divisor de cero en* $K[V_P(F)]$.

Observe el lector que las condiciones expuestas en las desigualdades (8.8.1) anteriores, nos permiten utilizar los Tests de Nulidad de polinomios expuestos en el Capítulo 3 para hallar un punto con fibra no ramificada. Además, hallado ese punto, la especialización de las variables libres de la Normalización de Noether nos ofrece inmediatamente una resolución a la Kronecker de la Fibra de Levantamiento $V_P(F)$. Esto es lo que resume el presente enunciado.

Proposición 8.8.2. *Existe un algoritmo probabilista que a partir de la resolución a la Kronecker de una variedad intersección completa reducida, calcula una resolución a la Kronecker de una fibra de levantamiento. El tiempo de ejecución de este algoritmo es polinomial en las cantidades*

$$deg(V(F))L,$$

*donde* $deg(V(F))$ *es el grado geométrico de la variedad intersección completa reducida en cuestión y* $L$ *es el tamaño de la descripción a la Kronecker de* $V(F)$.

**8.8.2. De la Fibra de Levantamiento a la Forma de Cayley–Chow.** El lector habrá observado que los Puntos de Levantamiento son aquellos puntos en los que tenemos las buenas condiciones para poder aplicar el algoritmo de Newton–Hensel, descrito en el Capítulo 7. Procederemos del modo siguiente :
Consideremos dado un punto de levantamiento $P \in K^{n-s}$, y una descripción de la Fibra de Levantamiento $V_P(F)$. Consideremos una descripción de la forma de Cayley–Chow de $V_P(F)$ y supongamos $M$ la matriz de la forma de Cayley–Chow de $V_P(F)$.
La matriz $M$ es una matriz cuyas coordenadas son polinomios con coeficientes en el anillo de polinomios $K[T_{n-s+1}, \ldots, T_n]$. Sea $N_F$ el operador de Newton definido por la

secuencia de polinomios $F := [f_1, \ldots, f_s]$, ésto es

$$N_F := N_F(X_{n-s+1}, \ldots, X_n) := \begin{pmatrix} X_{n-s+1} \\ \vdots \\ X_n \end{pmatrix} - D(F)^{-1}_{\underline{X}} \begin{pmatrix} f_1(\underline{X}) \\ \vdots \\ f_n(\underline{X}) \end{pmatrix},$$

donde $D(F)$ es la matriz jacobiana :

$$D(F) := \left( \frac{\partial f_i}{\partial X_j}(X_1, \ldots, X_n) \right)_{1 \leq i \leq, n-s+1 \leq j \leq n}.$$

Sean $M^{(P)}_{X_{n-s+1}}, \ldots, M^{(P)}_{X_n}$ las matrices de los tensores de multiplicación para la variedad $V_P(F)$.
Consideremos el vector de matrices

$$\begin{pmatrix} N^{(k)}_{n-s+1} \\ \vdots \\ N^{(k)}_n \end{pmatrix} := N^k_F(M^{(P)}_{X_{n-s+1}}, \ldots, M^{(P)}_{X_n}).$$

Este vector de matrices, nos permite generar una nueva matriz :

$$\mathcal{M}^{(k)} := T_1 N^{(k)}_{n-s+1} + \cdots + T_n N^{(k)}_n.$$

Proposición 8.8.3. *La matriz $\mathcal{M}^{(k)}$ verifica las siguientes propiedades :*

i) *La matriz $\mathcal{M}^{(k)}$ es una matriz cuyo número de filas y columnas coincide con $deg(V_P(F))$ y $deg(V(F))$.*
ii) *Las coordenadas de la matriz $\mathcal{M}^{(k)}$ con elementos en el anillo $R_P[T_{n-s+1}, \ldots, T_n]$, donde $R_P$ es el anillo de series de potencials formales :*

$$R_P := K[[X_1 - p_1, \ldots, X_{n-s} - p_{n-s}]].$$

iii) *Los coeficientes $a_\mu \in R_P$ del polinomio característico de la matriz $\mathcal{M}^{(k)}$ ( $\chi \in R_P[T_{n-s+1}, \ldots, T_n][T]$) con respecto a las variables $T_{n-s+1}, \ldots, T_n, T$ y los coeficientes $b_\mu \in R_P$ del Polinomio de Cayley–Chow de $V(F)$ con respecto al mismo grupo de variables, verifican :*

$$\|a_\mu - b_\mu\| \leq \frac{1}{2^{2^k}},$$

*donde $\| \cdot \|$ es la norma no arquimediana en $R_P$.*

Esta proposición nos permitirá construir la forma de Chow de $V(F)$ a partir del polinomio característico de $\mathcal{M}^{(k)}$, tras un número de iteraciones $k := O\left(log_2 log_2 deg(V(F))\right)$ y utilizando la técnica de evitación de divisiones de Strassen (cf. [**St, 73**]).

Teorema 8.8.4. *Existe un algoritmo que a partir de la resolución a la Kronecker de una fibra de levatamiento, calcula la forma de Cayley–Chow de la variedad intersección completa reducida. El tiempo de este algoritmo es polinomial en*

$$deg(V(F)), R, L,$$

*donde $deg(V(F)) = deg V_P(F)$ es el grado de la fibra de levantamiento y de la variedad, $R$ es la talla de la codificación a la Kronecker de la variedad, $L$ es la talla necesaria para evaluar los polinomios de entrada $F := [f_1, \ldots, f_s]$. El output de ese algoritmo es la forma de Cayley–Chow de $V(F)$ descrita como la lista de sus coeficientes con respecto a la variable de eliminación $T$ y los coeficientes aparecen descritos mediante esquemas de evaluación.*

De hecho, el algoritmo calcula el polinomio característico de $\mathcal{M}^{(k)}$, evitando divisiones y truncando en la cota de grado apropiada.

## 8.9. Eliminar una Ecuación.

Antes de Proceder a describir el algoritmo como proceso iterativo, necesitaremos discernir un elemento instrumental técnico adicional.
Supongamos dado $F := [f_1, \ldots, f_s]$ una sucesión de polinomios que definen una intersección completa reducida. Sea $V(F) \subseteq \mathbb{K}^n$ la variedad algebraica que definen, sea $\mathfrak{a}(F)$ el ideal que generan y supongamos, como anteriormente, que las variables están en posición de Noether.

$$A := K[X_1, \ldots, X_{n-s}] \hookrightarrow B := K[X_1, \ldots, X_n]/\mathfrak{a}(F).$$

Sea $f_{s+1} \in K[X_1, \ldots, X_n]$ un nuevo polinomio. Supongamos que, utilizando los algoritmos descritos en la Subsección 8.5.1 anterior, las variables se encuentran en posición de Noether con respecto al ideal $\mathfrak{a}(F) + (f_{s+1})$. De hecho, el método descrito en la Subsección 8.5.1 se basa en el principio siguiente :
Sea $m_{s+1} \in K[X_1, \ldots, X_{n-s}, T]$ el polinomio mínimo de $f_{s+1}$ con respecto a la variedad $V(F)$. Sea $a_0(X_1, \ldots, X_{n-s}) \in K[X_1, \ldots, X_{n-s}]$ el término independiente de tal polinomio. El cambio de variables efectuado ha sido elegido de tal modo que el tal polinomio $a_0$ es mónico con respecto a la variable $X_{n-s}$. En particular, el polinomio $a_0$ es un múltiplo del polinomio mínimo de $X_{n-s}$ con respecto al nuevo ideal $\mathfrak{a}(F) + (f_{s+1})$. Sin pérdida de la generalidad, supongamos que $a_0$ es libre de cuadrados.
Supongamos, además, que disponemos del elemento primitivo $u := \lambda_{n-s+1}X_{n-s+1} + \cdots \lambda_n X_n$ con respecto a la variedad $V(F)$. Sea $m_u \in K[X_1, \ldots, X_{n-s}, T]$ el polinomio mínimo de $u$ con respecto a $V(F)$. Finalmente, supongamos que $V(F) \cap V(f_{s+1})$ es una variedad intersección completa reducida y que $F_{s+1} := [f_1, \ldots, f_{s+1}]$ genera un ideal radical de altura $s+1$. En este caso, se tiene :

Lema 8.9.1. *Con las notaciones anteriores, sea $\lambda_{n-s} \in K$ tal que $Z := \lambda_{n-s}X_{n-s} + T$ es elemento primitivo del anillo intersección completa reducida :*

$$K[X_1, \ldots, X_{n-s}, T]/\mathfrak{b},$$

*donde $\mathfrak{b}$ es el ideal generado por $a_0$ y $m_u$. Entonces, la forma*

$$u_{s+1} := \lambda_{n-s}X_{n-s} + u \in K[X_1, \ldots, X_n],$$

*es un elemento primitivo de la variedad $V(F_{s+1})$ con respecto a la normalización de Noether :*

$$K[X_1, \ldots, X_{n-s-1}] \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{a}(F_{s+1}).$$

En particular, hemos reducido el cálculo de un nuevo elemento primitivo a un problema con dos polinomios mónicos libres de cuadrados en los que hay que eliminar dos variables. Es el principio subyacente a lo descrito en el Capítulo **??**. Para el cálculo de las nuevas parametrizaciones procederemos usando también los polinomios mínimos de las demás variables $X_{n-s+1}, \ldots, X_n$ junto con el polinomio $a_0$ usando la técnica "dos a dos" descrita en [**KrPa, 96**]. Esto nos conduce al siguiente enunciado :

Teorema 8.9.2. *Sea $F := [f_1, \ldots, f_s]$ una sucesión de polinomios en $K[X_1, \ldots, X_n]$ tales que generan un ideal $\mathfrak{a}(F)$ radical de altura $s$. Sea $f_{s+1}$ una nueva ecuación tal que la sucesión $F_{s+1} := [f_1, \ldots, f_s, f_{s+1}]$ que genera un ideal $\mathfrak{a}(F_{s+1})$ de altura $s+1$. Entonces, existe un algoritmo probabilista tal que dada una descripción a la Kronecker de $V(F)$ obtiene una descripción a la Kronecker de $V(F_{s+1})$. El tiempo de ejecución de ese algoritmo es polinomial en :*

$$deg(V(F)), deg(V(F_{s+1})), deg(f_{s+1}), L,$$

*donde $deg(V(F))$ es el grado geométrico de $V(F)$, $deg(V(F_{s+1})) \leq deg(V(F))deg(f_{s+1})$ es el grado geométrico de $V(F_{s+1})$, $deg(f_{s+1})$ es el grado total de $f_{s+1}$ y $L$ es el coste de evaluar $f_{s+1}$.*

## 8.10. Un algoritmo Iterativo e Intrínseco Muy eficiente.

Ha llegado el momento de exponer el enunciado principal de este Capítulo. Para ello, nos vamos a restringir a unas condiciones particulares de sucesión regular reducida. Debe indicarse que estas condiciones particulares no son especialmente restrictivas puesto que se pueden obtener iterativamente, mediante el uso de las versiones efectivas del Teorema de Bertini descritas como las Proposiciones 8.4.5 y 8.4.6 anteriores.
Supongamos, por tanto, que se nos da como INPUT una lista $F := [f_1, \ldots, f_s]$ de polinomios tales que se verifican las siguientes propiedades (*Sucesión Regular Reducida*) :

i) El ideal $\mathfrak{a}$ define una variedad equidimensional de dimensión $n - s$[13]
ii) Para cada $i$, $1 \leq i \leq s-1$ los ideales $\mathfrak{a}_i$ generados por $[f_1, \ldots, f_i]$ son ideales radicales de altura $i$. En particular, las variedades (llamadas intermedias) $V_i := V(\mathfrak{a}_i) \subseteq \mathbb{K}^n$ son variedades equidimensionales de dimensión $n - i$.

Denotemos por $F_i := [f_1, \ldots, f_i]$ las listas intermedias de ecuaciones polinomiales. Definamos el siguiente algoritmo :

---

INPUT : Una lista $F$ verificando las condiciones anteriores.

**Inicializar :**

- HALLAR LA NORMALIZACIÓN DE NOETHER DE $F_1$ (*Usando lo descrito en la Subsección 8.5.1*)
- HALLAR UNA FIBRA DE LEVANTAMIENTO $V_{P_1}(F_1)$ DE $V(F_1)$ (*Usando lo descrito en la Subsección 8.8.1*)

**Inducción :**
Para cada $i$, $2 \leq i \leq s-1$ **do** :
INPUT : Una descripción "a la Kronecker" de una Fibra de Levantamiento $V_{P_i}(F_i)$.

- HALLAR UNA DESCRIPCIÓN A LA CAYLEY–CHOW de $V(F_i)$ (*Usando lo descrito en la Subsección 8.8.2*).
- HALLAR UNA DESCRIPCIÓN "A LA KRONECKER" DE $V(F_i)$ (*Usando lo descrito en la Sección 8.7*).
- HALLAR UNA NORMALIZACIÓN DE NOETHER DE $V(F_{i+1})$ (*Usando lo descrito en la Subsección 8.5.1*).
- ELIMINAR LA NUEVA ECUACIÓN $f_{i+1}$ CON RESPECTO A $V(F_i)$ (*Usando lo descrito en la Sección 8.9*).
- HALLAR UNA DESCRIPCIÓN "A LA KRONECEKER" DE $V(F_{i+1})$ (*Usando lo descrito en la Sección 8.9*).
- HALLAR UNA FIBRA DE LEVANTAMIENTO $V_{P_{i+1}}(F_{i+1})$ (*Usando lo descrito en la Sección 8.8.1*).

**El Output de estas Iteraciones es dado mediante :**
Una Fibra de Levantamiento $V_{P_{s-1}}(F_{s-1})$.
**Conclusión del Algoritmo :**

- HALLAR UNA DESCRIPCIÓN A LA CAYLEY–CHOW DE $V(F_{s-1})$ (*Usando lo descrito en la Subsección 8.8.2*).
- HALLAR UNA DESCRIPCIÓN "A LA KRONECKER" DE $V(F_{s-1})$(*Usando lo descrito en la Sección 8.7*).
- HALLAR UNA NORMALIZACIÓN DE NOETHER DE $V(F_{s-1})$ (*Usando lo descrito en la Subsección 8.5.1*).
- ELIMINAR LA NUEVA ECUACIÓN $f_s$ CON RESPECTO A $V(F_{s-1})$ (*Usando lo descrito en la Sección 8.9*).

[13]También sería válido si fuera el ideal trivial (asunto que verificaríamos con el algoritmo) o si definiera una variedad cero–dimensional (aunque no fuera intersección completa).

OUTPUT : Una Descripción a la Kronecker de $V(F) = V(F_s)$.

---

TEOREMA 8.10.1. *Con las anteriores notaciones, dada una lista* $F := [f_1, \ldots, f_s]$ *definiendo una sucesión regular reducida. Existe un algoritmo probabilista que calcula una descripción a la Kronecker de la variedad* $V(F) \subseteq \mathbb{K}^n$. *El tiempo de ejecución de ese algoritmo, usando codificación de números racionales por esquemas de evaluación, es polinomial en las cantidades :*

$$d, \delta(F), L,$$

*donde* $d := max\{deg(f_i) \ : \ 1 \leq i \leq s\}$, $L$ *es la talla de la representación de los polinomios que aparecen en* $F$ *y*

$$\delta(F) := max\{deg(V(F_i)) \ : \ 1 \leq i \leq s-1\}.$$

# Bibliografía


[Ar, 06] E. Arrondo, *Another elementary proof of the Nullstellensatz.* Amer. Math. Monthly **113** (2006), 169171.

[AtMc, 69] M.F. Atiyah, I.G. Macdonald, *"Introduction to Commutative Algebra"*, Addison-Wesley Publishing Co., 1969. [Edición en español por Ed. Reverté, 1980].

[BaSh, 96] E. Bach, J. Shallit, *"Algorithmic Number Theory. Vol 1 : Efficient Algorithms"*, MIT Press, 1996.

[BeWe, 93] T. Becker, V. Weispfenning, *"Groebner bases: a computational approach to commutative algebra"*. Grad. Texts in Maths. **141**, Springer, 1993.

[Bkw, 84] S.J. Berkowicz, *On computing the determinant in small parallel time using a small number of processors.* Inf. Proc. Letters **18** (1984), 147–150.

[Be, 70] E.R. Berlekamp, *Factoring Polynomials over Large Finite Fields.* Mathematics of Computation **24**, (1970), 713–735.

[BCSS, 98] L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and real computation*, Springer-Verlag, New York, 1998.

[Bo, 67] N. Bourbaki, *"Algébre Commutative, Éléments de mathématique, Fascicule XXVIII, chapitres 1–7"*, Hermann 1961–.

[Br, 87] W. D. Brownawell, *Bounds for the degree in the Nullstellensatz.* Annals of Math. **126** (1987), 577591.

[BH, 93] W. Bruns, J. Herzog, *"Cohen-Macaulay rings"*. Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, 1993.

[Ca, 11] F. Cajori, *Horner's Methods of Approximation Anticipated by Ruffini.* Bull. Amer. Math. Soc. **17** (1911), 409-414.

[CGH, 88] L. Caniglia, A. Galligo and J. Heintz, *Borne simplement exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque*, C.R. Acad. Sci. Paris, t. **307**, Série I (1988), 255258.

[CaEi, 56] H. Cartan, S. Eilenberg, *"Homological algebra. With an appendix by David A. Buchsbaum"*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1999 [Reedición del original editado en Princeton en 1956].

[Ca, 71] J.W.S. Cassels, *"An Introduction to the geometry of numbers"*. Springer Verlag , 1971 (1st ed. 1959).

[CHMP, 01] D. Castro, K. Hägele, J.E.Morais, L. M. Pardo, *Kronecker's and Newton's approaches to Solving : A first Comparison.* J. of Complexity **17** (2001), 212–203.

[CoLiOS, 97] D. Cox, J. Little, D. O'Shea, *"Ideals, Varieties, and Algorithms"*, Springer, 1997 (1a. edición, 1992).

[CoLiOS, 98] ———, *"Using algebraic geometry"*. Graduate Texts in Mathematics **185**, Springer, 1998.

[EiMc, 45] S. Eilenberg, S. Mac Lane, General Theory of Natural Equivalence. *Trans. of the Amer. Math. Soc.* **58** (1945), 231–294.

[Ei, 95] D. Eisenbud, *"Commutative algebra: with a view toward algebraic geometry"*, Springer Verlag, 1995.

[vzGGe, 99] J. von zur Gathen, J. Gerhard, *"Modern Computer Algebra"*. Cambridge University Press, 1999.

[GiJe, 76] L. Gillman and M. Jerison, *"Rings of Continuous Functions"*. Springer-Verlag, New York, 1976.

[GuRo, 65] R.C. Gunning, H. Rossi, *"Analytic Functions of Several Complex Variables"*. Prentice–Hall, 1965.

[HMPS, 00] 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), 103183.

[HaWr, 38] G. H. Hardy, E. M. Wright, *"An Introduction to the Theory of Numbers"*. Oxford at the Clarendon Press, 1938.

[Hrt, 77] R. Hartshorne, *"Algebraic Geometry"*, Springer, 1977.

[He, 83] J. Heintz, *Fast quantifier elimination over algebraically closed fields*. Theoret. Comp. Sci. **24** (1983), 239–277.

[He, 26] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*. Math. Ann. **95** (1926), 736788.

[HiSt, 97] P. Hilton, U. Stammbach, *"A course in homological algebra. Second edition"*. Graduate Texts in Mathematics, **4**. Springer-Verlag, New York, 1997.

[Jod, 67] M.A. Jodeit, *Uniqueness in the Disision Algorithm*. Amer. Math. Monthly **74** (1967), 835-836.

[Jou, 83] J. P. Jouanolou, *Théorèmes de Bertini et applications*. Progress in Math. **42**, Birkhäuser, 1983.

[Ka, 70] I. Kaplansky, *"Commutative Rings"*, Allyn and Bacon, 1970.

[Ka$^2$, 83] L. Kaup, B. Kaup, *"Holomorphic Functions of Several Variables"*, Studies in Mathematics **3**, de Gruyter, 1983.

[Kn, 81] D.E. Knuth, *"The Art of Computer Programming, vol. 2 Seminumerical Algorithms"* Addison–Wesley, 1981.

[KMH, 89] H. Kobayashi, S. Moritsugu, R. W. Hogan, *On radical zero-dimensional ideals*. Journal of Symbolic Computation **8**, (1989), 545552.

[Kob, 77] N. Koblitz, *"p–adic numbers, p–adic analysis and Zeta–functions, 2nd Edition"* , GTM **58**, Springer, 1977.

[Kl, 88] J. Kollár, *Sharp Effective Nullstllensatz*. J. of A.M.S. **1** (1988), 963975.

[Kö, 1903] J. König. *"Einleitung in die allgemeine Theorie der algebraischen Grössen"*. Druck und Verlag von B.G. Teubner ,Leipzig, 1903.

[Ko, 92] D.C. Kozen, *"The Design and Analysis of Algorithms"*. Texts and Monographs in Computer Science, Springer Verlag, 1992.

[KrPa, 96] 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**, Birkhäuser Verlag, 1996, 193–254.

[KPS, 01] T. Krick, M. Sombra, L. M. Pardo, *Sharp Estimates for the Arithmetic Nullstellensatz*. Duke Math. Journal **109** (2001), 521598.

[Krn, 1882] L. Kronecker, *Grundzüge einer arithmetischen theorie de algebraischen grössen*.J. reine angew. Math. **92**(1882) 1122.

[Kr, 35] W. Krull, *"Idealtheorie"*. Ergebnisse der Mathematik, und ihrer Grenzgebiete, vol **4**, No. 3. Berlin, Julius Springer, 1935.

[Ku, 85] E. Kunz, *"Introduction to Commutative Algebra and Algebraic Geometry"*, Birkhäuser, 1985.

[Lf, 77] J.P. Lafon, *"Algèbre commutative"*, Hermann, 1977.

[Lm, 1844] G. Lamé, *Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entres deux nombres entiers*. Comptes Rendus Acad. Sci. **19** (1844), 876-870.

[Lgr, 1771] J.L. Lagrange, *Réflexions sur la résolution algébrique des équations*. Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, années 1770 et 1771, p.205-421.

[Lng, 72] S. Lang, *"Introduction to algebraic geometry"*. AddisonWesley, 1972.

[Mc, 75] S. Mac Lane, *"Homology. Reprint of the 1975 edition"*. Classics in Mathematics. Springer-Verlag, Berlin, 1995.

[Le, 84] M. Lejeune-Jalabert, *"Effectivité de Calculs Polynomiaux"*.Cours de DEA, Université de Grenoble, 1984.

[L$^3$, 82] A.K. Lenstra, H.W. Lenstra, L. Lovász, *"Factoring polynomials with rational coefficients"*. Mathematische Ann **261** (1982), 513–534.

[Mc, 16] F.S. Macaulay, *"The algebraic theory of modular systems"*.Cambridge Univ. Press, 1916.

[MaWü, 71] D. W. Masser and G. Wüstholz, *Fields of large transcendence degree generated by values of elliptic functions*. Invent. Math. **72** (1971) 407463.

[Ma, 80] H. Matsumura, *"Commutative Algebra (2nd. Edition)"*, Benjamin/Cummings, 1980.

[Ma, 89] ——— *"Commutative Ring Theory"*. Cambridge Studies in advanced Math. **8**, Cambridge Univ. Press, 1989.

[Mi, 89] M. Mignotte, *"Mathématiques pour le Calcul Formel"*, Presses Univ. de France, 1989.

[Mtz, 49] T. Motzkin, *The Euclidean algorithm*. Bull. Amer. Math. Soc., **55** (1949), 1142–1146.

[Nag, 75] M. Nagata, *"Local Rings"*, Robert E. Krieger, 1975.

[Nar, 68] R. Narasimhan, *"Analysis on Real and Complex Manifolds"*, North–Holland, 1968.

[Or, 13] Nuccio Ordine, *"L'utilità dell'Inutile. Manifesto"*. Bompiani, 2013.

[Os, 73] A.M. Ostrowski, *"Solutions of Equations in Euclidean and Banach Spaces"*, Academic Press, 1973.

[Pa, 95] L. M. Pardo, *How Lower and Upper Complexity Bounds meet in Elimination Theory*. In Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, Proc. AAECC–11, (G. Cohen, M. Giusti, T. Mora, eds.),Lecture Notes in Computer Science **948**, Springer , 1995, 33–69.

[Pa *et al.*, 1995a] Luis M. Pardo (con M. Giusti, J. Heintz, J.E. Morais), *When polynomial equation system can be "solved" fast?*, In Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, Proc. AAECC–11, (G. Cohen, M. Giusti & T. Mora, eds.), Lecture Notes in Computer Science **948**, Springer Verlag, 1995, 205–231.

[Pa *et al.*, 1997b] Luis M. Pardo (con M. Giusti, K. Hägele, J. Heintz, J.L. Montaña, J.E. Morais), *Lower Bounds for Diophantine Approximations*. J. of Pure and Applied Algebra **117 & 118** (1997), 277–317.

[PoZa, 89] M. Pohst, H. Zassenhaus, *"Algorithmic Algebraic Number Theory"*, Cambridge Univ. Press, 1989.

[Po, 66] L.S. Pontrjagin, *"Topological groups"*. Gordon and Breach, 1966.

[Rb, 29] G. Y. Rainich (pseudonym J.L. Rabinowitsch), *Zum Hilbertschen Nullstellensatz*. Math. Ann. **102** (1929), 520

[Ra *et al.*, 75] S. Raghavan, B. Singh, R. Sridharan, *"Homological Methods in Commutative Algebra"*, Tata Institute for Fund. Res., Oxford University Press, 1975.

[Rh, 62] T.S. Rhai, *A characterization of polynomial domians over a field*. Amer. Mathematical Monthly **69** (1962), 984-986.

[Ray, 78] P. Raynaud, *"Anneaux Locaux Henseliens",* Springer LNM, 1978.

[Re, 95] M. Reid, *"Undergraduate Commutative Algebra"*, Cambridge University Press, 1995.

[Ro, 94] H.E. Rose, *"A Course in Number Theory"*.2nd. ed., Oxford Sci. Publications, 1994.

[Shf, 74] I.R. Shafarevich, *"Basic Algebraic Geometry"*, Springer–Verlag, 1974.

[Shp, 00] R.Y. Sharp, *" Steps in commutative algebra"*. Cambridge University Press, 1990, (2nd. Ed. 2000).

[St, 69] V. Strassen, *Gaussian Elimination is not optimal*. Numer. Math. **13** (1969), 354–356.

[St, 73] V. Strassen, *Vermeidung von divisionen*. Crelle J. Reine Angew. Math. **264** (1973), 184–202.

[Wae, 49] B.L. van der Waerden, *"Modern Algebra" (vols. 1 y 2)*. F. Ungar, 194950.

[Wls, 73] J.C. Wilson, *A Principal Ideal Ring that is not a Euclidean Ring*. Mathematics Magazine, **46** (1973), 34–38.

[ZaSa, 60] O. Zariski, P. Samuel, *"Commutative Algebra", vols. I–II*, Van Nostrand, Princeton, 1958,1960.