Estimaciones para el Teorema de Ceros de Hilbert

Sombra, Martín

1998

Tesis presentada para obtener el grado de Doctor en Ciencias Matemáticas de la Universidad de Buenos Aires

Tesis

Presentada para aspirar al Título de

Doctor de la Universidad de Buenos Aires

Estimaciones para el Teorema de Ceros de Hilbert

Martín SOMBRA

Director: Joos HEINTZ

Departamento de Matemática

Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

1998

Estimates for Hilbert's Nullstellensatz

Abstract

We introduce the notion of *height* of an affine variety. This notion extends to general affine varieties the well-known notion of Weil height of a zero-dimensional variety and the notion of height a hypersurface. We obtain an Arithmetic Bézout's Inequality for the intersection of varieties.

We then study the quantitative aspect in the Nullstellensatz. We apply the notion of height of varieties in order to obtain new degree and height bounds for the polynomials in the Nullstellensatz. We also obtain the first affine *sparse* Nullstellensatz. The obtained bounds are essentially optimal in all the cases we consider,

As a consequence of these results, we obtain a lower bound for the diophantine approximation of positive-dimensional varieties.

Key words: Height of Varieties, Arithmetic Bézout's Inequality, Elimination, Nullstellensatz, Hilbert Function.

Resumen

Se introduce una nueva noción de *altura* para variedades afines. Esta noción extiende al caso de una variedad arbitraria la noción de altura de Weil de una variedad de dimensión cero y la noción de altura de una hipersuperficie. Se obtiene una Desigualdad de Bézout Aritmética para la intersección de variedades.

Se estudian luego los aspectos cuantitativos del Teorema de Ceros de Hilbert. La noción de altura de variedades se aplica para obtener nuevas cotas para los grados y para las alturas de los polinomios en el Nullstellensatz. Se obtiene además la primera versión *rala* del Teorema de Ceros afín. En todos los casos las cotas obtenidas son esencialmente optimales para el problema en cuestión.

Como consecuencia de estos resultados, se obtiene ademas una cota inferior para la aproximación diofántica entre variedades de dimensión positiva.

Palabras clave: Altura de Variedades, Desigualdad de Bézout Aritmética, Eliminación, Nullstellensatz, Función de Hilbert.

Índice General

Capítulo 1

Introducción

Muchos resultados centrales de Álgebra Conmutativa y de Geometría Algebraica son resultados de existencia no efectivos. Un ejemplo típico de esta situación es el *Teorema de Ceros* o *Nullstellensatz* de Hilbert.

Bajo una forma simplificada, este resultado dice lo siguiente:

Sean $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ tales que el sistema de ecuacione polinomiales

$$f_1(x) = 0, \ldots, f_s(x) = 0 \qquad (1)$$

no tiene ecuaciones en $\mathbb{C}^n$. El Teorema de Ceros dice entonces que existen polinomios $g_1, \ldots, g_s \in \mathbb{Q}[x_1, \ldots, x_n]$ que satisfacen la identidad

$$1 = g_1 f_1 + \cdots + g_s f_s \qquad (2)$$

Este resultado es una piedra angular de la Geometría Algebraica. Establece un estrecho vínculo entre objeto geométrico — el conjunto solución del sistema de ecuaciones (1) — y un aspecto algebraico — la pertenencia del 1 al ideal generado por $f_1, \ldots, f_s$.

Sin embargo, este es un enunciado meramente existencial que no brinda en principio ningún tipo de información sobre los polinomios $g_1, \ldots, g_s$. Es fundamental para las aplicaciones de este resultado poder estimar, por ejemplo, el grado y el tamaño bit de los coeficientes de los polinomios que aparecen en la identidad de Bézout (2). Esto es particularmente importante en las palicaciones a la Teoría de Números y a la Informática Teórica.

El propósito de esta memoria es el estudio *cuantitativo* del Teorema de Ceros en sus distintos aspectos. Asimismo tratamos también otros problemas relacionados, por ejemplo, estimaciones para la función de Hilbert de ideales homogéneos.

Nuestro esfuerzo está principalmente dirigido hacia los aspectos *aritméticos* de estas cuestiones. A pesar del interés que históricamente, desde Diofanto de Alejandría, ha habido por las cuestiones aritméticas de los sistemas de ecuaciones polinomiales, y del interés actual que existe por sus eventuales aplicaciones a la Informática, éste sigue siendo uno de los aspectos menos desarrollados de la Geometría Algebraica.

Nos proponemos entonces estudiar ciertos análogos aritméticos de algunos conceptos básicos de Geometría Algebraica.

Con este fin introducimos la noción de *altura* de una variedad aritmética y estudiamos sus propiedades, en particular su comportamiento con respecto a intersecciones. Este concepto es el análogo aritmético de la noción clásica de grado de una variedad. En nuestro tratamiento del Teorema de Ceros Aritmético, esta noción juega el rol de la noción de grado.

Como un objetivo de mayor alcance, nos proponemos entonces introducir nuevas técnicas y herramientas básicas que permitan entender y eventulmente resolver los problemas aritméticos en Álgebra Conmutativa y Geometría Algebraica.

En lo que sigue vamos a hacer un resumen de los problemas y de los resultados obtenidos.

Grado y Altura de Variedades. Teorema de Bézout

Un problema clásico de geometría algebraica es el enunciado conocido como Teorema de Bézout. El enunciado tiene la forma siguiente: el grado de la intersección de dos variedades algebraicas es igual al producto de los grados de estas dos variedades, es decir

$$\deg V \cap W = \deg V \cdot \deg W$$

El caso más simple es el de dos curvas planas de grados d y e respectivamente. Newton [108] observó que, si la intersección es finita, las abscisas — por ejemplo — de esta intersección están dadas por una ecuación de grado $d \cdot e$. Este resultado fue gradualmente mejorado durante el siglo XVIII, hasta que Bézout fue capaz de mostrar que, en general, la cantidad de puntos en la intersección de dos curvas planas de grados d y e respectivamente, es exactamente $d \cdot e$ si los puntos se cuentan con propiedad, al menos que tengan infinitos puntos en común.

En términos modernos, sean $C, D \subseteq \mathbb{P}^2(\mathbb{C})$ dos curvas proyectivas sin componentes en común, definidas por ecuaciones homogéneas $F(x, y, z) = 0$ y $G(x, y, z) = 0$ de grados d y e respectivamente. Entonces el teorema de Bézout dice

$$d \cdot e = \sum_{p \in C \cap D} i(C, D, p)$$

donde $i(C, D, p)$ es un entero positivo, la *multiplicidad de intersección*, que mide de alguna forma el orden de contacto entre C y D en el punto p. De hecho, Bézout probó en 1764, no sólo este enunciado, sino también la versión n-dimensional, es decir, el caso de n hipersuperficies en $\mathbb{P}^n$ que se intersectan en una cantidad finita de puntos [18], [19], [20], [21].

El problema consiste entonces en extender el teorema de Bézout al caso general. Con este objeto se introdujeron distintas nociones de grado y de multiplicidad de intersección.

En 1958, Sèrre [120] introdujo una definición de multiplicidad de intersección que le permitió a Iversen [76] demostrar el teorema de Bézout en el caso de una intersección propia, es decir, cuando $\dim V \cap W = \dim V + \dim W - n$ para $V, W \subseteq \mathbb{P}^n$. El teorema de Bézout clásico es un caso particular de este enunciado.

La pregunta natural es si es necesario que la intersección sea propia para que valga la igualdad de Bézout.

El primer resultado general en este sentido es el siguiente: sean $V, W \subseteq \mathbb{A}^n$ variedades afines. Entonces

$$\deg V \cap W \leq \deg V \cdot \deg W$$

Aquí el grado de una variedad irreducible $V \subseteq \mathbb{A}^n$ se define en el sentido clásico como el número de puntos en la intersección de V con la variedad lineal genérica de dimensión complementaria. El grado de una variedad reducible $V \subseteq \mathbb{A}^n$ se define como la suma de los grados de sus componentes irreducibles. Es decir, en esta desigualdad de Bézout no se consideran las multiplicidades de intersección.

En esta forma general, este enunciado fue demostrado por primera vez por Heintz [67] y por Sieveking [123], y publicado en [68] y [69].

Este enunciadofue demostrado también en el contexto proyectivo por Fulton y Mac Phersen [51], [52] y publicado en [50, Proposición 2.3] y en [53, Ejemplo 8.4.6]. En la Subsección 2.2.1 damos la demostración de este resultado, basada en la construcción *ruled join*.

Esta desigualdad de Bézout es una herramienta básica para aplicaciones de la geometría algebraica a otros campos, por ejemplo, a la teoría de números o al cálculo simbólico. De hecho, desigualdades de este tipo para la intersección de una variedad con una hipersuperficie se utilizan desde hace mucho tiempo [92], [128].

Esta desigualdad de Bézout fue posteriormente generalizada y refinada en el contexto de ciclos algebraicos por Fulton [53] y Vogel [136].

Posiblemente esta historia comience antes, y el descubrimiento de la desigualdad de Bézout no sea más que un re–descubrimiento. Sin embargo, la única referencia anterior de la que disponemos en este sentido, es un trabajo de Pieri [114] que considera el caso en que las intersecciones consisten en una componente de dimensión psitiva y puntos.

Posteriormente se han introducido nuevos refinamientos en las nociones de grado e índice de multiplicidad [9], [131], [104], [134]. Estas nociones se introdujeron para estudiar distintos aspectos computacionales en geometría algebraica, por ejemplo, para acotar la regularidad de Castelnuovo de una variedad.

El propósito de la primera parte de esta memoria es la formulación y el esstudio dentro del contexto aritmético de una noción análoga al concepto de grado. Esta es la noción de *altura* de una variedad aritmética.

Nuestro objetivo es contribuir al desarrollo de esta noción para obtener una herramienta básica de fácil uso para la aplicación de la geometría algebraica a otros campos. Nuestra motivación principal son las aplicaciones a la teoría de números y a la informática teórica.

Sea k_0 un cuerpo con fórmula del producto, y sea $k := \overline{k}_0$ su clausura algebraica. El ejemplo básico de un cuerpo con fórmula del producto es $\mathbb{Q}$, o más generalmente, un cuerpo de números, pero también se incluye el caso del cuerpo de funciones racionales de una variedad no–singular en codimensión 1.

Sea $V \subseteq \mathbb{A}^n(k)$ una k_0-variedad afín irreducible de dimensión r. Sea f_V su polinomio de Chow. Este es un pollinomio multi–homogéneo en $r+1$ grupos $U_1, \ldots, U_{r+1}$ de $n+1$ variables con coeficientes en k_0 y está unívocamente definido salvo por múltiplos escalares. Luego consideramos la *altura de Philippon* dada por la fórmula

$$h(V) := \sum_{v \in S_{k_0}} \lambda_v \log M(\sigma_v(f_V)) + \sum_{v \in M_{k_0} - S_{k_0}} \lambda_v \log |f_V|_v$$

donde M_k denota un conjunto propio de valores absolutos sobre k_0 que verifica la fórmula del producto con multiplicidades λ_v, S_{k_0} denota el conjunto de valores absolutos arquimedianos en M_{k_0}. Para $v \in S_{k_0}$, λ_v denota la inclusión correspondiente de k_0 en $\mathbb{C}$, y M la medida de Mahler.

Para una variedad arbitraria $V \subseteq \mathbb{A}^n$ definimos su *altura* como

$$h(V) := \sum_i h(V_i)$$

donde $V = \cup V_i$ es la descomposición de V en componentes irreducibles. Este es un número no negativo.

Sea $f \in \mathbb{Z}[x_1, \ldots, x_n]$ un polinomio separable y primitivo que define una hipersuperficie $V(f) \subseteq \mathbb{A}^n(\mathbb{C})$. luego

$$-2n \deg f \leq h(V(f)) - \log |f| \leq 3(n+1) \log(n+1) \deg f$$

donde $|f|$ denota el máximo de los valores absolutos de los coeficientes de f.

Sea $V \subseteq \mathbb{A}^n(\mathbb{C})$ una $\mathbb{Q}$ -variedad de dimensión 0. Luego

$$0 \leq h(V) - \overline{w}(V) \leq \log(n+1) \deg V$$

donde $\overline{w}$ denota la altura de Weil de V. Esta noción de altura extiende entonces la noción de altura de dimensión positiva.

Existe otra noción de altura de variedades aritméticas equidimensionales $V \subseteq \mathbb{A}^n(\mathbb{C})$ que ha devenido usual en teoría de eliminación algorítmica. Esta noción fue introducida por Giusti et al. [56] y usada, por ejemplo, en [64] y [63], y que ahora vamos a describir: sea r la dimensión de V y sea $\pi : V \to \mathbb{A}^{r+1}$ una proyección lineal. Es bien conocido que si π satisface ciertas condiciones de genericidad entonces $\overline{\pi(V)}$ es una hipersuperficie de $\mathbb{A}^{r+1}$ birracional a V. Luego la inversa $\psi : \overline{\pi(V)} - - \to V$ es una forma débil de parametrización de V, y es lo que se llama una *solución geométrica* de V.

Luego se define la *altura* $\eta(V)$ de V como la altura (logarítmica) de ψ, es decir, (esencialmente) la máxima longitud bits de los coeficientes de ψ.

La noción de solución geométrica es la forma de representar variedades propuesta por Kronecker en 1882 en su trabajo dedicado a Kummer [87] y descripta también por König [82], Macaulay [96] y Zariski [138], entre otros. Esto fue notado recientemente por Pardo [63].

La idea de Kronecker es la más efectiva en informática desde el punto de vista de la complejidad en tiempo y espacio de memoria [57], [58], [49], [85], [59], [56], [99], [105], [64], [63], [71].

Luego la altura $\eta(V)$ acota la longitud bit de los enteros que aparecen en los algoritmos de eliminación. Obtenemos las siguientes estimaciones (Corolario 2.3.14):

$$\eta(V) \leq \delta^2 h(V) + \log(n+1)\delta, \qquad\qquad h(V) \leq 6n^3 d\,\delta^2(\eta(V) + \delta^2)$$

que muestran que la noción de altura que consideramos en esta memoria acota (esencialmente) la altura de una solución geométrica. De hecho, ambas nociones resultan ser esencialmente equivalentes.

La estrecha relación entre la altura de la forma de Chow de una variedad irreducible y sus propiedades aritméticas ya fue notada por Weil [137]. La definición de altura de una variedad aritmética irreducible fue introducida y estudiada en teoría de números en relación con el estudio de criterios para la independencia algebraica por Nesterenko [106] y Philippon [111] [113]. La definición de altura que consideramos fue introducida y estudiada por Philippon en en caso en que k_0 es un cuerpo de números [111] y [113].

Como fue notado por Faltings en su trabajo sobre aproximación diofántica en variedades abelianas [46] la teoría de intersección aritmética puede utilizarse para definir la altura de una variedad aritmética irreducible $V \subseteq \mathbb{P}^n(\mathbb{C})$. Esta noción de altura fue retomada y ligeramente modificada por Bost, Gillet y Soulé [25].

Soulé [127] y Philippon [113] probaron que esta noción de altura es equivalente a la noción de altura que consideramos aquí.

Para la extensión de esta definición al caso de variedades seguimos la noción de grado de Heintz, es decir, no introducimos multiplicidades. La teoría de intersección que resulta es menos general que la de Fulton [53] y la de Vogel [136]. Sin embargo, tiene la ventaja de ser más simple y manejable, y resulta suficiente para la mayoría de las aplicaciones.

Obtenemos distintos resultados para la altura de variedades afines inspirados por la analogía existente entre altura y grado. Por ejemplo, estimamos la altura del producto de variedades (Teorema 2.4.2) y el comportamiento de la altura de una variedad con respecto a morfismos (Lema 2.4.5). También obtenemos un aestimación para la altura de la inversa de un morfismo birracional $\varphi : V \to \mathbb{A}^r$.

Resulta crucial el comportamiento de la altura con respecto a intersecciones. Obtenemos la siguiente *desigualdad de Bézout aritmética* (Teorema 2.4.3):

Teorema 1 *Sean* $V_1, \ldots, V_l \subseteq \mathbb{A}^n$. *Entonces*

$$h(\cap_i V_i) \leq 9n^2 (\prod_i \deg V_i)^4 \sum_i h(V_i)$$

Por otra parte,tanto Bost, Gilet y Soulé como Philippon han obtenido previamente versiones aritméticas del teorema de Bézout para el caso de variedades definidas sobre un cuerpo de números. En una forma simplicada el resultado que obtienen es el siguiente: sean $V, W \subseteq \mathbb{P}^n(\mathbb{C})$ variedades aritméticas.

Entonces

$$h(V \cap W) \leq \deg(W)h(V) + \deg(V)h(W) + c(n)\deg(V)\deg(W)$$

donde $c(n)$ es una constante que depende polinomialmente de n. Esta estimación es mucho más precisa que cualquier resultado contenido en esta memoria. El interés principal de nuestro resultado es su extensión al caso de característica positiva. Resultados similares para el caso $\mathrm{char}(k_0) > 0$ han sido recientemente obtenidos en forma independiente por Chardin y Philippon [38].

Por otra parte, casos particulares de la desigualdad de Bézout aritmético fueron obtenidos por Philippon [111], Krick y Pardo [85] y Faltings [46].

Referimos a los trabajos [93], [140] y [115] para otros aspectos de la teoría de altura de variedades.

Nuestra demostración es completamente algebraica. La idea central consiste en la aplicación formal del método de Newton para la aproximación de raíces de funciones. Esta idea fue aplicada por primera vez en el contexto de la teoría de eliminación por Giusti et al. en [59] y continuada en [56] y [71].

Consiste a grandes rasgos en lo siguiente: sea $\varphi : V \to \mathbb{A}^r$ un morfismo finito y sea $p \in \mathbb{A}^n$ un punto no ramificado de este morfismo. Luego aproximamos la inversa local en un punto $\xi \in \varphi^{-1}(p)$ del morfismo φ, hasta un nivel de aproximación que nos permite recuperar, en un sentido preciso,la variedad V.

Esta idea es conceptualmente simple y a la vez potente. Consiste esencialmente en la aplicación del teorema de la función inversa, y permite obtener propiedades de variedades de dimensión positiva a partir del estudio de una fibra cero-dimensional.

En particular obtenemos una cota para la altura de una variedad intersección completa en términos de la altura de la fibra cero–dimensional de un punto no ramificado con respecto a una proyección lineal (Corolario 2.2.11). Este es el resultado técnico central en nuestra demostración de la desigualdad de Bézout, y es probablemente el aporte original más relevante de esta memoria, en cuanto a la teoría de altura de variedades se refiere.

Teorema de Ceros. Historia

Sea $\mathbb{Q}[x_1,\ldots,x_n]$ el anillo de polinomios en n variables con coeficientes racionales y sea I un ideal de $k[x_1,\ldots,x_n]$.

El famoso Teorema de la Base o Bassatz de Hilbert [73] dice que existen polinomios $f_1,\ldots,f_s \in \mathbb{Q}[x_1,\ldots,x_n]$ tales que $I=(f_1,\ldots,f_s)$.

En términos modernos, el anillo $\mathbb{Q}[x_1,\ldots,x_n]$ es Noetheriano.

En particular todo ideal de $\mathbb{Q}\ [x_1,\ldots,x_n]$ se puede codificar en forma *finita*. Este es entonces el resultado que permite considerar el aspecto de la *efectividad* en álgebra conmutativa.

Un problema básico que se plantea — y tal vez el más inmediato — es el *problema de la pertenencia*: dados $g, f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$ *decidir* si g pertenece o no al ideal generado por $f_1,\ldots,f_s$. Estrechamente ligado a este, está el *problema de la representación*, que en el caso $g\in(f_1,\ldots,f_s)$ consiste efectivamente en *encontrar* polinomios $g_1,\ldots,g_s$ tales que

$$g = g_1\, f_1 + \cdots + g_s\, f_s \qquad (3)$$

Ambos problemas fueron planteados por el propio Hilbert, quien los consideraba como los problemas fundamentales del álgebra conmutativa.

Notamos que una cota para los grados de $g_1,\ldots,g_s$ permite, dados $g_1, f_1,\ldots,f_s$, decidir si la ecuación (3) es soluble o no. En el caso en que lo sea, podemos entonces encontrar *efectivamente* una solución, ya que reduce el sistema original a un sistema de ecuaciones k-lineales.

Luego el problema de la efectividad se tradujo en una primera etapa en el problema de acotar los grados de los polinomios $g_1,\ldots,g_s$.

Este problema fue resuelto por Hermann [72], quien fuera una alumna de Emmy Noether, que probó que $g\in(f_1,\ldots,f_s)$ si y sólo si existen $g_1,\ldots,g_s$ tales que

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

y $\deg g_i\, f_i \le \deg g + 2(1+d^2+\cdots+d^{2^n-1})$, donde d denota el máximo de los grados de $f_1,\ldots,f_s$.

Durante mucho tiempo se trató de mejorar esta cota, hasta que Mayr y Meyer probaron que este problema tiene un carácter intrínseco doblemente exponencial [103], [102].

El caso $g=1$, se tiene $1\in(f_1,\ldots,f_s)$ si y sólo si los polinomios $f_1,\ldots,f_s$ no tienen ceros comunes en $\mathbb{A}^n$. Este enunciado se conoce como el Teorema de Ceros de Hilbert [74], aunque probablemente fuera conocido previamente por Kronecker.

El teorema de ceros está entonces en estrecha relación con el *problema de la consistencia*, que consiste en decidir si la variedad definida por $f_1,\ldots,f_s$ es vacía o no. El teorema de ceros dice que esto pasa si y sólo si existen $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ que satisfacen la identidad de Bézout

$$1 = g_1 f_1 + \cdots + g_s f_s \qquad (4)$$

Keller y Gröbner conjeturaron que en este caso la cota para los grados es simplemente exponencial.

Esta conjetura fue resuelta por Brownawell [26], quien obtuvo la cota $\deg g_i f_i \leq 3n^2 d^n$ en el caso en que k sea un cuerpo de característica cero y por Caniglia, Galligo y Heintz [29] obtuvieron la cota $\deg g_i f_i \leq d^{n^2}$ para el caso en que k es un cuerpo de característica positiva.

Estos resultados fueron mejorados por Kollár [80] y por Fitchas y Galligo [48], quienes obtuvieron la cota

$$\deg f_i g_i \leq \max\{3, d\}^n$$

Esta cota es óptima en el caso $d \geq 3$, debido al conocido ejemplo de Mora, Lazzard, Masser, Philippon y Kollár:

$$f_1 := x_1^d, f_2 := x_1 x_n^{d-1} - x_2^d, \ldots, f_{n-1} := x_{n-2} x_n^{d-1} - x_{n-1}^d, f_n := x_{n-1} x_n^{d-1} - 1$$

En este caso es fácil ver para cualquier sistema de polinomios $g_1, \ldots, g_s$ que verifica (1) se tiene $\deg g_1 \geq d^n$.

Como consecuencia de estos resultados se obtuvo que el teorema de ceros está en la clase de complejidad PSPACE [32], [99], [100]. Recientemente Koiran probó que el teorema de ceros está en la clase Π_2 (módulo la Hipótesis de Riemann Generalizada) [79]. Esto contrasta fuertemente con la complejidad del problema de la pertenencia en el caso general, que por los resultados de Mayr y de Meyer, está en la clase EXPSPACE [103], [102].

Estas versiones efectivas del teorema de ceros tiene como consecuencia que la complejidad de muchos problemas de geometría algebraica computacional es simplemente exponencial: cálculo de la dimensión y del grado de una variedad [57], pertenencia al radical [41], descomposición de una variedad en componentes equidimensionales [58], versiones algorítmicas del teorema de Quillen–Suslin [48], [47].

Siguiendo este punto de vista, se ve que es necesario trabajar con matrices de tamaño $\binom{d^n+n}{n}$, y esto lleva entonces a algoritmos de complejidad d^{n^2}. Luego el punto de vista algorítmico tuvo que diferenciarse de las cotas de grado para poder obtener mejores algoritmos. Este es el punto de vista adoptado en los trabajos [61], [49], etc..

El teorema de ceros es uno de los resultados más básicos de geometría algebraica. Sus diferentes versiones efectivas se aplican en una variedad de situaciones: Lemas de Gelfond multivariados, desigualdades de Lojasiewicz, [77], consistencia sobre cuerpos primos de característica positiva, [64], [63], etc.. Se pueden encontrar otros resultados enlos papers [4], [12], [112], [119], [122] por nombrar unas pocas citas. Referimos a los surveys [11], [109], [132] para una introducción más completa a la historia de este problema, resultados principales y cuestiones abiertas.

Teorema de Ceros. Cotas de Grado

Consideramos en primer lugar las cotas de grado en el teorema de ceros. En este sentido obtenemos progresos sobre todas las cotas de grado conocidas.

Consideramos el teorema de ceros efectivo en su forma clásica. Sea $d_i : \deg f_i$ y supongamos que vale $d_1 \geq \cdots \geq d_s$. Obtenemos la cota de grado (Teorema 3.1.15):

$$\deg g_i f_i \leq 2\, d_s \prod_{j=1}^{\min\{n,s\}-1} d_j$$

Esta cota es interesante en el caso en que los polinomios $f_1, \ldots, f_s$ son cuadráticos. La mejor cota previa para este caso es $\deg g_i f_i \leq n2^{n+2}$ debida a Sabia y Solerno [119]. Nuestra estimación mejora esta cota a $\deg g_i f_i \leq 2^{n+1}$ que está muy cerca de la cota óptima esperada 2^n.

El comportamiento exponencial de las cotas de grado es inevitable, debido al ejemplo de Mora–Lazzard–Masser–Philippon. Sin embargo se ha observado que hay muchas instancias particulares en las cuales esta cota puede ser notablemente mejorada. Este hecho ha motivado la introducción de nuevos parámetros que permitan diferenciar familias especiales de sistemas polinomiales de ecuaciones para las cuales su comportamiento con respecto al problema en cuestión sea polinomial en lugar de exponencial [60], [59].

En este espíritu introducimos entonces un parámetro adicional asociado a un sistema de ecuaciones, su *grado algebraico*. A grandes rasgos, este invariante mide el grado de los ideales generados sucesivamente por $f_1, \ldots, f_s$. Referimos a la Sección 3.1.3 para la definición precisa de este parámetro.

Es el análogo algebraico de la noción de grado geométrico de un sistema de ecuaciones de Giusti et al. [59], Krick, Sabia y Solernó [86] y Sombra [125].

Se han obtenido cotas de grado para los polinomios en el teorema de ceros que dependen principalmente del grado geométrico (Nullstellensätze intrínsecos) [56], [86], [125]. Mostramos aquí que vale una cota similar reemplazando el grado geométrico del sistema polinomial dado por el grado algebraico (Teorema 3.1.17): sea $d := \max_i \deg f_i$ y sea δ el grado algebraico de este sistema polinomial. Obtenemos la cota de grado

$$\deg g_i f_i \leq \min\{n, s\}^2\, d\, \delta.$$

Se tiene la cota de Bézout $\delta(f_1, \ldots, f_s) \leq d^{n-1}$ y por lo tanto deducimos de la cota anterior

$$\deg g_i f_i \leq n^2 d^n,$$

es decir que recuperamos esencialmente las cotas conocidas en términos de d y n. El grado algebraico está acotado por el grado geométrico, y por lo tanto también recuperamos así las cotas conocidas que dependen del grado geométrico para el teorema de ceros. Luego este resultado contiene a todas las cotas de grado conocidas. Sin embargo el grado algebraico es puede ser mucho menor que el grado geométrico en ciertos casos particulares, y por lo tanto también puede ser mucho menor que la cota de Bézout d^{n-1} (Ejemplo 3.1.16). Concluímos entonces que la cota obtenida es mucho más precisa en estos casos que las cotas conocidas.

Teorema de Ceros. Cotas de Esparsitud

Consideramos luego el aspecto ralo o esparso en el teorema de ceros. Vamos a tomar como medida de la esparsitud la noción de *polítopo de Newton.*

Para un polinomio de Laurent $f = \sum_{i\in\mathbb{Z}^n} a_i\, x^i \in k[x_1,\dots,x_n,x_1^{-1},\dots,x_n^{-1}]$. Definimos su *soporte* como el conjunto $\{i : a_i \neq 0\}$, esto es, el conjunto de todos los exponentes de los monomios no nulos de f. Más generalmente, el soporte de una familia de polinomios de Laurent $f_1,\dots,f_s$ está definido como el conjunto de todos los exponentes de los monomios no nulos de todos los f_i.

El *polítopo de Newton* $\mathcal{N}(f_1,\dots,f_s)$ está definido como la cápsula convexa del soporte de $f_1,\dots,f_s$ y su *volumen no mezclado* $\mathcal{U}(f_1,\dots,f_s)$ está definido como $\rho!$ veces el volumen del polítopo $\mathcal{N}(f_1,\dots,f_s)$, donde ρ denota la dimensión de este polítopo.

El grado de un polinomio está acotado por un entero no–negativo d si y sólo si su polítopo de Newton está contenido en $d\cdot\Delta$, donde Δ denota el simplex standard de $\mathbb{R}^n$. Así la noción de polítopo de Newton da una caracterización más precisa de la estructura monomial de un polinomio que el grado. En particular, se pueden obtener cotas para los grados a partir de cotas para el polítopo de Newton. Este concepto fue introducido por Bernshtein [16] y Kushnirenko [88] para obtener versiones más refinadas del teorema de Bézout, y está ahora en la base de la teoría de eliminación esparsa. Dentro de esta teoría se diseñan algoritmos para explotar la esparsitud de los polinomios involucrados, y la esparsitud se mide usualmente en términos del polítopo de Newton de estos polinomios. Este es el punto de vista introducido por Sturmfels [129] y seguido, por ejemplo, en [33], [75], [116], [117], [135] por nombrar unas pocas referencias.

El aspecto esparso en el teorema de ceros también fue considerado por Canny y Emiris, quienes obtuvieron un teorema de ceros esparso efectivo pero sólo para el caso de $n+1$ polinomios de Laurent n–variados *genéricos* [33].

Aquí genérico se interpreta en el siguiente sentido: si uno restringe el soporte de cada f_i a un conjunto fijo $\mathcal{A}_i$ — restringiendo así los monomios que intervienen — el conjunto de coeficientes para los cuales el teorema de ceros de Canny–Emiris *falla* está en una subvariedad de codimensión ≥ 1 del espacio de coeficientes. Esto se deduce fácilmente del hecho de que su demostración depende de que no haya raíces a distancia teórica infinita. Notamos que en el caso en que esta hipótesis de genericidad se verifica, el resultado de Canny–Emiris da cotas al menos tan buenas como cualquier resultado enunciado en esta memoria.

La cuestión del teorema de ceros afín esparso estuvo abierta durante mucho tiempo. Obtuvimos el primer teorema de ceros afín esparso en [126]. Enunciamos este resultado en dos versiones (Teoremas 3.2.1 y 3.2.5).

Teorema 2 *Sean* $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ *polinomios sin ceros comunes en* $\mathbb{A}^n$. *Sea* $\mathcal{N}$ *el polítopo de Newton de los polinomios* $x_1, \dots, x_n, f_1, \dots, f_s$, *y sea* $\mathcal{U}$ *el volumen no mezclado de este polítopo. Entonces existen* $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ *tales que*

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

con $\mathcal{N}(g_i f_i) \subseteq n^{n+3} \mathcal{U}\, \mathcal{N}$ *para* $i = 1, \dots, s$.

Obtenemos un resultado análogo para el caso de polinomios de Laurent.

Teorema 3 *Sean* $f_1, \dots, f_s \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ *polinomios de Laurent sin ceros comunes en* $(\overline{k}^*)^n$. *Sea* $\mathcal{N}$ *el polítopo de Newton de* $f_1, \dots, f_s$, *y sea* $\mathcal{U}$ *el volumen no mezclado de este polítopo. Entonces existen* $a \in \mathbb{Z}^n$ *y* $g_1, \dots, g_s \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ *tales que*

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

con $a \in n^{2n+3} \mathcal{U}^2\, \mathcal{N}$ *y* $\mathcal{N}(g_i f_i) \subseteq n^{2n+3} \mathcal{U}^2\, \mathcal{N} - a$ *para* $i = 1, \dots,$

Sea $d := max_i \deg f_i$. Derivamos directamente del Teorema 3.2.1 la cota de grado

$$\deg g_i f_i \leq n^{n+3}\, d\, \mathcal{U}.$$

Obtenemos que en el peor caso vale la cota $\deg g_i f_i \leq n^{n+2}\, d^{n+1}$, ya que el volumen no mezclado de los polinomios $x_1, \dots, x_n, f_1, \dots, f_n$ está siempre acotado por d^n. Sin embargo nuestra cota de grado mejora considerablemente la cota usual en el caso en que el sistema polinomial de entrada sea esparso y $d \geq n$ (Ejemplo 3.2.4).

La demostración de ambos resultados es similar. Tiene como primer paso la reducción del sistema de ecuaciones original sobre el espacio afín o el toro a un sistema de ecuaciones lineales sobre una variedad tórica adecuada. El sistema resultante se resuelve entonces por aplicación de un Nullstellensatz efectivo para formas lineales en un anillo graduado Cohen–Macaulay (LemaPrincipal 3.1.7).

Como consecuencia se obtiene también un Nullstellensatz efectivo para anillos graduados Cohen–Macaulay que vale no sólo para formas lineales sino también para elementos homogéneos de grado arbitrario (Teorema 3.1.9).

Este lema se demuestra por medio de un argumento *combinatorio*. Consiste esencialmente en un método de deformación que permite reducirse al caso en que las ecuaciones se cortan en forma propia en el hiperplano $\{x_0 = 0\}$, que es un caso mucho más simple que el caso general.

Este es el método con el cual obtenemos las cotas de grado para el teorema de ceros.

Teorema de Ceros. Cotas de Altura

Consideramos el aspecto *aritmético* en el teorema de ceros y junto con algunas de sus consecuencias para la aproximación diofántica.

Sean $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ polinomios sin ceros comunes en $\mathbb{A}^n$. Entonces existen $a \in \mathbb{Z} - \{0\}$ y $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ tales que

$$a = g_1 f_1 + \cdots + g_s f_s$$

Se trata entonces de estimar tanto los grados de los g_i como sus alturas y la altura de a.

Este aspecto es importante en aproximación diofántica, para los así llamados Lemas de Gelfond multivariados, y para el problema de la consistencia sobre cuerpos primos de característica positiva [64], [63].

Sean $d := \max_i \deg f_i$ y $h := \max_i \overline{h}(f_i)$. A partir de la cota de grado conocidas se puede obtener la cota $h(g_i) \leq d^{n^2} h$ por aplicación directa de la regla de Cramer.

El problema fue considerado por primera vez por Berenstein e Yger [13], quienes obtuvieron

$$\deg g_i \leq d^{cn} \qquad\qquad h(g_i) \leq \kappa(n) d^{8n+5} h \qquad\qquad (1)$$

donde c es una constante universal y $\kappa(n)$ sólo depende de n. La demostración está fuertemente basada en técnicas de análisis complejo. Más tarde Krick y Pardo [85] obtuvieron la cota

$$\deg g_i \leq d^{c_1 n} \qquad\qquad h(g_i) \leq d^{c_2 n} h$$

donde $c_1, c_2 \leq 35$ [110].

La demostración es completamente algebraica y se basa en el análisis de la complejidad paralela del teorema de ceros.

Posteriormente Berenstein e Yger [15] mejoraron las cotas de altura y las extendieron al caso de un anillo diofántico [15], aunque la posibilidad de esta extensión ya era clara por los argumentos de Krick y Pardo.

Recientemente se han obtenido análogos aritméticos de Nullstellensatze intrínsecos [64]. Estos resultados están contenidos también en la tesis de Hägele [63].

Nos proponemos estudiar las cotas de altura para el teorema de ceros sobre una variedad.

La situación es análoga a la del Teorema 3.1.9 aunque ahora nos restringimos a una situación menos general aún que la de un anillo Cohen–Macaulay.

Obtenemos el siguiente resultado para el caso de una variedad intersección completa:

Teorema 4 *Sea $F_1, \ldots, F_{n-r} \in \mathbb{Z}[x_1, \ldots, x_n]$ una intersección completa que define una variedad $V := (F_1, \ldots, F_{n-r}) \subseteq \mathbb{A}^n$ de grado δ. Sean $f_1, \ldots, f_s \in \mathbb{Q}[x_1, \ldots, x_n]$ polinomios sin ceros comunes en V. Sean $d := \max_i \deg f_i$, $h := \max_i \overline{h}(f_i)$, $D := \max_i \deg F_i$*

y $H := \max_i \overline{h}(F_i)$. *Entonces existen* $a \in \mathbb{Z} - \{0\}$ *y* $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ *tales que*

$$\overline{a} = \overline{g}_1 \overline{f}_1 + \cdots + \overline{g}_s \overline{f}_s \qquad \in \mathbb{Q}[V]$$

con $\deg g_i \leq 10(n\,\delta\,D\,d^r)^4$ *y* $\overline{h}(a), \overline{h}(g_i) \leq 10(n\,\delta\,D\,d^r)^4(h(V) + H + h)$.

Obtenemos cotas similares para el caso $k[t_1, \ldots, t_m]$ (Teorema 3.3.2), y reobtenemos así el teorema de ceros paramétrico de Smietanski [124].

Para la demostración de este resultado nos basamos en la teoría de dualidad para álgebras de Gorenstein, siguiendo las líneas de Krick y Pardo [85]. Esta técnica ya fue empleada en el contexto del teorema de ceros por [49], [119], por nombrar algunas referencias. En nuestro caso la desigualdad de Bézout aritmética cumple con respecto a las cotas de altura el rol de la desigualdad de Bézout geométrica con respecto a las cotas para los grados, por ejemplo en [119].

Aplicamos este resultado a un problema de aproximación diofántica en variedades para estudiar la relación entre la noción de altura de variedades y sus aspectos *métricos*.

En el caso de una variedad cero–dimensional V, el grado cuenta la cantidad de puntos, y se tiene

$$\log ||V|| := \log(\max_{\xi \in V} ||\xi||) \leq h(V)$$

es decir que la altura acota la distancia al origen (ref).

Sean $V, W \subseteq \mathbb{A}^n$ $\mathbb{Q}$ –variedades disjuntas de dimensión positiva. Tratamos entonces el problema de acotar *inferiormente* la distancia entre V y W.

Sean V, $W \subseteq \mathbb{A}^n$ variedades intersección completa reducida de polinomios $F_1, \ldots, F_{n-r} \in \mathbb{Z}[x_1, \ldots, x_n]$ y $G_1, \ldots, G_{n-s} \in \mathbb{Z}[x_1, \ldots, x_n]$ respectivamente.

Sean $D := \max_i \deg F_i$, $H := \max_i \overline{h}(F_i)$, $d := \max_i \deg f_i$ y $h := \max_i \overline{h}(F_i)$. Entonces

$$\log(\mathrm{Dist}_\alpha(V, W)) \geq -((n \deg V \delta\, D\, d^r)^4(h(V) + H + h) + \log \alpha)$$

Para $\alpha \in \mathbb{R}_{>0}$ sea $\mathrm{Dist}_\alpha(V, W) := \inf \mathrm{Dist}(p, q)$, para $p \in V$ y $q \in W$ y $||p||, ||q|| \leq \alpha$.

Esta es una consecuencia directa de nuestro teorema de ceros sovbre variedades intersección completa. Casos particulares de este problema fueron también considerados por Giusti et al. [56].

Sean $V, W \subseteq \mathbb{A}^n$ variedades equidimensionales. Sean $r := \dim V$, $s := \dim W$, $\delta(V) := \deg V$ y $\delta(W) \deg W$. A partir del resultado anterior se obtiene la cota inferior

$$\log(\mathrm{Dist}_\alpha(V, W)) \geq -((n\,\delta(V)^n\,\delta(W)^n)^4\,(h(V) + h(W)) + \log \alpha)$$

para el caso general (Corolario 3.3.6).

Esta estimación parece estar lejos de la cota optimal. Más allá de los resultados obtenidos, tanto el teorema de ceros aritmético sobre variedades de dimensión positiva parecen seguir abiertos. En la Sección 3.3.3 formulamos una conjetura para el caso general del teorema de ceros aritmético sobre variedades que implicaría cotas optimales para el problema de la distancia entre variedades.

Resultados recientes de Kollár [81] muestran la validez de las cotas de grado propuestas y dan así sustento a esta conjetura.

Función de Hilbert. Cotas

Por último, consideramos el problema de estimar la función de Hilbert de un ideal homogéneo. Sea $I \subseteq k[x_0,\ldots,x_n]$ un ideal homogéneo y sea h_I su función de Hilbert. Entonces existe un polinomio $p_I = a_{r-1}t^{r-1} + \cdots + a_0 \in \mathbb{Q}[t]$ tal que

$$h_I(m) = p_I(m) \qquad\qquad m \gg 0$$

donde r denota la dimensión de Krull de I.

Consideramos el problema de estimar *globalmente* a h_I. Este problema fue considerado por primera vez por Nesterenko [107], quien probó que para un cuerpo k de característica cero y un ideal homogéneo primo $P \subseteq k[x_0,\ldots,x_n]$ de dimensión $r \geq 1$ vale

$$\binom{m+r}{r} - \binom{m-\deg P+r}{r} \leq h_P(m) \leq \deg P(4m)^{r-1} \qquad\qquad m \geq 1$$

Más tarde, Chardin [36] simplificó la demostración de Nesterenko y mejoró su cota superior. Obtuvo la cota

$$h_I(m) \leq \deg I\binom{m+r-1}{r-1} \qquad\qquad m \geq 1$$

para el caso de un cuerpo k perfecto y un ideal radical equidimensional homogéneo $I \subseteq k[x_0,\ldots,x_n]$ de dimensión $r \geq 1$. Esta estimación también fue obtenida por Kollár [36].

En esta dirección, obtenemos una cota inferior para la función de Hilbert de un ideal polinomial homogéneo arbitrario de dimensión $r+1$ (Teorema 4.3.2):

$$h_I(m) \geq \binom{m+r+1}{r+1} - \binom{m-\deg I+r+1}{r+1} \qquad\qquad m \geq 1$$

Obtenemos también una cota superior para la función de Hilbert de una sección genérica por una hipersuperficie f de un ideal $I \subseteq k[x_0,\ldots,x_n]$ homogéneo equidimensional y radical de dimensión $r+1 \geq 2$ (Teorema 4.3.18):

$$h_{(I,f)}(m) \leq 3\, \deg f\, \deg I \binom{m+r-1}{r-1}$$

para $m \geq 5\, r\, \deg I$.

El estudio del comportamiento global de la función del Hilbert de ideales homogéneos está relacionado con diversas cuestiones de álgebra conmutativa efectiva, en relación con la interpolación algebraica [37] y con modificaciones del algoritmo de Buchberger [133], [28], y de la teoría de números trascendentes, en el contexto de los Lemas de Ceros [17].

Capítulo 2

Altura de Variedades Afines

La noción de altura está en la base de toda aplicación de métodos geométricos en Teoría de Números. En este capítulo introducimos la noción dealtura de una variedad de dimensión positiva. Estudiamos sus propiedades básicas, sobre todo su comportamiento con respecto a proyecciones lineales e intersecciones finitas.

En la Sección 2.1 introducimos la noción de cuerpo k con fórmula del producto. Este concepto nos permite tratar de manera unificada los casos de un cuerpo de números y de un cuerpo de funciones. Luego definimos la altura de un polinomio en base a sus alturas locales en cada primo de k.

En la Sección 2.2 introducimos la noción de altura de una variedad como la altura global de su forma de Chow. Asimismo describimos su comportamiento con respecto a intersecciones con variedades lineales y a morfismos lienales.

La parte central de este Capítulo es la Sección 2.3, a pesar de su carácter relativamente técnico. Estudiamos la relación entre altura de una variedad y la altura de una fibra con respecto a una proyección finita (Corolario 2.3.14).

Finalmente, en la Sección 2.4 obtenemos la desigualdad de Bézout aritmética (Teorema 2.4.3) y estimamos la altura de la inversa de un morfismo birracional.

2.1 Altura de Polinomios

Esta sección es esencialmente preliminar. Tiene como propósito introducir las nociones básicas de toería de números que vamos a necesitar en las secciones siguientes, de fijar la notación. Todo el material incluído es perfectamente clásico. Nuestra presentación sigue los libros de Lang [92] y [90], y el trabajo de Philippon [111].

Introducimos la noción de cuerpo con fórmula del producto, junto con los principales ejemplos que vamos a considerar, el de un cuerpo de números y el de un cuerpo de funciones.

Luego introducimos las alturas locales de un polinomio, definiéndolas en base a la medida de Mahler en el caso arquimediano. Luego introducimos distintas definiciones de altura de un polinomio, en base a estas alturas locales.

2.1.1 Valores Absolutos

Sea k un cuerpo. Un *valor absoluto* v es una función real $x \mapsto |x| = |x|_v$ sobre k que satisface las siguientes propiedades:

1. Se tiene $|x| \geq 0$, y $|x| = 0$ si y sólo si $x = 0$.
2. $|xy| = |x||y|$ para todo $x, y \in k$.
3. $|x + y| \leq |x| + |y|$.

En el caso en que v satisface en lugar de 3. La condición más fuerte $|x+y| \leq \max\{|x|, |y|\}$ se dice que es *no-arquimediano.* Si $\mathrm{char}(k) = p > 0$ se tiene $|x + y| = |(x + y)^{p^N}|^{1/p^N} \rightarrow \max\{|x|, |y|\}$, es decir que $|\cdot|$ es no-arquimediano.

El valor absoluto definido como $|x| = 1$ para todo $x \neq 0$ se llama *trivial.*

Un valor absoluto define una métrica, y por lo tanto una topología. Dos valores absolutos se dicen *dependientes* si definen la misma topología, y se dicen *independientes* en caso contrario.

Sea k un cuerpo con un valor absoluto no trivial v. Denotamos por k_v la *completación* de k con respecto a v. El cuerpo k es denso en k_v, e induce un valor absoluto en k_v que extiende al valor absoluto de k y que también denotamos por v. El cuerpo k_v es único con esta condición, salvo isomorfismo.

En el caso en que el valor absoluto arquimediano se tiene $\mathrm{char}(k) = 0$. La restricción de v a $\mathbb{Q}$ es entonces dependiente del valor absoluto ordinario [6, 1.5], por lo tanto k_v es el cuerpo de los números reales o el de los números complejos y v es el valor absoluto ordinario. Esta es una consecuencia del teorema de Gelfand–Mazur [91, XII.2].

Supongamos ahora que k es completo con respecto a un valor absoluto v. Sea E una extensión algebraica de k. Entonces v tiene una única extensión a E.

Sea $\alpha \in E$ y sea $n := [k(\alpha) : k]$. Entonces

$$|\alpha| = |N_k^{k(\alpha)}(\alpha)|^{1/n},$$

donde $N_k^{k(\alpha)}$ denota la *norma* si además E es finita entonces E es completo.

Sea ahora k un cuerpo con un valor absoluto no trivial v. Vamos a describir cómo se extiende este valor absoluto a extensiones finitas de k.

Sea k_v la completación de k. Luego v se extiende en forma única a k_v, y por lo tanto también se extiende en forma única a su clausura algebraica $\overline{k}_v$.

Sea E una extensión finita de k y sea $\sigma : E \to \overline{k}_v$ una k-inmersión. Luego σ induce un valor absoluto w sobre E que extiende a v. Sea E_w la completación de E. Luego $E_w = Ek_v$.

Toda extensión de v a E está dada por una k-inmersión de E en $\overline{k}_v$. Dos k-inmersiones $\sigma, \tau : E \to \overline{k}_v$ dan lugar al mismo valor absoluto en E si y sólo si son conjugadas sobre k_v. En el caso en que E es puramente inseparable existe una única extensión de v a E.

Sea w una extensión de v a E. Notamos esto por $w|v$.

Definimos el *grado local* de E sobre k en w como

$$n_w := [E_w : k_v].$$

En el caso en que E es finita y separable se tiene

$$\sum_{w|v} n_w = [E : k]$$

y se tiene además $N_k^E(\alpha) = \prod_{w|v} N_{k_v}^{E_w}(\alpha)$. Luego

$$\sum_{w|v} n_w \log |\alpha|_w = \log N_k^E(\alpha)$$

para $\alpha \in E^*$.

Ahora vamos a considerar *familias* de valores absolutos sobre un cuerpo. Un conjunto M_k de valores absolutos sobre k se dice *propio* si todos sus valores absolutos son no triviales, independientes entre sí y si, dado $x \in k^*$ entonces $|x|_v = 1$ para casi todo $v \in M_k$. Esta definición extiende ligeramente la definición de Lang [92, 2.1].

En particular, si M_k es propio entonces contiene a lo sumo un número finito de valores absolutos arquimedianos. El conjunto de valores arquimedianos en M_k se denota por S_k y se llama el conjunto de *valores absolutos en el infinito.*

Sea M_k un conjunto propio de valores absolutos sobre k. Para cada $v \in M_k$, sea λ_v un número real positivo. Se dice que M_k satisface la *fórmula del producto con multiplicidades* λ_v si para todo $\alpha \in k^*$ se tiene

$$\prod_{v \in M_k} |\alpha|_v^{\lambda_v} = 1.$$

Por hipótesis existe a lo sumo un número finito de factores en este producto que no son iguales a 1, y por lo tanto el producto está bien definido. Equivalentemente

$$\sum_{v \in M_k} \lambda_v \log |\alpha|_v = 0$$

en notación aditiva. En este caso se dice que k es un *cuerpo con fórmula del producto* o un *FP-cuerpo*. Se dice que M_k satisface la *fórmula del producto* si $\lambda_v = 1$ para todo v.

Sea k un cuerpo con un conjunto propio M_k de valores absolutos que satisface la fórmula del producto con multiplicidades λ_v. Sea E una extensión finita de k y sea M_E el conjunto de valores absolutos sobre E que extienden a los valores absolutos de M_k. Es fácil verificar que M_E es también un conjunto propio de valores absolutos.

Queremos ver que M_E satisface también la fórmula del producto. Sea $H \subseteq E$ una subextensión separable maximal de k. Se tiene entonces la torre de extensiones $k \subseteq H \subseteq E$, donde $k \subseteq H$ es separable y $H \subseteq E$ es puramente inseparable. Sean $n := [E : k]_s = [H : k]$ y $p^r := [E : k]_i := [E : H]$ el grado de separabilidad y el grado de inseparabilidad de E sobre k, respectivamente.

Sea v un valor absoluto en M_k y sea w una extensión de v a E. Luego $k_v \subseteq H_w$ es separable y $H_w \subseteq E_w$ es puramente inseparable. Sea $n_w := [E_w : k_v]_s = [H_w : k_v]$, que coincide con la noción de grado local en el caso en que E es separable. Se tiene

$$\log |N_k^E(\alpha)|_v = \log |N_k^H(\alpha^{p^r})|_v = p^r \sum_{w \in M_E : w|v} n_w \log |\alpha|_w$$

ya que hay una correspondencia unívoca entre M_E y M_H. Luego

$$\sum_{v \in M_k} \sum_{w|v} \lambda_v \, p^r \, n_w \log |\alpha|_w = \sum_{v \in M_k} \lambda_v \log |N_k^E(\alpha)|_v = 0$$

para $\alpha \in E^*$, por la fórmula del producto en M_k. Luego M_E satisface la fórmula del producto con multiplicidades $\mu_w := \lambda_v [E_w : k_v]_s / n$.

Sea $k \subseteq E \subseteq F$ una torre de extensiones. Sea $v \in M_k$ y sean $w \in M_E$ y $z \in M_F$ valores absolutos tales que $z|w$ y $w|v$. Sean λ_v, μ_w y ν_z las multiplicidades de v, w y z respectivamente. Luego se verifica $\nu_z = \lambda_v \cdot \mu_w$ por la multiplicatividad del grado de separabilidad.

En adelante vamos a asumir que las multiplicidades están *normalizadas* de forma tal que $\sum_{v \in S_k} \lambda_b = 1$ y $\sum_{w/v} \mu_w = \lambda_v$.

2.1.2 Cuerpos de Números

El ejemplo clásico de un cuerpo con fórmula del producto es el de los números racionales $\mathbb{Q}$. Consideramos el conjunto propio M_Q de valores absolutos formado por el valor absoluto ordinario y los valores absolutos p-ádicos.

El *valor absoluto p-ádico* se define para cada primo $p \in \mathbb{Z}$ por la fórmula

$$|p^r m/n|_p := 1/p^r,$$

donde r es un entero y m, n son enteros no nulos no divisibles por p.

Todo valor absoluto sobre $\mathbb{Q}$ es dependiente de alguno de estos valores absolutos (Teorema de Ostrowski) [6, 1.5].

Si q es un primo entonces

$$\begin{aligned} |q|_p &= \begin{cases} 1 & \text{si} \quad p \neq q \\ 1/q & \text{si} \quad p = q \end{cases} \\ |q|_\infty &= q \end{aligned}$$

Luego M_Q satisface la fórmula del producto. Este argumento lo muestra para primos de $\mathbb{Z}$ y el caso general se sigue por multiplicatividad.

Para un cuerpo de números k, el conjunto M_k de valores absolutos que extienden a los valores absolutos de M_Q se llama el *conjunto canónico.* Luego M_k satisface la fórmula del producto con multiplicidades $\lambda_v := [k_v : \mathbb{Q}_p]$, donde $v \in M_k$ es un valor absoluto que extiende al valor absoluto p-ádico $|\cdot|_p$.

2.1.3 Cuerpos de Funciones

Sea k un cuerpo algebraicamente cerrado. Sea $V \subseteq \mathbb{P}^n$ una variedad proyectiva irreducible y sea $k(V)$ su cuerpo de funciones racionales.

Asumimos que V es *no-singular en codimensión 1*, es decir que toda subvariedad de codimensión 1 contiene al menos un punto regular de V. Este es el caso por ejemplo si V es no–singular, o más generalmente si es normal.

Sea $W \subseteq V$ una subvariedad irreducible de codimensión 1. Es un hecho básico de geometría algebraica que el anillo local $\mathcal{O}_W$ de W en $k(V)$ es un anillo de valuación discreta [7, Proposición 9.2].

Para $f \in k(V)^*$ notamos por ord_W el *orden* de f en W, es decir su orden en el anillo local $\mathcal{O}_W$.

Asociamos a W un valor absoluto no–arquimediano $|\cdot|_W$ definido como

$$|f|_W := e^{(-\mathrm{ord}_W f) \deg W}$$

para $f \neq 0$ y $|0|_W := 0$, donde $\deg W$ denota el *grado* de W el número de puntos de la intersección de W con una variedad lineal genérica de dimensión complementaria (Subsección 2.2.1).

Sea entonces $K := k(V)$ y sea M_K el conjunto de estos valores absolutos. Es un hecho elemental que este conjunto es un conjunto propio de valores absolutos, y *satisface la fórmula del producto* gradias a la relación $\sum_W \mathrm{ord}_W f \ \deg W = 0$ [66, II.6.4].

Esta fórmula del producto se puede escribir como

$$\prod_W |x|_W = 1,$$

ya que hay una biyección entre hipersuperficies irreducibles de V y valores absolutos en M_K.

Entendemos por un *cuerpo de funciones* K sobre un cuerpo de constantes k — no necesariamente algebraicamente cerrado — al cuerpo de funciones racionales $K := k(V)$ de una variedad irreducible $V \subseteq \mathbb{P}^n$ definida sobre k y no–singular en codimensión 1.

Determinamos ahora el conjunto de valores propios de K junto con sus multiplicidades. Toda hipersuperficie irreducible W de V induce un valor absoluto $|\cdot|_W$ sobre $\overline{k}(V)$ y por lo tanto induce un valor absoluto sobre $k(V)$ por restricción.

Dos hipersuperficies irreducibles W_1, $W_2 \subseteq V$ definen el mismo valor absoluto sobre $k(V)$ si y sólo si son conjugadas sobre k.

Luego tomamos a M_K el conjunto de valores absolutos $|\cdot|_W$, donde W recorre un sistema de representantes de las clases de conjugación de varias hipersuperficies irreducibles de V. Por lo anterior, este es un conjunto propio de valores absolutos sobre K, y satisface la fórmula de producto con multiplicidades λ_W, donde λ_W es el orden de la clase de conjugación de W.

Notamos que en este caso todos los valores absolutos en M_K son no–arquimedianos.

2.1.4 Alturas Locales

Sea k un FP-cuerpo, M_k un conjunto propio de valores absolutos que satisface la fórmula del producto con multiplicidades λ_v, y sea S_k el conjunto de valores absolutos arquimedianos en M_k. Para cada valor absoluto $v \in M_k$ denotamos por k_v la completación de k con respecto a v y por σ_v la inmersión canónica de k en k_v.

Sea P un polinomio en $k[x_1, \ldots, x_n]$. Definimos una *altura local* o *medida de Mahler local* $M_v(P)$ de P en v de la siguiente forma:

1. Si $v \notin S_k$, $M_v(P)$ es el máximo de los valores absolutos de los coeficientes de $\sigma_v(P)$.
2. Si $v \in S_k$ se tiene $k_v = \mathbb{R}$ ó $k_v = \mathbb{C}$. Luego $M_v(P)$ es la *medida de Mahler* de $\sigma_v(P)$, que se define como

$$M_v(P) = M(\sigma_v(P)) := \exp(\int_0^1 \cdots \int_0^1 \log|\sigma_v(P)(e^{2i\pi t_1}, \ldots, e^{2i\pi t_n})| dt_1 \cdots dt_n)$$

   para $P \neq 0$ y $M_v(0) := 0$. La función $\log|\sigma_v(P)|$ es integrable [118] y por lo tanto $M_v(P) = 0$ si y sólo si $P = 0$.

Alternativamente vamos a usar la medida de Mahler logarítmica, es decir $m_v(P) := \log M_v(P)$.

La medida de Mahler fue introducida por Lehmer [95] para el caso de un polinomio univariado $P = a_d \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{C}[x]$ en la forma

$$M(P) := |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$$

La igualdad entre las dos expresiones se deduce de la fórmula de Jensen. El caso general fue introducido y estudiado por Mahler [97].

La propiedad fundamental de estas alturas locales es su *multiplicatividad.* Se tiene

$$M_v(P\,Q) = M_v(P) \cdot M_v(Q)$$

para $P, Q \in k[x_1, \ldots, x_n]$. En el caso arquimediano esto se sigue directamente de la definición de la medida de Mahler, mientras que en el caso no–arquimediano se sigue del lema de Gauss.

Consideramos también la *altura local absoluta* que definimos como $\overline{m}_v(P) := \max\{0, m_v(P)\}$ para $P \in k[x_1, \ldots, x_n]$.

Sea $\mathcal{A} \subseteq k$ un conjunto finito. Luego definimos su valor absoluto (logarítmico) como *altura ordinaria* como $H_v(\mathcal{A}) := |\mathcal{A}|_v = \max_{a \in \mathcal{A}}\{|a|_v\}$. Asimismo consideramos su *altura logarítmica (ordinaria)* $h_v(\mathcal{A}) := \log H_v(\mathcal{A})$ y su *altura logarítmica absoluta* $\overline{h}_v(\mathcal{A}) := \max\{0, h_v(\mathcal{A})\}$.

Introducimos además otra medida para polinomios complejos, su *longitud*, que se define como

$$L(P) := \sum |a_i|$$

para $P = \sum a_i x^i \in \mathbb{C}[x_1, \ldots, x_n]$ y la *longitud logarítmica* $l(P) := \log L(P)$. Estas medidas están relacionadas [111], se tiene

$$M(P) \leq L(P) \leq (n+1)^{\deg P} M(P)$$

Se tiene $L(P+Q) \leq L(P) + L(Q)$ y por lo tanto

$$\begin{array}{rcll} M_v(P+Q) & \leq & M_v(P)(n+1)^{\deg P} + M_v(Q)(n+1)^{\deg Q} & v \in S_k \\ M_v(P+Q) & \leq & \max\{M_v(P), M_v(Q)\} \qquad v \notin S_k & \end{array}$$

Análogamente, se tiene la estimación

$$l(P_1 \cdots P_k) \leq \sum l(P_i) + \log(n+1) \sum \deg P_i$$

Se tiene la relación

$$\begin{array}{rcll} m_v(P) - \deg P - n \leq h_v(P) & \leq & m_v(P) + \deg P \log(n+1) & v \in S_k \\ h_v(P) & = & m_v(P) \qquad v \notin S_k & \end{array}$$

El siguiente lema técnico nos permite controlar el comportamiento de la altura local con respecto a la composición.

Lema 2.1.1 *Sean $f \in k[t_1, \ldots, t_m]$ y $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$. Sean $\deg g := \max_i \deg g_i$ y $\overline{m}_v(g) := \max_i \overline{m}_v(g_i)$. Sea $F \in k[x_1, \ldots, x_n]$ el polinomio dado por la composición de f con $g_1, \ldots, g_m$, es decir*

$$F := f(g_1, \ldots, g_m)$$

Entonces

$$\begin{aligned} m_v(F) &\leq m_v(f) + \deg f \cdot \overline{m}_v(g) + \deg f(\log(n+1) + \deg g \log(n+1)) \qquad v \in S_k, \\ m_v(F) &\leq m_v(f) + \deg f \cdot \overline{m}_v g \qquad v \notin S_k. \end{aligned}$$

Demostración. Sean $d := \deg f$ y $D := \deg g$. Sea $i = (i_1, \ldots, i_m) \in \mathbb{N}^m$ y $g := (g_1, \ldots, g_m)$. Consideramos en primer lugar el caso $v \in S_k$.

Se tiene $\overline{m}_v(g^i) \leq |i| \cdot \overline{m}_v(g)$. Luego $l(g^i) \leq d\,\overline{m}_v(g) + d\,D \log(n+1)$ para $|i| \leq d$ y por lo tanto

$$\begin{aligned} m_v(F) &\leq l(F) \leq l(f) + d\,\overline{m}_v(g) + d\,D\log(n+1) \\ &\leq m_v(f) + d\log(m+1) + d\,\overline{m}_v(g) + d\,(D+1)\log(n+1). \end{aligned}$$

El caso $v \notin S_k$ se sigue en forma parecida.

□

En particular, sean $f := \det(t_{ij}) \in k[(t_{ij})]$ y $g_{ij} \in k[x_1, \ldots, x_n]$. Luego

$$\begin{aligned} m_v(F) &\leq m\,\overline{m}_v(g) + m((d(g)+1)\log(n+1) + \log m) \qquad v \in S_k, \\ m_v(F) &\leq m\,\overline{m}_v(g) \qquad v \notin S_k, \end{aligned}$$

ya que $m_v(f) \leq l(f) \leq m \log m$ para $v \in S_k$ y $m_v(f) = 0$ para $v \notin S_k$.

Consideramos también el caso en que $t_1, \ldots, t_m$ son *grupos* de variables. Sean $t_i = (t_1, \ldots, t_{ik})$. Sean $g_{ij} \in k[x_1, \ldots, x_n]$, $g_i := (g_{i1}, \ldots, g_{ik})$ y sea $F := f(g_1, \ldots, g_m)$. Luego se tiene

$$\begin{aligned} m_v(F) &\leq m_v(f) + \textstyle\sum_{i=1}^m \deg_{t_i} f \cdot (\overline{m}_v(g_i) \\ &\quad + \textstyle\sum_{i=1}^m \deg_{ti} f(\log(k\,m+1) + \deg g \log(n+1)) \qquad v \in S_k \\ m_v(F) &\leq m_v(f) + \textstyle\sum_{i=1}^m \deg_{t_i} f \cdot (\overline{m}_v(g_i) \qquad v \notin S_k, \end{aligned}$$

donde $\deg_{ti} f$ denota el grado en el grupo de variables t_i. Esta estimación es más conveniente que el Lema 2.1.1 en algunas situaciones, y la utilizaremos ocasionalmente.

2.1.5 Alturas Globales

Sea k un FP-cuerpo con un conjunto propio de valores absolutos M_k que satisface la fórmula del producto con multiplicidades λ_v.

Sea P un polinomio en $k[x_1, \ldots, x_n]$. Se define la *altura invariante* o *medida de Mahler invariante* de P como

$$m(P) := \sum_v \lambda_v \, m_v(P)$$

para $P \neq 0$ y $m(0) := 0$. Esta noción fue introducida por Philippon [111, Definición 1.1.1].

Esta noción se puede extender a una extensión finita E de k. Sea M_E el conjunto de los valores absolutos sobre E que extienden a los valores absolutos en M_k. Sean μ_w las multiplicidades de M_E. Asumimos que estas multiplicidades están normalizadas de forma tal que vale

$$\sum_{w|v} \mu_w = \lambda_v.$$

Luego definimos de forma análoga $m(P) := \sum_w \mu_w \, m_w(P)$ para $P \in E[x_1, \ldots, x_n] - \{0\}$.

Por la normalización impuesta sobre las multiplicidades μ_w, esta última expresión no depende del cuerpo de E. Esto permite prolongar la función m al anillo de polinomios $\overline{k}[x_1, \ldots, x_n]$, y de esta forma nos podemos independizar del cuerpo de definición de los objetos — variedades y polinomios — con las que trabajamos.

Análogamente definimos la *altura absoluta* de P como $\overline{m}(P) := \sum \lambda_v \, \overline{m}_v(P)$.

Se tiene $m(\lambda P) = m(P)$ para $\lambda \in k^*$ por la fórmula del producto. Esta propiedad es la que justifica el nombre de invariante para la altura de m. Esta noción de altura satisface además

$$m(PQ) = m(P) + m(Q)$$

para $P, Q \neq 0$, por la multiplicatividad de las alturas locales. Otra propiedad importante de m es su *positividad*, es decir $m(P) \geq 0$ [111, 1.12].

Se tiene $m(P) \leq \overline{m}(P)$ para todo P, y además existe $\lambda \in k^*$ tal que $m(P) = \overline{m}(\lambda P)$ [111].

Estas propiedades hacen conveniente el uso de la altura invariante. Para el caso de un conjunto finito $\mathcal{A} \subseteq k$ introducimos su *altura de Weil (invariante)*, que se define como $h(\mathcal{A}) := \sum \lambda_v \, h_v(\mathcal{A})$. Análogamente introducimos la *altura de Weil (absoluta)* de $\mathcal{A}$ como $\overline{h}(\mathcal{A}) := \sum \lambda_v \, \overline{h}_v(\mathcal{A})$. Vamos a utilizar estas nociones, por ejemplo, para el caso de una familia finita de polinomios o de funciones racionales.

Estas nociones están relacionadas por

$$m(P) - \deg P - n \leq h(P) \leq m(P) + \log(n+1) \deg P$$

Sean $f \in k[t_1, \ldots, t_m]$ y $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$. Sea $F := f(g_1, \ldots, g_m)$. Del Lema 2.1.1 obetenemos

$$m(F) \leq m(f) + \deg f(\log(m+1) + \deg g \log(n+1))$$

Supongamos que k es el cuerpo de fracciones de un anillo factorial A. Este es el caso, por ejemplo, si k es el cuerpo de los números racionales o el cuerpo de funciones racionales n-variadas sobre un cuerpo de constantes dado. Sea M_A el conjunto de valores absolutos no-arquimedianos en M_k asociados a los elementos irreducibles de A y sea $S_A := M_k - M_A$. Sea $P \in A[x_1, \ldots, x_n]$ un polinomio primitivo. Luego $|P|_v = 1$ para todo $v \in M_A$ y por lo tanto

$$m(P) = \sum_{v \in S_A} \lambda_v \, m_v(P)$$

En el caso $A := \mathbb{Z}$ el conjunto S_A consiste sólo en el valor absoluto ordinario. Luego

$$m(P) = \log M(P)$$

para un polinomio primitivo $P \in \mathbb{Z}[x_1, \ldots, x_n]$. Análogamente $h(\mathcal{A}) = \log |\mathcal{A}| = \max_{a \in \mathcal{A}} |a|$ si para un conjunto primitivo $\mathcal{A} \subseteq \mathbb{Z}$.

En el caso $A := k[t_1, \ldots, t_m]$ el conjunto S_A consiste en el valor absoluto que corresponde al hiperplano del infinito $\{t_0 = 0\} \subseteq \mathbb{P}^m$. Luego

$$m(P) = h(P) = \deg_t P$$

para un polinomio primitivo $P \in k[t_1, \ldots, t_m][x_1, \ldots, x_n]$, donde $\deg_t P$ denota el grado de P en las variables $t_1, \ldots, t_m$.

2.2 Altura de Variedades

Esta Sección está dedicada a la definición de altura de variedades afines y a la derivación de sus propiedades más inmediatas.

En una primera parte nos dedicamos a los preliminares de carácter geométrico–algebraico. Introducimos la noción de grado de una variedad junto con sus propiedades básicas. Luego introducimos la forma de Chow de una variedad afín. Este es el objeto clásico arquetípico de teoría de eliminación.

Nos permite definir la altura de una variedad en base a la altura de este polinomio.

2.2.1 Grado

Introducimos primero la noción de grado para variedades irreducibles y luego la extendemos al caso general. Adoptamos aquí el punto de vista de Heintz [69].

Sea k un cuerpo algebraicamente cerrado y $V \subseteq \mathbb{A}^n$ una variedad irreducible de dimensión r. Consideramos el morfismo $\varphi : \mathbb{A}^{rn} \times V \to \mathbb{A}^{rn} \times \mathbb{A}^r$. Identificamos a $\mathbb{A}^{rn}$ con la variedad de las $r \times n$-matrices con coeficientes en k y definimos $\varphi(G, x) := (G, Gx)$

para $G \in \mathbb{A}^{rn}$ y $x \in V$. La fibra $\varphi^{-1}(G,b)$ de un elemento $(G,b) \in \mathbb{A}^{rn} \times \mathbb{A}^r$ corresponde a la intersección de V con los r hiperplanos afines definidos por (G,b).

La aplicación φ es dominante y la extensión $k(\mathbb{A}^{rn} \times \mathbb{A}^r) \hookrightarrow k(\mathbb{A}^{rn} \times V)$ es finita y separable [69]. Se tiene

$$\#\varphi^{-1}(G,b) \leq [k(\mathbb{A}^{rn} \times V) : k(\mathbb{A}^{rn} \times \mathbb{A}^r)]$$

para todo $(G,b) \in \mathbb{A}^{rn} \times \mathbb{A}^r$ con fibra finita y genéricamente vale la igualdad [69].

Sea $V \subseteq \mathbb{A}^n$ variedad irreducible, con $r = \dim V$. Luego el *grado* de V se define como

$$\begin{aligned} \deg V : &= [k(\mathbb{A}^{rn} \times V) : k(\mathbb{A}^{rn} \times \mathbb{A}^r)] \\ &= \sup\{\# V \cap H_1 \cap \cdots \cap H_r : H_1, \ldots, H_r \text{ hiperplanos afines} \\ &\qquad \text{de } \mathbb{A}^n \text{ tales que } V \cap H_1 \cap \cdots \cap H_r \text{ es finita }\}. \end{aligned}$$

Sea $V \subseteq \mathbb{A}^n$ una variedad y sea $V = \cup_i V_i$ su descomposición en componentes irreducibles. Entonces se define el grado de V como

$$\deg V := \sum_i \deg V_i.$$

El grado es siempre un entero positivo, y se verifica fácilmente que $\deg V = 1$ si y sólo si V es una variedad lineal. El grado de una hipersuperficie es igual al grado de cualquier generador de su ideal de definición. El grado de una variedad finita es su cardinal.

Para un morfismo lineal $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ y una variedad $V \subseteq \mathbb{A}^n$ se tiene $\deg \overline{\varphi(V)} \leq \deg V$.

El aspecto básico del grado es su comportamiento con respecto a intersecciones. La noción de grado introducida verifica la *desigualdad de Bézout* [69]. Se tiene

$$\deg V \cap W \leq \deg V \cdot \deg W$$

para $V, W \subseteq \mathbb{A}^n$ sin restricciones sobre el tipo de intersección. Con respecto al producto se tiene $\deg V \times W = \deg V \cdot \deg W$.

Sea $V \subseteq \mathbb{A}^n$ y sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Sea $d_i := \deg f_i$ y supongamos que vale $d_1 \geq \cdots \geq d_s$, y sea $r := \dim V$. Como consecuencia de la desigualdad de Bézout se tiene

$$\deg V \cap \{f_1 = 0, \ldots, f_s = 0\} \leq \deg V \prod_{i=1}^{r} d_i.$$

Otra consecuencia de la desigualdad de Bézout es la siguiente estimación para la imagen de una variedad por una aplicación racional. Es una variante de [70, Lema 1] y [119, Proposición 1].

Lema 2.2.1 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ una aplicación racional y sea $V \subseteq \mathbb{A}^n$ una variedad de dimensión r. Sean $f_i, g_i, \in k[x_1, \ldots, x_n]$ polinomios tales que $\varphi = (f_1/g_1, \ldots, f_m/g_m)$. Sea $d_i := \max\{\deg f_i, \deg g_i + 1\}$ y supongamos que vale $d_1 \geq \cdots \geq d_m$. Entonces $\deg \overline{\varphi(V)} \leq \deg V \prod_{i=1}^r d_i$.*

Demostración. Sea $\mathrm{Gr}\varphi$ el gráfico de φ. Luego

$$\mathrm{Gr}\varphi = V \cap \{g_1 \cdot y_1 - f_1, \ldots, g_m \cdot y_m - f_m\} \subseteq \mathbb{A}^n \times \mathbb{A}^m$$

y por lo tanto $\deg \mathrm{Gr}\varphi \leq \deg V \prod_{i=1}^{s} d_i$ donde $s := \dim \overline{\varphi(V)}$. Sea $\pi : \mathbb{A}^n \times \mathbb{A}^m \to \mathbb{A}^m$ la proyección $(x, y) \mapsto y$. Luego $\varphi(V) = \pi(\mathrm{Gr}\varphi)$ y así $\deg \overline{\varphi(V)} \leq \deg \mathrm{Gr}(V)$, de donde se deduce la cota anunciada. □

También se obtiene una cota para los grados de los polinomios que definen la inversa de un morfismo birracional de una variedad en un espacio afín.

Lema 2.2.2 *Sea $V \subseteq \mathbb{A}^n$ y $\varphi : V \to \mathbb{A}^r$ un morfismo birracional. Sean $f_i, g_i \in k[x_1, \ldots, x_n]$ tales que $\varphi = (f_1/g_1, \ldots, f_m/g_m)$. Sea $\psi := \varphi^{-1} = (h_1/k_1, \ldots, h_n/k_n)$ con $h_i, k \in k[x_1, \ldots, x_n]$ sin factores comunes. Sea $d_i := \max\{\deg f_i, \deg g_i + 1\}$. Entonces*

$$\deg h_i/k_i := \max\{\deg h_i, \deg k_i\} \leq \deg V \prod_{i=1}^{r} d_i.$$

Demostración. Se tiene

$$\overline{\mathrm{Gr}\psi} = \{k_1 x_1 - h_1, \ldots, k_n x_n - h_n\} \subseteq \mathbb{A}^r \times \mathbb{A}^n$$

y por lo tanto $V(k_i x_i - h_i) = \pi_i(\mathrm{Gr}\,\psi)$ donde $\pi_i : \mathbb{A}^r \times \mathbb{A}^n \to \mathbb{A}^{r+1}$ es la proyección $(y, x) \mapsto (y, x_i)$. Luego

$$\deg(k_i x_i - h_i) \leq \deg \mathrm{Gr}\,\psi \leq \deg V \prod_{i=1}^{r} d_i$$

ya que $k_i x_i - h_i$ es irreducible y el gráfico de ψ coincide con el de φ. □

Esta noción de grado se extiende también al caso de una variedad proyectiva. Sea $V \subseteq \mathbb{P}^n$ una variedad irreducible. El *grado* $\deg V$ de V se define como la cantidad de puntos en la intersección de V con una variedad lineal de dimensión complementaria, y se extiende igual que antes al caso de una variedad eventualmente reducible. El grado de una variedad afín $V \subseteq \mathbb{A}^n$ coincide entonces con el grado de su clausura proyectiva $\overline{V} \subseteq \mathbb{P}^n$.

Sea $V \subseteq \mathbb{P}^n$ una variedad irreducible de dimensión r. Sea $k[V]$ su anillo de coordenadas homogéneas es decir $k[V] := k[x_1, \ldots, x_n]/I(V)$ y sea $k[V]_m$ su parte graduada de grado m. Sea entonces

$$h_V(m) := \dim_k k[V]_m$$

su función de Hilbert. Luego h_V coincide con un polinomio de grado r para m suficientemente grande. El término principal de este polinomio es $\deg V/r!$. Esta última es una consecuencia del teorema de Bertini [78].

La desigualdad de Bézout también vale en el contexto proyectivo, y es, de hecho, equivalente a la versión afín [31]. Esta definición del grado vía función de Hilbert nos permite dar una demostración sencilla de la desigualdad de Bézout en el caso general. Damos aquí las líneas principales de la demostración de Fulton [50].

Sean $V \subseteq \mathbb{P}^m$, $W \subseteq \mathbb{P}^n$ variedades irreducibles de dimensiones r y s respectivamente. Sea $V\#W \subseteq \mathbb{P}^{m+n+1}$ el *join rule* de V y W, es decir, la variedad proyectiva a la k-álgebra graduada $k[V] \otimes_k k[W]$. Luego

$$h_{V\#W}(m) = \sum h_V(i)\, h_W(m-i) = \frac{\deg V \cdot \deg W}{(r+s+1)!} m^{r+s+1} + O(m^{r+s})$$

y por lo tanto $\deg V\#W = \deg V \cdot \deg W$.

Sean $V, W \subseteq \mathbb{P}^n$ variedades irreducibles. Luego $V \cap W = (V\#W) \cap \Delta$ donde Δ denota la diagonal $\{x_0 = y_0, \ldots, x_n = y_n\} \subseteq \mathbb{P}^{2n+1}$. Luego

$$\deg V \cap W \leq \deg V\#W = \deg V \cdot \deg W.$$

Este argumento demuestra la desigualdad de Bézout para el caso en que V, W son irreducibles. El caso general se deduce a éste pasando por la descomposición en variedades irreducibles.

Posteriormente se han obtenido versiones más refinadas de la desigualdad de Bézout que incluyen multiplicidades de intersección general.

Referimos a lo libros de Fulton [53] y Vogel [136] para los enunciados precisos de estos resultados.

2.2.2 Forma de Chow

La idea básica de la construcción de Chow es la de parametrizar el conjunto de las variedades proyectivas. El punto en esta construcción es el asociar a toda variedad $V \subseteq \mathbb{P}^n$ una hipersuperficie Φ_V en un espacio proyectivo. Seguimos en este punto el tratamiento de Shafarevich [121].

El conjunto de hiperplanos en un espacio proyectivo $\mathbb{P}^n$ es un espacio proyectivo, el *espacio proyectivo dual*, que se denota por $\mathbb{P}^{n*}$. En forma intrínseca, si $\mathbb{P}^n = \mathbb{P}S$ es el espacio proyectivo asociado a un espacio vectorial S, el espacio proyectivo dual es la proyectivización $\mathbb{P}^{n*} = \mathbb{P}S^*$ del espacio dual S^*.

Sea $V \subseteq \mathbb{P}^n$ una variedad equidimensional de dimensión r. Consideramos la variedad

$$\Gamma := \{(p, H_1, \ldots, H_{r+1}) : p \in V,\ p \in H_i \ \ \forall i\} \subseteq V \times \mathbb{P}^{n*} \times \cdots \times \mathbb{P}^{n*}$$

La imagen de Γ por la proyección canónica $\pi : \Gamma \to \mathbb{P}^{n*} \times \cdots \times \mathbb{P}^{n*}$ es una hipersuperficie cerrada Φ_V.

El polinomio f_V que define a Φ_V es único salvo por múltiplos escalares, y se llama *forma de Chow* o *forma eliminante* de V. Se tiene que f_V es un polinomio multihomogéneo de grado $\deg V$ en cada grupo de variables [121].

Además f_V es simétrico — salvo por $\pm$ — con respecto a permutaciones entre los grupos de variables. Esto se deduce del hecho de que la hipersuperficie Φ_V es simétrica con respecto a estas permutaciones. Se tiene entonces

$$f_V(H_1, \ldots, H_j, \ldots, H_i, \ldots, H_{r+1}) = \tau_{ij}\, f_V(H_1, \ldots, H_j, \ldots, H_i, \ldots, H_{r+1})$$

para algún $\tau_{ij} \in k^*$, y se tiene entonces $\tau_{ij}^2 = 1$, de donde $\tau_{ij} = 1$ o $\tau_{ij} = -1$.

Sea $V = \cup_i V_i$ la descomposición de V en componentes irreducibles. Luego vale $f_V = \prod_i f_{V_i}$ [111, 1.3].

El significado geométrico de la forma de Chow es claro. Dados hiperplanos $H_1, \ldots, H_{r+1} \subseteq \mathbb{P}^n$, entonces $f_V(H_1, \ldots, H_{r+1}) = 0$ si y sólo si $V \cap H_1 \cap \cdots \cap H_{r+1} \neq \emptyset$. En el caso $V = \mathbb{P}^n$ la forma f_V coincide con el determinante.

Asumimos como dada una elección de coordenadas en $\mathbb{P}^n$ e identificamos a $\mathbb{P}^{n*}$ con $\mathbb{P}^n$. Cada hiperplano genérico $H \in \mathbb{P}^{n*}$ lo identificamos con un punto $U \in \mathbb{P}^n$ de forma tal que $x \in H$ si y sólo si $U \cdot x = 0$.

Sea $V \subseteq \mathbb{A}^n$ una variedad afín equidimensional, con $r := \dim V$. Luego definimos *forma de Chow* f_V de V como la forma de Chow de su clausura proyectiva.

Sean $H_1, \ldots, H_{r+1} \subseteq \mathbb{A}^n$. La condición $V \cap H_1 \cap \cdots \cap H_{r+1} \neq \emptyset$ implica como antes $f_V(H_1, \ldots, H_{r+1}) = 0$ pero no vale la recíproca.

Ahora introducimos la noción de polinomio característico de una variedad. Consideramos al espacio afín $\mathbb{A}^{(r+1)(n+1)}$ como la variedad de las $(r+1)\times(n+1)$-matrices e introducimos el morfismo definido por

$$\omega_V : \mathbb{A}^{(r+1)(n+1)} \times V \to \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}, \qquad (G, b, x) \mapsto (G, b, Gx + b)$$

para $(G, b)G \in \mathbb{A}^{(r+1)n}$, $b \in \mathbb{A}^{r+1}$ y $x \in V$. Se tiene

$$\dim \omega_V(\mathbb{A}^{(r+1)(n+1)} \times V) = (r+1)(n+1) + r$$

y por lo tanto $\Omega_V := \overline{\mathrm{Im}\ (\omega_V)}$ es una hipersuperficie de $\mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$. El polinomio P_V que la define es único salvo por múltiplos escalares y lo llamamos el polinomio característico de V.

Sea $U \in \mathbb{A}^{(r+1)(n+1)}$ y sean $U_1, \ldots, U_{r+1}$ las filas de la matriz U. Sean $\eta_i := U_{i0} + U_{i1}x_1 + \cdots + U_{in}x_n$ formas lineales *genéricas*. Luego P_V se puede interpretar como un polinomio en el anillo $k[U, \eta]$.

La extensión $k(\mathbb{A}^{r(n+1)} \times \mathbb{A}^r) \hookrightarrow k(\mathbb{A}^{r(n+1)} \times V)$ es separable y finita de grado δ [69]. El polinomio P_V coincide con el polinomio característico del elemento η_{r+1} salvo por un factor en $k(U_1,\ldots,U_r)(\eta_1,\ldots,\eta_r)^*$. Se tiene además que las variables genéricas $\eta_1,\ldots,\eta_r$ están en posición de Noether con respecto a V, es decir, la extensión

$$k(\mathbb{A}^{r(n+1)})[\eta_1,\ldots,\eta_r] \hookrightarrow k(\mathbb{A}^{r(n+1)})[V]$$

es entera.

El siguiente lema nos da la relación entre f_V y P_V.

Lema 2.2.3 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional, con $r := \dim V$. Entonces*

$$P_V(U,\eta) = f_V \circ T(U,\eta)$$

con $T_i(U,\eta) := (U_{i0} - \eta_i, U_{i1},\ldots,U_{in})$.

Demostración. Sea $Q(U,\eta) := f_V \circ T(U,\eta)$. Luego $Q(U,0) = f_V$ y por lo tanto Q es no nulo. El polinomio Q es multihomogéneo en $U_1,\ldots,U_{r+1}$ de grado δ, y por lo tanto basta probar que Q se anula en V. Sea $\xi \in V$. Las formas lineales

$$L_i(x) := U_{i0} - \eta_i(\xi) + U_{i1}x_1 + \cdots + U_{in}x_n$$

se anulan para $x := \xi$, y por lo tanto $Q(U,\eta(\xi)) = 0$. □

Luego P_V es multihomogéneo de grado δ en los grupos de variables $U_1,\ldots,U_{r+1}$. Además tiene grado total δ en η, por la desigualdad de Bézout. Se tiene además

$$f_V(U) = P_V(U,0)$$

Sea $V \subseteq \mathbb{A}^n$ una variedad definida sobre un cuerpo perfecto k. Entonces su ideal de definición $I(V)$ está definido sobre k, [101, Teorema 26.3]. En particular su forma de Chow f_V y su polinomio característico P_V están también están definidos sobre k.

Determinamos ahora la forma de Chow de una hipersuperficie y de una variedad de dimensión 0.

Sea $V \subseteq \mathbb{A}^n$ una hipersuperficie definida por un polinomio separable f de grado δ.

Sea M la $n \times n$-matriz genérica $(U_{ij})_{1\le i,j\le n}$. Luego $M \cdot (x_k)_k = (\eta_k - U_{k0})_k$ y por lo tanto $\Delta\, x_k = (\Delta_{1k}\eta_1 + \cdots + \Delta_{nk}\eta_n) - (\Delta_{1k}U_{10} + \cdots + \Delta_{nk}U_{1n})$ donde $\Delta = \det M$ y Δ_{kl} denota el (k,l)-menor de la matriz M. Luego

$$f_V = \Delta^\delta f(-\Delta_1/\Delta,\ldots,-\Delta_n/\Delta)$$

donde Δ_j denota el determinante de la matriz que resulta de reemplazar en M la columna j por $(U_{10},\ldots,U_{n0})$.

Sea $V \subseteq \mathbb{A}^n$ una variedad de dimensión 0. Entonces

$$f_V = \prod_{\xi\in V}(U_0 + U_1\xi_1 + \cdots + U_n\xi_n)$$

2.2.3 Definición de Altura

Sea k un FP-cuerpo y sea $V \subseteq \mathbb{A}^n$ una variedad irreducible. Luego definimos la *altura* de V como la altura invariante de su polinomio de Chow, es decir

$$h(V) := m(f_V).$$

La indeterminación proveniente de la elección de la forma de Chow f_V desaparece gracias a la fórmula del producto.

Sea $V \subseteq \mathbb{A}^n$ y sea $V = \cup_i V_i$ su descomposición en componentes irreducibles. Entonces definimos la *altura* de V como

$$h(V) := \sum_i h(V_i)$$

Se tiene $h(V) \geq 0$. Si $V \subseteq \mathbb{A}^n$ es equidimensional entonces $h(V) = h(f_V)$ por la aditividad de f_V.

Ahora vamos a estudiar el comportamiento de la altura para el caso de una hipersuperficie y de una variedad de dimensión 0.

Lema 2.2.4 *Sea $V = \mathbb{A}^n$ una hipersuperficie definida por un polinomio separable $g \in k[x_1, \ldots, x_n]$. Entonces*

$$-3n \log(n+1) \deg g \leq h(V) - m(g) \leq 3\ (n+1) \log(n+1) \deg g$$

Demostración. Sea g^h la homogeneización de g en $k[x_0, \ldots, x_n]$. Entonces

$$f_V = g^h(-\Delta, -\Delta_1, \ldots, -\Delta_n)$$

donde Δ es el determinante de la matriz $M := (U_{ij})_{1 \leq i,j \leq n}$ y Δ_j es el determinante de la matriz que resulta de reemplazar en M la columna j por $(U_{1,0}, \ldots, U_{n,0})$.

Se tiene $\deg \Delta_i = n$, $m_v(\Delta_i) \leq l(\Delta_i) \leq n \log n$ para $v \in S_k$ y $m_v(\Delta_i) = 0$ para $v \notin S_k$. Luego

$$m(f_V) \leq n(g) + \deg f\ (\log(n+1) + n \log n + n)\ \log n(n+1)) \leq m(g) + 3(n+1) \log(n+1) \deg g$$

por Lema 2.1.1. Por otra parte se tiene $g = f_V \circ T(x)$ con $T_i(x) = (-x_i, 0, \ldots, 1, \ldots, 0)$. Luego $m(g) \leq m(f_V) + 3n \log(n+1) \deg g$. □

Lema 2.2.5 *Sea $V \subseteq \mathbb{A}^n$ una variedad de dimensión 0. Entonces*

$$0 \leq h(V) - w(V) \leq \log(n+1) \deg V$$

donde $w(V)$ denota la altura de Weil de la variedad afín V, es decir $w(V) := \sum_{\xi \in V} \overline{h}(\xi)$.

Demostración. Alcanza con considerar el caso en que V se reduce a un punto $\xi \in \mathbb{A}^n$. Luego $f_V = U_0 + \xi_1 U_1 + \cdots + \xi_n U_n$ y por lo tanto $m(f_V) \leq \overline{h}(\xi) + \log(n+1)$.

Por otra parte se tiene $m_v(f_V) \geq \overline{h}_v(\xi)$ para todo v. El caso en que v es arquimediano se sigue fácilmente de la definición de la medida de Mahler y de la fórmula

$$M(g) = a_d \prod_i \max\{1, |\alpha_i|\}$$

para polinomios univariados $g = a_d \prod_i (x - \alpha_i) \in \mathbb{C}[x]$. Se sigue entonces

$$m(f_V) \geq \overline{h}(\xi)$$

□

Vemos así que la noción de altura que consideramos es equivalente a la altura del polinomio que la define o a la altura de Weil según el caso. Aquí equivalente significa que la diferencia entre ambas cantidades está acotada por $c(n) \deg V$ donde $c(n)$ es polinomial en n.

2.2.4 Propiedades Básicas

Ahora vamos a establecer algunas de las propiedades más inmediatas de la altura. Consideramos primero su comportamiento bajo intersección con variedades lineales.

Lema 2.2.6 *Sea $V \subseteq \mathbb{A}^n$ y sea $r := \dim V$. Sea $H \subseteq \mathbb{A}^n$ un hiperplano y sea L el polinomio de grado 1 que lo define. Entonces $h(V \cap H) \leq h(V) + (r+1)(\overline{w}(L) + 4\log(n+1)) \deg(V)$.*

Demostración. Alcanza con considerar el caso en que V es irreducible. El caso $V \subseteq H$ es trivial ya que $f_{V \cap H} = f_V$.

Sea entonces $V \not\subseteq H$. Luego $V \cap H$ es una variedad equidimensional de dimensión $r-1$. Sea $g := f_V(U_1, \ldots, U_r, L)$. Luego $g(H_1, \ldots, H_r) = 0$ si $(V \cap H) \cap H_1 \cap \cdots \cap H_r \neq \emptyset$. Luego g es un múltiplo no nulo de $f_{V \cap H}$ y por lo tanto $m(f_{V \cap H}) \leq m(g)$ por la positividad de la altura m. Luego

$$m(f_{V \cap H}) \leq m(f_V) + \deg f_V(\overline{h}(L) + 4\log(n+1))$$

□

Podemos escribir el lema anterior en forma de desigualdad de Bézout como

$$h(V \cap H) \leq h(V) + (r+1) \deg V (h(H) + (3n+4)\log(n+1))$$

ya que se tiene $m(L) \leq h(H) + 3n\log(n+1)$ por el Lema 2.1.1, y además existe $\lambda \in k^*$ tal que $\overline{m}(L) = m(\lambda L)$. Podemos extender esta desigualdad al caso de la intersección de V con una variedad lineal.

Corolario 2.2.7 *Sea $V \subseteq \mathbb{A}^n$ y sea $r := \dim V$. Sean $L_1, \ldots, L_s \in k[x_1, \ldots, x_n]$ polinomios de grado 1, y sea $E \subseteq \mathbb{A}^n$ la variedad lineal $V(L_1, \ldots, L_s)$. Entonces*

$$h(V \cap E) \leq h(V) + (r+1) \deg V(\sum_i \overline{m}(L_i) + 4s \log(n+1))$$

$\square$

Sean $L_1, \ldots, L_{n-r} \in k[x_1, \ldots, x_n]$ polinomios de grado 1 que definen una variedad lineal E de dimensión r. Obtenemos del resultado anterior la cota

$$\begin{aligned} h(E) &\leq (n+1)(\textstyle\sum_i \overline{m}(L_i) + 4(n-r)\log(n+1)) \\ &\leq (n+1)(\textstyle\sum_i \overline{m}(L_i) + 4n \log(n+1)) \end{aligned}$$

ya que $h(\mathbb{A}^n) \leq n \log n$.

Consideramos ahora el comportamiento de la altura con respecto a morfismos lineales afines.

Lema 2.2.8 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ una aplicación lineal afín inversible y sea $V \subseteq \mathbb{A}^n$. Entonces*

$$h(\varphi(V)) \leq h(V) + 2(r+1)\log(n+1) \deg V\,(\overline{h}(\varphi) + 2\log(n+1) + 1)$$

Demostración. Sea $G := (U_{ij})_{ij}$ una $(r+1) \times n$-matriz genérica y sea $b := (U_{1,0}, \ldots, U_{r+1,0})$ una $(r+1) \times 1$-matriz genérica, y sea $U := (b, G)$. Luego $f_{\varphi(V)}(U) = 0$ si existe un punto $p \in V$ tal que $\varphi(x)$ está en el espacio lineal determinado por U, es decir $b + G \cdot \varphi(x) = 0$. Sea $(c, A) \in \mathbb{A}^n \times \mathbb{A}^{n \times n}$ la matriz de φ, con $A \in GL(n)$. Luego $b + G \cdot \varphi(x) = b + G \cdot + G \cdot A \cdot x$ y por lo tanto

$$f_{\varphi(V)}(U) = f_{\varphi(V)}(b, G) = f_V(b + G \cdot c, G \cdot A) = f_V(U \cdot \varphi).$$

Tenemos $\overline{m}(U \cdot \varphi) \leq \overline{h}(\varphi) + \log(n+1)$ y por lo tanto

$$m(f_{\varphi(V)}) \leq m(f_V) + (r+1) \deg V \log(r+1)(n+1)\overline{h}(\varphi) + \log(r+1)(n+1) + 1$$

$\square$

Lema 2.2.9 *Sea $i : \mathbb{A}^n \hookrightarrow \mathbb{A}^{n+p}$ la inclusión canónica $x \mapsto (x, 0)$ y sea $V \subseteq \mathbb{A}^n$. Entonces $h(i(V)) = h(V)$.*

Demostración. Se sigue directamente de la igualdad $f_{i(V)} = f_V$. $\square$

Lema 2.2.10 *Sea $\pi : \mathbb{A}^{n+p} \to \mathbb{A}^n$ la proyección $(x, y) \mapsto x$, y sea $V \subseteq \mathbb{A}^{n+p}$. Entonces $h(\overline{\pi(V)}) \leq h(V) + 4(r+1)\log(n+1) \deg V$.*

Demostración. Alcanza con considerar el caso en que V es irreducible. Sea $s := \dim \overline{\pi(V)}$. Consideramos primero el caso $s = r$.

Luego $f_{\pi(V)}$ es un factor no nulo de $f_V(U \cdot \pi)$.

Consideramos luego el caso $s < r$. Sea $\rho : \mathbb{A}^n \times \mathbb{A}^p \to \mathbb{A}^n \times \mathbb{A}^{r-s}$ una proyección tal que $\dim \overline{\rho(V)} = r$.

Sea $W := \overline{\rho(V)}$. Luego $\overline{\pi(W)} = \overline{\pi(V)}$ y se tiene $\dim \pi^{-1}(\xi) \geq r - s$ por el teorema de dimensión de fibras. Luego $W = \overline{\pi(V)} \times \mathbb{A}^{r-s}$. Luego existen coordenadas standard $y_1, \ldots, y_{r-s}$ tales que $\pi(V \cap \{y_1 = 0, \ldots y_{r-s} = 0\}) = \pi(V)$ y $\dim V \cap \{y_1 = 0, \ldots y_{r-s} = 0\}) = s = \dim \overline{\pi(V)}$. Sean $Z := V \cap \{y_1 = 0, \ldots y_{r-s} = 0\}) \subseteq \mathbb{A}^n$. Concluímos entonces que $f_{\pi(V)}$ es un factor de $f_Z(U \cdot \pi)$ y por lo tanto

$$m(f_{\overline{\pi(V)}}) \leq m(f_V) + 4(r+1)\log(n+1)\deg V$$

$\square$

Corolario 2.2.11 *Sea* $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ *una aplicación lineal afín y sea* $V \subseteq \mathbb{A}^n$. *Entonces* $h(\overline{\varphi(V)}) \leq h(V) + 2\,(r+1)\log(m+n+1)\deg V\,(\overline{h}(\varphi) + 2\log(n+1) + 1)$.

Demostración. La aplicación φ se descompone como $\varphi = i \circ \psi \circ \pi$, donde ψ es inversible, y i, π son la inclusión y la proyección canónicas respectivamente, y $\overline{h}(\psi) = \overline{h}(\varphi)$. $\square$

2.3 Estimaciones para Funciones Algebraicas

El Teorema de la Función Inversa es una de las herramientas más versátiles de Geometría Diferencial. No existe un análogo preciso de este resultado en el contexto de la Geometría Algebraica. Sin embargo existen situaciones donde se puede reemplazar este teorema por una versión más débil. La idea es clásica, y consiste en considerar inversas dadas por series de potencias formales.

En esta sección adoptamos este punto de vista como método para estudiar las propiedades de la altura. Como una consecuencia importante de este método obtenemos una relación precisa entre la altura de una variedad intersección completa de dimensión positiva y una de sus fibras cero–dimensionales con respecto a una proyección finita.

2.3.1 El Teorema de la Función Inversa

En este apartado vamos a estimar las derivadas de la inversa local de una aplicación regular.

A lo largo de esta sección k denota un FP-cuerpo con un conjunto propio M_k de valores absolutos que satisface la fórmula del producto con multiplicidades λ_v.

Ahora vamos a introducir algunas nociones básicas.

Sean $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ variedades y sea $\varphi : V \to W$ un morfismo regular en un punto $p \in W$. Entonces p es un punto *reducido* si su fibra $\varphi^{-1}(p)$ es reducida, es decir, si $I(V) + (\varphi - p)$ es un ideal radical de $k[x_1, \ldots, x_n]$.

Sea $\varphi : V \to W$ una aplicación regular y dominante. Luego la extensión de cuerpos $\varphi^* k(W) \hookrightarrow k(V)$ es finita. El grado de esta extensión se llama el *grado* de φ, es decir

$$\deg \varphi := [k(V) : \varphi^* k(W)].$$

Una aplicación $\varphi : V \to W$ es finita si la extensión $\varphi^* k[W] \hookrightarrow k[V]$ es entera. En particular φ es suryectiva y tiene fibras finitas.

Si $\varphi : V \to W$ es una aplicación finita de variedades irreducibles y W es normal, entonces $\#\varphi^{-1}(p) \leq \deg \varphi$. En el caso en que φ es *separable*, es decir la extensión $\varphi^* k(W) \hookrightarrow k(V)$ es separable, la igualdad $\#\varphi^{-1}(p) = \deg f$ se satisface genéricamente [121, II.5.3].

Este resultado vale más generalmente en el caso en que $\dim V = \dim W$, W es normal y φ es dominante [69, Proposición 1]. Esta generalización es importante para nuestras aplicaciones.

Un morfismo $\varphi : V \to W$ es *no ramificado* en $p \in W$ si $\#\varphi^{-1}(p) = \deg f$. El enunciado anteriormente citado dice entonces que si $\dim V = \dim W$, W es normal y φ es dominante, entonces el conjunto de puntos no ramificados de φ contiene un abierto no vacío.

Se tiene además que un punto no ramificado es reducido [121, II.5.3 Teorema 8].

Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un morfismo finito y sea $\psi = \sum_j b_j y^j \in k[[y_1, \ldots, y_n]]^n$ una familia finita de series de potencias formales.

Sea $m = (m_1, \ldots, m_n) \in \mathbb{N}^n$ y sea

$$\partial_m := \frac{1}{m!}(\frac{\partial}{\partial y})^m = \frac{1}{m_1!}(\frac{\partial}{\partial y_1})^{m_1} \cdots \frac{1}{m_n}(\frac{\partial}{\partial y_n})^{m_n}$$

de forma tal que $\partial_m \psi(0) = b_m$. Se tiene

$$\partial_m \psi^i = \partial_m(\overbrace{\psi_1 \cdots \psi_1}^{i_1} \cdots \overbrace{\psi_n \cdots \psi_n}^{i_n}) = \sum_l \partial_{l_1} \psi_1 \cdots \partial_{l_{|i|}} \psi_n$$

por la fórmula de Leibnitz, donde el multi–índice $l = (l_1, \ldots, l_{|i|})$ verifica $l_1 + \cdots + l_{|i|} = m$. Separamos en esta suma los términos en los que interviene ∂_m de los términos en los que sólo intervienen derivadas de orden menor. Luego

$$\partial_m \psi^i = \sum_{j=1}^{n} i_j (\psi_1^{i_1} \cdots \psi_j^{i_j - 1} \cdots \psi_n^{i_n}) \partial_m \psi_j + \sum_l \partial_{l_1} \psi_1 \cdots \partial_{l_{|i|}} \psi_n$$

donde la última suma se extiende sobre todos los l igual que antes tales que $l_k \neq m$ para todo k.

Sea $\varphi = \sum a_i x^i$. Luego $\partial_m(\varphi \circ \psi) = \sum a_i \partial_m \psi^i$ y obtenemos así la igualdad

$$\partial_m(\varphi \circ \psi) = (\mathrm{Diff}\ \varphi \circ \psi) \cdot \partial_m \psi + \sum_{i,l : l_k \neq m} a_i \partial_{l_1} \psi_1 \cdots \partial_{l_{|i|}} \psi_n \qquad (1)$$

donde Diff $\varphi := (\frac{\partial \varphi_i}{\partial x_j})_{ij}$ denota el *diferencial* de la función φ.

El siguiente resultado garantiza la existencia de una inversa *formal* de un morfismo regular.

Lema 2.3.1 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un morfismo dominante tal que la fibra de 0 es finita y reducida. Sea $\xi \in \varphi^{-1}(0)$. Entonces existe una única $\psi \in k[[y_1, \ldots, y_n]]^n$ tal que $\varphi \circ \psi = \mathrm{Id}$ y $\psi(0) = \xi$.*

Demostración. El punto $0 \in \mathbb{A}^n$ es reducido y la fibra $V_0 := \varphi^{-1}(0)$ es cero–dimensional. Sea $J = J_\varphi := \det(\mathrm{Diff}\ \varphi)$ el *Jacobiano* de φ. Luego $J(\xi) \neq 0$ para todo $\xi \in V_0$ por el Criterio Jacobiano [43, Teorema 18.15].

Vamos a construir familias de polinomios $\psi^{(d)} \in k[x_1, \ldots, x_n]^n$ de grado acotado por d tales que $\psi^{(d)}(0) = \xi$, $\psi^{(d)} \equiv \psi^{(d')} \mod (y_1, \ldots, y_n)^{d+1}$ para $d \leq d'$ y $\varphi \circ \psi^{(d)} \equiv \mathrm{Id} \mod (y_1, \ldots, y_n)^{d+1}$. Luego ψ se define como el límite de $\psi^{(d)}$ en $k[[y_1, \ldots, y_n]]^n$.

Hacemos esta construcción inductivamente. Sea $\psi^{(0)} := \xi$. Suponemos ahora que $\psi^{(d-1)}$ está construído. Sea $\psi^{(d)} := \psi^{(d-1)} + \sum_{|m|=d} b_m y^m$. En particular tenemos todas las derivadas en $y = 0$ de orden menor o igual que $d-1$ de $\psi^{(d)}$. Sea $m \in \mathbb{N}^n$ tal que $|m| = d$.

Se tiene $\partial_m(\varphi \circ \psi(d))(0) = \mathrm{Id}$ si $|m| = 1$ o $\partial_m(\varphi \circ \psi(d))(0) = 0$ en otro caso. Luego b_m queda unívocamente determinado por la fórmula (1) ya que Diff φ es no–singular, y $\psi^{(d)}$ satisface las condiciones requeridas. □

El resultado principal de esta sección es una estimación para el tamaño de las derivadas de ψ. La demostración de este resultado sigue una idea utilizada por Granville en el caso 1–dimensional [23].

Lema Principal 2.3.2 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un morfismo dominante tal que la fibra de 0 es finita y reducida. Sea $\xi \in \varphi^{-1}(0)$ y sea $\psi \in k[[y_1, \ldots, y_n]]^n$ tal que $\varphi \circ \psi = \mathrm{Id}$ y $\psi(0) = \xi$. Sea $d := \max_i \deg \varphi_i$. Entonces*

$$\begin{aligned}\log|\partial_m \psi(0)|_v &\le (3|m|-2)(n\, h_v(\varphi) + n\,(d-1) h_v(\xi) + \overline{h}_v(J_\varphi(\xi)^{-1}) \\ &\quad +3\,n\,d + 2\,n^2 + |m|) v \in S_k \\ \log|\partial_m \psi(0)|_v &\le (3|m|-2)(n\, h_v(\varphi) + n(d-1) h_v(\xi) + \overline{h}_v(J_\varphi(\xi)^{-1})) v \notin S_k\end{aligned}$$

para $m \in \mathbb{N}^n$, donde $J_\varphi(\xi)$ denota el Jacobiano de φ evaluado en ξ.

Demostración. Sea $\psi = \sum b_m y^m$. Vamos a acotar recursivamente las derivadas de ψ usando la fórmula (1).

Fijamos un valor absoluto $v \in M_k$ y consideramos por separado los casos $v \in S_k$ y $v \notin S_k$.

Procedemos por inducción en $|m|$. Tenemos $\log|b_0| = h_v(\xi)$. Sea $J_\varphi(\xi)$ el Jacobiano de φ evaluado en ξ. Sea κ la constante

$$\kappa := n\, h_v(\varphi) + n\,(d-1)\, h_v(\xi) + 3\,d\,n + 2\,n^2 + \overline{h}_v(J_\varphi(\xi)^{-1}) \ge 0$$

y suponemos que vale $\log|b_l| \le (3|l|-2)(\kappa + |l|)$ para $1 \le |l| \le m-1$.

Tenemos $\varphi \circ \psi = \mathrm{Id}$ y por lo tanto $\partial_m(\varphi \circ \psi) = 0$ para $|m| \ge 2$ y $\partial_m \varphi \circ \psi = m$ para $|m| = 1$. Sea $\varphi = \sum a_i x^i$ y sea

$$B_m := -\sum_{i,l: l_k \ne m} a_i\, \partial_{l_1} \psi_n(0) \cdots \partial_{l_{|i|}} \psi_n(0),$$

es decir, la segunda suma en la expresión (1) — con el signo opuesto. Luego

$$J_\varphi(\xi) \cdot \partial_m \psi(0) = \mathrm{Adj}\ {}^t(\mathrm{Diff}\ \varphi(\xi)) \cdot (B_m + \tau(m))$$

donde $\mathrm{Adj}\ {}^t$ denota la matriz adjunta traspuesta, y $\tau(m) = m$ para $|m| = 1$ y $\tau(m) = 0$ para $|m| \ge 2$.

Sea $\alpha_v(m) := \max_{l_k \neq m,\ i \leq d}\{\log|\partial_l \psi_1(0)| + \cdots + \log|\partial_{l_i}\psi_n(0)|\}$.

Para $|m| = 1$ se tiene $B_m = 0$ y por lo tanto $\log|b_m| \leq h_v(\mathrm{Adj}\ ^t(\mathrm{Diff}\ \varphi(\xi))) - h_v(J_\varphi(\xi)) \leq \kappa \leq (3|m| - 2)(\kappa + |m|)$. Consideramos entonces el caso $|m| \geq 2$.

En la definición de $\alpha_v(m)$ intervienen derivadas de orden $\geq m - 1$. Aplicamos la hipótesis inductiva y obtenemos

$$\alpha_v(m) \leq (3|m| - 4)(\kappa + |m| - 1) + (d-2)h_v(\xi) \leq (3|m| - 3)(\kappa + |m|)$$

ya que $\kappa \geq (d-2)h_v(\xi)$. Luego

$$\begin{aligned}
\log|B_m| &\leq \log\tbinom{d+n}{n} + \log\tbinom{d+m_1-1}{m_1-1}\cdots\tbinom{d+m_n-1}{m_n-1} + h_v(\varphi) + \alpha_v(m) \\
&\leq (d+n) + \textstyle\sum_{i=1}^n (d + m_i - 1) + h_v(\varphi) + \alpha_v(m) \\
&\leq (n+1)\,d + |m| + h_v(\varphi) + \alpha_v(m)
\end{aligned}$$

Ahora estimamos el valor absoluto de $\mathrm{Adj}\ ^t(\mathrm{Diff}\ \varphi(\xi))$. Tenemos

$$\begin{aligned}
\log|\mathrm{Diff}\ \varphi(\xi)| &\leq h_v(\varphi) + \log d + (d-1)h_v(\xi) + \log\tbinom{d+n}{n} \\
&\leq h_v(\varphi) + (d-1)h_v(\xi) + d + n + \log d
\end{aligned}$$

y por lo tanto

$$\begin{aligned}
\log|\mathrm{Adj}\ ^t(\mathrm{Diff}\ \varphi(\xi))| &\leq (n-1)\log|d\varphi(\xi)| + \log(n-1)! \\
&\leq (n-1)\,h_v(\varphi) + (n-1)\,(d-1)\,h_v(\xi) + (n-1)(d + n + \log d + \log n)
\end{aligned}$$

Concluímos entonces

$$\begin{aligned}
\log|b_m| &\leq \log|\mathrm{Adj}\ ^t(\mathrm{Diff}\ \varphi(\xi))| + \log|B_m| + \log n + \overline{h}_v(J_\varphi(\xi)^{-1}) \\
&\leq n\,h_v(\varphi) + n\,(d-1)\,h_v(\xi) + 3\,n\,d + 2\,n^2 + \overline{h}_v(J_\varphi(\xi)^{-1}) + |m| + \alpha_v(m) \\
&\leq (3|m| - 2)(\kappa + |m|)
\end{aligned}$$

El caso en que v es no–arquimediano se sigue de la misma manera. □

Sea K una extensión finita de k y sea $\varrho \in K^*$. Luego $\log|\varrho|_v \geq -[K : k]\,\overline{h}(\varrho)$ [111, Proposición 1.12 (vi)].

Se tiene $h_v(\varphi(\xi)) \leq h_v(\varphi) + d\,\overline{h}_v(\xi) + d + n$ para $v \in S_k$ y por lo tanto $h_v(J_\varphi(\xi)) \leq nh_v(\varphi(\xi))_v + \log n! \leq nh_v(\varphi) + n\,d\,\overline{h}_v(\xi) + nd + 2n^2$. Luego

$$\deg J_\varphi(\xi) \leq \deg\xi, \overline{h}(J_\varphi(\xi)^{-1}) \leq n\,h(\varphi) + n\,d\,\overline{h}(\xi) + n\,d + 2\,n^2$$

y por lo tanto

$$\log|J_\varphi(\xi)^{-1}| \geq -n\deg\xi(h(\varphi) + d\,\overline{h}(\xi) + d + 2n)$$

Obtenemos de aquí las estimaciones

$$\begin{aligned}
\log|\partial_m\psi(0)| &\leq (2\,|m| - 3)(2\,n\deg\xi(h(\varphi) + d\,\overline{h}(\xi) + 4\,d + 4\,n) + |m|) && v \in S_k \\
\log|\partial_m\psi(0)| &\leq (2|m| - 3)2\,n\ \deg\xi\,(h(\varphi) + d\,\overline{h}(\xi)) && v \notin S_k
\end{aligned}$$

2.3.2 Altura de Fibras vs. Altura de Variedades

En esta subsección estudiamos la relación entre la altura de una variedad y la altura de la fibra de una punto reducido con respecto a un morfismo lineal. Nuestro estudio se basa en los resultados del apartado anterior.

En primer lugar estimamos las derivadas de la inversa local de un morfismo.

Corolario 2.3.3 *Sean $F_1, \ldots, F_{n-r} \in k[x_1, \ldots, x_n]$ polinomios que forman una intersección completa reducida. Sea $V := V(F_1, \ldots, F_{n-r})$ y sea $\varphi : V \to \mathbb{A}^r$ un morfismo dominante tal que la fibra de 0 es finita y reducida. Sea $\xi \in \varphi^{-1}(0)$. Entonces existe $\psi \in k[[y_1, \ldots, y_r]]^n$ tal que $\psi(y) \in V$, $\varphi \circ \psi = \mathrm{Id}$ y $\psi(0) = \xi$. Sea $v \in M_k$. Se tiene además*

$$\begin{aligned}\log|\partial_m \psi|_v &\leq (3\,|m| - 2)(n\,h_v(\varphi, F) + n\,(d-1)\,h_v(\xi) + \overline{h}_v(J_{\varphi,F}(\xi)^{-1}) \\ &\quad +3nd + 2n^2 + |m|) v \in S_k \\ \log|\partial_m \psi|_v &\leq (3\,|m| - 2)(n\,h_v(\varphi, F) + n\,(d-1)\,h_v(\xi) + \overline{h}_v(J_{\varphi,F}(\xi)^{-1}) v \notin S_k\end{aligned}$$

para $m \in \mathbb{N}^n$.

Demostración. Este enunciado es una consecuencia directa del Lema Principal 2.3.2.

Consideramos el morfismo $\Phi : \mathbb{A}^n \to \mathbb{A}^n$ definido como $x \mapsto \Phi(x) := (\varphi(x), F(x))$. El hecho de que 0 sea un punto no reducido de φ implica en forma directa que es un punto no reducido de Φ, y se tiene $\xi \in \Phi^{-1}(0)$. Sea $\Psi \in k[[y_1, \ldots, y_r]]^n$ una inversa local de Φ en ξ. Luego $\psi := \Psi(y_1, \ldots, y_r, 0, \ldots, 0)$ verifica las condiciones requeridas.

Las cotas para las derivadas de ψ salen del Lema Principal 2.3.2. □

Sea $V \subseteq \mathbb{A}^n$ una variedad irreducible de dimensión r y sea $\varphi : V \to \mathbb{A}^r$ un morfismo dominante y separable. El resultado técnico principal de esta sección es una cota para la altura de la ecuación minimal de un elemento $f \in k(V)$ sobre $\varphi^* k(\mathbb{A}^r)$ en términos de la altura de una fibra no ramificada de φ.

Necesitamos los siguientes lemas:

Lema 2.3.4 *Sean $\zeta_1, \ldots, \zeta_k \in k[[y_1, \ldots, y_n]]$ y $\theta := \prod_j \zeta_j$. Sea $v \in M_k$ y $c_0, c_1 \geq 0$ constantes tales que $\log|\partial_m \zeta_j(0)|_v \leq c_0\,|m| + c_1$. Entonces*

$$\begin{aligned}\log|\partial_m \theta(0)|_v &\leq (c_0 + 1)\,|m| + (c_1 + n)\,k \qquad && v \in S_k \\ \log|\partial_m \theta(0)|_v &\leq c_0\,|m| + c_1\,k && v \notin S_k\end{aligned}$$

Demostración. Sean $\zeta_j = \sum_i a_i^{(j)} y^j$ y $\theta = \sum_m c_m\, y^m$. Luego $c_m = \sum_{i_1 + \cdots + i_k = m} a_{i_1}^{(1)} \cdots a_{i_k}^{(k)}$ y por lo tanto

$$|c_m|_v \leq \binom{m_1 + k - 1}{k-1} \cdots \binom{m_n + k - 1}{k-1} \max_{i_1 + \cdots + i_k = m} \{|a_{i_1}^{(1)}| \cdots |a_{i_k}^{(k)}|\}$$

para $v \in S_k$, de donde

$$\begin{aligned}
\log|c_m|_v &\le (m_1+k-1)+\cdots+(m_n+k-1)\\
&\quad + \max_{i_1+\cdots+i_k=m}\{(c_0\,|i_1|+c_1)+\cdots+(c_0\,|i_k|+c_1)\}\\
&= (c_0+1)\,|m|+(c_1+n)\,k
\end{aligned}$$

El caso $v \notin S_k$ se sigue en forma análoga. □

Corolario 2.3.5 *Sean* $\zeta_1,\ldots,\zeta_k \in k[[y_1,\ldots,y_n]]$, $f \in k[t_1,\ldots,t_k]$ *y sea* $\vartheta := f(\zeta_1,\ldots,\zeta_k) \in k[[y_1,\ldots,y_n]]$. *Sea* $v \in M_k$ *y* $c_0, c_1 \ge 0$ *constantes tales que* $\log|\partial_m\zeta_j(0)|_v \le c_0|m|+c_1$. *Entonces*

$$\begin{aligned}
\log|\partial_m\vartheta(0)|_v &\le (c_0+1)|m|+(c_1+n+1)\deg f+\log|f|_v+k && v\in S_k\\
\log|\partial_m\vartheta(0)|_v &\le c_0\,|m|+c_1\,\deg f+\log|f|_v && v\notin S_k
\end{aligned}$$

□

Proposición 2.3.6 *Sea* $\pi : V \to \mathbb{A}^r$ *una proyección lineal finita y separable, y* $V \subseteq \mathbb{A}^n$ *variedad equidimensional. Sea* $F := (F_1,\ldots,F_{n-r}) \subseteq k[x_1,\ldots,x_n]$ *una intersección completa reducida que contiene a* V. *Sea* $p \in \mathbb{A}^r$ *un punto no ramificado de* π *con respecto a* $V(F_1,\ldots,F_{n-r})$. *Sea* $f \in k[V]$ *y sea* $m_f \in k[\mathbb{A}^r][t]$ *su polinomio minimal sobre* $k[\mathbb{A}^r]$. *Entonces*

$$\begin{aligned}
\deg m_f &\le \deg f\,\deg V\\
h(m_f) &\le 6\,n^2\,(d(F)\,(\overline{h}(p)+2)+\overline{h}(F))\,\deg^2 V\,h(V_0)
\end{aligned}$$

donde $d(F) := \max_i \deg F_i$.

Demostración. El polinomio m_f es la ecuación de la imagen del morfismo $V \to \mathbb{A}^r$ definido por $x \mapsto (\pi(x), f(x))$. La cota de grado es entonces una consecuencia del teorema de Bézout.

Consideramos ahora las cotas para la altura local. Consideramos primero el caso en que $p = 0$ y V es irreducible. Sea $D := \deg\pi = [k(V) : \pi^*k(\mathbb{A}^r)] \le \delta := \deg V$ y sea $\{\xi_1,\ldots,\xi_D\} = \pi^{-1}(0) = V_0$ la fibra de π en 0. Sea ψ_i la inversa local de π en ξ_i.

Sea $m_f = a_0+\cdots+a_{\mu-1}t^{\mu-1}+t^\mu \in k[\mathbb{A}^r][t]$ el polinomio minimal de f. La variedad $\mathbb{A}^n$ es normal y por lo tanto el polinomio m_f está en $k[\mathbb{A}^r][t]$.

El polinomio característico $\chi_f(t) := \prod_{i=1}^D (t-f(\psi_i))$ anula a f, y por lo tanto m_f es un factor de este polinomio. Podemos suponer entonces sin pérdida de generalidad que vale

$$m_f(t) = \prod_{i=1}^{\mu}(t-f(\psi_i))$$

para algún $1 \le \mu \le D$.

Sea $\Delta := \deg m_f \leq \deg f \deg V$ el grado total de m_f. Luego alcanza con calcular los términos de grado $\leq \Delta$ en este producto.

Tenemos $\log |\partial_m \psi_i(0)|_v \leq c_0 |m| + c_1$ con $c_0 := 3(n\, h_v(F) + n\,(d-1)\, h_v(V_0) + \overline{h}_v(J_{\pi,F}(V_0)^{-1}) + 3nd + 2n^2 + \Delta)$ y $c_1 := h_v(V_0)$ para $v \in S_k$ y $|m| \leq \Delta$. Luego $a_{\mu-i}$ está formado por $\binom{\mu}{i}$ productos de $f(\psi_j)$ con i factores. Luego

$$\log |a_{\mu-i}|_v \leq (c_0 + 2)\Delta + ((c_1 + r + 1) \deg f + h_v(f) + n) + i + 1)\, i + i + \mu$$

por aplicación del Corolario 2.3.5. Por lo tanto

$$\begin{aligned} h(a_{\mu-i}) \quad &\leq \quad (3\, n\, h(F) + 3\, n\, d(F)\, h(V_0) + 3\, \overline{h}(J_{\pi,F}(V_0)) + 9\, n\, d + 6\, n^2 \\ &\quad\; +3\, \Delta + 2)\Delta + i((h(V_0) + r + 1) \deg f + h(f) + n + i + 2) + \mu \end{aligned}$$

Finalmente

$$\begin{aligned} \overline{h}(J_{\pi,F}(V_0)^{-1}) \quad &\leq \quad \textstyle\sum_\xi \overline{h}(J_{\pi,F}(\xi^{-1})) = \sum_\xi \overline{h}(J_{\pi,F}(\xi)) \leq D(n\, h(\pi(\xi), F(\xi)) + \log n!) \\ &\leq \quad D\, n(h(F) + d\, \overline{h}(\xi) + d + n) + \log n!) \leq n\, D(w(\pi, F) + d\, \overline{h}(\xi) + d + 2n) \end{aligned}$$

y concluímos entonces

$$\begin{aligned} h(a_{\mu-i}) \quad &\leq \quad 6\, n\, D\, h(F)\Delta + 6\, n\, \deg F\, \overline{h}(V_0))\, D\, \Delta + 12n(n + d)\Delta \\ &+ \quad 3\Delta^2 + i\, \deg f\, \overline{h}(V_0)) + i\, \overline{h}(f) + D((r + 1) \deg f + n + D + 3) \end{aligned}$$

El caso general se reduce al caso $p = 0$ aplicando una traslación $\tau : x \mapsto x - p$. Se tiene entonces $\overline{h}(\pi(x - p), F(x - p)) \leq \overline{h}(\pi, F) + d(\pi, F)\, \overline{h}(p) d(\pi, F) + n$. Luego

$$h(a_{\mu-i}) \leq 6\, n^2 (\deg f + \overline{h}(f))\, (d(F)\, (\overline{h}(p) + 2) + \overline{h}(F))\, \deg^2 V\, h(V_0)$$

El caso de una variedad reducible equidimensional $V \subseteq (F_1, \ldots, F_{n-r})$ se reduce a este caso. Sea $V = \cap_i V_i$ su descomposición en componentes irreducibles. Luego

$$m_f = \prod_i m_f^{(i)}$$

El caso $v \notin S_k$ se sigue en forma análoga. □

Sea $V \subseteq \mathbb{A}^n$ variedad irreducible de dimensión r. Sea $\pi : V \to \mathbb{A}^r$ un morfismo finito, y sea $\deg \pi$ su grado. Se tiene $\deg \pi \leq \deg V$. Sea $f \in k[V]$ un polinomio de grado d y altura h. Sea $m_f = t^\mu + a_{\mu-1}\, t^{\mu-1} + \cdots + a_0 \in k[x_1, \ldots, x_r][t]$ su polinomio minimal. Luego $\mu | \deg \pi$, y por lo tanto se tiene la relación

$$\mathrm{Tr}\ f = -(\deg \pi / \mu) \cdot a_{\mu-1}$$

y por lo tanto vale

$$\deg \mathrm{Tr}\ f \leq \deg f\, \deg V, \mathrm{Tr}\ f \leq 6\, n^2 (\deg f + \overline{h}(f))\, (d(F)\, (\overline{h}(p) + 2) + \overline{h}(F))\, \deg^2 V\, h(V_0)$$

En la demostración de la Proposición 2.3.6 es central la hipótesis de que la proyección $\pi : V \to \mathbb{A}^r$ es finita, y no meramente dominante. Existen sin embargo ciertas situaciones particulares en las que esta hipótesis se puede debilitar. En este sentido, el siguiente es un caso importante, ya que nos permite estimar la altura de la variedad en términos de la altura de la fibra en un punto no ramificado.

Teorema 2.3.7 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x := (x_1, \ldots, x_n) \mapsto \pi(x) := (x_1, \ldots, x_r)$. Supongamos que π es dominante y separable de grado δ. Sea $F_1, \ldots, F_{n-r} \in k[x_1, \ldots, x_n]$ una intersección completa reducida tal que $V \subseteq V(F_1, \ldots, F_{n-r})$. Sea $p \in \mathbb{A}^r$ un punto no ramificado de π. Entonces*

$$h(V) \leq 6\, n^4 (\deg f + \overline{h}(f))\, (d(F)\, (\overline{h}(p) + 2) + \overline{h}(F))\, \deg^2 V\, h(V_0)$$

Demostración. Alcanza con considerar el caso en que V es irreducible.

Consideramos la proyección genérica $\varpi : \mathbb{A}^{r(n+1)} \times V \to \mathbb{A}^{r(n+1)} \times \mathbb{A}^r$ definida por $(b, G, x) \mapsto (b, G, b + G \cdot x)$ para $(b, G) \in \mathbb{A}^{r(n+1)}$ y $x \in V$. Esta proyección es dominante y separable y se tiene $\deg \varpi = \deg V$ [69].

Sea G al matriz con filas $G_i := (0, \ldots, 1, \ldots, 0)$ para $i = 1, \ldots, r$. El punto $P := (0, G, p)$ es entonces un punto no ramificado de ϖ,

Sea $\chi(t) := t^\delta + b_{\delta-1}\, t^{\delta-1} + \cdots + b_0 \in k(\mathbb{A}^{r(n+1)})[\mathbb{A}^r][t]$ el polinomio característico de la forma lineal genérica $\eta_{r+1} := U_{r+1,0} + U_{r+1,1}\, x_1 + \cdots + U_{r+1,n}\, x_n$. Este polinomio coincide con el polinomio característico P_V de V, salvo por un factor en $k(\mathbb{A}^{r(n+1)})^*$.

Sea $a \in k[\mathbb{A}^{r(n+1)}] - \{0\}$ el coeficiente de η_{r+1}^δ en P_V. Luego a es un polinomio multihomogéneo de grado δ en cada grupo de variables $U_1, \ldots U_r$. Se tiene entonces $\chi = P_v / a$, y en particular $b_0(U, 0) = f_V / a$.

Por otra parte sea ψ_i la inversa local de ϖ en ξ_i. Luego

$$\chi = \prod (t - \eta_{r+1}(\psi_i))$$

El Lema Principal 2.3.2 nos permite entonces estimar los coeficientes de la serie de potencias de f_V / a.

Vamos a acotar ahora la altura de f_V. La clave de este resultado es la simetría de f_V y del hecho de que a no depende del grupo de variables U_{r+1}.

Sea $\Phi := a(U_2, \ldots, U_{r+1}) / A(U_1, \ldots, U_r)$. Esta función puede calcularse como $\Phi = (f_V / a(U_1, \ldots, U_r)) / (f_V / a(U_2, \ldots, U_{r+1}))$ por la simetría de f_V con respecto a permutaciones de variables. Luego

$$1/AaU_1, \ldots, U_r) = \Phi(U_1, \ldots, U_{r+1}) / a(U_2, \ldots, U_{r+1})$$

y por lo tanto $1/a(U_1, \ldots, U_r) = \Phi(U_1, \ldots, U_r, 1) / a(U_2, \ldots, U_r, b_{r+1})$ para todo b_{r+1} que no anule el denominador. Luego

$$1/a(U_1, \ldots, U_r) = \Phi(U_1, \ldots, U_r, b_{r+1}) \cdots \Phi(U_r, b_1, \ldots, b_{r-1}) / A(b_1, \ldots, b_{r-1})$$

y por lo tanto

$$f_V = b_0(U,0)\cdot \Phi(U_1,\dots,U_r,1)\cdots\Phi(U_r,1,\dots,1)/A(1)$$

Luego calculamos los coeficientes de esta expresión hasta grado $n\,\delta$ y obtenemos la cota anunciada.

□

Luego la altura de una variedad intersección completa está polinomialmente acotada por su grado, número de variedades, grado de los polinomios que la definen, y la altura de una fibra no ramificada.

Recíprocamente podemos acotar la altura de una fibra en términos de la altura de la variedad.

Vamos a considerar el caso de una proyección *lineal.* El caso general es una consecuencia de la desigualdad de Bézout aritmética, y se va a tratar en la Sección 4.

Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1,\dots,x_r)$. Supongamos que π es dominante y separable. Este es el caso, por ejemplo, si $x_1,\dots,x_r$ están en posición de Noether separable con respecto a V. Sea $p\in \mathbb{A}^r$. Luego

$$h(\pi^{-1}(p)) \le h(V) + r\deg V\, h(p) + 4r\log(n+1)\deg V$$

Lema 2.3.8 *Sea $V\subseteq \mathbb{A}^r$ una variedad equidimensional con $r := \dim V$. Sean $x_1,\dots,x_r$ variables en posición de Noether.*

Sea $E := k(\mathbb{A}^n)$ y $F := E\otimes_k k[V]$. Para $f\in F$ denotamos por $\eta_f : F\to F$ la aplicación lineal $g\mapsto fg$. Entonces $f\in B$ es un divisor de cero si y sólo si $\det(\eta_f) = 0$.

Demostración. Se tiene que f es un divisor de cero en $k[V]$ si y sólo si es un divisor de cero en F. El álgebra F es un E-espacio vectorial de dimensión finita y por lo tanto f es un divisor de cero si y sólo si η_f no es inyectiva, lo cual equivale a la condición $\det(\eta_f) = 0$. □

Lema 2.3.9 *Sean $f_i\in k[x_1,\dots,x_n][y_i]$ polinomios separables no nulos para $i=1,\dots,m$. Entonces $f_1,\dots,f_m$ es una sucesión regular reducida.*

Demostración. El ideal $I := (f_1,\dots,f_m)$ es radical en $k[x,y]$ si y sólo si es radical en $k(x)[y]$. Luego alcanza con considerar el caso $n=0$.

Sea J el Jacobiano de $f_1,\dots,f_m$. Se tiene

$$J := \det(\frac{\partial f_i}{\partial y_j}) = (\frac{\partial f_1}{\partial y_1})\cdots(\frac{\partial f_m}{\partial y_m})$$

Luego J no es un divisor de cero módulo I, y por lo tanto I es radical por el criterio del Jacobiano [43, Teorema 18.15]. □

Sea F_i la ecuación de la proyección $V \to \mathbb{A}^{r+1}$ definida por $x \mapsto (\pi(x), x_i)$ para $i = r+1, \ldots, n$. Luego F_i es separable, y por lo tanto $F_{r+1}, \ldots, F_n$ es una intersección completa reducida que contiene a V como una de sus componentes. Sea $J \in k[x_1, \ldots, x_n]$ el Jacobiano de F con respecto a las variables $x_{r+1}, \ldots, x_n$, es decir

$$J := \det(\frac{\partial F_i}{\partial x_j})_{ij}$$

y sea $\Delta : \det \eta_J$ la norma de J. Luego $\Delta \in k[x_1, \ldots, x_r] - \{0\}$ es un polinomio de grado $\leq (n-r)\delta^{n-r}$. Luego $p \in \mathbb{A}^r$ es un punto no ramificado de $\pi : V(F_{r+1}, \ldots, F_n) \to \mathbb{A}^r$ si y sólo si $\Delta(p) \neq 0$. En particular podemos suponer

$$h(p) \leq n \log \delta + \log n$$

Concluímos que existe un punto no ramificado $p \in \mathbb{A}^r$ de altura acotada por $n \log \delta + \log n$ tal que

$$h(\pi^{-1}(p)) \leq h(V) + n^2 \delta \log \delta + 4n \log(n+1)\delta$$

En particular obtenemos una cota para la altura del polinomio minimal de un elemento en $k[V]$. Este resultado es análogo aritmético de [119, Proposición 1].

Corolario 2.3.10 *Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional, con $r := \dim V$. Sean $x_1, \ldots, x_r$ variables en posición de Noether separable.*

Sea $f \in k[V]$ y sea $m_f \in k[\mathbb{A}^r][t]$ su polinomio minimal. Entonces

$$h(m_f) \leq 12n\delta^2\, h(V) + 6n\delta^2 \deg f\, h(V) + \delta^2 h(f) + \delta^3$$

Lema 2.3.11 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional, con $r := \dim V$. Entonces existe una sucesión regular reducida $F_1, \ldots, F_{n-r} \in k[x_1, \ldots, x_n]$ tal que $V \subseteq V(F_1, \ldots, F_{n-r})$, $\deg F_i \leq \deg V$ y $h(F_i) \leq h(V) + 2n \deg V$ para $i = 1, \ldots, n-r$.*

Demostración. Sean $x_1, \ldots, x_r$ variables tales que la proyección $\pi : V \to \mathbb{A}^r$ es finita. Luego tomamos F_i como la ecuación de la proyección $x \mapsto (\pi(x), x_i)$. □

En particular

$$\mathrm{Tr}\ f \leq 12n\delta^2\, h(V) + 6n\delta^2 \deg f\, h(V) + \delta^2 h(f) + \delta^3$$

2.3.3 Parametrizaciones

En esta sección vamos a estudiar la altura de la parametrización de una variedad en términos de un *elemento primitivo.* Las parametrizaciones permiten introducir otra noción de altura. Esta noción es natural en geometría algebraica computacional [56]. Mostramos que es equivalente en un sentido preciso a nuestra noción de altura.

Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional, con $r := \dim V$. Sean $x_1, \ldots, x_r$ variables en posición de Noether separable. Sean $E := k(\mathbb{A}^r)$, $F := E \otimes_k k[V]$ y sea $\eta \in k(V)$ un elemento primitivo. Es decir, $F = E[\eta]$. En lo que sigue vamos a considerar el caso en que η es una forma lineal. Sea $P \in k[\mathbb{A}^r][t]$ su polinomio minimal. Luego $P'k[V] \subseteq k[\mathbb{A}^r][\eta]$, y por lo tanto existen $v_{r+1}, \ldots, v_n \in k[\mathbb{A}^r][t]$ tales que

$$x_i = v_i(\eta)/P'(\eta) \qquad\qquad i = r+1, \ldots, n$$

Vamos a estimar los grados y las alturas de estas parametrizaciones v_i. Estas estimaciones son una consecuencia de la fórmula de traza de Tate (Sección ??).

Lema 2.3.12 *Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional, con $r := \dim V$. Sean $x_1, \ldots, x_n$ variables en posición de Noether separable. Sean $v_{r+1}, \ldots, x_n$ las parametrizaciones de $x_{r+1}, \ldots, x_n$ en términos de un elemento primitivo η. Entonces $\deg v_i \leq \delta^2 + \delta - 1$, $h(v_i) \leq \delta^2 h(V) + \log(n+1) h(\eta)\delta$*

Demostración. Sean $A := k[\mathbb{A}^r]$, $B := k[V]$. Sea $P \in A[t]$ el polinomio minimal de η. Luego $\deg P \leq \delta$. Escribimos

$$P(y) - P(x) = (y - x) \sum_{i=1}^{m} a_i(y) b_i(x)$$

con $a_i, b_i \in A[t]$. Podemos suponer $m \leq \delta^2$, $\deg a_i, \deg b_i \leq \delta - 1$ y $h(a_i), h(b_i) \leq h(P) + \log \delta$. Aplicamos la fórmula de Tate a este caso y obtenemos

$$P'f = \sum \mathrm{Tr}\ (f b_i) a_i(\eta) = v_i(\eta)$$

para $f \in k[V]$. Aplicamos esta fórmula al caso $f := x_j$. Tenemos $\deg \mathrm{Tr}\ (x_j b_i) \leq \delta^2$, $h(\mathrm{Tr}\ (x) j b_i) \leq \delta^2 h(V) + \log(n+1)\delta$ y por lo tanto concluímos $\deg v_i \leq \delta^2 + \delta - 1$, $h(v_i) \leq \delta^2 h(V) + \log(n+1) h(\eta)\delta$. $\square$

Lema 2.3.13 *Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional, con $r := \dim V$. Sean $x_1, \ldots, x_r$ variables en posición de Noether separable tal que $[k(V) : k(\mathbb{A}^r)] = \deg V$. Sea $\eta = b_1 x_1 + \cdots + b_n x_n$ un elemento primitivo. Sea P el polinomio minimal de η y $v_1, \ldots, v_n$ las parametrizaciones correspondientes. Entonces*

$$\begin{aligned} h(P, v) &\leq \delta^2 h(V) + \log(n+1) h(\eta)\delta \\ h(V) &\leq 6n^3 d\, \delta^2 (h(P, v) + \delta^2) \end{aligned}$$

Demostración. Sea $p \in \mathbb{A}^r$ un punto no ramificado de π tal que $h(p) \leq n \log \delta + \log n$. Se tiene entonces que la fibra $\pi^{-1}(p)$ tiene altura acotada por $h(P, v) + n\delta^2 \log \delta$. Por los resultados del apartado anterior obtenemos

$$h(V) \leq 6n^3 d\, \delta^2 h(P, v) + 6n^3 d\, \delta^3$$

Recíprocamente tenemos $P_V(T(x)) \neq 0$ para $T_i := (0, \ldots, 1, \ldots, 0)$ ya que T es no ramificado. Luego $h(P) \leq h(V)$ y

$$h(v_i) \leq \delta^2 h(V) + \log(n+1) h(\eta)\delta$$

por el Lema 2.1.1. □

Sea $V \subseteq \mathbb{A}^n$ k-variedad equidimensional, con $r := \dim V$. Sean $y_i := a_{i1}x_1 + \cdots + a_{in}x_n$ para $i = 1, \ldots, n-r$ variables en posición de Noether separable con respecto a V y sea $\eta := b_1x_1 + \cdots + b_nx_n$ un elemento primitivo. Sea $P \in k[y_1, \ldots, y_{n-r}][t]$ el polinomio minimal de η. Luego $\rho k[V] \subseteq k[y_1, \ldots, y_{n-r}][t]$ donde $\rho \in k[y_1, \ldots, y_{n-r}] - \{0\}$ es el discriminante de P conrespecto a t. Sean $v_1, \ldots, v_n \in k[y_1, \ldots, y_{n-r}][t]$ tales que $\rho x_i = v_i(\eta)$ para $i = 1, \ldots, n$.

Luego

$$I(V)_\rho = (P(\eta), \rho x_1 - v_1(\eta), \ldots, \rho x_n - v_n(\eta))_\rho$$

Este sistema de polinomios se denomina una *solución geométrica* de V [56], [105]. Luego se define la *altura* de V con respecto a la posición de Noether a y el elemento b como la altura de la solución geométrica que determina, es decir

$$h(V, a, b) := \max\{\overline{h}(P), \overline{h}(\rho), \overline{h}(v_1), \ldots, \overline{h}(v_n)\}$$

Luego se define la *altura* $hsg(V)$ de V como el máximo de este parámetro para a, b tales que $\overline{h}(a), \overline{b} \leq \deg(V)^{O(1)}$. Esta noción de altura fue introducida por Giusti et al. [56] para el caso en que V es intersección completa reducida, pero se extiende sin modificaciones esenciales al caso general.

Vamos a probar que esta noción de altura es equivalente a nuestra noción.

Corolario 2.3.14 *Sea $V \subseteq \mathbb{A}^n$ k-variedad equidimensional. Entonces*

$$\begin{aligned} hsg(V) &\leq \delta^2 h(V) + \log(n+1)\delta \\ h(V) &\leq 6n^3 d\, \delta^2 (hsg(V) + \delta^2) \end{aligned}$$

2.4 Aplicaciones

2.4.1 Una Desigualdad de Bézout Aritmética

En este apartado vamos a acotar la altura del producto y de la intersección de variedades. Para esto vamos a necesitar algunos resultados auxiliares.

Lema 2.4.1 *Sean $V \subseteq \mathbb{A}^m$, $W \subseteq \mathbb{A}^n$ variedades de dimensión 0. Entonces* $h(V \times W) \leq \deg(W)h(V) + \deg(V)h(W) + \log(m+n+1)\deg(V)\deg(W)$.

Demostración. Sean η y θ formas lineales genéricas en $k[\mathbb{A}^m]$ y en $k[\mathbb{A}^n]$ respectivamente. Sea

$$G := \prod_{\xi \in V} \prod_{\varsigma \in W} (\eta(\xi) + \theta(\varsigma))$$

Luego $G = \sum \eta(\xi)^i \theta(\varsigma)^j$. Cada término tiene altura acotada por $\deg(W)h(V) + \deg(W)$. Luego $h(G) \leq \deg(W)h(V) + \deg(V)h(W) + \log(m+n+1)\deg(V)\deg(W)$. El Lema se sigue entonces de la observación $f_{V \times W} = G(0)$. □

La siguiente es una estimación para la altura de un producto de variedades.

Teorema 2.4.2 *Sean $V_1, \ldots, V_l \subseteq \mathbb{A}^n$ variedades, con $r_i := \dim V_i$ y $\delta_i := \deg V_i$. Entonces*

$$h(V_i \times \cdots \times V_l) \leq 6l^3 n^3 (\prod \delta_i)^2 \max_i \delta_i \sum h(V_i)/\delta_i + (\prod \delta_i)^3$$

Demostración. Es suficiente considerar el caso en que V_i es irreducible para todo i. Sean $F_{i,1}, \ldots, F_{i,n-r_i} \in k[x_1, \ldots, x_n]$ tales que $\deg F_{ij} \leq \delta_i \, h(F_{ij}) \leq h(V_i)$ y $V_i \subseteq V(F_{i,1}, \ldots, F_{i,n-r_i})$. Luego F_{ij} es una sucesión regular en $k[\mathbb{A}^n]^{\otimes l}$ que contiene a $V_1 \times \cdots \times V_l$. Se tiene $\deg F_{ij} \leq \max_i \delta_i$ y $h(F_{ij}) \leq \max_i h(V_i)$.

Sea $p_i \in \mathbb{A}^n$ un punto no ramificado de $\pi_i : V_i \to \mathbb{A}^n$. Luego la fibra $\pi_i^{-1}(p) \subseteq V_i$ tiene altura acotada por $h(V_i)$. Luego $p := p_1 \times \cdots \times p_l$ es un punto no ramificado de $\pi := \pi_1 \times \cdots \times \pi_l$, y se tiene $\pi^{-1}(p) = \pi_1^{-1}(p_1) \times \cdots \times \pi_l^{-1}(p_l)$. Sean $r := \dim V_1 \times \cdots \times V_l = \sum r_i$ y $\delta := \deg V_1 \times \cdots \times V_l = \prod \delta_i$.

Luego

$$h(\pi^{-1}(p))/\delta \leq \sum h(V_i)/\delta_i + l \log(n+1)$$

y por lo tanto $h(V_1 \times \cdots \times V_l) \leq 6l^3 n^3 \max_i \delta_i \, \delta \sum h(V_i)/\delta_i + l^2 n^2 \delta^2$. □

Teorema 2.4.3 *(Desigualdad de Bézout Aritmética) Sean $V_1, \ldots, V_l \subseteq \mathbb{A}^n$ variedades, con $r_i := \dim V_i$, $\delta_i := \deg V_i$. Entonces*

$$h(V_1 \cap \cdots \cap V_l) \leq 6l^3 n^3 (\prod \delta_i)^2 \max_i \delta_i \sum h(V_i)/\delta_i + (\prod \delta_i)^3$$

Demostración. Se tiene $V_1 \cap \cdots \cap V_l = (V_1 \times \cdots \times V_l) \cap E$ donde $E \subseteq \mathbb{A}^{ln}$ es el espacio lineal $\{x_{11} - x_{21} = 0, \ldots, x_{1n} - x_{ln} = 0\}$. □

Corolario 2.4.4 *Sean $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ polinomios que definen una variedad V de dimensión cero. Sean $d := \max_i \deg f_i$, $h = \max_i h(f_i)$. Entonces*

$$h(V) \leq 6n^7 d^{2n+1} h + n^4 d^{3n}$$

Lema 2.4.5 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ un morfismo definido como $\varphi(x) := (\varphi_1(x), \ldots, \varphi_m(x))$ con $\varphi_i \in k[x_1, \ldots, x_n]$ y sea $V \subseteq \mathbb{A}^n$ una variedad. Sean $d := \max_i \deg \varphi_i$, $h := \max_i h(\varphi_i)$. Entonces*

$$h(\overline{\varphi(V)}) \leq 6(n+m)^6 d^{2n+1} \delta (h + h(V)) + 6(n+m)^2 d^{3n} \delta^2$$

Demostración. Sea $Z \subseteq \mathbb{A}^n \times \mathbb{A}^m$ el gráfico de φ restringido a V. Luego

$$Z = V(Y_1 - \varphi_1, \ldots, y_m - \varphi_m \cap V \times \mathbb{A}^m$$

y por lo tanto $h(\varphi(V)) = h(\pi(Z)) \leq h(Z) \leq 6(n+m)^6 d^{n+1} \delta (h + h(V)) + 6(n+m)^2 d^{2n} \delta^2$. □

2.4.2 Inversa de un Morfismo Birracional

Ahora consideramos el siguiente problema. Sea $\varphi : V \to W$ un morfismo birracional entre variedades aritméticas afines irreducibles $V \subseteq \mathbb{A}^n$ y $W \subseteq \mathbb{A}^m$. En esta situación queremos estimarla altura de su inversa.

Lema 2.4.6 *Sea $\varphi : V \to \mathbb{A}^m$ un morfismo birracional, con $V \subseteq \mathbb{A}^n$ variedad de dimensión r y grado δ. Sea $d := \deg \varphi$ y $h := h(\varphi)$. Entonces*

$$\deg \varphi^{-1} \leq d^m \delta \qquad h(\varphi^{-1}) \leq 6(n+m)^6 d^{2n+1} \delta (h + h(V)) + 6(n+m)^2 d^{3n} \delta^2$$

Demostración. Sea $\varphi^{-1} := \psi = (\psi_1, \ldots, \psi_n)$ Luego $\mathrm{Gr}\psi = \mathrm{Gr}\varphi$ y por lo tanto

$$\deg \mathrm{Gr}\psi \leq d^m \delta \qquad h(\mathrm{Gr}\psi) \leq 6(n+m)^6 d^{n+1} \delta (h + h(V)) + 6(n+m)^2 d^{2n} \delta^2$$

Sea $\pi_i : \mathrm{Gr}\psi \to \mathbb{A}^{m+1}$ definida como $(x, y) \mapsto (x_i, y)$. Luego $\overline{\pi_i(\mathrm{Gr}\psi)} = x_i - \psi_i$, y por lo tanto

$$\deg \psi_i \leq d^m \delta \qquad h(\psi_i) \leq 6(n+m)^6 d^{n+1} \delta (h + h(V)) + 6(n+m)^2 d^{2n} \delta^2$$

□

Este resultado también se puede obtener directamente de las estimaciones para el teorema de la función inversa en el caso en que $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ es un automorfismo, y en este caso la altura de la inversa depende sólo de la altura de una fibra.

Capítulo 3

Cotas para el Teorema de Ceros

3.1 Cotas de Grados

3.1.1 Notaciones y Convenciones

Denotamos por k un cuerpo infinito con una clausura algebraica denotada por $\overline{k}$. Todos los anillos a ser considerados en lo sucesivo son conmutativos y Noetherianos, y más precisamente k-álgebras finitamente generadas. El anillo de polinomios $k[x_0, \ldots, x_n]$ se denota alternativamente como S.

Como siempre, $\mathbb{P}^n$ y $\mathbb{A}^n$ denotan los espacios proyectivo y afín de dimensión n sobre $\overline{k}$, respectivamente. Una variedad no es necesariamente irreducible.

Sea J un ideal homogéneo en el anillo S/I. La *dimensión* de J se define como la dimensión de Krull del anillo cociente $(S/I)/J$ y se denota como $\dim J$. El *grado* de J se define como $(\dim J - 1)!$ veces el coeficiente principal del polinomio de Hilbert de la k-álgebra graduada $(S/I)/J$.

Sea $\varphi : A \to B$ un morfismo entre dos anillos, y sean I y J ideales de A y B respectivamente. Luego I^e denota la extensión del ideal I a B y J^c denota la contracción del ideal J a A. Dado un elemento $\alpha \in A$, denotamos por $\overline{\alpha}$ al elemento $\varphi(\alpha) \in B$. Vamos a usar esta notación cuando es claro del contexto el morfismo al cual nos referimos.

3.1.2 Un Nullstellensatz Efectivo sobre Anillos Graduados Cohen–Macaulay

Sea dado un ideal homogéneo Cohen-Macaulay I en el anillo $k[x_0, \ldots, x_n]$. Con esto queremos decir que el anillo cociente $k[x_0, \ldots, x_n]/I$ es un anillo Cohen–Macaulay. Sea r la dimensión de I. Suponemos también que está dado un elemento homogéneo p en S/I que no es un divisor de cero. Sean $\eta_1, \ldots, \eta_s \in S/I$ elementos homogéneos de grado uno –o formas lineales, por abuso de lenguaje– que definen la variedad vacía en el conjunto abierto $\{p \neq 0\}$ de $V(I)$. En esta situación, el teorema de ceros de Hilbert implica que

p pertenece al radical del ideal $(\eta_1, \ldots, \eta_s)$, esto es, $p \in \sqrt{(\eta_1, \ldots, \eta_s)}$. Equivalentemente tenemos que 1 está en el ideal $(\overline{\eta}_1, \ldots, \overline{\eta}_s)$ generado por $\overline{\eta}_1, \ldots, \overline{\eta}_s$ en el anillo $(S/I)_p$.

Vamos a dar una cota para el mínimo $D \in \mathbb{N}$ tal que p^D cae en el ideal $(\eta_1, \ldots, \eta_s)$ (Lema Principal 3.1.7). Esta cota depende del número de formas lineales, la dimensión y el grado del ideal I. Como una consecuencia de este resultado derivamos un teorema de ceros efectivo para anillos graduados Cohen–Macaulay (Teorema 3.1.9 y Corolario 3.1.3).

Sea A un anillo y sean $\alpha_1, \ldots, \alpha_t$ elementos de A. Entonces $\alpha_1, \ldots, \alpha_t$ se llama una *sucesión regular débil* si $\overline{\alpha}_i$ es un no–divisor de cero en el anillo $A/(\alpha_1, \ldots, \alpha_{i-1})$ for $i = 1, \ldots, t$. Notamos que esta definición defiere de la noción usual de sucesión regular sólo en un punto, en que permite que $\overline{\alpha}_t$ sea una unidad en $A/(\alpha_1, \ldots, \alpha_{t-1})$.

Lema 3.1.1 *Sean las notaciones como antes. Entonces existen formas lineales* $\zeta_1, \ldots, \zeta_t \in (\eta_1, \ldots, \eta_s)$ *para algún* $t \leq \min\{r, s\}$ *tales que* $\overline{\zeta}_1, \ldots, \overline{\zeta}_t$ *es una sucesión regular débil en* $(S/I)_p$ *y* $1 \in (\overline{\zeta}_1, \ldots, \overline{\zeta}_t)$

Demostración. Sean $z_i := \sum_{j=1}^{s} \lambda_{ij} \overline{\eta}_j$ combinaciones k-lineales genéricas de $\overline{\eta}_1, \ldots, \overline{\eta}_s$ para $i = 1, \ldots, s$. Se obtiene una sucesión secante maximal $z_1, \ldots, z_t$ para algún $t \leq s$, ya que el cuerpo k es infinito. Con esto queremos decir que $\dim(z_1, \ldots, z_i) = r - i - 1$ for $i = 1, \ldots, t-1$ y que $1 \in (z_1, \ldots, z_t)$. En particular vale $t \leq \min\{r, s\}$.

El anillo $(S/I)_p$ es Cohen–Macaulay ya que es la localización de un anillo Cohen–Macaulay. Luego $z_1, \ldots, z_t$ es una sucesión regular en $(S/I)_p$.

Tomamos $\zeta_i := \sum_{j=1}^{s} \lambda_{ij} \eta_j$ para $i = 1, \ldots, t$. Luego $\zeta_i \in (\eta_1, \ldots, \eta_s)$ y $\overline{\zeta}_i = z_i$ para $i = 1, \ldots, s$ como se quería. □

Luego podemos suponer sin pérdida de generalidad que $\overline{\eta}_1, \ldots, \overline{\eta}_s$ es una sucesión regular débil en $(S/I)_p$ y que vale $s \leq r$. Asumimos esto de ahora en adelante. Luego vamos a mostrar que $\eta_1, \ldots, \eta_s$ pueden ser reemplazados por polinomios de grado controlado que forman una sucesión regular en S/I (Corolario 3.1.3).

El siguiente lema es una generalización de [69, Remark 4].

Lema 3.1.2 *Sea dado un ideal homogéneo equidimensional* $K \subseteq k[x_0, \ldots, x_n]$ *y puntos* $\xi_1, \ldots, \xi_m \in \mathbb{P}^n$ *fuera de* $V(K)$. *Entonces existe un polinomio homogéneo* g *en* K *tal que* $\deg g \leq \deg K$ *y que vale* $g(\xi_i) \neq 0$.

Demostración. El caso en que K es un ideal primo homogéneo se sigue directamente de [69, Remark 4].

Consideremos el caso general. Para cada ideal primo asociado P de K tomamos un polinomio homogéneo g_P tal que $\deg g_P \leq \deg P$ y $g_P(\xi_i) \neq 0$ para $i = 1, \ldots, m$. Sea Q_P el el ideal P-primario correspondiente en la descomposición de K. Sea $l(Q_P)$ la longitud de Q_P, esto es, la longitud de $(S/Q_P)_P$ como un S/P-módulo. Entonces sea

$$g := \prod_P g_P^{l(Q_P)},$$

donde el producto se toma sobre todos los ideales primos asociados de K. Luego $g(\xi_i) \neq 0$ para $i = 1, \ldots, m$, y tenemos también que el polinomio g está en el ideal K por [27, Lemma 1] y la cota de grado $\deg g \leq \sum_P l(Q_P) \deg P = \deg K$ vale por [136, Proposición 1.49]. Se sigue que g satisface las condiciones enunciadas. □

En lo que sigue vamos a denotar por J_i la contracción al anillo S/I del ideal $(\overline{\eta}_1, \ldots, \overline{\eta}_i) \subseteq (S/I)_p$ y por δ_i el grado del ideal homogéneo J_i para $i = 1, \ldots, s$.

Corolario 3.1.3 *Sean la notaciones como antes. Entonces existen elementos homogéneos $h_1, \ldots, h_s \in S/I$ que satisfacen las siguientes condiciones:*

i) $h_i \equiv p^{c_i}\eta_i \mod J_{i-1}$ *para algún* $c_i \geq 0$,

ii) $h_1, \ldots, h_s$ *es una sucesión regular,*

iii) $\deg h_i \leq \deg J_{i-1} + \deg p - 1$,

for $i = 1, \ldots, s$.

Demostración. Procedemos por inducción en i. Por hipótesis p es un no–divisor de cero en S/I y por lo tanto el morfismo canónico $S/I \to (S/I)_p$ es inyectivo. El hecho de que $\overline{\eta}_1$ no sea un divisor de cero en $(S/I)_p$ inplica que η_1 no es un divisor de cero en S/I.

Ahora sea $i \geq 2$ y supongamos que los elementos $h_1, \ldots, h_{i-1}$ ya están construídos. Sea H_{i-1} el ideal generado por $h_1, \ldots, h_{i-1}$ en S/I. Sea $H_{i-1} = (\cap_j Q_j) \cap (\cap_l R_l)$ la descomposición primaria de H_{i-1}, con $p \notin \sqrt{Q_j}$ y $p \in \sqrt{R_l}$. Nuestro objetivo es encontrar un elemento homogéneo h_i en S/I que no esté en ninguno de los ideales primarios asociados de H_{i-1}.

Recordamos que el ideal H_{i-1} no tiene componentes inmers ya que está generado por una sucesión regular en un anillo Cohen–Macaulay. Por otro lado el ideal J_{i-1} tiene la descomposición primaria $\cap_j Q_j$ y por lo tanto se sigue que $V(R_l) \not\subseteq V(J_{i-1})$ vale para cada l. Elegimos un punto ξ_l que esté en $V(R_l) - V(J_{i-1})$ y un elemento homogéneo $g \in J_{i-1}$ tal que $\deg g \leq \deg J_{i-1}$ y $g(\xi_l) \neq 0$ para cada l. La existencia de g está garantizada por el lema previo. Multiplicando eventualmente a g con formas lineales podemos suponer sin pérdida de generalidad que vale $\deg g = c_i \deg p + 1$ para algún $c_i \geq 0$. En particular podemos asumir que vale $\deg g \leq \deg J_{i-1} + \deg p - 1$. Finalmente ponemos

$$h_i := ag + p^{c_i}\eta_i$$

para algún escalar $a \in k$ indeterminado. Entonces h_i es homogéneo y vale $h_i \equiv p^{c_i}\eta_i \mod J_{i-1}$. Luego h_i no pertenece a $\sqrt{Q_j}$, ya que tanto p como eta_i no son divisores de cero modulo J_{i-1}. Tenemos también que $h_i(\xi_l) = a\,g(\xi_l) + (p^{c_i}\eta_i)(\xi_l) \neq 0$ para una elección genérica de a, lo cual fuerza $h_i \notin \sqrt{R_l}$. □

Fijamos la siguiente notación. Sean $h_1, \ldots, h_s \in S/I$ los polinomios homogéneos introducidos en el Corolario 3.1.3, y sean $H_i := (h_1, \ldots, h_i)$ y $L_i := (\eta_1, \ldots, \eta_i)$ los ideales homogéneos sucesivamente generados por $h_1, \ldots, h_s$ y $\eta_1, \ldots, \eta_s$ respectivamente.

Escribamos $h_i = l_i + p^{c_i}\eta_i$ para algún $l_i \in J_{i-1}$ y $c_i \geq 0$. Luego pongamos $\gamma_i := \delta_{i-1} - \delta_i$, y sea $\lambda_i := \sum_{j=1}^{i}(\gamma_j + c_j)$ y $\mu_i := \sum_{j=1}^{i}((i-j+1)\gamma_j + (i-j)c_j)$ para $i = 1, \ldots, s$.

Dado un ideal K in S/I denotamos como K^u la parte equidimensional de K, esto es, el ideal equidimensional dado como la intersección de las componentes primarias de K de dimensión máxima.

Lema 3.1.4 *Sea dado un elemento $q \in J_i$ para algún $1 \leq i \leq s$. Entonces $p^{\gamma_i}q \in (J_{i-1}, \eta_i)^u$.*

Demostración. Sea $(\cap_j Q_j) \cap (\cap_l R_l)$ la descomposición primaria del ideal $(J_{i-1}, \eta_i)^u$, con $p \notin \sqrt{Q_j}$ y $p \in \sqrt{R_l}$. Entonces el ideal J_i tiene la descomposición primaria $\cap_j Q_j$. Sea $K_i := \cap_l R_l$ la intersección de las otras componentes primarias. Entonces K_i es un ideal equidimensional que está contenido en la hipersuperficie $\{p = 0\}$.

Los ideales $(J_{i-1}, \eta_i)^u$ y (J_{i-1}, η_i) tienen el mismo grado ya que difieren sólo en un ideal de codimensión al menos $i+1$. El grado de (J_{i-1}, η_i) es δ_{i-1}, ya que η_i no es un divisor de cero mod J_{i-1}, y por lo tanto el grado de K_i es igual a $\gamma_i = \delta_{i-1} - \delta_i$. Luego p^{γ_i} está en el ideal K_i [27, Lemma 1] y concluimos que $p^{\gamma_i}q \in (\cap_j Q_j) \cap (\cap_l R_l) = (J_{i-1}, \eta_i)^u$ como enunciamos. □

Los dos siguientes enunciados (Lemas 3.1.5 y 3.1.6) son extensiones simples de [42, Lemmas 6.1 y 6.2].

Lema 3.1.5 *Sea dado un elemento $q \in J_i$ para algún $1 \leq i \leq s$. Entonces $p^{\lambda_i}q \in H_i$.*

Demostración. Procedemos por inducción en i. Primero $p^{\gamma_1}q \in (\eta_1)^u$ por Lema 3.1.4. Tenemos también que $(\eta_1)^u = (\eta_1)$ y por lo tanto la afirmación es válida para $i = 1$.

Sea $i \geq 2$ y asumamos que el enunciado vale para $i-1$. Por Lema 3.1.4, $p^{\gamma_i}q \in (J_{i-1}, \eta_i)^u$, esto es, $p^{\gamma_i}q$ pertenece a la intersección de las componentes primarias de dimensión $r-i$ del ideal (J_{i-1}, η_i). La intersección de las otras componentes primarias es un ideal de codimensión al menos $i+1$. Luego existe una sucesión regular $w_1, \ldots, w_{i+1}$ dentor de este ideal, ya que S/I es un anillo Cohen–Macaulay. Tenemos que $w_j p^{\gamma_i} q \in (J_{i-1}, \eta_i)$ y por lo tanto existe $u_j \in J_{i-1}$ y $v_j \in S/I$ tales que $w_j p^{\gamma_i} q = u_j + v_j\eta_i$ para $j = 1, \ldots, i+1$. Entonces

$$w_j p^{\gamma_i + c_i} q = p^{c_i} u_j + p^{c_i} v_j \eta_i = p^{c_i} u_j + v_j(h_i - l_i) = (p^{c_i} u_j - v_j l_i) + v_j h_i.$$

Luego $p^{\gamma_i + c_i} u_j - v_j l_i \in J_{i-1}$ y por la hipótesis inductiva $p^{\lambda_{i-1}}(p^{\gamma_i + c_i} u_j - v_j l_i)$ está en el ideal H_{i-1}. Entonces $w_j p^{\lambda_i} q \in H_i$ holds for $j = 1, \ldots, i+1$, ya que $\lambda_i = \lambda_{i-1} + \gamma_i - c_i$.

El ideal H_i está generado por una sucesión regular $h_1, \ldots, h_i$ y y por lo tanto es un ideal equidimensional de dimensión $r-i$. Luego para cada ideal primo asociado P de H_i existe algún j tal que $w_j \notin P$. Concluímos que $p^{\lambda_i} q \in H_i$. □

Lema 3.1.6 *Sean dados un elemento $q \in J_i$ para algún $1 \leq i \leq s$. Entonces $p^{\mu_i} q \in L_i$.*

Demostración. Vamos a proceder por inducción en i. El caso $i = 1$ se sigue de la misma forma que en el lema anterior porque $L_1 = H_1$ y $\mu_1 = \lambda_1$.

Sea $i \geq 2$. Entonces $p^{\lambda_i} q$ está en H_i por el Lema 3.1.5. Escribamos $p^{\lambda_i} q = u + v\, h_i$ para algún $u \in H_{i-1}$ y $v \in S/I$. Luego $p^{\lambda_i} q - v\, h_i \in H_{i-1}$ y por lo tanto $p^{\lambda_i} q - p^{c_i}\, v\, \eta_i$ está en el ideal J_{i-1} porque $H_{i-1} \subseteq J_{i-1}$ y $h_i \equiv p^{c_i}\, \eta_i \mod J_{i-1}$. Esto implica a su vez que $p^{\lambda_i - c_i} q - v\, \eta_i \in J_{i-1}$.

De la hipótesis inductiva obtenemos que $p^{\mu_{i-1}}(p^{\lambda_i - c_i}\, q - v\, \eta_i$ está en L_{i-1} y por lo tanto $p^{\mu_{i-1} + \lambda_i - c_i} q \in L_i$. El enunciado se sigue de la observación de que $\mu_i = \mu_{i-1} + \lambda_i - c_i$. □

Lema Principal 3.1.7 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo Cohen–Macaulay de dimensión r. Sea dado además un elemento homogéneo $p \in k[x_0, \ldots, x_n]/I$ que no es un divisor de cero y formas lineales $\eta_1, \ldots, \eta_s \in k[x_0, \ldots, x_n]/I$ tales que p está en el radical del ideal $(\eta_1, \ldots, \eta_s)$. Entonces*

$$p^D \in (\eta_1, \ldots, \eta_s)$$

con $D := \min\{r, s\}^2 \deg I$.

Demostración. Por Lema 3.1.1 podemos suponer sin pérdida de generalidad que $\overline{\eta}_1 \ldots, \overline{\eta}_s$ es una sucesión regular débil en $(S/I)_p$ y que $s \leq r$. Por Lema 3.1.6 sólo queda acotar μ_s. Hacemos uso de las estimaciones $\gamma_i, c_i \leq \delta_{i-1}$ y obtenemos la cota

$$\begin{aligned} \mu_s &= \textstyle\sum_{j=1}^{s}((s-j+1)\gamma_j + (s-j)c_j) \\ &\leq \textstyle\sum_{j=1}^{s}((s-j+1)\delta_{j-1} + (s-j)\delta_{j-1}) \leq s^2 \deg I. \end{aligned}$$

□

Comparar con Caniglia, Galligo y Heintz [29, Proposiciíon 10], Smietanski [124, Lema 1.44], y Sturmfels, Trung y Vogel [131, Teoremas 2.1 y 5.3]

El resto de la sección está dedicado a la extensión de los resultados previos al caso en que tenemos dados elementos homogéneos de grado arbitrario en lugar de formas lineales. Primero establecemos algunas generalidades sobre la inmersión de Veronese.

Denotemos por N el entero $\binom{n+d}{d} - 1$ y sean $a_0, \ldots, a_N$ los exponentes de los distintos monomios de grado d en S. Sea

$$v_d : \mathbb{P}^n \to \mathbb{P}^N, \qquad x := (x_0 : \cdots : x_n) \mapsto (x^{a_0} : \cdots : x^{a_N})$$

la aplicación de Veronese. Este es un morfismo regular de variedades proyectivas y por lo tanto su imagen es una subvariedad cerrada de $\mathbb{P}^N$. Esta variedad se llama la variedad de Veronese y se denota como $v_{n,d}$. Sea $I(v_{n,d})$ su ideal de definición y denotemos por $S(d) := k[y_0, \ldots, y_N]/I(v_{n,d})$ su anillocde coordenadas homogéneo. La aplicación de Veronese induce entonces una inclusión de k-álgebras $i_d : S(d) \hookrightarrow S$ definida por $y_j \mapsto x^{a_j}$ para $j = 0, \ldots, N$.

Sea dado un ideal J en S y sea $J(d)$ su contracción al anillo $S(d)$. Identificando al anillo cociente $S(d)/J(d)$ con su imagen en S/J a través de la inclusión $i_d : S(d)/J(d) \hookrightarrow S/J$ obtenemos la descomposición en partes graduadas

$$S(d)/J(d) = \oplus_j (S/J)_{dj}.$$

Sean $h_{J(d)}$ y h_J las funciones de Hilbert de $J(d)$ y J respectivamente. Entonces $h_{J(d)}(m) = h_J(dm)$ para $m \in \mathbb{N}$. Se sigue que los ideales $J(d)$ y J tienen la misma dimensión y sus grados estan relacionados por la fórmula $\deg J(d) = d^{\dim J - 1} \deg J$.

Lema 3.1.8 *Sea J un ideal homogéneo Cohen-Macaulay en S y sea $J(d)$ su contración al anillo $S(d)$. Entonces $J(d)$ es un ideal Cohen-Macaulay.*

Demostración. Denotemos por A y B los anillos cocientes $S(d)/J(d)$ y S/J respectivamente. Identificamos A con su imagen en B a través de la inclusión i_d.

Vamos a probar que A es un anillo Cohen-Macaulay. Como A es un anillo garduado, alcanza con exhibir una sucesión regular de elementos homogéneos de longitud igual a la dimensión de A.

Sea e la dimensión del anillo B, que es también la dimensión de A. Sea $\beta_1, \ldots, \beta_e$ una sucesión regular en B de elementos homogéneos. Sean $\alpha_i := \beta_i^d$ para $i = 1, \ldots, e$. Entonces $\alpha_1, \ldots, \alpha_e$ son elementos de A que forman una sucesión regular en B, por [101, Theorem. 16.1]. Afirmamos que también forman una sucesión regular maximal en A. Sólo tenemso que probar que α_i no es un divisor de cero en $A/(\alpha_1, \ldots, \alpha_{i-1})$ para $i = 1, \ldots, e$. Sea $\zeta \in A$ un elemento tal que $\zeta \alpha_i \in (\alpha_1, \ldots, \alpha_{i-1})$. Entonces existen elementos homogéneos $\zeta_1, \ldots, \zeta_{i-1} \in B$ tales que $\zeta = \zeta_1\alpha_1 + \cdots + \zeta_{i-1}\alpha_{i-1}$ ya que $\alpha_1, \ldots, \alpha_{i-1}$ es una sucesión regular en B. Una verificación fácil muestra que $\zeta_1, \ldots, \zeta_{i-1}$ pueden ser elegidos de forma tal que estén en A, de donde se sigue que $\zeta \in (\alpha_1, \ldots, \alpha_{i-1})$. □

Teorema 3.1.9 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo Cohen-Macaulay. Sea dado demás un elemento homogéneo $p \in k[x_1, \ldots, x_n]/I$ que no es un divisor de cero y elementos homogéneos $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]/I$ tales que p está en el radical del ideal $(f_1, \ldots, f_s)$. Sea r la dimensión de I y sea d el grado máximo de f_i para $i = 1, \ldots, s$. Entonces*

$$p^D \in (f_1, \ldots, f_s)$$

con $D := r^2 d^r \deg I$.

Demostración. Primero notamos que los cero en $V(I)$ de los polinomios $\{f_i\}_i$ coinciden con los ceros en $V(I)$ de los polinomios $\{x_j^{d-\deg f_i} f_i\}_{ij}$. Tenemos también que $x_j^{d-\deg f_i} f_i$ está en el ideal $(f_1, \ldots, f_s)$ para todo i y j. Entonces podemos suponer sin pérdida de generalidad que f_i es un polinomio homogéneo de grado d para $i = 1, \ldots, s$. Notamos sin embargo que el número de polinomios de entrada se agrandó en esta etapa preparativa.

Sea $i_d : S(d) \hookrightarrow S$ la inclusión de k-álgebras inducida por la aplicación de Veronese map y sea $I(d)$ la contracción del ideal I al anillo $S(d)$. Entonces tenemos la inclusión $i_d : S(d)/I(d) \hookrightarrow S/I$ y la descomposición in graded parts $i_d(S(d)/I(d)) = \oplus_j (S/I)_{dj}$. Tomamos una forma lineal $\eta_i \in S(d)/I(d)$ tal que $i_d(\eta_i) = f_i$ para $i = 1, \ldots, s$, que existe ya que la inclusión i_d es una biyección en grado uno. Tomamos también un elemento homogéneo $q \in S(d)/I(d)$ tal que $i_d(q) = p^d$.

La aplicación $v_d : V(I) \to V(I(d))$ es una aplicación dominante y regular de variedades proyectivas y por lo tanto es suryectiva. Luego los ceros de las formas lineales $\eta_1, \ldots, \eta_s$ están contenidos en la imagen de los ceros de los polinomios $f_1, \ldots, f_s$. Los ceros comunes de $f_1, \ldots, f_s$ están en la hipersuperficie $\{p^d = 0\}$ de $V(I)$ y tenemos además que $v_d(\{p^d = 0\}) = \{q = 0\}$. Entonces la subvariedad de $V(I(d))$ definida por $\eta_1, \ldots, \eta_s$ está en la hipersuperficie $\{q = 0\}$.

Por Lema 3.1.8 el ideal $I(d)$ es Cohen–Macaulay, y tenemos también que q no es un divisor de cero modulo $I(d)$. Luego estamos en las hipótesis del Lema Principal 3.1.7. Como consecuencia obtenemos que vale

$$q^{r^2 \deg I(d)} \in (\eta_1, \ldots, \eta_s).$$

Finalmente aplicamos el morfismo i_d a la expresión anterior y obtenemos que vale

$$p^{d\, r^2\, (d^{r-1} \deg I)} \in (f_1, \ldots, f_s),$$

ya que $\deg I(d) = d^{r-1} \deg I$. □

Corolario 3.1.10 *Sea dado un ideal $I \subsetneq k[x_1, \ldots, x_n]$. Asumamos además que la homogeneización I^h del ideal I en el anillo $k[x_0, \ldots, x_n]$ es un ideal Cohen-Macaulay. Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polinomios sin ceros comunes en la variedad afín $V(I)$. Entonces existen $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ tales que*

$$1 \equiv g_1 f_1 + \cdots + g_s f_s \qquad (\text{mod } I)$$

con $\deg g_i f_i \leq (r+1)^2 d^{r+1} \deg I^h$ *para* $i = 1, \ldots, s$.

Demostración. Por hipótesis el ideal I^h es un ideal homogéneo y Cohen–Macaulay de dimensión $r+1$. Tenemos también que x_0 no es un divisor de cero modulo I^h.

Sea f_i^h la homogeneización de f_i para $i = 1, \ldots, s$. Los polinomios homogéneos $f_1^h, \ldots, f_s^h$ no tienen ningún cero en común en $V(I^h)$ fuera del hiperplano $\{x_0 = 0\}$. Por Teorema 3.1.9 existen polinomios homogéneos $v_1, \ldots, v_s \in S$ tales que vale

$$x_0^{(r+1)^2 d^{r+1}} = v_1 f_1^h + \ldots + v_s f_s^h \qquad (\text{mod } I^h)$$

con $\deg v_i f_i^h = (r+1)^2 d^{r+1}$. El corolario se sigue entonces evaluando $x_0 := 1$. □

Sean las notaciones como en el Corolario 3.1.10. En el caso en que I es el ideal cero, esto es, en la situación del Nullstellensatz efectivo clásico, obtenemos la cota de grado

$$\deg g_i f_i \leq (r+1)^2 d^{r+1}.$$

3.1.3 Cotas Mejoradas para los Grados

En esta sección consideramos las cotas de grado en el Nullstellensatz. Vamos a aplicar los métodos usados en la Sección 1 en un modo directo –sin referencia a la aplicación de Veronese– en la situación del Nullstellensatz efectivo clásico. La demostración sigue las mismas líneas y por lo tanto vamos a omitir algunas verificaciones con el fin de evitar repeticiones innecesarias.

Asumamos que están dados polinomios homogéneos $f_1, \ldots, f_s$ en $k[x_0, \ldots, x_n]$ sin ceros comunes a distancia finita. En esta situación vamos a dar una cota para el mínimo $D \in \mathbb{N}$ tal que $x_0^D \in (f_1, \ldots, f_s)$.

Vamos a asumir sin pérdida de generalidad que $s \leq n+1$ y que $\overline{f}_1, \ldots, \overline{f}_s$ es una sucesión regular débil en $k[x_0, \ldots, x_n]_{x_0}$. Sea d_i el grado de f_i para $i = 1, \ldots, s$. Vamos a suponer también que $d_2 \geq \cdots \geq d_s$ y que vale $d_s \geq d_1$. Como antes estao polinomios pueden obtenerse como combinaciones lineales de los polinomios originales, eventualmente multiplicados por potencias de x_0.

Denotemos como antes por J_i la contracción al S del ideal $(\overline{f}_1, \ldots, \overline{f}_i) \subseteq S_{x_0}$ para $i = 1, \ldots, s$. Hacemos la convención $J_0 := (0)$.

Lema 3.1.11 *Sean las notaciones como antes. Entonces existen polinomios homogéneos $h_1, \ldots, h_s \in k[x_0, \ldots, x_n]$ que satisfacen las siguientes condiciones:*

i) $h_i \equiv x_0^{c_i} f_i \mod J_{i-1}$ *para algún* $c_i \in \mathbb{N}$,

ii) $h_1, \ldots, h_s$ *es una sucesión regular,*

iii) $\deg h_i \leq \max\{\deg J_{i-1}, \deg f_i\}$,

para $i = 1, \ldots, s$.

□

Introducimos la siguiente notación. Sea δ_i el grado del ideal homogéneo J_i para $i = 0, \ldots, s$. Recordamos la desigualdad de Bézout $\delta_i \leq \prod_{j=1}^{i} d_j$. Denotamos entonces por γ_i al entero $d_i \delta_{i-1} - \delta_i$ para $i = 1, \ldots, \min\{n, s\}$ y $\gamma_{n+1} := \delta_n + d_{n+1} - 1$. También sea $\delta := \max\{\delta_i : i = 1, \ldots, s-1\}$ y $d := \max\{d_i : i = 1, \ldots, s-1\}$.

Recordamos que dado un ideal I en S denotamos por I^u su parte equidimensional.

Lema 3.1.12 *Sea dado un polinomio* $q \in J_i$ *para algún* $1 \leq i \leq s$. *Entonces* $x_0^{\gamma_i} q \in (J_{i-1}, \eta_i)^u$.

Demostración. El caso $i \leq n$ es exactamente como en el Lema 3.1.6. Luego vamos a considerar sólo el caso $i = n+1$.

El ideal J_n tiene dimensión uno y su grado es δ_n. Luego $(J_n, f_{n+1})_m = S_m$ para $m \geq \delta_n + d_{n+1} - 1$ ya que f_{n+1} no es un divisor de cero modulo J_n [125, Theorem. 2.23]. Se sigue que $x_0^{\gamma_{n+1}} \in (J_n, f_{n+1})$ y en particular $x_0^{\gamma_{n+1}} q \in (J_n, f_{n+1})^u$. □

Ahora sean $h_1, \ldots, h_s$ los polinomios homogéneos introducidos en el Lema 3.1.11. Ponemos $\mu_i := \sum_{j=2}^{i}((i-j+1)\gamma_j + (i-j)c_j)$ para $i = 1, \ldots, \min\{n, s\}$ y $\mu_{n+1} := \mu_n + \gamma_{n+1}$, donde c_i denota el entero $\deg h_i - \deg f_i$.

Denotamos por L_i al ideal homogéneo $(f_1, \ldots, f_i)$ para $i = 1, \ldots, s$.

Lema 3.1.13 *Sea dado un polinomio* $q \in J_i$ *para algún* $1 \leq i \leq s$. *Entonces* $x_0^{\mu_i} q \in L_i$.

Demostración. El caso $i \leq n$ es exactamente como en el Lema 3.1.6. Luego vamos a considerar sólo el caso $i = n+1$.

Por el lema anterior $x_0^{\gamma_{n+1}} q \in (J_n, f_{n+1})^u = (J_n, f_{n+1})$ y por lo tanto $x_0^{\gamma_{n+1}} q - u\, f_{n+1} \in J_n$ para algún polinomio $u \in S$. Aplicamos entonces la hipótesis inductiva y obtenemos que $x_0^{\mu_n}(x_0^{\gamma_{n+1}} q - u\, f_{n+1}) \in L_n$ de donde se sigue que $x_0^{\mu_{n+1}} q \in L_{n+1}$. □

Sólo queda entonces acotar μ_s. Vamos a tratar dos tipos diferentes de cotas. Una depende como simepre del número de variables y de los grados de los polinomios de entrada, y la otra depende además de los grados de ciertos ideales asociados a esots polinomios.

Lema 3.1.14 *Sean las notaciones como antes. Entonces* $\mu_s \leq \min\{n, s\}^2 d\, \delta$. *En el caso en que* $\deg f_i \geq 2$ *para* $i = 1, \ldots, s$ *tenemos que* $\mu_s \leq 2 \prod_{j=1}^{\min\{n,s\}} d_j$.

Demostración. Descomponemos el entero μ_s en dos términos y los estimamos separadamente. Primero consideramos el término $\sum_{j=2}^{s}(s-j)\, c_j$. We have that $c_i \leq \max\{\delta_{i-1} - d_i, 0\}$. En particular $c_2 = 0$ como $\delta_1 = d_1$ y $d_1 \leq d_2$. Entonces

$$\begin{aligned}
\textstyle\sum_{j=2}^{s}(s-j)\, c_j &\leq \textstyle\sum_{j=3}^{s-1}(s-j)\,(d_1 \cdots d_{j-1} - d_j) \\
&\leq \textstyle(\sum_{j=3}^{s-1}(s-j)/d_j \cdots d_{s-2})\, d_1 \cdots d_{s-2} - \sum_{j=2}^{s-1}(s-j)\, d_j \\
&\leq 4\, d_1 \cdots d_{s-2} - d_{s-1},
\end{aligned}$$

bajo la hipótesis $d_i \geq 2$ for $i = 1, \ldots, s$. Tenemos también $\sum_{j=2}^{s-1}(s-j)\, c_j \leq \sum_{j=2}^{s-1}(s-j)\, \delta = \frac{1}{2}(s-2)(s-1)\, \delta$.

Ahora estimamos el otro término. Consideramos primero el caso $s \leq n$. Entonces

$$\begin{aligned}
\textstyle\sum_{j=2}^{s}(s-j+1)\,\gamma_j &= \textstyle\sum_{j=2}^{s}(s-j+1)\,(d_j\,\delta_{j-1}-\delta_j) \\
&= (s-1)\,d_2\,\delta_1 + \textstyle\sum_{j=3}^{s}((s-j+1)\,d_j-(s-j))\,\delta_{j-1}-\delta_n \\
&\leq d_1\cdots d_s - \delta_s,
\end{aligned}$$

de donde obtenemos la cota $\mu_s = \sum_{j=2}^{s}(s-j+1)\,\gamma_j + \sum_{j=2}^{s-1}(s-j)\,c_j \leq (d_1\cdots d_s - \delta_s) + (4\,d_1\cdots d_{s-2} - d_{s-1}) \leq 2\,d_1\cdots d_s$.

En el caso $s = n+1$ tenemos que $\mu_{n+1} = \mu_n + \gamma_{n+1}$ de donde se sigue que $\mu_{n+1} \leq (2\,d_1\cdots d_n - \delta_n - d_{n-1}) + (\delta_n + d_{n+1} - 1) \leq 2\,d_1\cdots d_n$.

Por otra parte tenemos también la estimación $\sum_{j=2}^{s}(s-j+1)\,\gamma_j \leq \frac{1}{2}(s-1)\,s\,d\,\delta$ de donde concluímos que vale $\mu_s \leq \frac{1}{2}(s-1)\,s\,d\,\delta + \frac{1}{2}(s-2)\,(s-1)\,\delta \leq (s-1)^2\,d\,\delta$ como enunciamos. □

Teorema 3.1.15 *Sean dados polinomios homogéneos $f_1,\ldots,f_s \in k[x_0,\ldots,x_n]$ tales que x_0 está en el radical del ideal $(f_1,\ldots,f_s)$. Sea d_i el grado de f_i para $i = 1,\ldots,s$ y asumamos que vale $d_1 \geq \cdots \geq d_s$. Entonces vale*

$$x_0^D \in (f_1,\ldots,f_s)$$

con $D := 2\,d_s\prod_{i=1}^{\min\{n,s\}-1} d_i$.

Demostración. Por Lemas 3.1.13 y 3.1.14 sólo queda considerar el caso en que algún f_i tiene grado uno.

Por hipótesis $f_1,\ldots,f_s$ están ordenados de forma tal que vale $d_1 \geq \cdots \geq d_s$. Sea r máximo tal que $d_r \geq 2$, de forma tal que los polinomios $f_{r+1},\ldots,f_s$ tienen todos grado uno. Podemos asumir sin pérdida de generalidad que son k-linealmenet independientes. Podemos suponer que ni 1 ni x_0 están en el k-espcio lineal generado por $f_{r+1},\ldots,f_s$ ya que si este es el caso el enunciado es trivial.

Sean $y_0,\ldots,y_{n+r-s-1} \in S$ polinomios de grado uno que completan $f_{r+1},\ldots,f_s$ a un cambio lineal de variables. Suponemos además que $y_0 = x_0$. La inclusion natural $k[y_0,\ldots,y_{n+r-s-1}] \hookrightarrow k[x_0,\ldots,x_n]/(f_{r+1},\ldots,f_s)$ es un isomorfismo. Sea v_i un polinomio homogéneo en $k[y_0,\ldots,y_{n+r-s-1}]$ tal que $v_i \equiv f_i \mod (f_{r+1},\ldots,f_s)$ para $i = 1,\ldots,r$. Entonces x_0 está en el radical del ideal $(v_1,\ldots,v_r)$ de $k[y_0,\ldots,y_{n+r-s-1}]$ y vale $\deg v_i \leq d_i$ para $i = 1,\ldots,r$.

Sea E el entero $2\prod_{i=1}^{r}\deg v_i$ de tal forma que $E \leq D := 2\,d_s\prod_{i=1}^{\min\{n,s\}-1} d_i$. Entonces $x_0^D \in (v_1,\ldots,v_r)$ de donde se sigue que $x_0^D \in (f_1,\ldots,f_s)$ como enunciamos. □

Luego la cota enunciada en la introducción se sigue de este resultado homogeneizando el sistema de entrada y considerando el grado de los polinomios en una representación de x_0^D.

Ahora vamos a probar el Teorema enunciado en la Introducción. Primero recordamos la definición de grado algebraico de un sistema polinomial.

Sean $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ polinomios sin ceros comunes en $\mathbb{A}^n$. Dado una matriz $s \times s$ $\lambda = (\lambda_{ij})_{ij}$ con entradas en $\overline{k}$ denotamos por $h_i(\lambda)$ las combinaciones lineales $\sum_j \lambda_{ij} g_j$ inducidas por λ para $i = 1, \ldots, s$. Consideramos el conjunto de matrices $s \times s$ Γ tales que para cualquier λ en Γ los polinomios $h_1(\lambda), \ldots, h_{t-1}(\lambda)$ forman una sucesión regular en $\overline{k}[x_1, \ldots, x_n]$ y $1 \in (h_1(\lambda), \ldots, h_t(\lambda))$ para algún $t = t(\lambda) \leq \min\{n, s\}$.

Para cada $\lambda \in \Gamma$ y $i = 1, \ldots, t-1$ denotamos por $J_i(\lambda) \subseteq k[x_0, \ldots, x_n]$ la homogeneización del ideal $(h_1(\lambda), \ldots, h_i(\lambda))$. Entonces sea $\delta(\lambda)$ el máximo grado de los ideales homogéneos $J_i(\lambda)$ para $i = 1, \ldots, t-1$.

El *grado algebraico* del sistema polinomial $g_1, \ldots, g_s$ se define como el mínimo de $\delta(\lambda)$ sobre todas las matrices $\lambda \in \Gamma$.

La noción de grado geométrico de [86] y [125] se define en una forma análoga como el mínimo de $\delta(\lambda)$ para $\lambda \in \Gamma$, con la hipótesis adicional de que los ideales $J_i(\lambda)$ son radicales para $i = 1, \ldots, t-1$. Otra diferencia es que en el caso en que la caracterísitica de k es positiva los polinomios $h_j(\lambda)$ se toman como combinaciones lineales de los polinomios $\{x_j f_i\}_{ij}$.

La noción de grado geométrico de [59] es similar a la de [86], [125], la única diferencia es que no se define como un mínimo sino como el valo de $\delta(\lambda)$ para una elección genérica de λ.

Luego el grado algebraico está acotado por el grado geométrico, en cualquiera de las versiones de este último que consideremos. El siguiente ejemplo muestra que en realidad puede ser mucho más chico. Es una variante de [86, Example].

Ejemplo 3.1.16 Consideremos el sistema polinomial

$$f_1 := 1 - x_1 x_2^d,\ f_2 := x_2 - x_3^d,\ \ldots,\ f_{n-1} := x_{n-1} - x_n^d,\ f_n := x_n^2$$

para algún $d \geq 3$. Es fácil verificar que estos polinomios no tienen ceros comunes en $\mathbb{A}^n$. Denotemos por δ_g y por δ_a el grado geométrico —en el sentido de [86], [125]— y el grado algebraico de este sistema polinomial, respectivamente. Vamos a calcular ambos enteros para este ejemplo particular.

Sea λ una matriz $l \times n$ con entradas en $\overline{k}$ para algún $l \leq n$, y sea $h_i := \sum_j \lambda_{ij} f_j$ las combinaciones lineales inducidas para $i = 1, \ldots, n$.

Aplicamos a esta matriz el método de eliminación de Gauss por filas, usando como pivots las columnas de λ por orden ascendiente. Operaciones elementales invertibles por filas producen polinomios $q_1, \ldots, q_l$ generan el mismo ideal que $h_1, \ldots, h_l$. Para nuestro sistema particular esto corresponde a la eliminación sucesiva de las variables $x_1, \ldots, x_n$ en las ecuaciones $h_1, \ldots, h_l$. Luego en el caso en que $l \leq n-1$ la variedad afín definida por $h_1, \ldots, h_l$ puede ser parametrizada expresando a las variables como funciones racionales de las variables libres. Se sigue en este caso que el ideal $(h_1, \ldots, h_l)$ tiene dimensiónal menos $n - l$.

Primero consideramos el grado geométrico de este sistema. Los polinomios $f_1, \ldots, f_n$ forman una sucesión regular débil, $1 \in (f_1, \ldots, f_n)$ y el ideal $(f_1, \ldots, f_i)$ es radical para $i = 1, \ldots, n-1$. Tenemos que $\deg V(f_1, \ldots, f_i) = d^i$ para $i = 1, \ldots, n-1$ de donde se sigue que $\delta_g \leq d^{n-1}$.

Por otra paret, sea λ una matriz $l \times n$ con entradas en $\overline{k}$ y sea $h_1, \ldots, h_l$ las combinaciones lineales correspondientes. Asumamos que $h_1, \ldots, h_l$ es una sucesión regular débil, $1 \in (h_1, \ldots, h_l)$ y que $(h_1, \ldots, h_i)$ es un ideal radical para $i = 1, \ldots, l$. En particulas obtenemos que l es igual a n y que $(h_1, \ldots, h_{n-1})$ es un ideal radical uno–dimensional.

Aplicamos el método de eliminación arriba descrito a la matriz formada por las primeras $n-1$ filas de λ y denotamos por $q_1, \ldots, q_{n-1}$ los polinomios obtenidos. Afirmamos que ninguna columna i falla en ser un pivot para $i = 1, \ldots, n-1$. Supongamos que no es el caso. Entonces $q_1, \ldots, q_{n-2}$ son polinomios que no dependen de x_n y que generan un ideal uno–dimensional en $\overline{k}[x_1, \ldots, x_{n-1}]$. Además $q_{n-1} = x_n^2$ y porl o tanto el ideal $(q_1, \ldots, q_{n-1}) \subseteq \overline{k}[x_1, \ldots, x_n]$ no es radical, contradiciendo nuestra hipótesis.

Luego existen escalares $a_1, \ldots, a_{n-1} \in \overline{k}$ tales que $q_i = f_i + a_i f_n$ para $i = 1, \ldots, n-1$. Deducimos que la variedad $V(h_1, \ldots, h_{n-1})$ puede ser parametrizada por una aplicación $\varphi :$ A char'27 $\to$ A char'27 definida por $t \mapsto \varphi(t) = (\varphi_1(t), \ldots, \varphi_n(t))$, donde $\varphi_i \in \overline{k}(t)$ es una función racional de grado d^{n-i} for $i = 1, \ldots, n$. Obtenemos que $\deg V(h_1, \ldots, h_{n-1}) = d^{n-1}$ de donde se sigue la cota inferior $\delta_g \geq d^{n-1}$. Combinando esto con la estimación previa concluímos que $\delta_g = d^{n-1}$.

Ahora consideramos el grado algebraico del sistema. Now we consider the algebraic degree of the system. Los polinomios $f_n, \ldots, f_1$ forman una sucesión regular débil y $1 \in (f_n, \ldots, f_1)$. Tenemos que $(f_n, \ldots, f_{n-i+1}) = (x_n^2, x_{n-1}, \ldots, x_{n-i+1})$ para $i = 1, \ldots, n$ de donde se sigue que $\delta_a \leq 2$. Además, cualquier combinación lineal no trivial de $f_1, \ldots, f_n$ tiene grado al menos dos y por lo tanto $\delta_a \geq 2$. Concluimos que $\delta_a = 2$.

Obtenemos la siguiente cota de grado por aplicación directa de los Lemas 3.1.13 y 3.1.14.

Teorema 3.1.17 *Sean dados polinomios homogéneos $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ tales que x_0 está en el radical del ideal $(f_1, \ldots, f_s)$. Sea f_i^a la afinización de f_i para $i = 1, \ldots, s$. Sea d el máximo grado de f_i para $i = 1, \ldots, s$ y sea δ el gardo del sistema polinomial $f_1^a, \ldots, f_s^a$. Entonces vale*

$$x_0^D \in (f_1, \ldots, f_s)$$

con $D := \min\{n, s\}^2 \, d \, \delta$.

□

Si aplicamos esta cota de grado al ejemplo anterior obtenemos que existen $g_1, \ldots, g_n \in k[x_1, \ldots, x_n]$ que satisfacen

$$1 = g_1 f_1 + \cdots + g_n f_n,$$

con $\deg g_i f_i \leq 2 n^2 d$ para $i = 1, \ldots, s$. de hecho tenemos la identidad

$$1 = f_1 + x_1 x_2^{d-1} f_2 + x_1 x_2^{d-1} x_3^{d-1} f_3 + \cdots + x_1 x_2^{d-1} \cdots x_{n-1}^{d-1} x_n^{d-2} f_n$$

3.2 Teoremas de Ceros Esparso Efectivos

En esta sección nos vamos a dedicar al Nullstellensatz esparso efectivo (Teoremas 2 y 3) y a la derivación de algunas de sus consecuencias.

Primeso vamos a introducir notación y a enunciar algunos hechos básicos de geometría poliedral y variedades tóricas. Usamos como referencias los libros [54] y [130] para la demostración de estos hechos y para una base mas general en estos temas.

Sea dados un conjunto finito de vectores enteros $\mathcal{A} \subseteq \mathbb{Z}^n$. La cápsula convexa de $\mathcal{A}$ como un subconjunto de $\mathbb{R}^n$ se denota como conv $(\mathcal{A})$. El cono sobre conv $(\mathcal{A})$ se denota por pos $(\mathcal{A})$.

El conjunto $\mathcal{A}$ es *graduado* si existe un vector entero $\omega \in \mathbb{Z}^n$ tal que $< a, \omega >= 1$ vale para todo $a \in \mathcal{A}$, esto es, cuando el conjunto $\mathcal{A}$ está en un hiperplano afín que no contiene al origen.

Sea $\mathbb{Z}\mathcal{A}$ el $\mathbb{Z}$-módulo generado por $\mathcal{A}$. Sea $\mathbb{R}\mathcal{A}$ el espacio lineal generado por $\mathcal{A}$, de forma tal que $\mathbb{Z}\mathcal{A}$ es un retículo en $\mathbb{R}\mathcal{A}$. Sea ρ la dimensión de este espacio lineal. Consideramos entonces la forma euclidiana de volumen en $\mathbb{R}A$, normalizada de tal forma que el retículo $\mathbb{Z}\mathcal{A}$ tiene covolumen $\rho!$ o equivalentemente, tal que cada simplex primitivo del retículo tiene volumen unitario. El *volumen* normalizado Vol $(\mathcal{A})$ del conjunto $\mathcal{A}$ se define como el volumen de su cápsula convexa con respecto a esta forma de volumen.

Obtenemos directamente de la definición la cota

$$\mathrm{Vol}\ (\mathcal{A}) \leq \rho!\,\mathrm{vol}(\mathrm{conv}\ (\mathcal{A})),$$

donde vol(conv $(\mathcal{A})$) denota el volumen de la cápsula convexa de $\mathcal{A}$ con respecto a la forma de volumen usual no normalizada de $\mathbb{R}^n$.

Sea $\mathbb{N}\mathcal{A}$ el semigrupo generado por $\mathcal{A}$. Este semigrupo está siempre contenido en el semigrupo pos $(\mathcal{A}) \cap \mathbb{Z}\mathcal{A}$. El conjunto $\mathcal{A}$ se dice *normal* o *saturado* si vale la igualdad $\mathbb{N}\mathcal{A} = \mathrm{pos}\ (\mathcal{A}) \cap \mathbb{Z}\mathcal{A}$.

Un polítopo $\mathbb{P}$ se dice *entero* si es la cápsula convexa de un conjunto finito de vectores enteros.

Sea § un simplex entero. Entonces § se dice *unimodular* si su interior no contiene ningún vector entero. Sea $\{s_1, \ldots, s_k\}$ el conjunto de vértices de §. Entonces tenemos que § es unimodular si y sólo si el conjunto de vectores enteros $\{s_2 - s_1, \ldots, s_k - s_1\}$ es normal.

Sea $\mathcal{P}$ un polítopo entero. Una subdivisión de $\mathcal{P}$ se dice *unimodular* si está formada por simplices enteros y unimodulares.

Dado un polítopo entero $\mathcal{P}$ in $\mathbb{R}^n$, denotamos por $\mathcal{A}(\mathcal{P})$ al conjunto $\{1\} \times (\mathcal{P} \cap \mathbb{Z}^n)$, que es un conjunto graduado de vectores enteros en $\mathbb{Z}^{n+1}$. Notamos que el conjunto $\mathcal{A}(\mathcal{P})$ es normal en el caso en que $\mathcal{P}$ admite una subdivisión unimodular.

Con respecto a la geometría tórica vamos a seguir las líneas de [130]. Este punto de vista difiere del usal en geometría algebraica. Es más combinatorio y se adecúa mejor a nuestros propósitos.

Sea dado de nuevo un conjunto finito de vectores enteros $\mathcal{A} = \{a_1, \ldots, a_N\}$ en $\mathbb{Z}^n$. Asociamos al conjunto $\mathcal{A}$ el morfismo

$$\varphi_{\mathcal{A}} : k[y_1, \ldots, y_N] \to k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}], \qquad y_i \to x^{a_i}.$$

El núcleo de esta aplicación es un ideal primo $I_{\mathcal{A}}$ of $k[y_1, \ldots, y_N]$, llamado el *ideal tórico* asociado al conjunto $\mathcal{A}$. Este ideal define una *variedad tórica afín* $X_{\mathcal{A}}$ como el lugar de sus ceros en $\mathbb{A}^N$. Esta variedad es irreducible y su dimensión es igual al rango del $\mathbb{Z}$-módulo $\mathbb{Z}\mathcal{A}$.

La k-álgebra $k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ es el anillo de coordenadas del toro $(\overline{k}^*)^n$. Luego la aplicación $\varphi_{\mathcal{A}}$ induce una aplicación dominante $(\overline{k}^*)^n \to X_{\mathcal{A}}$. La imagen de esta aplicación se llama el *toro* $T_{\mathcal{A}}$ de la variedad tórica afín $X_{\mathcal{A}}$. Este toro es igual al conjunto abierto $\{y_1 \cdots y_N \neq 0\}$ de $X_{\mathcal{A}}$.

El ideal $I_{\mathcal{A}}$ es homogéneo si y sólo si el conjunto $\mathcal{A}$ es graduado. En este caso el conjunto $\mathcal{A}$ define una *variedad tórica proyectiva* $Y_{\mathcal{A}}$ como el lugar de los ceros del ideal $I_{\mathcal{A}}$ en el espacio proyectivo $\mathbb{P}^{N-1}$. La dimensión de $Y_{\mathcal{A}}$ es igual al rango de $\mathbb{Z}\mathcal{A}$ menos uno, y su grado es igual al volumen normalizado del conjunto $\mathcal{A}$.

Sea $\mathcal{A} = \{a_1, \ldots, a_N\} \subseteq \mathbb{Z}^n$ un conjunto graduado. La intersección de la variedad proyectiva $Y_{\mathcal{A}}$ con la carta afín $\{y_i \neq 0\} \cong \mathbb{A}^{N-1}$ es igual a la variedad tórica asociada al conjunto

$$\mathcal{A} - a_i := \{a_1 - a_i, \ldots, a_{i-1} - a_i, a_{i+1} - a_i, \ldots, a_N - a_i\}.$$

DE hecho $Y_{\mathcal{A}}$ está cubierta irredundantemente por las variedades afines $X_{\mathcal{A}-a_i}$, donde a_i corre sobre los vértices del polítopo conv $(\mathcal{A})$.

La k-álgebra $k[y_1, \ldots, y_N]/I_{\mathcal{A}}$ es canónicamente isomorfa al álgebra de semigrupo $k[\mathbb{N}\mathcal{A}]$. Esta álgebra es normal si y sólo si el conjunto $\mathcal{A}$ es normal. Recordamos el teorema de Hochster de que la k-álgebra $k[\mathbb{N}\mathcal{A}]$ es un dominio Cohen–Macaulay en el caso en que el conjunto $\mathcal{A}$ es normal.

Sea dado un polítopo entero $\mathcal{P}$ en $\mathbb{R}^n$. Este polítopo determina un abanico $\Delta_{\mathcal{P}}$ y una variedad tórica *abstract* completa $X_{\mathcal{P}} = X(\Delta_{\mathcal{P}})$. Esta variedad viene equipada con un divisor de Cartier amplio $D_{\mathcal{P}}$. Este divisor de Cartier define entonces una aplicación $\varphi_{\mathcal{P}} : X_{\mathcal{P}} \to \mathbb{P}^{N-1}$, donde N denota la cardinalidad del conjunto $\{\mathcal{P} \cap \mathbb{Z}^n\}$. La imagen de esta aplicación es la variedad proyectiva $Y_{\mathcal{A}(\mathcal{P})}$, donde el conjunto $\mathcal{A}(\mathcal{P})$ se define como antes como $\{1\} \times (\mathcal{P} \cap \mathbb{Z}^n)$ [54, Section 3.4]. El divisor $(n-1)D_{\mathcal{P}}$ es muy amplio [45], y por lo tanto el conjunto graduado $\mathcal{A}((n-1)\mathcal{P})$ es normal.

Teorema 3.2.1 *Sean dados polinomios $p, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ tales que p está en el radical del ideal $(f_1, \ldots, f_s)$. Sea $\mathcal{P}$ un polítopo entero que contiene al polítopo de Newton de los polinomios $1, x_1, \ldots, x_n, f_1, \ldots, f_s$. Asumamos además que $\mathcal{A}(\mathcal{P})$ es un conjunto* *normal de vectores enteros en* $\mathbb{Z}^{n+1}$. *Entonces existe* $D \in \mathbb{N}$ *y* $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ *tal que vale*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

con $D \leq n! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$ *y* $\mathcal{N}(g_i f_i) \subseteq (1 + \deg p)\, n! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})\, \mathcal{P}$ *para* $i = 1, \ldots, s$.

Demostración. Sea $\mathcal{B} = \{b_0, \ldots, b_N\}$ el conjunto de vectores enteros $\mathcal{P} \cap \mathbb{Z}^n$, de forma tal que $\mathcal{A}(\mathcal{P}) = \{1\} \times \mathcal{B}$. Asumamos que $b_0 = (0, \ldots, 0)$. Consideramos el morfismo de k-álgebras

$$\psi : k[y_1, \ldots, y_N] \to k[x_1, \ldots, x_n], \qquad y_i \mapsto x^{b_i}.$$

El núcleo de este morfismo es el ideal de definición $I_{\mathcal{B}-b_0}$ de la variedad tórica afín $X_{\mathcal{B}-b_0}$. Esta variedad afín es la intersección de la variedad tórica proyectiva $Y_{\mathcal{A}(\mathcal{P})}$ con la carta afín $\{y_0 \neq 0\}$ of $\mathbb{P}^N$. Además la aplicación ψ induce un isomorfismo $\mathbb{A} \to X_{\mathcal{B}-b_0}$.

Sea ζ_i un polinomio de grado uno en $k[y_1, \ldots, y_N]$ tal que $\psi(\zeta_i) = f_i$ para $i = 1, \ldots, s$. Tomamos también un polinomio q en $k[y_1, \ldots, y_N]$ de grado menor o igual que el grado de de p tal que $\psi(q) = p$. Entonces $\zeta_1, \ldots, \zeta_s$ no tienen ceros comunes en $X_{\mathcal{B}-b_0}$ afuera de la hipersuperficie $\{q = 0\}$.

Sean $\eta_1, \ldots, \eta_s, u$ la homogeneización de $\zeta_1, \ldots, \zeta_s, q$ en $k[y_0, \ldots, y_N]$ respectivamente. Entonces las formas lineales $\eta_1, \ldots, \eta_s$ no tienen ceros comunes en $Y_{\mathcal{A}(\mathcal{P})}$ afuera de la hipersuperficie $\{y_0\, u = 0\}$.

Por hipótesis el conjunto $\mathcal{A}(\mathcal{P})$ es normal, y por lo tanto $I_{\mathcal{A}(\mathcal{P})}$ es un ideal primo homogéneo y Cohen–Macaulay de $k[y_0, \ldots, y_N]$ de dimensión menor o igual que $n + 1$. Tenemos también que $y_0\, u$ no es un divisor de cero modulo $I_{\mathcal{A}(\mathcal{P})}$. Luego estamos en las hipótesis del Lema Principal 3.1.7. Sea D el entero $\min\{n+1, s\}^2 \deg Y_{\mathcal{A}(\mathcal{P})}$. Obtenemos que existen elementos homogéneos $\alpha_1, \ldots, \alpha_s \in k[y_0, \ldots, y_N]/I_{\mathcal{A}(\mathcal{P})}$ de grado $(1 + \deg u)\, D - 1$ que satisfacen

$$(y_0\, u)^D = \alpha_1 \eta_1 + \cdots + \alpha_s \eta_s.$$

Finalmente evaluamos $y_0 := 1$ y aplicamos el morfismo ψ a la identidad anterior. Obtenemos

$$p^D = g_1 f_1 + \cdots + g_s f_s,$$

donde pusimos $g_i(x) := \alpha_i(1, x^{b_1}, \ldots, x^{b_N})$ para $i = 1, \ldots, s$. Tenemos las estimaciones $\deg u \leq \deg p$ y $\deg Y_{\mathbb{A}(\mathcal{P})} \leq n! \operatorname{vol}(\mathcal{P})$. Concluímos que $D \leq n! \min\{n+1, s\} \operatorname{vol}(\mathcal{P})$ y que el polítopo $\mathbb{N}(f_i g_i)$ está contenido en $((1 + \deg p)\, n! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P}))\, \mathcal{P}$ para $i = 1, \ldots, s$. $\square$

Derivamos del teorema anterior la siguiente cota de grado.

Corolario 3.2.2 *Sean las notaciones como en el Teorema 3.2.1. Sea* d *el máximo grado de los polinomios* f_i *para* $i = 1, \ldots, s$. *Entonces existen* $D \in \mathbb{N}$ *y* $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ *tales que*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

con $D \leq n! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$ *y* $\deg g_i f_i \leq d(1+\deg p)\, n! \min\{n+1, s,\}^2 \operatorname{vol}(\mathcal{P})$ *para* $i = 1, \ldots, s$.

$\square$

Vamos a mostrar con un ejemplo que esta cota de grado puede ser mucho más precisa que la usual en el caso en que el sistema dado sea esparso. Primero necesitamos el siguiente resultado auxiliar.

Lema 3.2.3 *Sea* $\mathcal{P}_d$ *el polítopo entero* $\{x = (x_1, \ldots, x_n) \in \mathbb{R}^n : x_1, \ldots, x_n \geq 0,\ x_1 + \cdots + x_{n-1} \leq 1,\ x_n \leq d\}$ *para algún* $d \in \mathbb{N}$. *Entonces* $\mathcal{P}_d$ *admite una subdivisión unimodular.*

Demostración. Sean $e_1, \ldots, e_{n-1}$ los vectores unitarios standard de $\mathbb{R}^{n-1}$. Sea § el simplex de $\mathbb{R}^{n-1}$ con vértices $(0, \ldots, 0), e_1, \ldots, e_{n-1}$, de forma tal que $\mathcal{P}_d = \mathcal{S} \times [0, d]$. Tenemos la subdivisión $\mathcal{P}_d = \cup_{i=0}^{d-1} (\mathcal{P}_1 + i\, e)$, donde $e \in \mathbb{R}^n$ denota el vector $(0, \ldots, 0, 1)$. Luego es suficiente mostrar que $\mathcal{P}_1$ admite una subdivisión unimodular.

Sea α_i , $\beta_i \in \mathbb{R}^n$ los vectores $e_i \times \{0\}$, $e_i \times \{1\}$ respectivamente, para $i = 1, \ldots, n-1$, y $(0, \ldots, 0, 0)$, $(0, \ldots, 0, 1)$ para $i = n$. Sea $§_i$ el simplex entero determinado por los vectores $\alpha_1, \ldots, \alpha_i, \beta_i, \ldots, \beta_n$ for $i = 1, \ldots, n$.

Se verifica fácilmente que los símplices $§_i$ y $§_j$ se intersecan en una cara propia para $i \neq j$, de forma tal que $§_1, \ldots, §_n$ son esencialmente disjuntos. Tenemos también que $\operatorname{vol}(§) = 1/(n-1)!$ y que $\operatorname{vol}(§_i) = 1/n!$ para $i = 1, \ldots, n$, y por lo tanto $§_1, \ldots, §_n$ forma una subdivisión unimodular de $\mathcal{P}_1$ como se quería. $\square$

Ejemplo 3.2.4 Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polinomios sin ceros comunes en $\mathbb{A}^n$. dhar '27 Asumamos además que $\deg_{x_1, \ldots, x_{n-1}} f_i \leq 1$ y que $\deg_{x_n} f_i \leq d$ vale para $i = 1, \ldots, s$. Sea $\mathcal{P}_d$ como antes el polítopo $\{x \in \mathbb{R}^n : x_1, \ldots, x_n \geq 0,\ x_1 + \cdots + x_{n-1} \leq 1,\ x_n \leq d\}$. Entonces $\mathcal{P}_d$ contiene al polítopo de Newton de los polinomios $1, x_1, \ldots, x_n, f_1, \ldots, f_s$ y el conjunto $\mathcal{A}(\mathcal{P})$ es normal por el lema anterior. Luego estamos en las hipótesis del Corolario 3.2.2 y podemos concluir que existen $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ tales que

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

con $\mathcal{N}(g_i f_i) \subseteq d\, n \min\{n+1, s\}^2 \mathcal{P}_d$ para $i = 1, \ldots, s$, ya que el volumen de $\mathcal{P}_d$ es igual a $d/(n-1)!$. En particular obtenemos la cota de grado $\deg g_i f_i \leq (n+1)^3 (d+1)^2$, que es mucho más precisa que la estimación $\deg g_i f_i \leq (d+1)^n$ que se sigue de la aplicación directa de la cota usual de grado.

Sean las notaciones de nuevo como en el Teorema 3.2.1. Sea $\mathbb{N}$ el polítopo de Newton de los polinomios $1, x_1, \ldots, x_n, f_1, \ldots, f_s$ y sea $\mathcal{U}$ el volumen no mezclado de este polítopo. Asumamos que $n \geq 2$. En esta situación podemos tomar el polítopo $\mathcal{P}$ como $(n-1)\,\mathbb{N}$. Obtenemos entonces las cotas

$$D \leq n^{n+2}\, \mathcal{U}, \qquad \mathcal{N}(g_i f_i) \subseteq ((1 + \deg p)\, n^{n+3}\, \mathcal{U})\, \mathbb{N}.$$

Es fácil verificar que estas cotas también valen cuando $n = 1$. Luego el Teorema 2 se sigue de esta observación en el caso particular $p = 1$. Observamos que en este caso la condición $0 \in \mathcal{P}$ es redundante.

Obtenemos un resultado similar en el caso de polynomios de Laurent.

Teorema 3.2.5 *Sean dados polinomios de Laurent $p, f_1, \ldots, f_s \in k[x_1^{-1}, \ldots, x_n^{-1}, x_1, \ldots, x_n]$ tales que p está en el radical del ideal $(f_1, \ldots, f_s)$. Sea $\mathcal{P}$ un polítopo entero que contiene al polítopo de Newton de $p, f_1, \ldots, f_s$. Sea ρ su dimensión. Asumamos además que $\mathcal{A}(\mathcal{P})$ es un conjunto normal de vectores enteros en $\mathbb{Z}^{n+1}$. Entonces existe $D \in \mathbb{N}$, $a \in \mathbb{Z}^n$ y $g_1, \ldots, g_s \in k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ tal que*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

con $D \leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$, $a \in (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2 \mathcal{P}$ *y* $\mathbb{N}(g_i f_i) \subseteq (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2\, \mathcal{P} - a$ *para* $i = 1, \ldots, s$.

Demostración. Como antes denotamos por $B = \{b_0, \ldots, b_N\}$ al conjunto de vectores enteros $\mathcal{P} \cap \mathbb{Z}^n$. Asumamos por el momento que $b_0 = (0, \ldots, 0)$. Consideramos el morfismo

$$\psi : k[y_1, \ldots, y_N] \to k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}], \qquad y_i \mapsto x^{b_i}.$$

El núcleo de este morfismo es el ideal de definición $I_{\mathcal{B}-b_0}$ de la variedad tórica afín $X_{\mathcal{B}-b_0}$. Sea T el toro de esta variedad tórica. Entonces tenemos que $X_{\mathcal{B}-b_0}$ es igual a la intersección de la variedad proyectiva $Y_{\mathcal{A}(\mathcal{P})}$ con la carta afín $\{y_0 \neq 0\}$ of $\mathbb{P}^N$, y que T es también el toro de $Y_{\mathcal{A}(\mathcal{P})}$. Recordamos que este tor es igual al abierto $\{y_0 \cdots y_N = 0\}$ de $Y_{\mathcal{A}(\mathcal{P})}$.

La aplicación ψ induce una suyección $(\overline{k}^*)^n \to T$. Sea $\zeta_1, \ldots, \zeta_s, q$ elementos de grado uno en $k[y_1, \ldots, y_N]$ tales que $\psi(\zeta_i) = f_i$ para $i = 1, \ldots, s$ y $\psi(q) = p$. Entonces $\zeta_1, \ldots, \zeta_s$ no tienen ceros comunes en T afuera del hiperplano $\{q = 0\}$.

Sea $\eta_1, \ldots, \eta_s, u$ la homogeneización de $\zeta_1, \ldots, \zeta_s, q$ en $k[y_0, \ldots, y_N]$ respectivamente. Entonces las formas lineales $\eta_1, \ldots, \eta_s$ no tienen ceros comunes en $Y_{\mathcal{A}(\mathcal{P})}$ afuera de la hipersuperficie $\{y_0 \cdots y_N\, u = 0\}$.

Sea $V(\eta_1, \ldots, \eta_s)$ la subvariedad de $Y_{\mathcal{A}(\mathcal{P})}$ definida por las formas lineales $\eta_1, \ldots, \eta_s$. Por la desigualdad de Bézout, el número de componentes irreducibles de $V(\eta_1, \ldots, \eta_s)$ no es mayor que el grado de $Y_{\mathcal{A}(\mathcal{P})}$. Denotemos por δ el grado de $Y_{\mathcal{A}(\mathcal{P})}$, de forma tal que vale $\delta \leq \rho! \operatorname{vol}(\mathcal{P})$. En nuestra situación esto implica que $V(\eta_1, \ldots, \eta_s)$ está en la unión de a lo sumo δ hiperplanos. EStos hiperplanos está definidos por variables $y_{i_1}, \ldots, y_{i_l}$, y eventualmente también por la forma lineal u, dependiendo de si $\eta_1, \ldots, \eta_s$ tienen un cero común en T en el hiperplano $\{u = 0\}$ o no. Sea Π el producto de stas equaciones, que es un polinomio de grado menor o igual a δ.

Por hipótesis el conjunto $\mathcal{A}(\mathcal{P})$ es normal y por lo tanto $I_{\mathcal{A}(\mathcal{P})}$ es un ideal primo homogéneo y Cohen–Macaulay de $k[y_0, \ldots, y_N]$. Tenemos también que Π no es un divisor de cero modulo este ideal. Luego estamos en las hipótesis del Lema Principal 3.1.7. Sea E el entero $\min\{n+1,s\}^2 \deg Y_{\mathcal{A}(\mathcal{P})}$. Entonces existem elementos homogéneos $\alpha_1,\ldots,\alpha_s \in k[y_0,\ldots,y_N]/I_{\mathcal{A}(\mathcal{P})}$ de grado $\deg \Pi\ E-1$ tales que

$$\Pi^E = \alpha_1\eta_1+\cdots+\alpha_s\eta_s$$

Evaluamos $y_0 := 1$ y aplicamos el morfismo ψ a la identidad anterior. Obtenemos

$$p^D = g_1 f_1+\cdots+g_s f_s,$$

donde pusimos $g_i(x) := (x^{b_{i_1}}\cdots x^{b_{i_l}})^{-1}\,\alpha_i(1,x^{b_1},\ldots,x^{b_N})$ para $i=1,\ldots,s$ y $D:=E$ en el caso en que u aparece como un factor de Π y $D:=1$ en otro caso. Luego vale $D \le \rho!\,\min\{n+1,s\}^2\,\mathrm{vol}(\mathcal{P})$ y el polítopo $\mathbb{N}(g_if_i)$ está contenido en $(\rho!\,\mathrm{vol}(\mathcal{P})\,E-1)\,\mathcal{P}-(b_{i_1}+\cdots+b_{i_l})$ para $i=1,\ldots,s$. Tenemos que $\deg\Pi \le \deg Y_{\mathcal{A}(\mathcal{P})} \le \rho!\,\mathrm{vol}(\mathcal{P})$ y que $i_1+\ldots+i_k \in \deg Y_{\mathcal{A}(\mathcal{P})}\,\mathcal{P}$.

Ahora consideramos el caso general. Sea b_0 un vector entero en $\mathcal{P}$, y sea $\mathbf{Q}$ el polítopo $\mathcal{P}-b_0$. Por las consideraciones anteriores existe $D\in\mathbb{N}$, $a_0\in\mathbb{Z}^n$ y $g_1,\ldots,g_s \in k[x_1,\ldots,x_n,x_1^{-1},\ldots,x_n^{-1}]$ tales que

$$p^D = g_1f_1+\cdots+g_sf_s$$

con $D \le \rho!\,\min\{n+1,s\}^2\,\mathrm{vol}(\mathbf{Q})$, $a_0 \in \rho!\,\mathrm{vol}(\mathbf{Q})\ \mathcal{Q}$ y $\mathbb{N}(g_if_i) \subseteq (\rho!\,\min\{n+1,s\}\,\mathrm{vol}(\mathbf{Q}))^2\ \mathbf{Q}-a_0$ para $i=1,\ldots,s$.

Sea a el vector entero $a_0+(\rho!\,\min\{n+1,s\}\,\mathrm{vol}(\mathcal{P}))^2\,b_0$. Entonces a está en el polítopo $(\rho!\,\min\{n+1,s\}\,\mathrm{vol}(\mathcal{P}))^2\ \mathcal{P}$ y tenemos también que vale $\mathbb{N}(g_if_i) \subseteq (\rho!\,\min\{n+1,s\}\,\mathrm{vol}(\mathcal{P}))^2\,\mathcal{P}-a$ para $i=1,\ldots,s$ como afirmamos. □

Sean las notaciones como en el Teorema 3.2.5. Sea $\mathbb{N}$ el polítopo de Newton de $p,f_1,\ldots,f_s$ y sea $\mathcal{U}$ el volumen no mezclado de este polítopo. Asumamos además que $n\ge 2$. En esta situación podemos tomar el polítopo $\mathcal{P}$ como $(n-1)\,\mathbb{N}$. Obtenemos las cotas

$$D \le n^{n+2}\,\mathcal{U}, \qquad\qquad \mathcal{N}(g_if_i) \subseteq (n^{2n+3}\,\mathcal{U})\ \mathcal{N}-a.$$

para algún $a \in (n^{2n+3}\,\mathcal{U})\,\mathbb{N}$. Como antes, es fácil verifical que las mismas cotas valen en el caso $n=1$. Luego el Teorema 3 se sigue de esta observación en el caso particular $h=1$.

Sea dada una función racional $q\in k(x_1,\ldots,x_n)$ y sea $q=f/g$ una representación de q como el cociente de dos polinomios sin factores comunes. Entonces el *grado* de q se define como $\deg q := \max\{\deg f, \deg g\}$.

Derivamos del Teorema 3.2.5 la siguiente cota de grado.

Corolario 3.2.6 *Sean las notaciones como en el Teorema 3.2.5. Sea d el máximo grado de loa polinomios de Laurent f_i para $i=1,\ldots,s$. Entonces existen $D\in\mathbb{N}$ y $g_1,\ldots,g_s \in k[x_1,\ldots,x_n,x_1^{-1},\ldots,x_n^{-1}]$ tales que*

$$p^D = g_1f_1+\cdots+g_sf_s$$

3.3 Cotas de Altura

3.3.1 División módulo Variedades Intersección Completa

La fórmula de la traza de Tate ha sido utilizada recientemente en distintos trabajos sobre distintos aspectos de la teoría de eliminación. Hay dos aplicaciones principales de la fórmula de la traza: cálculo de bases monomiales de grado bajo [3], [10], [34], [2] y división módulo variedades intersección completa [49], [85], [119], [64], por nombrar sólo algunas referencias. En estas páginas vamos a seguir este último punto de vista para resolver el siguiente problema.

Sea A un anillo de polinomios sobre un cuerpo k. Vamos a suponer que k es la clausura algebraica de un FP-cuerpo k_0. Sea $A[x] := A[x_1, \ldots, x_n]$ el anillo de polinomios n-variados con coeficientes en A y sea K su cuerpo de fracciones. Sea $f_1, \ldots, f_n \in A[x_1, \ldots, x_n]$ una intersección completa reducida de polinomios de grado a lo sumo d con respecto a las variables $x_1, \ldots, x_n$ que generan un ideal radical $(f_1, \ldots, f_n)$.

Consideramos la A-álgebra

$$B := A[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$$

Suponemos que $A \hookrightarrow B$ es un morfismo finito, que corresponde a una normalización de Noether de la variedad $V(f_1, \ldots, f_n)$. Luego B es un A-módulo libre de rango acotado por el grado de la variedad $V(f_1, \ldots, f_n)$.

Sean entonces $f, g \in A[x_1, \ldots, x_n]$ tales que $\overline{f}$ es un no–divisor de cero en B y $\overline{f} | \overline{g}$ en B. Esto es, existe algún polinomio $q_1 \in A[x_1, \ldots, x_n]$ tal que $\overline{g} = \overline{q} \cdot \overline{f}$.

En esta situación queremos resolver el problema de la *división*, es decir, encontrar $q \in A[x_1, \ldots, x_n]$ de bajo grado y altura tal que $\overline{g} = \overline{q}_1 \cdot \overline{f}$.

Resolvemos este problema mediante el uso de fórmulas de traza.

Resumimos el resultado principal de esta subsección en la siguiente proposición [85, Teorema 29].

Proposición 3.3.1 *Sea $A := k[t_1, \ldots, t_m]$ y sea $A[x_1, \ldots, x_n]$ el anillo de polinomios n-variados sobre k. Sea $f := (f_1, \ldots, f_n) \in A[x]$ una intersección completa reducida y sea $B := A[x]/f$. Sea $d := \max_i \deg f_i$ y $h_v := \max_i h_v(f_i)$.*

Sean $f, g \in A[x]$ tales que $\overline{f} \in B$ no es un divisor de cero y $\overline{f} | \overline{g} en B$. Entonces existe $q \in A[x]$ tal que $\overline{g} = \overline{q} \cdot \overline{f}, \deg_x q \leq n(d-1), \deg_t q \leq (2nd + \deg_{xg}) \deg V, \overline{h}(q) \leq 12n\delta^4(\deg g h(V) + h(g)) + \delta^5$.

Vamos a describir los aspectos básicos de la teoría de dualidad en álgebras de Gorenstein. La referencia básica es el libro de Kunz [89].

Consideramos a $B^* := \mathrm{Hom}_A(B, A)$ como un B-módulo con la multiplicación definida como $b \cdot \tau(x) := \tau(bx)$ para $b \in B$ y $\tau \in B^*$.

El dual B^* es un B-módulo libre de rango uno, debido a que B es una A-álgebra Gorenstein. Un generador σ de B^* como B-módulo, se llama una *traza* de B.

Hay dos elementos relevantes en B^*, que denotamos como Tr y σ. El primero, Tr , es la *traza canónica* de B, y se define de la siguiente manera. Dado $b \in B$, sea $\eta_b(x) : B \to B$ el morfismo A-lineal definido como $\eta_b(x) := bx$ para $x \in B$. Luego Tr (b) se define como la traza del endomorfismo η_b de B. Esta definición tiene sentido, ya que B es un A-módulo libre.

la traza standard no es en general una traza de B, es decir, Tr no es un generador de B^*. Ahora vamos a introducir σ_1 que es una traza, en el sentido anterior.

Sean $y_1, \ldots, y_n$ nuevas variables y sea $y := (y_1, \ldots, y_n)$. Sea entonces $f_i^y := f_i(y_1, \ldots, y_n)$. Luego los polinomios $f_i^y - f_i$ pertenecen al ideal $(y_1 - x_1, \ldots, y_n - x_n)$. Sean entonces $l_{ij} \in A[x, y]$ tales que

$$f_i^y - f_i = \sum_{j=1}^{n} l_{ij}(y_j - x_j)$$

Estos polinomios no son únicos.

Consideramos entonces el determinante Δ de la matriz $(l_{ij})_{ij}$, que se puede escribir como

$$\Delta = \sum_m a_m(x) \cdot b_m(y)$$

Nuevamente, a_m, b_m no son únicos. El polinomio Δ se llama un *determinante pseudo-jacobiano* de la intersección completa $f_1, \ldots, f_n$.

Sea $\overline{J}$ la clase en B del detrminante Jacobiano $J(f_1, \ldots, f_n)$.

Sea $c_m := b_m(x)$. Luego tenemos la identidad

$$\overline{J} = \sum_m \overline{a}_m \cdot \overline{b}_m$$

Esto justifica el nombre de "pseudo-jacobiano" para el polinomio Δ.

La imagen del polinomio Δ en el anillo $A[x, y]/)f_1, \ldots, f_n, f_1^y, \ldots, f_n^y)$ es independiente de la elección de l_{ij}, a_m y b_m.

Luego existe una única traza $\sigma \in B^*$ tal que

$$\overline{1} = \sum_m \sigma(\overline{a}_m) \cdot \overline{c}_m$$

La propiedad principal de la traza σ es la identidad

$$\overline{g} = \sum_m \sigma(\overline{g} \cdot \overline{a}_m) \cdot \overline{c}_m$$

para todo $g \in A[x]$. Esta identidad se conoce como la *fórmula de la traza de Tate* [89, Apéndice F].

Ambos elementos, Tr y σ, están relacionados por la identidad

$$\overline{J} \cdot \sigma = \mathrm{Tr}$$

Notamos que los polinomios l_{ij} se pueden elegir de grado a lo sumo $d-1$, y por lo tanto los polinomios a_m, c_m se pueden elegir de grado a lo sumo $n(d-1)$.

Luego la fórmula de traza se puede aplicar al cálculo de sistemas de generadores de bajo grado de B como A-módulo. Obviamente el conjunto de polinomios $\{c_m\}_m$ de grado a lo sumo $n(d-1)$ genera B como A-módulo.

La fórmula de la traza de Tate resuelve el problema de la división.

Demostración de la Proposición 3.3.1. Sean K el cuerpo de fracciones de A y $L := K \otimes_A B$. El hecho de que B es un A-módulo libre implica que todo morfismo $\tau \in B^*$ se extiende en forma única a un morfismo $\tau \in \mathrm{Hom}_K(L, K)$.

Luego $\overline{f}$ es una unidad en L ya que es un no-divisor de cero en B. Sea $q_1 \in K[x_1, \ldots, x_n]$ tal que $\overline{q}_1 \cdot \overline{f} = \overline{g}$ en B. Luego $\overline{q}_1 = \overline{f}^{-1} \cdot \overline{g}$ en L. Concluímos que para todo $h \in A[x_1, \ldots, x_n]$

$$\sigma(\overline{f}^{-1} \cdot \overline{g} \cdot \overline{h} = \sigma(\overline{q}_1 \cdot \overline{h}) \in A$$

Sea entonces

$$q := \sum_m \sigma(\overline{f}^{-1} \cdot \overline{g} \cdot \overline{a}_m) c_m \in A[x_1, \ldots, x_n]$$

Luego $\overline{q} \cdot \overline{f} = \overline{g}$ en B, y se tiene obviamente $\deg_x q \leq n(d-1)$.

Sea $l_{ij} := (f_i(y_1, \ldots, y_j, x_{j+1}, \ldots, x_n) - f_i(y_1, \ldots, y_{j-1}, x_j, \ldots, x_n))(y_j - x_j)$. Luego $h_v(l_{ij}) \leq h_v(f_i) + \log d$. Luego $h_v(\Delta) \leq m_v(\Delta) + n(d-1)\log(2n+1) \leq n\, m_v((l_{ij})_{ij}) + 2n\, d \log(n+1)$, y por lo tanto $h_v(a_m), h_v(c_m) \leq n\, h_h(f_i) + 2n\, d \log(n+1)$.

Sean $\delta := \deg V(f_1, \ldots, f_n)$ y $h := h(V(f_1, \ldots, f_n))$. En esta situación se tiene $\deg m_f \leq \deg_x f \deg V$. Sea $m_f = t^\mu + \alpha_{\mu-1} t^{\mu-1} + \cdots + \alpha_0 \in A[t]$ el polinomio minimal de f sobre K, y sea $f^* := t^{\mu-1} + \alpha_{\mu-1} t^{\mu-2} + \cdots + \alpha_1$. Luego $\overline{f}\,\overline{f}^* = -\alpha_0 \in A - \{0\}$ y tenemos $\deg \alpha_0, \deg f^* \leq f\, \delta, \overline{w}(\alpha_0) \overline{h}(f^*) \leq 12n\, \delta^2(\deg f\, h(V) + \overline{w}(f)) + \delta^3$.

Hacemos lo mismo para J y obtenemos polinomios $J^* \in A[x_1, \ldots, x_n]$ y $\beta_0 \in A - \{0\}$ tal que $\overline{J}\,\overline{J}^* = -\beta_0$ en B, con $\deg \beta_0, \deg J^* \leq n(d-1)\delta$ y $\overline{w}(\beta_0), \overline{w}(J^*) \leq 12n\, \delta^2(\deg J\, h(V) + \overline{w}(J)) + \delta^3 \leq 12n^2\, \delta^2(d\, h(V) + h) + \delta^3$.

Luego $\deg \mathrm{Tr}\ (\overline{J}^* \cdot \overline{f}^* \cdot \overline{g} \cdot a_m) \leq \delta \deg_t(\overline{J}^* \cdot \overline{f}^* \cdot \overline{g} \cdot \overline{a}_m) \leq \delta(n(d-1) + \deg f + \deg_t\, g + n(d-1)) \leq \delta(2n\, d + \deg_t\, g)$ y se tiene además

$$\begin{aligned}
\overline{w}(\mathrm{Tr}\ (\overline{J}^* \cdot \overline{f}^* \cdot \overline{g} \cdot \overline{a}_m)) &\leq 12n\, \delta^2(\deg_t(J^* \cdot f^* \cdot g \cdot a_m) h(V) + w(J^* \cdot f^* \cdot g \cdot a_m)) + \delta^3 \\
&\leq 12n\, \delta^4(\deg g\, h(V) + h(g)) + \delta^5
\end{aligned}$$

Concluímos entonces $\deg_t q \leq (2n\,d + \deg_t g)$, $m(g) \leq 12n\,\delta^4(\deg g\, h(V) + h(g)) + \delta^5$ por la multiplicatividad de la medida de Mahler.

$\square$

La fórmula de la traza resuelve también el problema de la *interpolación*: dado $g \in A[x]$, encontrar $g_1 \in A[x]$ de bajo grado con respecto a las variables $x_1, \ldots, x_n$ y baja altura tal que $\overline{g} = \overline{g}_1$ en B.

Este es un caso particular del problema de la división, con $f = 1$. La fórmula de la trza muestra que el polinomio

$$g_1 := \sum_m \sigma(\overline{g} \cdot \overline{a}_m) \cdot c_m \in A[x_1, \ldots, x_n]$$

verifica $\overline{g} = \overline{g}_1$ en B, y por la Proposición 3.3.1 se tiene $\deg_x g_1 \leq n(d-1)$, $\deg_t g_1 \leq (2n\,d + \deg g)\deg V$, $h(g_1) \leq 12n\,\delta^4(\deg g\, h(V) + h(g)) + \delta^5$.

3.3.2 Un Teorema de Ceros Aritmético para Variedades Intersección Completa

Sea k la clausura algebraica de un FP-cuerpo k_0. Sea $F_1, \ldots, F_{n-r} \in k[x_1, \ldots, x_n]$ una intersección completa reducida de polinomios que definen un ideal radical $(F_1, \ldots, F_{n-r})$.

Sea $V := V(F_1, \ldots, F_{n-r}) \subseteq \mathbb{A}^n$ la variedad de dimensión r definida por estos polinomios. Sean $D := \max_i \deg F_i$, $H := \max_i \overline{h}(F_i)$, $\delta := \deg V$. Luego se tiene las estimaciones

$$\delta \leq D^{n-r} \qquad\qquad h(V) \leq 6n^7 D^{2(n-r)+1} H$$

debidas a la desigualdad de Bézout. De todas formas estos parámetros pueden ser mucho menores que estas estimaciones.

Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polinomios que definen la variedad vacía en V. El teorema de ceros dice entonces que existen $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ tales que se verifica la identidad de Bézout

$$\overline{1} = \overline{g}_1 \overline{f}_1 + \cdots + \overline{g}_s \overline{f}_s \qquad\qquad \in k[V]$$

En este apartado vamos a tratar el *teorema de ceros aritmético sobre* V, que consiste en encontrar polinomios $g_1, \ldots, g_s$ que satisfagan la desigualdad anterior, y que tengan bajo grado y altura.

Resolvemos este problema usando el teorema de división 3.3.1, siguiendo [85]. El resultado principal de esta subsección es el siguiente.

Teorema 3.3.2 *(Teorema de Ceros Aritmético) Sean $F_1, \ldots, F_{n-r} \in k[x_1, \ldots, x_n]$ intersección completa reducida de polinomios que definen una variedad $V = V(F_1, \ldots, F_{n-r}) \subseteq \mathbb{A}^n$.*

Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ *polinomios sin ceros comunes en* V *. Sea* $D := \max_i \deg F_i$ *,* $d := \max_i \deg f_i$ *,* $H := \max_i \overline{h}(F_i)$ *y* $h := \max_i \overline{h}(f_i)$ *. Entonces existen* $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ *tales que*

$$\overline{1} = \overline{g}_1 \overline{f}_1 + \cdots + \overline{g}_s \overline{f}_s \in k[V]$$

tales que $\deg g_i \leq 2n^2 d^{n+2}\delta$ *,* $\overline{h}(g_i) \leq 6n^6 \delta^7 d^{3i+3} h(V) h$ *.*

Notamos además que $g_1, \ldots, g_s$ están definidos sobre el mismo cuerpo que $F_1, \ldots, F_{n-r}$, $f_1, \ldots, f_s$.

En el caso $k_0 := \mathbb{Q}$ y $V := \mathbb{A}^n$ reobtenemos los resultados de [13] y [85]. Tenemos que existen $a \in \mathbb{Z} - \{0\}$ y $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ tales que

$$a = g_1 f_1 + \cdots + g_s f_s$$

con $\deg g_i \leq 2n^2 d^{n+2}\delta$, $h(a)$, $\overline{h}(g_i) \leq 6n^6 \delta^7 d^{3i+3} h(V) h$.

En el caso $k_0 := F(t_1, \ldots, t_m)$, es decir, k_0 es el cuerpo de funciones racionales en m variables sobre un cuerpo F , y $V := \mathbb{A}^n$, reobtenemos los resultados de Smietanski [124]. Tenemos que existen $a \in F[t_1, \ldots, t_m] - \{0\}$ y $g_1, \ldots, g_s \in F[t_1, \ldots, t_m][x_1, \ldots, x_n]$ tales que

$$a = g_1 f_1 + \cdots + g_s f_s$$

con $\deg_t a \leq 2n^2 d^{n+2}\delta$, $\deg_x a$, $\deg_x g_i \leq 6n^6 \delta^7 d^{3i+3} h(V) h$.

Para poder aplicar el teorema de división necesitamos preparar los polinomios $f_1, \ldots, f_s$ y poner a las variables $x_1, \ldots, x_n$ en posición general, sin afectar esencialmente el grado y la altura.

Necesitamos reemplazar a $f_1, \ldots, f_s$ por una sucesión regular reducida en $k[V]$ y a $x_1, \ldots, x_n$ por variables $y_1, \ldots, y_n$ tales que $y_1, \ldots, y_{r-i}$ es una normalización de Noether de $V_i := V \cap \{f_1 = 0, \ldots, f_i = 0\}$.

Primero mostramos que $f_1, \ldots, f_s$ pueden reemplazarse por una sucesión regular reducida.

Lema 3.3.3 *Con la misma notación, existen* $h_1, \ldots, h_t \in \underline{\ }(f_1, \ldots, f_s)$ *sucesión regular débil reducida en* $k[V]$ *tal que* $t \leq \min\{r, s\} \deg h_i \leq d+1$ *y* $\overline{h}(h_i) \leq h + j \log(d+1) + \log \delta$ *.*

Demostración. Construímos inductivamente los polinomios h_i como combinaciones lineales de los f_i . Suponemos que $h_1, \ldots, h_j$ ya están construídos. Sea

$$h_{j+1} := \sum u_{kl}\, x_k\, f_l + \sum u_i\, f_i$$

con u_i , u_{kl} variables. Sea $V_j := V \cap \{h_1 = 0, \ldots, h_j = 0\}$ y sean $y_1, \ldots, y_{r-j}$ variables arbitrarias que representan una normalización de Noether de V_j . Sea

$$\phi := \det \eta_{h+1} \in k[u_{kl}]$$

Luego ϕ es un polinomio no nulo por la condición de que $f_1, \ldots, f_s$ definen la variedad vacía en V_j. Se tiene $\deg \phi \le \deg V_j \le (d+1)^j \deg V$.

Por otra parte, sea $J \in k[u_{kl}][x_1, \ldots, x_n]$ el determinante de la matriz Jacobiana de $F_1, \ldots, F_{n-r}, h_1, \ldots, h_{j+1}$ con respecto a las variables ligadas $y_{r-j+1}, \ldots, y_n$. Luego J es un no–divisor de cero, como consecuencia del teorema de Bertini y del Criterio Jacobiano [61].

Se tiene $\deg J \le n - r + j$ en u. Luego $\psi := \det J \in k[u_{kl}]$ es un polinomio no nulo de grado a lo sumo $(n-r+j)\delta_j = (n-r+j)(d+1)^j\delta$. Luego $\phi\psi$ es un polinomio no nulo de grado acotado por $D^j\delta$ y por lo tanto existen $a = a_{kl} \in k$ tales que $\phi(a)\,\psi(a) \neq 0$ y $\overline{h}(a) \le j\log(d+1) + \log\delta$. En el caso en que $\mathrm{char}(k) = 0$ tomamos $a_{kl} \in \mathbb{Z}$, en otro caso tomamos a_{kl} de altura ≤ 1.

El polinomio $h_{j+1} := h_{j+1}(a)$ satisface las condiciones del enunciado.

□

El paso siguiente es poner a las variables $y_1, \ldots, y_n$ en posición de Noether simultáneamente para todas las variedades que se consideran. Con esto queremos decir, $y_1, \ldots, y_{r-j}$ en posición de Noether con respecto a $V_j := V \cap \{h_1, \ldots, h_j = 0\}$ para todo j.

Lema 3.3.4 *Con la misma notación, existen un cambio de variables $y_1, \ldots, y_n \in k[x_1, \ldots, x_n]$ tales que $y_1, \ldots, y_{r-j}$ está en posición de Noether con respecto a V_j para todo j. Se tiene además $\overline{h}(y_i) \le r^2\log(d+1)\mathrm{Tr}\ \log\delta$.*

Demostración. Sean $y_i = U_{i0} + U_{i1}x_1 + \cdots + u_{in}x_n$ formas lineales genéricas.

Sea $A_{V_j} \in k[U_1, \ldots, U_{r-j}]$ el coeficiente principal del polinomio eliminante de V_j. Sea $a = (a_1, \ldots, a_n)$ tal que

$$A_{V_1}(a) \cdots A_{V_t}(a) \neq 0$$

Se puede tomar a_i de altura acotada por $r^2\log(d+1)\mathrm{Tr}\ \log\delta$. Luego $y_i := y_i(a_i)$ verifica las condiciones del enunciado. □

Ahora probamos el Teorema 3.3.2

Demostración del Teorema 3.3.2. Por los Lemas 3.3.3 y 3.3.4 podemos suponer sin pérdida de generalidad que $s \le r$, $\overline{f}_1, \ldots, \overline{f}_s$ es una sucesión regular en $k[V]$ y que V_i está en posición de Noether con respecto a las variables $x_1, \ldots, x_{r-i}$ para todo i.

Sea entonces $A_i := k[x_1, \ldots, x_{r-i}]$ y $B_i := k[V]/(f_1, \ldots, f_i)$.

Luego $B_i := A_i[x_{r-i+1}, \ldots, x_n]/(F_1, \ldots, F_{n-r}, f_1, \ldots, f_i)$, $(F_1, \ldots, f_i)$ es una intersección completa reducida, y $A_i \hookrightarrow B_i$ es una extensión entera. Luego podemos aplicar el Teorema de División 3.3.1.

Vamos a construir inductivamente $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ tales que

$$\overline{1} = \overline{g}_1 \overline{f}_1 + \cdots + \overline{g}_s \overline{f}_s \in k[V]$$

Dado $\overline{b}_{i+1} \in (\overline{f}_{i+1}) \subseteq B_i$ existe $\overline{g}_{i+1} \in B_i$ tal que

$$\overline{b}_{i+1} = \overline{g}_{i+1} \overline{f}_{i+1} \in B_i$$

Luego hacemos $b_s := 1$ y $b_i := b_{i+1} - g_{i+1} f_{i+1}$. Se tiene entonces $\overline{b}_i \in (\overline{f}_i) \subseteq B_{i-1}$, y vale

$$1 = g_1 f_1 + \cdots + g_s f_s \qquad \text{en } k[V]$$

Luego controlamos el grado y la altura de $g_{i+1} \in A_i[x_{r-i+1}, \ldots, x_n]$ por medio del teorema de división.

Dado un polinomio $g \in A_i[x_{r-i+1}, \ldots, x_n]$ vamos a denotar por $\deg^0 g$ su grado en las variables *libres* $x_1, \ldots, x_{r-i}$ y por $\deg^* g$ su grado con respecto a las variables dependientes $x_{r-i+1}, \ldots, x_n$.

Supongamos entonces $\deg^\circ g_{j+1} \leq 2n^2 d^{j+2} \delta$ y $\deg^* g_{j+1} \leq n\, d$ para $j \geq i+1$. Luego $\deg^* g_{i+1} n\, d$ y $\deg^\circ g_{i+1} \leq 2n\, d \deg^* b_{i+1} \deg V_i$. Se tiene $V_i = V \cap \{f_1 = 0, \ldots, f_i = 0\}$ y por lo tanto $\deg V_i \leq d^i \delta$. Se tiene $b_{i+1} = 1 - g_s f_s \cdots g_{i+2} f_{i+2}$ y por lo tanto $\deg^* b_{i+1} \leq n(d+1)$. Luego $\deg^\circ g_{i+1} \leq 2n^2 d^{i+2} \delta$.

Supongamos además $\overline{h}(g_{j+1}) \leq \overline{h}(g_{i+1}) \leq 6n^6 \delta^7 d^{3j+3} m(V) h$ para $j \geq i+1$. Tenemos $h(g_{i+1}) \leq 12n\delta_i^4 (\deg b_{i+1} h(V_i) + h(b_{i+1}))$. Luego $\deg(b_{i+1}) \leq 2n^2 d^{i+1} \delta$, $h(b_i) \leq 6n^6 d^{2i} \delta^3 (m(V) + h)$. Además $h(V_i) \leq 6n^6 d^{2i} \delta^3 (m(V) + h)$ y por lo tanto

$$h(g_{i+1}) \leq 6n^6 \delta^7 d^{3i+3} (m(V) + h)$$

$\square$

3.3.3 Distancia entre Variedades

La altura de una variedad nos permite estimar la localización de sus puntos. Por ejemplo, si $V \subseteq \mathbb{A}^n(\mathbb{C})$ es una variedad cero–dimensional definida sobre $\overline{\mathbb{Q}}$, entonces $m(V)$ acota a la altura de Weil de V, y por lo tanto

$$V \subseteq \{p \in \mathbb{A}^n(\mathbb{C}) : ||p||_\infty \leq \exp(m(V))\}$$

donde $||p||_i nfty := \max_i |p_i|$ denota la norma del supremo.

En esta sección vamos a obtener cotas inferiores para la distancia entre dos variedades aritméticas.

Estas estimaciones dependen del grado y de la altura de la variedad y de los polinomios que la definen.

Sean $V, W \subseteq \mathbb{A}^n(\mathbb{C})$ variedades aritméticas, y sea $\rho \geq 0$.

Luego definimos $\mathrm{Dist}_\rho(V, W)$ la distancia entre V y W en la bola $B(0, \rho)$. Definimos también $\mathrm{Dist}_\rho(V, W)$ como la distancia entre V y W en $\mathbb{C}^n$.

Sean $V, W \subseteq \mathbb{A}^n$ variedades aritméticas tales que $V \cap W = \emptyset$. Este problema está en estrecha relación con el Nullstellensatz aritmético.

Se tiene $1 \in I(V) + I(W)$. Supongamos entonces que existe $F \in I(W)$ tal que

$$1 \equiv F(\bar{x}) \qquad \mod I(V)$$

con $\deg F = \delta$ y $h(F) = \eta$.

Sea $\rho \geq 0$ y sean $p \in V$ y $q \in W$ tales que $p, q \in B(0, \rho)$.

Sea $\epsilon := ||q - p||$ y supongamos que $\epsilon < 1$.

Desarrollamos F alrededor de q. Se tiene entonces

$$F(\bar{x}) = \sum_i A_i (x - q)^i$$

con $A_i = \partial_i F(q)$. Se tiene entonces $\log |A_i| \infty \leq \eta + \delta(\log \rho + \log n)$. Evaluamos $x := p$ y queda

$$\begin{aligned} 0 &\leq \log |F(p)| \leq \log(\max_i |A_i| \infty) + \delta \log n + \log \epsilon \\ &\leq \eta + \delta(\log \rho + 2 \log n) + \log \epsilon \end{aligned}$$

es decir

$$-\log \epsilon \leq \eta + \delta \log n^2 \rho$$

Luego podemos usar los resultados de la sección anterior en el caso en que V y W sean intersección completa reducida.

Sean r, s la dimensión de V y de W respectivamente. Sean $f_1, \ldots, f_{n-r}$ y $h_1, \ldots, h_{n-s}$ polinomios en $\mathbb{Q}[x_1, \ldots, x_n]$ tales que

$$I(V) = f_1, \ldots, f_{n-r} \qquad I(W) = h_1, \ldots, h_{n-s}$$

Sean d_0, d el máximo de los grado de f_i y h_j para $i = 1, \ldots, n-r$ y $j = 1, \ldots, n-s$ respectivamente. Análogamente sean h_0, h el máximo de las alturas de f_i y h_j.

En esta situación aplicamos el Nullstellensatz aritmético y obtenemos que existe $F \in I(W)$ tal que

$$1 \equiv F(\bar{x}) \qquad \mod I(V)$$

con $\deg F \leq 2n^2 d_0 d^r \deg(V)$ y $h(F) \leq 2n^2 d_0 d^r \deg(V)(h_0 + h + h(V))$.

Teorema 3.3.5 *Sean $V, W \subseteq \mathbb{A}^n$ variedades aritméticas tales que $V \cap W = \emptyset$. Sean r, s la dimensión de V y de W respectivamente. Supongamos además que V y W son intersección completa reducida de polinomios $f_1, \ldots, f_{n-r}$ y $h_1, \ldots, h_{n-s}$.*

Sean d_0, d y h_0, h el máximo de los grados y de las alturas de f_i y h_j para $i = 1, \ldots, n-r$ y $j = 1, \ldots, n-s$ respectivamente. Entonces

$$-\log(\mathrm{Dist}_\rho(V,W)) \leq 2n^2 d_0 d^r \deg(V)(h_0 + h + h(V) + \log 2n^2\rho)$$

para $\rho > 0$.

Sean $V, W \subseteq \mathbb{A}^n$ variedades aritméticas equidimensionales tales que $V \cap W = \emptyset$. Conjeturamos en este caso que existen $F \in I(V), G \in I(W)$ tales que

$$1 = F(\bar{x}) + G(\bar{x})$$

con $\deg F, \deg G \leq \deg(V)\deg(W)$ y $h(F), h(G) \leq \deg(V)h(W) + \deg(W)h(V)$.

De aquíse deducirá

$$-\log(\mathrm{Dist}_\rho(V,W) \leq \deg(V)h(W) + \deg(W)h(V) + \deg(V)\deg(W)\log n^2\rho$$

De todas formas podemos obtener del resultado anterior una cota para el caso general.

Corolario 3.3.6 *Sean $V, W \subseteq \mathbb{A}^n$ variedades aritméticas equidimensionales tales que $V \cap W = \emptyset$. Entonces*

$$-\log(\mathrm{Dist}_\rho(V,W) \leq 2n^2 \deg(V)^{n-r}\deg(W)^{n-s}(h(V) + h(W))$$

para $\rho > 0$.

Demostración. Sean δ, ζ y η, θ el grado y la altura de V y W respectivamente.

Sea $W = \cup_i W_i$ la descomposición de W en componentes irreducibles, y sea $q_i \in W_i$.

Sea $P_V(\eta_1, \ldots, \eta_{r+1})$ el polinomio de Chow de V, y sean $\bar{u}_1, \ldots, \bar{u}_r \in \mathbb{Z}^{n+1}$ tales que $P_V(\bar{\eta}_1, \ldots, \bar{\eta}_r, \eta_{r+1}) \neq 0$. Se puede suponer $h(u_j) \leq \log\delta$.

Luego existe $\bar{u}_{r+1} \in \mathbb{Z}^{n+1}$ que separa V de los q_i y tal que $h(\bar{u}_{r+1} \leq \log\zeta$. De esta forma obtenemos polinomios $F_1, \ldots, F_{n-r} \in \mathbb{Q}[x_1, \ldots, x_n]$ que forman una intersección completa reducida tales que

$$V \subseteq \mathcal{V} := V(F_1, \ldots, F_{n-r})$$

con $\deg F_i \leq \delta$ y $h(F_i) \leq \eta + \delta\log\zeta$ para $i = 1, \ldots, n-r$. Análogamente existen $G_1, \ldots, G_{n-s} \in \mathbb{Q}[x_1, \ldots, x_n]$ intersección completa reducida tales que

$$W \subseteq \mathcal{W} := V(G_1, \ldots, G_{n-s})$$

con $\deg G_i \leq \zeta$ y $h(G_i) \leq \theta + n\zeta\log\delta$ para $i = 1, \ldots, n-s$.

Se tiene entonces

$$\mathcal{V} \cap \mathcal{W} = \emptyset$$

con $\deg\mathcal{V} \leq \delta^{n-r}, \deg\mathcal{W} \leq \zeta^{n-s}, h(\mathcal{V} \leq \delta^{2(n-r)}(\eta+\delta\log\zeta)$ y $h(\mathcal{W}) \leq \zeta^{2(n-s)}(\theta+n\zeta\log\delta)$.

Luego

$$-\log(\mathrm{Dist}_\rho(V,W) \leq -\log(\mathrm{Dist}_\rho(V,W) \leq 2n^2\delta^{n-r}\zeta^{n-s}(\eta + \theta + \zeta\log\delta + \delta\log\zeta)$$

□

Capítulo 4

Cotas para la Función de Hilbert

4.1 Notaciones y Convenciones

El anillo $k[x_0, \ldots, x_n]$ se va denatar alternativamente como R o R_k.

Sea $I \subseteq k[x_0, \ldots, x_n]$ sea un ideal homogéneo. Entendemos por la dimensión de I la the dimensión de la variedad proyectiva que define y vamos a denotarla por $\dim I$, de forma tal que $\dim I = \dim_{\mathrm{krull}} I - 1$.

Sea $J \subseteq k[x_1, \ldots, x_n]$ un ideal afín. Entendemos por la dimensión de J su dimensión de Krull. En cada aparición va a ser claro del contexto a qué noción nos estamos refiriendo.

Un ideal $I \subseteq k[x_0, \ldots, x_n]$ es *equidimensional* si sus ideales primos asociados tienen todos la misma dimensión. En particular, I no tiene componentes inmersas.

Dado un ideal $I \subseteq k[x_0, \ldots, x_n]$, entonces $I^e := \bar{k} \otimes_k I \subseteq \bar{k}[x_0, \ldots, x_n]$ es el ideal extendido I en $\bar{k}[x_0, \ldots, x_n]$.

Dado $I \subseteq R_k$ un ideal homogéneo,

$$V(I) := \{x \in \mathbb{P}^n : f(x) = 0 \ \ \forall f \in I\} \subseteq \mathbb{P}^n$$

es la variedad proyectiva definida por I. recíprocamente, dada una variedad $V \subseteq \mathbb{P}^n$

$$I_k(V) := \{f \in R_k : f|_V \equiv 0\} \subseteq R_k$$

y $I(V) := I_{\bar{k}}(V) \subseteq \bar{k}[x_0, \ldots, x_n]$ es el ideal de definición V.

dado un R-módulo graduado M y $m \in \mathbb{Z}$, M_m es la parte homogénea de grado m.

Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo. La *función de Hilbert* o *función característica* del ideal I

$$\begin{aligned} h_I :\ & \mathbb{Z} \to \mathbb{Z} \\ & m \mapsto \dim_k(k[x_0, \ldots, x_n]/I)_m \end{aligned}$$

Dada una variedad $V \subseteq \mathbb{P}^n$ entonces h_V is la función de Hilbert de $I(V)$.

Dado $f \in k[x_0,\ldots,x_n]$ un polinomio, $f^a \in k[x_1,\ldots,x_n]$ su afinización y dado $I \subseteq k[x_0,\ldots,x_n]$ un ideal homogéneo, $I^a \subseteq k[x_1,\ldots,x_n]$ es su afinización.

Recíprocamente, dado un polinomio afín $g \in k[x_1,\ldots,x_n]$, $g^h \in k[x_0,\ldots,x_n]$ es su homogeneización, y dado $J \subseteq k[x_1,\ldots,x_n]$ un ideal afín, denotamos como $J^h \subseteq k[x_0,\ldots,x_n]$ su homogeneización.

4.2 Preliminares sobre Función de Hilbert

En esta sección enunciamos algunas propiedades bien conocidas de la función de Hilbert de un ideal polinomial homogéneo. Al mismo tiempo vamos a probar algunas en el caso en que no haya ninguna referencia disponible.

Ahora prestamos atención a la función de Hilbert de un ideal homogéneo. Sea $I \subseteq k[x_0,\ldots,x_n]$ un ideal homogéneo de dimensión d. Existe un polinomio $p_I \in \mathbb{Q}[t]$ de grado d, y $m_0 \in \mathbb{Z}$ tales que

$$h_I(m) = p_I(m)$$

para $m \geq m_0$. El polinomio p_I se llama *polinomio de Hilbert* del ideal I.

El grado del ideal homogéneo $I \subseteq k[x_0,\ldots,x_n]$ puede definirse a través de su polinomio de Hilbert.

Sea $I \subseteq k[x_0,\ldots,x_n]$ un ideal homogéneo de dimensión d, con $d \geq 0$. Sea $p_I = a_d\, t^d + \ldots + a_0 \in \mathbb{Q}[t]$ su polinomio de Hilbert. Entonces el *grado (algebraico)* del ideal I se define como

$$\deg I := d!\ a_d \ \in \mathbb{N}$$

Si $I \subseteq k[x_0,\ldots,x_n]$ es un ideal homogéneo de dimensión-1, entonces I es un $(x_0,\ldots,x_n)$-ideal primario, y el *grado* de I se define como la longitud del k-módulo $k[x_0,\ldots,x_n]/I$, que es igual a su dimensión como k-espacio lineal. También acordamos que $\deg k[x_0,\ldots,x_n] = 0$.

Denotamos por $\operatorname{irr} I$ el número de componentes irreducibles de $V(I) \subseteq \mathbb{P}^n$.

Sean I, $J \subseteq k[x_0,\ldots,x_n]$ ideales homogéneos. Entonces tenemos la siguiente sucesión exacta de k-álgebras graduadas

$$\begin{array}{ccccc} 0 \to R/I\cap J \to & R/I \oplus R/J & \to & R/I+J & \to 0 \\ & (f,g) & \longmapsto & f-g & \end{array}$$

de donde se sigue que

$$h_{I\cap J}(m) = h_I(m) + h_J(m) - h_{I+J}(m) \qquad\qquad m \geq 1$$

En particular, si $\dim I > \dim J$, entonces $\deg I \cap J = \deg I$.

Sea k un cuerpo perfecto, $I \subseteq k[x_0, \ldots, x_n]$ un ideal radical homogéneo, y sea $I = \cap_P P$ la descomposición primaria minimal de I. En esta situación tenemos que

$$\deg I = \sum_{P:\ \dim P = \dim I} \deg V(P)$$

(ver [136, Prop. 1.49] [65, Prop. 13.6]), y entonces del grado del ideal I puede ser calcular a partir de los grados de las variedades definidas por sus ideales primos asociados de dimensión máxima.

Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal radical homogéneo, y $I = \cap_P P$ la descomposición primaria minimal de I. De la inclusión canónica de módulos graduados

$$R_k/I \hookrightarrow \bigoplus_P R_k/P$$

deducimos que

$$h_I(m) \leq \sum_P h_P(m) \qquad\qquad m \geq 1$$

Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo, y $I^e \subseteq \bar{k}[x_0, \ldots, x_n]$ si ideal extendido. Sea

$$k[x_0, \ldots, x_n]/I = \bigoplus_m (k[x_0, \ldots, x_n]/I)_m$$

la descomposición de $k[x_0, \ldots, x_n]/I$ en partes homogéneas. Entonces

$$(\bar{k}[x_0, \ldots, x_n]/I^e)_m = \bar{k} \otimes_k (k[x_0, \ldots, x_n]/I)_m \qquad\qquad m \in \mathbb{Z}$$

y por lo tanto $h_{I^e}(m) = h_I(m)$, i.e. la función de Hilbert es invariante bajo cambios del cuerpo de base. En particular

$$\deg I^e = \deg I$$

Tenemos también que existen $y_0, \ldots, y_d \in \bar{k}[x_0, \ldots, x_n]$ formas lineales algebraicamente independientes tales que

$$\bar{k}[y_0, \ldots, y_d] \hookrightarrow \bar{k}[x_0, \ldots, x_n]/I^e$$

es un inclusion de $\bar{k}$-álgebras, y por lo tanto

$$h_I(m) = h_{I^e}(m) \geq \dim_{\bar{k}}(\bar{k}[y_0, \ldots, y_d])_m = \binom{m+d}{d}$$

Vamos a necesitar la siguiente identidad para los número combinatorios.

Lema 4.2.1 *Sean* $d \geq 0$, $D \geq 1$, $m \in \mathbb{Z}$. *Entonces*

$$\binom{m+d+1+D}{d+1} - \binom{m+d+1}{d+1} = \sum_{i=1}^{D} \binom{m+d+i}{d}$$

Demostración. El caso $D = 1$ es fácil. En el caso en que $D > 1$, tenemos

$$\binom{m+d+1+D}{d+1} - \binom{m+d+1}{d+1} = \sum_{i=1}^{D}\{\binom{m+d+i+1}{d+1} - \binom{m+d+i}{i}\} = \sum_{i=1}^{D}\binom{m+d+i}{d}$$

□

Vamos a apelar a la caracterización de Macaulay de la función de Hilbert de un ideal homogéneo polinomial.

Dado enteros positivos i, c, la *i-expansión binomial* de r es la única expresión

$$c = \binom{c(i)}{i} + \ldots + \binom{c(j)}{j}$$

con $c(i) > \ldots > c(j) \geq j \geq 1$.

Sea $c = \binom{c(i)}{i} + \ldots + \binom{c(j)}{j}$ la i-expansión binomial de c. Entonces ponemos

$$c^{\langle i \rangle} := \binom{c(i)+1}{i+1} + \ldots + \binom{c(j)+1}{j+1}$$

Notamos que esta expresión es la $i+1$-expansión binomial de $c^{\langle i \rangle}$.

Nota 4.2.2 Sea b, c, $i \in \mathbb{Z}_{>0}$. Entonces es fácil ver que $b \geq c$ si y sólo si $(b(i), \ldots, b(j))$ es mayor o igual que $(c(i), \ldots, c(j))$ en el orden lexicográfico, y por lo tanto $b \geq c$ si y sólo si $b^{\langle i \rangle} \geq c^{\langle i \rangle}$.

Recordamos que una sucesión de enteros no-negativos $(c_i)_{i \in \mathbb{Z}_{\geq 0}}$ se llama una *O-sequence* si

$$c_0 = 1 \qquad c_{i+1} \leq c_i^{\langle i \rangle} \qquad i \geq 1$$

Tenemos entonces

Proposición 4.2.3 *(Macaulay, [62]). Sea $h : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$. Entonces h es la función de Hilbert de un ideal polinomial homogéneo si y sólo si*

$$(h(i))_{i \in \mathbb{Z}_{\geq 0}}$$

es una O-sucesión.

□

4.3 Cotas para la Función de Hilbert

En esta sección vamos a derivar cotas inferiores y superiores para la función de Hilbert de un ideal polinomial homogéneo. Esats estimaciones dependen de la dimensión y del grado del ideal en cuestión, y eventualmente de su longitud.

Vamos a deducir primero una cota inferior para la función de Hilbert de un ideal polinomial homogéneo.

Vamos a considerar separadamente el caso en que $\dim I = 0$.

Lema 4.3.1 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo equidimensional de dimensión 0. Entonces*

$$\begin{array}{rclr} h_I(m) & \geq & m+1 & \deg I - 2 \geq m \geq 0 \\ h_I(m) & = & \deg\ I & m \geq \deg I - 1 \end{array}$$

Proof. Tenemos que $I^e \subseteq \bar{k}[x_0, \ldots, x_n]$ es un ideal equidimensional de dimensión cero [139, Ch. VII, S31, Th. 36, Cor.1]. Ya que $\bar{k}$ es un cuerpo infinito, existe una forma lineal $u \in \bar{k}[x_0, \ldots, x_n]$ que no es un divisor de cero modulo I^e. Entonces

$$h_I(m) - h_I(m-1) = h_{I^e}(m) - h_{I^e}(m-1) = h_{(I^e,u)}(m)$$

Sea m_0 mínimo tal que

$$h_{I^e}(m) = \deg\ I^e = \deg\ I$$

para $m \geq m_0$. Entonces $h_{(I^e,u)}(m) \geq 1$ para $0 \leq m \leq m_0 - 1$ y $h_{(I^e,u)}(m) = 0$ para $m \geq m_0$, y así tenemos que

$$h_I(m) = h_{I^e}(m) \geq m+1 \qquad \deg I - 2 \geq m \geq 0$$

y también $h_I(m) = h_{I^e}(m) = \deg\ I$ para $m \geq \deg I - 1$. □

Teorema 4.3.2 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo de dimensión d, con $d \geq 0$. Entonces*

$$h_I(m) \geq \binom{m+d+1}{d+1} - \binom{m-\deg I+d+1}{d+1} \qquad m \geq 1$$

Demostración. Sea $I^e = \bigcap_P Q_P$ una descomposición primaria minimal be a minimal de I^e, y sea

$$I^* = \cap_{\dim P = \dim I^e} Q_P$$

la intersección de las componentes primarias de I^e de dimensión máxima, que es un ideal equidimensional de dimensión d. Entonces $h_I(m) = h_{I^e}(m) \geq h_{I^*}(m)$ para $m \geq 1$, y tenemos que que

$$\deg I = \deg I^*$$

Vamos a proceder por inducción en d. Consideremos primero $d = 0$. Tenemos entonces

$$h_I(m) = h_{I^e}(m) \geq h_{I^*}(m) \geq \binom{m+1}{1} - \binom{m-\deg I+1}{1} \qquad m \geq 1$$

por el Lema 4.3.1 aplicado a I^*.

Ahora sea $d \geq 1$. Sea $u \in \bar{k}[x_0, \ldots, x_n]$ una forma lineal que no es un divisor de cero modulo I^*. Entonces tenemos que

$$h_{I^*}(m) - h_{I^*}(m-1) = h_{(I^*,u)}(m)$$

Luego $\dim(I, u) = d - 1$ y $\deg\,(I^*, u) = \deg\, I^* = \deg\, I$. Por la hipótesis inductiva

$$h_{I^*}(m) - h_{I^*}(m-1) = h_{(I^*,u)}(m) \geq \binom{m+d}{d} - \binom{m-\deg I+d}{d} \qquad m \geq 1$$

Luego

$$\begin{aligned} h_I(m) &\geq h_{I^*}(m) = \textstyle\sum_{j=0}^{m} h_{(I^*,u)}(j) \geq \\ &\geq \textstyle\sum_{j=0}^{m}\{\binom{j+d}{d} - \binom{j-\deg I+d}{d}\} = \binom{m+d+1}{d+1} - \binom{m-\deg I+d+1}{d+1} \qquad m \geq 1 \end{aligned}$$

por Lema 4.3.1. □

Esta desigualdad extiende la estimación de Nesterenko para el caso de un ideal primo [107, S6, Prop. 1] al caso de un ideal arbitrario.

Nota 4.3.3 Por el teorema de persistencia de Gotzmann [62] tenemos que para un ideal homogéneo $I \subseteq k[x_0, \ldots, x_n]$ de dimensión d existe $m_0 \in \mathbb{Z}$ tal que such that

$$h_I(m) \geq \binom{m+d+1}{d+1} - \binom{m-\deg I+d+1}{d+1} \qquad m \geq m_0$$

como fue notado en [22, Rem. 0.6]. Nuestro teorema muestra que esta desigualdad vale globalmente, no sólo para valores grandes de m.

Dado un ideal homogéneo $I \subseteq k[x_0, \ldots, x_n]$ de dimensión $d \geq 0$, sea

$$H_I(t) := \sum_{m=0}^{\infty} h_I(m)\, t^m$$

su serie de Hilbert–Poincaré. Luego el resultado anterior dice que

$$H_I(t) \geq \frac{1 - t^{\deg I}}{(1-t)^{d+2}}$$

en el sentido de que la desigualdad vale para cada término de las series de potencias.

Esta estimación es óptima en términos de la dimensión y el grado del ideal I. Los casos extremos corresponden a hipersuperficies de subespacios lineales de $\mathbb{P}^n$. Esto puede deducirse de [22, Cor. 2.8], que a su vez depende del teorema de Gotzmann. Damos aquí una prueba autocontenida de este hecho.

Proposición 4.3.4 *Sea* $I \subseteq k[x_0, \ldots, x_n]$ *un ideal homogéneo. Entonces*

$$h_I(m) = \binom{m+d+1}{d+1} - \binom{m-\deg I+d+1}{d+1} \qquad m \geq 1$$

si y sólo si existen $u_1, \ldots, u_{n-d-1} \in k[x_0, \ldots, x_n]$ *formas linealmente independientes y* $f \notin (u_1, \ldots, u_{n-d-1})$ *tales que* $I = (u_1, \ldots, u_{n-d-1}, f)$.

Demostración. Sean $u_1, \ldots, u_{n-d-1} \in k[x_0, \ldots, x_n]$ formas linealmente independientes y $f \notin (u_1, \ldots, u_{n-d-1})$. Sea $I := (u_1, \ldots, u_{n-d-1}, f)$. Entonces f no es un divisor de cero modulo modulo $(u_1, \ldots, u_{n-d-1})$, y por lo tanto

$$\begin{aligned} h_I(m) &= h_{(u_1,\ldots,u_{n-d-1})}(m) - h_{(u_1,\ldots,u_{n-d-1})}(m - \deg f) = \\ &= \binom{m+d+1}{d+1} - \binom{m-\deg f+d+1}{d+1} = \binom{m+d+1}{d+1} - \binom{m-\deg I+d+1}{d+1} \end{aligned}$$

Recíprocamente, sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo tal que

$$h_I(m) = \binom{m+d+1}{d+1} - \binom{m-\deg I+d+1}{d+1} \qquad m \geq 1$$

Entonces $h_I(1) \leq d+2$, i. e. $\dim_k I_1 \geq n-d-1$. Sean $u_1, \ldots, u_{n-d-1} \in I_1$ formas linealmente independientes. Tenemos que

$$\begin{aligned} h_I(m) &= \binom{m+d+1}{d+1} & \deg\ I - 1 \geq m \geq 1 \\ h_I(\deg\ I) &= \binom{\deg I+d+1}{d+1} - 1 \end{aligned}$$

Luego

$$\begin{aligned} h_I(m) &= h_{(u_1,\ldots,u_{n-d-1})}(m) & \deg I - 1 \geq m \geq 1 \\ h_I(\deg\ I) &< h_{(u_1,\ldots,u_{n-d-1})}(\deg\ I) \end{aligned}$$

y por lo tanto existe $f \in I-(u_1, \ldots, u_{n-d-1})$ con $\deg f = \deg\ I$. Sea $J := (u_1, \ldots, u_{n-d-1}, f) \subseteq k[x_0, \ldots, x_n]$. Luego $J \subseteq I$ y $h_J(m) = h_I(m)$ para todo $m \geq 0$, y por lo tanto $J = I$. □

Nos dedicamos ahora a las cotas superiores. Con respecto a esto tenemos dos estimaciones diferentes. La primera cota es precisa para valores chicos y la segunda para valores grandes.

La primera cota superior se va a deducir de una serie de resultados previos y observaciones.

Sea $V \subseteq \mathbb{P}^n$ una variedad. Entonces la *clausura lineal* de V es es menor espacio lineal de $\mathbb{P}^n$ que contiene a V, y se denota por $L(V)$.

Nota 4.3.5 Sea $E \subseteq \mathbb{P}^n$ un espacio lineal. Entonces su ideal de definición $I(E) \subseteq R_{\bar{k}}$ está generado por formas lineales, y es fácil ver que

$$\dim E = n - \dim_{\bar{k}} I(E)$$

Sea $V \subseteq \mathbb{P}^n$ una variedad, y sea $L \in R_{\bar{k}}$ una forma lineal. Entonces $L|_V \equiv 0$ si y sólo $L|_{L(V)} \equiv 0$, y por lo tanto

$$I(L(V)) = (I(V)_1) \subseteq \bar{k}[x_0, \ldots, x_n]$$

En particular tenemos

$$h_V(1) = n + 1 - \dim_{\bar{k}} \ I_{\bar{k}}(V)_1 = \dim L(V) + 1$$

La siguiente proposición muestra que la dimensión de la clausura lineal está acotada en términos de la dimensión y del grado de la variedad. Es una consecuencia del teorema de Bertini [78, Th. 6.3]. Una demostración se puede encontrar en [65, Cor. 18.12].

Proposición 4.3.6 *Sea $V \subseteq \mathbb{P}^n$ una variedad irreducible . Entonces*

$$\dim L(V) + 1 \leq \deg V + \dim V$$

□

La siguiente es una estimación del grado de la imagen de una variedad bajo una aplicación regular. Es una variante de [70, Lemma 1] y [119, Prop. 1].

Proposición 4.3.7 *Sea $V \subseteq \mathbb{P}^n$ una variedad, $f_0, \ldots, f_N \in \bar{k}[x_0, \ldots, x_n]$ olinomios homogéneosde grado D que definen una aplicación regular*

$$\begin{aligned} \varphi : \ & \mathbb{P}^n \longrightarrow \mathbb{P}^N \\ & x := (x_0 : \ldots : x_n) \mapsto (f_0(x) : \ldots : f_N(x)) \end{aligned}$$

Entonces $\deg \varphi(V) \leq \deg V \ D^{\dim V}$.

Demostración. Podemos suponer sin pérdida de generalidad que V es irreducible. Sea $d := \dim \ \varphi(V)$, y sean $H_1, \ldots, H_d \subseteq \mathbb{P}^n$ hiperplanos tales que

$$\#(\varphi(V) \cap H_1 \cap \ldots \cap H_d) = \deg \ \varphi(V)$$

Para $i = 1, \ldots, d$, sean $L_i \in R_{\bar{k}}$ formas lineales tales que $H_i = \{L_i = 0\}$. Entonces

$$\#(\varphi(V) \cap H_1 \cap \ldots \cap H_d)$$

está acotado por el número de componentes irreducibles de $\varphi^{-1}(\varphi(V) \cap H_1 \cap \ldots \cap H_d)$ y por lo tanto tenemos que

$$\begin{aligned} \#(\varphi(V) \cap H_1 \cap \ldots \cap H_d) & \leq \deg \ \varphi^{-1}(\varphi(V) \cap H_1 \cap \ldots \cap H_d) = \\ & = \deg \ (V \cap \textstyle\bigcap_{i=1}^d V(L_i(f_0, \ldots, f_N))) \leq \deg V \ D^d \end{aligned}$$

por la desigualdad de Bézout. Tenemos entonces que

$$\deg \varphi(V) \leq \deg V \ D^{\dim V}$$

ya que $\dim \ \varphi(V) \leq \dim \ V$. □

Ahora se sigue fácilmente la desigualdad deseada para el caso de una variedad irreducible.

Proposición 4.3.8 *Sea $V \subseteq \mathbb{P}^n$ una variedad irreducible de dimensión d, con $d \geq 0$. Entonces*

$$h_V(m) \leq \deg V \; m^d + d \qquad\qquad m \geq 1$$

Demostración. Para $n, m \in \mathbb{N}$, sea

$$\begin{aligned} v_m: \;\; & \mathbb{P}^n \longrightarrow \mathbb{P}^{\binom{n+m}{n}} \\ & (x_0 : \ldots : x_n) \mapsto (x^{(i)})_{|i|=m} \end{aligned}$$

la aplicación de Veronese de grado m. Entonces $v_m|_V : V \mapsto v_m(V)$ s un morfismo birregular de grado m, y por lo tanto tenemos que

$$h_{v_m(V)}\,(k) = h_V(mk) \qquad\qquad k \geq 1$$

En particular tenemos que

$$h_V(m) = h_{v_m(V)}\,(1) = \dim L(V) + 1$$

por la Nota 4.3.5, y por lo tanto

$$h_V(m) \leq \deg v_m(V) + \dim v_m(V) \leq \deg V \; m^d + d$$

por aplicación de las Proposiciones 4.3.7 y 4.3.8. □

Sea puede extender esta cota al caso más general de un ideal radical equidimensional en $k[x_0, \ldots, x_n]$.

Teorema 4.3.9 *Sea k un cuerpo perfecto y $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo equidimensional de dimensión d, con $d \geq 0$. Entonces*

$$h_I(m) \leq \deg I \; m^d + \operatorname{irr} I \; d \qquad\qquad m \geq 1$$

Demostración. Sea $I^e \subseteq R_{\bar{k}}$ el ideal extendido de I en $R_{\bar{k}}$. Entonces I^e es un ideal radical equidimensional de dimensión d [139, Ch. VII, S31, Th. 36, Cor. 1] [101, Th. 26.3]. Sea $I^e = \cap_P P$ la descomposición primaria minimal de I^e. Entonces

$$h_I(m) \leq \sum_P h_P(m)$$

de donde

$$h_I(m) \leq \sum_P \left(degV(P)\; m^d + d\right) = \deg I \; m^d + \operatorname{irr} I \; d \qquad\qquad m \geq 1$$

por la Proposición 4.3.8. □

Esta desigualdad tiene el mismo orden de crecimiento de h_I. Vemos también que no mejora la estimación

$$h_I(m) \leq \deg I \binom{m+d-1}{d} + \operatorname{irr} I \binom{m+d-1}{d-1} \qquad m \geq 1$$

que se sigue de los argumentos de Chardin [36].

Del comportamiento asintótico $h_I(m) \sim \frac{\deg I}{d!} m^d$ vemos que esta desigualdad es precisa para valores grandes de m sólo cuando $d = 1$. En este caso, la desigualdad es óptima enb términos del grado y la longitud del ideal, y podemos determinar los casos extremales.

Sean $V, W \subseteq \mathbb{P}^n$ variedades. Entonces V, W son *proyectivamente equivalentes* si existe un automorfismo $A \in PGL_{n+1}(\bar{k})$ tal que $W = A(V)$ [65, p. 22].

Nota 4.3.10 Sean $V, W \subseteq \mathbb{P}^n$ variedades. Entonces V, W son proyectivamente equivalentes si y sólo si sus anillos coordenados $\bar{k}[V]$, $\bar{k}[W]$ son isomorfos como $\bar{k}$-álgebras graduadas. en particular sus funciones de Hilbert coinciden.

Una curva $C \subseteq \mathbb{P}^n$ se llama una *rational normal curve* si es proyectivamente equivalente a $v_n(\mathbb{P}^1)$. Entonces C es no degenerada, es decir $L(C) = \mathbb{P}^n$ [65, Example 1.14], y su grado es n [65, Exerc. 18.8]. Por la Proposición 4.3.8 el grado de C es mínimo con la condición de no-degeneración. De hecho, las curvas normales racionales están cvaracterizadas por estas dos propiedades [65, Prop. 18.9].

Ahora sean $l, n \in \mathbb{N}$, $\delta = (\delta_1, \ldots, \delta_l) \in \mathbb{N}^l$ tales que $|\delta| := \delta_1 + \ldots + \delta_l \leq n + 1 - l$. Para $1 \leq j \leq l$, let $n_j := \delta_1 + \ldots + \delta_j + j$, y consideramos la inclusión de espacios lineales dada por

$$\begin{aligned} \mathbb{P}^{\delta_j} &\hookrightarrow \mathbb{P}^n \\ (x_0 : \ldots : x_{\delta_j}) &\mapsto (\overbrace{0 : \ldots : 0}^{n_{j-1}} : x_0 : \ldots : x_{\delta_j} : 0 : \ldots : 0) \end{aligned}$$

Los subespacios lineales $i_j(\mathbb{P}^{\delta_j}) \subseteq \mathbb{P}^n$ son disjuntos entre sí. Sea

$$C(n, \delta) := \bigcup_{j=1}^{l} i_j(v_{\delta_j}(\mathbb{P}^1)) \subseteq \mathbb{P}^n$$

Una curva $C \subseteq \mathbb{P}^n$ es proyectivamente equivalente a $C(n, \delta)$ si y sólo si existen $E_1, \ldots, E_l \subseteq \mathbb{P}^n$ espacios lineales disjuntos tales que $\dim E_j = \delta_j$, $C \subseteq \cup_j E_j$, y

$$C_j := C \cap E_j \subseteq E_j$$

es una curva racional normal para $1 \leq j \leq l$.

Sea $V \subseteq \mathbb{P}^n$ una variedad. Entonces V está *definida sobre* k si $I_{\bar{k}}(V) = \bar{k} \otimes_k I_k(V) \subseteq \bar{k}[x_0, \ldots, x_n]$, es decir si su ideal de definición está generado sobre k.

El siguinete lema es bien conocido, lo probamos aquí por falta de referencia adecuada.

Lema 4.3.11 *Sean $\varphi : \mathbb{P}^n \to \mathbb{P}^N$ una aplicación regular definida sobre k, $V \subseteq \mathbb{P}^n$ una variedad definida sobre k. Entonces $\varphi(V) \subseteq \mathbb{P}^N$ está definida sobre k.*

Proof. Tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} k[x_0,\ldots,x_N] & \xrightarrow{\varphi_k^*} & k[V] \\ \downarrow & & \downarrow \\ \bar{k}[x_0,\ldots,x_N] & \xrightarrow{\varphi_{\bar{k}}^*} & \bar{k}[V] \end{array}$$

con $\ker\varphi_k^* = I_k(W)$ y $\ker\varphi_{\bar{k}}^* = I_{\bar{k}}(W)$. Tenemos $\bar{k}\otimes_k k[V] \cong \bar{k}[V]$ ya que V está definida sobre k, y tensorizando con $\bar{k}$ obtenemos

$$\begin{array}{ccc} \bar{k}[x_0,\ldots,x_N] & \xrightarrow{\bar{k}\otimes_k\varphi_k^*} & \bar{k}\otimes_k k[V] \\ \| & & \| \\ \bar{k}[x_0,\ldots,x_N] & \xrightarrow{\varphi_{\bar{k}}^*} & \bar{k}[V] \end{array}$$

con $\ker \bar{k}\otimes_k \varphi_k^* = \bar{k}\otimes_k I_k(W)$, de donde se deduce $I_{\bar{k}}(W) = \bar{k}\otimes_k I_k(W)$, es decir que $I_{\bar{k}}(W)$ está definida sobre k. □

Sea $v_n : \mathbb{P}^1 \to \mathbb{P}^n$ la aplicación de Veronese de grado n y sea $C_n := v_n(\mathbb{P}^1)$ su imagen. Por el lema anterior C_n está definida sobre k.

Para $1 \le j \le l$, sea $C_j := i_j(C_{\delta_j}) \subseteq \mathbb{P}^n$. Entonces

$$C(n,\delta) = \bigcup_{j=1}^{l} i_j(v_{\delta_j}(\mathbb{P}^1))$$

es la descomposición minimal de $C(n,\delta)$ en curvas irreducibles. Luego $C(n,\delta)$ está definida también sobre k, y por lo tanto

$$\text{irr } I_k(C(n,\delta)) = l, \qquad \deg I_k(C(n,\delta)) = |\delta|$$

Lema 4.3.12 *Sean $V, W \subseteq \mathbb{P}^n$ variedades. Entonces*

$$I(V) + I(W) = (x_0,\ldots,x_n)$$

si y sólo si V, W están en subespacios lineales disjuntos de $\mathbb{P}^n$.

Proof. Sean $V, W \subseteq \mathbb{P}^n$ variedades, están en espacios lineales disjuntos si y sólo si

$$L(V) \cap L(W) = \emptyset$$

Sean $L_V := I(L(V))$, $L_W := I(L(W))$. Por la Nota 4.3.5 tenemos

$$L_V = (I(V)_1) \subseteq I(V)$$
$$L_W = (I(W)_1) \subseteq I(W)$$

En particular L_V, L_W están generados por formas lineales, y por lo tanto

$$L_V + L_W = I(L(V) \cap L(W))$$

Sean $V, W \subseteq \mathbb{P}^n$ tales que $L(V) \cap L(W) = \emptyset$. Entonces

$$L_V + L_W = (x_0, \ldots, x_n)$$

y por lo tanto $I(V) + I(W) = (x_0, \ldots, x_n)$. Recíprocamente, supongamos que $I(V) + I(W) = (x_0, \ldots, x_n)$. Entonces

$$x_0, \ldots, x_n \in I(V)_1 + I(W)_1$$

Luego $L_V + L_W = (x_0, \ldots, x_n)$ y por lo tanto $L(V) \cap L(W) = \emptyset$ □

Proposición 4.3.13 *Sean k un cuerpo perfecto y $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo radical y equidimensional de dimensión uno. Entonces*

$$h_I(m) = \deg I \; m + \operatorname{irr} I \qquad\qquad m \geq 1$$

si y sólo si existen $\delta \in \mathbb{N}^l$ with $l := \operatorname{irr} I$, tales que $|\delta| = \deg I$, y una curva $C \subseteq \mathbb{P}^n$ definida sobre k proyectivamente equivalente a $C(n, \delta)$ tal que $I = I_k(C)$.

Demostración. Sea $C \subseteq \mathbb{P}^n$ una curva defnida sobre k proyectivamente equivalente a $C(n, \delta)$ para algún $\delta \in \mathbb{N}^l$ y $l = \operatorname{irr} I$. Entonces $\bar{k} \otimes_k I_k(C) = I_{\bar{k}} \subseteq R_{\bar{k}}$ y por lo tanto

$$\operatorname{irr} I_k(C) = \operatorname{irr} I(C(n, \delta)) = l, \qquad\qquad \deg I_k(C) = \deg I(C(n, \delta)) = |\delta|$$

Queremos probar que

$$h_{I_k(C)}(m) = |\delta| \; m + l \qquad\qquad m \geq 1$$

Tenemos que $h_{I_k(C)}(m) = h_C(m) = h_{C(n,\delta)}(m)$ y por lo tanto es suficiente con probar

$$h_{C(n,\delta)}(m) = |\delta| m + l \qquad\qquad m \geq 1$$

Vamos a proceder por inducción en l. Sea $C_d := v_d(\mathbb{P}^1)$. Tenemos la inclusión de $\bar{k}$-álgebras graduadas

$$\begin{array}{rcl} \bar{k}[C_d] \cong & \bar{k}[x_0, \ldots, x_d]/I_{\bar{k}}(C_d) & \overset{v_d^*}{\hookrightarrow} \bar{k}[x, y] \\ & x_i \longmapsto x^i y^{d-i} & \end{array}$$

Tenemos entonces que

$$\bar{k}[C_d] \cong \bigoplus_{j=0}^{\infty} \bar{k}[x, y]_{dj}$$

de donde $h_{C_d}(m) = d\,m + 1$ for $m \geq 1$, y por lo tanto la afirmación vale para $l = 1$. Sea $l > 1$, y sea

$$C(n,\delta) = \bigcup_j C_j$$

la descomposición minimal de $C(n,\delta)$ en curvas irreducibles. Entonces $C_1 \cup \ldots \cup C_{l-1}$, C_l están en espacios lineales disjuntos y por lo tanto

$$I(C_1 \cup \ldots \cup C_{l-1}) + I(C_l) = (x_0, \ldots, x_n)$$

por Lema 4.3.12. Tenemos entonces

$$h_C(m) = h_{C_1 \cup \ldots \cup C_{l-1}}(m) + h_{C_l}(m) \qquad m \geq 1$$

y de la hipótesis inductiva obtenemos

$$h_C(m) = \{(\delta_1 + \ldots + \delta_{l-1})\,m + (l-1)\} + \{\delta_l\,m + 1\} = |\delta|\,m + l \qquad m \geq 1$$

Ahora vamos a probar la recíproca. Tenemos que I^e es un ideal radical, y por lo tanto I^e es el ideal de alguna curva $C \subseteq \mathbb{P}^n$ definida sobre k.

Vamos a proceder por inducción en $l := \operatorname{irr} I$. Sea $l = 1$, es decir $C \subseteq \mathbb{P}^n$ irreducible. Entonces

$$\dim L(C) = h_C(1) - 1 = \deg C$$

y por lo tanto $C \subseteq L(C)$ es una curva irreducible y no degenerada de grado mínimo. Tenemos entonces que $C \subseteq L(C)$ es una curva normal racional [65, Prop. 18.9].

Sea $l > 1$, y supongamos que la afirmación está probada para $l(I) \leq l - 1$ y K un cuerpo arbitrario. En particular es válida para $\bar{k}$, la clausura algebraica de k. Sea $C = C_1 \cup \ldots \cup C_l$ la descomposición minimal de C en curvas irreducibles. Entonces

$$h_C(m) = h_{C_1 \cup \ldots \cup C_{l-1}}(m) + h_{C_l}(m) - h_{I(C_1 \cup \ldots \cup C_{l-1}) + I(C_l)}(m) \qquad m \geq 1$$

Deducimos del Teorema 4.3.9 que

$$\begin{aligned} h_{C_l}(m) = &\ \delta_l\,m + 1 \\ h_{C_1 \cup \ldots \cup C_{l-1}}(m) = &\ (\delta_1 + \ldots + \delta_{l-1})\,m + (l-1) \end{aligned}$$

y por lo tanto $C_l \subseteq L(C_l)$ es una curva racional normal, y por la hipótesis inductiva $C_1 \cup \ldots \cup C_{l-1}$ es proyectivamente equivalente a $C(n, (\deg C_1, \ldots, \deg C_{l-1}))$. Luego

$$h_C(m) = |\delta| m + l - h_{I(C_1 \cup \ldots \cup C_{l-1}) + I(C_l)}(m) \qquad m \geq 1$$

y por lo tanto

$$I(C_1 \cup \ldots \cup C_{l-1}) + I(C_l) = (x_0, \ldots, x_n)$$

Luego $C_1 \cup \ldots \cup C_{l-1}$, C_l están en espacios lineales disjuntos por Lema 4.3.12, y por lo tanto C es proyectivamente equivalente a $C(n, (\deg C_1, \ldots, \deg C_l))$. □

Ahora vamos a deducir otra cota superior para la función de Hilbert de un ideal radical equidimensional. El siguiente lema es bien conocido, lo probamos aquí por falta de una referencia adecuada.

Lema 4.3.14 *Sea A un dominio de integridad, K su cuerpo cociente, L una extensión finita separable de K, B la clausura integral de A in L. Sea $\eta \in B$ tal que $L = K[\eta]$, y sea $f \in K[t]$ su polinomio minimal. Entonces*

$$f'(\eta)B \subseteq A[\eta]$$

Proof. Sea $M \subseteq L$ un A-módulo. Entonces

$$M' := \{x \in L : \mathrm{Tr}\ {}^{L}_{K}(xM) \subseteq A\}$$

Se llama el *módulo complementario* (relativo a la traza) de M [90, Ch. III, §1].

Es inmediato que si $M \subseteq B$ entonces $M' \supseteq B$. Tenemos que

$$A[\eta]' = \frac{A[\eta]}{f'(\eta)}$$

(ver [90, Ch. III, Prop. 2, Cor.]) y por lo tanto

$$B \subseteq A[\eta]' = \frac{A[\eta]}{f'(\eta)}$$

□

Cuando A is un dominio integralmente cerrado, tenemos que $f \in A[t]$, y por lo tanto la última afirmación dice en el lenguaje de la teoría de dependencia entera que en este caso $f'(\eta)$ está en el conductor de B en $A[\eta]$.

Teorema 4.3.15 *Sea k un cuerpo perfecto y $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo radical y equidimensional de dimensión d, con $d \geq 0$. Entonces*

$$h_I(m) \leq \binom{m+\deg I+d}{d+1} - \binom{m+d}{d+1} \qquad m \geq 1$$

Proof. Vamos a considerar primero el caso en que $P \subseteq \bar{k}[x_0, \ldots, x_n]$ es un ideal primo homogéneo.

El cuerpo $\bar{k}$ es algebraicamente cerrado, y por lo tanto es infinito y perfecto. Sean $y_0, \ldots, y_d, \eta \in \bar{k}[x_0, \ldots, x_n]$ formas lineales tales que

$$\bar{k}[y_0, \ldots, y_d] \hookrightarrow \bar{k}[x_0, \ldots, x_n]/P$$

sea una inclusión entera de $\bar{k}$-álgebras graduadas y tales que si K, L son los cuerpos cocientes de $\bar{k}[y_0, \ldots, y_d]$, $\bar{k}[x_0, \ldots, x_n]/P$ respectivamente, entonces $K \hookrightarrow L$ es separable algebraica y $L = K[\eta]$.

Sea $A := \bar{k}[y_0, \ldots, y_d]$, $B := \bar{k}[x_0, \ldots, x_n]/P$. Como una consecuencia del Krull's Hauptidealsatz tenemos que

$$A[\eta] \cong A[t]/(F)$$

donde $F \in \bar{k}[y_0, \ldots, y_d][t]$ es un polinomio homogéneo no nulo. Tenemos entonces

$$\dim_{\bar{k}}(A[\eta])_m = h_{(F)}(m) = \binom{m+d+1}{d+1} - \binom{m-\deg F+d+1}{d+1}$$

Tenemos también

$$A[\eta] \hookrightarrow B \hookrightarrow \frac{A[\eta]}{F'(\eta)}$$

por Lema 4.3.14, y así

$$\binom{m+d+1}{d+1} - \binom{m-\deg F+d+1}{d+1} \leq h_P(m) \leq \binom{m+\deg F+d}{d+1} - \binom{m+d}{d+1} \qquad m \geq 1$$

Deducimos que $\deg F = \deg P$, y por lo tanto

$$h_P(m) \leq \binom{m+\deg P+d}{d+1} - \binom{m+d}{d+1} \qquad m \geq 1$$

Ahora vamos a extender esta cota al caso de un ideal equidimensional. Tenemos que I^e es un ideal radical y equidimensional. Sea $I^e = \cap_P P$ la descomposición primaria de I^e. Tenemos

$$h_I(m) \leq \sum_P \left\{\binom{m+\deg P+d}{d+1} - \binom{m+d}{d+1}\right\} \qquad m \geq 1$$

Tenemos entonces

$$h_I(m) \leq \sum_P \sum_{i=0}^{\deg P-1} \binom{m+d+i}{d} \leq \sum_{i=0}^{\deg I-1} \binom{m+d+i}{d} = \binom{m+\deg I+d}{d+1} - \binom{m+d}{d+1}$$

□

Nota 4.3.16 Esta desigualdad es precisa para valores grandes de m, como se ve comparándola con el término principal del polinomio de Hilbert de I.

De la expresión

$$h_I(m) \leq \binom{m+\deg I+i}{d+1} - \binom{m+d}{d+1} = \sum_{i=0}^{\deg I-1} \binom{m+d+i}{d}$$

vemos que no mejora la estimación de Chardin [36, Th.]

$$h_I(m) \leq \deg I \binom{m+d}{d} = \sum_{i=0}^{\deg I-1} \binom{m+d}{d}$$

en ningún caso. Sin embargo notamos que la demostración es más simple y que podemos utilizarla en nuestras aplicaciones en lugar de la cota de Chardin obteniendo resultados muy similares.

Sea k un cuerpo perfecto, $I \subseteq k[x_0, \ldots, x_n]$ Un ideal homogéneo radical y equidimensional de dimensión $d \geq 0$, y sea H_I su serie de Hilbert–Poincaré. Luego el resultado anterior dice que

$$t^{\deg I - 1} H_I(t) \leq \frac{1 - t^{\deg I}}{(1-t)^{d+2}}$$

en el sentido de que esta desigualdad vale para cada término de las series de potencias.

Dearivamos ahora una cota superior para la función de Hilbert de una sección generica por una hipersuperficie de un ideal radical y equidimensional, que es un ideal que no es necesariamente radical ni equidimensional. Este resultado es una aplicación de nuestras cotas superiores e inferiores para la función de Hilbert. función de Hilbert. El uso de nuestra cota superior (Theorem 4.3.15) puede ser reemplazado por la estimación de Chardin [36, Teorema] pero la cota obtenida es esencialmente la misma. De esta manera mantenemos nuestra exposición autocontenida.

Lema 4.3.17 *Sea k un cuerpo perfecto y $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo radical y equidimensional de dimensión d, con $d \geq 1$, y sea $\eta \in k[x_0, \ldots, x_n]$ una forma lineal que no es un divisor de cero modulo I. Entonces existe m_0 tal que*

$$h_{(I,\eta)}(m_0) \leq \binom{m_0+d}{d} - \binom{m_0+d-3\deg I}{d}$$

y $3 \deg I \leq m_0 \leq 5\, d \deg I$.

Demostración. Sea $\delta := \deg I$, $k := 3\,\delta$, $l := 2\,\delta$, $m := 5\, d\, \delta$. Queremos probar que

$$\sum_{j=0}^{l-1} \left\{ \binom{m-j+d}{d} - \binom{m-j+d-k}{d} \right\} \geq \sum_{j=0}^{l-1} h_{(I,\eta)}(m-j)$$

Tenemos que

$$\sum_{j=0}^{l-1} \left\{ \binom{m+d-j}{d} - \binom{m+d-k-j}{d} \right\} = \left\{ \binom{m+d+1}{d+1} - \binom{m+d+1-l}{d+1} \right\} - \left\{ \binom{m+d+1-k}{d+1} - \binom{m+d+1-k-l}{d+1} \right\}$$

Tenemos también

$$\sum_{j=0}^{l-1} h_{(I,\eta)}(m-j) = h_{(I,\eta^r)}(m) \leq \left\{ \binom{m+d+\delta}{d+1} - \binom{m+d}{d+1} \right\} - \left\{ \binom{m+d+1-l}{d+1} - \binom{m+d+1-\delta-l}{d+1} \right\}$$

por aplicación de los Teoremas 4.3.2 y 4.3.15. Luego alcanza con probar

$$\begin{aligned} \left\{ \binom{m+d+1-\delta}{d+1} - \binom{m+d+1-\delta-l}{d+1} \right\} \quad & - \left\{ \binom{m+d+1-k}{d+1} - \binom{m+d+1-k-l}{d+1} \right\} \geq \\ & \geq \left\{ \binom{m+d+\delta}{d+1} - \binom{m+d}{d+1} \right\} - \left\{ \binom{m+d+1}{d+1} - \binom{m+d+1-\delta}{d+1} \right\} \end{aligned}$$

Tenemos que

$$\begin{aligned} \left\{ \binom{m+d+1-\delta}{d+1} - \binom{m+d+1-\delta-l}{d+1} \right\} \quad & - \left\{ \binom{m+d+1-k}{d+1} - \binom{m+d+1-k-l}{d+1} \right\} = \\ & = \textstyle\sum_{i=1}^{l} \left\{ \binom{m+d+1-\delta-i}{d} - \binom{m+d+1-k-i}{d} \right\} = \\ & = \textstyle\sum_{i=1}^{l} \sum_{j=1}^{k-\delta} \binom{m+d+1-\delta-i-j}{d-1} \geq l\,(k-\delta) \binom{m+d-1-k-l}{d-1} \end{aligned}$$

y

$$\begin{aligned}\{\tbinom{m+d+\delta}{d+1}-\tbinom{m+d}{d+1}\}-\{\tbinom{m+d+1}{d+1} &- \tbinom{m+d+1-\delta}{d+1}\} = \sum_{i=1}^{\delta}\{\tbinom{m+d+\delta-i}{d}-\tbinom{m+d+1-i}{d}\} = \\ &= \sum_{i=1}^{\delta}\sum_{j=1}^{\delta}\tbinom{m+d+\delta-i-j}{d-1} \leq \delta^2\tbinom{m+d-1+\delta}{d-1}\end{aligned}$$

y por lo tanto alcanza con probar

$$4=\frac{l\,(k-\delta)}{\delta^2} \geq \frac{\binom{m+d-1+\delta}{d-1}}{\binom{m+d-1-k-l}{d-1}}$$

Esto es claro cuando $d=1$, ya que en este caso el lado derecho de esta expresión of this expression es igual a 1. Cuando $d \geq 2$ tenemos que

$$\frac{\binom{m+d-1+\delta}{d-1}}{\binom{m+d-1-k-l}{d-1}} = \prod_{j=1}^{d-1}\frac{m+\delta+j}{m-k-l+j} \leq (1+\frac{6/5}{d-1})^{d-1} \leq e^{\frac{6}{5}}$$

y por lo tanto nuestra afirmación se sigue, y concluimos que

$$h_{(I,\eta)}(m_0) \leq \tbinom{m_0+d}{d}-\tbinom{m_0+d-3\deg I}{d}$$

para algún m_0 tal que $5\,d\,\delta-2\,\delta+1 \leq m_0 \leq 5\,d\,\delta$.

□

Teorema 4.3.18 *Sea k un cuerpo perfecto y $I \subseteq k[x_0,\ldots,x_n]$ un ideal homogéneo radical y equidimensional de dimensión d, con $d \geq 0$, y sea $f \in k[x_0,\ldots,x_n]$ un no divisor de cero modulo I. Entonces*

$$\begin{aligned} h_{(I,f)}(m) &\leq \deg\, I & & m \geq 1 \\ h_{(I,f)}(m) &= 0 & & m \geq \deg\, I+\deg f-1 \end{aligned}$$

si $d=0$ y

$$h_{(I,f)}(m) \leq 3\,\deg f\,\deg I\tbinom{m+d-1}{d-1}$$

si $d \geq 1$ y $m \geq 5\,d\deg I$.

Demostración. Sea $\delta := \deg I$, $d_0 := \deg f$. Tenemos

$$h_{(I,f)}(m) = h_I(m) - h_I(m-d_0)$$

Consideramos primero el caso $d=0$. Entonces $h_I(m) \leq \delta$ para $m \geq 1$ y $h_I(m)=\delta$ para $m \geq \delta-1$ por Lema 4.3.14, y así

$$h_{(I,f)}(m) = 0 \qquad\qquad m \geq \delta+d_0-1$$

Ahora sea $d \geq 1$. Tenemos que I^e es un ideal radical y equidimensional y por lo tanto existe un forma lineal $\eta \in k[x_0,\ldots,x_n]$ que no es un divisor de cero modulo I^e. Por Lema 4.3.12

$$h_{(I^e,\eta)}(m_0) \leq \tbinom{m+d}{d}-\tbinom{m+d-3\deg I}{d}$$

para algún $3 \deg I \leq m_0 \leq 5\, d \deg I$.

Sea $m \geq 3\,\delta$. Tenemos entonces que

$$\binom{m+d}{d} - \binom{m+d-3\deg I}{d} = \sum_{j=1}^{3\,\delta} \binom{m+d-j}{m-j+1}$$

el la m–expansión binomial de $\binom{m+d}{d} - \binom{m+d-3\deg I}{d}$, y por lo tanto

$$h_{(I,\eta)}(m) \leq \binom{m+d}{d} - \binom{m+d-3\,\delta}{d}$$

para $m \geq m_0$ por el teorema de Macaulay y la Nota 4.2.2. Tenemos entonces

$$h_{(I,f)}(m) = h_{(I^e,f)}(m) = \sum_{j=0}^{d_0-1} h_{(I^e,\eta)}(m-j) \leq 3\, d_0\, \delta \binom{m+d-1}{d-1}$$

para $m \geq 5\, d\, \delta$.

Bibliografía

[1] M. S. ALMEIDA, *Función de Hilbert de álgebras graduadas y Nullstellensatz afín efectivo*, Tesis de Licenciatura, Univ. Buenos Aires, 1995.

[2] M. ALMEIDA, L. DÁLFONSO, P. SOLERNÓ, *Sur les degrées des bases de modules libres sur lánneau de polynomes*, aparecerá en *Math. Zeitschrift.*

[3] M. E. ALONSO, E. BECKER, M.-F. ROY, T. WÖRMANN, *Zeros, multiplicities and idempotents for zerodimensional systems,* en L. González-Vega y T. Recio, eds., Algorithms in algebraic geometry and applications, Proceedings MEGA'94, Birkäuser Progress in Math. **143**, Bikhäuser, Basel, 1996, pp. 1–15.

[4] F. AMOROSO, *On a conjecture of C. Berenstein y A. Yger*, in L. González-Vega y T. Recio, eds., Algorithms in algebraic geometry and applications, Proceedings MEGA'94, Birkäuser Progress in Math. **143**, Bikhäuser, Basel, 1996, pp. 17–28.

[5] I. ARMENDÁRIZ, P. SOLERNÓ, *On the computation of the radical of a polynomial complete intersection,* en G. Cohen, M. Giusti y T. Mora, eds., Proceedings AAECC-11, Lect. Notes. Comput. Sci. **948**, pp. 106–119, Springer, Berlin, 1995.

[6] E. ARTIN, *Algebraic numbers and algebraic functions,* Gordon and Breach, 1967.

[7] M. F. ATIYAH, I. G. MACDONALD, *Introduction to commutative algebra,* Adison-Wesley, 1969.

[8] H. BASS, E. CONNELLE, T. WRIGHT, *The jacobian conjeture: reduction of degree and formal expansion of the inverse,* Bull. AMS, **7** (1982), pp. 287-330.

[9] D. BAYER, D. MUMFORD, *What can be computed in algebraic geometry?,* In: Eisenbud, D. and Robbiano, L. (eds): Computational Algebraic Geometry and Commutative Algebra, Cambridge Univ. Press, (1993), pp. 1–48.

[10] E. BECKER, J. P. CARDINAL, M.-F. ROY, Z. SZAFRANIEC, *Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levine formula,* en L. González-Vega y T. Recio, eds., Algorithms in algebraic geometry and applications, Proceedings MEGA'94, Birkäuser Progress in Math. **143**, Bikhäuser, Basel, 1996, pp. 79–104.

[11] C. A. BERENSTEIN, D. C. STRUPPA, *Recent improvements in the complexity of the effective Nullstellensatz,* Linear Alg. Appl. **157** (1991), pp. 203-215.

[12] C. A. BERENSTEIN, A. YGER, *Bounds for the degrees in the division problem,* The Michigan Mathematical Journal **37** (1990), pp. 25–43.

[13] C. A. BERENSTEIN, A. YGER, *Effective Bézout identities in* $\mathbb{Q}[x_1, \ldots, x_n]$, Acta Math. **166** (1991), pp. 69–120.

[14] C. A. BERENSTEIN, A. YGER, *Une formule de Jacobi et ses conséquences,* Ann. Sci. E. N. S. **24** (1991), pp. 363-377.

[15] C. A. BERENSTEIN, A. YGER, *Residue calculus and effective Nullstellensatz,* Manuscrito, 1996.

[16] D. N. BERNSHTEIN, *The number of root of a system of equations,* Funcional Analysis and its Applications **9** (1975), pp. 183–185 (translated from Russian).

[17] D. BERTRAND, *Lemmes des zéros et nombres trascendants* Sém. Bourbaki 652, Astérisque 145-146, pp. 21–44, Soc. Math. France, 1987.

[18] É. BÉZOUT, *Sur le degré des équations résultantes de l' évanouissement des inconnus,* Mémoires presentés par divers savants á lÁcadémie des sciences de lÍnstitut de France, (1764).

[19] É. BÉZOUT, *Sur le degré résultant des méthodes délimination entre plusieurs équations,* Mémoires presentés par divers savants á lÁcadémie des sciences de lÍnstitut de France, (1764).

[20] É. BÉZOUT, *Sur le degré des équations résultantes de lévanouissement des inconnus,* Historie de á lÁcadémie Royale des Sciences, année (1764), pp. 288–338, Paris (1767).

[21] É. BÉZOUT, *Théorie générale des équations algébriques,* Paris, 1970.

[22] A. BIGATTI, A. GERAMITA, J. MIGLIORE, *Geometric consequences of extremal behavior in a theorem of Macaulay,* Trans. Amer. Math. Soc. **346** (1994), pp. 203–235.

[23] E. BOMBIERI, *The Mordell conjecture revisited,* Manuscrito.

[24] J.-B. BOST, H. GILLET, C. SOULÉ, *Une analogue arithmétique du théorème de Bézout,* C. R. Acad. Sci. Paris Sér. I Math. **312** (1991), pp. 845–848.

[25] J.-B. BOST, H. GILLET, C. SOULÉ, *Height of proyective varieties and positive Green forms,* J. Amer. Math. Soc. **7** (1994), pp. 903–1027.

[26] W. D. BROWNAWELL, *Bounds for the degrees in the Nullstellensatz,* Ann. of Math. **126** (1987), pp. 577-591.

[27] W. D. BROWNAWELL, D. W. MASSER, *Multiplicity estimates for analytic functions II,* Duke J. Math. **47** (1980), pp. 273–295.

[28] M. CABOARA, G. DE DOMINICIS, L. ROBBIANO, *Multigraded Hilbert Functions and Buchberger Algorithm,* In Y. N. Lakshman, ed., Proceedings ISSAC–96, ACM, 1996, pp. 72–78.

[29] L. CANIGLIA, A. GALLIGO, J. HEINTZ, *Some new effectivity bounds in computational geometry,* in T. Mora, ed., Proceedings AAECC–6, Lect. Notes in Comput. Sci. 357, Springer, 1989, pp. 131–151.

[30] L. CANIGLIA, A. GALLIGO, J. HEINTZ, *Borne simplemente exponentielle pour les degrés dans les théoremes des zéros sur un corps de charactéristique quelconte,* C. R. Acad. Sci. Paris **307** (1988), pp. 255–258.

[31] L. CANIGLIA, A. GALLIGO, J. HEINTZ, *Equations for the projective closure y effective Nullstellensatz,* Discrete Appl. Math. **33** (1991), pp. 11–23.

[32] J. CANNY, *Some algebraic and geometric computations in PSPACE,* Proc. 20th. Annual ACM Symposium on Theory of Computing (1988), pp. 460–467.

[33] J. CANNY, I. EMIRIS, *A subdivision-based algorithm for the sparse resultant,* Preprint, 1996.

[34] J. P. CARDINAL, *Dualité et algorithmes itératives pour la solution des systèmes polinomiaux,* Tesis, Université de Rennes I, France, 1993.

[35] D. CASTRO, *Sobre la complejidad de la aproximación diofántica y los fundamentos del análisis numérico,* Master's thesis, Universidad de Cantabria, Santander, Spain, 1997.

[36] M. CHARDIN, *Une majoration pour la fonction de Hilbert et ses conséquences pour l' interpolation algébrique,* Bull. Soc. Math. France **117** (1989), pp. 305–318.

[37] M. CHARDIN, P. PHILIPPON, *Régularité et interpolation,* Manuscrito, Univ. de Paris, 1997.

[38] M. CHARDIN, P. PHILIPPON, aparecerá en *Proc. du Coloque à CIRM,* 1998.

[39] A. L. CHISTOV, *Polynomial-time computation of the dimension of the components of algebraic varieties in zero-characteristic,* Manuscrito Université Paris Val de Marne.

[40] V. I. DANILOV, *The geometry of toric varieties,* Russian Math. Surveys **33** (1978), pp. 97–154.

[41] A. DICKENSTEIN, M. GIUSTI, N. FITCHAS, C. SESSA, *The membership problem for unmixed polynomial ideals is solvable in single exponential time,* Discrete and Applied Mathematics **33** (1991), pp. 73–94.

[42] T. W. DUBÉ, *A combinatorial proof of the effective Nullestellensatz,* J. Symb. Comp. **15** (1993), pp. 277–296.

[43] D. EISENBUD, *Commutative algebra with a view toward algebraic geometry,* Graduate texts in Math. 150, Springer–Verlag, 1995.

[44] M. ELKADI, *Bornes pour le degré et les hauteurs dans le problème de division,* Michigan Math. **40** (1993), pp. 609–618.

[45] G. EWALD, U. WESSELS, *On the ampleness of invertible sheaves in complete toric varieties,* Results Math. **25** (1991), pp. 275–278.

[46] G. FALTINGS, *Diophantine approximation on abelian varieties,* Ann. Math. **133** (1991), pp. 549–576.

[47] N. FITCHAS, *Algorithmic aspects of Suslin's solution of Serre's Conjeture,* Computational Complexity **33** (1993), pp. 31–55.

[48] N. FITCHAS, A. GALLIGO, *Nullstellensatz effectif et conjecture de Sèrre (théorème de Quillen-Suslin) pour le Calcul Formel,* Math. Nachr. **149** (1990), pp. 231–253.

[49] N. FITCHAS, M. GIUSTI, F. SMIETANSKI, *Sur la complexité du théoreme des zéros,* en J. Gudat et. al., *Approximation and Optimization in the Caribbean II,* Proc. 2nd. Int. Conf. on Non-linear Optimization and Approximation, vol. 8 of *Approximation and Optimization,* pp. 247–329, Peter Lange Verlag, Frankfurt am Main, 1995.

[50] W. FULTON, *Introduction to intersection theory in algebraic geometry,* Expository Lectures from the CBMS Regional Conference held at George Mason Univ., 1984.

[51] W. FULTON, *Intersection theory,* Curso, Summer School, Cortona, 1980.

[52] W. FULTON, *Intersection theorems,* Conferencia, Forschungsinstitut Oberwolfach, 1981.

[53] W. FULTON, *Intersection theory,* Erg. Math., 3. Folge., 2. Bd., Springer–Verlag, 1984.

[54] W. FULTON, *Introduction to toric varieties,* Ann. Math. Studies **131**, Princeton Univ. Press, 1993.

[55] I. GELFAND, M. KAPRANOV, A. ZELEVINSKY, *Discriminants, resultants, and multidimensional determinants,* Birkhäuser, 1994.

[56] M. GIUSTI, K. HÄGELE, J. HEINTZ, J. L. MONTAÑA, J. E. MORAIS, L. M. PARDO, *Lower bounds for diophantine approximation,* J. Pure Appl. Algebra **117** & **118** (1997), pp. 277–317.

[57] M. GIUSTI, J. HEINTZ, *Algorithmes — disons rapides — pour la décomposition d' une varieté en composantes irréductibles et équidimensionelles,* en T. Mora y C. Traverso, eds., Proc. MEGA'90, Birkhäuser Progress in Math. **94** (1991), pp. 169–194.

[58] M. GIUSTI, J. HEINTZ, *La détermination des points isolés et de la dimension d' une varieté algebrique peut se faire en temps polynomial,* en D. Eisenbud y L. Robbiano, eds., Computational Algebraic Geometry and Commutative Algebra, Cambridge Univ. Press, (1993), pp. 216–256.

[59] M. GIUSTI, J. HEINTZ, J. E. MORAIS, J. MORGENSTERN, L. M. PARDO, *Straight–line programs in elimination theory,* J. Pure Appl. Algebra **124** (1998), pp. 101–146.

[60] M. GIUSTI, J. HEINTZ, J. E. MORAIS, L. M. PARDO, *When polynomial equation systems can be solved fast?,* en G. Cohen, M. Giusti y T. Mora, eds., Proceedings AAECC–11, Lect. Notes. Comput. Sci. **948**, pp. 205–231, Springer, Berlin, 1995.

[61] M. GIUSTI, J. HEINTZ, J. SABIA, *On the efficiency of effective Nullstellensätze,* Comput. Complexity **3** (1993), pp. 56–95.

[62] M. GREEN, *Restrictions of linear series to hyperplanes, y some results of Macaulay y Gotzmann. Algebraic curves y projective geometry* (Proceedings, Trento, 1988), Lect. Notes in Math. 1389, pp. 76–85, Springer–Verlag, 1989.

[63] K. HÄGELE, *Tesis (en preparación),* Univ. de Cantabria, 1998.

[64] K. HÄGELE, J. E. MORAIS, L. M. PARDO, M. SOMBRA, *On the intrinsic complexity of the arithmetic Nullstellensatz,* Preprint, 1998.

[65] J. HARRIS, *Algebraic geometry: a first course,* Graduate Texts in Math. 133, Springer, Berlin, 1992.

[66] R. HARTSHORNE, *Algebraic geometry,* Graduate Texts in Math. 52, Springer–Verlag, 1977.

[67] J. HEINTZ, *Definability bounds in algebraically closed fields and a note on the degree of in affine algebraic geometry,* Manuscrito, Univ. Zürich, 1977.

[68] J. HEINTZ, *Definability bounds of first order theories of algebraically closed fields,* en L. Budach, ed., Proc. Fundamentals of Comput. Theory FCT'79, Akademie–Verlag (1979), pp. 160–186.

[69] J. HEINTZ, *Definability and fast quantifier elimination in algebraically closed fields,* Theoret. Comput. Sci. **24** (1983), pp. 239-277.

[70] J. HEINTZ, M. SIEVEKING, *Lower bounds for polynomials with algebraic coefficients,* Theoret. Comput. Sci. **11**, pp. 321–330 (1980).

[71] J. HEINTZ, T. KRICK, S. PUDDU, J. SABIA, A. WAISSBEIN, *Deformation techniques for efficient polynomial equation solving,* aparecerá en *Proc. MEGA '98.*

[72] G. HERMANN, *Die Frage der endlich vielen Schritte in der Theorie de Polynomideale,* Math. Ann. **95** (1926), pp. 736–788.

[73] D. HILBERT, *Über die Theorie von algebraischen Formen,* Math. Ann. **36** (1890), pp. 473–534.

[74] D. HILBERT, *Über die vollen Invariantensysteme,* Math. Ann. **42** (1893), pp. 313–373.

[75] B. HUBER, B. STURMFELS, *A polyhedral method for solving sparse polynomial systems,* Math. Comp. **64** (1995), pp. 1541–1555.

[76] B. IVERSEN, *Noetherian Graded Modules I,* Manuscrito Math. Institut Aarhus Univ. **29** (1972).

[77] S. JI, J. KOLLÁR, B. SHIFFMAN, *A Global Lojasiewicz Inequality for Algebraic Varieties,* Trans. Amer. Math. Soc. **329** (1992), pp. 813–818.

[78] J.-P. JOUANOLOU, *Théorèmes de Bertini et applications,* Progress in Math. 42, Birkhäuser, 1983.

[79] P. KOIRAN, *Hilbert's Nullstellensatz is in the polynomial hierarchy,* J. Complexity **12** (1996).

[80] J. KOLLÁR, *Sharp effective Nullstellensatz,* J. Amer. Math. Soc. **1** (1988), pp. 963–975.

[81] J. KOLLÁR, *Effective Nullstellensatz for arbitrary ideals,* Manuscrito, Univ. of Utah, 1998.

[82] J. KÖNIG, *Einleitung in die allgemeine Theorie der algebraischen Grössen,* Leipzig (1903).

[83] T. KRICK, LOGAR, *Memberships problems, representation problems and the computation of the radical for one-dimensional ideals,* Efective Methods in Algebraic Geometry, (T. Mora, C. Traverso, Eds.), Progress in Math. **94**, Bikhäuser, 1991, pp. 203–216.

[84] T. KRICK, L. M. PARDO, *Un approche informatique pour l' approximation diophantienne,* C. R. Acad. Sci. Paris **318** (1994), pp. 407–412.

[85] T. KRICK, L. M. PARDO, *A computational method for diophantine approximation,* in L. González-Vega y T. Recio, eds., Algorithms in algebraic geometry and applications, Proceedings MEGA'94, Birkäuser Progress in Math. **143**, Bikhäuser, Basel, 1996, pp. 193–253.

[86] T. KRICK, J. SABIA, P. SOLERNÓ, *On intrinsic bounds in the Nullstellensatz,* AAECC Journal **8** (1997), pp. 125–134.

[87] L. KRONECKER, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen,* Crelle J. Reine Angew. Math. AAECC Journal **92** (1881–1882), pp. 1–122: Werke, Vol. II, Leipzig, Teubner, 1897, pp. 237–287.

[88] A. G. KUSHNIRENKO, *Newton polytopes and the Bézout theorem,* Functional Analysis and its Applications **10** (1976), pp. 82–83 (translated from Russian).

[89] E. KUNZ, *Kähler differentials,* Advances Lectures in Mathematics, Vieweg-Verlag, 1986.

[90] S. LANG, *Algebraic Number Theory,* Addison-Wesley, 1970.

[91] S. LANG, *Algebra (3rd. ed.),* Addison-Wesley, 1971.

[92] S. LANG, *Fundamentals of diophantine geometry,* Springer–Verlag, 1983.

[93] M. LAURENT, *Hauteur de matrices dínterpolation,* Approximations Diophantiennes et Nombres Transcendants (Luminy 1990) (P. Philippon, ed.), de Gruyter, Berlin, (1992), pp. 215–238.

[94] D. LAZARD, *Algèbre linéaire sur* $k[x_1, \ldots, x_n]$ *et élimination,* Bull. Soc. Math. France **105** (1977), pp. 165–190.

[95] D. H. LEHMER, *Factorization of certain cyclotomic functions,* Ann. of Math. **34** (1993), pp. 461–479.

[96] F. S. MACAULAY, *The algebraic Theory of modular systmems,* Cambridge Univ. Press, 1916.

[97] K. MALHER, *On some inequalities for polynomials in several variables,* J. London Math. Soc. **37** (1962), pp. 341–344.

[98] D. W. MASSER, G. WÜSTHOLZ, *Fields of large trascendence degree generated by values of elliptic functions,* Invent. Math. **72** (1971), pp. 407–463.

[99] G. MATERA, *Sobre la complejidad en espacio y tiempo de la eliminación geométrica,* Tesis, Univ. de Buenos Aires,1997.

[100] G. MATERA, J. M. TURULL, *The space complexity of elimination theory: Upper bounds,* Foundations of Comput. Math., Springer–Verlag (1997), pp. 267–276.

[101] H. MATSUMURA, *Commutative ring theory,* Cambridge Univ. Press, 1986.

[102] E. MAYR, *Membership in polynomial ideals over* $\mathbb{Q}$ *is exponential space complete,* Proceedings 6th. Annual Symposium on Theoretical Aspects of Computer Science, Springer Lectures Notes in Computer Science **349** (1989), pp. 400–406.

[103] E. MAYR, A. MEYER, *The complexity of the word problem for commutative semigroups,* Adv. Math. **46** (1982), pp. 305–329.

[104] C. MIYAZAKI, W. VOGEL, *Towards a theory of arithmetic degrees,* aparecerá en *Manuscripta Math.*.

[105] J. E. MORAIS SAN MIGUEL, *Resolución eficaz de sistemas de ecuaciones polinomiales,* Tesis, Univ. de Cantabria, 1997.

[106] Y. NESTERENKO, *Estimates for the order of zeros of functions of a certain class and applications in the theory of numbers,* Math. URSS Izvestija **11** (1977), pp. 239–270.

[107] Y. NESTERENKO, *Estimates for the characteristic function of a prime ideal,* Math. URSS Sbornik **51** (1985), pp. 9–32.

[108] J. NEWTON, *Geometria analytica,* 1680.

[109] L. M. PARDO, *How upper and lower bounds meet in elimination theory,* in G. Cohen, M. Giusti y T. Mora, eds., Proceedings AAECC–11, Lect. Notes. Comput. Sci. **948**, pp. 33–69, Springer, Berlin, 1995.

[110] L. M. PARDO, *Comunicación personal,* 1997.

[111] P. PHILIPPON, *Critères pour líndépendance algébrique,* Inst. Hautes Études Sci. Publ. Math. **64** (1986), pp. 5–52.

[112] P. PHILIPPON, *Dénominateurs dans le théorème des zeros de Hilbert,* Acta Arith. **58** (1990), pp. 1–25.

[113] P. PHILIPPON, *Sur des hauteurs alternatives, I,* Math. Ann. **289** (1991), pp. 255–283; *II,* Ann. Inst. Fourier **44** (1994), pp. 1043–1065; *III,* J. Math. Pures Appl. **74** (1995), pp. 345–365.

[114] M. PIERI, *Formule di coincidenza per le serie algebriche* ∞^n *di coppie di punti dello spazio a* n *dimensioni,* Rend. Circ. Mat. Palermo **5** (1891), pp. 252–268.

[115] G. REMOND, aparecerá en *Proc. du Coloque à CIRM,* 1998.

[116] J. M. ROJAS, *Toric generalized characteristic polynomials,* Preprint, 1997.

[117] J. M. ROJAS, *Toric laminations, sparse generalized characteristic polynomials, and a refinement of Hilbert's tenth problem,* Preprint, 1997.

[118] W. RUDIN, *Function theory in the unit ball of* $\mathbb{C}^n$, Grundlehren der matematischen Wissenchaften **241**, Springer–Verlag, 1980.

[119] J. SABIA, P. SOLERNÓ, *Bounds for traces in complete intersections y degrees in the Nullstellensatz,* AAECC Journal **6** (1995), pp. 353–376.

[120] J.–P. SÈRRE, *Algèbre locale-Multiplicités,* Lecture Notes in Math. Vol 11, Springer (1965).

[121] I. R. SHAFAREVICH, *Basic algebraic geometry,* Springer–Verlag, 1974.

[122] B. SHIFFMAN, *Degree bounds for the division problem in polynomial ideals,* Michigan Math. J. **36** (1989), pp. 163–171.

[123] M. SIEVEKING, *On the notion of degree end its applications to complexity theory by Strassen,* Manuscrito, Univ. Bielefeld, 1977.

[124] F. SMIETANSKI, *Quelques bornes effectives pour le théoreme des zeros avec parametres,* These, Univ. Nice–Sophia Antipolis, 1994.

[125] M. SOMBRA, *Bounds for the Hilbert function of polynomial ideals y for the degrees in the Nullstellensatz,* J. Pure Appl. Algebra **117 & 118** (1997), pp. 565–599.

[126] M. SOMBRA, *A sparse effective Nullstellensatz,* aparecerá en *Adv. Appl. Math.*.

[127] C. SOULÉ, *Géometrie dÁrakelov et nombres trascendants,* J. Arithmétiques de Luminy (17–21 Juillet 1989), Asterisque 198–200 (1991), pp. 355–371.

[128] V. STRASSEN, *Die Berechnugskomplexitat von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten,* Numer. Math. **20** (1973), pp. 238–251.

[129] B. STURMFELS, *Sparse elimination theory,* in D. Eisenbud y L. Robbiano, eds., Proceedings of the Cortona conference on computational algebraic geometry y commutative algebra, Symposia Matematica XXXIV, Ist. Naz. di Alta Matematica, Cambridge Univ. Press, 1993, pp. 377–396.

[130] B. STURMFELS, *Gröbner bases y convex polytopes,* Univ. Lect. Series **8**, Amer. Math. Soc., 1996.

[131] B. STURMFELS, N. V. TRUNG, W. VOGEL, *Bounds on degrees of projective schemes,* Math. Ann. **302** (1995), pp. 417–432.

[132] B. TEISSIER, *Résultats récents dálgèbre commutative effective,* Sém. Bourbaki 718, Astérisque 189–190, pp. 107–131, Soc. Math. France, 1991.

[133] C. TRAVERSO, *Hilbert Functions and the Buchberger Algorithm,* J. Symbolic Comp. **22** (1996), pp. 355–376.

[134] W. VASCONCELOS, *The degrees of graded modules,* Notas de Curso, Summer School on Commutative Algebra, Centre de Recerca Matematica, Bellaterra, España, 1996.

[135] J. VERSCHELDE, P. VERLINDEN, R. COOLS, *Homotopies exploiting Newton polytopes for solving sparse polynomial systems,* SIAM J. Numer. Anal. **31** (1994), pp. 915–930.

[136] W. VOGEL, *Lectures on results on Bézout theorem,* Tata Lect. Notes **74**, Springer, Berlin, 1984.

[137] A. WEIL, *Number theory and algebraic geometry,* Proc. Int. Math. Congress, vol. II, Cambridge, 1950, pp. 90–100.

[138] O. ZARISKI, *Algebraic surfaces,* Classics in Math., Springer, 1995.

[139] O. ZARISKI, P. SAMUEL, *Commutative algebra, 2 vols.,* Van Nostrand, New York, 1958, 1960.

[140] S. ZHANG, *Positive line bundles on arithmetic surfaces,* Ann. of Math. **136**, (1992), pp. 569–587.