Tesis

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

Martín Sombra

Director: Joos Heintz

Estimaciones para el Teorema de Ceros de Hilbert

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires 1998

A Luciana

Agradecimientos

En primer lugar, deseo expresar mi profundo agradecimiento hacia Joos Heintz. El apoyo recibido, junto con la libertad que me ha dado y la confianza que ha depositado en mí han sido fundamentales para la realización de este trabajo. Más importante aún, sin embargo, han sido las enseñanzas que me ha sabido transmitir a través de su propio ejemplo de honestidad y de pasión por la ciencia.

Mi formación científica y mi trabajo han tenido el aporte y la influencia de muchas personas con las cuales he tenido la oportunidad de colaborar o de discutir: M. Almeida, B. Castaño, M. Chardin, A. Di Scala, A. Dickenstein, A. Dubson, M. Giusti, K. Hägele, T. Krick, G. Matera, J. E. Morais, G. Oleaga, L. M. Pardo, P. Philippon, G. Piñeiro, R. Sendra, P. Solernó y B. Sturmfels.

Agradezco al personal de los Departamentos de Matemática de la Universidad Nacional de La Plata y de la Universidad de Buenos Aires por haber contribuido a crear un ambiente favorable para mi trabajo. De la misma manera, agradezco al personal del Laboratoire GAGE, École Polytechnique, París, Francia, del Departamento de Matemáticas, Universidad de Alcalá, Alcalá de Henares, España, y del Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Santander, España, por su hospitalidad durante diversas estadías cortas que he realizado.

Esta tesis fue parcialmente financiada por el CONICET, la Universidad Nacional de La Plata, la Universidad de Buenos Aires y la Fundación Antorchas, a través de distintos subsidios para la investigación.

Quiero agradecer además a aquellas personas que forman parte de mi vida cotidiana y afectiva. Todos ellos han contribuido positivamente, de una forma o de otra, a la realización de este trabajo.

A mis amigos, por la sana camaradería y el apoyo recibido a lo largo de estos años.

A mis padres y a mis hermanos, mi familia, por su amor y comprensión, y por su apoyo incondicional.

Y finalmente a Luciana, quien ha tipeado esta memoria y — por sobre todo — me ha acompañado a lo largo de este tiempo. A ella está dedicada esta tesis.

Índice General

Estimaciones para el Teorema de Ceros de Hilbert

Resumen

Se introduce una nueva noción de altura de variedades afines. Esta noción extiende al caso de una variedad arbitraria la noción de altura de Weil de una variedad de dimensión 0 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 en el teorema de ceros de Hilbert. Se aplica la noción de altura de variedades para obtener nuevas cotas para el grado y para la altura de los polinomios en el teorema de ceros. Se obtiene además la primera versión rala del teorema de ceros afín. En todos los caso que se consideran, las cotas obtenidas son esencialmente óptimas.

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

Palabras clave: altura de variedades, desigualdad de Bézout aritmética, eliminación, teorema de ceros, función de Hilbert.

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 approximation of positive–dimensional varieties.

Key words: height of varieties, arithmetic Bézout's inequality, elimination, Nullstellensatz, Hilbert function.

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, su enunciado es el siguiente:

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

$$f_1(x) = 0, \ldots, f_s(x) = 0 \tag{0.1}$$

no tiene soluciones 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 de Bézout

$$1 = g_1 f_1 + \cdots + g_s f_s. \tag{0.2}$$

Este resultado es una de las piedras angulares de la geometría algebraica. Establece un estrecho vínculo entre un objeto geométrico — el conjunto solución del sistema de ecuaciones 0.1 — y un aspecto algebraico — la pertenencia del 1 al ideal generado por $f_1, \ldots, f_s$.

Este es un enunciado meramente existencial que no brinda ningún tipo de información sobre los polinomios $g_1, \ldots, g_s$. Sin embargo, es crucial para las aplicaciones disponer de estimaciones para — por ejemplo — el grado y el tamaño bit de los coeficientes de los polinomios que aparecen en la identidad 0.2. Esto es particularmente importante en las aplicaciones 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 otros problemas relacionados, como ser estimaciones globales para la función de Hilbert de ideales homogéneos.

Nuestro esfuerzo está principalmente dirigido hacia el estudio de los aspectos *aritméticos* de estos problemas. Con este fin introducimos una noción de *altura* para variedades aritméticas de dimensión positiva. Este concepto es el análogo aritmético de la noción clásica de grado de una variedad, y juega un rol central en nuestro tratamiento del teorema de ceros aritmético. Estudiamos las propiedades básicas de esta noción de altura, en particular su comportamiento con respecto a intersecciones.

Los aspectos aritméticos de los sistemas de ecuaciones polinomiales constituyen una de las motivaciones históricas de la geometría algebraica. Además existe actualmente un fuerte interés por estas cuestiones, debido a sus eventuales aplicaciones a la informática. Como un objetivo de mayor alcance, nos proponemos introducir nuevas técnicas y herramientas que contribuyan a entender y eventualmente a resolver los problemas aritméticos en álgebra conmutativa y en geometría algebraica.

En lo que sigue hacemos una introducción a los problemas que consideramos, junto con un resumen de los resultados presentados en esta memoria.

Grado y Altura de Variedades. Teorema de Bézout

Un problema clásico de geometría algebraica es el enunciado conocido como teorema de Bézout. Este 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 [105] 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. Finalmente, Bézout fue capaz de mostrar que la cantidad de puntos — contados con propiedad — en la intersección de dos curvas planas de grados d y e respectivamente, es exactamente $d \cdot e$, 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. El teorema de Bézout dice entonces

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

donde $i(C, D, \xi)$ es un entero positivo, la *multiplicidad de intersección*, que mide el orden de contacto entre C y D en el punto ξ. Notamos además que Bézout probó en 1764 la versión n–dimensional de este resultado, es decir, el caso de n hipersuperficies en $\mathbb{P}^n$ que se intersectan en una cantidad finita de puntos [18], [19], [20], [21].

Se plantea entonces el problema de extender el teorema de Bézout al caso general. El obstáculo principal consiste en definir en forma adecuada las nociones de grado y de multiplicidad de intersección.

En 1958, Sèrre [116] introdujo una definición de multiplicidad de intersección que le permitió a Iversen [74] demostrar el teorema de Bézout en el caso en que la intersección es propia, es decir, cuando $\dim V \cap W = \dim V + \dim W - n$ para $V, W \subseteq \mathbb{P}^n$. El teorema clásico de Bézout es un caso particular de este enunciado.

Surge entonces como un problema natural el extender esta identidad al caso en que la intersección no sea propia. El primer resultado general en este sentido tiene la forma de una desigualdad. El enunciado es el siguiente: sean $V, W \subseteq \mathbb{A}^n$ variedades afines. Entonces

$$\deg V \cap W \le \deg V \cdot \deg W.$$

Aquí el grado $\deg V$ 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 una 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

$$\deg V = \sum_i \deg V_i$$

donde $V = \cup_i V_i$ es la descomposición de V en componentes irreducibles.

En esta desigualdad de Bézout no se consideran multiplicidades de intersección. Como contrapartida tiene la ventaja de ser válida sin hipótesis adicionales sobre el tipo de intersección. Esto la convierte en una herramienta versátil en las aplicaciones de la geometría algebraica a otros campos, por ejemplo, a la teoría de números o al cálculo simbólico.

Este enunciado fue demostrado por primera vez en 1977 por Heintz [65] y por Sieveking [119], y publicado en [66], [67]. Más tarde fue demostrado también por Fulton, Lazarsfeld y MacPherson [49], [50] y publicado en [53]. La desigualdad de Bézout fue posteriormente generalizada y refinada en el contexto de ciclos algebraicos por Fulton y MacPherson [51] y por Vogel [131].

El propósito de la primera parte de esta memoria consiste en la formulación y el estudio de la noción de *altura* de variedades. Este concepto es el análogo aritmético de la noción de grado.

Sea k un cuerpo con fórmula del producto. El ejemplo básico es $\mathbb{Q}$, o más generalmente un cuerpo de números. Otro ejemplo de cuerpo con fórmula del producto es el cuerpo de funciones racionales de una variedad no–singular en codimensión 1.

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

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

donde M_k denota un conjunto propio de valores absolutos sobre k que verifica la fórmula del producto con multiplicidades λ_v, y S_k denota el conjunto de valores absolutos arquimedianos de M_k. Para $v \in S_k$, σ_v denota la inclusión correspondiente de k en $\mathbb{C}$, y M denota 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 $V = \cup_i V_i$ es la descomposición de V en componentes irreducibles. La altura de una variedad es un número no–negativo.

Esta noción extiende al caso general las nociones de altura de una hipersupeficie y de altura de Weil de una variedad de dimensión 0. Sea $f = \sum_i a_i x^i \in \mathbb{Z}[x_1, \ldots, x_n]$ un polinomio separable y primitivo que define una hipersuperficie $V(f) \subseteq \mathbb{A}^n(\mathbb{C})$. Se tiene entonces

$$-4\,(n+1)\log(n+1)\deg f \leq h(V(f)) - h(f) \leq 4\,(n+1)\log(n+1)\deg f$$

donde $h(f) := \log(\max_i |a_i|)$ denota la altura logarítmica de f. En el caso en que $V \subseteq \mathbb{A}^n(\mathbb{C})$ es una $\overline{\mathbb{Q}}$–variedad de dimensión 0 se tiene

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

donde $w(V)$ denota la altura de Weil de V.

La estrecha relación entre la altura de la forma de Chow de una variedad irreducible y sus propiedades aritméticas fue notada por Weil [132]. La definición de altura de una variedad a través de su forma Chow fue introducida y estudiada por Nesterenko [103] y Philippon [108], [110] en el contexto de la teoría de números trascendentes, en relación con los criterios para la independencia algebraica. La definición de altura de una variedad irreducible que consideramos en esta memoria fue introducida por Philippon [108], [110] para el caso en que k es un cuerpo de números.

Extendemos esta definición al caso de variedades reducibles siguiendo la definición de grado de Heintz, es decir, no consideramos multiplicidades de intersección. La teoría de intersección que resulta es menos general que la de Fulton–MacPherson [51] y la de Vogel [131]. Sin embargo, tiene la ventaja de ser más simple y manejable, y resulta suficiente para la mayoría de las aplicaciones.

Por otra parte, en el contexto de la teoría de intersección aritmética — o teoría de Arakelov — se ha considerado desde hace algún tiempo otra noción de altura de variedades aritméticas irreducibles. Esta noción fue introducida por Faltings en su trabajo sobre aproximación diofántica en variedades abelianas [45] y luego retomada por Bost, Gillet y Soulé [24], [25]. Soulé [124] y Philippon [110] probaron que esta noción de altura es equivalente en un sentido preciso a la noción de altura que consideramos en esta memoria.

Existe otra noción de altura de variedades aritméticas $V \subseteq \mathbb{A}^n(\mathbb{C})$ que ha devenido usual en teoría de eliminación computacional. Esta noción fue introducida por Giusti et al. [54] y retomada, por ejemplo, en [62], [61]. A grandes resgos, consiste en lo siguiente: sea $V \subseteq \mathbb{A}^n(\mathbb{C})$ una $\mathbb{Q}$–variedad equidimensional de dimensión r, y sea $\pi : V \to \mathbb{A}^{r+1}$ una proyección lineal. Es bien conocido que si π satisface ciertas condiciones de genericidad entonces $\overline{\pi(V)} \subseteq \mathbb{A}^{r+1}$ es una hipersuperficie birracional a V. Luego la inversa $\pi^{-1} : \overline{\pi(V)} \to V$ puede considerarse como una forma débil de parametrización de la variedad V. Esta parametrización π^{-1} se llama una *solución geométrica* de V.

Luego se define la *altura* $\eta(V)$ de V como la altura logarítmica de π^{-1}, es decir, la máxima longitud bit de sus coeficientes. La indeterminación proveniente de la elección de la proyección π se resuelve mediante una elección adecuada. Referimos a la subsección 1.3.4 para la definición precisa y para una discusión más amplia de estas cuestiones.

La noción de solución geométrica es la forma de representar variedades algebraicas propuesta por Kronecker [85] en su memoria de 1882. Esta noción fue descripta también por König [80], Macaulay [94] y Zariski [133], entre otros. Esto fue notado recientemente por

Pardo [61]. Entre las distintas representaciones de variedades, la idea de Kronecker ha resultado ser la más eficiente en teoría de eliminación computacional, desde el punto de vista de la complejidad en tiempo y espacio de memoria de los algoritmos [55], [56], [48], [83], [57], [54], [97], [102], [62], [61], [69].

La altura $\eta(V)$ acota la longitud bit de los enteros que intervienen en los algoritmos de eliminación. Por lo tanto, juega un rol importante en el estudio de la complejidad de estos algoritmos.

Esta noción de altura es *polinomialmente* equivalente a la altura h. Obtenemos las siguientes estimaciones (Teorema 1.3.23):

$$\eta(V) \leq c_1\,\delta^4 h(V) + c_2\,\delta^6, \qquad h(V) \leq c_3\,\delta^{12}\,\eta(V) + c_4\,\delta^{13},$$

donde c_1, c_2, c_3, c_4 dependen polinomialmente de n.

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 (Proposición 1.4.3) y el comportamiento de la altura de una variedad con respecto a morfismos (Lema 1.4.6). Obtenemos además una estimación para la altura de la inversa de un morfismo birracional $\varphi : V \to \mathbb{A}^r$ (Proposiciones 1.4.7 y 1.4.8).

Un aspecto crucial es el comportamiento de la altura con respecto a intersecciones. En este sentido obtenemos la siguiente *desigualdad de Bézout aritmética* (Teorema 1.4.4):

Teorema 1 *Sean $V_1, \ldots, V_l \subseteq \mathbb{A}^n$ variedades. Sea δ_i el grado de V_i y sea $\delta := \prod_i \delta_i$. Entonces*

$$h(V_1 \cap \cdots \cap V_l) \leq c_1\,\delta^8 \sum_i h(V_i) + c_2\,\delta^9.$$

Aquí c_1, c_2 dependen polinomialmente de n.

Por otra parte, tanto Bost–Gillet–Soulé [24] como Philippon [110] 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 enunciado es el siguiente: sean $V, W \subseteq \mathbb{P}^n(\mathbb{C})$ variedades aritméticas. Entonces

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

Esta estimación es mucho más precisa que cualquier resultado contenido en esta memoria. El interés principal de nuestra desigualdad de Bézout radica en la extensión al caso de característica positiva. Resultados similares han sido recientemente obtenidos en forma independiente del autor por Chardin y Philippon [37].

Casos particulares del teorema de Bézout aritmético fueron obtenidos anteriormente por Philippon [108], Faltings [45] y Krick y Pardo [83]. Otros aspectos de la teoría de altura de variedades fueron considerados en los trabajos [91], [135], [111].

Nuestra demostración de la desigualdad de Bézout aritmética es completamente algebraica. La idea central consiste en la aplicación formal del método de Newton–Hensel para la aproximación de raíces de funciones. Esta idea fue aplicada por primera vez en el contexto de la teoría de eliminación algorítmica por Giusti et al. en [57] y continuada en [54], [69]. A grandes rasgos, consiste en lo siguiente: sea $\varphi : V \to \mathbb{A}^r$ un morfismo finito y sea $p \in \mathbb{A}^r$ un punto no ramificado de φ. Luego aproximamos la inversa local de φ en un punto $\xi \in \varphi^{-1}(p)$ hasta un nivel suficiente como para recuperar, en un sentido preciso, la variedad V.

Esta idea es conceptualmente simple y potente a la vez. Permite obtener propiedades de variedades de dimensión positiva a partir del estudio de una fibra 0-dimensional.

En particular obtenemos una cota para la altura de una variedad intersección completa en términos de la altura de la fibra 0–dimensional de un punto no ramificado con respecto a una proyección lineal (Teorema 1.3.14). Este resultado es la parte técnica central de nuestra demostración de la desigualdad de Bézout, y es probablemente — en cuanto a la teoría de altura de variedades — el aporte original más relevante de esta memoria.

Teorema de Ceros. Historia

Sea $\mathbb{Q}[x_1, \dots, x_n]$ el anillo de polinomios n–variados con coeficientes racionales y sea I un ideal de $\mathbb{Q}[x_1, \dots, x_n]$. El célebre Teorema de la Base o Bassatz de Hilbert [71] dice entonces que existen polinomios $f_1, \dots, f_s \in \mathbb{Q}[x_1, \dots, x_n]$ tales que $I = (f_1, \dots, f_s)$, o en términos modernos, que el anillo $\mathbb{Q}[x_1, \dots, x_n]$ es Noetheriano.

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

En este sentido, un problema básico que se plantea — y tal vez el más inmediato — es el *problema de la pertenencia*: dados polinomios $g, f_1, \dots, f_s \in \mathbb{Q}[x_1, \dots, x_n]$, decidir si g pertenece o no al ideal generado por $f_1, \dots, f_s$. Estrechamente ligado a este, está el *problema de la representación*, que consiste en encontrar efectivamente $g_1, \dots, g_s \in \mathbb{Q}[x_1, \dots, x_n]$ tales que

$$g = g_1\, f_1 + \cdots + g_s\, f_s \tag{0.3}$$

en el caso en que $g \in (f_1, \dots, f_s)$.

Notamos que una cota para los grados de $g, \dots, g_s$ permite, dados $g_1, f_1, \dots, f_s$, decidir si la ecuación 0.3 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 $\mathbb{Q}$–lineales. Luego el problema de la efectividad se tradujo en una primera etapa en el problema de acotar los grados de los polinomios $g_1, \dots, g_s$.

Este problema fue resuelto por Hermann [70], quien fuera una alumna de Emmy Noether. Sea k un cuerpo y sean $g, f_1, \dots, f_s$ polinomios en $k[x_1, \dots, x_n]$. Sea $d := \max_i \deg f_i$. Hermann probó entonces que $g \in (f_1, \dots, f_s)$ si y sólo si existen $g_1, \dots, g_s$ tales que

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

con $\deg g_i\, f_i \le \deg g + 2\,(1 + d^2 + \cdots + d^{2^{n-1}})$.

Durante mucho tiempo se trató de mejorar esta cota, hasta que Mayr y Meyer [101], [100] probaron que es esencialmente óptima, es decir, que las cotas de grado para este problema tienen un carácter intrínseco doblemente exponencial.

En el caso particular $g = 1$, se tiene $g \in (f_1, \dots, f_s)$ si y sólo si los polinomios $f_1, \dots, f_s$ no tienen ceros comunes en $\mathbb{A}^n$. Este enunciado se conoce como el teorema de ceros de Hilbert [72], aunque probablemente fuera conocido previamente por Kronecker. Este caso particular del problema de la pertenencia está entonces en estrecha relación con el *problema de la consistencia*, que consiste en decidir si la variedad afín definida por $f_1, \dots, f_s$ es vacía o no. El teorema de ceros dice que esto pasa si y sólo si existen polinomios $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ que satisfacen la identidad de Bézout

$$1 = g_1 f_1 + \cdots + g_s f_s. \tag{0.4}$$

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 $\deg g_i f_i \le 3n^2 d^n$ para el caso $\operatorname{char}(k) = 0$, y por Caniglia, Galligo y Heintz [29], quienes obtuvieron la cota $\deg g_i f_i \le d^{n^2}$ para el caso $\operatorname{char}(k) > 0$.

Estos resultados fueron mejorados por Kollár [78] y por Fitchas y Galligo [47], quienes obtuvieron en forma independiente la estimación

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

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

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

En este caso es fácil ver para cualquier sistema de polinomios $g_1, \dots, g_n$ que verifica la identidad 0.1 se tiene $\deg g_1 \ge d^n$.

Como consecuencia de estos resultados se obtuvo que el teorema de ceros está en la clase de complejidad PSPACE [32], [97], [98]. Además, Koiran probó recientemente que el teorema de ceros está en la clase Π_2, si se asume la Hipótesis de Riemann Generalizada [77]. Esto contrasta fuertemente con el comportamiento del problema de la pertenencia en el caso general, que — por los resultados de Mayr y Meyer — es un problema completo en la clase EXPSPACE [101], [100].

Estas versiones efectivas del teorema de ceros tienen como consecuencia que una amplia serie de problemas de geometría algebraica computacional tienen complejidad simplemente exponencial: cálculo de la dimensión y del grado de una variedad [55], pertenencia al radical [40], descomposición de una variedad en componentes equidimensionales [56] y versiones algorítmicas del teorema de Quillen–Suslin [47], [46].

El teorema de ceros es un resultado básico en geometría algebraica. Sus diferentes versiones efectivas se aplican además en una variedad de situaciones: lemas de Gelfond multivariados, desigualdades de Lojasiewicz, [75], [121], consistencia sobre cuerpos primos de característica positiva, [62], [61], etc.. Se pueden encontrar otros resultados en los papers

[4], [12], [109], [115], [118] por nombrar sólo unas pocas referencias. Referimos además a los surveys [11], [106], [128] 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 para los grados de los polinomios en el teorema de ceros. Obtenemos distintos progresos sobre todas las cotas conocidas.

En primer lugar, consideramos el teorema de ceros efectivo en su forma clásica. Sea $d_i := \deg f_i$ y supongamos que se tiene $d_1 \ge \cdots \ge d_s$. Obtenemos la cota de grado (Teorema 2.1.10):

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

Esta cota es particularmente interesante en el caso en que los polinomios $f_1, \dots, f_s$ son cuadráticos. La mejor cota previa para este caso es $\deg g_i f_i \le n\, 2^{n+2}$, debida a Sabia y Solernó [115]. Nuestra estimación mejora esta cota a $\deg g_i f_i \le 2^{n+1}$, 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–Lazard–Masser–Philippon–Kollár. Sin embargo se ha observado que hay muchas instancias particulares en las cuales esta cota puede ser mejorada. Este hecho ha motivado la introducción de nuevos parámetros que permiten diferenciar familias especiales de sistemas de ecuaciones cuyo comportamiento con respecto al problema en cuestión es polinomial en lugar de exponencial [58], [57].

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 $f_1, \dots, f_s$. Es el análogo algebraico de la noción de grado geométrico de un sistema de ecuaciones introducida por Giusti et al. [57], y retomada por Krick, Sabia y Solernó [84] y por el autor [122]. Referimos a la sección 2.1.2 para la definición precisa de estas nociones.

Se han obtenido previamente distintas cotas de grado para los polinomios en el teorema de ceros que dependen principalmente del grado geométrico (Nullstellensätze intrínsecos) [54], [57], [84], [122]. Mostramos aquí que vale una cota similar reemplazando el grado geométrico del sistema de ecuaciones dado por su grado algebraico (Teorema 2.1.15). Sean $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ polinomios sin ceros comunes en $\mathbb{A}^n$. Sea $d := \max_i \deg f_i$ y sea δ el grado algebraico de este sistema de ecuaciones. Obtenemos entonces la estimación

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

Se tiene $\delta \le d^{n-1}$ por el teorema de Bézout, y por lo tanto deducimos de lo anterior

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

es decir, recuperamos esencialmente las cotas conocidas en términos de d y n. Por otra parte, el grado algebraico está acotado por el grado geométrico, y por lo tanto también recuperamos así las cotas conocidas en términos del grado geométrico. Luego este resultado contiene a todas las cotas de grado conocidas anteriormente.

Sin embargo, el grado algebraico 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 2.1.1). Concluimos entonces que el resultado obtenido es mucho más preciso en estos casos que las cotas conocidas.

Teorema de Ceros. Cotas de Esparsitud

Luego consideramos las cotas de esparsitud en el teorema de ceros.

Para un polinomio de Laurent $f = \sum_{i \in \mathbb{Z}^n} a_i x^i \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$, su *soporte* está definido como el conjunto $\{i : a_i \neq 0\}$, es decir, 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 $f_1, \dots, f_s$. 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 de la estructura monomial de un polinomio más precisa que el grado. En particular, se pueden obtener cotas para los grados a partir de cotas para el polítopo de Newton.

El concepto de polítopo de Newton fue introducido por Bernshtein [16] y Kushnirenko [86] con el objeto de obtener versiones más refinadas del teorema de Bézout, y está hoy en día en la base de la teoría de eliminación rala. Dentro de esta teoría se diseñan algoritmos que explotan 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 [125] y seguido, por ejemplo, en [33], [73], [112], [113], [130] por nombrar sólo unas pocas referencias.

El aspecto ralo en el teorema de ceros fue también considerado por Canny y Emiris, quienes obtuvieron un teorema de ceros ralo 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 se restringe el soporte de cada f_i a un conjunto fijo $\mathcal{A}_i$ — restringiendo así los monomios que pueden intervenir — 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 existan raíces a distancia tórica infinita. Notamos que en el caso en que esta hipótesis de genericidad se verifica, el resultado de Canny–Emiris es al menos tan preciso como cualquier resultado obtenido en esta memoria.

El problema de estimar las cotas para la esparsitud en el teorema de ceros ha permanecido abierto durante mucho tiempo. Obtuvimos el primer teorema de ceros ralo efectivo en [123]. Enunciamos este resultado en dos versiones (Teoremas 2.2.1 y 2.2.3).

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

Obtenemos un resultado análogo para el caso de un sistema 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 $a \in n^{2n+3}\,\mathcal{U}^2 \cdot \mathcal{N}$ *y* $\mathcal{N}(g_i f_i) \subseteq n^{2n+3}\,\mathcal{U}^2 \cdot \mathcal{N} - a$ *para* $i = 1, \dots, s$.

Sea $d := \max_i \deg f_i$. Derivamos directamente del teorema 2 la cota de grado

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

En el peor caso se obtiene la cota $\deg g_i f_i \le n^{n+2}\, d^{n+1}$, ya que el volumen no mezclado de los polinomios $x_1, \dots, x_n, f_1, \dots, f_n$ está 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 ralo y $d \ge n$ (Ejemplo 2.2.1).

La demostración de ambos resultados es similar. El primer paso consiste en 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 teorema de ceros efectivo para formas lineales en un anillo graduado Cohen–Macaulay (Lema Principal 2.1.1). Este lema se demuestra por medio de un argumento combinatorio. Consiste esencialmente en un método de deformación que permite reducir el caso general al caso en que las ecuaciones se cortan en forma propia en el hiperplano $\{x_0 = 0\}$. Este caso se resuelve aplicando técnicas clásicas de eliminación. que es un caso mucho más simple que el caso general.

Como consecuencia se obtiene además un teorema de ceros efectivo sobre anillos graduados Cohen–Macaulay, que vale no sólo para formas lineales, sino también para elementos homogéneos de grado arbitrario (Teorema 2.1.8).

Teorema de Ceros. Cotas de Altura

Finalmente, consideramos el aspecto aritmético en el teorema de ceros, junto con algunas de sus consecuencias para la aproximación diofántica entre variedades de dimensión positiva.

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

$$a = g_1 \, f_1 + \cdots + g_s \, f_s. \tag{0.5}$$

Tratamos entonces el problema de estimar tanto los grados de los polinomios g_i como sus alturas, y la altura del entero a. Estas estimaciones son importantes en aproximación diofántica. Se aplican a los lemas de Gelfond multivariados y al problema de la consistencia sobre cuerpos primos de característica positiva [62], [61].

Sean d, h el máximo de los grados y de las alturas de los polinomios f_i, respectivamente. A partir de las cotas para los grados en el teorema de ceros, la ecuación 0.5 puede traducirse en un sistema de ecuaciones $\mathbb{Q}$–lineales. De esta forma se obtiene una cota del tipo $d^{n^2}h$ para la altura de los polinomios g_i y del entero a, por aplicación de la regla de Cramer.

Se conjeturó, sin embargo, que estas estimaciones podían ser esencialmente mejoradas. Este problema fue considerado primeramente por Berenstein e Yger [13], quienes obtuvieron

$$\deg g_i \leq d^{c\,n}, \qquad h(a), h(g_i) \leq \kappa(n) \, d^{8n+5} h,$$

donde c es una constante universal y $\kappa(n)$ sólo depende de n. Su demostración está fuertemente basada en técnicas de análisis complejo.

Un poco más tarde, Krick y Pardo [82], [83] obtuvieron las estimaciones

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

donde c_1, c_2 son constantes universales. De hecho, se pueden tomar $c_1, c_2 \leq 35$ [107]. Su demostración es completamente algebraica y se basa en técnicas de dualidad en álgebras de Gorenstein.

Posteriormente, Berenstein e Yger [15] mejoraron ligeramente estas cotas de altura y las extendieron al caso más general de un anillo diofántico [15]. Sin embargo, cabe señalar que la posibilidad de esta extensión ya era evidente a partir de los argumentos de Krick–Pardo.

Recientemente hemos obtenido, en colaboración con Hägele, Morais y Pardo, el análogo aritmético de los Nullstellensätze intrínsecos [62]. Este resultado está contenido en la tesis de Hägele [61].

El problema que nos proponemos consiste en estimar la altura de los polinomios en el teorema de ceros sobre una variedad. La situación es análoga a la del teorema 2.1.8, 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 2.3.2):

Teorema 4 *Sea* $F := \{F_{r+1}, \ldots, F_n\} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ *una intersección completa reducida que define una variedad* $V := V(F) \subseteq \mathbb{A}^n$ *de dimensión* r *y grado* δ.

Sean $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ *polinomios sin ceros comunes en* V. *Sean* $d := \max_i \deg f_i$ *y* $h := \max_i h(f_i)$, *y sean* $D \geq d, \deg F$ *y* $H \geq h, h(F)$.

Entonces existen $a \in \mathbb{Z} - \{0\}$ *y* $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ *tales que*

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

con $\deg g_i \leq 5\, n^2\, D\, d^{2\,r}\, \delta^2$ *y* $h(a),\, h(g_i) \leq c\, D^2 (d^r\, \delta)^{12} (H + h(V) + d^r\, \delta)\,.$

La constante c en este enunciado depende polinomialmente de n.

Obtenemos cotas similares para el caso en que $\mathbb{Z}$ se reemplaza por el anillo de polinomios $k[t_1, \ldots, t_m]$ (Teorema 2.3.2). Reobtenemos de esta manera el teorema de ceros paramétrico de Smietanski [120].

La demostración de este resultado se basa esencialmente en la teoría de dualidad para álgebras de Gorenstein y sigue las líneas de la demostración de Krick–Pardo [83]. Esta técnica ya fue empleada previamente en el contexto de los teoremas de ceros efectivos, por ejemplo, por [48], [115]. En nuestro caso, la desigualdad de Bézout aritmética cumple con respecto a las cotas de altura, el rol que cumple la desigualdad de Bézout clásica con respecto a las cotas para los grados.

La noción de altura de una variedad está en estrecha relación con sus aspectos métricos. Por ejemplo, si $V \subseteq \mathbb{A}^n(\mathbb{C})$ es una $\mathbb{Q}$–variedad de dimensión 0, entonces

$$\log ||V|| := \log(\max_{\xi \in V} ||\xi||) \leq h(V) + \log(n+1) \deg V$$

es decir, la altura acota la distancia de V al origen.

En este sentido, consideramos el siguiente problema: sean $V, W \subseteq \mathbb{A}^n$ $\mathbb{Q}$–variedades tales que $V \cap W = \emptyset$. Tratamos entonces el problema de acotar inferiormente la distancia entre V y W.

Para V, $W \subseteq \mathbb{A}^n$ variedades y $\alpha \in \mathbb{R}_{\geq 0}$, definimos la función *distancia* como

$$\mathrm{dist}_\alpha(V, W) := \inf\{||p - q|| : p \in V,\ q \in W,\ \ \log ||p||,\ \log ||q|| \leq \alpha\}.$$

El siguiente resultado es una consecuencia directa de nuestro teorema de ceros sobre variedades intersección completa:

Sean $V, W \subseteq \mathbb{A}^n(\mathbb{C})$ $\mathbb{Q}$–variedades tales que $V \cap W = \emptyset$. Sean r, s la dimensión de V y de W respectivamente. Sea δ el grado de V. Asumimos que V y W son variedades intersección completa reducida de polinomios $f := \{f_1, \ldots, f_{n-r}\}, g := \{g_1, \ldots, g_{n-s}\} \subseteq k[x_1, \ldots, x_n]$ respectivamente. Sean $d := \deg f$, $h := \overline{m}(f)$, $D := \deg g$ y $H := \overline{m}(g)$. Entonces

$$\log(\mathrm{dist}_\alpha(V, W)) \geq -c(n)\, d^2\, D^{12\,r+2}\, \delta^{12} (h + H + h(V) + D^r\, \delta + \log \alpha)$$

para $\alpha > 0$.

Casos particulares de este problema fueron considerados previamente por Giusti et al. [54].

Este resultado nos permite obtener la siguiente estimación para el caso general (Corolario 2.3.6). Sean $V, W \subseteq \mathbb{A}^n$ variedades equidimensionales tales que $v \cap W = \emptyset$. Sean r, s

la dimensión de V y de W respectivamente, y a sumimos que $r+s \geq n+1$. Se tiene entonces

$$\log(\mathrm{dist}_\alpha(V,W)) \geq -c(n)(\deg V)^{12\,s}\,(\deg W)^{12\,r}(h(V)+h(W)-\log\alpha).$$

Estos resultados parecen estar lejos aún de las cotas óptimas, y constituyen sólo un primer paso hacia la solución de este problema. En la sección 2.3.3 formulamos una conjetura para el caso general del teorema de ceros aritmético sobre variedades. Esta conjetura implica cotas inferiores optimales para la aproximación entre variedades de dimensión positiva. Resultados recientes de Kollár [79] muestran la validez de las cotas de grado propuestas y dan así sustento a nuestra conjetura.

Función de Hilbert. Cotas

Sea k un cuerpo. Para un ideal homogéneo I de $k[x_0,\ldots,x_n]$ denotamos por h_I su *función de Hilbert*, es decir

$$h_I : \mathbb{Z} \to \mathbb{Z}, \qquad\qquad m \mapsto \dim(k[x_0,\ldots,x_n]/I)_m.$$

Sea $p_I \in \mathbb{Q}[t]$ su polinomio de Hilbert, de forma tal que se tiene $h_I(m) = p_I(m)$ para valores grades de m.

Sea r la dimensión de I. Luego p_I es un polinomio de grado $r-1$ y su coeficiente principal es igual a $\deg I/(r-1)!$. Luego la función de Hilbert h_I se comporta asintóticamente como

$$h_I \sim (\deg I/(r-1)!)\, m^{r-1}.$$

Existen, sin embargo, situaciones en donde es importante disponer de estimaciones de $h_I(m)$ para valores pequeños de m.

Consideramos entonces el problema de estimar *globalmente* a h_I. Este problema fue primeramente considerado por Nesterenko [104], quien probó que para un ideal primo homogéneo P de $k[x_0,\ldots,x_n]$ de dimensión $r \geq 1$ se tiene

$$\tbinom{m+r}{r} - \tbinom{m-\deg P+r}{r} \leq h_P(m) \leq \deg P\,(4m)^{r-1}.$$

Más tarde, Chardin [35] simplificó la demostración de Nesterenko y mejoró su cota superior. Obtuvo la estimación

$$h_I(m) \leq \deg I\,\tbinom{m+r-1}{r-1}$$

para el caso de un cuerpo k perfecto y un ideal radical equidimensional homogéneo I de $k[x_0,\ldots,x_n]$ de dimensión $r \geq 1$.

En esta dirección, obtenemos una cota inferior para la función de Hilbert de un ideal polinomial homogéneo arbitrario de dimensión $r \geq 1$ (Teorema 3.1.2):

$$h_I(m) \geq \tbinom{m+r}{r} - \tbinom{m-\deg I+r}{r}.$$

Esta cota es óptima en términos de la dimensión y el grado del ideal I. Obtenemos además una cota superior para la función de Hilbert de la intersección — en el nivel de ideales — de un ideal $I \subseteq k[x_0, \ldots, x_n]$ homogéneo radical y equidimensional de dimensión $r \geq 2$ con un polinomio $f \in k[x_0, \ldots, x_n]$ (Teorema 3.2.8). Se tiene

$$h_{(I,f)}(m) \leq 3 \deg f \cdot \deg I \tbinom{m+r-2}{r-2}$$

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

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 [36] y con modificaciones del algoritmo de Buchberger [129], [28]. Se aplica además en teoría de números trascendentes, en el contexto de los lemas de ceros [17].

Capítulo 1

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 de altura de una variedad de dimensión positiva. Estudiamos sus propiedades básicas, sobre todo su comportamiento con respecto a morfismos lineales y a intersecciones.

En la sección 1.1 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 su altura local en cada primo de k.

En la sección 1.2 introducimos la noción de altura de una variedad como la altura global de su forma de Chow. Asimismo describimos su comportamiento con respecto a morfismos lineales y a intersecciones con hiperplanos.

La sección 1.3 constituye la parte central de este capítulo. Está fundamentalmente dedicada al estudio de la relación entre altura de una variedad y la altura de una fibra con respecto a una proyección finita (Teorema 1.3.14 y Proposición 1.3.9).

Finalmente, en la sección 1.4 obtenemos la desigualdad de Bézout aritmética (Teorema 1.4.4) y estimamos la altura de la inversa de un morfismo birracional.

1.1 Altura de Polinomios

Esta sección es esencialmente preliminar. Tiene como propósito introducir las nociones básicas de teoría de números que vamos a necesitar en las secciones siguientes y de fijar la notación. Todo el material incluído es perfectamente clásico. Nuestra presentación sigue los libros de Lang [90] y [88], el libro de Artin [6] y el trabajo de Philippon [108].

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

Luego introducimos la altura local de un polinomio, definiéndola en el caso arquimediano en base a la medida de Mahler. A partir de esta noción introducimos distintas definiciones de altura para un polinomio.

1.1.1 Valores Absolutos

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

1. Se tiene $|x| \geq 0$, y $|x| = 0$ si y sólo si $x = 0$.
2. $|x \cdot y| = |x| \cdot |y|$ 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 $\operatorname{char}(k) = p > 0$ se tiene $|x+y| = |(x+y)^{p^N}|^{1/p^N} \to \max\{|x|, |y|\}$, 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.

Sea k un cuerpo con un valor absoluto arquimediano v. Luego se tiene $\operatorname{char}(k) = 0$. La restricción de v a $\mathbb{Q}$ es entonces dependiente del valor absoluto ordinario [6, Sección 1.5]. Por lo tanto la completación 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 [89, Sección 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 se tiene

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

donde $N_k^{k(\alpha)}(\alpha)$ denota la *norma* de $\alpha \in k(\alpha)$ sobre k. Si además la extensión E es finita entonces E es completo cos respecto a este valor absoluto.

Sea ahora k un cuerpo con un valor absoluto no trivial v. Vamos a describir cómo se prolonga 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 de E en $\overline{k}_v$. Luego σ induce un valor absoluto w sobre E que extiende a v. Sea E_w la completación de E. Luego se tiene $E_w = E \cdot k_v$.

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 sobre 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 $w|v$. Luego se define 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 [90, Sección 2.1].

En particular, si M_k es propio, contiene entonces 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 está bien definido. Equivalentemente se tiene

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

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. Luego M_E es también un conjunto propio de valores absolutos.

Queremos ver que M_E satisface además la fórmula del producto con multiplicidades μ_w. 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 $n_w := [E_w : k_v]_s = [H_w : k_v]$. Este entero coincide con el grado local de E sobre k en w 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

$$\mu_w := \lambda_v [E_w : k_v]_s / [E : k]_s.$$

Sea $k \subseteq E \subseteq F$ una torre de extensiones. Sean $v \in M_k$, $w \in M_E$ 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.

Sea k un FP–cuerpo y sea E una extensión finita de k. En adelante vamos a asumir que las multiplicidades de M_k y de M_E están *normalizadas* de forma tal que se verifica $\sum_{v \in S_k} \lambda_v = 1$ y $\sum_{w|v} \mu_w = \lambda_v$.

1.1.2 Cuerpos de Números

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

El *valor absoluto p–ádico* $|\cdot|_p$ 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, Sección 1.5].

Si q es un primo de $\mathbb{Z}$ 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 $M_{\mathbb{Q}}$ 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 $M_{\mathbb{Q}}$ se llama el *conjunto canónico*. Luego M_k satisface la fórmula del producto con multiplicidades $\lambda_v := [k_v : \mathbb{Q}_p]$, para un valor absoluto $v \in M_k$ que extiende al valor absoluto p–ádico $|\cdot|_p$.

1.1.3 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 simple 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 entonces 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 la hipersuperficie W un valor absoluto no–arquimediano $|\cdot|_W$ definido como

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

para $f \neq 0$ y $|0|_W := 0$, donde $\deg W$ denota el *grado* de W, es decir, el número de puntos de la intersección de W con una variedad lineal genérica de dimensión complementaria. Referimos a la subsección 1.2.1 para una discusión más amplia de esta noción.

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*, gracias a la relación

$$\sum_W \mathrm{ord}_W f \cdot \deg W = 0$$

Para una demostración de este resultado referimos al libro de Hartshorne [64, II.6.4].

Esta fórmula del producto se puede escribir también como

$$\prod_W |f|_W = 1$$

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 como el conjunto de valores absolutos $|\cdot|_W$, donde W recorre un sistema de representantes de las clases de conjugación de 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.

1.1.4 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 $k[x_1, \dots, x_n]$. Definimos la *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

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

   para $P \neq 0$ y $M_v(0) := 0$. La función $\log|\sigma_v(P)|$ es integrable [114] 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 [93] para el caso de un polinomio univariado $P = a_d \prod_{i=1}^d (x - \alpha_i) \in \mathbb{C}[x]$ bajo la forma

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

La igualdad entre las dos expresiones de $M(P)$ se deduce de la fórmula de Jensen. El caso general fue introducido y estudiado por Mahler [95].

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

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

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* de P, 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* o *altura ordinaria* como $H_v(\mathcal{A}) := |\mathcal{A}|_v = \max_{a \in \mathcal{A}}\{|a|_v\}$, es decir, el máximo de los valores absolutos de los elementos de A. Asimismo consideramos su *altura (ordinaria) logarítmica* $h_v(\mathcal{A}) := \log H_v(\mathcal{A})$ y su *altura (ordinaria) 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

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

para $P = \sum_i a_i\, x^i \in \mathbb{C}[x_1, \ldots, x_n]$, y la *longitud logarítmica* $l(P) := \log L(P)$. Estas nociones están relacionadas [108], por las estimaciones

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

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

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

Análogamente, se tiene la estimación

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

Por otra parte, se tiene además, la relación siguiente entre la medida de Mahler y la altura ordinaria

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

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

Lema 1.1.1 *Sean $f \in k[t_1, \dots, t_m]$ y $g_1, \dots, g_m \in k[x_1, \dots, x_n]$. Sean $\deg g := \max_i \deg g_i$ y $\overline{m}_v(g) := \max_i \overline{m}_v(g_i)$. Sea $F \in k[x_1, \dots, x_n]$ el polinomio dado por la composición de f con $g_1, \dots, g_m$, es decir*

$$F := f(g_1, \dots, g_m).$$

Entonces

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

Demostración. Sean $d := \deg f$ y $D := \deg g$. Sean $i := (i_1, \dots, i_m) \in \mathbb{N}^m$ y $g := (g_1, \dots, g_m)$. 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

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

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

□

En particular, sea $f := \det(t_{ij}) \in k[(t_{ij})_{ij}]$ el determinante de la $m \times m$–matriz $(t_{ij})_{ij}$ y sean $g_{ij} \in k[x_1, \dots, x_n]$. Luego

$$\begin{aligned} m_v(F) &\leq m\,\overline{m}_v(g) + m(\deg g \, \log(n+1) + 3\log(m+1)), \qquad v \in S_k, \\ m_v(F) &\leq m\,\overline{m}_v(g), \qquad v \notin S_k, \end{aligned}$$

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

1.1.5 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 $k[x_1, \dots, x_n]$. 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 para el caso de un cuerpo de números [108, Definición 1.1.1].

Esta noción puede extenderse 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 en forma análoga $m(P) := \sum_w \mu_w \, m_w(P)$ para $P \in E[x_1, \ldots, x_n] - \{0\}$. Esta última expresión no depende del cuerpo de E, gracias a la normalización impuesta sobre las multiplicidades μ_w. 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 los 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 m. Esta noción de altura satisface además

$$m(P \cdot Q) = m(P) + m(Q)$$

para $P, Q \neq 0$, por la multiplicatividad de las alturas locales. Otra propiedad importante de m es su *positividad*, es decir $m(P) \geq 0$ [108, Proposición 1.12].

Se tiene $m(P) \leq \overline{m}(P)$ para todo P, y además existe $\lambda \in k^*$ tal que $m(P) = \overline{m}(\lambda P)$ [108].

Estas propiedades hacen conveniente el uso de la altura invariante como medida de un polinomio. 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

$$\begin{aligned} m(P) - \deg P - n &\leq h(P) \leq m(P) + \log(n+1) \deg P, \\ \overline{m}(P) - \deg P - n &\leq \overline{h}(P) \leq \overline{m}(P) + \log(n+1) \deg P. \end{aligned}$$

Una propiedad importante de las alturas absolutas es que acotan a las alturas locales, es decir

$$m_v(P) \leq \overline{m}(P), \qquad\qquad h_v(\mathcal{A}) \leq \overline{h}(\mathcal{A}),$$

para todo $v \in M_k$.

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 1.1.1 obtenemos

$$m(F) \leq m(f) + \deg f \cdot \overline{m}(g) + \deg f (\log(m+1) + \deg g \, \log(n+1)).$$

En lo que sigue vamos a necesitar algunos lemas técnicos. La siguiente es una estimación para la altura de la raíz de un polinomio univariado.

Lema 1.1.2 *Sea $p \in k[t]$ un polinomio de grado d, y sea $\xi \in \overline{k}$ una raíz de p. Entonces*

$$\overline{h}(\xi) \leq h(p) + \log d.$$

Demostración. Podemos suponer sin pérdida de generalidad que p es mónico. Sea $p = t^d + a_{d-1}\, t^{d-1} + \cdots + a_0 \in k[t]$ y sea $q := -a_{d-1}\, t^{d-1} - \cdots - a_0$. Luego

$$\xi^d = -(a_{d-1}\, \xi^{d-1} + \cdots + a_d) = q(\xi)$$

Consideramos primeramente el caso $v \in S_k$. Luego $|\xi|^d \leq \max\{1, |\xi|\}^{d-1}\, L(q)$ y por lo tanto

$$\overline{h}_v(\xi) \leq \overline{h}_v(q) + \log d$$

En el caso $v \notin S_k$ se tiene $\overline{h}_v(\xi) \leq \overline{h}_v(q)$ y por lo tanto

$$\overline{h}(\xi) \leq \overline{h}(q) + \log d = h(p) + \log d$$

ya que $\overline{h}_v(q) = h_v(p)$ para todo v. □

Para un polinomio $P \in k[t_1, \ldots, t_m][x_1, \ldots, x_n]$ se define por $\deg^{(t)} P$ y por $\deg^{(x)} P$ el grado de P en las variables $t_1, \ldots, t_m$ y $x_1, \ldots, x_n$ respectivamente.

El siguiente resultado muestra que existen puntos de baja altura que no anulan un polinomio dado.

Lema 1.1.3 *Sea $P \in k[t_1, \ldots, t_m][x_1, \ldots, x_n]$ un polinomio no nulo de grado d en las variables $t_1, \ldots, t_m$. Entonces existe $\xi \in k^m$ tal que $P(\xi, x) \neq 0$ y $\overline{h}(\xi) \leq d$.*

Demostración. Este resultado se sigue fácilmente tomando $\xi \in \mathbb{Z}^m$ en el caso $\mathrm{char}\,(k) = 0$ y $\xi \in \overline{\mathbb{F}}_p^n$ en el caso $\mathrm{char}\,(k) = p > 0$. Aquí $\overline{\mathbb{F}}_p^n$ denota la clausura algebraica del cuerpo primo $\mathbb{F}_p^n$. □

Supongamos que k es el cuerpo de fracciones de un anillo factorial A. Este es el caso, por ejemplo, si k es el cuerpo $\mathbb{Q}$ de los números racionales o el cuerpo de funciones racionales n–variadas $k_0(t_1, \ldots, t_m)$ sobre un cuerpo de constantes k_0 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, es decir, tal que sus coeficientes no tienen factores comunes. 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 $h(\mathcal{A}) = \log |\mathcal{A}| = \max_{a \in \mathcal{A}} |a|$ 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 $P \in k[t_1, \ldots, t_m][x_1, \ldots, x_n]$.

1.2 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. Esta noción nos permite definir la altura de una variedad como la altura de su forma de Chow.

1.2.1 Grado

En primer lugar introducimos la definición de grado de una variedad afín irreducible y luego la extendemos al caso general. Adoptamos el punto de vista de Heintz [67].

Sea k un cuerpo algebraicamente cerrado y sea $V \subseteq \mathbb{A}^n$ 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 [67]. Se tiene además

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

para todo $(G, b) \in \mathbb{A}^{rn} \times \mathbb{A}^r$ con fibra finita, y vale la igualdad para (G, b) en un abierto de $\mathbb{A}^{rn} \times \mathbb{A}^r$ [67].

Sea $V \subseteq \mathbb{A}^n$ una variedad irreducible de dimensión r. Luego el *grado* de V se define como

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

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 tiene $\deg V = 1$ 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 igual a 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* [67]. 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 de V y W. Con respecto al producto se tiene $\deg V \times W = \deg V \cdot \deg W$.

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

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

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 [68, Lema 1] y [115, Proposición 1].

Lema 1.2.1 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ un morfismo 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. Asumimos sin pérdida de generalidad que f_i y g_i no tienen factores comunes. Luego

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

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 por lo tanto $\deg \overline{\varphi(V)} \leq \deg \mathrm{Gr}(\varphi)$, de donde se deduce la cota anunciada. $\square$

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

Sea $q \in k(x_1, \ldots, x_n)$ una función racional, y sean f , $g \in k[x_1, \ldots, x_n]$ polinomios sin factores comunes tales que $q = f/g$. Luego definimos el *grado* de q como

$$\deg q := \max\{\deg f, \deg g\}.$$

Lema 1.2.2 *Sea* $V \subseteq \mathbb{A}^n$ *una variedad y sea* $\varphi : V \to \mathbb{A}^r$ *un morfismo birracional. Sea* $\psi := \varphi^{-1} = (\psi_1, \ldots, \psi_n)$ *la inversa de* φ *, con* $\psi_i \in k(y_1, \ldots, y_r)$ *. Sean* $f_i, g_i \in k[x_1, \ldots, x_n]$ *polinomios tales que* $\varphi = (f_1/g_1, \ldots, f_r/g_r)$ *. Sea* $d_i := \max\{\deg f_i, \deg g_i + 1\}$ *y supongamos que vale* $d_1 \geq \cdots \geq d_m$ *. Entonces*

$$\deg \psi_i \leq \deg V \prod_{i=1}^{r} d_i.$$

Demostración. Sea p_i , $q_i \in k[y_1, \ldots, y_r]$ polinomios sin factores comunes tales que $\psi_i = p_i/q_i$. Se tiene entonces

$$\overline{\mathrm{Gr}(\psi)} = \{q_1\, x_1 - p_1, \ldots, q_n\, x_n - p_n\} \subseteq \mathbb{A}^r \times \mathbb{A}^n$$

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

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

ya que el polinomio $q_i\, x_i - p_i$ 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 la variedad 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 reducible. El grado de una variedad afín $V \subseteq \mathbb{A}^n$ coincide entonces con el grado de su clausura proyectiva $\overline{V} \subseteq \mathbb{P}^n$.

Existen distintas definiciones alternativas del grado de una variedad proyectiva. Una de las más usuales es a través de la función de Hilbert, y permite extender la noción de grado al contexto de ideales. Introducimos ahora la noción de función de Hilbert. En el capítulo 3 hacemos un estudio de esta noción desde el punto de vista cuantitativo.

Sea S al anillo de polinomios $k[x_0, \ldots, x_n]$. Dado un S–módulo graduado M y un entero $m \in \mathbb{Z}$, denotamos por M_m la parte homogénea de M de grado m .

Sea I un ideal homogéneo de $k[x_0, \ldots, x_n]$. La *función de Hilbert* o *función característica* del ideal I se define como

$$h_I : \mathbb{Z} \to \mathbb{Z}, \qquad\qquad m \mapsto \dim_k(k[x_0, \ldots, x_n]/I)_m.$$

Sea $r + 1 := \dim I \geq 0$. Luego existe un polinomio $p_I = a_r\, t^r + \cdot + a_0 \in \mathbb{Q}[t]$ de grado r y $m_0 \in \mathbb{Z}$ tales que

$$h_I(m) = p_I(m) \qquad\qquad m \geq m_0.$$

El polinomio p_I es el *polinomio de Hilbert* del ideal I . Entonces el *grado* del ideal I se define entonces como

$$\deg I := r!\; a_r.$$

Sea $V \subseteq \mathbb{P}^n$ una variedad irreducible de dimensión r. Sea $k[V]$ su anillo de coordenadas homogéneas, es decir

$$k[V] := k[x_0, \ldots, x_n]/I(V)$$

donde $I(V) \subseteq k[x_0, \ldots, x_n]$ denota el ideal de definición de V. 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 $m \gg 0$. El término principal de este polinomio es igual a $\deg V/r!$, es decir, que la definición de grado vía función de Hilbert coincide con la definición usual de grado para el caso de una variedad irreducible. Esta última es una consecuencia del teorema de Bertini [76].

Estudiamos ahora la relación entre el grado de un ideal y el grado de la variedad que define. Introducimos previamente la noción de longitud de un ideal primario.

Sea P un ideal primo homogéneo de $k[x_0, \ldots, x_n]$ y sea Q un ideal P–primario. Luego se define la longitud $l(Q)$ de Q como la longitud de $(S/Q)_P$ como un S/P–módulo. Equivalentemente, $l(Q)$ es igual a la longitud de una cadena maximal de ideales P–primarios de la forma

$$P = Q_1 \supset \cdots \supset Q_l = Q.$$

Este número es finito, y se tiene $l(Q) = 1$ si y sólo si Q es primo.

Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo y sea $I = \cap_P Q_P$ una descomposición primaria minimal de I. Entonces se tiene

$$\deg I = \sum_P l(Q_P) \deg V(P)$$

donde la suma se hace sobre los primos asociados de I de dimensión igual a la dimensión de I [131, Proposición 1.49], [63, Proposición 13.6]. En particular, el grado de un ideal homogéneo sólo depende de su parte equidimensional de dimensión máxima.

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 [51].

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 *ruled join* de V y W, es decir, la variedad proyectiva asociada a la k–álgebra graduada $k[V] \otimes_k k[W]$. Luego $\dim V \# W = r + s + 1$ y se tiene

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

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

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

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

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

Posteriormente se han obtenido versiones más generales y refinadas de la desigualdad de Bézout que incluyen multiplicidades de intersección. Referimos a lo libros de Fulton [51] y Vogel [131] para los enunciados precisos de estos resultados.

1.2.2 Forma de Chow y Polinomio Característico

La idea básica de la construcción de Chow es la de parametrizar el conjunto de las variedades proyectivas. El punto en esta construcción consiste en asociar a toda variedad $V \subseteq \mathbb{P}^n$ una hipersuperficie Φ_V en un espacio proyectivo. En lo que sigue vamos a describir esta construcción. Seguimos en este punto el tratamiento de Shafarevich [117].

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.

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 $p \in H$ si y sólo si $U \cdot p = 0$ para $p \in \mathbb{P}^n$. Luego f_V se identifica con un polinomio en $r+1$ grupos de $n+1$ variables. Este polinomio es multihomogéneo de grado $\deg V$ en cada uno de estos grupos de variables [117].

Se tiene además que f_V es simétrico — salvo por $\pm$ — con respecto a permutaciones entre estos grupos de variables. Esto se deduce del hecho de que la hipersuperficie Φ_V es simétrica con respecto a estas permutaciones y por lo tanto

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

para algún $\tau_{ij} \in k^*$. Se tiene entonces $\tau_{ij}^2 = 1$, de donde $\tau_{ij} \pm 1$.

Sea $V = \cup_i V_i$ la descomposición de V en componentes irreducibles. Luego se tiene

$$f_V = \prod_i f_{V_i}.$$

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 $V = \mathbb{P}^n$ el polinomio f_V coincide con el determinante.

Sea $V \subseteq \mathbb{A}^n$ una variedad afín equidimensional de dimensión r. Definimos la *forma de Chow* f_V de V como la forma de Chow de su clausura proyectiva $\overline{V} \subseteq \mathbb{P}^n$.

Sean $H_1, \ldots, H_{r+1} \subseteq \mathbb{A}^n$ hiperplanos afines. 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. De hecho se tiene $f_V(H_1, \ldots, H_{r+1}) = 0$ si y sólo si $\overline{V} \cap H_1 \cap \cdots \cap H_{r+1} \neq \emptyset$.

Introducimos ahora la noción de polinomio característico de una variedad afín V. Esta noción es fundamental en nuestro tratamiento de la altura de una variedad. Este concepto es muy cercano a la noción de forma de Chow. A grandes rasgos describe la ecuación minimal de una forma lineal con respecto a una normalización de Noether genérica de la variedad V.

Sea $V \subseteq \mathbb{A}^n$ una variedad afín equidimensional. Consideramos a los espacios afines $\mathbb{A}^{(r+1)}$ y $\mathbb{A}^{(n+1)n}$ como las variedades de las $(r+1) \times 1$–matrices y de las $(r+1) \times n$–matrices con coeficientes en k, respectivamente. Consideramos el morfismo

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

para $b \in \mathbb{A}^{r+1}$, $G \in \mathbb{A}^{(r+1)n}$ y $x \in V$. Para $b \in \mathbb{A}^{r+1}$ y $G \in \mathbb{A}^{(r+1)n}$ fijos, el morfismo ϖ_V se corresponde con la proyección de V al subespacio afín de $\mathbb{A}^n$ determinado por b y G. Se tiene $\varpi_V^{-1}(b, G, \mathbb{A}^{r+1}) = V$ y por lo tanto

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

por el teorema de dimensión de fibras. Luego la clausura de la imagen de ϖ_V es una hipersuperficie $\Omega_V := \overline{\mathrm{Im}\ (\varpi_V)}$ de $\mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}$. El polinomio P_V que define esta hipersuperficie es único salvo por múltiplos escalares, y se llama el *polinomio característico* de la variedad V.

Sean $U := (U_{ij})_{ij}$ y $T := (T_k)$ una $(r+1) \times (n+1)$–matriz y una $(r+1) \times 1$–matriz formadas por variables U_{ij} y T_k respectivamente. Sean además

$$\eta_i := U_{i0} + U_{i1}x_1 + \cdots + U_{in}x_n$$

formas lineales *genéricas*. El morfismo

$$\varpi_V^* : k[\mathbb{A}^{(r+1)} \times \mathbb{A}^{(r+1)n} \times \mathbb{A}^{(r+1)}] \to k[\mathbb{A}^{(r+1)} \times \mathbb{A}^{(r+1)n} \times V]$$

está entonces definido por $U_{ij} \mapsto U_{ij}$ y $T_k \mapsto \eta_k$. El núcleo de este morfismo es un ideal principal y $P_V \in k[U, T]$ es un generador de este ideal.

La extensión $k(\mathbb{A}^{r(n+1)} \times \mathbb{A}^r) \hookrightarrow k(\mathbb{A}^{r(n+1)} \times V)$ definida por $U_{ij} \mapsto U_{ij}$ y $T_k \mapsto \eta_k$ para $i, k = 1, \ldots, r$ y $j = 0, \ldots, n$ es entera. En otros términos, la proyección genérica

$$V \to \mathbb{A}^r, \qquad\qquad x \mapsto (\eta_1(x), \ldots, \eta_r(x))$$

es una normalización de Noether de la variedad V.

Sean $E := k(\mathbb{A}^{r(n+1)} \times \mathbb{A}^r)$ y $F := k(\mathbb{A}^{r(n+1)} \times V)$. Luego F es una E–álgebra reducida de dimensión 0, y la extensión $E \hookrightarrow F$ es separable y finita de grado $\deg V$ [67].

Sean $E' := k(U_{r+1}) \otimes_k E$ y $F' := k(U_{r+1}) \otimes_k F$. Luego η_{r+1} es un elemento primitivo de F' sobre E', es decir

$$F' = E'[\eta_{r+1}].$$

Consideramos entonces la aplicación E'–lineal inducida por la multiplicación por η_{r+1}, es decir

$$L_{\eta_{r+1}} : F' \to F', \qquad\qquad g \mapsto \eta_{r+1} \cdot g.$$

Luego P_V coincide con el polinomio característico de $L_{\eta\, r}$, salvo por un factor en $k(U_1, \ldots, U_r, T_r, \ldots, T_r)^*$. Esto justifica el nombre de polinomio característico de V para el polinomio P_V.

Se tiene además $\deg^{(T)} P_V \leq \deg V$, donde $\deg^{(T)}$ denota el grado en las variables $T_1, \ldots, T_{r+1}$. Esta estimación se sigue directamente de la definición de P_V como la ecuación de una proyección lineal de V en un espacio afín $\mathbb{A}^{r+1}$. De la observación de que P_V es — esencialmente — el polinomio característico de η_{r+1} se deduce

$$\deg^{(T)} P_V = \deg V.$$

Sea $V = \cup_i V_i$ la descomposición de V en componentes irreducibles. Luego se tiene

$$P_V = \prod_i P_{V_i}.$$

El siguiente resultado muestra la estrecha relación entre el polinomio característico y la forma de Chow de una variedad .

Lema 1.2.3 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r. Entonces*

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

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

Demostración. Alcanza con considerar el caso en que V es irreducible. Sea $Q(U, T) := (f_V \circ \alpha)(U, T)$. Vamos a probar la igualdad $P_V = Q$. Se tiene $Q(U, 0) = f_V$ y por lo tanto Q es no nulo. 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 $Q(U, \eta(\xi)) = f_V(L_1, \ldots, L_{r+1})$ es idénticamente 0. Luego Q es múltiplo de P_V. Por otra parte se tiene que $Q(U, 0) = f_V(U)$ y por lo tanto Q es irreducible. Concluimos entonces $P_V = Q$. $\square$

En particular se tiene

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

Además P_V es un polinomio homogéneo de grado $\deg V$ en el grupo de variables (U_i, T_i) para todo i.

Sea $V \subseteq \mathbb{A}^n$ una variedad definida sobre un cuerpo perfecto k, no necesariamente algebraicamente cerrado. Entonces su ideal de definición $I(V)$ está definido sobre k [99, Teorema 26.3]. En particular su polinomio característico P_V y su forma de Chow f_V están definidos sobre k.

En lo que sigue 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 $M = (U_{ij})_{1\le i,j\le n}$ una $n \times n$–matriz formada por variables. Luego se tiene

$$U_{i1}\, x_1 + \cdots + U_{in}\, x_n = \eta_i - U_{i0}$$

y por lo tanto

$$\Delta\ x_i = (\Delta_{1i}\eta_1 + \cdots + \Delta_{ni}\eta_n) - (\Delta_{1i}U_{10} + \cdots + \Delta_{ni}U_{n0})$$

donde Δ denota el determinante de la matriz M y Δ_{ij} denota el (i,j)–menor de M. Sea entonces M' la $n \times (n+1)$–matriz de variables que resulta de adjuntar la columna $(U_{10}, \ldots, U_{n0})$ a la matriz M. Luego se tiene

$$f_V = \Delta_0^{\delta}\, f(\Delta_1/\Delta_0, \ldots, \Delta_n/\Delta_0)$$

donde Δ_i denota $(-1)^i$ veces el determinante de la matriz que resulta de suprimir la columna i en la matriz M'.

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

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

1.2.3 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 una variedad* de V como

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

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

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

Lema 1.2.4 *Sea $V \subseteq \mathbb{A}^n$ una hipersuperficie definida por un polinomio separable $g \in k[x_1, \ldots, x_n]$. Entonces*

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

Demostración. Sea g^h la homogeneización de g en $k[x_0, \ldots, x_n]$ y sea $M' = (U_{ij})_{ij}$ una $n \times (n+1)-$matriz de variables. Entonces

$$f_V = g^h(\Delta_0, \Delta_1, \ldots, \Delta_n)$$

donde Δ_i es $(-1)^i$ veces el determinante de la matriz que resulta de suprimir en M' la columna i.

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

$$m(f_V) \leq m(g) + \deg g\,(\log(n+1) + n\log n + n\ \log(n^2+n)) \leq m(g) + 3(n+1)\log(n+1)\deg g$$

por el lema 1.1.1. Por otra parte se tiene $g = f_V \circ \alpha(x)$ con $T_i(x) = (-x_i, 0, \ldots, 1, \ldots, 0)$, y por lo tanto

$$m(g) \leq m(f_V) + n\ \deg g(\log(n^2+n) + \log 2 + \log(n+1)) \leq 3(n+1)\log(n+1)\deg g.$$

□

Sea $V \subseteq \mathbb{A}^n$ una variedad afín de dimensión 0. Entonces se define la altura de Weil $w(V)$ de V como

$$w(V) := \sum_{\xi \in V} \overline{h}(\xi).$$

Lema 1.2.5 *Sea $V \subseteq \mathbb{A}^n$ una variedad de dimensión 0. Entonces*

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

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 $\overline{h}(f_V) = \overline{h}(\xi)$. Luego se tiene

$$\overline{h}(\xi) - \log(n+1) \leq m(f_V) \leq \overline{h}(\xi) + \log(n+1)$$

□

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 una cantidad que depende polinomialmente de n.

1.2.4 Propiedades Básicas

Ahora vamos a establecer algunas de las propiedades básicas de esta altura de variedades. Consideramos en primer lugar su comportamiento bajo intersección con variedades lineales.

Lema 1.2.6 *Sea* $V \subseteq \mathbb{A}^n$ *una variedad de dimensión* r. *Sea* $H \subseteq \mathbb{A}^n$ *un hiperplano y sea* $L \in k[x_0, \ldots, x_n]$ *una ecuación de* H. *Entonces*

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

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

Asumimos entonces $V \not\subseteq H$. Luego $V \cap H$ es una variedad equidimensional de dimensión $r-1$. Sea $g := f_V(U_1, \ldots, U_r, L)$.

Sean $H_1, \ldots, H_r$ hiperplanos de $\mathbb{P}^n$. Luego $g(H_1, \ldots, H_r) = 0$ si y sólo si $(\overline{V} \cap H) \cap H_1 \cap \cdots \cap H_r \neq \emptyset$ donde $\overline{V} \subseteq \mathbb{P}^n$ denota la clausura proyectica de V. Luego g es un múltiplo no nulo de $f_{V \cap H}$. Luego $m(f_{V\cap H}) \leq m(g)$ por la positividad de la altura m y por lo tanto

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

□

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

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

ya que existe $\lambda \in k^*$ tal que $\overline{m}(\lambda L) = m(L) = h(H)$. Esta desigualdad se extiende sin dificultad al caso de la intersección de V con una variedad lineal.

Corolario 1.2.7 *Sea* $V \subseteq \mathbb{A}^n$ *una variedad de dimensión* r. *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*

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

□

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

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

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

Sea $\psi : \mathbb{A}^n \to \mathbb{A}^m$ un morfismo racional, y sean $\psi_i \in k[x_1, \ldots, x_n]$ funciones racionales tales que $\psi = (\psi_1, \ldots, \psi_m)$. Entonces se define la *altura* de ψ como

$$\overline{h}(\psi) := \max_i \overline{h}(\psi_i).$$

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

Lema 1.2.8 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un morfismo lineal afín inversible y sea $V \subseteq \mathbb{A}^n$ una variedad de dimensión r. Entonces*

$$h(\varphi(V)) \leq h(V) + (r+1)\,(\overline{h}(\varphi) + 5\log(n+1)\deg V.$$

Demostración. Sean G y b una $(r+1)\times n$–matriz y una $(r+1)\times 1$–matriz con coeficientes en k respectivamente, y sea $U := (b, G)$.

Sea $W := \varphi(V)$ y sea $\overline{V} \subseteq \mathbb{P}^n$ la clausura proyectiva de V. Luego $f_W(b, G) = 0$ si y sólo si existe un punto $\xi \in \overline{V}$ tal que $\varphi(\xi)$ está en el espacio lineal determinado por (b, G), es decir $b + G \cdot \varphi(x) = 0$.

Sea $(c, A) \in \mathbb{A}^n \times \mathbb{A}^{n\times n}$ la matriz asociada a φ, con $A \in GL_n(k)$ de forma tal que se tiene $\varphi(x) = c + A \cdot x$. Luego $b + G \cdot \varphi(x) = b + G \cdot c + G \cdot A \cdot x$ y por lo tanto

$$f_W\,(U) = f_W\,(b, G) = f_V(b + G \cdot c, G \cdot A).$$

Si definimos $U \cdot \varphi$ como $(b + G \cdot c, G \cdot A)$ se tiene entonces

$$f_{\varphi(V)}(U) = f_V(U \cdot \varphi).$$

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

$$\begin{aligned} m(f_W) &\leq m(f_V) + \deg f_V(\overline{m}(U\cdot\varphi) + 2\log(r+1)(n+1)) \\ &\leq m(f_V) + (r+1)(\overline{h}(\varphi) + 5\log(n+1))\deg V. \end{aligned}$$

□

Lema 1.2.9 *Sea $i : \mathbb{A}^n \hookrightarrow \mathbb{A}^{n+p}$ la inclusión $x \mapsto (x, 0)$ y sea $V \subseteq \mathbb{A}^n$ una variedad de dimensión r. Entonces $h(i(V)) = h(V)$.*

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

Lema 1.2.10 *Sea $\pi : \mathbb{A}^{n+p} \to \mathbb{A}^n$ la proyección $(x, y) \mapsto x$, y sea $V \subseteq \mathbb{A}^{n+p}$ una variedad de dimensión r. Entonces*

$$h(\overline{\pi(V)}) \leq h(V) + 5\,r\,(r+1)\log(n+p+1)\deg V.$$

Demostración. Alcanza con considerar el caso en que V es irreducible. Sea $W := \overline{\pi(V)}$ y sea $s := \dim W$. Luego existen coordenadas standard $y_1, \ldots, y_{r-s}$ tales que la proyección

$$\varpi : \mathbb{A}^n + p \to \mathbb{A}^n \times \mathbb{A}^{r-s}, \qquad\qquad x \mapsto (\varpi(x), y_1, \ldots, y_{r-s})$$

verifica $\dim \varpi(V) = r$. Sea entonces $Z := \overline{\varpi(V)}$. Luego $\overline{\pi(Z)} = W$ y se tiene $\dim \pi^{-1}(\xi) \geq r - s$ para todo $\xi \in W$, por el teorema de dimensión de fibras. Luego $W = Z \times \mathbb{A}^{r-s}$, y por lo tanto

$$W = Z \cap V(y_1, \ldots, y_{r-s}).$$

Se tiene $h(W) \leq h(Z) + 4(r-s)(r+1)\log(n+p+1)\deg V$ por el corolario 1.2.7, y alcanza entonces con acotar la altura de Z.

El polinomio $f_Z(U)$ es un factor de $f_V(U \cdot \pi)$, y por lo tanto

$$m(f_Z) \leq h(V) + 5(r+1)\log(n+p+1)\deg V.$$

Luego se tiene

$$m(f_W) \leq h(V) + 5(r-s)(r+1)\log(n+p+1)\deg V.$$

□

Proposición 1.2.11 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ un morfismo lineal afín y sea $V \subseteq \mathbb{A}^n$ una variedad de dimensión r. Entonces*

$$h(\overline{\varphi(V)}) \leq h(V) + (r+1)\,(\overline{h}(\varphi) + 5(r+1)^2 \log(n+1)\deg V.$$

Demostración. La aplicación φ se descompone como $\varphi = i \circ \psi \circ \pi$, donde $\psi : \mathbb{A}^p \to \mathbb{A}^p$ es inversible, e $i : \mathbb{A}^p \to \mathbb{A}^m$, $\pi : \mathbb{A}^n \to \mathbb{A}^p$ son la inclusión y la proyección canónicas respectivamente Se tiene $p := \operatorname{rank}(\varphi)$ y $\overline{h}(\psi) \leq \overline{h}(\varphi)$. La proposición se sigue entonces de los lemas previos. □

1.3 Estimaciones para Funciones Algebraicas

El teorema de la función inversa es una de las herramientas más versátiles de geometría diferencial. Lamentablemente 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 funciones inversas dadas por series de potencias formales.

En esta sección adoptamos este punto de vista como método para estudiar las propiedades de la altura de variedades de dimensión positiva. 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 0–dimensionales con respecto a una proyección finita.

1.3.1 El Teorema de la Función Inversa

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

En primer lugar introducimos algunas nociones básicas que vamos a utilizar en lo que sigue.

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

Sea $\varphi : V \to W$ un morfismo regular entre dos variedades $V \subseteq \mathbb{A}^n$ y $W \subseteq \mathbb{A}^m$ y sea $p \in W$ un punto. Entonces p es un punto *reducido* con respecto a φ 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 entre dos variedades irreducibles V, W de igual dimensión. 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

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

En el caso en que W es normal se tiene $\#\varphi^{-1}(p) \leq \deg \varphi$. En el caso en que φ es *separable*, es decir cuando la extensión $\varphi^* k(W) \hookrightarrow k(V)$ es separable, la igualdad $\#\varphi^{-1}(p) = \deg \varphi$ se satisface genéricamente [67, Proposición 1].

Un morfismo $\varphi : V \to W$ es *no ramificado* en un punto $p \in W$ si $\#\varphi^{-1}(p) = \deg \varphi$. El enunciado anterior dice 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 de W. Notamos que un punto no ramificado es también reducido [117, Sección II.5.3, Teorema 8].

Estas nociones y resultados se extienden sin dificultad al caso en que V es equidimensional, en lugar de irreducible. En todas nuestras aplicaciones la variedad W es un espacio afín.

Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un morfismo 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.

Para $m = (m_1, \ldots, m_n) \in \mathbb{N}^n$ definimos el operador

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

de forma tal que se tiene $\partial_m \psi(0) = b_m$. Sea $i = (i_1, \ldots, i_n) \in \mathbb{N}^n$. Luego

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

por la fórmula de Leibnitz. La suma se toma sobre todos los $l = (l_1, \ldots, l_{|i|}) \in (\mathbb{N}^n)^{|i|}$ tales que $l_1 + \cdots + l_{|i|} = m$. Separamos en esta suma los términos en los que interviene ∂_m de los términos en los que sólo intervienen derivadas de orden menor. Luego queda

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

donde esta última suma se extiende sobre todos los l como el párrafo anterior tales que $l_k \neq m$ para todo k.

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

$$\partial_m(\varphi \circ \psi) = (\mathrm{Diff}(\varphi) \circ \psi) \cdot \partial_m \psi + \sum_i \sum_{l\,:\, l_k \neq m} a_i\, \partial_{l_1} \psi_1 \cdots \partial_{l_{|i|}} \psi_n \tag{1.1}$$

donde $\mathrm{Diff}(\varphi) := (\frac{\partial \varphi_i}{\partial x_j})_{ij}$ denota el *diferencial* o *matriz Jacobiana* de la función φ. Asimismo denotamos por $J_\varphi := \det(\mathrm{Diff}(\varphi))$ el *Jacobiano* de φ.

El siguiente resultado garantiza la existencia de una inversa *formal* de un morfismo dominante en un punto reducido.

Lema 1.3.1 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un morfismo dominante tal que la fibra del punto $0 \in \mathbb{A}^n$ 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. La fibra $V_0 := \varphi^{-1}(0)$ es reducida y 0–dimensional. Sea $J := J_\varphi$ el Jacobiano de φ. Por el criterio Jacobiano se tiene $J(\xi) \neq 0$ para todo $\xi \in V_0$ [42, Teorema 18.15].

Vamos entonces a construir familias de polinomios $\psi^{(d)} \in k[x_1, \ldots, x_n]^n$ de grado acotado por d que verifican las siguientes condiciones

1. $\psi^{(d)}(0) = \xi$.
2. $\psi^{(d)} \equiv \psi^{(d')} \pmod{(y_1, \ldots, y_n)^{d+1}}$, para $d \leq d'$.
3. $\varphi \circ \psi^{(d)} \equiv \mathrm{Id} \pmod{(y_1, \ldots, y_n)^{d+1}}$.

Luego ψ se define como el límite en $k[[y_1, \ldots, y_n]]^n$ de la sucesión $\psi^{(d)}$. La unicidad de ψ se desprende a su vez de la unicidad de esta construcción.

Hacemos esta construcción inductivamente. Sea $\psi^{(0)} := \xi$. Sea $d \geq 1$ y asumimos que $\psi^{(d-1)}$ está construído. Sea $\psi^{(d)} := \psi^{(d-1)} + \sum_{|m|=d} b_m\, y^m$ con coeficientes b_m a ser determinados.

Sea $m \in \mathbb{N}^n$ tal que $|m| = d$. Se tiene $\partial_m(\varphi \circ \psi^{(d)})(0) = m$ para $|m| = 1$ y $\partial_m(\varphi \circ \psi^{(d)})(0) = 0$ en otro caso. Todas las derivadas en $y = 0$ de $\psi^{(d)}$ de orden menor o igual a $d-1$ están determinadas. Luego b_m queda unívocamente determinado por la fórmula 1.1 ya que la matriz Jacobiana $\mathrm{Diff}(\varphi)$ es no–singular en ψ. La familia de polinomios $\psi^{(d)}$ satisface las condiciones requeridas. $\square$

El resultado principal de esta sección consiste en 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 1.3.2 *Sea* $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ *un morfismo dominante tal que la fibra del punto* $0 \in \mathbb{A}^n$ *es finita y reducida. Sean* $\xi \in \varphi^{-1}(0)$ *y* $\psi \in k[[y_1, \dots, y_n]]^n$ *tales que* $\varphi \circ \psi = \mathrm{Id}$ *y* $\psi(0) = \xi$ *. Sean* $d := \max_i \deg \varphi_i$ *y* $h_v := \max_i h_v(\varphi_i)$ *para* $v \in M_k$ *. Entonces*

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

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

Demostración. Sea $\psi = \sum_j b_j\, y^j$. Fijamos un valor absoluto $v \in M_k$. Consideramos en primer lugar el caso en que $v \in S_k$. Luego vamos a acotar recursivamente las derivadas de ψ usando la identidad 1.1.

Hacemos inducción en $|m|$. Tenemos $\log|b_0| = h_v(\xi)$ y por lo tanto el enunciado vale para $m = 0$. Sea $J_\varphi(\xi)$ el Jacobiano de φ evaluado en ξ . Denotamos por κ la constante

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

Vamos a probar la estimación $\log|b_m|_v \leq (3|m|-2)(\kappa + |m|)$ para $|m| \geq 1$. Sea entonces $m \geq 1$ y supongamos que vale $\log|b_l| \leq (3|l|-2)(\kappa + |l|)$ para $1 \leq |l| \leq m-1$.

Se tiene $\varphi \circ \psi = \mathrm{Id}$ y por lo tanto $\partial_m(\varphi \circ \psi) = m$ para $|m| = 1$ y $\partial_m(\varphi \circ \psi) = 0$ para $|m| \geq 2$. Sea $\varphi = \sum_i a_i\, x^i$ y sea

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

es decir, la segunda suma en la expresión 1.1 — con el signo opuesto. Luego obtenemos la identidad

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

donde Adj^t denota la matriz adjunta traspuesta, y la constante τ se define como $\tau(m) = m$ para $|m| = 1$ y $\tau(m) = 0$ para $|m| \geq 2$.

Estimamos entonces el valor absoluto de la matriz $\mathrm{Adj}^t(\mathrm{Diff}(\varphi)(\xi))$. Se tiene

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

y por lo tanto

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

Para $|m| = 1$ se tiene $B_m = 0$ y por lo tanto

$$\log|b_m| \leq \log|\mathrm{Adj}^t(\mathrm{Diff}(\varphi)(\xi))| - h_v(J_\varphi(\xi)) \leq \kappa \leq (3|m|-2)(\kappa + |m|).$$

Consideramos entonces el caso $|m| \geq 2$. Sea

$$\alpha_v(m) := \max_{i,l_j}(\log|\partial_{l_1}\psi_1(0)| + \cdots + \log|\partial_{l_i}\psi_n(0)|)$$

donde $i \leq d$ y $l_j \in \mathbb{N}^n$ verifican $l_j \neq m$ y $l_1 + \cdots + l_i = m$. En la definición de $\alpha_v(m)$ sólo intervienen derivadas de orden $\leq m - 1$. Aplicamos la hipótesis inductiva y obtenemos

$$\alpha_v(m) \leq (3|m| - 4)(\kappa + |m| - 1) + (d-2)\,\overline{h}_v(\xi) \leq (3|m| - 3)(\kappa + |m|)$$

ya que $\kappa \geq (d-2)\,\overline{h}_v(\xi)$. Luego

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

Concluimos entonces

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

El caso en que v es no–arquimediano se sigue en forma análoga. □

El término que corresponde al Jacobiano se puede acotar en función de los demás parámetros. Mantenemos la misma notación del lema principal 1.3.2. Sea $v \in S_k$ un valor absoluto arquimediano y sean $\overline{h}_v := \max_i \overline{h}_v(\varphi_i)$ y $\overline{h} := \max_i h(\varphi_i)$. Se tiene $\overline{h}_v(\varphi(\xi)) \leq \overline{h}_v + d\,\overline{h}_v(\xi) + d + n$ y por lo tanto

$$h_v(J_\varphi(\xi)) \leq n\,\overline{h}_v(\varphi(\xi)) + \log n! \leq n\,\overline{h}_v + n\,d\,\overline{h}_v(\xi) + n\,d + 2n^2.$$

Análogamente, se obtiene $h_v(J_\varphi(\xi)) \leq n\,\overline{h}_v + n\,d\,\overline{h}_v(\xi)$ para $v \notin S_k$. Se tiene entonces

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

Obtenemos de aquí las estimaciones

$$\begin{aligned}
\log|\partial_m\psi(0)|_v &\leq (3\,|m| + 1)\,(2\,n\overline{h} + 2\,n\,d\,\overline{h}(\xi) + 4\,n\,d + 4\,n^2 + |m|), && v \in S_k, \\
\log|\partial_m\psi(0)|_v &\leq (3|m| + 1)(2\,n\,\overline{h} + 2\,n\,d\,\overline{h}(\xi)), && v \notin S_k.
\end{aligned}$$

Luego las derivadas de ψ se pueden acotar en términos de su orden, del grado y altura del morfismo φ, y de la altura de la fibra ξ.

Como consecuencia del resultado anterior obtenemos una estimación para las derivadas de la inversa local de un morfismo $\varphi : V \to \mathbb{A}^r$ para el caso en que V es una variedad intersección completa.

Corolario 1.3.3 *Sea $V \subseteq \mathbb{A}^n$ una variedad intersección completa reducida de polinomios $F_{r+1}, \ldots, F_n \in k[x_1, \ldots, x_n]$. Sea $\varphi : V \to \mathbb{A}^r$ un morfismo dominante tal que la fibra del punto $0 \in \mathbb{A}^r$ es finita y reducida. Sean $\xi \in \varphi^{-1}(0)$ y $\psi \in k[[y_1, \ldots, y_r]]^n$ tales que $\varphi \circ \psi = \mathrm{Id}$, $\psi(0) = \xi$ y $\psi(y) \in V$ para $y \in \mathbb{A}^r$. Sean $d := \max_{ij}\{\deg \varphi_i, \deg F_j\}$ y $h_v := \max_{ij}\{h_v(\varphi_i), h_v(F_j)\}$ para $v \in M_k$. Entonces*

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

para $m \in \mathbb{N}^n$, donde $J := J_{\varphi,F}$ denota el Jacobiano del morfismo $\mathbb{A}^n \to \mathbb{A}^n$ definido por $x \mapsto (\varphi(x), F(x))$.

Demostración. Sea $\Phi : \mathbb{A}^n \to \mathbb{A}^n$ el morfismo definido por $x \mapsto \Phi(x) := (\varphi(x), F(x))$. El hecho de que 0 sea un punto reducido de φ implica en forma directa que es también un punto reducido de Φ, por el criterio Jacobiano. Se tiene además $\xi \in \Phi^{-1}(0)$. Sea $\Psi \in k[[y_1, \ldots, y_r]]^n$ una inversa local de Φ en ξ. Luego $\psi := \Psi(y_1, \ldots, y_r, 0, \ldots, 0)$ satisface las condiciones requeridas.

Las cotas para las derivadas de ψ se siguen del lema principal 1.3.2. □

1.3.2 Cotas para la Traza

En esta subsección tratamos el problema de estimar la altura de la ecuación minimal de un elemento en el anillo de coordenadas de una variedad V con respecto a una normalización de Noether. Una característica destacable de estas estimaciones es que no dependen de la altura de la variedad V sino solamente de la altura de la fibra de un punto no ramificado con respecto a la posición de Noether.

Introducimos algunas definiciones básicas que vamos a necesitar en lo que sigue.

Sea $F := \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ una familia finita de polinomios. Luego F es una *intersección completa* si el ideal $(F) := (F_{r+1}, \ldots, F_n)$ de $k[x_1, \ldots, x_n]$ tiene dimensión r. Se dice que F es una *intersección completa reducida* si se tiene además que el ideal (F) es radical.

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

Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y sea $\pi : V \to \mathbb{A}^r$ una proyección finita separable. El resultado técnico principal de esta subsección es una cota para la altura de la ecuación minimal de un elemento $f \in k[V]$ sobre $\pi^* k[\mathbb{A}^r]$ en términos de la altura de la fibra de un punto no ramificado de π.

Teorema 1.3.4 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $F := \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ una intersección completa reducida que define una variedad $W := V(F) \subseteq \mathbb{A}^n$ que contiene a V.*

Sea $\pi : W \to \mathbb{A}^r$ la proyección lineal $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es finita y separable, y que $0 \in \mathbb{A}^r$ es un punto no ramificado de π. Sean $d := \deg F$ y $h := h(F)$. Sea $f \in k[V]$, y sea $m_f \in k[\mathbb{A}^r][t]$ el polinomio minimal de f sobre $k[\mathbb{A}^r]$. Entonces

$$\begin{aligned} \deg m_f &\leq \deg f \cdot \delta, \\ m(m_f) &\leq c_1 \deg f \cdot \delta \cdot h(\pi^{-1}(0)) + c_2 (\deg f)^2 \, \delta^2 + c_3 \, \delta \cdot h(f), \end{aligned}$$

donde c_1, c_2, c_3 sólo dependen de n, d y h.

La cota de grado para m_f fue obtenida previamente por Sabia y Solernó [115]. En el enunciado anterior se pueden tomar $c_1 := 8\, n\, d$, $c_2 := 8\, n\, (h + 2d + 3n + 7)$ y $c_3 := 4$.

Para la demostración de este resultado vamos a necesitar los siguientes lemas técnicos.

Lema 1.3.5 *Sean $\zeta_1, \ldots, \zeta_s \in k[[y_1, \ldots, y_n]]$, y sea $\theta \in k[[y_1, \ldots, y_n]]$ la serie de potencias*

$$\theta := \prod_j \zeta_j.$$

Sea $v \in M_k$ y sean $c_0, c_1 \geq 0$ constantes tales que $\log |\partial_m \zeta_j(0)|_v \leq c_0 \, |m| + c_1$. Entonces

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

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

Demostración. Sean $\zeta_j = \sum_i a_i^{(j)} \, y^i$ y $\theta = \sum_m c_m \, y^m$. Luego $c_m = \sum_{i_1 + \cdots + i_s = m} a_{i_1}^{(1)} \cdots a_{i_s}^{(s)}$. Consideramos en primer lugar el caso $v \in S_k$. Se tiene entonces

$$|c_m| \leq \prod_{l=1}^{n} \tbinom{m_l + s - 1}{s-1} \max_{i_1 + \cdots + i_s = m} \prod_{j=1}^{s} |a_{i_j}^{(j)}|$$

de donde

$$\begin{aligned} \log |c_m| &\leq \textstyle\sum_{l=1}^{n} (m_l + s - 1) + \max_{i_1 + \cdots + i_s = m} \sum_{j=1}^{s} (c_0 \, |i_j| + c_1) \\ &\leq (c_0 + 1)\, |m| + (c_1 + n)\, s. \end{aligned}$$

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

Corolario 1.3.6 *Sean $\zeta_1, \ldots, \zeta_s \in k[[y_1, \ldots, y_n]]$, $f \in k[t_1, \ldots, t_s]$, y sea $\vartheta \in k[[y_1, \ldots, y_n]]$ la serie dada por la composición de f con $\zeta_1, \ldots, \zeta_s$, es decir*

$$\vartheta := f(\zeta_1, \ldots, \zeta_s).$$

Sea $v \in M_k$ y sean $c_0, c_1 \geq 0$ constantes tales que $\log |\partial_m \zeta_j(0)|_v \leq c_0 |m| + c_1$. Entonces

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

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

Demostración. Sea $v \in S_k$. Sea $f = \sum_i a_i t^i$. Luego $\vartheta = \sum_i a_i \zeta^i = \sum_m c_m y^m$ y por lo tanto

$$\log |c_m| \leq (c_0 + 1)\,|m| + (c_1 + n)\ \deg f + \log |f| + \deg f + s.$$

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

Corolario 1.3.7 *Sean $\zeta_1, \ldots, \zeta_s \in k[[y_1, \ldots, y_n]]$, y sea $q = f/g \in k(t_1, \ldots, t_s)$ una función racional tal que $g(\zeta_1, \ldots, \zeta_s)(0) = 1$. Sea $\vartheta \in k[[y_1, \ldots, y_n]]$ la serie de potencias dada por la composición*

$$\vartheta := q(\zeta_1, \ldots, \zeta_s).$$

Sea $v \in M_k$ y sean c_0, $c_1 \geq 0$ constantes tales que $\log |\partial_m \zeta(0)|_v \leq c_0|m| + c_1$. Entonces

$$\begin{aligned} \log |\partial_m \zeta(0)|_v &\leq (\overline{h}_v(g) + (c_1 + n + 7s) \deg g + c_0)|m| + h_v(f) + (c_1 + n + 4s) \deg f, \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad v \in S_k, \\ \log |\partial_m \zeta(0)|_v &\leq (\overline{h}_v(g) + c_1 \deg g + c_0)|m| + h_v(f) + c_1 \deg f, \qquad\qquad v \notin S_k, \end{aligned}$$

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

Demostración. Se tiene

$$\vartheta = f(\zeta) \sum_{i \geq 0} (1 - g(\zeta))^i.$$

Sea $\vartheta = \sum_m c_m y^m$. Sea $m \in \mathbb{N}^n$. En el cálculo de c_m sólo aportan los términos de grado $\leq |m|$, y por lo tanto se tiene

$$\log |c_m|_v \leq \log |f(\zeta) \sum_{i=0}^{|m|} (1 - g(\zeta))^i|_v.$$

Consideramos en primer lugar el caso $v \in S_k$. Sea $F := f \sum_{i=0}^{|m|} (1 - g)^i$. Luego se tiene $\deg F \leq \deg f + |m| \deg g$ y

$$\begin{aligned} \log |F|_v &\leq m_v\,(f) + |m|\, m_v\,(1 - g) + (\deg f + |m| \deg g) \log(s + 1) + \log(|m| + 1) \\ &\leq h_v\,(f) + |m|\, \overline{h}_v\,(g) + (s + 1) \deg f + (s + 1)\,|m| \deg g + 3\,s\,|m| \end{aligned}$$

Aplicamos entonces el corolario 1.3.3 y obtenemos

$$\begin{aligned} \log |c_m|_v &\leq (c_0 + 1)\,|m| + (c_1 + n + 1) \deg F + \log |F|_v + s \\ &\leq (c_0 + (c_1 + n + s + 2) \deg g + \overline{h}_v(g) + 3s + 1)\,|m| \\ &\quad +(c_1 + s + n + 2) \deg f + h_v(f) + s \end{aligned}$$

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

Lema 1.3.8 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un morfismo dominante tal que la fibra $V_0 := \varphi^{-1}(0)$ del punto $0 \in \mathbb{A}^n$ es finita y reducida. Sean $d := \max_i \deg \varphi_i$ y $h := \max_i \overline{h}(\varphi_i)$. Entonces*

$$\overline{h}(J_\varphi(V_0)^{-1}) \leq n\, d\, h(V_0) + n\,(h + d + 3n) \deg V_0$$

donde $J_\varphi(V_0)^{-1} \subseteq k$ denota el conjunto $\{J_\varphi(\xi)^{-1} : \xi \in V_0\}$.

Demostración. Se tiene $\overline{h}(J_\varphi(\xi)^{-1}) = \overline{h}(J_\varphi(\xi)) \leq n\,h + n\,d\,\overline{h}(\xi) + n\,d + 2\,n^2$ para $\xi \in V_0$. Luego

$$\begin{aligned} \overline{h}(J_\varphi(V_0)^{-1}) &\leq \textstyle\sum_\xi \overline{h}(J_\varphi(\xi)^{-1}) \leq n\,d\,w(V_0) + n\,(h+d+2n)\,\deg V_0 \\ &\leq n\,d\,h(V_0) + n\,(h+d+2n+1)\,\deg V_0 \end{aligned}$$

donde $w(V_0) := \sum_\xi \overline{h}(\xi)$ denota la altura de Weil de V_0. □

Demostración del Teorema 1.3.4. Consideramos primeramente el caso en que V es irreducible. El polinomio m_f es una ecuación minimal para la imagen del morfismo $V \to \mathbb{A}^r$ definido por $x \mapsto (\pi(x), f(x))$. La cota de grado se sigue del teorema de Bézout (Lema 1.2.1).

Estimamos ahora la altura local del polinomio m_f. Sea $D := \deg V_0 \leq \delta$ y sea $V_0 = \{\xi_1, \dots, \xi_D\}$ la fibra en 0 de la proyección $\pi : V \to \mathbb{A}^r$, y sea $\psi_i \in k[[y_1, \dots, y_r]]^n$ la inversa local de π en ξ_i para $\xi_i \in V_0$.

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

$$\chi_f := \prod_{i=1}^{D} (t - f(\psi_i)) \in k[\mathbb{A}^r][t]$$

el polinomio característico de f. Luego $\chi_f(f) = 0$ y por lo tanto m_f es un factor de χ_f. Se puede suponer sin pérdida de generalidad que $\xi_1, \dots, \xi_D$ están ordenados de forma tal que se tiene

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

Sea $\Delta := \deg m_f \leq \deg f \cdot \deg V$ el grado total de m_f. Luego alcanza con estimar los coeficientes de los monomios de grado $\leq \Delta$ en este producto.

Consideramos en primer lugar el caso $v \in S_k$. Se tiene $\log|\partial_m\,\psi_i(0)| \leq c_0|m| + c_1$ con

$$c_1 := c_1(v) := n\,d\,h_v\,(V_0) + \overline{h}_v\,(J(V_0)^{-1}) + n\,h_v + 3\,n\,d\, + 2\,n^2 + \Delta$$

y $c_0 := c_0(v) := 3\,c_1$. Aquí se denota $h_v := h_v(F)$, y por J el Jacobiano del endomorfismo de $\mathbb{A}^n$ definido por $x \mapsto (\pi(x), F(x))$. Esta estimación es válida para $m \in \mathbb{N}^n$ tal que $|m| \leq \Delta$. Se sigue entonces

$$\log|\partial_m\, f(\psi_i)| \leq (c_0 + 1)\,|m| + (c_1 + r + 1) \deg f + \log|f| + n$$

por el corolario 1.3.3, y por lo tanto

$$\begin{aligned} \log|m_f| &\leq (c_0 + 2)\,\Delta + ((c_1 + r + 1) \deg f + \log|f| + n + r + 1)\,\mu \\ &\leq ((c_0 + c_1 + r + 3)\,\deg f + \log|f| + 2n + 1)\,\delta. \end{aligned}$$

El caso $v \notin S_k$ se trata en forma análoga. Se sigue entonces

$$\begin{aligned} h(m_f) &\leq 4\,\deg f(n\,d\,h(V_0) + \overline{h}(J(V_0)^{-1}) + h + 3\,n\,d\, + 2(n+1)^2 + \deg f \cdot \delta + h(f))\,\delta \\ &\leq 8\,n\,d\,\deg f \cdot \delta \cdot h(V_0) + 8\,n\,(h + 2\,n + 3\,n)\,(\deg f)^2\,\delta^2\, + 4\,\delta \cdot + h(f) \end{aligned}$$

por el lema 1.3.5, y por lo tanto

$$m(m_f) \leq c_1 \deg f \cdot \delta \cdot h(V_0) + c_2 (\deg f)^2 \, \delta^2 + c_3 \, \delta \cdot m(f)$$

con $c_1 := 8\,n\,d$, $c_2 := 8\,n(h + 2\,d + 3\,n + 7)$ y $c_3 := 4$.

El caso de una variedad equidimensional V se reduce al caso anterior. Sea $V = \cup_i V_i$ su descomposición en componentes irreducibles, y sea $m_f^{(i)}$ el polinomio minimal de f en $k[V_i]$. Luego se tiene

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

□

En lo que sigue obtenemos a partir de este resultado una cota para la altura del polinomio minimal de f en términos de la altura de V, y en particular, una cota para la altura de la traza de f.

Sea $\pi : V \to \mathbb{A}^r$ una proyección lineal finita y separable, y sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional. Sea $\zeta \in k[V]$ un elemento primitivo de V y sea $P \in k[\mathbb{A}^r][t]$ su ecuación minimal. Luego P es un polinomio separable de grado $\deg \pi$. Luego $p \in \mathbb{A}^r$ es un punto reducido con respecto a π si y sólo si $P(p)(t)$ es separable. En particular $\#\pi^{-1}(p) = \deg \pi$. La condición de ser reducido es entonces equivalente — en esta situación — a la condición de ser no ramificado.

Sea $\pi : V \to \mathbb{A}^r$ una proyección lineal de una variedad equidimensional $V \subseteq \mathbb{A}^n$ en un subespacio afín. Asumimos que π es una normalización de Noether separable de V. En esta situación vamos a tratar la relación entre la altura de V y la altura de la fibra de π en un punto no ramificado.

El siguiente resultado muestra que existen puntos no ramificados con respecto a π de baja altura y nos da estimación la altura de su fibra.

Proposición 1.3.9 *Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \dots, x_r)$, y sea V una variedad equidimensional de dimensión r y grado δ. Asumimos que π es finita y separable. Entonces existe un punto $p \in \mathbb{A}^r$ no ramificado con respecto a π tal que*

$$h(p) \leq c_1(n) \log \delta + c_2(n).$$

Se tiene además $h(\pi^{-1}(p)) \leq h(V) + c_3(n)\delta \log \delta + c_4(n)\delta$.

Se pueden tomar $c_1 := n$, $c_2 := 2\,n$, $c_3 := n^3$, $c_4 := 6\,n^2 \log(n+1)$. Este resultado es consecuencia de una serie de lemas previos que ahora vamos a demostrar.

Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r. Sea $\pi : V \to \mathbb{A}^r$ un morfismo lineal dominante. Este es el caso, por ejemplo, si π es una proyección lineal que representa una normalización de Noether de V. Sean $E := k(\mathbb{A}^r)$ y $F := E \otimes_k k[V]$. Luego F es un E–espacio vectorial de dimensión $[F : E] \leq \deg V$. Para $f \in F$, denotamos por L_f la aplicación lineal

$$L_f : F \to F, \qquad g \mapsto f \cdot g.$$

Se definen entonces la *traza* $\mathrm{Tr}(f)$ y la *norma* $N(f)$ de f como la traza y el determinante de la aplicación lineal L_f, es decir

$$\mathrm{Tr}(f) := \mathrm{Tr}_E^F(f) = \mathrm{Tr}(L_f), \qquad\qquad N(f) := N_E^F(f) = \det(L_f).$$

Lema 1.3.10 *Con la misma notación del párrafo anterior, se tiene que un elemento $f \in k[V]$ es divisor de cero si y sólo si $\det(L_f) = 0$.*

Demostración. El elemento f es divisor de cero en $k[V]$ si y sólo si es 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 la aplicación L_f no es inyectiva, lo cual equivale a la condición $\det(L_f) = 0$. □

Sean $F_{r+1}, \ldots, F_n \in k[x_1, \ldots, x_n]$. Entonces $F_{r+1}, \ldots, F_n$ forman una *sucesión regular* en $k[x_1, \ldots, x_n]$ si $\overline{F}_{i+1}$ no es un divisor de cero ni una unidad en el anillo cociente $k[x_1, \ldots, x_n]/(F_{r+1}, \ldots, F_n)$.

Lema 1.3.11 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r. Entonces existe una sucesión regular reducida de polinomios $F_{r+1}, \ldots, F_n \in k[x_1, \ldots, x_n]$ tales que $V \subseteq V(F_{r+1}, \ldots, F_n)$ y*

$$\deg F_i \leq \deg V, \qquad\qquad m(F_i) \leq h(V) + c(n) \deg V,$$

para todo i.

Se puede tomar $c := 5\,(n+1)^2 \log(n+1)$.

Demostración. Asumimos sin pérdida de generalidad que $x_1, \ldots, x_r$ son algebraicamente independientes en $k[V]$. Luego la proyección $\pi : V \to \mathbb{A}^r$ definida por $x \mapsto (x_1, \ldots, x_r)$ es dominante.

Luego sea F_i la ecuación de la proyección de V por el morfismo $x \mapsto (\pi(x), x_i)$ para $i = r+1, \ldots, n$. Afirmamos que $F_{r+1}, \ldots, F_n$ cumple con las condiciones del enunciado.

Los polinomios F_i son polinomios separables en variables separadas, y por lo tanto forman una sucesión regular reducida que contiene a V. Esto se sigue del lema anterior y del criterio Jacobiano. Se tiene además $\deg F_i \leq \deg V$ y

$$m(F_i) \leq h(V(F_i)) + 3\,(r+2) \deg F_i \leq h(V) + 5(n+1)^2 \log(n+1) \deg V$$

por aplicación de la proposición 1.2.11 y el lema 1.2.4. □

Demostración de la Proposición 1.3.9. Sean $F_{r+1}, \ldots, F_n \in k[x_1, \ldots, x_n]$ polinomios de grado acotado por δ que forman una sucesión regular reducida que contiene a V. Sea $W := V(F_{r+1}, \ldots, F_n) \subseteq \mathbb{A}^n$. El polinomio F_i es la ecuación de la proyección $\pi_i : V \to \mathbb{A}^{r+1}$ definida por $x \mapsto (\pi(x), x_i)$, y por lo tanto la proyección $\pi : W \to \mathbb{A}^r$ es dominante y separable.

Sea $J \in k[x_1, \ldots, x_n]$ el Jacobiano de los F_i con respecto a las variables $x_{r+1}, \ldots, x_n$, es decir
$$J := \det(\frac{\partial F_i}{\partial x_j})_{ij}.$$

Luego $\overline{J} \in k[W]$ es no–divisor de cero. Sea $\Delta := \det L_J \in k[\mathbb{A}^r] - \{0\}$ la norma de J. Luego Δ es un polinomio no nulo de grado

$$\deg \Delta \leq (n-r)\, \delta^{n-r}.$$

Por el criterio Jacobiano, $p \in \mathbb{A}^r$ es un punto reducido de $\pi : W \to \mathbb{A}^r$ si y sólo si $\Delta(p) \neq 0$. En nuestra situación, esto equivale al hecho de que p sea un punto no ramificado.

Luego existe $p = (p_1, \ldots, p_r) \in \mathbb{A}^r$ no ramificado tal que $\overline{h}(p_i) \leq \deg \Delta$, por el lema 1.1.3, y por lo tanto
$$h(p) \leq (n-r) \log \delta + \log(n-r) + n.$$

Por otra parte se tiene $\pi^{-1}(p) = V \cap V(x_1 - p_1, \ldots, x_r - p_r)$ y por lo tanto

$$\begin{aligned} h(\pi^{-1}(p)) &\leq h(V) + (r+1) (\textstyle\sum_i (\overline{h}(p_i) + \log 2) + 4\, r \log(n+1))\delta \\ &\leq h(V) + r\,(r+1)\,((n-r)\log\delta + \log(n-r) + \log 2 + 4\, \log(n+1))\, \delta. \end{aligned}$$

$\square$

La siguiente es la cota para la altura del polinomio minimal de un elemento en $k[V]$. Este resultado es análogo aritmético de [115, Proposición 1].

Corolario 1.3.12 *Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es finita y separable. Sea $f \in k[V]$, y sea $m_f \in k[\mathbb{A}^r][t]$ el polinomio minimalde f sobre $k[\mathbb{A}^r]$. Entonces*

$$m(m_f) \leq c_1 (\deg f)^2\, \delta^2\, h(V) + c_2\, (\deg f)^2\, \delta^4 + c_3\, \delta \cdot h(f)$$

donde c_1, c_2, c_3 sólo dependen de n.

Se pueden tomar $c_1 := 8\,n$, $c_2 := 96\,(n+1)^4$ y $c_3 := 4$.

Demostración. Este resultado se sigue directamente de la proposición 1.3.9 y del teorema 1.3.4. Hacemos aquí los cálculos correspondientes.

Por el teorema 1.3.4 existe un punto no ramificado $p \in \mathbb{A}^r$ de π tal que

$$\overline{h}(p_i) \leq (n-r) \log \delta + \log(n-r).$$

Aplicamos a la variedad V la traslación τ definida por $x \mapsto (x_1 - p_1, \ldots, x_r - p_r, x_{r+1}, \ldots, x_n)$. Se tiene
$$h(\tau(V)) \leq h(V) + (n+1)^2\, \delta\, (\log \delta + 6)$$

y por el lema 1.3.11 existe una intersección completa reducida $F := \{F_{r+1}, \dots, F_n\} \subseteq k[x_1, \dots, x_n]$ tal que la variedad $W := V(F) \subseteq \mathbb{A}^n$ contiene a V. Se tiene $\deg F_i \leq \delta$ y

$$h(F \circ \tau) \leq h(V) + (n+1)^2 (\log \delta + 5 \log(n+1) + 6)\, \delta.$$

Se tiene además

$$h(\tau(V)_0) \leq h(V) + (n+1)^2 (\log \delta + 4 \log(n+1) + 6)\, \delta$$

donde $\tau(V)_0$ denota la fibra del punto $0 \in \mathbb{A}^r$ con respecto a la proyección $\tau \circ \pi$. Concluimos entonces

$$m(m_f) \leq c_1 (\deg f)^2\, \delta^2\, h(V) + c_2 (\deg f)^2\, \delta^4 + c_3\, \delta\, h(f)$$

con $c_1 := 8\,n$, $c_2 := 96\,(n+1)^4$ y $c_3 := 4$. □

Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \dots, x_r)$. Asumimos que π es finita. Luego la inclusión $k[x_1, \dots, x_r] \hookrightarrow k[V]$ es entera. Denotamos por $\deg^\circ f$ y $\deg^* f$ el grado f en las variables libres $x_1, \dots, x_r$ y en las variables dependientes $x_{r+1}, \dots, x_n$ respectivamente.

El resultado siguiente es una estimación para el grado y las altura de la traza de f. Estas estimaciones son cruciales para nuestra demostración del teorema de ceros aritmético (Teorema 2.3.2).

Proposición 1.3.13 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \dots, x_r)$. Asumimos que π es finita y separable. Sea $f \in k[V]$. Entonces*

$$\begin{aligned} \deg \mathrm{Tr}(f) &\leq \deg^* f \cdot \delta + \deg^\circ f, \\ m(\mathrm{Tr}(f)) &\leq c_1 (\deg^* f)^2\, \delta^2\, h(V) + c_2 (\deg^* f)^2\, \delta^4 + h(f) \end{aligned}$$

donde c_1, c_2, c_3 sólo dependen de n.

Se pueden tomar $c_1 := 8\,n$, $c_2 := 10^2\,(n+1)^4$.

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

$$m_f = t^\mu + a_{\mu-1}\, t^{\mu-1} + \cdots + a_0 \in k[\mathbb{A}^r][t]$$

el polinomio minimal de f. Se tiene $\mu | \deg \pi$ y por lo tanto $\mathrm{Tr}(f) = -(\deg \pi / \mu) a_{\mu-1}$.

Consideramos en primer lugar el caso de un monomio $\theta := x^i = x_{r+1}^{i_{r+1}} \cdots x_n^{i_n}$. Sea $d := |i|$ el grado de θ. Se tiene entonces

$$\begin{aligned} \deg \mathrm{Tr}(\theta) &\leq d \cdot \delta, \\ m(\mathrm{Tr}(\theta)) &\leq d^2\, \delta^2 (c_1\, h(V) + c_2\, \delta^2) + \log \delta + d \cdot \delta\, \log(r+1) \end{aligned}$$

por el teorema 1.3.4 y el corolario 1.3.12, donde c_1, c_2 denotan las constantes del corolario 1.3.12. Luego se tiene

$$\begin{aligned} \deg \mathrm{Tr}(f) &\leq \deg^* f \cdot \delta + \deg^\circ f, \\ m(\mathrm{Tr}(f)) &\leq (\deg^* f)^2 \cdot \delta^2 (c_1\, h(V) + (c_2 + n + 1) \delta^2) + h(f) + d + n. \end{aligned}$$

por la linealidad de la traza. □

1.3.3 Altura de Fibras vs. Altura de Variedades

La aplicación más importante de los resultados de las subsecciones 1.3.1 y 1.3.2 consiste en la estimación de la altura de una variedad de dimensión positiva en términos de la altura de una fibra 0–dimensional. Este apartado está enteramente dedicado a la demostración de este resultado. El enunciado es el siguiente:

Teorema 1.3.14 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $F := \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ una intersección completa reducida que define una variedad $W := V(F) \subseteq \mathbb{A}^n$ que contiene a V.*

Sea $\pi : W \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es dominante y separable de grado δ, y que $0 \in \mathbb{A}^r$ es un punto no ramificado de π. Entonces

$$h(V) \leq c_1\, \delta^5\, h(\pi^{-1}(0)) + c_2\, \delta^7$$

donde c_1, c_2 dependen sólo de n, $\deg F$, $h(F)$.

Sean $d := \deg F$ y $h := h(F)$. Luego se pueden tomar $c_1 := 216\,(n+1)^4\, d^2$ y $c_2 := 456\,(n+1)^4\, n\,(h + 2d + 3n + 3)$. Primeramente vamos a establecer algunos resultados auxiliares.

Lema 1.3.15 *Sea $F := \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ una intersección completa reducida que define una variedad $W := V(F) \subseteq \mathbb{A}^n$. Sea $\pi : W \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es finita y separable de grado δ, y que $0 \in \mathbb{A}^r$ es un punto no ramificado de π. Entonces existe una forma lineal $y \in k[x_1, \ldots, x_n]$ tal que la proyección*

$$\pi_i : W \to \mathbb{A}^r, \qquad x \mapsto (x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_r)$$

es finita y separable de grado δ, y $0 \in \mathbb{A}^r$ es un punto no ramificado de π_i para todo i. Se tiene además

$$m(y) \leq (r+2)\log\delta + n + 1.$$

Demostración. Sea

$$\chi := t^\delta + a_{\delta-1}\, t^{\delta-1} + \cdots + a_0 \in k[U][\mathbb{A}^r][t]$$

el polinomio característico de la forma lineal genérica $\eta := U_0 + U_1\, x_1 + \cdots + U_n\, x_n$. Sea $\alpha_i \in k[U]$ el coeficiente de x_i^δ en χ para $i = 1, \ldots, r$. Luego α_i es un polinomio no nulo de grado δ. Esto es una consecuencia del hecho de que la proyección π tiene grado δ.

Por otra parte, sea $\rho \in k[\mathbb{A}^r][U]$ el discriminante de χ con respecto a t. Luego $\rho(0, U) \neq 0$, por la hipótesis de que $0 \in \mathbb{A}^r$ es un punto no ramificado. Se tiene $\deg \rho(0, U) \leq \delta^2$. El polinomio $\psi := \rho \prod_i \alpha_i$ tiene grado acotado por δ^{r+2}. Sea $c \in k^{(r+1)(n+1)}$ tal que

$$\psi(c) \neq 0.$$

La forma lineal $y := \eta(c)$ satisface las condiciones del enunciado.

□

Mantenemos la notación del enunciado del teorema 1.3.14 y del lema precedente. Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$, y sea $V_0 := \pi^{-1}(0)$ la fibra del punto $0 \in \mathbb{A}^r$ con respecto a π. Consideramos las proyecciones

$$\pi_i : V \to \mathbb{A}^r, \qquad\qquad x \mapsto (x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_r)$$

para $i = 1, \ldots, r$ y denotamos por $V_i := \pi_i^{-1}(0)$ la fibra del punto $0 \in \mathbb{A}^r$ con respecto a π_i. El siguiente resultado muestra que la altura de las fibras V_i está acotado por la altura de la fibra V_0.

Lema 1.3.16 *Mantenemos la notación del párrafo anterior. Asumimos además* $y = x_{r+1}$. *Entonces*

$$h(V_i) \leq c_1\, \delta^3\, h(V_0) + c_2\, \delta^4$$

para $i = 1, \ldots, r$, *donde* c_1, c_2 *dependen sólo de* n, $\deg F$, $h(F)$.

Se pueden tomar $c_1 := 16\, n\, d$ y $c_2 := 24\, n\, (h + 2d + 3n)$.

Demostración. Asumimos sin pérdidad de generalidad $i = 1$. Sea

$$m_i = t^\delta + a_{\delta-1}\, t^{\delta-1} + \cdots + a_0 \in k[x_1, \ldots, x_r][t]$$

el polinomio minimal de la forma lineal x_i con respecto a la proyección π. En particular m_{r+1} es el polinomio minimal de y. Por la hipótesis de que π_1 es finita y separable de grado δ, se tiene que m_{r+1} coincide con el polinomio minimal de x_1, salvo por un factor en k^*.

Sea $\zeta = (\zeta_1, \ldots, \zeta_n) \in V_1$ un punto en la fibra de π_1. Luego sea $q_1 := m_{r+1}(t, 0, \ldots, 0) \in k[t]$. Luego $q_1(\zeta_1) = 0$ y por lo tanto

$$\overline{h}(\zeta_1) \leq h(q_1) + \log \delta \leq h(m_{r+1}) + \log \delta$$

por el lema 1.1.2. Sea además $q_i := m_i(\zeta_1, 0, \ldots, 0, t) \in k[t]$. Se tiene $q_i(\zeta_i) = 0$ para $i = r + 2, \ldots, n$, y por lo tanto

$$\begin{aligned} \overline{h}(\zeta_i) &\leq h(q_i) + \log \delta \leq \delta \cdot h(m_1) + h(m_i) + 2 \log(\delta + 1) \\ &\leq (\delta + 1)(c_1\, \delta \cdot h(V_0) + c_2\, \delta^2) + 2 \log(\delta + 1) \end{aligned}$$

donde c_1, c_2 son las constantes del teorema 1.3.4. Concluimos entonces

$$h(V_1) \leq \delta((\delta + 1)(c_1 \delta \cdot h(V_0) + c_2\, \delta^2) + 2 \log(\delta + 1)) + \delta \log(n + 1)$$

$\square$

Sean $\mathbb{A}^r$ y $\mathbb{A}^{r\, n}$, consideradas como las variedades de las $r \times 1$–matrices y de las $r \times n$–matrices con coeficientes en k. Consideramos entonces la proyección genérica definida por

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

Este morfismo es dominante y separable de grado δ [67]. Sea $\chi = t^\delta + b_{\delta-1}\, t^{\delta-1} + \cdots + b_0 \in k(U)[T]$ el polinomio característico de la forma lineal genérica

$$\eta_{r+1} := U_{r+1,0} + U_{r+1,2}x_1 + \cdots + U_{r+1,n}x_n.$$

Sea además $P_V = a_\delta\, t^\delta + \cdots + a_0 \in k[U,T]$ el polinomio característico de V, expandido con respecto a las potencias de $t := T_{r+1}$. Se tiene entonces

$$P_V = a_\delta \cdot \chi.$$

Sea $f_V \in k[U]$ el polinomio de Chow de V. Sean $\alpha := a_\delta$ y $\beta := b_0(U,0)$. Se tiene $f_V = P(U,0)$ y por lo tanto

$$f_V = \alpha \cdot \beta.$$

El polinomio de Chow f_V es homogéneo de grado δ en cada grupo de variedades U_i, y es además simétrico — salvo por $\pm$ — con respecto a permutaciones entre estos grupos de variables. El polinomio α es homogéneo de grado δ con respecto a los grupos de variables $U_1, \ldots, U_r$, y no depende de U_{r+1}. Referimos a la subsección 1.2.2 para una discusión más detallada de estas cuestiones.

Consideramos las proyecciones

$$\pi_i : V \to \mathbb{A}^r, \qquad\qquad x \mapsto (x_1, \ldots, \overset{i}{\widehat{x_i}}, \ldots, x_{r+1})$$

para $i = 1, \ldots, r+1$. Asumimos que π_i es finita y separable de grado δ.

Sea $B := (c, A) \in \mathbb{A}^{r+1} \times \mathbb{A}^{(r+1)n}$ la matriz que corresponde a la proyección $V \to \mathbb{A}^{r+1}$ definida por $x \mapsto (x_1, \ldots, x_{r+1})$. Se tiene $c = 0$ y $A_i = (0, \ldots, 1, \ldots, 0)$. Asumimos además

$$f_V(B) \neq 0.$$

El siguiente lema muestra que el polinomio de Chow f_V se puede expresar en términos del polinomio característico χ de la forma lineal η_{r+1}.

Lema 1.3.17 *Mantenemos la notación de la discusión precedente. Entonces*

$$f_V = \lambda \cdot \beta \cdot \prod_{i=1}^{r} \beta(B_1, \ldots, B_i, U_{i+1}, \ldots, U_r, U_i)/\beta(B_1, \ldots, B_{i-1}, U_i, \ldots, U_r, B_i)$$

para algún $\lambda \in k^*$.

Demostración. Se tiene

$$f_V = \alpha(U_1, \ldots, U_r) \cdot \beta(U_1, \ldots, U_{r+1}) = \pm\alpha(U_2, \ldots, U_{r+1}) \cdot \beta(U_2, \ldots, U_{r+1}, U_1)$$

gracias a la simetría de f_V. Luego se tiene

$$\alpha = \pm\alpha(U_2, \ldots, U_{r+1}) \cdot \beta(U_2, \ldots, U_{r+1}, U_1)/\beta(U_1, \ldots, U_{r+1}).$$

Esta expresión no depende del grupo de variables U_{r+1}, y por lo tanto

$$\alpha = \pm\beta(U_2,\ldots,U_r,B_1,U_1)/\beta(U_1,\ldots,U_r,B_1)\cdot\alpha(U_2,\ldots,U_r,B_1)$$

donde B_1 denota la 1–fila de la matriz $B = (c, A)$. Aplicando sucesivamente este principio obtenemos la identidad

$$\alpha = \pm\alpha(B_1,\ldots,B_r)\prod_{i=1}^{r}\beta(U_{i+1},\ldots,U_r,B_1,\ldots,B_i,U_i)/\beta(U_i,\ldots,U_r,B_1,\ldots,B_i).$$

El enunciado se sigue entonces por la simetría de β con respecto a permutaciones entre $U_1,\ldots,U_r$. □

Demostración del Teorema 1.3.14. Alcanza con considerar el caso en que V es irreducible.

A lo largo de esta demostración vamos a mantener la notación introducida en la discusión previa al lema 1.3.17. Asumimos por el momento $y = x_{r+1}$, es decir, que las todas las proyecciones

$$\pi_i : V \to \mathbb{A}^r, \qquad\qquad x \mapsto (x_1,\ldots,\overset{i}{\widehat{x_i}},\ldots,x_{r+1})$$

son finitas y separables de grado δ.

Vamos a utilizar la identidad introducida en el lema 1.3.17 para calcular el desarrollo del polinomio de Chow f_V alrededor del punto $B \in \mathbb{A}^{(r+1)(n+1)}$.

Sea E_i la matriz asociada a la proyección π_i, es decir, la matriz que se obtiene a partir de la matriz B suprimiendo la i–fila B_i. El punto $P_i := (E_i, 0) \in \mathbb{A}^r\times\mathbb{A}^{r\,n}\times\mathbb{A}^r$ es entonces un punto no ramificado de la proyección genérica ϖ. Sea

$$Z_i := \varpi^{-1}(P_i) = E_i\times V_i \subseteq \mathbb{A}^r\times\mathbb{A}^{r\,n}\times\mathbb{A}^n$$

la fibra de ϖ en el punto P_i. Sea $\rho_j \in Z_i$ y sea $\psi_j^{(i)} \in k[[U-E_i,T]]$ la inversa local de la proyección ϖ en el punto ρ_j. Se tiene entonces la identidad

$$\chi = \prod_{j=1}^{\delta}(t - \eta_{r+1}(\psi_j^{(i)}))$$

y en particular

$$\beta = \pm\prod_{j=1}^{\delta}\eta_{r+1}(\psi_j^{(i)}(U,0)).$$

Esta identidad nos permite estimar el valor absoluto de las derivadas de β en el punto $E_i \in \mathbb{A}^r\times\mathbb{A}^{rn}$. Hacemos

$$\begin{aligned}\vartheta_j^{(i)} &:= \eta_{r+1}(\psi_j^{(i)}(B_1,\ldots,B_i,U_{i+1},\ldots,U_r,0))(U_i),\\ \varrho_j^{(i)} &:= \eta_{r+1}(\psi_j^{(i)}(B_1,\ldots,B_{i-1},U_i,\ldots,U_r,0))(B_i).\end{aligned}$$

y se tiene entonces la indentidad

$$f_V = \lambda\prod_j\zeta_j\cdot\prod_{ij}\vartheta_j^{(i)}/\prod_{ij}\cdot\varrho_j^{(i)}$$

por el lema 1.3.17. Sea $v \in M_k$ un valor absoluto, y sean $C_0 := C_0(v)$, $C_1 := C_1(v) \geq 0$ constantes no–negativas tales que

$$\log|\partial_m \psi_j^{(i)}(B,0)| \leq C_0(v)\,|m| + C_1(v)$$

para $|m| \leq \deg f_V = (r+1)\,\delta$.

Consideramos en primer lugar el caso $v \in S_k$. Entonces se pueden tomar

$$\begin{aligned} C_1(v) \;&:=\; (r+1)(n+1)\,\overline{h}(V_i) + \overline{h}_v(J(V_i)^{-1}) + (r+1)(n+1)h_v \\ &\quad +3\,(r+1)(n+1)\,d + 2\,(r+1)^2(n+1)^2 + (r+1)\delta \end{aligned}$$

y $C_0(v) := 3C_1(v)$, por el corolario 1.3.3. Aquí J denota el Jacobiano del endomorfismo de $\mathbb{A}^r \times \mathbb{A}^{rn} \times \mathbb{A}^n$ definido por $x \mapsto (\varpi(x), F(x))$.

Sea $\alpha := \prod_{ij} \varrho_j^{(i)}(B) \in k^*$. Se tiene entonces

$$\begin{aligned} \log|f_V|_V \;&\leq\; ((C_1 + (r+1)(n+1) + 7\,(2r+1)\delta)\,r\,\delta + C_0 + \overline{h}_v(\alpha^{-1}))\,\delta \\ &\quad +(C_1 + (r+1)(n+1) + 4\,(2r+1)\,\delta)(r+1)\,\delta + \log|\lambda| \\ &\leq\; (C_1 + 2(n+1)\,\delta\,C_1 + 24\,(n+1)^3\,\delta^2 + \overline{h}_v(\alpha^{-1}))\,\delta + \log|\lambda| \end{aligned}$$

por el corolario 1.3.7 El caso $v \notin S_k$ se trata en forma análoga. Se tiene $\alpha = \prod_{j=1}^{\delta} \beta(E_i, B_i)$, y por lo tanto

$$-\log|\alpha| \leq \overline{h}(\alpha) \leq \delta \sum_v C_1(v).$$

Luego se tiene

$$h(f_V(U-B)) \leq \kappa_1\,\delta^2\,\overline{h}(V_i) + \kappa_2\,\delta^3 + \delta\cdot\overline{h}(\alpha)$$

por aplicación del lema 1.3.8. Aquí se tiene

$$\kappa_1 := 8(n+1)^3\,d, \qquad\qquad \kappa_2 := 8(n+1)^3(h+d+3(n+1)).$$

Se tiene además $\overline{h}_v(\alpha) \leq C_1(v)$ y por lo tanto

$$\overline{h}_v(\alpha) \leq \kappa_3\,\overline{h}(V_i) + \kappa_4\delta$$

con $\kappa_3 := 2(n+1)^2 d$ y $\kappa_4 := 2(n+1)^2(h+2d+3(n+1))$. Deducimos entonces

$$h(f_V(U-B)) \leq \kappa_5\,\delta^5\,\overline{h}(V_0) + \kappa_6\,\delta^6$$

por aplicación del lema 1.3.16. Aquí se tiene $\kappa_5 := 216\,(n+1)^4\,d^2$ y $\kappa_6 := 450\,(n+1)^4\,d$ $(h+2d+3n+3)$. Se tiene entonces

$$m(f_V) \leq \kappa_5\,\delta^5\,\overline{h}(V_0) + \kappa_6\,\delta^6 + 4(n+1)^3\delta.$$

Consideramos ahora el caso general. Sea $y \in k[x_1,\ldots,x_n]$ la forma lineal que se obtiene a partir del lema 1.3.15. Se tiene, en particular,

$$m(y) \leq (r+2)\log\delta + (n+1).$$

Sea entonces $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ una aplicación lineal inversible tal que $\varphi(y) = x_{r+1}$ y tal que $\varphi(x_i) = x_i$ para $i = 1, \ldots, r$. Se puede suponer $h(\varphi)$, $h(\varphi^{-1}) \leq 2(n+1)\delta$. Se tiene entonces

$$h(\varphi(V)) \leq \kappa_5\, \delta^5 \cdot \overline{h}(\varphi(V_0)) + \kappa_6\, \delta^6 \leq \kappa_5\, \delta^5 \cdot \overline{h}(V_0) + (\kappa_6 + 7(n+1))\, \delta^7$$

y por lo tanto

$$h(V) \leq \kappa_5\, \delta^5\, \overline{h}(V_0) + (\kappa_6 + 11(n+1)^2)\, \delta^7.$$

$\square$

1.3.4 Parametrizaciones

En esta subsección introducimos la noción de solución geométrica para una variedad de dimensión positiva. Esta noción es una forma débil de parametrización de variedades. Luego estudiamos la relación entre la altura de una variedad y la altura de su solución.

Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ una proyección lineal finita y separable. Sean $E := k(\mathbb{A}^r)$ y $F := E \otimes_k k[V]$. Luego F es una E–álgebra finita y separable de grado $\deg \pi \leq \delta$. Una forma lineal $\zeta \in k[x_1, \ldots, x_r]$ es un *elemento primitivo* de V con respecto a π si se tiene

$$F = E[\zeta].$$

Podemos interpretar esta noción en términos geométricos. La E–álgebra F es el anillo de coordenadas de una variedad 0–dimensional $V_F \subseteq \mathbb{A}^{n-r}(\overline{E})$. Luego una forma lineal $\zeta \in k[x_1, \ldots, x_r]$ es un elemento primitivo de V si y sólo si la proyección

$$V_F \to \mathbb{A}^1, \qquad\qquad x \mapsto \zeta(x)$$

separa los puntos de V_F, es decir, $\zeta(\xi) \neq \zeta(\varrho)$ para $\xi, \varrho \in V_F$, $\xi \neq \varrho$.

Introducimos ahora los aspectos básicos de teoría de dualidad algebraica que vamos a utilizar en lo que sigue. Nos restringimos por el momento al caso 1–dimensional. La referencia standard es el libro de Kunz [87]. Para el caso 1–dimensional referimos también al libro de Lang [88]. Tratamos el caso n–dimensinal en la subsección 2.3.1.

Sea A el anillo de polinomios $k[x_1, \ldots, x_r]$. Sea $A[t]$ el anillo de polinomios 1–variados con coeficientes en A y sea $P \in A[t]$ un polinomio separable de grado d. Consideramos entonces el A–álgebra

$$B := A[t]/(P).$$

Asumimos que la inclusión $A \hookrightarrow B$ es finita o, equivalentemente, que P es un polinomio mónico con respecto a t. Hacemos entonces

$$P(u) - P(t) = (u - t) \sum_{i=0}^{d-1} b_i(t)\, u^i$$

con $b_i \in A[t]$. Se tiene entonces

$$P' \cdot \overline{g} = \sum_i \operatorname{Tr}(\overline{g} \cdot \overline{b}_i)\, t^i$$

para $g \in A[t]$, donde P' denota la derivada de P con respecto a la variable t. Esta identidad es un caso particular de la fórmula de traza de Tate. Esta fórmula nos permita controlar la representación del elemento $\overline{P'} \cdot \overline{g}$ en la base $\{1, \ldots, t^{d-1}\}$.

Sea E el cuerpo de fracciones de A y $F := E \otimes_k B$. La fórmula de Tate se extiende por linealidad al caso $g \in E[t]$.

Sea C la clausura entera de A en F. Se tiene entonces

$$P' \cdot c = \sum_i \operatorname{Tr}(c \cdot \overline{b}_i)\, t^i$$

para $c \in C$. Luego se tiene $\operatorname{Tr}(c \cdot \overline{b}_i) \in A$, ya que A es integralmente cerrado. Obtenemos entonces la inclusión

$$P' \cdot c \subseteq B.$$

Introducimos ahora la noción de solución geométrica de una variedad. Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ un morfismo lineal finito y separable. Sea $\zeta \in k[x_1, \ldots, x_n]$ un elemento primitivo de V y sea $P \in k[\mathbb{A}^r][t]$ su polinomio minimal. La k–álgebra $k[V]$ es entera sobre $k[\mathbb{A}^r]$ y por lo tanto se tiene

$$P' \cdot k[V] \subseteq k[A^r][\zeta].$$

Sea $\rho := \operatorname{discr}(P) \in k[\mathbb{A}^r] - \{0\}$ el discriminante de P. Luego P' divide a ρ en $k[\mathbb{A}^r][t]$ y por lo tanto

$$\rho \cdot k[V] \subseteq k[A^r][y].$$

En particular se tiene $k[V]_\rho = k[A^r][y]_\rho$. En términos geométricos, la proyección

$$\psi : V \to \mathbb{A}^{r+1}, \qquad x \mapsto (\varphi(x), \zeta(x)),$$

es un isomorfismo de V en la hipersuperficie $V(P) \subseteq \mathbb{A}^{r+1}$ en el abierto $\{\rho \neq 0\}$. Sean $v_i \in k[A^r][t]$ tales que

$$\rho \cdot x_i = v_i(\zeta), \qquad \deg^{(t)} v_i \leq d - 1,$$

para $i = 1, \ldots, n$. Los polinomios v_i son las *parametrizaciones* de V con respecto a π y a ζ. Sea $I(V) \subseteq k[x_1, \ldots, x_n]$ el ideal de definición de V. Luego se tiene

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

Equivalentemente, el morfismo

$$\varphi : V(P)_\rho \to V_\rho, \qquad y \mapsto (v_1, (y)/\rho(y), \ldots, v_n(y)/\rho(y))$$

es la inversa de la proyección ψ en el abierto $\{\rho \neq 0\}$. El morfismo φ representa una forma débil de parametrización de la variedad V.

Notamos que el sistema de polinomios $P, v_1, \ldots, v_n$ está unívocamente determinado por la variedad V, la proyección π, y el elemento primitivo ζ. Este sistema de polinomios es la *solución geométrica* de la variedad V asociada a π y ζ.

El siguiente resultado muestra la existencia de una proyección lineal π y un elemento primitivo ζ de baja altura.

Lema 1.3.18 *Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional de dimensión r y grado δ. Entonces existe una proyección $\pi : V \to \mathbb{A}^r$ finita y separable, y un elemento primitivo ζ de V con respecto a π tales que $h(\pi)$, $h(\zeta) \leq 2 \log \delta$.*

Demostración. Sea $P_V \in k[U, T]$ el polinomio característico de V y sea

$$P_V = a_\delta \, t^\delta + \cdots + a_0$$

su desarrollo con respecto a la variable $t := T_{r+1}$. Sea $\rho := \operatorname{discr}(P)$ el discriminante de P_V con respecto a t. Sea $B \in k^{(r+1)(n+1)}$ tal que

$$a_\delta \cdot \rho\,(B) \neq 0.$$

Luego las formas lineales $y_i := \eta_i\,(B_i) = B_{i0} + B_{i1} x_1 + \cdots + B_{in}$ determinan una proyección $\pi := (y_1, \ldots, y_r)$ finita y separable y un elemento primitivo $\zeta := y_{r+1}$.

Los polinomios a_δ, ρ son no nulos de grado acotado por δ y $\delta^2 - \delta$ respectivamente, en cada grupo de variables U_i. Luego B se puede tomar de altura acotada por $2 \log \delta$. $\square$

En lo que sigue estudiamos la relación entre la altura de una variedad y la altura de su solución geométrica. El siguiente resultado muestra que la altura de la solución geométrica está acotada — polinomialmente — por la altura de la variedad.

Proposición 1.3.19 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es finita y separable y que $\zeta := x_{r+1}$ es un elemento primitivo de V. Sean $P, v_1, \ldots, v_n \in k[\mathbb{A}^r][t]$ el polinomio minimal de ζ y las parametrizaciones de V, respectivamente. Entonces*

$$\begin{aligned}
\deg P &\leq \delta, \\
\deg v_i &\leq 2\,\delta^2, \\
m(P) &\leq h(V) + c_1 \delta, \\
\overline{m}(v_i) &\leq c_2\,\delta^4\,h(V) + c_3\,\delta^6,
\end{aligned}$$

donde c_1, c_2, c_3 sólo dependen de n.

Se pueden tomar $c_1 := 5(n+1)^2 \log(n+1)$, $c_2 := 14(n+1)^2 \log(n+1)$ y $c_3 := 10^2 (n+1)^4$.

Demostración. El polinomio P es la ecuación de la proyección $V \to \mathbb{A}^{r+1}$ y por lo tanto $\deg P \leq \delta$. Se tiene además

$$h(P) \leq h(V) + 5(r+1)^2 \log(n+1)\delta$$

por la proposición 1.2.11.

Ahora estimamos el grado y la altura de las parametrizaciones por medio de la fórmula de traza Tate. Sea $P(t) = \sum_{i=0}^{d} a_i\, t^i$. Se tiene

$$P(u) - P(t) = (u-t) \sum_{i=0}^{\delta-1} b_i(u)\, t^i$$

con $b_i = \sum_{j=i}^{\delta} a_j\, u^{j-i}$. Luego se tiene $\deg b_i = \delta - i$ y $m(b_i) \leq m(P) + \delta \log(n+1)$. Por otra parte, sea $\rho := \operatorname{discr}(P)$ el discriminante de P, y sea $\varrho \in k[\mathbb{A}^r][t]$ tal que $\rho = P' \cdot \varrho$. Luego se tiene

$$v_j = \varrho \sum_i \operatorname{Tr}(x_j \cdot \overline{b}_i)\, t^i.$$

Se tiene $\deg \varrho = \delta^2 - 2\delta$ y $\deg \operatorname{Tr}(x_j \cdot \overline{b}_i) \leq \delta(\delta - i + 1)$ y por lo tanto $\deg v_j \leq 2\,\delta^2$. En cuanto a las estimaciones de altura, se tiene

$$\begin{aligned} m(\operatorname{Tr}(x_j \cdot \overline{b}_i)) &\leq c_1\, \delta^4\, h(V) + c_2\, \delta^6 + c_3\, \delta \cdot h(P) \\ &\leq (c_1 + 6(n+1)^2 \log(n+1))\delta^4\, h(V) + c_2\, \delta^6 \end{aligned}$$

donde c_1, c_2 son las constantes de la proposición 1.3.13. Se tiene además

$$\begin{aligned} m(\varrho) &\leq m(\varrho) \leq 2\,\delta(m(P) + 3\delta \log(n+1) + 2\log \delta) \\ &\leq 2\,\delta \cdot h(V) + 12\,\delta^2 \log(n+1). \end{aligned}$$

Concluimos entonces

$$\begin{aligned} m(v_j) &\leq m(\varrho) + \max_i m(\operatorname{Tr}(x_j \cdot \overline{b}_i)) + \delta^2 \log(n+1) + \log \delta \\ &\leq c_2\, \delta^4\, h(V) + c_3\, \delta^6 \end{aligned}$$

con $c_2 := 14(n+1)^2 \log(n+1)$ y $c_3 := 97(n+1)^4$. □

La noción de solución geométrica permite introducir una definición alternativa de altura de una variedad de dimensión positiva.

Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional de dimensión r y grado δ. Sea $(P, v_1, \ldots, v_n)$ la solución geométrica de V con respecto a una proyección finita y separable $\pi : V \to \mathbb{A}^r$ y un elemento primitivo ζ. Luego se define la *altura* de V con respecto a π y a ζ como

$$\eta(V, \pi, \zeta) := h(P, v_1, \ldots, v_n).$$

Para una variedad V fija, esta noción de altura es una *función*, y no un único parámetro. Se puede obtener un único parámetro asociado a V, definiendo su *altura* η como

$$\eta(V) := \max_{\pi, \zeta} \eta(V, \pi, \zeta)$$

donde $\pi : V \to \mathbb{A}^r$ es una proyección finita y separable y ζ es un elemento primitivo tales que

$$h(\pi), h(\zeta) \leq \kappa \log \delta$$

para una constante universal κ suficientemente grande que asegure que efectivamente existan π y ζ que satisfagan estas condiciones. El lema 1.3.18 muestra que se puede tomar $\kappa := 2$. Esta noción de altura fue introducida por Giusti et al. [54] para el caso en que V es intersección completa reducida Notamos que se extiende sin modificaciones esenciales al caso general.

En lo que sigue vamos a probar que esta noción de altura es polinomialmente equivalente a la noción de altura definida a partir del polinomio de Chow. El resto de esta sección está dedicado a la demostración de este resultado. Mostramos en primer lugar que esta noción de altura de una fibra de π.

Lema 1.3.20 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es finita y separable, que $0 \in \mathbb{A}^r$ es un punto no ramificado de π, y que $\zeta := x_{r+1}$ es un elemento primitivo de V. Entonces*

$$h(\pi^{-1}(0)) \leq 4\,\delta^2\,\eta(V, \pi, \zeta) + 4\,\delta^3.$$

Demostración. Sea $V_0 := \pi^{-1}(0)$ la fibra del punto $0 \in \mathbb{A}^r$ y sea $\xi = (\xi_1, \ldots, \xi_n) \in V_0$. Sea $P \in k[x_1, \ldots, x_r][t]$ el polinomio minimal de ζ. Luego se tiene $P(0, \ldots, 0, \xi_{r+1}) = 0$ y por lo tanto

$$\overline{h}(\xi_{r+1}) \leq \eta + \log \delta.$$

Para $r + 2 \leq i \leq n$ denotamos por v_i la parametrización de x_i, y sea $\rho := \mathrm{discr}(P)$ el discriminante de P. Luego se tiene

$$\xi_i = v_i(0)(\xi_{r+1})/\rho(0)$$

y por lo tanto

$$\begin{aligned} \overline{h}(\xi_i) &\leq \overline{h}(v_i(0)(\xi_{r+1})) + \overline{h}(\rho(0)) \leq \eta + 2\,\delta^2(\eta + \log \delta) + \log 2\,\delta^2 + \eta \\ &\leq 4\,\delta^2 \cdot \eta + 4\,\delta^3. \end{aligned}$$

□

Lema 1.3.21 *Sea $V \subseteq \mathbb{A}^n$ una variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es finita y separable y que $\zeta := x_{r+1}$ es un elemento primitivo de V. Entonces existe una intersección completa reducida $F = \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ que define una variedad $V(F) \subseteq \mathbb{A}^n$ que contiene a V tal que*

$$\deg F_i \leq \delta, \qquad\qquad m(F_i) \leq c_1\,\delta^3 \cdot \eta(V) + c_2\,\delta^4,$$

donde c_1, c_2 dependen solamente de n.

Se pueden tomar $c_1 := 3$ y $c_2 := 12\log(n+1)$.

Demostración. La demostración de este resultado es análoga a la del lema 1.3.11. Tomamos a F_i como la ecuación de la proyección $V \to \mathbb{A}^{r+1}$ definida por $x \mapsto (\pi(x), x_i)$.

Sea $E := k(\mathbb{A}^r)$ y sea $F := E \otimes k[V]$. Luego F es una $E-$álgebra de dimensión $D := \deg \pi \leq \delta$. Sea $M = (M_{ij})_{ij} \in k^{D\times D}$ la matriz de la aplicación $L_\zeta : F \to F$ en la base $\{1, \ldots, \zeta_0^{D-1}\}$. Sea v_i la parametrización de x_i y sea ρ el discriminante del polinomio minimal P de ζ. Luego

$$N_i := v_i(M)/\rho$$

es la matriz de la aplicación $L_{x_i} : F \to F$. Sea $\chi_i \in k[\mathbb{A}^r][t]$ el polinomio característico de N_i. Luego la ecuación F_i es un factor de χ.

Se tiene $\deg M_{ij} \leq \delta$ y $\overline{m}(M_{ij}) \leq \eta + \delta \log(n+1)$. Luego $\deg v_i(M) \leq 2\delta^3$ y

$$\begin{aligned} \overline{m}(v_i(M)) &\leq m(v_i) + 2\,\delta^2(\max_{ij} \overline{m}(M_{ij}) + \log(r+1) + \delta \log(r+1)) \\ &\leq 3\,\delta^2 \cdot \eta + 8\log(n+1)\delta^3. \end{aligned}$$

Luego se tiene

$$\begin{aligned} m(F_i) &\leq \overline{m}(\chi) \leq \delta\,(3\,\delta^2\,\eta + 8\log(n+1)\,\delta^3 + (2\,\delta^3+1)\log(n+1) + \log\delta) \\ &\leq 3\,\delta^3\,\eta + 12\,\log(n+1)\,\delta^4. \end{aligned}$$

□

Corolario 1.3.22 *Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional de dimensión r y grado δ. Sea $\pi : V \to \mathbb{A}^r$ la proyección $x \mapsto (x_1, \ldots, x_r)$. Asumimos que π es finita y separable de grado δ, y que $0 \in \mathbb{A}^r$ es un punto no ramificado de V. Asumimos además que $\zeta := x_{r+1}$ es un elemento primitivo de V. Entonces*

$$\begin{aligned} \eta(V, \pi, \zeta) &\leq c_1\,\delta^4\,h(V) + c_2\,\delta^6, \\ h(V) &\leq c_3\,\delta^{12}\,\eta(V, \pi, \zeta) + c_4\,\delta^{13} \end{aligned}$$

donde c_1, c_2, c_3, c_4 dependen solamente de n.

Se pueden tomar $c_3 := 2\cdot 10^3\,(n+1)^4$ y $c_4 := 5\cdot 10^3\,(n+1)^5$.

Demostración. La primera parte se sigue directamente de la proposición 1.3.19. Consideramos entonces la segunda estimación.

Sea $F = \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ una intersección completa reducida que define una variedad $W := V(F) \subseteq \mathbb{A}^n$ que contiene a V. Sean $d := \deg F$ y $h := h(F)$. Luego se tiene

$$h(V) \leq 4\,c_1\,\delta^7\,\eta(V, \pi, \zeta) + (4\,c_1 + c_2)\,\delta^8$$

por aplicación del lema anterior y del teorema 1.3.14. Aquí c_1, c_2 son las constantes que intervienen en el enunciado del teorema 1.3.14. Se tiene entonces

$$h(V) \leq c_3\,\delta^{12} \cdot \eta(V, \pi_0, \zeta_0) + c_4\,\delta^{13}$$

con $c_3 := 2\cdot 10^3\,(n+1)^4$ y $c_4 := 5\cdot 10^3\,(n+1)^5$. □

Este resultado nos permite concluir que h y η son polinomialmente equivalentes, es decir

$$\eta(V) \leq (n\,\delta \cdot h(V))^{c_1}, \qquad\qquad h(V) \leq (n\,\delta \cdot \eta(V))^{c_2}$$

donde $c_1\,,\ c_2 \geq 0$ son constantes universales.

Teorema 1.3.23 *Sea $V \subseteq \mathbb{A}^n$ variedad equidimensional de dimensión r y grado δ. Entonces*

$$\eta(V) \leq c_1\,\delta^4\,h(V) + c_2\,\delta^6, \qquad\qquad h(V) \leq c_3\,\delta^{12}\,\eta(V) + c_4\,\delta^{13},$$

donde $c_1\,,\ c_2\,,\ c_3\,,\ c_4$ sólo dependen de n.

Se pueden tomar $c_1 := 14\,(n+1)^2 \log(n+1)\,,\ c_2 := 2 \cdot 10^2\,(n+1)^7\,,\ c_3 := 2 \cdot 10^3\,(n+1)^4$ y $c_4 := 10^4\,(n+1)^5$.

Demostración. Sea $\pi : V \to \mathbb{A}^r$ una proyección lineal finita y separable y sea ζ un elemento primitivo de V. Asumimos además $h(\pi), h(\zeta) \leq 2\,\log\delta$.

Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ una aplicación lineal inversible tal que $\pi = (\varphi_1, \ldots, \varphi_r)$ y $\zeta = \varphi_{r+1}$. Podemos asumir entonces $h(\varphi) \leq 2\,\log\delta$, y por lo tanto, $h(\varphi^{-1}) \leq 2\,n\,\log\delta + n\,\log n$.

Sea $p \in \mathbb{A}^r$ un punto no ramificado de la proyección

$$\varphi^{-1}(V) \to \mathbb{A}^r, \qquad\qquad x \mapsto (x_1, \ldots, x_r).$$

Por la proposición 1.3.9 podemos asumir $h(p) \leq n\,\log\delta + 2n$. Sea entonces $\tau : \mathbb{A}^n \to \mathbb{A}^n$ la traslación $x \mapsto x + p$, y sea $\phi := \tau \circ \varphi$. Sea $W := \phi^{-1}(V) \subseteq \mathbb{A}^n$. Luego la proyección

$$\pi_0 : W \to \mathbb{A}^r, \qquad\qquad x \mapsto (x_1, \ldots, x_r)$$

es finita y separable, $0 \in \mathbb{A}^r$ es no ramificado y $\zeta_0 := x_{r+1}$ es un elemento primitivo de W.

Se tiene $\phi^{-1} = \varphi^{-1} - \varphi^{-1} \circ \tau$ y por lo tanto $h(\phi) \leq 2\,n\,\log\delta + 2n$ y $h(\phi^{-1}) \leq 4\,n\ \log\delta + 2\,n\,\log n$. Luego se tiene

$$\eta(W, \pi_0, \zeta_0) \leq \eta(V, \pi, \zeta) + h(\phi^{-1}) \leq \eta(V, \pi, \zeta) + 4\,n\,\log\delta + 2n$$

y

$$h(W) \leq h(V) + 5\,(n+1)^2\,(4\,\log\delta + 7\log n + 1)\,\delta.$$

Por lo tanto

$$\begin{aligned} \eta(V, \pi, \zeta) &\leq \eta(W, \pi, \zeta) + 2\,n\,\log\delta + 2\,n \\ &\leq c_1\,\delta^4\,h(W) + c_2\,\delta^6 + 2\,n\,\log\delta + 2\,n \\ &\leq c_5\,\delta^4\,h(V) + c_6\,\delta^6 \end{aligned}$$

donde $c_1\,,\ c_2\,,$ son las constantes que intervienen en el enunciado del corolario 1.3.22. Se pueden tomar $c_5 := 14(n+1)^2 \log(n+1)$ y $c_6 := 130(n+1)^7$.

Por otra parte, la hipótesis $h(\pi) \leq 2\log\delta$ nos permite suponer sin pérdida de generalidad $\deg\pi = \delta$. Luego podemos aplicar el teorema 1.3.14 y nos queda entonces

$$\begin{aligned} h(V) &\leq h(W) + (r+1)(2\log\delta + 7(r+1)\log(n+1))\,\delta \\ &\leq c_3\,\delta^{12}\,\eta(W,\pi_0,\zeta_0) + c_4\,\delta^{13} + (r+1)(2\log\delta + 7(r+1)\log(n+1))\,\delta \\ &\leq c_7\,\delta^{12}\,\eta(V) + c_8\,\delta^{13} \end{aligned}$$

donde c_3, c_4 son las constantes que intervienen en el enunciado del corolario 1.3.22. Se pueden tomar $c_7 := 2\cdot 10^3(n+1)^4$ y $c_8 := 10^4(n+1)^5$. □

1.4 Aplicaciones

Los resultados de la sección anterior muestran la estrecha relación existente entre la altura de una variedad y la altura de una fibra de una proyección finita. Estos resultados permiten reducir el estudio de la altura de una variedad al estudio de la altura de una fibra 0–dimensional.

En esta sección aplicamos estos resultados en diversas situaciones. La aplicación más notoria es la desigualdad de Bézout aritmética (Teorema 1.4.4). Obtenemos además una estimación para la altura de la inversa de un morfismo birracional de una variedad en un espacio afín (Proposición 1.4.7, 1.4.8).

1.4.1 Una Desigualdad de Bézout Aritmética

Esta subsección está dedicada a la demostración de la desigualdad de Bézout aritmética y a la derivación de algunas de sus consecuencias. En primer lugar estimamos la altura del producto de variedades.

Lema 1.4.1 *Sean $V \subseteq \mathbb{A}^m$, $W \subseteq \mathbb{A}^n$ variedades de dimensión 0. Entonces*

$$h(V\times W) \leq \deg(W)\cdot h(V) + \deg(V)\cdot h(W) + c(m,n)\,\deg(V)\cdot\deg(W).$$

Se puede tomar $c(m,n) := \log(m+1) + \log(n+1)$.

Demostración. Sean

$$\begin{aligned} \zeta &:= U_0 + U_1\,y_1 + \cdots U_m\,y_m \in k[U][\mathbb{A}^m], \\ \eta &:= U_1'\,x_1 + \cdots + U_n'\,x_n \in k[U'][\mathbb{A}^n] \end{aligned}$$

formas lineales genéricas. Luego

$$F := \prod_{\xi\in V}\prod_{\rho\in W}(\zeta(\xi) + \eta(\rho)) \in k[U,U'][\mathbb{A}^m\times\mathbb{A}^n]$$

es el polinomio de Chow de $V\times W$. Luego se tiene

$$F = \prod_{\xi\in V} f_W(\zeta(\xi), U_1',\ldots,U_n').$$

Sean $\delta := \deg V$ y $\delta' := \deg W$. Luego

$$\begin{array}{rcl} m(F) & = & \sum_\xi m(f_W(\zeta(\xi), U'_1, \ldots, U'_n)) \\ & \leq & \sum_\xi m(f_W) + \delta' \left(m(\zeta(\xi)) + \log(m+1) + \log(n+1) \right) \\ & \leq & \delta \cdot m(f_W) + \delta' \cdot m(F_V) + (\log(m+1) + \log(n+1)) \delta \cdot \delta'. \end{array}$$

$\square$

Corolario 1.4.2 *Sean* $V_1 \subseteq \mathbb{A}^{n_1}, \ldots, V_l \subseteq \mathbb{A}^{n_l}$ *variedades de dimensión 0. Sea* δ_i *el grado de* V_i. *Sean* $n := \sum n_i$ *y* $\delta := \prod_i \delta_i$. *Entonces*

$$h(V_1 \times \cdots \times V_l)/\delta \leq \sum_i h(V_i)/\delta_i + 2\, l\, \log(n+1).$$

$\square$

.

Proposición 1.4.3 *Sean* $V_1 \subseteq \mathbb{A}^{n_1}, \ldots, V_l \subseteq \mathbb{A}^{n_l}$ *variedades. Sea* δ_i *el grado de* V_i. *Sean* $n := \sum_i n_i$ *y* $\delta := \prod_i \delta_i$. *Entonces*

$$h(V_1 \times \cdots \times V_l) \leq c_1\, \delta^8 \sum_i h(V_i) + c_2\, \delta^9$$

donde c_1, c_2 *dependen solamente de* n.

Se pueden tomar $c_1 := 10^3\,(n+1)^4$ y $c_2 := 2 \cdot 10^3\,(n+1)^7$.

Demostración. Es suficiente considerar el caso en que V_i es irreducible para todo i. Sea r_i la dimensión de V_i. Sean $F_{ij} \in k[x_1^{(i)}, \ldots, x_{n_i}^{(i)}]$ polinomios tales que $F_i := \{F_{i,r_i+1}, \ldots, F_{i,n_i}\}$ es una intersección completa reducida que define una variedad $W_i := V(F_i) \subseteq \mathbb{A}^{n_i}$ que contiene a V_i. Asumimos además

$$\deg F_{ij} \leq \delta_i, \qquad\qquad m(F_{ij}) \leq h(V_i) + c_1\, \delta_i,$$

con $c_1 := 5\,(n+1)^2 \log(n+1)$. Luego $F := \{F_{ij}\}_{ij} \subseteq k[x_1, \ldots, x_n]$ es una intersección completa reducida tal que la variedad $W := V(F) = W_1 \times \cdots \times W_l \subseteq \mathbb{A}^n$ contiene a $V := V_1 \times \cdots \times V_l$. Se tiene

$$\deg F_{ij} \leq \max_i \delta_i, \qquad\qquad m(F_i) \leq \max_i h(V_i) + c_1 \max_i \delta_i.$$

Sea $\pi_i : V_i \to \mathbb{A}^{r_i}$ una proyección finita y separable de grado δ_i tal que $0 \in \mathbb{A}^{r_i}$ un punto no ramificado de π_i. Asumimos

$$h(\pi_i) \leq c_2(n_i) \log \delta_i + c_3(n_i)$$

con $c_2(n) := n$ y $c_3(n) := 2n$. Sea $r := \sum_i r_i = \dim V$. Luego la proyección $\pi := \pi_1 \times \cdots \pi_l : V \to \mathbb{A}^r$ es finita y separable de grado δ y $0 \in \mathbb{A}^r$ es un punto no ramificado de π. Se tiene además

$$h(\pi) \le c_2(n) \log(\max_i \delta_i) + c_3(n).$$

Sea $\varpi_i : \mathbb{A}^{n_i} \to \mathbb{A}^{r_i}$ la proyección $x \mapsto (x_1, \ldots, x_{r_i})$, y sea $\varphi_i : \mathbb{A}^{n_i} \to \mathbb{A}^{n_i}$ una transformación afín inversible tal que $\varpi_i = \pi_i \circ \varphi_i$. Podemos suponer entonces

$$h(\varphi_i) \le h(\pi_i), \qquad\qquad h(\varphi_i^{-1}) \le n_i\, h(\pi_i) + n_i \log n_i.$$

Sea $Z_i := \varphi_i^{-1}(V) \subseteq \mathbb{A}^{n_i}$, y sean

$$\begin{aligned} \varphi &:= \varphi_1 \times \cdots \times \varphi_l : \mathbb{A}^n \to \mathbb{A}^n, \\ Z &:= Z_1 \times \cdots \times Z_l = \varphi^{-1}(V) \subseteq \mathbb{A}^n. \end{aligned}$$

Se tiene entonces

$$h(Z_i) \le h(V_i) + 7(n_i+1)^3\, \delta_i^2.$$

Sea $Z_{i0} := \varpi_i^{-1}(0) \subseteq \mathbb{A}^{n_i}$ la fibra de ϖ_i en 0 y sea $Z_0 := Z_{1,0} \times \cdots \times Z_{l,0} = \varpi^{-1}(0) \subseteq \mathbb{A}^n$ la fibra de $\varpi := \varpi_1 \times \cdots \times \varpi_l$ en $0 \in \mathbb{A}^n$. Luego

$$h(Z_{i0}) \le h(Z_i) + (n_i+1)^3\, \delta_i \le h(V_i) + 8(n_i+1)^3\, \delta_i^2.$$

Por el lema 1.4.1 obtenemos entonces

$$h(Z_0) \le \delta \sum_i h(Z_{i0}) + 2\, l \log(n+1)\, \delta \le \delta \sum_i h(V_i) + 10\, l(n+1)^3\, \delta^2.$$

Se sigue entonces

$$\begin{aligned} h(V) &\le h(Z) + 8(n+1)^3\, \delta \le \kappa_1\, \delta^5 \cdot h(Z_0) + \kappa_2\, \delta^7 + 8(n+1)^3\, \delta^2 \\ &\le \kappa_1\, \delta^6 \textstyle\sum_i h(V_i) + (10\, l(n+1)^3\, \kappa_1 + \kappa_2 + 8(n+1)^3)\, \delta^7 \end{aligned}$$

por el teorema 1.3.14 donde κ_1, κ_2 son las constantes que intervienen en el enunciado de este teorema. Concluimos entonces

$$h(V) \le c_4\, \delta^8 \sum_i h(V_i) + c_5\, \delta^9$$

con $c_4 := 10^3\, (n+1)^4$ y $c_5 := 2 \cdot 10^3\, (n+1)^7$. □

Teorema 1.4.4 *(Desigualdad de Bézout Aritmética) Sean $V_1, \ldots, V_l \subseteq \mathbb{A}^n$ variedades. Sea δ_i el grado de V_i y sea $\delta := \prod_i \delta_i$. Entonces*

$$h(V_1 \cap \cdots \cap V_l) \le c_1\, \delta^8 \sum h(V_i) + c_2\, \delta^9$$

donde c_1, c_2 dependen solamente de n.

De hecho se pueden tomar $c_1 := 10^3\, (n+1)^4$ y $c_2 := 2 \cdot 10^3\, (n+1)^7$.

Demostración. Esta estimación se sigue directamente de la proposición 1.4.3 y de la identidad

$$V_1 \cap \cdots \cap V_l = (V_1 \times \cdots \times V_l) \cap E \subseteq E$$

donde $E \cong \mathbb{A}^n$ es el espacio lineal $\{x_{1,1} - x_{2,1} = 0, \ldots, x_{1,n} - x_{l,n} = 0\} \subseteq \mathbb{A}^{l\,n}$. □

Como un caso particular de este resultado, obtenemos la siguiente estimación para la altura de la intersección de una variedad con una hipersuperficie.

Corolario 1.4.5 *Sea* $V \subseteq \mathbb{A}^n$ *variedad de grado* δ *y sean* $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ *polinomios de grado acotado por* d *y medida de Mahler acotada por* h *. Entonces*

$$h(V \cap V(f_1, \ldots, f_s)) \leq c_1\,(d^s\,\delta)^8\,(h + h(V)) + c_2\,(d^s\,\delta)^9.$$

Se pueden tomar $c_1 := 10^3\,(n+1)^5$ y $c_2 := 2 \cdot 10^3\,(n+1)^7$.

Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polinomios que definen una variedad $V := V(f_1, \ldots, f_s) \subseteq \mathbb{A}^n$ de dimensión 0. Se tiene en particular

$$w(V) \leq c_1(n)\,d^{8\,n}\,h + c_2(n)\,d^{9\,n}$$

donde $w(V) := \sum_{\xi \in V} \overline{h}(\xi)$ denota la altura de Weil de V y c_1 , c_2 sólo dependen de n .

Obtenemos la siguiente estimación para la altura de la imagen de una variedad por un morfismo.

Lema 1.4.6 *Sea* $V \subseteq \mathbb{A}^n$ *una variedad y sea* $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ *un morfismo racional. Sean* f_i *,* $g_i \in k[x_1, \ldots, x_n]$ *polinomios tales que* $\varphi = (f_1/g_1, \ldots, f_m/g_m)$ *. Sean* $d := \max_i\{\deg f_i, \deg g_i + 1\}$ *y* $h := \max_i \overline{h}(f_i/g_i)$ *. Entonces*

$$h(\overline{\varphi(V)}) \leq c_1\,(d^m\,\delta)^8 (h + h(V)) + c_2\,(d^m\,\delta)^9$$

donde c_1 *,* c_2 *dependen solamente de* n *.*

Se pueden tomar $c_1 := 10^3\,(n+1)^5$ y $c_2 := 3 \cdot 10^3 (n+1)^7$.

Demostración. Sea $\mathrm{Gr}(\varphi) \subseteq \mathbb{A}^n \times \mathbb{A}^m$ el gráfico de $\varphi : V \to \mathbb{A}^m$. Luego

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

y por lo tanto $\varphi(V) = \pi(\mathrm{Gr}(\varphi))$, donde $\pi : \mathbb{A}^n \times \mathbb{A}^m$ denota la proyección $(x, y) \mapsto y$. Luego se tiene $m(g_i\,x_i - f_i) \leq h + d + n + 2$ y por lo tanto

$$h(\overline{\varphi(V)}) \leq c_1\,(d^m\,\delta)^8 (h + h(V)) + c_2\,(d^m\,\delta)^9.$$

con $c_1 := 10^3\,(n+1)^5$ y $c_2 := 3 \cdot 10^3 (n+1)^7$. □

1.4.2 Inversa de un Morfismo Birracional

Sea $\varphi : V \to \mathbb{A}^r$ un morfismo birracional entre una variedad equidimensional $V \subseteq \mathbb{A}^n$ y un espacio afín $\mathbb{A}^r$. La siguiente es una estimación para la altura de la inversa de φ.

Proposición 1.4.7 *Sea $V \subseteq \mathbb{A}^n$ una variedad y sea $\varphi : V \to \mathbb{A}^r$ un morfismo birracional. Sean f_i, $g_i \in k[x_1, \ldots, x_n]$ tales que $\varphi = (f_1/g_1, \ldots, f_r/g_r)$. Sean $\delta := \deg V$, $d := \max_i\{\deg f_i, \deg g_i + 1\}$ y $h := \max_i h(f_i/g_i)$. Entonces*

$$h(\varphi^{-1}) \leq c_1\,(d^r \cdot \delta)^8 (h + h(V)) + c_2\,(d^r\,\delta)^9$$

donde c_1, c_2 dependen solamente de n.

Se pueden tomar $c_1 := 10^3\,(n+1)^5$ y $c_2 := 3 \cdot 10^3 (n+1)^7$.

Demostración. Sea $\varphi^{-1} := \psi = (h_1/k_1, \ldots, h_n/k_n)$ con h_i, $k_i \in k[x_1, \ldots, x_r]$ polinomios sin factores comunes. Se tiene

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

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

$$\begin{aligned} h(h_i/k_i) &\leq m(k_i\,x_i - h_i) + d\,\log(r+1) \\ &\leq c_1\,(d^r \cdot \delta)^8 (h + h(V)) + c_2\,(d^r \cdot \delta)^9 \end{aligned}$$

donde $k_i\,x_i - h_i$ es un polinomio irreducible y el gráfico de ψ coincide con el gráfico de φ. Aquí c_1, c_2 denotan las constantes que intervienen en la desigualdad de Bézout.

□

En el caso particular en que $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ es un automorfismo podemos obtener una estimación para la altura de la inversa directamente a partir de los resultados de la subsección 1.3.1. φ.

Proposición 1.4.8 *Sea $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ un automorfismo de $\mathbb{A}^n$, y sea $\psi := \varphi^{-1}$ su inversa. Sea $d := \max_i \deg \varphi_i$ y $h := \max_i h(\varphi_i)$. Entonces*

$$h(\psi) \leq 8\,n\,d^n (h + d\,\overline{h}(\xi)) + 4\,d^{2\,n} + 36\,d\,n^2\,d^{n+1},$$

donde $\xi := \varphi^{-1}(0)$ denota la fibra del punto $0 \in \mathbb{A}^n$.

Demostración. Sea $\psi = (g_1, \ldots, g_n)$ con $g_i \in k[x_1, \ldots, x_n]$. Se tiene $\deg g_i \leq d^n$ por el lema 1.2.2. Luego

$$h_v(\psi) \leq (3\,d^n + 1)(n\,d \cdot h_v(\xi) + \overline{h}_v(J_\varphi\,(\xi)^{-1}) + n\,h_v + 3n\,d + 2\,n^2 + d^n)$$

para $v \in S_k$, donde $h_v := h_v(\varphi)$, $\xi := \varphi^{-1}(0)$ y J_φ denota el Jacobiano de φ. Análogamente

$$h_v(\psi) \le (3\,d^n + 1)(n\,d \cdot \overline{h}_v(\xi) + \overline{h}_v(J_\varphi(\xi)^{-1}) + n\,d\,h_v)$$

en el caso $v \notin S_k$. Se tiene entonces

$$h(\psi) \le 4\,d^n(n\,d\,\overline{h}(\xi) + \overline{h}(J_\varphi(\xi)^{-1}) + n\,h + 3\,n\,d + 2\,n^2 + d^n).$$

Por otra parte, se tiene además $\overline{h}(J_\varphi(\xi)^{-1}) \le n\,d\,\overline{h}(\xi) + n(h + d + 3\,n)$. Concluimos

$$h(\psi) \le 4\,d^n(2\,n\,d \cdot \overline{h}(\xi) + 2\,n\,h + 36\,n^2\,d + d^n).$$

$\square$

La altura de la fibra ξ se puede estimar como

$$\overline{h}(\xi) \le c_1\,d^{8\,n}\,h + c_2\,d^{9\,n},$$

donde c_1 , c_2 son las constantes que intervienen en el enunciado del corolario 1.4.5. A partir del resultado anterior obtenemos la estimación

$$h(\psi) \le c_3\,d^{9\,n+1}\,h + c_4\,d^{10\,n+1}$$

con $c_3 := 5 \cdot 10^3\,(n+1)^6$ y $c_4 := 10^4\,(n+1)^7$.

Capítulo 2

Cotas para el Teorema de Ceros

Nuestro tratamiento del teorema de ceros se basa principalmente en dos técnicas. Cada una de estas técnicas se aplica en distintas situaciones, y son, en gran medida, complementarias entre sí.

La primera técnica fue desarrollada por Dubé [41] y el autor [122], [123]. Se trata de un método combinatorio. La idea principal consiste en trasladar el problema en cuestión al espacio proyectivo $\mathbb{P}^n$ — visto como una completación del espacio afín — para luego deformar las ecuaciones adecuadamente. De esta forma se reduce el problema al caso en que las ecuaciones se cortan en forma propia, que se resuelve fácilmente aplicando técnicas clásicas de eliminación.

Este método es eficiente con respecto a las cotas de grado. Por otra parte, es aplicable sobre anillos más generales que el anillo de polinomios. Este último aspecto es crucial para la obtención de las versiones ralas del teorema de ceros.

La segunda técnica se basa en ideas de Jacobi sobre dualidad en anillos intersección completa reducida. La ventaja más sobresaliente de este método es que permite obtener identidades *explícitas* para los polinomios en el teorema de ceros. Esto permite controlar otros parámetros — además del grado — y ya fue aplicado con éxito para controlar la altura y la complejidad de evaluación de los polinomios en el teorema de ceros [59], [48], [83], [62], etc..

Aplicamos este método para obtener cotas de altura esencialmente óptimas para el teorema de ceros sobre variedades intersección completa (Teorema 2.3.2). Este resultado nos permite obtener cotas inferiores para la aproximación entre variedades de dimensión positiva.

2.1 Cotas de Grados

En esta sección tratamos las cotas de grado para los polinomios en el teorema de ceros.

En primer lugar consideramos las versiones efectivas del teorema de ceros sobre anillos Cohen–Macaulay (Teorema 2.1.8 y Corolario 2.1.9). Este resultado constituye la parte central de nuestra derivación del teorema de ceros esparso.

Luego consideramos el teorema de ceros efectivo en su forma clásica. Obtenemos nuevas cotas para los grados para el caso de un sistema de ecuaciones cuadráticas (Teorema 2.1.10).

Obtenemos además una cota para los grados en términos de un nuevo parámetro, el grado algebraico de un sistema de ecuaciones (Teorema 2.1.15). Esta cota contiene esencialmente a todas las cotas conocidas, y las mejora en ciertos casos particulares.

2.1.1 Un Teorema de Ceros Efectivo sobre Anillos Graduados Cohen–Macaulay

A lo largo de esta sección, denotamos por k un cuerpo infinito y por $\overline{k}$ su clausura algebraica. Alternativamente, denotamos por S al anillo de polinomios $k[x_0, \ldots, x_n]$.

Para un ideal homogéneo J del anillo de polinomios $k[x_0, \ldots, x_n]$, denotamos por $\dim J$ denota la dimensión de Krull del anillo cociente $k[x_0, \ldots, x_n]/J$. El *grado* $\deg J$ de J se define como $(\dim J - 1)!$ veces el coeficiente principal del polinomio de Hilbert de la k–álgebra graduada $k[x_0, \ldots, x_n]/J$.

Un anillo graduado A es *Cohen–Macaulay* si contiene una sucesión regular de elementos homogéneos de longitud igual a la dimensión de A. En particular A es equidimensional, y el cociente de A por cualquier sucesión regular de elementos homogéneos es Cohen–Macaulay.

Sea I un ideal homogéneo Cohen–Macaulay del anillo de polinomios $k[x_0, \ldots, x_n]$, es decir, tal que el anillo cociente $k[x_0, \ldots, x_n]/I$ es Cohen–Macaulay. Sea r la dimensión de I y sea $V(I) \subseteq \mathbb{P}^n$ la variedad definida por I en el espacio proyectivo.

Sea $p \in S/I$ elemento homogéneo que es un no–divisor de cero. Sean $\eta_1, \ldots, \eta_s \in S/I$ elementos homogéneos de grado 1 — o, más brevemente, formas lineales — que definen la variedad vacía en el abierto $\{p \neq 0\}$ de $V(I)$. En esta situación, el teorema de ceros de Hilbert implica que p pertenece al radical del ideal $(\eta_1, \ldots, \eta_s)$, es decir,

$$p \in \sqrt{(\eta_1, \ldots, \eta_s)}.$$

Equivalentemente se tiene 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 $(S/I)_p$. Aquí $(S/I)_p$ denota la localización del anillo S/I con respecto al conjunto multiplicativo $\{p^i\}_{i \geq 0}$.

En esta situación vamos a dar una cota para el mínimo $D \in \mathbb{N}$ tal que p^D pertenece al ideal $(\eta_1, \ldots, \eta_s)$. Enunciamos el resultado principal de esta sección, y lo derivamos más adelante como consecuencia de una serie de resultados auxiliares.

Lema Principal 2.1.1 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo Cohen–Macaulay de dimensión r. Sean $p \in k[x_0, \ldots, x_n]/I$ un elemento homogéneo no–divisor de cero y $\eta_1, \ldots, \eta_s \in k[x_0, \ldots, x_n]/I$ formas lineales tales que p está en el radical del ideal $(\eta_1, \ldots, \eta_s)$. Entonces*

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

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

Casos particulares de este resultado fueron obtenidos previamente por Caniglia, Galligo y Heintz [29, Proposición 10] y Smietanski [120, Lema 1.44].

Como consecuencia de este resultado derivamos un teorema de ceros efectivo para anillos graduados Cohen–Macaulay (Teorema 2.1.8 y Corolario 2.1.9).

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

Considerando combinaciones k–lineales genéricas, nos podemos reducir sin pérdida de generalidad al caso en que $\overline{\eta}_1, \dots, \overline{\eta}_s \in (S/I)_p$ es una sucesión regular débil y $s \leq r$. Asumimos esto de ahora en adelante. Luego vamos a mostrar que las formas lineales $\eta_1, \dots, \eta_s$ pueden ser reemplazadas por polinomios de grado controlado que forman una sucesión regular en S/I. Este resultado está enunciado en el corolario 2.1.3, y constituye la parte técnica central en la demostración del lema principal 2.1.1.

El siguiente lema es una generalización de [67, Nota 4].

Lema 2.1.2 *Sea $K \subseteq k[x_0, \dots, x_n]$ un ideal homogéneo equidimensional, y sean $\xi_1, \dots, \xi_m \in \mathbb{P}^n$ puntos afuera de $V(K)$. Entonces existe un polinomio homogéneo $g \in K$ tal que $\deg g \leq \deg K$ y $g(\xi_i) \neq 0$ para todo i.*

Demostración. 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 $i = 1, \dots, m$. Esto es claro a partir de una proyección genérica. 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. 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 $i = 1, \dots, m$, g está en el ideal K por [27, Lema 1] y se verifica la cota de grado

$$\deg g \leq \sum_P l(Q_P) \deg P = \deg K.$$

□

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

Corolario 2.1.3 *Con la misma notación del párrafo anterior, existen elementos homogéneos $h_1, \dots, h_s \in S/I$ que satisfacen las siguientes condiciones:*

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

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

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

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

Demostración. Hacemos 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 $\overline{\eta}_1$ sea un no–divisor de cero en $(S/I)_p$ implica que η_1 es un no–divisor de cero en S/I.

Ahora sea $i \geq 2$ y supongamos que $h_1, \ldots, h_{i-1}$ 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 $h_i \in S/I$ que no esté en ninguno de los ideales primarios asociados de H_{i-1}.

Recordamos que H_{i-1} no tiene componentes inmersas ya que es un ideal 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 $V(R_l) \not\subseteq V(J_{i-1})$ para todo l. Para cada l tomamos entonces un punto $\xi_l \in V(R_l) - V(J_{i-1})$ y un elemento homogéneo $g \in J_{i-1}$ tal que $\deg g \leq \deg J_{i-1}$ y $g(\xi_l) \neq 0$. La existencia de g está garantizada por el lema anterior. 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 suponer que vale $\deg g \leq \deg J_{i-1} + \deg p - 1$. Sea entonces

$$h_i := a\, g + p^{c_i} \cdot \eta_i$$

para algún escalar $a \in k$, a ser determinado en lo que sigue. Entonces h_i es homogéneo y se tiene $h_i \equiv p^{c_i} \cdot \eta_i \pmod{J_{i-1}}$. Luego h_i no pertenece a $\sqrt{Q_j}$, ya que tanto p como η_i son no–divisores de cero modulo J_{i-1}. Luego $h_i(\xi_l) = a\, g(\xi_l) + (p^{c_i} \cdot \eta_i)(\xi_l) \neq 0$ para una elección genérica de a, y por lo tanto se tiene $h_i \notin \sqrt{R_l}$. □

Fijamos la siguiente notación. Sean $h_1, \ldots, h_s \in S/I$ los polinomios homogéneos introducidos en el corolario 2.1.3, 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.

Sea $h_i = l_i + p^{c_i} \cdot \eta_i$ para algún $l_i \in J_{i-1}$ y $c_i \geq 0$. Luego sea $\gamma_i := \delta_{i-1} - \delta_i$, y sean

$$\lambda_i := \sum_{j=1}^{i} (\gamma_j + c_j), \qquad \mu_i := \sum_{j=1}^{i} ((i-j+1)\gamma_j + (i-j)c_j)$$

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

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

Lema 2.1.4 *Sea* $q \in J_i$ *para algún* $1 \leq i \leq s$*. Entonces* $p^{\gamma_i} \cdot q \in (J_{i-1}, \eta_i)^u$*.*

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, de forma tal que K_i es un ideal equidimensional 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 sólo difieren en un ideal de codimensión al menos $i+1$. Luego $\deg(J_{i-1}, \eta_i) = \delta_{i-1}$, ya que η_i es un no–divisor de cero módulo J_{i-1}, y por lo tanto $\deg K_i = \gamma_i = \delta_{i-1} - \delta_i$. Luego p^{γ_i} está en el ideal K_i [27, Lema 1] y concluimos que $p^{\gamma_i} \cdot q \in (\cap_j Q_j) \cap (\cap_l R_l) = (J_{i-1}, \eta_i)^u$ como enunciamos.
$\square$

Los dos enunciados siguientes (Lemas 2.1.5 y 2.1.6) son simples extensiones de [41, Lemas 6.1 y 6.2].

Lema 2.1.5 *Sea $q \in J_i$ para algún $1 \leq i \leq s$. Entonces $p^{\lambda_i} \cdot q \in H_i$.*

Demostración. Hacemos inducción en i. Tenemos $p^{\gamma_1} q \in (\eta_1)^u$ por el lema 2.1.4. Además $(\eta_1)^u = (\eta_1)$ 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 el lema 2.1.4 se tiene $p^{\gamma_i} \cdot q \in (J_{i-1}, \eta_i)^u$, es decir, que $p^{\gamma_i} \cdot q$ pertenece a la intersección de todas las componentes primarias de dimensión $r - i$ del ideal (J_{i-1}, η_i). La intersección de las otras componentes primarias forma un ideal de codimensión al menos $i + 1$ y por lo tanto existe una sucesión regular $w_1, \ldots, w_{i+1}$ dentro de este ideal. Esto se desprende del hecho de que S/I es un anillo Cohen–Macaulay. Se tiene que $w_j \cdot p^{\gamma_i} \cdot q \in (J_{i-1}, \eta_i)$ y por lo tanto existen $u_j \in J_{i-1}$ y $v_j \in S/I$ tales que $w_j \cdot p^{\gamma_i} \cdot q = u_j + v_j \cdot \eta_i$ para todo g. Entonces

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

Luego $p^{\gamma_i + c_i} \cdot u_j - v_j \cdot l_i \in J_{i-1}$ y por la hipótesis inductiva $p^{\lambda_{i-1}}(p^{\gamma_i + c_i} \cdot u_j - v_j \cdot l_i)$ está en el ideal H_{i-1}. Luego tenemos $w_j \cdot p^{\lambda_i} \cdot q \in H_i$ 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 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 $w_j \notin P$. Concluimos entonces que $p^{\lambda_i} \cdot q \in H_i$. $\square$

Lema 2.1.6 *Sea $q \in J_i$ para algún $1 \leq i \leq s$. Entonces $p^{\mu_i} \cdot q \in L_i$.*

Demostración. Hacemos inducción en i. El caso $i = 1$ se sigue de la misma forma que en el lema anterior ya que $L_1 = H_1$ y $\mu_1 = \lambda_1$.

Sea $i \geq 2$. Entonces $p^{\lambda_i} \cdot q$ está en H_i por el lema 2.1.5. Sea $p^{\lambda_i} \cdot q = u + v \cdot h_i$ para algún $u \in H_{i-1}$ y $v \in S/I$. Luego $p^{\lambda_i} \cdot q - v \cdot h_i \in H_{i-1}$ y por lo tanto $p^{\lambda_i} \cdot q - p^{c_i} \cdot v \cdot \eta_i \in J_{i-1}$ debido a que $H_{i-1} \subseteq J_{i-1}$ y $h_i \equiv p^{c_i} \cdot \eta_i \pmod{J_{i-1}}$. Esto implica a su vez $p^{\lambda_i - c_i} \cdot q - v \cdot \eta_i \in J_{i-1}$.

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

Demostración del Lema Principal 2.1.1. Podemos suponer sin pérdida de generalidad que $\overline{\eta}_1, \dots, \overline{\eta}_s$ es una sucesión regular débil en $(S/I)_p$ y que $s \le r$. Por el lema 2.1.6 sólo queda acotar μ_s. Hacemos uso de las estimaciones $\gamma_i, c_i \le \delta_{i-1}$ y obtenemos la cota

$$\begin{array}{rcl} \mu_s & = & \sum_{j=1}^{s}((s-j+1)\,\gamma_j + (s-j)\,c_j) \\ & \le & \sum_{j=1}^{s}((s-j+1)\,\delta_{j-1} + (s-j)\,\delta_{j-1}) \le s^2 \deg I. \end{array}$$

□

El resto de esta subsección está dedicado a la extensión de este resultado al caso en que reemplazamos las formas lineales por elementos homogéneos de grado arbitrario. Primeramente establecemos algunas generalidades sobre la aplicación de Veronese.

Denotemos por N al entero $\binom{n+d}{d} - 1$, y sean $a_0, \dots, a_N$ los exponentes de los distintos monomios de grado d en $k[x_0, \dots, x_n]$. Sea

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

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 por $v_{n,d}$. Sea $I(v_{n,d})$ su ideal de definición y denotamos por $S^{(d)} := k[y_0, \dots, y_N]/I(v_{n,d})$ su anillo de coordenadas homogéneas. 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 $j = 0, \dots, N$.

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

$$S^{(d)}/J^{(d)} = \oplus_j \, (S/J)_{d\,j}.$$

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

Lema 2.1.7 *Sea J un ideal homogéneo Cohen–Macaulay de S y sea $J^{(d)}$ su contracción 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. Alcanza con exhibir una sucesión regular de elementos homogéneos de longitud igual a la dimensión de A.

Sea $e := \dim B = \dim A$. Sea $\beta_1, \dots, \beta_e$ una sucesión regular en B de elementos homogéneos y sea $\alpha_i := \beta_i^d$. Luego $\alpha_1, \dots, \alpha_e$ son elementos de A que forman una sucesión regular en B [99, Teorema 16.1]. Afirmamos que también forman una sucesión regular maximal en A. Sólo tenemos que probar que $\overline{\alpha_i}$ 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 $\zeta\cdot\alpha_i\in(\alpha_1,\ldots,\alpha_{i-1})$. 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 $\zeta\in(\alpha_1,\ldots,\alpha_{i-1})$. □

Teorema 2.1.8 *Sea $I\subseteq k[x_0,\ldots,x_n]$ un ideal homogéneo Cohen–Macaulay. Sea $p\in k[x_1,\ldots,x_n]/I$ un elemento homogéneo no–divisor de cero y sean $f_1,\ldots,f_s\in k[x_0,\ldots,x_n]/I$ elementos homogéneos tales que p está en el radical del ideal $(f_1,\ldots,f_s)$. Sean $r:=\dim I$ y $d:=\max_i\deg f_i$. Entonces*

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

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

Demostración. Notamos en primer lugar que los ceros en $V(I)$ de los polinomios $\{f_i\}_i$ coinciden con los ceros en $V(I)$ de los polinomios $\{x_j^{d-\deg f_i}f_i\}_{ij}$. Se tiene además $x_j^{d-\deg f_i}f_i\in(f_1,\ldots,f_s)$. 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 pudo haber aumentado en esta etapa preparatoria.

Sea $i_d:S^{(d)}\hookrightarrow S$ la inclusión de k–álgebras inducida por la aplicación de Veronese y sea $I^{(d)}$ la contracción del ideal I al anillo $S^{(d)}$. Esta inclusión es una biyección en grado 1. Sea entonces $\eta_i\in S^{(d)}/I^{(d)}$ una forma lineal tal que $i_d(\eta_i)=f_i$ para $i=1,\ldots,s$. 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 η_i están contenidos en la imagen de los ceros de los polinomios f_i. Los ceros comunes de $f_1,\ldots,f_s$ están en la hipersuperficie $\{p^d=0\}$ de $V(I)$ y se tiene además que $v_d(\{p^d=0\})=\{q=0\}$. Entonces la subvariedad de $V(I^{(d)})$ definida por $\eta_1,\ldots,\eta_s$ está contenida en la hipersuperficie $\{q=0\}$.

Por el lema 2.1.7 el ideal $I^{(d)}$ es Cohen–Macaulay, y además q no es un divisor de cero módulo $I^{(d)}$. Estamos entonces en las hipótesis del lema principal 2.1.1. Luego se tiene

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

Aplicamos el morfismo i_d a la expresión anterior y obtenemos

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

por la igualdad $\deg I^{(d)}=d^{r-1}\deg I$. □

Corolario 2.1.9 *Sea $I\subseteq k[x_1,\ldots,x_n]$ un ideal tal que su homogeneización I^h en el anillo $k[x_0,\ldots,x_n]$ es Cohen–Macaulay. Sean $f_1,\ldots,f_s\in k[x_1,\ldots,x_n]$ polinomios sin* *ceros comunes en la variedad afín* $V(I) \subseteq \mathbb{A}^n$ *. Entonces existen* $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ *tales que*

$$\overline{1} = \overline{g}_1 \, \overline{f}_1 + \cdots + \overline{g}_s \, \overline{f}_s \in k[x_1, \dots, x_n]/I$$

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

Demostración. El ideal I^h es un ideal homogéneo y x_0 es un no–divisor de cero módulo I^h. Por hipótesis I^h es un ideal Cohen–Macaulay de dimensión $r+1$.

Sea f_i^h la homogeneización de f_i. Los polinomios homogéneos $f_1^h, \dots, f_s^h$ no tienen ningún cero en común en $V(I^h)$ fuera del hiperplano $\{x_0 = 0\}$. Por el teorema 2.1.8 existen polinomios homogéneos $v_1, \dots, v_s \in S$ tales que

$$x_0^{(r+1)^2 \, d^{r+1}} = v_1 f_1^h + \ldots + v_s f_s^h \in k[x_1, \dots, x_n]/I^h$$

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

Con la notación del corolario 2.1.9, en el caso en que $I = 0$ — esto es, en la situación del teorema de ceros efectivo clásico — obtenemos la cota de grado

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

2.1.2 Cotas Mejoradas para los Grados

En esta subsección consideramos las cotas de grado en el contexto del teorema de ceros efectivo cásico. Vamos a aplicar el método utilizado en la subsección 2.1.1 en un modo directo — sin referencia a la aplicación de Veronese. La demostración sigue las mismas líneas, y por lo tanto vamos a omitir algunas verificaciones con el fin de evitar repeticiones innecesarias.

Sean $f_1, \dots, f_s \in k[x_0, \dots, x_n]$ polinomios homogéneos sin ceros comunes en el hiperplano $\{x_0 = 0\} \subseteq \mathbb{P}^n$. En esta situación vamos a dar una cota para el mínimo $D \in \mathbb{N}$ tal que $x_0^D \in (f_1, \dots, f_s)$.

Consideramos en primer lugar las cotas para el teorema de ceros en su forma clásica y obtenemos el siguiente resultado.

Teorema 2.1.10 *Sean* $f_1, \dots, f_s \in k[x_0, \dots, x_n]$ *polinomios homogéneos tales que* x_0 *está en el radical del ideal* $(f_1, \dots, f_s)$*. Sea* $d_i := \deg f_i$ *y supongamos que vale* $d_1 \geq \cdots \geq d_s$*. Entonces*

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

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

Este resultado se sigue de una serie de resultados auxiliares.

Vamos a suponer sin pérdida de generalidad que $s \leq n+1$ y que $\overline{f}_1, \dots, \overline{f}_s$ es una sucesión regular débil en $k[x_0, \dots, x_n]_{x_0}$. Sea $d_i := \deg f_i$ y supongamos que se tiene $d_2 \geq \cdots \geq d_s$

y $d_s \geq d_1$. Como antes, estos 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 anillo de polinomios S del ideal $(\overline{f}_1, \dots, \overline{f}_i) \subseteq S_{x_0}$, con la convención $J_0 := (0)$.

Lema 2.1.11 *Con la notación del párrafo anterior existen* $h_1, \dots, h_s \in k[x_0, \dots, x_n]$ *polinomios homogéneos que satisfacen las siguientes condiciones:*

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

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

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

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

□

Introducimos la siguiente notación. Sea $\delta_i := \deg J_i$ de forma tal que se tiene

$$\delta_i \leq \prod_{j=1}^{i} d_j$$

por la desigualdad de Bézout. Sean entonces por $\gamma_i := d_i\, \delta_{i-1} - \delta_i$ para $i = 1, \dots, \min\{n, s\}$ y $\gamma_{n+1} := \delta_n + d_{n+1} - 1$. Sean también $\delta := \max\{\delta_i : i = 1, \dots, s-1\}$ y $d := \max\{d_i : i = 1, \dots, s-1\}$. Para un ideal I de S denotamos por I^u su parte equidimensional.

Lema 2.1.12 *Sea* $q \in J_i$ *para algún* $1 \leq i \leq s$ *. Entonces* $x_0^{\gamma_i} \cdot q \in (J_{i-1}, \eta_i)^u$.

Demostración. El caso $i \leq n$ se trata exactamente como en el lema 2.1.4. Consideramos el caso $i = n+1$.

El ideal J_n tiene dimensión 1 y grado 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 módulo J_n , por el lema 3.1.1. Se sigue $x_0^{\gamma_{n+1}} \in (J_n, f_{n+1})$ y en particular $x_0^{\gamma_{n+1}} \cdot q \in (J_n, f_{n+1})^u$. □

Ahora sean $h_1, \dots, h_s$ los polinomios homogéneos introducidos en el lema 2.1.11. Sean

$$\begin{aligned} \mu_i &:= \textstyle\sum_{j=2}^{i} ((i-j+1)\,\gamma_j + (i-j)\,c_j), && \text{para } i = 1, \dots, \min\{n, s\} \\ \mu_{n+1} &:= \mu_n + \gamma_{n+1}, \end{aligned}$$

donde c_i denota el entero $\deg h_i - \deg f_i$. Denotamos por L_i al ideal homogéneo de S generado por $f_1, \dots, f_i$.

Lema 2.1.13 *Sea* $q \in J_i$ *para algún* $1 \leq i \leq s$ *. Entonces* $x_0^{\mu_i} \cdot q \in L_i$.

Demostración. El caso $i \leq n$ se trata exactamente como en el lema 2.1.6. Consideramos el caso $i = n+1$.

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

Luego queda solamente acotar a μ_s. Vamos a tratar dos tipos diferentes de cotas. Una depende como siempre 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 estos polinomios.

Lema 2.1.14 *Se tiene* $\mu_s \leq \min\{n,s\}^2 \, d\,\delta$. *En el caso en que* $\deg f_i \geq 2$ *para todo* i, *se tiene* $\mu_s \leq 2 \prod_{j=1}^{\min\{n,s\}} d_j$.

Demostración. Descomponemos al entero μ_s en dos términos y los estimamos separadamente. En primer lugar consideramos el término $\sum_{j=2}^{s} (s-j)\, c_j$. Se tiene $c_i \leq \max\{\delta_{i-1} - d_i, 0\}$. En particular $c_2 = 0$ ya que $\delta_1 = d_1$ y $d_1 \leq d_2$. Luego

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

bajo la hipótesis $d_i \geq 2$ para todo i. Se tiene 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 primeramente el caso $s \leq n$. Se tiene

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

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

Por otra parte se tiene también la estimación $\sum_{j=2}^{s} (s-j+1)\,\gamma_j \leq \frac{1}{2}\,(s-1)\,s\,d\,\delta$ de donde concluimos $\mu_s \leq \frac{1}{2}\,(s-1)\,s\,d\,\delta + \frac{1}{2}\,(s-2)\,(s-1)\,\delta \leq (s-1)^2\,d\,\delta$. □

Demostración del Teorema 2.1.10. Por los lemas 2.1.13 y 2.1.14 sólo queda por considerar el caso en que alguno de los f_i tiene grado 1.

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 $f_{r+1}, \ldots, f_s$ son polinomios de grado 1. Podemos asumir sin pérdida de generalidad que estos polinomios son k–linealmente independientes.

Suponemos además que ni 1 ni x_0 están en el k–espacio lineal generado por $f_{r+1}, \ldots, f_s$, ya que en ambos casos el enunciado es trivial.

Sean $y_0, \ldots, y_{n+r-s-1} \in S$ polinomios de grado 1 que completan a $f_{r+1}, \ldots, f_s$ a un cambio lineal de variables. Suponemos además $y_0 = x_0$. 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 $v_i \equiv f_i \pmod{(f_{r+1}, \ldots, f_s)}$ 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 se satisface $\deg v_i \leq d_i$.

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

La cota para el teorema de ceros enunciada en la página 9 de 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 obtener la cota para los polinomios en el teorema de ceros en términos del grado algebraico del sistema de polinomios. En lo que sigue introducimos esta noción.

Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polinomios sin ceros comunes en $\mathbb{A}^n$. Sea $\lambda = (\lambda_{ij})_{ij} \in \overline{k}^{s \times s}$ una $s \times s$–matriz arbitraria con entradas en $\overline{k}$. Denotamos por $h_i(\lambda)$ las combinaciones lineales $\sum_j \lambda_{ij}\, f_j$ inducidas por la matriz λ para $i = 1, \ldots, s$.

Consideramos el conjunto Γ de $s \times s$–matrices tales que para toda $\lambda \in \Gamma$ 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 $t = t(\lambda) \leq \min\{n, s\}$. Este conjunto es no vacío, y de hecho contiene un abierto no vacío de $\overline{k}^{s \times s}$.

Para cada $\lambda \in \Gamma$ e $i = 1, \ldots, t-1$ denotamos por $J_i(\lambda)$ la homogeneización en $k[x_0, \ldots, x_n]$ 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 $f_1, \ldots, f_s$ se define como

$$\delta(f_1, \ldots, f_s) := \min\{\delta(\lambda) : \lambda \in \Gamma\}$$

La noción de grado geométrico de Krick, Sabia y Solernó [84] y del autor [122] se define en forma análoga como el mínimo valor que toma $\delta(\lambda)$ para $\lambda \in \Gamma$, con la hipótesis adicional de que los ideales $J_i(\lambda)$ sean radicales para $i = 1, \ldots, t-1$. Otra diferencia es que en el caso en que $\mathrm{char}\,(k) > 0$ los polinomios $h_j(\lambda)$ se toman como combinaciones lineales de los polinomios $\{x_j \cdot f_i\}_{ij}$.

La noción de grado geométrico de Giusti et al. [57] es similar a la noción descripta en el párrafo anterior. La única diferencia consiste en que este parámetro no se define como un mínimo, sino como el valor de $\delta(\lambda)$ para una elección genérica de λ.

Luego el grado algebraico está acotado por el grado geométrico, en cualquiera de las dos versiones de este último que se considere. El siguiente ejemplo muestra que en ciertos casos particulares puede ser mucho menor. Es una variante de [84, Ejemplo 2].

Ejemplo 2.1.1 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 $d \geq 2$. Es fácil verificar que estos polinomios no tienen ceros comunes en $\mathbb{A}^n$. Vamos a calcular el grado geométrico δ_g — en el sentido de [84], [122] — y el grado algebraico δ_a para este ejemplo particular. Obtenemos $\delta_g = d^{n-1}$ y $\delta_a = 2$, y de esta forma mostramos que el grado algebraico puede ser mucho menor que el grado geométrico en algunos casos particulares.

En primer lugar consideramos el grado geométrico. Los polinomios $f_1, \ldots, f_n$ forman una sucesión regular, $1 \in (f_1, \ldots, f_n)$ y el ideal $(f_1, \ldots, f_i)$ es radical para $i = 1, \ldots, n-1$. Se tiene $\deg V(f_1, \ldots, f_i) = d^i$ para $i = 1, \ldots, n-1$ y por lo tanto $\delta_g \leq d^{n-1}$.

Sean $h_i := \sum_j \lambda_{ij} f_j$ combinaciones $\overline{k}$–lineales de $f_1, \ldots, f_n$ para $i = 1, \ldots, l$. Supongamos que $1 \in (h_1, \ldots, h_n)$ y que $(h_1, \ldots, h_i)$ es un ideal radical de dimensión $n - i$ para $i = 1, \ldots, l-1$. Vamos a probar $l = n$ y $\deg V(h_1, \ldots, h_{n-1}) \geq d^{n-1}$.

Podemos asumir sin pérdida de generalidad que las combinaciones lineales h_i están es forma escalonada — en el sentido de álgebra lineal — es decir

$$h_i = f_{n(i)} + \sum_{j > n(i)} a_{ij} f_j$$

con $n(1) < \cdots < n(l)$. En nuestro caso particular, esta representación nos permite eliminar las variables $x_{n(1)}, \ldots, x_{n(l)}$ del sistema de ecuaciones $h_1, \ldots, h_l$, ya que cada variable x_i no interviene en f_j para $j > i$. Luego la variedad $V(h_1, \ldots, h_l)$ se puede parametrizar expresando a estas variables como funciones racionales de las otras para $l \leq n-1$. Se sigue que $V(h_1, \ldots, h_l)$ tiene dimensión $n - l$, y por lo tanto $l = n$ y $(h_1, \ldots, h_{n-1})$ es un ideal radical de dimensión 1.

Luego supongamos $n(j) \neq j$ para algún $j \leq n-1$. Luego $h_n = x_n^2$, y es fácil verificar que existen polinomios $g_1, \ldots, g_{n-2} \in k[x_1, \ldots, x_{n-1}]$ tales que $(h_1, \ldots h_{n-1}) = (g_1, \ldots, g_{n-2}, x_n^2)$. Luego $(h_1, \ldots h_{n-1})$ no es radical, lo cual contradice nuestra hipótesis.

Se tiene entonces $h_i = f_i + \sum_{j > i} a_{ij} f_j$ y por lo tanto la curva $V(h_1, \ldots, h_{n-1})$, se puede parametrizar como $t \mapsto \varphi(t) = (\varphi_1(t), \ldots, \varphi_n(t))$, de donde $\varphi_i \in \overline{k}(t)$ es una función racional de grado d^{n-i-1}. Luego $\deg V(h_1, \ldots, h_{n-1}) = d^{n-1}$, de donde se sigue la cota inferior $\delta_g \geq d^{n-1}$. Combinando esto con la estimación anterior concluimos $\delta_g = d^{n-1}$.

Luego consideramos el grado algebraico. Los polinomios $f_n, \ldots, f_1$ forman una sucesión regular débil y $1 \in (f_n, \ldots, f_1)$. Se tiene $(f_n, \ldots, f_{n-i+1}) = (x_n^2, x_{n-1}, \ldots, x_{n-i+1})$ de donde se sigue $\delta_a \leq 2$. Además toda combinación lineal h de $f_1, \ldots, f_n$ tiene grado a lo sumo 2, y por lo tanto $\delta_a \geq \deg h \geq 2$. Concluimos entonces $\delta_a = 2$.

Obtenemos la siguiente cota de grado por aplicación directa de los lemas 2.1.13 y 2.1.14.

Teorema 2.1.15 *Sean $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ polinomios homogéneos de grado acotado por d tales que x_0 está en el radical del ideal $(f_1, \ldots, f_s)$. Sea f_i^a la afinización de f_i. Sea δ el grado algebraico del sistema de ecuaciones $f_1^a, \ldots, f_s^a$. Entonces*

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

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

$\square$

La cota enunciada en la página 9 de la introducción se sigue directamente de este resultado.

Aplicando esta cota de grado al ejemplo anterior deducimos 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 se tiene la identidad

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

2.2 Cotas de Esparsitud

En esta sección consideramos el aspecto ralo — o esparso — en el teorema de ceros. Como anticipamos en la introducción, vamos a considerar como medida de la esparsitud de un polinomio o de una familia de polinomios, a su polítopo de Newton. Como consecuencia de estos resultados obtenemos además distintas cotas de grado para los polinomios en el teorema de ceros.

En primer lugar vamos a introducir notación y a enunciar algunos hechos básicos de geometría poliedral y de variedades tóricas que vamos a utilizar a lo largo de esta sección. Referimos a los libros Fulton [52] y Sturmfels [126] para la demostración de estos enunciados y para un tratamiento más amplio de estos temas.

Sea $\mathcal{A} \subseteq \mathbb{Z}^n$ un conjunto finito de vectores enteros. La *cápsula convexa* de $\mathcal{A}$ como un subconjunto de $\mathbb{R}^n$ se denota por $\mathrm{conv}(\mathcal{A})$. El *cono* sobre $\mathrm{conv}(\mathcal{A})$ se denota por $\mathrm{pos}(\mathcal{A})$, esto es, $\mathrm{pos}(\mathcal{A}) := \mathbb{R}_{\geq 0} \cdot \mathrm{conv}(\mathcal{A})$.

El conjunto $\mathcal{A}$ es *graduado* si existe un vector entero $\omega \in \mathbb{Z}^n$ tal que $< a, \omega >= 1$ para todo $a \in \mathcal{A}$, esto es, cuando $\mathcal{A}$ está en un hiperplano afín que no contiene al origen.

Sea $\mathbb{Z} \cdot \mathcal{A}$ el $\mathbb{Z}$–módulo generado por $\mathcal{A}$. Sea $\mathbb{R} \cdot \mathcal{A}$ el espacio lineal generado por $\mathcal{A}$, de forma tal que $\mathbb{Z} \cdot \mathcal{A}$ es un retículo de $\mathbb{R} \cdot \mathcal{A}$. Sea ρ la dimensión de este espacio lineal. Consideramos entonces la forma euclidiana de volumen en $\mathbb{R} \cdot \mathcal{A}$, normalizada de forma tal que cada simplex primitivo del retículo $\mathbb{Z} \cdot \mathcal{A}$ tiene volumen unitario. El *volumen* normalizado $\mathrm{Vol}(\mathcal{A})$ 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 $\mathrm{vol}(\mathrm{conv}(\mathcal{A}))$ denota el volumen de $\mathrm{conv}(\mathcal{A})$ con respecto a la forma de volumen usual (no–normalizada) de $\mathbb{R}^n$.

Sea $\mathbb{N} \cdot \mathcal{A}$ el semigrupo generado por $\mathcal{A}$. Este semigrupo está siempre contenido en el semigrupo $\operatorname{pos}(\mathcal{A}) \cap \mathbb{Z} \cdot \mathcal{A}$. El conjunto $\mathcal{A}$ se dice *normal* o *saturado* si se verifica la igualdad $\mathbb{N} \cdot \mathcal{A} = \operatorname{pos}(\mathcal{A}) \cap \mathbb{Z} \cdot \mathcal{A}$.

Un polítopo $\mathcal{P}$ se dice *entero* si es la cápsula convexa de un conjunto finito de vectores enteros.

Sea $\mathcal{S}$ un simplex entero. Entonces $\mathcal{S}$ se dice *unimodular* si su interior no contiene ningún vector entero. Sea $\{s_1, \ldots, s_k\}$ el conjunto de vértices de $\mathcal{S}$. Entonces $\mathcal{S}$ 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 símplices 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 seguimos el punto de vista de Sturmfels [126]. Este punto de vista difiere del usual en geometría algebraica. Es más combinatorio y se adecúa mejor a nuestros propósitos.

Sea $\mathcal{A} = \{a_1, \ldots, a_N\} \in \mathbb{Z}^n$ un conjunto finito de vectores enteros. 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 $I_{\mathcal{A}}$ de $k[y_1, \ldots, y_N]$, 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 $\mathbb{Z} \cdot \mathcal{A}$.

La k–álgebra $k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ es el anillo de coordenadas del toro $(\overline{k}^*)^n$. La aplicación $\varphi_{\mathcal{A}}$ induce una aplicación dominante $(\overline{k}^*)^n \to X_{\mathcal{A}}$. La imagen de esta aplicación es el *toro* $T_{\mathcal{A}}$ de la variedad tórica afín $X_{\mathcal{A}}$. Este toro es igual al abierto $\{y_1 \cdots y_N \neq 0\} \subseteq X_{\mathcal{A}}$.

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 $\mathbb{P}^{N-1}$. Se tiene

$$\dim Y_{\mathcal{A}} = \operatorname{rank} \mathbb{Z} \cdot \mathcal{A} - 1, \qquad \deg Y_{\mathcal{A}} = \operatorname{Vol}(\mathcal{A}).$$

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 de forma irredundante por las variedades afines $X_{\mathcal{A}-a_i}$, donde a_i recorre los vértices del polítopo $\operatorname{conv}(\mathcal{A})$.

La k–álgebra $k[y_1,\dots,y_N]/I_{\mathcal{A}}$ 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. La k–álgebra $k[\mathbb{N}\cdot\mathcal{A}]$ es un dominio Cohen–Macaulay en el caso en que el conjunto $\mathcal{A}$ es normal (Teorema de Hochster).

Sea $\mathcal{P}\subseteq\mathbb{R}^n$ un polítopo entero. Este polítopo determina un abanico $\Delta_{\mathcal{P}}$ y una variedad tórica completa $X_{\mathcal{P}}=X(\Delta_{\mathcal{P}})$. Esta variedad viene provista de un divisor de Cartier amplio $D_{\mathcal{P}}$. Este divisor de Cartier define 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 $\{1\}\times(\mathcal{P}\cap\mathbb{Z}^n)$ [52, Sección 3.4]. El divisor $(n-1)D_{\mathcal{P}}$ es muy amplio [44], y por lo tanto el conjunto graduado $\mathcal{A}((n-1)\,\mathcal{P})$ es normal.

Teorema 2.2.1 *Sean $p,f_1,\dots,f_s\in k[x_1,\dots,x_n]$ polinomios tales que p está en el radical del ideal $(f_1,\dots,f_s)$. Sea $\mathcal{P}\subseteq\mathbb{R}^n$ un polítopo entero que contiene al polítopo de Newton de los polinomios $1,x_1,\dots,x_n,f_1,\dots,f_s$. Supongamos además que el conjunto $\mathcal{A}(\mathcal{P})\subseteq\mathbb{Z}^{n+1}$ es normal. Entonces existen $D\in\mathbb{N}$ y $g_1,\dots,g_s\in k[x_1,\dots,x_n]$ tales que*

$$p^D=g_1f_1+\cdots+g_sf_s$$

con $D\leq\ n!\,\min\{n+1,s\}^2\,\mathrm{vol}(\mathcal{P})$ y $\mathcal{N}(g_if_i)\subseteq\ (1+\deg p)\,n!\,\min\{n+1,s\}^2\,\mathrm{vol}(\mathcal{P})\cdot\mathcal{P}$ para $i=1,\dots,s$.

Demostración. Sea $\mathcal{B}=\{b_0,\dots,b_N\}:=\mathcal{P}\cap\mathbb{Z}^n$, de forma tal que se tiene $\mathcal{A}(\mathcal{P})=\{1\}\times\mathcal{B}$. Asumimos $b_0=(0,\dots,0)$. Consideramos el morfismo de k–álgebras

$$\psi:k[y_1,\dots,y_N]\to k[x_1,\dots,x_n],\qquad\qquad y_i\mapsto x^{b_i}.$$

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 es la intersección de la variedad tórica proyectiva $Y_{\mathcal{A}(\mathcal{P})}$ con la carta afín $\{y_0\neq0\}$ of $\mathbb{P}^N$. Además la aplicación ψ induce un isomorfismo $\mathbb{A}^n\to X_{\mathcal{B}-b_0}$.

Sea $\zeta_i\in k[y_1,\dots,y_N]$ un polinomio de grado 1 tal que $\psi(\zeta_i)=f_i$ para $i=1,\dots,s$. Tomamos también un polinomio $q\in k[y_1,\dots,y_N]$ de grado menor o igual que el grado de p tal que $\psi(q)=p$. Luego $\zeta_1,\dots,\zeta_s$ no tienen ceros comunes en $X_{\mathcal{B}-b_0}$ afuera de la hipersuperficie $\{q=0\}$.

Sean $\eta_1,\dots,\eta_s,u$ las homogeneizaciones de $\zeta_1,\dots,\zeta_s,q$ en $k[y_0,\dots,y_N]$, respectivamente. Entonces las formas lineales $\eta_1,\dots,\eta_s$ no tienen ceros comunes en $Y_{\mathcal{A}(\mathcal{P})}$ afuera de la hipersuperficie $\{y_0\cdot u=0\}$.

Por hipótesis $\mathcal{A}(\mathcal{P})$ es normal, y por lo tanto $I_{\mathcal{A}(\mathcal{P})}$ es un ideal primo homogéneo Cohen–Macaulay de $k[y_0,\dots,y_N]$ de dimensión menor o igual a $n+1$. Además $y_0\cdot u$ es un no–divisor de cero módulo $I_{\mathcal{A}(\mathcal{P})}$, y por lo tanto estamos en las hipótesis del lema principal 2.1.1. Sea $D:=\ \min\{n+1,s\}^2\deg Y_{\mathcal{A}(\mathcal{P})}$. Luego existen $\alpha_1,\dots,\alpha_s\in k[y_0,\dots,y_N]/I_{\mathcal{A}(\mathcal{P})}$ elementos homogéneos de grado $\ (1+\deg u)\,D-1\ $ que satisfacen

$$(y_0\cdot u)^D=\alpha_1\eta_1+\cdots+\alpha_s\eta_s.$$

Evaluamos $y_0 := 1$ y aplicamos el morfismo ψ a la identidad anterior. Obtenemos

$$p^D = g_1 f_1 + \cdots + g_s f_s,$$

con $g_i(x) := \alpha_i(1, x^{b_1}, \ldots, x^{b_N})$. Se tiene $\deg u \leq \deg p$ y $\deg Y_{\mathcal{A}(\mathcal{P})} \leq n! \operatorname{vol}(\mathcal{P})$. Concluimos entonces

$$\begin{aligned} D &\leq n! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}), \\ \mathcal{N}(f_i\, g_i) &\subseteq ((1 + \deg p)\, n! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})) \cdot \mathcal{P} \end{aligned}$$

para $i = 1, \ldots, s$. □

Derivamos del resultado anterior la siguiente cota de grado.

Corolario 2.2.2 *Mantenemos la notación del teorema 2.2.1. Sea* $d := \max_i \deg f_i$. *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* $i = 1, \ldots, s$.

□

Vamos a exhibir un ejemplo que muestra que esta cota de grado puede ser mucho más precisa que la usual en el caso de un sistema de ecuaciones ralo.

Ejemplo 2.2.1 Sean

$$f_i := a_{i0} + a_{i1}x_1 + \cdots + a_{in}x_n + b_{i1}x_1 \cdots x_n + \cdots + b_{id}(x_1 \cdots x_n)^d,$$

para $i = 1, \ldots, s$, polinomios sin ceros comunes en $\mathbb{A}^n$. Sea

$$\mathcal{P}_d := \operatorname{conv}(0, e_1, \ldots, e_n, d\,(e_1 + \cdots + e_n)) \subseteq \mathbb{R}^n$$

de forma tal que $\mathcal{P}_d$ contiene al polítopo de Newton de los polinomios $1, x_1, \ldots, x_n, f_1, \ldots, f_s$. Se tiene la descomposición

$$\mathcal{P}_d = \cup_{ij}\, Q_{ij}$$

con $Q_{ij} := ((j-1)\,(e_1 + \cdots + e_n), e_1, \ldots, \widehat{e_i}, \ldots, e_n, j\,(e_1 + \cdots + e_n))$ para $i = 1, \ldots, n$ y $j = 1, \ldots, d$. Luego $\mathcal{P}_d$ es unimodular y por lo tanto el conjunto $\mathcal{A}(\mathcal{P})$ es normal. Estamos así en la hipótesis del corolario 2.2.2. Concluimos 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 $\mathcal{N}(g_i f_i) \subseteq n\, d \min\{n+1, s\}^2\, \mathcal{P}_d$, ya que el volumen de $\mathcal{P}_d$ es $d/(n-1)!$. En particular obtenemos la cota de grado

$$\deg g_i f_i \leq (n+1)^4\, d^2$$

que es mucho más precisa que la estimación $\deg g_i f_i \leq n^n\, d^n$ que se obtiene por aplicación directa de las cotas usuales.

Mantenemos la notación del teorema 2.2.1. Sea $\mathcal{N} := \mathcal{N}(1, x_1, \dots, x_n, f_1, \dots, f_s)$ y sea $\mathcal{U}$ el volumen no mezclado de este polítopo. Asumimos $n \geq 2$. En esta situación podemos tomar a $\mathcal{P}$ como $(n-1)\mathcal{N}$. Obtenemos entonces las cotas

$$D \leq n^{n+2}\,\mathcal{U}, \qquad\qquad \mathcal{N}(g_i f_i) \subseteq ((1 + \deg p)\, n^{n+3}\,\mathcal{U})\;\mathcal{N}.$$

Es fácil verificar que estas cotas siguen siendo válidas en el caso $n = 1$. El teorema 2 se sigue de esta observación en el caso particular $p = 1$. En este caso la condición $0 \in \mathcal{P}$ es redundante.

Notamos que la noción ingenua de esparsitud, basada en la cantidad de monomios no nulos en cada polinomio, no da mejores cotas que las conocidas para los grados en el teorema de ceros. Esto se sigue del ejemplo de Mora–Lazard–Masser–Philippon–Kollár.

Obtenemos un resultado similar en el caso de un sistema de polinomios de Laurent.

Teorema 2.2.3 *Sean $p, f_1, \dots, f_s \in k[x_1^{-1}, \dots, x_n^{-1}, x_1, \dots, x_n]$ polinomios de Laurent tales que p está en el radical del ideal $(f_1, \dots, f_s)$. Sea $\mathcal{P} \subseteq \mathbb{R}^n$ un polítopo entero que contiene al polítopo de Newton de $p, f_1, \dots, f_s$ y sea $\rho := \dim \mathcal{P}$. Asumimos además que el conjunto $\mathcal{A}(\mathcal{P}) \subseteq \mathbb{Z}^{n+1}$ es normal. Entonces existen $D \in \mathbb{N}$, $a \in \mathbb{Z}^n$ y $g_1, \dots, g_s \in k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ tales que*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

con $D \leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$, $a \in (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2 \cdot \mathcal{P}$ *y* $\mathcal{N}(g_i f_i) \subseteq (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2 \cdot \mathcal{P} - a$ *para* $i = 1, \dots, s$.

Demostración. Como antes denotamos por $B = \{b_0, \dots, b_N\}$ al conjunto de vectores enteros $\mathcal{P} \cap \mathbb{Z}^n$. Asumimos por el momento $b_0 = (0, \dots, 0)$. Consideramos entonces el morfismo

$$\psi : k[y_1, \dots, y_N] \to k[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}], \qquad\qquad y_i \mapsto x^{b_i}.$$

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 $X_{\mathcal{B}-b_0}$ 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 T es también el toro de $Y_{A(\mathcal{P})}$. Recordamos que este toro coincide con el abierto $\{y_0 \cdots y_N = 0\}$ de $Y_{A(\mathcal{P})}$.

La aplicación ψ induce una suryección $(\overline{k}^*)^n \to T$. Sea $\zeta_1, \dots, \zeta_s, q \in k[y_1, \dots, y_N]$ polinomios de grado 1 tales que $\psi(\zeta_i) = f_i$ y $\psi(q) = p$. Entonces $\zeta_1, \dots, \zeta_s$ no tienen ceros comunes en T afuera del hiperplano $\{q = 0\}$.

Sean $\eta_1, \dots, \eta_s, u$ las homogeneizaciones de $\zeta_1, \dots, \zeta_s, q$ en $k[y_0, \dots, y_N]$, respectivamente. Entonces las formas lineales $\eta_1, \dots, \eta_s$ no tienen ceros comunes en $Y_{\mathcal{A}(\mathcal{P})}$ afuera de la hipersuperficie $\{y_0 \cdots y_N\, u = 0\}$.

Sea $V(\eta_1, \dots, \eta_s)$ la subvariedad de $Y_{\mathcal{A}(\mathcal{P})}$ definida por $\eta_1, \dots, \eta_s$. Por la desigualdad de Bézout, el número de componentes irreducibles de $V(\eta_1, \dots, \eta_s)$ está acotado por $Y_{\mathcal{A}(\mathcal{P})}$. Sea $\delta := \deg Y_{\mathcal{A}(\mathcal{P})}$, 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 contenida 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 del hecho de que si $\eta_1, \ldots, \eta_s$ tengan un cero común en T en el hiperplano $\{u = 0\}$ o no. Sea Π el producto de estas ecuaciones, que es por lo tanto 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 $k[y_0, \ldots, y_N]$. Además Π es un no–divisor de cero módulo $I_{\mathcal{A}(\mathcal{P})}$, y por lo tanto estamos en las hipótesis del lema principal 2.1.1. Sea $E := \min\{n+1, s\}^2 \deg Y_{\mathcal{A}(\mathcal{P})}$. Entonces existen $\alpha_1, \ldots, \alpha_s \in k[y_0, \ldots, y_N]/I_{\mathcal{A}(\mathcal{P})}$ polinomios homogéneos de grado $E \cdot \deg \Pi - 1$ 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

$$p^D = g_1 f_1 + \cdots + g_s f_s,$$

con $g_i(x) := (x^{b_{i_1}} \cdots x^{b_{i_l}})^{-1} \alpha_i(1, x^{b_1}, \ldots, x^{b_N})$ y $D := E$ en el caso en que u aparece como un factor de Π y $D := 1$ en caso contrario. Luego se tiene

$$\begin{aligned} D &\leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P}), \\ \mathcal{N}(g_i f_i) &\subseteq (\rho! \operatorname{vol}(\mathcal{P})\, E - 1)\ \mathcal{P} - (b_{i_1} + \cdots + b_{i_l}) \end{aligned}$$

Se tiene $\deg \Pi \leq \deg Y_{\mathcal{A}(\mathcal{P})} \leq \rho! \operatorname{vol}(\mathcal{P})$ y $i_1 + \ldots + i_k \in \deg Y_{\mathcal{A}(\mathcal{P})}\ \mathcal{P}$.

Ahora consideramos el caso general. Sea b_0 un vector entero en $\mathcal{P}$, y sea $\mathcal{Q} := \mathcal{P} - b_0$. Por lo anterior existen $D \in \mathbb{N}$, $a_0 \in \mathbb{Z}^n$ y $g_1, \ldots, g_s \in k[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ tales que

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

con $D \leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{Q})$, $a_0 \in \rho! \operatorname{vol}(\mathcal{Q})\ \mathcal{Q}$ y $\mathcal{N}(g_i f_i) \subseteq (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{Q}))^2\ \mathcal{Q} - a_0$ para $i = 1, \ldots, s$.

Sea $a := a_0 + (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2 \cdot b_0$. Concluimos

$$\begin{aligned} a &\in (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2\ \mathcal{P}, \\ \mathcal{N}(g_i f_i) &\subseteq (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2\ \mathcal{P} - a, \end{aligned}$$

para $i = 1, \ldots, s$. □

Mantenemos la notación del teorema 2.2.3. Sea $\mathcal{N}$ el polítopo de Newton de $p, f_1, \ldots, f_s$ y sea $\mathcal{U}$ el volumen no mezclado de este polítopo. Asumimos además que $n \geq 2$. En esta situación podemos tomar a $\mathcal{P}$ como al polítopo $(n-1)\mathcal{N}$. Obtenemos las cotas

$$D \leq n^{n+2} \mathcal{U}, \qquad \mathcal{N}(g_i f_i) \subseteq (n^{2n+3} \mathcal{U}) \cdot \mathcal{N} - a.$$

para algún $a \in (n^{2n+3} \mathcal{U}) \cdot \mathcal{N}$. Como antes, es fácil verificar que estas mismas cotas valen también en el caso $n = 1$. El teorema 3 se sigue de esta observación en el caso particular

$p = 1$.

Para una función racional $q = f/g \in k(x_1, \ldots, x_n)$ definida como el cociente de dos polinomios sin factores comunes, se define el *grado* de q como

$$\deg q := \max\{\deg f, \deg g\}.$$

Derivamos del teorema 2.2.3 la siguiente cota de grado:

Corolario 2.2.4 *Mantenemos la notación del teorema 2.2.3. Sea* $d := \max_i \deg f_i$. *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*

$$p^D = g_1 f_1 + \cdots + g_s f_s$$

con $D \leq \rho! \min\{n+1, s\}^2 \operatorname{vol}(\mathcal{P})$, $a \in (\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2 \cdot \mathcal{P}$ *y* $\deg(g_i f_i) \leq d\,((1 + \deg p)\rho! \min\{n+1, s\} \operatorname{vol}(\mathcal{P}))^2$ *para* $i = 1, \ldots, s$.

$\square$

2.3 Cotas de Altura

2.3.1 División módulo Variedades Intersección Completa

La fórmula de la traza de Tate ha sido utilizada recientemente en distintos trabajos sobre 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 [48], [83], [115], [62], por nombrar sólo algunas referencias. En esta subsección vamos a seguir este último punto de vista.

Sea k un FP–cuerpo y sea $A := k[t_1, \ldots, t_m]$ un anillo de polinomios sobre k. 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. Para $f \in A[x]$ denotamos por $\deg^{(t)} f$ y $\deg^{(x)} f$ el grado de f en las variables $t_1, \ldots, t_m$ y $x_1, \ldots, x_n$ respectivamente.

Sea $F := \{F_1, \ldots, F_n\} \subseteq A[x_1, \ldots, x_n]$ una intersección completa reducida de polinomios de grado acotado por d en las variables $x_1, \ldots, x_n$, que genera un ideal radical $(F) := (F_1, \ldots, F_n)$. Consideramos el A–álgebra

$$B := A[x]/(F) = A[x_1, \ldots, x_n]/(F_1, \ldots, F_n).$$

Asumimos que $A \hookrightarrow B$ es una inclusión finita y separable, que corresponde a una normalización de Noether de la variedad $V(F) \subseteq \mathbb{A}^n$. Luego B es un A–módulo libre de rango acotado por el grado de la variedad $V(F)$.

Sean entonces $f, g \in A[x_1, \ldots, x_n]$ polinomio 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 $\overline{g} = \overline{q}_1 \cdot \overline{f}$. Este apartado está dedicado al problema de la *división*, que consiste en encontrar un polinomio $q \in A[x_1, \dots, x_n]$ de bajo grado y altura tal que $\overline{g} = \overline{q} \cdot \overline{f}$. Resolvemos este problema mediante el uso de la fórmula de la traza.

El siguiente es el resultado principal de esta subsección. Este resultado es un refinamiento del teorema de división de Krick–Pardo [83, Teorema 29].

Proposición 2.3.1 *(Teorema de División) Sea $A := k[t_1, \dots, t_m]$ y sea $A[x] := A[x_1, \dots, x_n]$ el anillo de polinomios n–variados con coeficientes en A. Sea $F := \{F_1, \dots, F_n\} \subseteq A[x]$ una intersección completa reducida que define una variedad $V := V(F) \subseteq \mathbb{A}^n$ de grado δ. Sean $d := \deg F$, $h := m(F)$. Sea $B := A[x]/(F)$, y asumimos que $A \hookrightarrow B$ es una inclusión finita y separable,*

Sean $f, g \in A[x]$ polinomios tales que $\overline{f} \in B$ es un no–divisor de cero y $\overline{f} \mid \overline{g}$ en B.

Entonces existe $q \in A[x]$ tal que

$$\overline{g} = \overline{q} \cdot \overline{f} \in B$$

que satisface

$$\begin{aligned}
\deg^{(x)} q &\leq n\,(d-1),\\
\deg^{(t)} q &\leq (2\,n\,d + \deg f)\,\delta^2 + \deg^{(x)} g \cdot \delta + \deg^{(t)} g,\\
m(q) &\leq c\,(d^2\,\delta^4 + (\deg f)^2\,\delta^4 + (\deg^{(x)} g)^2\,\delta^2)(h + h(V) + \delta^2) + 5\,\delta(h + m(f)) + m(g),
\end{aligned}$$

donde c sólo depende de m, n.

Se puede tomar $c := 10^3\,(m+n+1)^6$.

Este resultado es una consecuencia de la fórmula de traza de Tate. En lo que sigue vamos a describir los aspectos básicos de la teoría de dualidad en álgebras de Gorenstein necesarios para su demostración. La referencia standard es el libro de Kunz [87].

Consideramos a $B^* := \mathrm{Hom}_A(B, A)$ como un B–módulo con la multiplicación definida por $b \cdot \tau(x) := \tau(b \cdot x)$ para $b \in B$ y $\tau \in B^*$. El módulo dual B^* es un B–módulo libre de rango 1, debido a que B es una A–álgebra de Gorenstein. Un generador σ de B^* como B–módulo se llama una *traza* de B.

Hay dos elementos relevantes en B^*, que denotamos por Tr y σ. El primero, Tr, es la *traza canónica* de B, y se define de la siguiente manera. Dado $b \in B$, sea $L_b(x) : B \to B$ el morfismo A–lineal definido por $L_b(x) := b \cdot x$ para $x \in B$. Luego $\mathrm{Tr}(b)$ se define como la traza del endomorfismo L_b de B. Esta definición tiene sentido, ya que B es un A–módulo libre.

La traza canónica no es en general una traza de B, es decir, Tr no es un generador de B^*. Ahora vamos a introducir a σ, que es una traza en este sentido.

Sean $y_1, \dots, y_n$ nuevas variables y sea $y := (y_1, \dots, y_n)$. Sean $F_i^{\langle x \rangle} := F_i(x)$ y $F_i^{\langle y \rangle} := F_i(y)$. El polinomio $F_i^{\langle x \rangle} - F_i^{\langle y \rangle}$ pertenece al ideal $(y_1 - x_1, \dots, y_n - x_n)$. Sean $l_{ij} \in A[x, y]$

tales que

$$F_i^{\langle y \rangle} - F_i^{\langle x \rangle} = \sum_{j=1}^{n} l_{ij}\,(y_j - x_j).$$

Notamos que los polinomios l_{ij} no son únicos. Consideramos el determinante Δ de la matriz $(l_{ij})_{ij}$, que se puede escribir como

$$\Delta = \sum_m a_m(x) \cdot b_m(y)$$

con $a_m \in A[x]$ y $b_m \in A[y]$. Nuevamente, los polinomios a_m, b_m no están unívocamente determinados. El polinomio Δ se llama un *determinante pseudo–Jacobiano* de la intersección completa F.

Sea $c_m := b_m(x)$. 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

$$\overline{g} = \sum_m \sigma(\overline{g} \cdot \overline{a}_m) \cdot \overline{c}_m \in B$$

para todo $g \in A[x]$. Esta identidad se conoce como la *fórmula de la traza de Tate* [87, Apéndice F].

Sea $\overline{J}$ la clase en B del Jacobiano $J(F)$. Se tiene la identidad

$$\overline{J} = \sum_m \overline{a}_m \cdot \overline{b}_m$$

que justifica el nombre de pseudo–Jacobiano para Δ.

Los elementos Tr y σ están relacionados por la identidad

$$\overline{J} \cdot \sigma = \mathrm{Tr}$$

es decir, $\mathrm{Tr}(b) = \sigma(\overline{J} \cdot b)$ para todo $b \in B$.

Notamos que los polinomios l_{ij} se pueden elegir de grado acotado por $d-1$, y por lo tanto los polinomios a_m, c_m se pueden elegir de grado acotado por $n\,(d-1)$. La fórmula de la traza se puede aplicar entonces 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 a B como un A–módulo.

Demostración de la Proposición 2.3.1. Mantenemos la notación de la discusión anterior. Sea K el cuerpo de fracciones de A y sea $L := K \otimes_A B$. El hecho de que B es un A–módulo libre implica que el morfismo $\sigma \in B^*$ se extiende en forma única a un morfismo $\sigma \in \mathrm{Hom}_K(L, K)$.

El polinomio f es un no–divisor de cero en B y por lo tanto es una unidad en L. Sea $q_1 \in A[x_1, \ldots, x_n]$ tal que $\overline{q}_1 \cdot \overline{f} = \overline{g}$ en B. Luego $\overline{q}_1 = \overline{f}^{-1} \cdot \overline{g}$ en L y por lo tanto

$$\sigma(\overline{f}^{-1} \cdot \overline{g} \cdot \overline{p}) = \sigma(\overline{q}_1 \cdot \overline{p}) \in A$$

para $p \in A[x_1, \ldots, x_n]$. Consideramos entonces el polinomio

$$q := \sum_m \sigma(\overline{f}^{-1} \cdot \overline{g} \cdot \overline{a}_m)\, c_m = \sum_m \operatorname{Tr}(\overline{J}^{-1} \cdot \overline{f}^{-1} \cdot \overline{g} \cdot a_m)\, c_m \in A[x_1, \ldots, x_n].$$

Como consecuencia de la fórmula de la traza de Tate se tiene $\overline{q} \cdot \overline{f} = \overline{g}$ en B. Se tiene

$$\deg^{(x)} q \leq n(d-1).$$

En lo que sigue vamos a estimar el grado con respecto a las variables $t_1, \ldots, t_m$ y la altura del polinomio q. Sea

$$l_{ij} := (F_i(y_1, \ldots, y_j, x_{j+1}, \ldots, x_n) - F_i(y_1, \ldots, y_{j-1}, x_j, \ldots, x_n))/(y_j - x_j) \in A[x, y]$$

de forma tal que se verifica $F_i^{\langle y \rangle} - F_i^{\langle x \rangle} = \sum_j l_{ij}\,(y_j - x_j)$. Se tiene $\deg l_{ij} \leq d-1$ y $\overline{m}(l_{ij}) \leq h + 2\,(m+n)\,d$, y por lo tanto

$$\begin{aligned} \deg a_m, \deg c_m &\leq n\,(d-1), \\ \overline{m}(a_m), \overline{m}(c_m) &\leq n\,h + 5\,(m+n)^2\,d. \end{aligned}$$

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

$$f^* := f^{\mu-1} + \alpha_{\mu-1}f^{\mu-2} + \cdots + \alpha_1 \in A[x].$$

Se tiene entonces $\overline{f} \cdot \overline{f}^* = -\alpha_0 \in A - \{0\}$. Se tiene $\deg m_f \leq \deg f \cdot \delta$ por el teorema 1.3.4 y por lo tanto

$$\deg \alpha_0, \deg f^* \leq 2 \deg f \cdot \delta.$$

Por otra parte se tiene $m(m_f) \leq c_1(\deg f)^2 \cdot \delta^2(h(V) + \delta^2) + c_2\,\delta \cdot m(f)$, por el corolario 1.3.12. Las constantes c_1, c_2 sólo dependen de m, n, y se puede tomar $c_1 := 96\,(m+n+1)^4$ y $c_2 := 4$. Queda entonces

$$m(\alpha_0), m(f^*) \leq (c_1+1)(\deg f)^2\,\delta^2(h(V) + \delta^2) + (c_2+1)\,\delta \cdot m(f).$$

Se tiene además $\deg J \leq n(d-1)$ y $m(J) \leq n\,h + 7\,n\,(2n+m)\,d$. En forma análoga obtenemos polinomios $J^* \in A[x]$ y $\beta_0 \in A - \{0\}$ tales que $\overline{J} \cdot \overline{J}^* = -\beta_0$ en B. Se tienen las estimaciones

$$\begin{aligned} \deg \beta_0, \deg J^* &\leq 2\,n\,d\,\delta, \\ m(\beta_0), m(J^*) &\leq (c_1+1)(n\,d\,\delta)^2(h(V)+\delta^2) + (c_2+1)(n\,h + 7\,n\,(2n+m)\,d)\,\delta. \end{aligned}$$

Sea $\Lambda_m := \operatorname{Tr}(\overline{J}^* \cdot \overline{f}^* \cdot \overline{g} \cdot \overline{a}_m)$. Luego

$$\begin{aligned} \deg^{(t)} \Lambda_m &\leq (2n\,d\,\delta + 2\deg f \cdot \delta + \deg^{(x)} g)\,\delta + \deg^{(t)} g, \\ m(\Lambda_m) &\leq c\,(d^2\,\delta^4 + (\deg f)^2\,\delta^4 + (\deg^{(x)} g)^2\,\delta^2)(h + h(V) + \delta^2) \\ &\quad +5\,\delta\,(h + m(f)) + m(g). \end{aligned}$$

por la proposición 1.3.13, con $c := 5 \cdot 10^2\,(m+n+1)^6$. Se tiene

$$\alpha_0 \cdot \beta_0 \cdot q = \sum_m \Lambda_m$$

y por lo tanto

$$\begin{aligned}
\deg^{(t)} q &\le (2\,n\,d\,\delta + 2\deg f \cdot \delta + \deg^{(x)} g)\,\delta + \deg^{(t)} g, \\
m(q) &\le c\,(d^2\,\delta^4 + (\deg f)^2\,\delta^4 + (\deg^{(x)} g)^2\,\delta^2)(h + h(V) + \delta^2) \\
&\quad +5\,\delta\,(h + m(f)) + m(g) + n\,d + n.
\end{aligned}$$

□

Consideramos también el problema de la *interpolación*: dado un polinomio $g \in A[x]$, encontrar $g_1 \in A[x]$ de grado acotado por $n\,d$ con respecto a las variables $x_1, \ldots, x_n$ tal que $\overline{g} = \overline{g}_1$ en B. Este es un caso particular del problema de la división. Mantenemos la notación de la proposición 2.3.1. La fórmula de la traza 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. Se tiene

$$\begin{aligned}
\deg^{(x)} g_1 &\le n\,d, \\
\deg^{(t)} g_1 &\le 2\,n\,d\,\delta^2 + \deg^{(x)} g \cdot \delta + \deg^{(t)} g, \\
m(g_1) &\le c\,(d^2\,\delta^4 + \deg^{(x)} g)^2\,\delta^2)(h + h(V) + \delta^2) + 5\,\delta\,h + m(g).
\end{aligned}$$

2.3.2 Un Teorema de Ceros Aritmético sobre Variedades Intersección Completa

Sea k un FP–cuerpo. Sea $F := \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ una intersección completa reducida de polinomios que definen una variedad $V := V(F) \subseteq \mathbb{A}^n$.

Sean $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polinomios sin ceros comunes en V . El teorema de ceros de Hilbert dice entonces que existen $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ tales que

$$\overline{1} = \overline{g}_1\,\overline{f}_1 + \cdots + \overline{g}_s\,\overline{f}_s \in k[V].$$

Vamos a tratar el problema de acotar los grados y las alturas de $g_1, \ldots, g_s$. Resolvemos este problema usando el teorema de división 2.3.1. En este punto seguimos las líneas de la demostración de Krick–Pardo [83].

Teorema 2.3.2 *(Teorema de Ceros Aritmético) Sea k un FP–cuerpo y sea $F := \{F_{r+1}, \ldots, F_n\} \subseteq k[x_1, \ldots, x_n]$ una intersección completa reducida que define una variedad $V := V(F) \subseteq \mathbb{A}^n$ de grado δ .*

Sean $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ *polinomios sin ceros comunes en* V. *Sean* $d := \max_i \deg f_i$ *y* $h := \max_i \overline{m}(f_i)$, *y sean* $D \geq d, \deg F$ *y* $H \geq h, \overline{m}(F)$.

Entonces existen $g_1, \dots, g_s \in k[x_1, \dots, x_n]$ *tales que*

$$\overline{1} = \overline{g}_1 \, \overline{f}_1 + \cdots + \overline{g}_s \, \overline{f}_s \in k[V]$$

con $\deg g_i \leq 5\, n^2 \, D \, d^{2\,r} \, \delta^2$ *y* $\overline{m}(g_i) \leq c\, D^2 (d^r \, \delta)^{12} (H + h(V) + d^r \, \delta)$, *donde* c *sólo depende de* n.

Se puede tomar $c := 10^8 \, (n+1)^{16}$. Se tienen las estimaciones

$$\deg V \leq D^{n-r}, \qquad h(V) \leq \kappa_1(n) \, D^{8\,(n-r)} \, H + \kappa_2(n) D^{9\,(n-r)},$$

aunque estos parámetros pueden ser mucho menores en algunos casos particulares.

Aplicamos el resultado anterior al caso $k := \mathbb{Q}$ y $V := \mathbb{A}^n$. Sean $f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n]$ polinomios enteros sin ceros comunes en $\mathbb{A}^n$. Sean $d := \max_i \deg f_i$ y $h := \max_i h(f_i)$. Obtenemos entonces que existen $a \in \mathbb{Z} - \{0\}$ y $g_1, \dots, g_s \in \mathbb{Z}[x_1, \dots, x_n]$ tales que

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

con $\deg g_i \leq 5\, n^2 \, d^{2\,r}$ y $h(a), h(g_i) \leq c(n) \, d^{12\,r} \, (h + d^r)$. De esta forma reobtenemos esencialmente los resultados de Berenstein-Yger [13] y Krick–Pardo [83].

Consideramos luego el caso $k := k_0(t_1, \dots, t_m)$ y $V := \mathbb{A}^n$. Sea $A := k_0[t_1, \dots, t_m]$ el anillo de polinomios m–variados sobre un cuerpo k_0. Sean $f_1, \dots, f_s \in A[x_1, \dots, x_n]$ polinomios sin ceros comunes en $\mathbb{A}^n$. Sean $d := \max_i \deg^{(t)} f_i$ y $h := \max_i \deg^{(x)}(f_i)$. Entonces existen $a \in A - \{0\}$ y $g_1, \dots, g_s \in A[x_1, \dots, x_n]$ tales que

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

con $\deg^{(x)} g_i \leq 5\, n^2 \, d^{2\,r}$ y $\deg^{(t)} a, \deg^{(t)} g_i \leq c(n) \, d^{12\,r} \, (h + d^r)$. De esta forma reobtenemos el teorema de ceros paramétrico de Smietanski [120].

El resto de esta subsección está dedicado a la demostración del teorema 2.3.2. Para poder aplicar el teorema de división necesitamos preparar previamente los polinomios $f_1, \dots, f_s$ y poner a las variables $x_1, \dots, x_n$ en posición general.

En primer lugar mostramos que los polinomios $f_1, \dots, f_s$ pueden reemplazarse por una sucesión regular reducida.

Lema 2.3.3 *Mantenemos la notación del teorema 2.3.2. Entonces existen polinomios* $h_1, \dots, h_t \in (f_1, \dots, f_s)$ *para algún* $t \leq \min\{r, s\}$ *que forman una sucesión regular reducida débil en* $k[V]$ *tales que*

$$\deg h_i \leq d + 1, \qquad \overline{m}(h_i) \leq h + \log \delta + 4\, n\, d.$$

Demostración. Construimos inductivamente a los polinomios h_i como combinaciones lineales de los polinomios f_i, eventualmente multiplicados por variables. Asumimos que $h_1, \ldots, h_i$ ya están construídos. Sean u_i, u_{kl} variables y sea

$$H_{i+1} := \sum_i u_i\, f_i + \sum_{k\,l} u_{kl}\, x_k \cdot f_l.$$

Sea $V_i := V \cap V(h_1, \ldots, h_i) \subseteq \mathbb{A}^n$ la variedad definida por $h_1, \ldots, h_i$ en V. Sean $y_1, \ldots, y_n$ variables tales que $y_1, \ldots, y_{r-i}$ están en posición de Noether con respecto a V_i para todo i.

Sean entonces $A_i := k[u][y_1, \ldots, y_{r-i}]$, E_i el cuerpo de fracciones de A_i y $F_i := E_i \otimes_k k[V_i]$. Luego F_i es una E_i–álgebra finita de dimensión $[F_i : E_i] \leq d^i \cdot \delta$. Sea $L_{i+1} : F_i \to F_i$ la aplicación $g \mapsto H_{i+1} \cdot g$, y sea

$$\phi := \det L_{i+1} \in k[u]$$

la norma de H_{i+1} sobre E_i. Luego $\phi \neq 0$, ya que $f_1, \ldots, f_s$ definen la variedad vacía en V_i. Se tiene además $\deg \phi \leq (d+1)^i \deg V$.

Por otra parte, sea $J \in k[u][x_1, \ldots, x_n]$ el Jacobiano de $F_1, \ldots, F_{n-r}, h_1, \ldots, h_i, H_{i+1}$ con respecto a las variables $y_{r-i}, \ldots, y_n$. Luego J es no–divisor de cero en $k[V]$. Esto es una consecuencia del teorema de Bertini y del Criterio Jacobiano [59]. Consideramos la norma de J, es decir

$$\psi := \det L_J \in k[u].$$

Se tiene $\deg^{(u)} J \leq n - r + i$ y por lo tanto ψ es un polinomio no nulo de grado acotado por $(n-r+i)\,(d+1)^i\,\delta$. Luego $\phi \cdot \psi$ es un polinomio no nulo tal que

$$\deg \phi \cdot \psi \leq n\,(d+1)^i\,\delta.$$

Luego tanto existe $a \in k^{(n+1)\,s}$ tal que $\phi \cdot \psi(a) \neq 0$ y $\overline{h}(a) \leq i \log(d+1) + \log \delta + \log n$. El polinomio $h_{j+1} := H_{j+1}(a)$ satisface las condiciones del enunciado.

□

El paso siguiente consiste en poner a las variables $y_1, \ldots, y_n$ en posición de Noether simultáneamente con respecto a todas las variedades que se consideran.

Lema 2.3.4 *Mantenemos la notación del párrafo anterior. Sea $V_i := V \cap V(h_1, \ldots, h_i) \subseteq \mathbb{A}^n$ la variedad definida por $h_1, \ldots, h_i$ en V. Entonces existen variables $y_1, \ldots, y_r \in k[x_1, \ldots, x_n]$ tales que $y_1, \ldots, y_{r-i}$ están en posición de Noether separable con respecto a V_i para todo i. Se tiene además*

$$\overline{h}(y_i) \leq 2\,r\,(d+1) + \log \delta.$$

Demostración. Sean

$$Y_i = U_{i0} + U_{i1} x_1 + \cdots + u_{in} x_n$$

formas lineales genéricas para $i = 1, \ldots, r$. Sea $a_i \in k[U]$ el coeficiente principal del polinomio característico P_{V_i} de la variedad V_i, y sea $\rho_i \in k[U, T]$ el discriminante de

P_{V_i}. Sea entonces $b := \prod_i a_i \cdot \rho_i$. Luego b es un polinomio no nulo de grado acotado por $r\,(d+1)^{2r}\,\delta^2$ en cada grupo de variables U_i. Sea $a \in k^{r(n+1)}$ tal que

$$b(a) \neq 0.$$

Se puede tomar a_i de altura acotada por $\log r + 2\,r\,\log(d+1) + 2\,\log\delta$. Luego $y_i := Y_i(a)$ verifica las condiciones del enunciado. □

Demostración del Teorema 2.3.2. Mantenemos la notación de los lemas anteriores. Sea $V_i := V \cap V(f_1,\dots,f_i) \subseteq \mathbb{A}^n$ como la variedad definida por $f_1,\dots,f_i$ en V. Se tiene

$$\deg V_i \leq d^i\,\delta, \qquad\qquad h(V_i) \leq \kappa_1\,(d^i\,\delta)^8 (h + h(V)) + \kappa_2\,(d^i\,\delta)^9$$

donde κ_1, κ_2 son las constantes que intervienen en el enunciado del corolario 1.4.5. Primeramente consideramos el caso en que $s \leq r$, $\overline{f}_1,\dots,\overline{f}_s \in k[V]$ es una sucesión regular, y las variables $x_1,\dots,x_{r-i}$ están en posición de Noether con respecto a V_i para todo i.

Sea entonces $A_i := k[x_1,\dots,x_{r-i}]$ y $B_i := k[V]/(f_1,\dots,f_i) = k[V_i]$. Luego $F_1,\dots,F_{n-r}$, $f_1,\dots,f_i \in k[x_1,\dots,x_n]$ forman una intersección completa reducida, y $A_i \hookrightarrow B_i$ es una inclusión entera y separable. Estamos entonces en condiciones de aplicar el teorema de división 2.3.1.

Vamos a construir inductivamente $g_1,\dots,g_s \in k[x_1,\dots,x_n]$ tales que

$$\overline{1} = \overline{g}_{i+1}\,\overline{f}_{i+1} + \cdots + \overline{g}_s\,\overline{f}_s \in k[V_i].$$

Para un polinomio $g \in A_i[x_{r-i+1},\dots,x_n]$ denotamos por $\deg^\circ g$ y por $\deg^* g$ su grado en las variables *libres* $x_1,\dots,x_{r-i}$ y en las variables dependientes $x_{r-i+1},\dots,x_n$ respectivamente.

Hacemos inducción en i. En primer lugar tomamos $g_s \in A_{s-1}[x_{r-s},\dots,x_n]$ tal que

$$\overline{1} = \overline{g_s}\,\overline{f_s} \in B_{s-1}$$

con $\deg^* g_s \leq n\,D$, $\deg^\circ g_s \leq 3\,n\,D\,d^{2\,s-2}\,\delta^2$ y $\overline{m}(g_s) \leq c\,D^2\,(d^{s-1}\,delta)^{12}\,(h + h(V) + d^{s-1}\,\delta)$. Se puede tomar $c := 10^7\,(n+1)^{13}$.

Ahora sea $i \leq s-1$. Hacemos

$$b_{i+1} = 1 - g_{i+1}f_{i+1} + \cdots + g_s f_s \in A_i[x_{r-1+1},\dots,x_n].$$

Luego $\overline{f}_{i+1} \in B_1$ es un no–divisor de cero, y se tiene $\overline{f}_{i+1}\,|\,\overline{b}_{i+1}$ en B_i. Aplicamos el teorema de división y obtenemos un polinomio g_{i+1} de grado y altura controlada tal que $\overline{b}_{i+1} = \overline{g}_{i+1}\cdot\overline{f}_{i+1}$ en B_i. Se tiene

$$\begin{aligned}
\deg^* g_{i+1} &\leq n\,D,\\
\deg^\circ g_{i+1} &\leq 3\,n\,D\,\delta_i^2 + \deg^* b_{i+1}\cdot\delta_i + \deg^\circ b_{i+1},\\
\overline{m}(b_{i+1}) &\leq c_1(2\,D^2\,\delta_i^4 + (\deg^* b_{i+1})^2\,\delta_i^2)(H + h(V_i) + \delta_i^2) + m(b_{i+1}),
\end{aligned}$$

con $c_1 := (10^3+1)(n+1)^6$. Tratamos en primer lugar la cota de grado del polinomio g_{i+1} con respecto a las variables libres. Asumimos $\deg^\circ g_j \le 4\,(s-j+1)\,n\,D\,d^{2\,s}\,\delta^2 - d$ para $j = s, \ldots, i+2$. Se tiene entonces

$$\deg^\circ g_{i+1} \le 4\,(s-i)\,n\,D\,d^{2\,s}\,\delta^2 - d$$

Tratamos ahora la cota para la altura de g_{i+1}. Se tiene

$$h(V_i) \le \kappa_1 (d^s\,\delta)^8 (h + h(V)) + \kappa_2 (d^s\,\delta)^9$$

por la desigualdad de Bézout aritmética. Asumimos entonces

$$\overline{m}(g_j) \le c_2 (s-j+1)\,D^2\,(d^s\,\delta)^{12} (H + h(V) + d^s\,\delta)$$

para $j = s, \ldots, i+2$, con $c_2 := 2 \cdot 10^7\,(n+1)^{15}$. Se obtiene

$$\overline{m}(g_{i+1}) \le c_2 (s-i)\,D^2\,(d^s\,\delta)^{12} (H + h(V) + d^s\,\delta).$$

El caso general se reduce a este por medio de los lemas 2.3.3 y 2.3.4. $\square$

2.3.3 Distancia entre Variedades

En esta subsección estudiamos los aspectos métricos de las variedades. La altura de una variedad nos permite estimar la localización de sus puntos. Por ejemplo, en el caso en que $V \subseteq \mathbb{A}^n(\mathbb{C})$ es una $\mathbb{Q}$–variedad de dimensión 0 se tiene

$$V \subseteq \{\xi \in \mathbb{A}^n : \log ||\xi|| \le h(V) + \log(n+1)\,\delta\}$$

donde $||\xi|| := \max_i |\xi_i|$ denota la norma del supremo.

Sean $V, W \subseteq \mathbb{A}^n(\mathbb{C})$ $\mathbb{Q}$–variedades y sea $\alpha > 0$. Definimos la función *distancia* $\mathrm{dist}_\alpha(V, W)$ como la distancia entre V y W en la bola $B(0, \alpha) := \{\xi \in \mathbb{A}^n : ||\xi|| \le \alpha\}$. Para $V, W \subseteq \mathbb{A}^n$ $\mathbb{Q}$–variedades tales que $V \cap W = \emptyset$ consideramos el problema de estimar la distancia entre V y W.

Este problema está en estrecha relación con el teorema de ceros aritmético sobre variedades. En la situación que consideramos se tiene $1 \in I(V) + I(W)$. Sea $F \in I(W)$ tal que

$$1 \equiv \overline{F} \in k[V]$$

con $\deg F = D$ y $\overline{h}(F) = H$. Vamos a mostrar que una cota para D, H implica en forma directa una estimación para la distancia entre V y W.

Sea $\alpha > 0$, y sean $\xi \in V$ y $\varrho \in W$ tales que $\xi, \varrho \in B(0, \alpha)$. Desarrollamos a F alrededor de ϱ. Se tiene

$$F = \sum_i a_i\,(x - \varrho)^i$$

con $a_i := \partial_i F(\varrho)$. Se tiene $\log |a_i| \le H + (\log \alpha + \log n)\,D$. Sea $\epsilon := ||\xi - \varrho||$ y supongamos que se tiene $\epsilon \le 1$. Evaluamos $x := \xi$ y queda

$$\begin{aligned} 0 &\le \log |F(\xi)| \le \log(\max_i |a_i|) + D + n + \log \epsilon \\ &\le H + (\log \alpha + 2\,n)\,D + \log \epsilon \end{aligned}$$

es decir
$$-\log(\mathrm{dist}_\alpha(V,W)) \le H + (2\,n + \log\alpha)\,D.$$

A partir de los resultados de la subsección anterior obtenemos la siguiente estimación para el caso en que V y W son variedades intersección completa reducida.

Teorema 2.3.5 *Sean $V,W \subseteq \mathbb{A}^n(\mathbb{C})$ $\mathbb{Q}$–variedades tales que $V \cap W = \emptyset$. Sean r,s la dimensión de V y de W respectivamente. Sea δ el grado de V. Asumimos que V y W son variedades intersección completa reducida de polinomios $f := \{f_1,\dots,f_{n-r}\}, g := \{g_1,\dots,g_{n-s}\} \subseteq k[x_1,\dots,x_n]$, respectivamente. Sean $d := \deg f$, $h := \overline{m}(f)$, $D := \deg g$ y $H := \overline{m}(g)$. Entonces*

$$\log(\mathrm{dist}_\alpha(V,W)) \ge -c\,d^2\,D^{12\,r+2}\,\delta^{12}(h + H + h(V) + D^r\,\delta + \log\alpha)$$

para $\alpha > 0$, donde c sólo depende de n.

□

Se puede tomar $c := 2\cdot 10^8\,(n+1)^{16}$. A partir de este resultado derivamos la siguiente cota para el caso general.

Corolario 2.3.6 *Sean $V,W \subseteq \mathbb{A}^n(\mathbb{C})$ $\mathbb{Q}$–variedades tales que $V \cap W = \emptyset$. Sean r, s la dimensión de V y de W respectivamente, y asumimos $r + s \ge n+1$. Entonces*

$$\log(\mathrm{dist}_\alpha(V,W)) \ge -c(n)\,(\deg V)^{12\,s}\,(\deg W)^{12\,r}(h(V) + h(W) - \log\alpha)$$

para $\alpha > 0$, donde c sólo depende de n.

Se puede tomar $c := 10^9\,(n+1)^{16}$.

Demostración. Las variedades V, W están contenidas en variedades intersección completa reducida X, $Y \subseteq \mathbb{A}^n$ tales que $X \cap Y = \emptyset$. La variedad $X \subseteq \mathbb{A}^n$ está definida por polinomios $f_1,\dots,f_{n-r} \in k[x_1,\dots,x_n]$ tales que

$$\deg f_i \le \deg V, \qquad\qquad \overline{m}(f_i) \le h(V) + 10\,n^2\,\deg V.$$

Análogamente la variedad $Y \subseteq \mathbb{A}^n$ está definida por polinomios $g_1,\dots,g_{n-s} \in k[x_1,\dots,x_n]$, y valen cotas análogas para los grados y las alturas de estos polinomios. Luego la estimación para la distancia entre V y W se sigue del resultado anterior.

□

Esta estimación parece estar lejos de ser óptima en términos de el grado y la altura de las variedades V y W. Formulamos la siguiente conjetura para el caso general del teorema de ceros aritmético sobre variedades.

Conjetura 2.3.1 *Sea* k *un* FP *–cuerpo. Sean* V *,* $W \in \mathbb{A}^n$ k *–variedades tales que* $V \cap W = \emptyset$ *. Entonces existe* $F \in I(W)$ *tal que*

$$\overline{1} = \overline{F} \in k[V]$$

con $\deg F \leq \deg V \cdot \deg W$ *y* $m(F) \leq \deg V \cdot h(W) + \deg W \cdot h(V) + c(n) \deg V \cdot \deg W$ *.*

Resultados recientes de Kollár [79] muestran la validez de la cota de grado propuesta, y dan así sustento a nuestra conjetura.

Por la discusión anterior al teorema 2.3.5, esta conjetura implica — en el caso de ser cierta — la estimación

$$-\log(\mathrm{dist}_\alpha(V, W)) \leq \deg V \cdot h(W) + \deg W \cdot h(V) + (c(n) + 2\,n + \log \alpha) \deg V \cdot \deg W$$

para la distancia entre V y W .

Capítulo 3

Cotas para la Función de Hilbert

En este capítulo tratamos el problema de estimar globalmente la función de Hilbert de un ideal homogéneo de $k[x_0,\dots,x_n]$. Obtenemos una cota inferior para la función de Hilbert de un ideal homogéneo arbitrario (Teorema 3.1.2). Obtenemos además cotas superiores para el caso de un ideal primo (Teoremas 3.2.2 y 3.2.6) y para el caso de la suma de un ideal primo y un ideal principal (Teorema 3.2.8). Las cotas obtenidas dependen del grado de la dimensión del ideal en cuestión, y son esencialmente óptimas en términos de estos parámetros.

3.1 Cotas Inferiores

A lo largo de esta sección denotamos por k un cuerpo perfecto y por $\overline{k}$ su clausura algebraica. Para un ideal homogéneo I de $k[x_0,\dots,x_n]$, denotamos por $\dim I$ la dimensión de Krull del anillo cociente $k[x_0,\dots,x_n]/I$.

Sea I un ideal homogéneo de $k[x_0,\dots,x_n]$. La *función de Hilbert* o *función característica* de I se define como

$$h_I : \mathbb{Z} \to \mathbb{Z}, \qquad\qquad m \mapsto \dim_k(k[x_0,\dots,x_n]/I)_m.$$

Para una variedad proyectiva $V \subseteq \mathbb{P}^n$ denotamos por h_V la función de Hilbert de su ideal de definición $I(V)$.

Sea $I \subseteq k[x_0,\dots,x_n]$ un ideal homogéneo de dimensión r. Sea $p_I = a_{r-1}\, t^{r-1} + \cdots + a_0 \in \mathbb{Q}[t]$ su polinomio de Hilbert, de forma tal que se tiene

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

El *grado* $\deg I$ del ideal I se define como

$$\deg I := (r-1)!\; a_{r-1}.$$

Sea $I \subseteq k[x_0,\dots,x_n]$ un ideal radical homogéneo y sea $I = \cap_P P$ su descomposición primaria minimal. Luego se tiene

$$\deg I = \sum_{P} \deg V(P)$$

donde la suma se hace sobre los primos asociados P de I tales que $\dim P = \dim I$, y $\deg V(P)$ denota el grado de la variedad proyectiva $V(P) \subseteq \mathbb{P}^n$. Referimos a la subsección 1.2.1 para una discusión más detallada sobre la noción de grado de ideales y de variedades proyectivas.

Sean I, $J \subseteq k[x_0, \ldots, x_n]$ ideales homogéneos. Se tiene entonces la sucesión exacta de k–álgebras graduadas

$$\begin{array}{ccccc} 0 \to S/I \cap J \to & S/I \oplus S/J & \to & S/I + J & \to 0 \\ & (f, g) & \longmapsto & f - g & \end{array}$$

de donde se obtiene la identidad $h_{I\cap J}(m) = h_I(m) + h_J(m) - h_{I+J}(m)$. Se tiene en particular $\deg I \cap J = \deg I$ en el caso en que $\dim I > \dim J$.

Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo, y sea $f \in k[x_0, \ldots, x_n]$ un polinomio homogéneo de grado d que es un no–divisor de cero módulo I. Se tiene la sucesión exacta

$$0 \to S/I \xrightarrow{f} S/I \to S/(I, f) \to 0$$

y por lo tanto $h_{(I,f)}(m) = h_I(m) - h_I(m - d)$ y $\deg(I, f) = \deg f \cdot \deg I$.

Sea I un ideal homogéneo de $k[x_0, \ldots, x_n]$ y sea I^e el ideal extendido a $\overline{k}[x_0, \ldots, x_n]$. Entonces $h_I = h_{I^e}$, y en particular $\deg I^e = \deg I$. La propiedad de I de ser radical y equidimensional también se preserva por extensión del cuerpo de base [99, Teorema 26.3]. Esto nos permite asumir sin pérdida de generalidad que el cuerpo k es algebraicamente cerrado.

Consideramos en primer lugar el problema de acotar inferiormente la función de Hilbert de un ideal polinomial homogéneo arbitrario I de $k[x_0, \ldots, x_n]$. Nuestra demostración se basa en la reducción del caso general al caso en que $\dim I = 1$, es decir, cuando la variedad proyectiva $V(I)$ es finita. Consideramos este caso separadamente.

Lema 3.1.1 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo equidimensional de dimensión 1. Entonces*

$$\begin{array}{rclr} h_I(m) & \geq & m + 1, & m = 0, \cdots, \deg I - 2, \\ h_I(m) & = & \deg\ I, & m \geq \deg I - 1. \end{array}$$

Demostración. Sea m_0 el menor entero tal que h_I coincide con p_I, es decir, $h_I(m) = \deg\ I$ para $m \geq m_0$.

Asumimos que k es algebraicamente cerrado, y en particular infinito. Sea $\eta \in S$ una forma lineal no–divisor de cero módulo I. Se tiene entonces $h_{(I,\eta)}(m) = h_I(m) - h_I(m - 1)$.

Luego $h_{(I,\eta)}(m) \geq 1$ para $m = 0, \ldots, m_0 - 1$ y $h_{(I,\eta)}(m) = 0$ para $m \geq m_0$. Obtenemos así

$$h_I(m) \geq m + 1, \qquad\qquad m = 0, \ldots, \deg I - 2$$

y $h_I(m) = \deg\ I$ para $m \geq \deg I - 1$.

$\square$

Para $n, i \in \mathbb{Z}, i \geq 0$ definimos el número combinatorio $\binom{n}{i}$ como

$$\binom{n}{i} = \begin{cases} n!/i!(n-i)!, & \text{si} \quad n \geq 0, \\ 0, & \text{si} \quad n < 0. \end{cases}$$

Se tiene la identidad

$$\binom{m+r+D}{r} - \binom{m+r}{r} = \sum_{i=1}^{D} \binom{m+r-1+i}{r-1}.$$

El lema anterior se puede entonces escribir como $h_I(m) \geq \binom{m+1}{1} - \binom{m-\deg I+1}{1}$.

Teorema 3.1.2 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo de dimensión r, con $r \geq 1$. Entonces*

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

Demostración. Hacemos inducción en r. El caso $r = 1$ se sigue del lema 3.1.1. Luego consideramos el caso $r \geq 2$. Sea I^u la parte equidimensional de I. Se tiene entonces $h_I(m) \geq h_{I^u}(m)$ y $\deg I = \deg I^u$.

Sea $\eta \in \overline{k}[x_0, \ldots, x_n]$ una forma lineal no–divisor de cero módulo I^u. Luego $\dim(I^u, \eta) = r - 1$ y $\deg\ (I^u, \eta) = \deg\ I^u = \deg\ I$. Por la hipótesis inductiva se tiene

$$h_{(I^u,\eta)}(m) \geq \binom{m+r-1}{r-1} - \binom{m-\deg I+r-1}{r-1}.$$

Se tiene $h_{I^u}(m) = \sum_{j=0}^{m}(h_{I^u}(j) - h_{I^u}(j-1)) = \sum_{j=0}^{m} h_{(I^u,\eta)}(j)$ y por lo tanto

$$h_I\,(m) \geq h_{I^u}(m) \geq \sum_{j=0}^{m}\left\{\binom{j+r-1}{r-1} - \binom{j-\deg I+r-1}{r-1}\right\} = \binom{m+r}{r} - \binom{m-\deg I+r}{r}.$$

$\square$

Esta desigualdad extiende la estimación de Nesterenko para el caso de un ideal primo [104] al caso de un ideal arbitrario.

Para un ideal homogéneo $I \subseteq k[x_0, \ldots, x_n]$ denotamos por $H_I(t) := \sum_{m=0}^{\infty} h_I(m)\, t^m$ su *serie de Hilbert–Poincaré*. Sea $r := \dim I$. El resultado anterior puede ser enunciado como

$$H_I(t) \geq \frac{1 - t^{\deg I}}{(1-t)^{r+1}}$$

en el sentido de que esta desigualdad se verifica para cada término de estas series de potencias.

El teorema de persistencia de Gotzmann [60] implica que para un ideal homogéneo I de $k[x_0, \ldots, x_n]$ de dimensión r existe un entero $m_0 \in \mathbb{Z}$ tal que

$$h_I(m) \geq \binom{m+r}{r} - \binom{m - \deg I + r}{r}, \qquad m \geq m_0,$$

como fue notado en [22]. Nuestro teorema muestra que esta desigualdad vale globalmente, no sólo para valores grandes de m.

Nuestra estimación es óptima en términos de la dimensión y del grado del ideal I. En la siguiente proposición establecemos los casos extremales, que corresponden a hipersuperficies de subespacios lineales de $\mathbb{P}^n$. Esto es otra consecuencia del teorema de Gotzmann [22]. En lo que sigue damos una demostración autocontenida de este hecho.

Proposición 3.1.3 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo. Entonces*

$$h_I(m) = \binom{m+r}{r} - \binom{m-D+r}{r}$$

para todo m si y sólo si existe un cambio de variables $y_0, \ldots, y_n$ y un polinomio homogéneo $f \in k[y_0, \ldots, y_r]$ de grado D tal que

$$I = (f, y_{r+1}, \ldots, y_n).$$

Demostración. El polinomio f es un no–divisor de cero módulo el ideal $J := (y_{r+1}, \ldots, y_n)$ y por lo tanto se tiene

$$h_I(m) = h_J(m) - h_J(m - \deg f) = \binom{m+r}{r} - \binom{m-D+r}{r}.$$

Recíprocamente, sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo tal que

$$h_I(m) = \binom{m+r}{r} - \binom{m-D+r}{r}$$

para todo m. Luego $h_I(1) \leq r+1$, es decir $\dim_k I_1 \geq n - r$. Luego existe un cambio lineal de variables $y_0, \ldots, y_n$ tal que $y_{r+1}, \ldots, y_n \in I_1$. Sea $J := (y_{r+1}, \ldots, y_n)$. Se tiene

$$\begin{aligned} h_I(m) &= \binom{m+r}{r} = h_J(m), & m = 0, \ldots, D-1, \\ h_I(D) &= \binom{D+r}{r} - 1 < h_J(D). \end{aligned}$$

Sea $f \in I - J$ tal que $\deg f = D$. Sea $K := J + (f)$. Luego $K \subseteq I$ y $h_K(m) = h_I(m)$ para todo m, de donde concluimos $K = I$. □

3.2 Cotas Superiores

En esta sección consideramos el problema de acotar superiormente la función de Hilbert de un ideal homogéneo. Tratamos en primer lugar el caso de un ideal radical.

Sea $V \subseteq \mathbb{P}^n$ una variedad. Entonces la *clausura lineal* de V se define como la menor variedad lineal $L(V)$ de $\mathbb{P}^n$ que contiene a V.

Sea $E \subseteq \mathbb{P}^n$ una variedad lineal. Entonces su ideal de definición $I(E)$ está generado por formas lineales, y se tiene

$$\dim E = n - \dim_k I(E)_1.$$

Sea $V \subseteq \mathbb{P}^n$ una variedad y sea $L \in S$ una forma lineal. Entonces $L|_V \equiv 0$ si y sólo $L|_{L(V)} \equiv 0$. Luego el ideal de definición de $L(V)$ está generado por la parte de grado 1 de $I(V)$, es decir

$$I(L(V)) = (I(V)_1).$$

En particular tenemos

$$h_V(1) = n + 1 - \dim_k \ I_k\,(V)_1 = \dim L(V) + 1.$$

La dimensión de la clausura lineal de una variedad $V \subseteq \mathbb{P}^n$ se puede acotar en términos de su dimensión y de su grado. Se tiene

$$\dim L(V) + 1 \leq \deg V + \dim V.$$

Esta estimación es una consecuencia del teorema de Bertini [76, Teorema 6.3]. Puede encontrarse una demostración en el libro de Harris [63, Corolario 18.12].

La siguiente es una estimación para la función de Hilbert de una variedad irreducible.

Proposición 3.2.1 *Sea $V \subseteq \mathbb{P}^n$ una variedad irreducible de dimensión d, con $d \geq 0$. Entonces*

$$h_V(m) \leq \deg V \ m^d + d, \qquad\qquad m \geq 0.$$

Demostración. Para $n, m \in \mathbb{N}$, sea $N := \binom{m+n}{n} - 1$ y sea

$$v_m : \mathbb{P}^n \longrightarrow \mathbb{P}^N, \qquad\qquad (x_0 : \cdots : x_n) \mapsto (x^{(i)})_{|i|=m}$$

la aplicación de Veronese de grado m. Entonces $v_m|_V : V \mapsto v_m(V)$ es un morfismo birregular de grado m, y por lo tanto $h_{v_m(V)}\,(l) = h_V(m\,l)$. En particular se tiene

$$h_V(m) = h_{v_m(V)}\,(1) = \dim L(v_m(V)) + 1$$

y por lo tanto

$$h_V(m) \leq \deg v_m(V) + \dim v_m(V) \leq \deg V \ m^d + d.$$

□

Se puede extender esta estimación al caso más general de un ideal radical equidimensional de $k[x_0, \ldots, x_n]$.

Teorema 3.2.2 *Sea k un cuerpo perfecto y sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo radical y equidimensional de dimensión r, con $r \geq 1$. Entonces*

$$h_I(m) \leq \deg I \ m^{r-1} + \operatorname{irr} I \ (r-1), \qquad\qquad m \geq 1.$$

donde $\operatorname{irr} I$ *denota la cantidad de componentes irreducibles de la variedad* $V(I)$.

Demostración. Asumimos sin pérdida de generalidad que k es algebraicamente cerrado. Sea $I = \cap_P P$ la descomposición primaria minimal de I. De la inclusión canónica de módulos graduados

$$S/I \hookrightarrow \bigoplus_P S/P$$

se obtiene $h_I(m) \leq \sum_P h_P(m)$. Luego

$$h_I(m) \leq \sum_P (\deg V(P)\ m^{r-1} + r - 1) = \deg I\ m^{r-1} + \operatorname{irr} I\ (r-1)$$

por la proposición 3.2.1. □

Esta desigualdad tiene el mismo orden de crecimiento de h_I. No mejora, sin embargo, la estimación

$$h_I(m) \leq \deg I \tbinom{m+r-2}{r-1} + \operatorname{irr} I \tbinom{m+r-2}{r-2}$$

que se obtiene a partir de los argumentos de Chardin [35].

A partir del comportamiento asintótico de la función de Hilbert

$$h_I(m) \sim (\deg I/(r-1)!)\, m^{r-1}$$

se ve que esta desigualdad es precisa para valores grandes de m sólo cuando $r = 2$. En este caso, la estimación es óptima en términos de $\deg I$ y de $\operatorname{irr} I$. En lo que sigue vamos a determinar los casos extremales.

Sean $V, W \subseteq \mathbb{P}^n$ variedades. Entonces V, W son *proyectivamente equivalentes* si existe un automorfismo $A \in PGL_{n+1}(\overline{k})$ tal que $W = A(V)$ [63, p. 22]. Esta propiedad es equivalente al hecho de que los anillos de coordenadas $\overline{k}[V]$, $\overline{k}[W]$ sean isomorfos como $\overline{k}$–álgebras graduadas. En este caso las funciones de Hilbert de V y de W coinciden.

Una curva $C \subseteq \mathbb{P}^n$ proyectivamente equivalente a $v_n(\mathbb{P}^1)$ se llama una *curva racional normal*. Una curva racional normal C es no degenerada, es decir $L(C) = \mathbb{P}^n$, y tiene grado n. Luego el grado de C es el mínimo grado que puede tener una curva de $\mathbb{P}^n$ no degenerada [63, Corolario 18.12]. De hecho, las curvas racionales normales están caracterizadas por esta propiedad [63, Proposición 18.9].

Sean ahora $l, n \in \mathbb{N}$ y $\delta = (\delta_1, \ldots, \delta_l) \in \mathbb{N}^l$ tales que $|\delta| = \delta_1 + \ldots + \delta_l \leq n + 1 - l$. Hacemos $n_j := \delta_1 + \ldots + \delta_j + j$, para $j := 1, \ldots, l$, y consideramos la inclusión de variedades lineales definida por

$$i_j : \mathbb{P}^{\delta_j} \hookrightarrow \mathbb{P}^n, \qquad (x_0 : \ldots : x_{\delta_j}) \mapsto (\overbrace{0 : \ldots : 0}^{n_{j-1}} : x_0 : \ldots : x_{\delta_j} : 0 : \ldots : 0).$$

Las variedades lineales $i_1(\mathbb{P}^{\delta_1}), \ldots, i_l(\mathbb{P}^{\delta_l})$ son disjuntas entre sí. Definimos una curva $C(n,\delta) \subseteq \mathbb{P}^n$ como

$$C(n,\delta) := \bigcup_{j=1}^{l} i_j(v_{\delta_j}(\mathbb{P}^1)) \subseteq \mathbb{P}^n$$

Una curva $C \subseteq \mathbb{P}^n$ es proyectivamente equivalente a $C(n,\delta)$ si y sólo si existen $E_1, \ldots,$ $E_l \subseteq \mathbb{P}^n$ variedades lineales disjuntas 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 todo j.

Sea $V \subseteq \mathbb{P}^n$ una variedad. Entonces V está *definida sobre* k si su ideal de definición está generado sobre k. El siguiente lema es bien conocido, lo probamos aquí por falta de una referencia adecuada.

Lema 3.2.3 *Sean $\varphi : \mathbb{P}^n \to \mathbb{P}^N$ una aplicación regular definida sobre k, y sea $V \subseteq \mathbb{P}^n$ una variedad definida sobre k. Entonces la variedad $\varphi(V) \subseteq \mathbb{P}^N$ está definida sobre k.*

Demostración. Tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} k[x_0, \ldots, x_N] & \xrightarrow{\varphi_k^*} & k[V] \\ \downarrow & & \downarrow \\ \overline{k}[x_0, \ldots, x_N] & \xrightarrow{\varphi_{\overline{k}}^*} & \overline{k}[V] \end{array}$$

Luego $\ker \varphi_k^* = I_k(W)$ y $\ker \varphi_{\overline{k}}^* = I_{\overline{k}}(W)$, donde $I_k(W)$, $I_{\overline{k}}(W)$ denotan el ideal de la variedad W en $k[x_0, \ldots, x_N]$ y $\overline{k}[x_0, \ldots, x_N]$, respectivamente. Se quiere ver $I_{\overline{k}}(W) = \overline{k} \otimes_k I_k(W)$. Se tiene $\overline{k} \otimes_k k[V] \cong \overline{k}[V]$, ya que V está definida sobre k. Tensorizando con $\overline{k}$ obtenemos

$$\begin{array}{ccc} \overline{k}[x_0, \ldots, x_N] & \xrightarrow{\overline{k} \otimes_k \varphi_k^*} & \overline{k} \otimes_k k[V] \\ \| & & \| \\ \overline{k}[x_0, \ldots, x_N] & \xrightarrow{\varphi_{\overline{k}}^*} & \overline{k}[V] \end{array}$$

con $\ker \overline{k} \otimes_k \varphi_k^* = \overline{k} \otimes_k I_k(W)$. Concluimos entonces

$$I_{\overline{k}}(W) = \overline{k} \otimes_k I_k(W),$$

y por lo tanto 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 la curva C_n está definida sobre k.

Sea $C_j := i_j(C_{\delta_j}) \subseteq \mathbb{P}^n$ para $j = 1, \ldots, l$. Entonces $C(n,\delta) = \bigcup_j C_j$ es la descomposición minimal de $C(n,\delta)$ en curvas irreducibles. Luego $C(n,\delta)$ también está definida sobre k, y por lo tanto

$$\operatorname{irr} I_k(C(n,\delta)) = l, \qquad \deg I_k(C(n,\delta)) = |\delta|.$$

Lema 3.2.4 *Sean $V, W \subseteq \mathbb{P}^n$ variedades. Entonces*

$$I(V) + I(W) = (x_0, \ldots, x_n)$$

si y sólo si V y W están contenidas en subvariedades lineales disjuntas de $\mathbb{P}^n$.

Demostración. Las variedades V y W están en espacios lineales disjuntos si y sólo si sus clausuras lineales son disjuntas. Sean $L_V := I(L(V))$, $L_W := I(L(W)) \subseteq \overline{k}[x_1, \ldots, x_n]$. Se tiene

$$L_V = (I(V)_1), \qquad\qquad L_W = (I(W)_1).$$

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 se verifica $I(V) + I(W) = (x_0, \ldots, x_n)$. Luego $L_V + L_W = (x_0, \ldots, x_n)$ y por lo tanto $L(V) \cap L(W) = \emptyset$ □

Proposición 3.2.5 *Sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo radical y equidimensional de dimensión 2. Entonces*

$$h_I(m) = \deg I \ m + \operatorname{irr} I$$

para todo $m \geq 1$, si y sólo si existe una curva $C \subseteq \mathbb{P}^n$ definida sobre k proyectivamente equivalente a $C(n, \delta)$, tal que $I = I_k(C)$ para algún $\delta \in \mathbb{N}^l$, con $l := \operatorname{irr} I$ y $|\delta| = \deg I$.

Demostración. Sea $C \subseteq \mathbb{P}^n$ una curva definida sobre k proyectivamente equivalente a $C(n, \delta)$ para algún $l \in \mathbb{N}$ y $\delta \in \mathbb{N}^l$. Sea $I := I_k(C)$. Luego

$$\operatorname{irr} I = \operatorname{irr} C(n, \delta) = l, \qquad\qquad \deg\, I = \deg\, C(n, \delta) = |\delta|.$$

Queremos probar entonces $h_I(m) = |\delta|\, m + l$. Hacemos inducción en l. Sea $C := v_\delta(\mathbb{P}^1)$. Por la inclusión de $\overline{k}$−álgebras graduadas

$$\overline{k}[C] \overset{v_\delta^*}{\hookrightarrow} \overline{k}[x, y], \qquad\qquad x_i \longmapsto x^i y^{|\delta| - i}$$

obtenemos la descomposición en partes graduadas $\overline{k}[C] \cong \bigoplus_{j=0}^{\infty} \overline{k}[x, y]_{|\delta|\, j}$. Luego $h_I(m) = h_C(m) = \delta\, m + 1$ para $m \geq 1$, y por lo tanto la afirmación se verifica para $l = 1$.

Sea $l \geq 2$ y sea

$$C(n, \delta) = \bigcup_j C_j$$

la descomposición minimal de $C(n, \delta)$ en curvas irreducibles. Luego $C_1 \cup \ldots \cup C_{l-1}$, C_l están en espacios lineales disjuntos y por lo tanto se tiene

$$I(C_1 \cup \ldots \cup C_{l-1}) + I(C_l) = (x_0, \ldots, x_n)$$

por el lema 3.2.4. Luego $h_C(m) = h_{C_1 \cup \ldots \cup C_{l-1}}(m) + h_{C_l}(m)$ para $m \geq 1$, y por la hipótesis inductiva obtenemos

$$h_I(m) = h_C(m) = ((\delta_1 + \ldots + \delta_{l-1})\, m + (l - 1)) + (\delta_l\, m + 1) = |\delta|\, m + l, \qquad m \geq 1.$$

Ahora vamos a probar la recíproca. Sea $C \subseteq \mathbb{P}^n$ una curva definida sobre k tal que $I = I_k(C)$.

Hacemos inducción en $l := \operatorname{irr} I$. Consideramos en primer lugar el caso $l = 1$, es decir, cuando $C \subseteq \mathbb{P}^n$ irreducible. Se tiene

$$\dim L(C) = h_C(1) - 1 = \deg C$$

y por lo tanto $C \subseteq L(C)$ es una curva irreducible y no degenerada de grado mínimo. Luego $C \subseteq L(C)$ es una curva racional normal [63, Proposición 18.9].

Ahora sea $l \geq 2$. Sea $C = C_1 \cup \ldots \cup C_l$ la descomposición minimal de C en curvas irreducibles, y sea δ_i el grado de c_i. 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 3.2.2 que $h_{C_l}(m) = \delta_l \; m + 1$, $h_{C_1 \cup \ldots \cup C_{l-1}}(m) = (\delta_1 + \ldots + \delta_{l-1}) \; m + (l-1)$ y $h_{I(C_1 \cup \ldots \cup C_{l-1}) + I(C_l)}(m) = 0$ para $m \geq 1$.

Luego $C_l \subseteq L(C_l)$ es una curva racional normal, y por la hipótesis inductiva $C_1 \cup \ldots \cup C_{l-1}$ es proyectivamente equivalente a $C(n, (\delta_1, \ldots, \delta_{l-1}))$.

Además

$$I(C_1 \cup \ldots \cup C_{l-1}) + I(C_l) = (x_0, \ldots, x_n).$$

Por el lema 3.2.4 las curvas $C_1 \cup \ldots \cup C_{l-1}$ y C_l están contenidas en variedades lineales disjuntas, y por lo tanto C es proyectivamente equivalente a $C(n, (\delta_1, \ldots, \delta_l))$. □

Ahora vamos a deducir otra cota superior para la función de Hilbert de un ideal radical equidimensional.

Sea $V \subseteq \mathbb{P}^n$ una variedad irreducible de dimensión $r-1$. Sean $y_0, \ldots, y_{r-1}$ variables en posición de Noether separable con respecto a V. Sea A el anillo de polinomios $\overline{k}[y_0, \ldots, y_{r-1}]$ y sea B el anillo de coordenadas homogéneas $\overline{k}[V]$ de V, de forma tal que $A \hookrightarrow B$ es una inclusión entera. Sean K, L los cuerpos de fracciones de A y de B respectivamente. Luego $K \hookrightarrow L$ es una extensión separable de grado $D := [L : K]$. Sea $\eta \in B$ una forma lineal tal que $L = K[\eta]$. Luego

$$A[\eta] \subseteq B.$$

Sea $f \in A[t]$ el polinomio minimal de η sobre A. Sea $b \in B$. Luego

$$f'(\eta) \cdot b = \sum_m \operatorname{Tr}(b \cdot a_m) \, c_m$$

por la fórmula de traza de Tate, con $a_m, c_m \in A[\eta]$. Luego $\operatorname{Tr}(b \cdot a_m) \in A$, y por lo tanto $f'(\eta) \cdot b \in A[\eta]$, es decir

$$f'(\eta) \cdot B \subseteq A[\eta].$$

El lenguaje de la teoría de dependencia entera, esta última afirmación dice que $f'(\eta)$ está en el conductor de B en $A[\eta]$.

De esta última inclusión obtenemos la estimación

$$h_V(m) \leq \binom{m+D+r-1}{r} - \binom{m+r-1}{r}$$

En particular se sigue $D = [L : K] = \deg V$.

Teorema 3.2.6 *Sea k un cuerpo perfecto y sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo radical y equidimensional de dimensión r, con $r \geq 1$. Entonces*

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

Demostración. Asumimos sin pérdida de generalidad que k es algebraicamente cerrado. El caso en que I es un ideal primo de $k[x_0, \ldots, x_n]$ se sigue de la discución anterior. En el caso general, consideramos la descomposición primaria $I = \cap_P P$ de I y obtenemos

$$\begin{aligned} h_I(m) &\leq \textstyle\sum_P \left\{\binom{m+\deg P+r-1}{r} - \binom{m+r-1}{r}\right\} = \sum_P \sum_{i=0}^{\deg P-1} \binom{m+r-1+i}{r-1} \\ &\leq \textstyle\sum_{i=0}^{\deg I-1} \binom{m+r-1+i}{r-1} = \binom{m+\deg I+r-1}{r} - \binom{m+r-1}{r} \end{aligned}$$

□

Esta estimación es asintótica a h_I y por lo tanto es mucho más precisa que el teorema 3.2.2 para valores grandes de m. De la expresión

$$h_I(m) \leq \binom{m+\deg I+i}{r} - \binom{m+r-1}{r} = \sum_{i=0}^{\deg I-1} \binom{m+r-1+i}{r-1}$$

vemos que tampoco mejora la estimación de Chardin

$$h_I(m) \leq \deg I \binom{m+r-1}{r-1} = \sum_{i=0}^{\deg I-1} \binom{m+r-1}{r-1}$$

en ningún caso [35]. Sin embargo, notamos que nuestra demostración es mucho más simple y que podemos utilizarla en nuestras aplicaciones (Teorema 3.2.8) en lugar de la cota de Chardin obteniendo resultados similares.

Esta estimación también se puede expresar entérminos de la serie de Hilbert–Poincaré H_I de I como

$$t^{\deg I-1} H_I(t) \leq \frac{1 - t^{\deg I}}{(1-t)^{r+1}}$$

en el sentido de que esta desigualdad es válida para cada término de estas series de potencias.

Derivamos ahora una cota superior para la función de Hilbert de la intersección — al nivel de ideales — de un ideal radical y equidimensional con una hipersuperficie. Este ideal no es necesariamente ni radical ni equidimensional. Este resultado es una aplicación de nuestras cotas superiores e inferiores para la función de Hilbert. El uso de nuestra cota superior (Teorema 3.2.6) puede ser reemplazado por la estimación de Chardin [35] pero la cota obtenida es esencialmente la misma. De esta manera nuestra exposición se mantiene autocontenida.

Lema 3.2.7 *Sea* $I \subseteq k[x_0,\dots,x_n]$ *un ideal homogéneo radical y equidimensional de dimensión* r *, con* $r \geq 2$ *, y sea* $\eta \in k[x_0,\dots,x_n]$ *una forma lineal no–divisor de cero módulo* I *. Entonces existe* $m_0 \in \mathbb{Z}$ *tal que*

$$h_{(I,\eta)}(m_0) \leq \binom{m_0+r-1}{r-1} - \binom{m_0+r-1-3\deg I}{r-1}$$

con $3 \deg I \leq m_0 \leq 5\,(r-1)\deg I$ *.*

Demostración. Sean $\delta := \deg I$, $k := 3\,\delta$, $l := 2\,\delta$, $m := 5\,d\,\delta$. Vamos a probar

$$\sum_{j=0}^{l-1}\{\binom{m-j+r-1}{r-1} - \binom{m-j+r-1-k}{r-1}\} \geq \sum_{j=0}^{l-1} h_{(I,\eta)}(m-j)$$

Esta estimación implica $h_{(I,\eta)}(m_0) \leq \binom{m_0+r-1}{r-1} - \binom{m_0+r-1-3\delta}{r-1}$ para algún $m_0 \in \mathbb{Z}$ tal que $5\,(r-1)\,\delta - 2\,\delta + 1 \leq m_0 \leq 5\,(r-1)\,\delta$. Se tiene

$$\sum_{j=0}^{l-1}\{\binom{m+r-1-j}{r-1} - \binom{m+r-1-k-j}{r-1}\} = \{\binom{m+r}{r} - \binom{m+r-l}{r}\} - \{\binom{m+r-k}{r} - \binom{m+r-k-l}{r}\}.$$

Se tiene también

$$\sum_{j=0}^{l-1} h_{(I,\eta)}(m-j) = h_{(I,\eta^l)}(m) \leq \{\binom{m+r-1+\delta}{r} - \binom{m+r-1}{r}\} - \{\binom{m+r-l}{r} - \binom{m+r-\delta-l)}{r}\}$$

por aplicación de los teoremas 3.1.2 y 3.2.6. Luego alcanza con probar

$$\begin{aligned}\{\binom{m+r-\delta}{r} - \binom{m+r-\delta-l}{r}\} \quad & -\{\binom{m+r-k}{r} - \binom{m+r-k-l}{r}\} \geq \\ & \geq \{\binom{m+r-1+\delta}{r} - \binom{m+r-1}{r}\} - \{\binom{m+r}{r} - \binom{m+r-\delta}{r}\}.\end{aligned}$$

Se tiene

$$\begin{aligned}\{\binom{m+r-\delta}{r} - \binom{m+r-\delta-l}{r}\} \quad & -\{\binom{m+r-k}{r} - \binom{m+r-k-l}{r}\} \\ & = \textstyle\sum_{i=1}^{l}\{\binom{m+r-\delta-i}{r-1} - \binom{m+r-k-i}{r-1}\} \\ & = \textstyle\sum_{i=1}^{l}\sum_{j=1}^{k-\delta}\binom{m+r-\delta-i-j}{r-2} \geq l\,(k-\delta)\binom{m+r-2-k-l}{r-2}\end{aligned}$$

y

$$\begin{aligned}\{\binom{m+r-1+\delta}{r} - \binom{m+r-1}{r}\} - \{\binom{m+r-1+1}{r} \quad & - \quad \binom{m+r-\delta}{r}\} = \textstyle\sum_{i=1}^{\delta}\{\binom{m+r-1+\delta-i}{r-1} - \binom{m+r-i}{r-1}\} \\ & = \quad \textstyle\sum_{i=1}^{\delta}\sum_{j=1}^{\delta}\binom{m+r-1+\delta-i-j}{r-2} \leq \delta^2\binom{m+r-2+\delta}{r-2}\end{aligned}$$

y por lo tanto alcanza con probar

$$4 = l\,(k-\delta)/\delta^2 \geq \binom{m+r-2+\delta}{r-2}/\binom{m+r-2-k-l}{r-2}.$$

Esto es claro para $r = 2$, ya que en este caso el lado derecho de esta expresión es igual a 1. En el caso $r \geq 3$ se tiene

$$\binom{m+r-2+\delta}{r-2}/\binom{m+r-2-k-l}{r-2} = \prod_{j=1}^{r-2}(m+\delta+j)/(m-k-l+j) \leq (1+(6/5)/(r-2))^{r-2} \leq e^{6/5}$$

de donde se sigue nuestra afirmación. Concluimos entonces

$$h_{(I,\eta)}(m_0) \leq \binom{m_0+r-1}{r-1} - \binom{m_0+r-1-3\,\delta}{r-1}$$

para algún entero m_0 tal que $5\,(r-1)\,\delta - 2\,\delta + 1 \leq m_0 \leq 5\,(r-1)\,\delta$.

□

En lo que sigue introducimos la caracterización de Macaulay de la función de Hilbert de un ideal homogéneo.

Dado enteros positivos i, $c \in \mathbb{N}$, la i–*expansión binomial* de c es la única expresión

$$c = \binom{c(i)}{i} + \cdots + \binom{c(j)}{j}$$

con $c(i) > \cdots > c(j) \geq j \geq 1$.

Dada $c = \binom{c(i)}{i} + \ldots + \binom{c(j)}{j}$ la i–expansión binomial de c, se define $c^{\langle i \rangle}$ como

$$c^{\langle i \rangle} := \binom{c(i)+1}{i+1} + \ldots + \binom{c(j)+1}{j+1}.$$

Notamos que esta expresión es la $i+1$–expansión binomial de $c^{\langle i \rangle}$.

Sean b, c, $i \in \mathbb{N}$. Entonces es fácil ver que $b \geq c$ si y sólo si $(b(i), \ldots, b(j))$ es mayor o igual que $(c(i), \ldots, c(j))$ con respecto al orden lexicográfico. En particular $b \geq c$ si y sólo si $b^{\langle i \rangle} \geq c^{\langle i \rangle}$.

Una sucesión de enteros no–negativos $(c_i)_{i \in \mathbb{N}}$ se llama una O–*sucesión* en el caso en que $c_0 = 1$ y $c_{i+1} \leq c_i^{\langle i \rangle}$ para todo i.

Una función $h : \mathbb{N} \to \mathbb{N}$ es la función de Hilbert de un ideal polinomial homogéneo si y sólo si la sucesión $(h(i))_i \in \mathbb{N}$ es una O–sucesión. Esta es la caracterización de Macaulay de la función de Hilbert de un ideal polinomial homogéneo [94].

Teorema 3.2.8 *Sea k un cuerpo perfecto y sea $I \subseteq k[x_0, \ldots, x_n]$ un ideal homogéneo radical y equidimensional de dimensión r, con $r \geq 2$, Sea $f \in k[x_0, \ldots, x_n]$ un polinomio no–divisor de cero módulo I. Entonces*

$$h_{(I,f)}(m) \leq 3 \deg f \cdot \deg I \binom{m+r-2}{r-2}$$

para $m \geq 5\,(r-1) \deg I + \deg f$.

Demostración. Sean $d := \deg f$ y $\delta := \deg I$. Luego

$$h_{(I,f)}(m) = h_I(m) - h_I(m-d).$$

Asumimos que k es algebraicamente cerrado. Sea $\eta \in k[x_0, \ldots, x_n]$ forma lineal no–divisor de cero módulo I. Por el lema 3.2.7 existe $m_0 \in \mathbb{Z}$ tal que $3\,\delta \leq m_0 \leq 5\,(r-1)\,\delta$ tal que

$$h_{(I,\eta)}(m_0) \leq \binom{m+r-1}{r-1} - \binom{m+r-1-3\,\delta}{r-1}.$$

Sea $m \geq 3\,\delta$. Luego

$$\binom{m+r-1}{r-1} - \binom{m+r-1-3\,\delta}{r-1} = \sum_{j=1}^{3\,\delta} \binom{m+r-1-j}{m-j+1}$$

es la $m-$expansión binomial de $\binom{m+r-1}{r-1} - \binom{m+r-1-3\,\delta}{r-1}$, y por lo tanto

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

para $m \geq m_0$. Esto es una consecuencia del teorema de Macaulay. Concluimos entonces

$$h_{(I,f)}(m) = \sum_{j=0}^{d-1} h_{(I,\eta)}(m-j) \leq 3\,d\,\delta \binom{m+r-2}{r-2}$$

para $m \geq 5\,(r-1)\,\delta + d$.

$\square$

Sean d y δ el grado de f y de I , respectivamente. En el caso $\dim I = 1$ se tiene $h_I(m) \leq \delta$, y vale la igualdad para $m \geq \delta - 1$. Se tiene entonces

$$h_{(I,f)}(m) = 0$$

para $m \geq \delta + d - 1$.

Bibliografía

[1] M. Almeida, *Función de Hilbert de álgebras graduadas y Nullstellensatz afín efectivo*, Tesis de Licenciatura, Univ. Buenos Aires, 1995.

[2] M. Almeida, L. D'Alfonso, P. Solernó, *Sur les degrés des bases de modules libres sur l'anneau des polynômes,* aparecerá en *Math. Z.*.

[3] M. E. Alonso, E. Becker, M.–F. Roy, T. Wörmann, *Zeros, multiplicities and idempotents for zero–dimensional systems,* en L. González–Vega y T. Recio, eds., Algorithms in algebraic geometry and applications, Proc. MEGA'94, Progress in Math. **143**, Birkhäuser, 1996, pp. 1–15.

[4] F. Amoroso, *On a conjecture of C. Berenstein and A. Yger*, en L. González–Vega y T. Recio, eds., Algorithms in algebraic geometry and applications, Proc. MEGA'94, Progress in Math. **143**, Birkhäuser, 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., Proc. AAECC–11, Lect. Notes. in Comput. Sci. **948**, Springer–Verlag, 1995, pp. 106–119.

[6] E. Artin, *Algebraic numbers and algebraic functions,* Gordon and Breach, 1967.

[7] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra,* Addison–Wesley, 1969.

[8] B. Bank, M. Giusti, J. Heintz, G. Mbakop, *Polar varieties, real equation solving, and data structures: the hypersurface case,* J. Complexity **13** (1997), pp. 5–27.

[9] D. Bayer, D. Mumford, *What can be computed in algebraic geometry?,* en D. Eisenbud y L. Robbiano, 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, Proc. MEGA'94, Progress in Math. **143**, Birkhäuser, 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,* Michigan Math. J. **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, Univ. Maryland, 1996.

[16] D. N. Bernshtein, *The number of root of a system of equations,* Functional Analysis and its Applications **9** (1975), pp. 183–185.

[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 l'Académie des Sciences de l'Institut de France, 1764.

[19] É. Bézout, *Sur le degré résultant des méthodes d'elimination entre plusieurs équations,* mémoires presentés par divers savants á l'Académie des Sciences de l'Institut de France, 1764.

[20] É. Bézout, *Sur le degré des équations résultantes de l'évanouissement des inconnus,* Historie de l'Académie Royale des Sciences, année 1764, París, 1767, pp. 288–338.

[21] É. Bézout, *Théorie générale des équations algébriques,* París, 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 **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,* en Y. N. Lakshman, ed., Proc. ISSAC–96, ACM, 1996, pp. 72–78.

[29] L. Caniglia, A. Galligo, J. Heintz, *Some new effectivity bounds in computational geometry,* en T. Mora, ed., Proc. AAECC–6, Lect. Notes in Comput. Sci. 357, Springer–Verlag, 1989, pp. 131–151.

[30] L. Caniglia, A. Galligo, J. Heintz, *Borne simplemente exponentielle pour les degrés dans le théoreme 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 and effective Nullstellensatz,* Discrete Appl. Math. **33** (1991), pp. 11–23.

[32] J. Canny, *Some algebraic and geometric computations in PSPACE,* Proc. 20th. Annual ACM Symp. on Theory of Computing (1988), pp. 460–467.

[33] J. Canny, I. Emiris, *A subdivision–based algorithm for the sparse resultant,* Manuscrito, Univ. Nice–Sophia Antipolis, 1996.

[34] J. P. Cardinal, *Dualité et algorithmes itératives pour la solution des systèmes polinomiaux,* Tesis, Univ. Rennes I, 1993.

[35] 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.

[36] M. Chardin, P. Philippon, *Régularité et interpolation,* Manuscrito, Univ. Paris, 1997.

[37] M. Chardin, P. Philippon, aparecerá en Proc. Coloque à CIRM, 1998.

[38] A. L. Chistov, *Polynomial–time computation of the dimension of the components of algebraic varieties in zero–characteristic,* Manuscrito, Univ. Paris Val de Marne.

[39] V. I. Danilov, *The geometry of toric varieties,* Russian Math. Surveys **33** (1978), pp. 97–154.

[40] A. Dickenstein, M. Giusti, N. Fitchas, C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time,* Discrete Appl. Math. **33** (1991), pp. 73–94.

[41] T. W. Dubé, *A combinatorial proof of the effective Nullestellensatz,* J. Symb. Comp. **15** (1993), pp. 277–296.

[42] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry,* Graduate texts in Math. 150, Springer–Verlag, 1995.

[43] M. Elkadi, *Bornes pour le degré et les hauteurs dans le problème de division,* Michigan Math. J. **40** (1993), pp. 609–618.

[44] G. Ewald, U. Wessels, *On the ampleness of invertible sheaves in complete toric varieties,* Results Math. **25** (1991), pp. 275–278.

[45] G. Faltings, *Diophantine approximation on abelian varieties,* Ann. Math. **133** (1991), pp. 549–576.

[46] N. Fitchas, *Algorithmic aspects of Suslin's solution of Sérre's Conjeture,* Comput. Complexity **33** (1993), pp. 31–55.

[47] 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.

[48] N. Fitchas, M. Giusti, F. Smietanski, *Sur la complexité du théoreme des zéros,* en J. Gudat et. al., eds., Approximation and optimization **8** , Peter Lange Verlag, 1995, pp. 247–329.

[49] W. Fulton, *Intersection theory,* Notas de curso, Cortona, 1980.

[50] W. Fulton, *Intersection theorems,* Conferencia, Forschungsinstitut Oberwolfach, 1981.

[51] W. Fulton, *Intersection theory,* Erg. Math., 3. Folge., 2. Bd., Springer–Verlag, 1984.

[52] W. Fulton, *Introduction to toric varieties,* Ann. Math. Studies **131**, Princeton Univ. Press, 1993.

[53] W. Fulton, R. Lazarsfeld, *Positivity and excess intersection,* Enumerative and classical geometry, Niza 1981, Progress in Math. **24**, Birkhäuser, 1982, pp. 97–105.

[54] 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.

[55] 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., Effective methods in algebraic geometry, Proc. MEGA'90, Progress in Math. **94**, Birkhäuser, 1991, pp. 169–194.

[56] 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.

[57] 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.

[58] 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., Proc. AAECC–11, Lect. Notes. Comput. Sci. **948**, Springer–Verlag, 1995. pp. 205–231.

[59] M. Giusti, J. Heintz, J. Sabia, *On the efficiency of effective Nullstellensätze,* Comput. Complexity **3** (1993), pp. 56–95.

[60] M. Green, *Restrictions of linear series to hyperplanes, and some results of Macaulay and Gotzmann,* Algebraic curves and projective geometry, Proc. Trento'88, Lect. Notes in Math. **1389**, Springer–Verlag, 1989, pp. 76–85.

[61] K. Hägele, *Intrinsic height estimates for the Nullstellenstaz,* Tesis, Univ. Cantabria, 1998.

[62] K. Hägele, J. E. Morais, L. M. Pardo, M. Sombra, *On the intrinsic complexity of the arithmetic Nullstellensatz,* Manuscrito, Univ. Cantabria, 1998.

[63] J. Harris, *Algebraic geometry: a first course,* Graduate Texts in Math. 133, Springer–Verlag, 1992.

[64] R. Hartshorne, *Algebraic geometry,* Graduate Texts in Math. 52, Springer–Verlag, 1977.

[65] J. Heintz, *Definability bounds in algebraically closed fields and a note on degree in affine algebraic geometry,* Manuscrito, Univ. Zürich, 1977.

[66] 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.

[67] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields,* Theoret. Comput. Sci. **24** (1983), pp. 239-277.

[68] J. Heintz, M. Sieveking, *Lower bounds for polynomials with algebraic coefficients,* Theoret. Comput. Sci. **11** (1980), pp. 321–330.

[69] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, *Deformation techniques for efficient polynomial equation solving,* aparecerá en Proc. MEGA'98.

[70] G. Hermann, *Der Frage der endlich vielen Schritte in der Theorie der Polynomideale,* Math. Ann. **95** (1926), pp. 736–788.

[71] D. Hilbert, *Über die Theorie von algebraischen Formen,* Math. Ann. **36** (1890), pp. 473–534.

[72] D. Hilbert, *Über die vollen Invariantensysteme,* Math. Ann. **42** (1893), pp. 313–373.

[73] B. Huber, B. Sturmfels, *A polyhedral method for solving sparse polynomial systems,* Math. Comp. **64** (1995), pp. 1541–1555.

[74] B. Iversen, *Noetherian graded modules I,* Manuscrito, Math. Institut Aarhus Univ. **29**, 1972.

[75] S. Ji, J. Kollár, B. Shiffman, *A global Lojasiewicz inequality for algebraic varieties,* Trans. Amer. Math. Soc. **329** (1992), pp. 813–818.

[76] J.–P. Jouanolou, *Théorèmes de Bertini et applications,* Progress in Math. **42**, Birkhäuser, 1983.

[77] P. Koiran, *Hilbert's Nullstellensatz is in the polynomial hierarchy,* J. Complexity **12** (1996), pp. 273–286.

[78] J. Kollár, *Sharp effective Nullstellensatz,* J. Amer. Math. Soc. **1** (1988), pp. 963–975.

[79] J. Kollár, *Effective Nullstellensatz for arbitrary ideals,* Manuscrito, Univ. Utah, 1998.

[80] J. König, *Einleitung in die allgemeine Theorie der algebraischen Grössen,* Leipzig, 1903.

[81] T. Krick, A. Logar, *Membership problems, representation problems, and the computation of the radical for one–dimensional ideals,* en T. Mora y C. Traverso, eds., Effective methods in algebraic geometry, Progress in Math. **94**, Birkhäuser, 1991, pp. 203–216.

[82] T. Krick, L. M. Pardo, *Une approche informatique pour l'approximation diophantienne,* C. R. Acad. Sci. Paris **318** (1994), pp. 407–412.

[83] T. Krick, L. M. Pardo, *A computational method for diophantine approximation,* en L. González–Vega y T. Recio, eds., Algorithms in algebraic geometry and applications, Proc. MEGA'94, Birkäuser Progress in Math. **143**, Birkhäuser, Basel, 1996, pp. 193–253.

[84] T. Krick, J. Sabia, P. Solernó, *On intrinsic bounds in the Nullstellensatz,* AAECC J. **8** (1997), pp. 125–134.

[85] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen,* Crelle J. Reine Angew. Math. **92** (1881–1882), pp. 1–122 : Werke, Vol. II, Leipzig, Teubner, 1897, pp. 237–287.

[86] A. G. Kushnirenko, *Newton polytopes and the Bézout theorem,* Functional Analysis and its Applications **10** (1976), pp. 82–83.

[87] E. Kunz, *Kähler differentials,* Adv. Lect. in Math., Vieweg–Verlag, 1986.

[88] S. Lang, *Algebraic Number Theory,* Addison–Wesley, 1970.

[89] S. Lang, *Algebra,* Addison–Wesley, 1971.

[90] S. Lang, *Fundamentals of diophantine geometry,* Springer–Verlag, 1983.

[91] M. Laurent, *Hauteur de matrices d'interpolation,* en P. Philippon, ed., Approximations diophantiennes et nombres transcendants, Proc. Luminy'90, de Gruyter, 1992, pp. 215–238.

[92] D. Lazard, *Algèbre linéaire sur* $k[x_1, \ldots, x_n]$ *et élimination,* Bull. Soc. Math. France **105** (1977), pp. 165–190.

[93] D. H. Lehmer, *Factorization of certain cyclotomic functions,* Ann. of Math. **34** (1993), pp. 461–479.

[94] F. S. Macaulay, *The algebraic theory of modular systmems,* Cambridge Univ. Press, 1916.

[95] K. Mahler, *On some inequalities for polynomials in several variables,* J. London Math. Soc. **37** (1962), pp. 341–344.

[96] D. W. Masser, G. Wüstholz, *Fields of large trascendence degree generated by values of elliptic functions,* Invent. Math. **72** (1971), pp. 407–463.

[97] G. Matera, *Sobre la complejidad en espacio y tiempo de la eliminación geométrica,* Tesis, Univ. Buenos Aires, 1997.

[98] G. Matera, J. M. Turull, *The space complexity of elimination theory: Upper bounds,* Foundations of Comput. Math., Springer–Verlag 1997, pp. 267–276.

[99] H. Matsumura, *Commutative ring theory,* Cambridge Univ. Press, 1986.

[100] E. Mayr, *Membership in polynomial ideals over* $\mathbb{Q}$ *is exponential space complete,* Proc. 6th. Annual Symp. on Theoretical Aspects of Computer Science, Lect. Notes in Comput. Sci. **349**, Springer–Verlag, 1989, pp. 400–406.

[101] E. Mayr, A. Meyer, *The complexity of the word problem for commutative semigroups,* Adv. Math. **46** (1982), pp. 305–329.

[102] J. E. Morais, *Resolución eficaz de sistemas de ecuaciones polinomiales,* Tesis, Univ. Cantabria, 1997.

[103] 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.

[104] Y. Nesterenko, *Estimates for the characteristic function of a prime ideal,* Math. URSS Sbornik **51** (1985), pp. 9–32.

[105] J. Newton, *Geometria analytica,* 1680.

[106] L. M. Pardo, *How upper and lower bounds meet in elimination theory,* en G. Cohen, M. Giusti y T. Mora, eds., Proc. AAECC–11, Lect. Notes. in Comput. Sci. **948**, , Springer–Verlag, 1995, pp. 33–69.

[107] L. M. Pardo, *Comunicación personal,* 1997.

[108] P. Philippon, *Critères pour l'indépendance algébrique,* Inst. Hautes Études Sci. Publ. Math. **64** (1986), pp. 5–52.

[109] P. Philippon, *Dénominateurs dans le théorème des zeros de Hilbert,* Acta Arith. **58** (1990), pp. 1–25.

[110] 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.

[111] G. REMOND, aparecerá en Proc. Coloque à CIRM, 1998.

[112] J. M. ROJAS, *Toric intersection theory for affine root counting,* aparecerá en J. Pure Appl. Algebra.

[113] J. M. ROJAS, *Toric laminations, sparse generalized characteristic polynomials, and a refinement of Hilbert's tenth problem,* Foundations of Comput. Math., Springer–Verlag 1997.

[114] W. RUDIN, *Function theory in the unit ball of* $\mathbb{C}^n$, Grundlehren der matematischen Wissenchaften **241**, Springer–Verlag, 1980.

[115] J. SABIA, P. SOLERNÓ, *Bounds for traces in complete intersections and degrees in the Nullstellensatz,* AAECC J. **6** (1995), pp. 353–376.

[116] J.–P. SÈRRE, *Algèbre locale–Multiplicités,* Lecture Notes in Math. **11**, Springer–Verlag, 1965.

[117] I. R. SHAFAREVICH, *Basic algebraic geometry,* Springer–Verlag, 1974.

[118] B. SHIFFMAN, *Degree bounds for the division problem in polynomial ideals,* Michigan Math. J. **36** (1989), pp. 163–171.

[119] M. SIEVEKING, *On the notion of degree and its applications to complexity theory by Strassen,* Manuscrito, Univ. Bielefeld, 1977.

[120] F. SMIETANSKI, *Quelques bornes effectives pour le théoreme des zeros avec paramètres,* Tesis, Univ. Nice–Sophia Antipolis, 1994.

[121] P. SOLERNÓ, *Complejidad de conjuntos semi–algebraicos,* Tesis, Univ. Buenos Aires, 1989.

[122] M. SOMBRA, *Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz,* J. Pure Appl. Algebra **117 & 118** (1997), pp. 565–599.

[123] M. SOMBRA, *A sparse effective Nullstellensatz,* aparecerá en *Adv. Appl. Math.*.

[124] C. SOULÉ, *Géometrie d'Arakelov et nombres trascendants,* J. Arithmétiques, Luminy'89, Asterisque 198–200 (1991), pp. 355–371.

[125] B. STURMFELS, *Sparse elimination theory,* en D. Eisenbud y L. Robbiano, eds., Computational algebraic geometry and commutative algebra, Cambridge Univ. Press, 1993, pp. 377–396.

[126] B. STURMFELS, *Gröbner bases and convex polytopes,* Univ. Lect. Series **8**, Amer. Math. Soc., 1996.

[127] B. STURMFELS, N. V. TRUNG, W. VOGEL, *Bounds on degrees of projective schemes,* Math. Ann. **302** (1995), pp. 417–432.

[128] B. TEISSIER, *Résultats récents d'algèbre commutative effective,* Sém. Bourbaki 718, Astérisque 189–190, pp. 107–131, Soc. Math. France, 1991.

[129] C. TRAVERSO, *Hilbert Functions and the Buchberger Algorithm,* J. Symbolic Comp. **22** (1996), pp. 355–376.

[130] J. VERSCHELDE, P. VERLINDEN, R. COOLS, *Homotopies exploiting Newton polytopes for solving sparse polynomial systems,* SIAM J. Numer. Anal. **31** (1994), pp. 915–930.

[131] W. Vogel, *Lectures on results on Bézout theorem,* Tata Lect. Notes **74**, Springer–Verlag, Berlin, 1984.

[132] A. Weil, *Number theory and algebraic geometry,* Proc. Int. Math. Congress, vol. II, Cambridge, 1950, pp. 90–100.

[133] O. Zariski, *Algebraic surfaces,* Classics in Math., Springer–Verlag, 1995.

[134] O. Zariski, P. Samuel, *Commutative algebra, 2 vols.,* Van Nostrand, New York, 1958, 1960.

[135] S. Zhang, *Positive line bundles on arithmetic surfaces,* Ann. of Math. **136**, (1992), pp. 569–587.

Notación

Índice Temático