Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Máster

Máster en Matemáticas

Sumas iteradas y función de Hilbert, un ejemplo de interacción entre la Combinatoria Aditiva y el Álgebra Conmutativa

Autor:

Mario González Sánchez

Tutor:

Dr. Philippe T. Gimenez Martín

Agradecimientos

A Philippe, por aceptar dirigir este trabajo, proponerme este tema que me entusiasmó desde el primer día y ayudarme siempre que lo he necesitado. También quiero agradecer a todos los profesores que de algún modo han influido en el camino que he seguido. En particular, gracias a Ana por animarme a cursar la asignatura Álgebra Conmutativa y Computacional. Sin ese consejo, quizá nunca hubiera desarrollado esta pasión por el Álgebra Conmutativa.

A mis padres, mi hermana y mis amigos, por ser mi apoyo en los momentos más complicados, sobre todo durante los períodos de exámenes en estos $5 + 1$ años.

Resumen

Dados un subconjunto finito A de un semigrupo abeliano $(G, +)$, y un entero positivo s, denotamos sA al conjunto formado por todas las sumas de s elementos de A y denominamos a estos conjuntos los *conjuntos suma* de A. La combinatoria aditiva centra su estudio en estos conjuntos suma y, en particular, la teoría aditiva de números se reduce al caso en que G es el grupo de los números enteros. En este trabajo se revisan algunos conceptos de álgebra conmutativa y combinatoria aditiva y se estudian las interacciones entre estas dos áreas.

Índice general

Introducción

Desde sus inicios, el álgebra conmutativa ha tenido siempre profundas interacciones con otras disciplinas de las matemáticas como la geometría algebraica, la teoría de números, la teoría de representaciones o la topología algebraica. A estas disciplinas se han ido añadiendo con el tiempo otras de aparición más reciente como la combinatoria algebraica, el álgebra computacional, la teoría de códigos y la criptografía. El objetivo de este trabajo es estudiar las interacciones del álgebra conmutativa (y la geometría algebraica) con la combinatoria aditiva.

La teoría aditiva de números es un área relativamente nueva de las matemáticas que forma parte de la combinatoria aditiva y pone el foco en el estudio de la estructura aditiva de los subconjuntos finitos de números enteros. Se centra esencialmente en los denominados conjuntos suma (*sumset*), es decir, $A_1 + \cdots + A_s$ siendo $A_i \subset \mathbb{Z}$ un conjunto de enteros para cada $i = 1, \ldots, s$. Cuando los s conjuntos son todos iguales, $A_1 = \cdots = A_s = A$, el conjunto suma correspondiente se denota sA. Los resultados de teoría aditiva de números se agrupan en dos grandes categorías: un problema directo en teoría aditiva de números es un problema en el cual se pretende determinar la estructura o algunas propiedades de los conjuntos suma sA a partir de propiedades de A; mientras un problema inverso busca el objetivo contrario, es decir, deducir propiedades sobre A a partir de propiedades de sus conjuntos suma.

La conexión entre la combinatoria aditiva y el álgebra conmutativa comenzó en 1992 con el trabajo de Khovanskii [20], en el que asocia un módulo graduado a cada subconjunto finito $A \subset G$ de un semigrupo abeliano, de modo que los valores de su función de Hilbert coinciden con los cardinales de los conjuntos suma de A. Después de este primer acercamiento, esta vía no ha sido explorada de nuevo hasta el trabajo [11] de Eliahou y Mazumdar, publicado este año en *Journal of Algebra*. Al mismo tiempo, se han establecido más conexiones en los recientes trabajos de Elias [12] (pendiente de publicación en *Mediterranean Journal of Mathematics*) y Colarte-Gómez, Elías y Miró Roig [3] (publicado en *Collectanea Mathematica* este mismo año).

El objetivo de este trabajo consiste en comprender primero algunos resultados de teoría aditiva de números y combinatoria aditiva para después establecer algunas conexiones entre estas áreas y el álgebra conmutativa. El trabajo se estructura como sigue:

- En el capítulo 1 recordamos algunos conceptos de álgebra conmutativa e introducimos conceptos nuevos que no se estudian ni en el grado ni en el máster, como son

la profundidad o las álgebras monomiales.

- En el capítulo 2 introducimos los conceptos y resultados básicos de la teoría aditiva de números, así como algunos resultados más avanzados de combinatoria aditiva.
- El objetivo del capítulo 3 es presentar la construcción de Eliahou y Mazumdar del artículo [11], donde asocian a cada subconjunto finito A de un semigrupo abeliano G una k-álgebra graduada estándar.
- En los capítulos 4 y 5, la filosofía es asociar objetos geométricos a cada subconjunto finito A de un grupo abeliano G. En particular, en el capítulo 4 nos centramos en el caso $G = \mathbb{Z}$, mientras que en el capítulo 5 nos centramos en el caso $G = \mathbb{Z}^n$ para $n \geq 1$.

Hemos agrupado los capítulos en dos partes por afinidad en los contenidos: la parte I está constituida por los capítulos 1 y 2, puesto que aquí se introducen los resultados básicos de álgebra conmutativa y combinatoria aditiva. En la parte II se incluyen los capítulos 3, 4 y 5, en los que se presentan las interacciones entre ambas disciplinas.

Notación

- Todos los anillos se suponen conmutativos y unitarios. En general, los anillos se denotan por R, $\mathfrak{p} \subset R$ denota un ideal primo y $\mathfrak{m} \subset R$ un ideal maximal.
  El símbolo $\simeq$ denota isomorfismo de anillos, módulos, álgebras,... según el contexto.
- k denota un cuerpo en principio arbitrario, $\mathbb{Z}$ denota el conjunto de números enteros, $\mathbb{R}$ los números reales y $\mathbb{C}$ los complejos. Además, denotamos $\mathbb{N} = \{1, 2, 3, \dots\}$ y $\mathbb{N}_0 = \{0, 1, 2, \dots\}$.
- No distinguimos entre semigrupo y monoide. Todos los semigrupos que consideramos suponemos que tienen elemento neutro.
- Reservamos el término variedad afín (resp. proyectiva) para los subconjuntos algebraicos afines (resp. proyectivos) que son irreducibles. Las coordenadas homogéneas en el espacio proyectivo $\mathbb{P}^n_k$ se denotan $(x_0 : x_1 : \cdots : x_n)$.
- dim denota la dimensión de un anillo o de un espacio vectorial, según el contexto en el que se utilice (en cada caso se especifica).
- Si $a, b \in \mathbb{Z}$, denotamos $[a, b] = \{n \in \mathbb{Z} : a \leq n \leq b\}$. Además, si $x \in \mathbb{R}$, $\lfloor x \rfloor$ denota parte entera de x (función suelo) y $\lceil x \rceil$ denota la función techo de x.
- El símbolo $\subset$ denota "contenido o igual" y para denotar una contención estricta utilizamos el símbolo $\subsetneq$.
- Si G es un grupo abeliano y $A, B \subset G$ son subconjuntos finitos, $|A|$ denota el cardinal de A, $A - B = \{a - b : a \in A, b \in B\}$ denota la diferencia de los dos conjuntos, mientras que $A \setminus B = \{a \in A : a \notin B\}$ denota la diferencia conjuntista. Si $A \cap B = \emptyset$, denotamos $A \sqcup B = A \cup B$ y si $A = \{a\}$, denotamos $a - B = \{a\} - B$.

Parte I

Preliminares

Capítulo 1

Preliminares de Álgebra Conmutativa

En este primer capítulo vamos a introducir y repasar algunos conceptos y resultados de álgebra conmutativa y geometría algebraica que utilizaremos en los siguientes capítulos. Para no extendernos demasiado, hemos optado por incluir únicamente algunas demostraciones de los resultados presentados para ilustrar algunas de las técnicas habituales.

Comenzamos repasando algunos conceptos sobre anillos y módulos graduados en la sección 1.1. Posteriormente, en 1.2 hablamos de resoluciones libres graduadas. Aquí, el resultado más importante es el teorema de las sizigias de Hilbert. Mediante el estudio de las resoluciones libres, introducimos el concepto de regularidad de Castelnuovo-Mumford y la dimensión proyectiva de un módulo graduado. En la sección 1.3 introducimos el concepto de profundidad y el de anillo y módulo Cohen-Macaulay, que utilizaremos en el capítulo 4. Una de las herramientas más importantes que vamos a usar es la función de Hilbert, que desarrollamos en la sección 1.4, donde incluimos el teorema de Macaulay que caracteriza exactamente qué funciones son la función de Hilbert de alguna k-álgebra graduada estándar. Por último, en la sección 1.5 introducimos algunos conceptos sobre ideales tóricos. En particular, en los capítulos posteriores utilizaremos curvas monomiales y proyecciones monomiales de variedades de Veronese.

Las referencias principales empleadas en este capítulo son: [1], [2], [5], [8], [29] y [30] para la parte de álgebra conmutativa y [18] y [19] para la parte de geometría algebraica.

1.1. Anillos y módulos graduados

Sea G un semigrupo conmutativo con elemento neutro.

Definición 1.1.1. Un *anillo G-graduado* es un anillo R junto con una descomposición

$$R = \bigoplus_{g \in G} R_g,$$

donde R_g es un subgrupo aditivo de R para todo $g \in G$, y tal que $R_g R_h \subset R_{g+h}$, $\forall g, h \in G$.

Ejemplo 1.1.2. El ejemplo clásico de anillo graduado es el anillo de polinomios $R = k[x_1, \ldots, x_n]$ con la *graduación estándar*, es decir, considerando $G = \mathbb{N}_0$ y R_j el subconjunto de R formado por los polinomios homogéneos de grado j, para cada $j \in \mathbb{N}_0$. Aunque los grados en el anillo de polinomios son no negativos, a veces resulta más cómodo considerar

$$R = \bigoplus_{j \in \mathbb{Z}} R_j, \text{ donde } R_j = \{0\} \text{ para todo } j < 0.$$

Es usual denotar al anillo de polinomios $k[x_1, \ldots, x_n]$ por S cuando pensamos en él como un anillo graduado con la graduación estándar, $S = k[x_1, \ldots, x_n]$. A veces, incluiremos una variable más, $S = k[x_0, x_1, \ldots, x_n]$ o consideraremos n variables pero comenzando a numerar en 0, $S = k[x_0, \ldots, x_{n-1}]$.

Definición 1.1.3. Dado un anillo graduado $R = \bigoplus_{g \in G} R_g$, un *$R$-módulo graduado* es un R-módulo M junto con una descomposición

$$M = \bigoplus_{g \in G} M_g,$$

siendo M_g un subgrupo aditivo de M para cada $g \in G$, de modo que $R_g M_h \subset M_{g+h}$ para cada $g, h \in G$.

Ejemplo 1.1.4.

(1) Si consideramos $S = k[x_1, \ldots, x_n]$, graduado con la graduación estándar, e $I \subset S$ un ideal, I es un S-módulo graduado si, y solo si, es homogéneo. Es decir, si existen polinomios homogéneos $f_1, \ldots, f_r$ tales que $I = \langle f_1, \ldots, f_r \rangle$.

(2) Para el mismo anillo $S = k[x_1, \ldots, x_n]$ (con la graduación estándar), podemos considerar el S-módulo libre de rango $m \in \mathbb{N}$, S^m. Entonces,

$$S^m := \bigoplus_{j \in \mathbb{N}_0} (S^m)_j,$$

donde definimos $(S^m)_j := (S_j)^m$. A esta graduación la denominaremos la *graduación estándar* en S^m.

Una graduación en $\mathbb{Z}$ se puede modificar "desplazando" los grados. Si $R = \oplus_{j \in \mathbb{Z}} R_j$ es un anillo graduado, $M = \oplus_{j \in \mathbb{Z}} M_j$ es un R-módulo graduado y $d \in \mathbb{Z}$, entonces podemos considerar una nueva graduación en M dada por

$$M = \bigoplus_{j \in \mathbb{Z}} \left(M(d)\right)_j, \text{ donde } \left(M(d)\right)_j = M_{d+j}.$$

Ejemplo 1.1.5. En $S = k[x, y]$, si consideramos S^2 con la graduación estándar, $(x^2 + xy, -xy)$ es homogéneo de grado 2, es decir, pertenece a $(S^2)_2$. Sin embargo, considerándolo como un elemento de $S^2(-3)$ es homogéneo de grado 5, es decir, $(x^2 + xy, -xy) \in (S^2(-3))_5$.

Con más generalidad, si $S = k[x_1, \ldots, x_n]$, lo que estamos haciendo en $S^m(-d)$ es asignar a los elementos de la base estándar $\mathbf{e}_1, \ldots, \mathbf{e}_m$ peso d. Es decir, si consideramos en S^m la graduación estándar y $\mathbf{f} \in (S^m)_j$ un elemento homogéneo de grado j, entonces escribiendo $\mathbf{f}$ de la forma

$$\mathbf{f} = (f_1, \ldots, f_m) = f_1\mathbf{e}_1 + \ldots + f_m\mathbf{e}_m,$$

se tiene $\deg f_i\mathbf{e}_i = j + d$, para todo i. Es decir, $\mathbf{v}$ es homogéneo de grado $d+j$ en $S^m(-d)$. Una variante de este proceso nos permite dar una nueva graduación sobre S^m. Si asignamos a $\mathbf{e}_1, \ldots, \mathbf{e}_m$ pesos $d_1, \ldots, d_m$, respectivamente, esto define una nueva graduación sobre S^m que denotaremos $S(-d_1) \oplus \cdots \oplus S(-d_m)$. Este proceso nos va a permitir ver polinomios que no son homogéneos para la graduación estándar como polinomios homogéneos para esta nueva graduación.

Definición 1.1.6. Sean R un anillo graduado, M, N dos R-módulos $\mathbb{Z}$-graduados,

$$R = \bigoplus_{j\in\mathbb{Z}} R_j,\ M = \bigoplus_{j\in\mathbb{Z}} M_j,\ N = \bigoplus_{j\in\mathbb{Z}} N_j,$$

y $\varphi\colon M \to N$ un homomorfismo de módulos.

- Se dice que φ es un *homorfismo graduado de grado d* si para cada $j \in \mathbb{Z}$ se tiene $\varphi(M_j) \subset N_{j+d}$.
- Se dice que φ es graduado si es graduado de grado 0.

1.2. Resoluciones libres graduadas

Sean R un anillo y M un R-módulo finitamente generado. Elegir un sistema de generadores $\{f_1, \ldots, f_t\}$ de M equivale a considerar un homomorfismo $\varphi : R^t \twoheadrightarrow M$ sobreyectivo o, lo que es lo mismo, una sucesión exacta

$$R^t \xrightarrow{\varphi} M \to 0.$$

Definición 1.2.1. En la situación anterior, llamaremos *primer módulo de sizigias* de $\{f_1, \ldots, f_t\}$ al núcleo del homomorfismo φ, y lo denotaremos

$$\mathrm{Syz}\,(f_1, \ldots, f_t) = \ker(\varphi).$$

Observación 1.2.2. (1) El módulo $\mathrm{Syz}\,(f_1, \ldots, f_t)$ depende del sistema de generadores fijado en M, no únicamente del módulo M. Por lo tanto, escribiremos $\mathrm{Syz}\,(f_1, \ldots, f_t)$ en lugar de $\mathrm{Syz}\,(M)$ siempre que pueda haber lugar a confusión.

(2) Aunque el módulo M sea finitamente generado, $\mathrm{Syz}\,(f_1, \ldots, f_t)$ no tiene por qué serlo en general. No obstante, si R es noetheriano, entonces R^t es noetheriano, luego $\mathrm{Syz}\,(f_1, \ldots, f_t)$ está finitamente generado.

A partir de aquí, supondremos que el anillo R es noetheriano y M es un R-módulo finitamente generado. En este caso tenemos que $\mathrm{Syz}(f_1,\ldots,f_t)$ es un módulo finitamente generado, y elegir un sistema de generadores es equivalente a elegir un homomorfismo sobreyectivo $\psi : R^s \to \mathrm{Syz}(f_1,\ldots,f_t) = \ker(\varphi)$. Como ψ es sobreyectivo, entonces $\mathrm{im}(\psi) = \ker(\varphi)$, por lo que la sucesión

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \to 0 \tag{1.2.1}$$

es exacta. Ahora, $\mathrm{Syz}(f_1,\ldots,f_t) \subset R^t$ es de nuevo un R-módulo finitamente generado y podemos interesarnos por su primer módulo de sizigias, que se denomina *segundo módulo de sizigias* de $\{f_1,\ldots,f_t\}$, y se denota $\mathrm{Syz}(\mathrm{Syz}(f_1,\ldots,f_t))$. De nuevo, la elección de un sistema de generadores $h_1,\ldots,h_r$ para $\mathrm{Syz}(\mathrm{Syz}(f_1,\ldots,f_t))$ extiende la sucesión (1.2.1) a una sucesión exacta de la forma

$$R^r \xrightarrow{\lambda} R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \to 0.$$

Este proceso se puede iterar, considerando cada vez las sizigias del nuevo módulo de sizigias.

Definición 1.2.3. Sean R un anillo noetheriano y M un R-módulo finitamente generado. Una *resolución libre* de M es una sucesión exacta de la forma

$$\ldots \xrightarrow{\varphi_2} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} R^{\beta_0} \xrightarrow{\varphi_0} M \to 0,$$

donde cada $F_i \simeq R^{\beta_i}$ es un R-módulo libre de rango $\beta_i \in \mathbb{N}$.
Si existe un número l tal que $F_{l+1} = F_{l+2} = \cdots = 0$ y $F_l \neq 0$, entonces diremos que la resolución es *finita de longitud* l. En este caso, escribiremos la resolución como

$$0 \to F_l \xrightarrow{\varphi_l} \cdots \to R^{\beta_0} \xrightarrow{\varphi_0} M \to 0.$$

Observación 1.2.4. (1) Calculando los sucesivos módulos de sizigias, podemos construir una resolución libre de cualquier R-módulo libre M. Sin embargo, esta resolución no es única y depende fuertemente de todos los sistemas de generadores que vamos eligiendo en el procedimiento.

(2) En general, la resolución que hemos construido puede tener longitud infinita. La resolución termina si para algún $i \geq 0$, $\ker \varphi_i = \{0\}$.

Ejemplo 1.2.5. Consideramos el anillo $R = k[x]/\langle x^2\rangle$, y el ideal $I = \langle \bar{x}\rangle \subset R$, donde $\bar{x}$ denota la clase de x en el anillo cociente R. La sucesión exacta

$$\begin{array}{rcl} \cdots \to R \to \cdots \to R \xrightarrow{\varphi_2} R \xrightarrow{\varphi_1} R \xrightarrow{\varphi_0} I \to 0 \\ \bar{x} \longmapsto 1 \longmapsto \bar{x} \end{array}$$

es una resolución libre de $\langle \bar{x}\rangle$ como R-módulo, y es infinita.

La noetherianidad del anillo R no garantiza que este proceso termine. Lo que lo garantiza es el teorema de las sizigias de Hilbert.

Teorema 1.2.6 (Teorema de las sizigias de Hilbert, [5, §6.2, Thm. 2.1])**.**
Si $R = k[x_1, \ldots, x_n]$, entonces todo R-módulo finitamente generado admite una resolución libre de longitud menor o igual que n (el número de variables).

Ejemplo 1.2.7. Consideramos el anillo $R = \mathbb{Q}[x, y, z, w]$, los polinomios $f_1 = x^2 - yw$, $f_2 = xy - zw$, $f_3 = y^2 - xz$ y el ideal $I = \langle f_1, f_2, f_3 \rangle \subset R$.
Con la ayuda de Singular [7], podemos calcular el primer módulo de sizigias de I, que es

$$\mathrm{Syz}\,(f_1, f_2, f_3) = \left\langle \begin{pmatrix} y \\ -x \\ w \end{pmatrix}, \begin{pmatrix} -z \\ y \\ -x \end{pmatrix} \right\rangle = \ker(\varphi_0).$$

Consideramos ahora el homomorfismo de módulos $\varphi_1 : R^2 \to R^3$ dado por la matriz cuyas columnas son los generadores de $\mathrm{Syz}\,(f_1, f_2, f_3)$. Este morfismo verifica $\ker(\varphi_1) = \{0\}$, por lo que se tiene la siguiente sucesión exacta:

$$0 \to R^2 \xrightarrow{\varphi_1} R^3 \xrightarrow{\varphi_0} I \to 0,$$

que es una resolución libre de I como R-módulo. Además, podemos escribir explícitamente los homomorfismos φ_0, φ_1 en términos matriciales

$$0 \to R^2 \xrightarrow{\begin{pmatrix} y & -z \\ -x & y \\ w & -x \end{pmatrix}} R^3 \xrightarrow{(f_1\ f_2\ f_3)} I \to 0.$$

```
> ring r = 0, (x,y,z,w), dp;
> poly f1 = x2-yw;
> poly f2 = xy-zw;
> poly f3 = y2-xz;
> ideal I = f1,f2,f3;
> syz(I);
_[1]=x*gen(2)-y*gen(1)-w*gen(3)
_[2]=x*gen(3)-y*gen(2)+z*gen(1)
> syz(syz(I));
_[1]=0
```

En general, si $S = k[x_1, \ldots, x_n]$, una resolución libre de un S-módulo finitamente generado (en particular, de un ideal) se representará de la siguiente manera:

$$0 \to S^{\beta_p} \xrightarrow[\varphi_p]{\Lambda_p} \cdots \xrightarrow[\varphi_2]{\Lambda_2} S^{\beta_1} \xrightarrow[\varphi_1]{\Lambda_1} S^{\beta_0} \xrightarrow[\varphi_0]{\Lambda_0} M \to 0,$$

donde Λ_i es una matriz de tamaño $\beta_{i-1} \times \beta_i$ con coeficientes en S, y además verifica $\Lambda_{i-1}\Lambda_i = 0$ para todo $i = 1, \ldots, p$.

Lo que no es satisfactorio es la no unicidad de la resolución libre de un ideal, y el hecho de que dependa tanto de la elección de todos los sistemas de generadores. Esto se puede solucionar cuando comenzamos con un ideal homogéneo, o de forma más general, con un módulo graduado. El objetivo es, por tanto, graduar todos los módulos de sizigias.

Definición 1.2.8. Si $S = k[x_1, \ldots, x_n]$ (con la graduación estándar) y M es un S-módulo graduado finitamente generado, una *resolución libre graduada* de M es una resolución libre de la forma

$$\cdots \to F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0,$$

donde $F_j = S(-d_{j,1}) \oplus \cdots \oplus S(-d_{j,p_j})$ es un S-módulo graduado y φ_j es un homomorfismo graduado (de grado cero) para todo $j \geq 0$.

En el caso de resoluciones libres graduadas, también se verifica el teorema de las sizigias de Hilbert, en la siguiente versión graduada.

Teorema 1.2.9 (Teorema de las sizigias de Hilbert graduado, [5, §6.3, Thm. 3.8])**.** Si $S = k[x_1, \ldots, x_n]$, entonces todo S-módulo graduado y finitamente generado admite una resolución graduada finita de longitud menor o igual que n.

Definición 1.2.10. Sea M un S-módulo graduado. Una resolución graduada de M de la forma

$$\cdots \to F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$

se dice que es *minimal* si en las matrices que representan los homomorfismos graduados no hay constantes no nulas (es decir, si para todo i, $\ker \varphi_i \subset \mathfrak{m}F_i$, siendo $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$).

El hecho de que una resolución graduada sea minimal hace que sea única salvo isomorfismo, concepto que definimos a continuación.

Definición 1.2.11. Dos resoluciones graduadas

$$\ldots \to F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$
$$\ldots \to G_1 \xrightarrow{\psi_1} G_0 \xrightarrow{\psi_0} M \to 0$$

se dice que son *isomorfas* si existen homomorfismos graduados $\alpha_j : F_j \to G_j$ de grado 0 tales que $\psi_0 \circ \alpha_0 = \varphi_0$ y, para cada $j \geq 1$, el diagrama

$$\begin{array}{ccc} F_j & \xrightarrow{\varphi_j} & F_{j-1} \\ \downarrow{\scriptstyle \alpha_j} & & \downarrow{\scriptstyle \alpha_{j-1}} \\ G_j & \xrightarrow{\psi_j} & G_{j-1} \end{array}$$

es conmutativo, es decir, $\alpha_{j-1} \circ \varphi_j = \psi_j \circ \alpha_j$.

Teorema 1.2.12 ([5, §6.3, Thm. 3.13])**.** Dado un S-módulo graduado M, dos resoluciones graduadas minimales de M son isomorfas.

Dado un S-módulo graduado finitamente generado M, la "unicidad" de la resolución libre minimal graduada de M nos proporciona información numérica asociada al módulo M. Esta información se organiza en una tabla denominada el diagrama de Betti de M.

Diagrama de Betti . Ahora que tenemos garantizada la unicidad (salvo isomorfismo), podemos hablar de *la resolución libre minimal graduada* de un S-módulo graduado finitamente generado M, que existe siempre por el teorema de las sizigias graduado (teorema 1.2.9). Sea

$$0 \to F_p \to \cdots \to F_0 \to M \to 0$$

la resolución libre minimal graduada de M, donde $F_i = \oplus_j S(-j)^{\beta_{i,j}}$ para cada i; es decir, el módulo libre F_i está generado por $\beta_{i,j}$ elementos de grado j, para cada j. Los números $\beta_{i,j} = \beta_{i,j}(M)$ se llaman los *números de Betti graduados* de M y se presentan normalmente en una tabla, que se llama el *diagrama de Betti* de M, en el que la entrada correspondiente a la columna i y la fila j es el número $\beta_{i,i+j}$:

	i
j	$\beta_{i,i+j}$

Observación 1.2.13. Como en la resolución libre minimal graduada de M el grado mínimo en cada paso aumenta estrictamente, si $\beta_{ij} = 0$ para cada $j \leq j_0$, entonces $\beta_{i+1,j} = 0$ para todo $j \leq j_0 + 1$. Esta es la razón por la que el elemento correspondiente a la columna i y la fila j en el diagrama de Betti es $\beta_{i,i+j}$.

A partir del diagrama de Betti podemos extraer algunos invariantes importantes del módulo M:

Definición 1.2.14. Sea M un S-módulo graduado finitamente generado. Se llama *dimensión proyectiva* de M, y se denota $\mathrm{pd}(M)$, a la mínima longitud de todas las resoluciones libres graduadas de M.

Por el teorema 1.2.12, la dimensión proyectiva de M coincide con la longitud de la resolución libre minimal graduada de M. Además, podemos leer la dimensión proyectiva del diagrama de Betti de M, puesto que $\mathrm{pd}(M)$ es la etiqueta de la última columna del diagrama de Betti, esto es,

$$\mathrm{pd}(M) = \mathrm{máx}\{i : \beta_{i,j}(M) \neq 0 \text{ para algún } j\}.$$

Definición 1.2.15. Sea M un S-módulo graduado finitamente generado. La *regularidad de Castelnuovo-Mumford* de M es

$$\mathrm{reg}(M) = \mathrm{máx}\{j - i : \beta_{i,j}(M) \neq 0\}.$$

Notemos que la regularidad de Castelnuovo-Mumford es la etiqueta de la última fila del diagrama de Betti, es decir, la altura de la tabla.

Dado un S-módulo graduado finitamente generado M, $\mathrm{pd}(M)$ y $\mathrm{reg}(M)$ son dos medidas de la complejidad del ideal. El teorema de las sizigias de Hilbert graduado (teorema 1.2.9) afirma que $\mathrm{pd}(M) \leq n$. La regularidad de Castelnuovo-Mumford, por el contrario,

no se puede acotar de una manera tan sencilla en general, por lo que ha sido (y sigue siendo) objeto de estudio durante muchos años y ha dado lugar a diversas conjeturas, como la de Eisenbud-Goto, que se creía cierta (y se demostró en muchos casos particulares) hasta 2017, cuando J. McCullough e I. Peeva [23] encontraron toda una familia de contraejemplos que desmontaron la conjetura.

Conjetura 1.2.16 (de Eisenbud-Goto, [9])**.** Supongamos que el cuerpo k es algebraicamente cerrado y denotamos $S = k[x_1, \ldots, x_n]$. Si $I \subset S$ es un ideal primo homogéneo tal que $I \subset \langle x_1, \ldots, x_n \rangle^2$, entonces

$$\operatorname{reg}(I) \leq \deg(S/I) - \operatorname{codim}(I) + 1,$$

donde

- $\deg(S/I)$ denota la multiplicidad de S/I (también llamada grado, ver observación 1.4.7).
- $\operatorname{codim}(I)$ es la codimensión de I (que coincide con su altura).

Observación 1.2.17. Si $I \subset S = k[x_1, \ldots, x_n]$ es un ideal homogéneo, entonces

$$\operatorname{pd}(S/I) = \operatorname{pd}(I) + 1,$$
$$\operatorname{reg}(S/I) = \operatorname{reg}(I) - 1.$$

Esto se ve fácilmente observando que, si la resolución libre minimal graduada de I se escribe

$$0 \to F_p \to \cdots \to F_0 \to I \to 0,$$

entonces la resolución libre minimal graduada de S/I es

$$0 \to F_p \to \cdots \to F_0 \to S \to S/I \to 0,$$

y viceversa.

Observación 1.2.18. Desde el punto de vista computacional, existen métodos efectivos para encontrar la resolución libre minimal graduada de cualquier S-módulo finitamente generado M. El método más habitual es la denominada *resolución de Schreyer* [5, §6.3] que, mediante la definición de un orden monomial adecuado en cada módulo de sizigias permite encontrar una resolución libre graduada, a partir de la cual se puede obtener la resolución libre minimal graduada del módulo de partida.

1.3. Profundidad. Anillos y módulos Cohen-Macaulay

Sean R un anillo y M un módulo sobre R. Se dice que un elemento $x \in R$ es *M-regular* si no es un divisor de cero en M, es decir: si $xm = 0$ para algún $m \in M$, entonces $m = 0$.

Definición 1.3.1. Una sucesión $x_1, \ldots, x_r$ de elementos de R se dice que es *M-regular* (o que es una *M-sucesión*) si se verifican las dos condiciones siguientes:

(1) Para cada $i = 1 \ldots, r$, x_i es un elemento $(M/\langle x_1, \ldots, x_{i-1}\rangle M)$-regular.

(2) $M/\langle x_1, \ldots, x_r\rangle M \neq 0$.

Una sucesión R-regular se llama simplemente *sucesión regular*.

Observación 1.3.2. Una situación muy habitual se tiene cuando $(R, \mathfrak{m})$ es un anillo local y M es un R-módulo finitamente generado. En este caso, si $\langle x_1, \ldots, x_r\rangle \subset \mathfrak{m}$, entonces la condición (2) se verifica de forma automática por el *Lema de Nakayama*.

Ejemplo 1.3.3. El ejemplo paradigmático de sucesión regular es la sucesión $x_1, \ldots, x_n$ (o cualquier permutación de esta) formada por las n indeterminadas del anillo de polinomios $R = k[x_1, \ldots, x_n]$.

Si además suponemos que R es un anillo noetheriano y $x_1, \ldots, x_r$ es una M-sucesión, entonces está claro que la sucesión $\langle x_1\rangle \subset \langle x_1, x_2\rangle \subset \cdots \subset \langle x_1, \ldots, x_r\rangle$ es estrictamente creciente. Por lo tanto, una M-sucesión se puede extender a una sucesión *maximal*, en el sentido que definimos a continuación:

Definición 1.3.4. Dados $I \subset R$ un ideal y $x_1, \ldots, x_r$ una sucesión M-regular, diremos que la sucesión es *maximal* (en I) si para cualquier $x_{r+1} \in R$ ($x_{r+1} \in I$), $x_1, \ldots, x_r, x_{r+1}$ no es una sucesión M-regular.

El resultado clave de esta sección es el siguiente:

Teorema 1.3.5 (Rees, [2, Thm. 1.2.5])**.** Sean R un anillo Noetheriano, M un R-módulo finitamente generado e $I \subset R$ un ideal tal que $IM \neq M$. Entonces todas las sucesiones M-regulares maximales (en I) tienen la misma longitud.

Este resultado nos permite dar la definición de profundidad de un R-módulo M, donde R es un anillo local.

Definición 1.3.6. Sean $(R, \mathfrak{m})$ un anillo noetheriano local y M un R-módulo finitamente generado.

(1) La *profundidad* de M, denotada $\operatorname{depth}(M)$, es la longitud de las sucesiones M-regulares maximales contenidas en $\mathfrak{m}$.

(2) Diremos que M es un *módulo Cohen-Macaulay* si $\operatorname{depth}(M) = \dim(M)$, donde $\dim(M)$ denota la dimensión de Krull de M. Si $I \subset R$ es un ideal y $M = R/I$ es Cohen-Macaulay, diremos que I es *Cohen-Macaulay*.

(3) Diremos que un *anillo* R es *Cohen-Macaulay* si R es Cohen-Macaulay visto como R-módulo.

Observación 1.3.7. Si R es un anillo graduado, un ideal homogéneo $\mathfrak{m} \subset R$ se dice que es **maximal* si para cualquier ideal homogéneo I tal que $\mathfrak{m} \subsetneq I$ se tiene $I = R$. Cuando R tiene un único ideal **maximal* $\mathfrak{m}$, decimos que R es un anillo **local*, y lo denotamos $(R, \mathfrak{m})$. La razón por la que se introduce esta notación en [2] es que, cuando trabajamos con anillos graduados, los anillos *locales juegan el mismo papel que los anillos locales y cumplen resultados análogos a los que verifican los anillos locales. Nosotros vamos a aplicar las definiciones y resultados sobre profundidad en el anillo de polinomios $S = k[x_1, \ldots, x_n]$, que es un anillo *local.

Ejemplo 1.3.8. De nuevo, el mejor ejemplo de anillo Cohen-Macaulay es el del anillo de polinomios $R = k[x_1, \ldots, x_n]$, para el cual tenemos $\dim(R) = \operatorname{depth}(R) = n$.

Proposición 1.3.9 ([2, Prop. 1.2.12])**.** Sean $(R, \mathfrak{m})$ un anillo noetheriano local y $M \neq 0$ un R-módulo finitamente generado. Entonces $\operatorname{depth}(M) \leq \dim M$.

Teorema 1.3.10 (Fórmula de Auslander-Buchsbaum, [2, Thm. 1.3.3])**.**
Sean $S = k[x_1, \ldots, x_n]$ y $M \neq 0$ un S-módulo graduado finitamente generado. Entonces

$$\operatorname{pd}(M) + \operatorname{depth}(M) = \operatorname{depth}(S) = n.$$

Observación 1.3.11.

(1) Por el teorema de las sizigias de Hilbert graduado (teorema 1.2.9), $\operatorname{pd}(M) \leq n$. La fórmula de Auslander-Buchsbaum indica que la diferencia entre esos dos números es igual a la profundidad de M.

(2) En particular, podemos obtener la profundidad de un S-módulo graduado finitamente generado a partir del diagrama de Betti.

1.4. Función de Hilbert

Denotamos $S = k[x_1, \ldots, x_n]$ el anillo de polinomios en las variables $x_1, \ldots, x_n$ con coeficientes en el cuerpo k, con la graduación estándar. En esta sección recordamos el concepto de función y polinomio de Hilbert, así como su significado geométrico. Además, presentamos una caracterización de las funciones numéricas $\mathbb{N}_0 \to \mathbb{N}_0$ que son la función de Hilbert de alguna k-álgebra graduada estándar, este resultado se debe a Macaulay.

Definición 1.4.1. Si $M = \oplus_{d \in \mathbb{N}_0} M_d$ es un S-módulo graduado finitamente generado, su *función de Hilbert* es la función $\operatorname{HF}_M : \mathbb{N}_0 \to \mathbb{N}_0$ definida por

$$\operatorname{HF}_M(d) = \dim_k M_d,$$

donde $\dim_k M_d$ denota la dimensión de M_d como k-espacio vectorial (que es finita para todo d).

Obviamente, esto se puede extender a una función $\operatorname{HF}_M : \mathbb{Z} \to \mathbb{N}_0$ si M es $\mathbb{Z}$-graduado.

Notación. Si $I \subset S$ es un ideal homogéneo y $M = S/I$, denotaremos la función de Hilbert de M simplemente por HF_I.

Ejemplo 1.4.2.

- Sea $M = S = k[x_1, \ldots, x_n]$. Entonces, para cada $d \in \mathbb{N}_0$, $H_S(d)$ es igual al número de monomios en n variables de grado exactamente d, esto es,

$$\operatorname{HF}_S(d) = \dim_k S_d = \binom{d+n-1}{n-1}.$$

De hecho, si convenimos que $\binom{\lambda}{\mu} = 0$ para $\lambda < \mu$, entonces la fórmula anterior es válida para todo $d \in \mathbb{Z}$.

- De manera análoga, si $M = S(e)$ para un cierto $e \in \mathbb{Z}$, entonces

$$\mathrm{HF}_{S(e)}(d) = \mathrm{HF}_S(e+d) = \binom{e+d+n-1}{n-1}$$

para todo $d \in \mathbb{Z}$.

En el ejemplo anterior observamos que la función de Hilbert de S y la de $S(e)$ son funciones polinómicas. Esto es algo general, y es lo siguiente que vamos a demostrar. Para ello, primero probamos que la función de Hilbert es aditiva en sucesiones exactas cortas.

Lema 1.4.3. Sean M, N y P tres S-módulos graduados finitamente generados. Si tenemos una sucesión exacta corta

$$0 \to M \xrightarrow{\alpha} P \xrightarrow{\beta} N \to 0,$$

donde α y β son homomorfismos graduados (de grado cero), entonces $\mathrm{HF}_P = \mathrm{HF}_M + \mathrm{HF}_N$.

Demostración. Para cada $d \in \mathbb{N}_0$, de la sucesión exacta del enunciado obtenemos la siguiente sucesión exacta corta de k-espacios vectoriales de dimensión finita

$$0 \to M_d \xrightarrow{\alpha} P_d \xrightarrow{\beta} N_d \to 0.$$

Entonces el resultado se obtiene aplicando la conocida fórmula

$$\dim_k P_d = \dim_k \ker(\beta) + \dim_k \mathrm{im}(\beta).$$

□

Proposición 1.4.4 ([5, §6.4, Prop. 4.7])**.** Sean $S = k[x_1, \ldots, x_n]$ y M un S-módulo graduado finitamente generado. Entonces, para cada resolución libre graduada de M

$$0 \to F_p \xrightarrow{\varphi_p} F_{p-1} \xrightarrow{\varphi_{p-1}} \ldots \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0,$$

se verifica

$$\mathrm{HF}_M(d) = \dim_k M_d = \sum_{j=0}^{p} (-1)^j \dim_k (F_j)_d = \sum_{j=0}^{p} (-1)^j \mathrm{HF}_{F_j}(d).$$

Demostración. Para cada $j = 0, \ldots, p$ consideramos la sucesión exacta corta

$$0 \to G_{j+1} \hookrightarrow F_j \xrightarrow{\varphi_j} G_j \to 0, \tag{1.4.1}$$

donde $G_j = \mathrm{im}(\varphi_j)$ para $j = 0, \ldots, p$ y $G_{p+1} = 0$, notemos que $G_0 = \mathrm{im}(\varphi_0) = M$. Aplicando el lema 1.4.3 a cada sucesión (1.4.1) tenemos que

$$\begin{aligned}\sum_{j=0}^{p} (-1)^j \mathrm{HF}_{F_j}(d) &= \sum_{j=0}^{p} (-1)^j \left[\mathrm{HF}_{G_j}(d) + \mathrm{HF}_{G_{j+1}}(d)\right] \\ &= (\mathrm{HF}_{G_0}(d) + \mathrm{HF}_{G_1}(d)) - (\mathrm{HF}_{G_1}(d) + \mathrm{HF}_{G_2}(d)) + \cdots + (-1)^p \left(\mathrm{HF}_{G_p}(d) + \mathrm{HF}_{G_{p+1}}(d)\right) \\ &= \mathrm{HF}_{G_0}(d) = \mathrm{HF}_M(d).\end{aligned}$$

□

Teorema 1.4.5 (Hilbert, [5, §6.4, Prop. 4.7])**.** Si $S = k[x_1, \ldots, x_n]$ y M es un S-módulo graduado finitamente generado, entonces existe un polinomio $\mathrm{HP}_M \in \mathbb{Q}[z]$ (único) tal que

$$\mathrm{HP}_M(d) = \mathrm{HF}_M(d)$$

para todo $d \in \mathbb{N}_0$ suficientemente grande.

Demostración. Aplicando el lema 1.4.3 tenemos que, para un módulo libre desplazado de la forma

$$N = S(-e_1) \oplus \cdots \oplus S(-e_m),$$

su función de Hilbert es

$$\mathrm{HF}_N(d) = \sum_{l=1}^{m} \binom{d - e_l + n - 1}{n - 1}.$$

Denotamos $\delta = \mathrm{pd}(M)$ y sea

$$0 \to \oplus_j S(-j)^{\beta_{\delta,j}} \to \cdots \to \oplus_j S(-j)^{\beta_{0,j}} \to M \to 0,$$

la resolución libre minimal graduada de M, que existe por el teorema 1.2.9. Aplicando la proposición 1.4.4 deducimos que

$$\mathrm{HF}_M(d) = \sum_{i,j \mid \beta_{i,j} \neq 0} \binom{d - j + n - 1}{n - 1}.$$

Si consideramos el polinomio

$$\mathrm{HP}_M(d) = \sum_{i,j \mid \beta_{i,j} \neq 0} \beta_{i,j} \frac{(d - j + n - 1)(d - j + n - 2) \ldots (d - j + 1)}{(n - 1)!},$$

entonces es claro que $\mathrm{HF}_M(d) = \mathrm{HP}_M(d)$ si d verifica $d - j + n - 1 \geq 0$ para todo j. □

Definición 1.4.6. En las condiciones del teorema anterior, el polinomio HP_M se denomina *polinomio de Hilbert* de M y el mínimo número d para el que se tiene la igualdad $\mathrm{HF}_M(d) = \mathrm{HP}_M(d)$ se llama la *regularidad de la función de Hilbert*, y se denota $\mathrm{r}(M)$.

Notación. Si $I \subset S$ es un ideal homogéneo, el polinomio de Hilbert de S/I se denotará simplemente HP_I.

Notemos que la demostración del teorema 1.4.5 es constructiva, es decir, nos permite calcular el polinomio de Hilbert de manera explítica si conocemos la resolución libre minimal graduada de M. Si no queremos calcular esta resolución, podemos acudir directamente a SINGULAR. Una forma posible de calcular la función de Hilbert de M es a partir de la *serie de Hilbert* (ver [1, Chap. 11]), y para calcular el polinomio de Hilbert podemos acudir a la librería "poly.lib".

Observación 1.4.7. Supongamos que el cuerpo k es algebraicamente cerrado, denotamos $S = k[x_0, x_1, \ldots, x_n]$ y consideramos un ideal homogéneo $I \subset S$. En este caso, el polinomio de Hilbert de S/I contiene información geométrica sobre el conjunto algebraico que define I en el espacio proyectivo $\mathbb{P}^n$,

$$V(I) = \{(a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n : f(a_0, a_1, \ldots, a_n) = 0, \text{ para todo } f \in I \text{ homogéneo}\}.$$

En particular,

- El grado e del polinomio HP_I es la *dimensión (proyectiva)* del conjunto algebraico $V(I)$, es decir, $e = \deg(\mathrm{HP}_I) = \dim(S/I) - 1$, donde dim denota la dimensión de Krull.
- El término líder de HP_I se escribe de la forma $\frac{c}{e!}z^e$, donde c es el *grado de* $V(I)$, esto es, el número de puntos en los que una variedad lineal genérica de dimensión $n - e$ corta a $V(I)$.

Presentamos ahora dos resultados que relacionan la regularidad del polinomio de Hilbert de un S-módulo M finitamente generado con su regularidad de Castelnuovo-Mumford.

Proposición 1.4.8 ([8, Thm. 4.2])**.** Sea M un módulo graduado finitamente generado sobre el anillo de polinomios $S = k[x_1, \ldots, x_n]$. Entonces se verifican las siguientes propiedades:

(1) $\mathrm{r}(M) \leq \mathrm{reg}(M) + 1$.

(2) Si M es un módulo de dimensión proyectiva δ, entonces $\mathrm{r}(M) \leq \mathrm{reg}(M) + \delta - (n-1)$.

(3) Si $X \subset \mathbb{P}^{n-1}$ es una variedad proyectiva (irreducible) y $M = S/I(X)$, donde $I(X)$ denota el ideal de anulación de X, entonces $\mathrm{r}(M) \leq \mathrm{reg}(M)$.

Demostración.

(1) Se deduce a partir de (2) teniendo en cuenta que la dimensión proyectiva de M es $\mathrm{pd}(M) \leq n - 1$ por el teorema de las sizigias de Hilbert graduado (teorema 1.2.9).

(2) Por hipótesis, la resolución libre minimal graduada de M se escribe

$$0 \to \oplus_j S(-j)^{\beta_{\delta,j}} \to \cdots \to \oplus_j S(-j)^{\beta_{0,j}} \to M \to 0,$$

y tenemos que $\mathrm{reg}(M) = \max\{j - i : \beta_{i,j} \neq 0\}$. Como hemos visto en la prueba del teorema 1.4.5, $\mathrm{HF}_M(d)$ y $\mathrm{HP}_M(d)$ coinciden si $d - j + n - 1 \geq 0$ para todo j. Tomamos índices i, j tales que $\beta_{i,j} \neq 0$ y sea $d \geq \mathrm{reg}(M) + \delta - (n-1)$, entonces

$$d - j + n - 1 \geq \mathrm{reg}(M) + \delta - j \geq j - i + i - j = 0,$$

de donde se deduce la desigualdad del enunciado.

(3) Como X es irreducible, entonces el ideal $I(X)$ es primo y la profundidad de M es $\operatorname{depth}(M) \geq 1$. Por lo tanto, de la fórmula de Auslander-Buchsbaum (teorema 1.3.10) deducimos que

$$\operatorname{pd}(M) = n - \operatorname{depth}(M) \leq n - 1,$$

y el resultado se concluye aplicando (2).

□

Proposición 1.4.9 ([8, Cor. 4.8])**.** Sea M un S-módulo graduado finitamente generado. Si M es Cohen-Macaulay, entonces

$$\operatorname{r}(M) = 1 - \operatorname{depth}(M) + \operatorname{reg}(M) = 1 - \dim(M) + \operatorname{reg}(M),$$

donde $\dim(M)$ denota la dimensión de Krull de M.

1.4.1. Álgebras graduadas estándar

Definición 1.4.10. Una *k-álgebra graduada estándar* es una k-álgebra R junto con una descomposición $R = \oplus_{d\in\mathbb{N}_0} R_d$ verificando $R_0 = k$, $R_i R_j \subset R_{i+j}$ para todo $i, j \in \mathbb{N}_0$, y tal que está finitamente generada como k-álgebra por un número finito de elementos de R_1 (es decir, por elementos de grado 1).

De la definición anterior se sigue que cada R_d es un espacio vectorial de dimensión finita sobre k. Además, como R está generada como k-álgebra por R_1, tenemos $R_i R_j = R_{i+j}$ para todo $i, j \in \mathbb{N}_0$. Al igual que hicimos en la definición 1.4.1, definimos la *función de Hilbert* de R como la aplicación $\operatorname{HF}_R : \mathbb{N}_0 \to \mathbb{N}_0$ dada por $\operatorname{HF}_R(d) = \dim_k (R_d)$ para cada $d \in \mathbb{N}_0$, donde $\dim_k R_d$ denota la dimensión de R_d como k-espacio vectorial. Notemos que para cualquier álgebra graduada estándar R se tiene $\operatorname{HF}_R(0) = 1$. Además, R está generada como k-álgebra por cualesquiera $\operatorname{HF}_R(1)$ elementos linealmente independientes de R_1. El teorema 1.4.5 también se verifica para k-álgebras graduadas estándar.

Para caracterizar las funciones de Hilbert de las k-álgebras graduadas estándar, usaremos la representación binomial de un número.

Lema 1.4.11 ([2, Lemma 4.2.6])**.** Sean $a \geq i \geq 1$ enteros positivos. Entonces existen unos únicos números naturales $a_i > a_{i-1} > \cdots > a_1 \geq 0$ tales que

$$a = \binom{a_i}{i} + \binom{a_{i-1}}{i-1} + \cdots + \binom{a_1}{1}. \tag{1.4.2}$$

La ecuación (1.4.2) se denomina la *i-ésima representación binomial* de a y los números $a_1, \ldots, a_i$ se llaman los *i-ésimos coeficientes de Macaulay* de a.

Notación. Si $a = \sum_{j=1}^{i} \binom{a_j}{j}$ es la i-ésima representación binomial de a, denotamos $a^{\langle i \rangle} = \sum_{j=1}^{i} \binom{a_j+1}{j+1}$ y $0^{\langle i \rangle} = 0$.

Ejemplo 1.4.12. Por ejemplo, si $a = 15$ e $i = 3$, podemos escribir 15 de la manera siguiente:

$$15 = \binom{5}{3} + \binom{3}{2} + \binom{2}{1},$$

de donde se sigue que $a_3 = 5 > a_2 = 3 > a_1 = 2$. Además,

$$15^{\langle 3\rangle} = \binom{6}{4} + \binom{4}{3} + \binom{3}{2} = 22.$$

El siguiente resultado de Macaulay caracteriza las funciones numéricas (es decir, las aplicaciones $\mathbb{N}_0 \to \mathbb{N}_0$) que son la función de Hilbert de alguna k-álgebra graduada estándar.

Teorema 1.4.13 (Macaulay, [2, Thm. 4.2.10])**.** Sea $h : \mathbb{N}_0 \to \mathbb{N}_0$ una función numérica. Las siguientes dos condiciones son equivalentes:

(a) Existe una k-álgebra graduada estándar R cuya función de Hilbert verifica $\mathrm{HF}_R(d) = h(d)$ para todo $d \in \mathbb{N}_0$.

(b) La función h verifica $h(0) = 1$ y $h(d+1) \leq h(d)^{\langle d\rangle}$ para todo $d \in \mathbb{N}$.

Ejemplo 1.4.14. Consideramos la función $h : \mathbb{N}_0 \to \mathbb{N}_0$ dada por $h(0) = 1$, $h(1) = 5$, $h(2) = 15$, $h(3) = 33$, $h(4) = 61$, $h(5) = 100$, $h(6) = 152$. Entonces se tiene $h(1)^{\langle 1\rangle} = 15$, $h(2)^{\langle 2\rangle} = 33$, $h(3)^{\langle 3\rangle} = 61$, $h(4)^{\langle 4\rangle} = 100$, $h(5)^{\langle 5\rangle} = 152$. Por lo tanto, aplicando el teorema 1.4.13, existe una k-álgebra graduada estándar R cuya función de Hilbert verifica $\mathrm{HF}_R(d) = h(d)$ para cada $d \leq 6$.
Por ejemplo, podemos tomar $R = S/I$, donde $S = k[x_1, \ldots, x_5]$ e $I = \langle x_5^3, x_4x_5^2, x_3^3x_5^2\rangle$. Esto se puede comprobar usando SINGULAR.

```
> ring r = 0, x(1..5), dp;
> ideal I = x(5)^3, x(4)*x(5)^2, x(3)^3*x(5)^2;
> hilb(std(I),1);
1,0,0,-2,1,-1,2,-1,0
```

La serie de Hilbert de R es

$$\frac{1 - 2t^3 + t^4 - t^5 + 2t^6 - t^7}{(1-t)^5} = 1 + 5t + 15t^2 + 33t^3 + 61t^4 + 100t^5 + 152t^6 + \ldots$$

1.5. Álgebras monomiales

Las variedades monomiales juegan un papel clave en este trabajo. Por lo tanto, en esta sección vamos a estudiar los anillos de coordenadas de estas variedades monomiales, que se denominan *álgebras monomiales*.

Consideramos el anillo de polinomios en las variables $t_1, \ldots, t_r$, $k[\mathbf{t}] = k[t_1, \ldots, t_r]$, y un conjunto finito de monomios de este anillo, que denotamos $\mathcal{M} = \{m_1, \ldots, m_n\}$. Cada monomio m_i se escribe de la forma $m_i = \mathbf{t}^{\alpha_i}$ para cada $i = 1, \ldots, n$, siendo $\alpha_i \in \mathbb{N}_0^r$ un multi-índice.

Definición 1.5.1. El *subanillo monomial engendrado por* $\mathcal{M}$ es la k-subálgebra

$$k[\mathcal{M}] = k[m_1, \ldots, m_n] \subset k[t_1, \ldots, t_r].$$

Observación 1.5.2. El anillo $k[\mathcal{M}]$ es igual al anillo del semigrupo $\mathcal{S} = \langle \alpha_1, \ldots, \alpha_n \rangle \subset \mathbb{N}_0^r$, es decir, el semigrupo generado por los exponentes de los monomios $m_1, \ldots, m_n$. Por lo tanto, $k[\mathcal{M}]$ está generado como k-espacio vectorial por el conjunto $\{\mathbf{t}^\alpha : \alpha \in \mathcal{S}\}$.

Notemos que el anillo $k[\mathcal{S}] \subset k[\mathbf{t}]$ es un anillo graduado, con la graduación heredada de $k[\mathbf{t}]$. Consideramos el morfismo de k-álgebras definido por

$$\varphi : k[x_1, \ldots, x_n] \to k[t_1, \ldots, t_r], \ \varphi(x_i) = m_i.$$

Entonces es claro que φ es un morfismo graduado si consideramos $k[x_1, \ldots, x_n]$ con la graduación dada por $\deg(x_i) = \deg(m_i)$.

Definición 1.5.3. Con las notaciones anteriores,

- El núcleo de φ, $\mathfrak{p}_\mathcal{M} = \ker \varphi$ se llama el *ideal de presentación* o *ideal tórico* de $k[\mathcal{M}]$ con respecto a $m_1, \ldots, m_r$.
- La *matriz asociada a* $k[\mathcal{M}]$ es la matriz Λ de tamaño $r \times n$ cuya columna i-ésima es el vector dado por el multi-índice $\alpha_i \in \mathbb{N}_0^r$.

Por el primer teorema de isomorfía de anillos, es claro que $k[\mathcal{M}] \simeq k[x_1, \ldots, x_n]/\mathfrak{p}_\mathcal{M}$, puesto que φ es un morfismo de anillos sobreyectivo.

Proposición 1.5.4 ([29, Prop. 7.1.2])**.** El ideal de presentación $\mathfrak{p}_\mathcal{M}$ de $k[\mathcal{M}]$ es un ideal primo, binomial y homogéneo (para la graduación dada por $\deg(x_i) = \deg(m_i)$, $i = 1, \ldots, n$).

Demostración. Notemos que $k[x_1, \ldots, x_n]/\mathfrak{p}_\mathcal{M} \simeq k[\mathcal{M}] \subset k[t_1, \ldots, t_r]$ es un dominio, luego $\mathfrak{p}_\mathcal{M}$ es primo. Además, $\mathfrak{p}_\mathcal{M}$ es homogéneo por ser φ un morfismo graduado.
Veamos que $\mathfrak{p}_\mathcal{M}$ es binomial. Para ello, consideramos el ideal $I \subset k[x_1, \ldots, x_n]$ generado por los binomios de $\mathfrak{p}_\mathcal{M}$ y veamos que $I = \mathfrak{p}_\mathcal{M}$. Como $\mathfrak{p}_\mathcal{M}$ es homogéneo, es suficiente probar que $(\mathfrak{p}_\mathcal{M})_d \subset I$ para todo d. Sea $h \in (\mathfrak{p}_\mathcal{M})_d$ y escribimos $h = \sum_{i=1}^r a_{\gamma_i} \mathbf{x}^{\gamma_i}$ para ciertos $a_{\gamma_i} \in k^*$ y monomios $\mathbf{x}^{\gamma_i} \in k[x_1, \ldots, x_n]_d$. Razonamos por inducción sobre $r \geq 2$. El caso $r = 2$ está claro por la definición de I. Supongamos entonces que $r \geq 3$. Como $h \in \mathfrak{p}_\mathcal{M}$, tenemos que $\sum_{i=1}^r a_{\gamma_i} \mathbf{m}^{\gamma_i} = 0$ (donde $\mathbf{m}^{\gamma_i}$ denota $m_1^{(\gamma_i)_1} \ldots m_n^{(\gamma_i)_n}$). Entonces hay dos opciones, o bien $h = 0$, en cuyo caso es claro que $h \in I$; o bien existen dos índices $1 \leq i < j \leq r$ tales que $\mathbf{m}^{\gamma_i} = \mathbf{m}^{\gamma_j}$. Por simplicidad, supongamos que $i = 1$ y $j = 2$. Entonces podemos escribir

$$h = a_{\gamma_1} (\mathbf{x}^{\gamma_1} - \mathbf{x}^{\gamma_2}) + (a_{\gamma_2} + a_{\gamma_1}) \mathbf{x}^{\gamma_2} + \sum_{i=3}^r a_{\gamma_i} \mathbf{x}^{\gamma_i} = a_{\gamma_1} (\mathbf{x}^{\gamma_1} - \mathbf{x}^{\gamma_2}) + g,$$

y aplicando la hipótesis de inducción a g concluimos la prueba. □

Los ideales tóricos (o de presentación) aparecen de forma natural cuando consideramos variedades definidas paramétricamente por monomios. Denotamos por $X \subset k^n$ el conjunto definido paramétricamente por

$$\begin{cases} x_1 &= m_1(t_1, \ldots, t_r) \\ & \vdots \\ x_n &= m_n(t_1, \ldots, t_r) \end{cases}$$

cuando $(t_1, \ldots, t_r) \in k^r$. La clave está en que el ideal de anulación de este subconjunto de k^n es exactamente el ideal de presentación $\mathfrak{p}_{\mathcal{M}}$, siempre que el cuerpo k sea infinito.

Proposición 1.5.5 ([29, Cor. 7.1.12])**.** Si el cuerpo k es infinito, entonces el ideal de anulación de X, $I(X)$, cuyos elementos son los polinomios $f \in k[x_1, \ldots, x_n]$ que se anulan en todos los puntos de X coincide con el ideal $\mathfrak{p}_{\mathcal{M}}$.

La prueba de este resultado se apoya en la teoría de la eliminación, la clave está en que el ideal de presentación $\mathfrak{p}_{\mathcal{M}}$ se puede escribir

$$\mathfrak{p}_{\mathcal{M}} = \langle x_1 - m_1, \ldots, x_n - m_n \rangle \cap k[x_1, \ldots, x_n].$$

Además, es sencillo calcular este ideal en ejemplos concretos gracias a las bases de Gröbner y los órdenes de eliminación (también llamados órdenes producto, ver [4, §3.1, Thm. 2]).

Ejemplo 1.5.6. Sea $k = \mathbb{C}$ el cuerpo de los números complejos y consideramos el conjunto $X \subset \mathbb{C}^3$ definido paramétricamente por

$$\begin{cases} x = t^7 \\ y = t^8 \\ z = t^9 \end{cases}$$

para $t \in \mathbb{C}$. Como el cuerpo $\mathbb{C}$ es infinito, el ideal de presentación de $\mathbb{C}[t^7, t^8, t^9]$ coincide con el ideal de anulación de $I(X)$ y ambos son iguales a

$$\mathfrak{p} = I(X) = \left\langle x - t^7, y - t^8, z - t^9 \right\rangle \cap \mathbb{C}[x, y, z] = \left\langle y^2 - xz, x^4 y - z^4, x^5 - yz^3 \right\rangle.$$

```
> ring r = 0,(x,y,z,t),dp;
> ideal I = x-t7,y-t8,z-t9;
> ideal J = eliminate(I,t);
> J;
J[1]=y2-xz
J[2]=x4y-z4
J[3]=x5-yz3
```

Veamos ahora qué pasa si trabajamos en un cuerpo finito. Por ejemplo, supongamos que $k = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ es el cuerpo finito de dos elementos. En este caso, el ideal de presentación del anillo monomial $\mathbb{F}_2[t^7, t^8, t^9]$ se calcula igual que antes (basta poner 2 en la característica del cuerpo) y obtenemos el mismo resultado,

$$\mathfrak{p} = \left\langle y^2 + xz, x^4 y + z^4, x^5 + yz^3 \right\rangle.$$

Sin embargo, este ideal no es igual a $I(X)$. Notemos que para $k = \mathbb{F}_2$ tenemos

$$X = \{(t^7, t^8, t^9) : t \in \mathbb{F}_2\} = \{(t, t, t) : t \in \mathbb{F}_2\} \subset \mathbb{F}_2^3$$

es una recta $\mathbb{F}_2^3$, y es inmediato comprobar que sus ecuaciones vienen dadas por $I(X) = \langle x + y, x + z\rangle \neq \mathfrak{p}$.

Aplicando una de las definiciones equivalentes de dimensión (la que tiene que ver con el grado de trascendencia), se prueba fácilmente el resultado siguiente:

Proposición 1.5.7 ([29, Prop. 7.1.17])**.** Si $k[\mathcal{M}]$ es un subanillo monomial sobre un cuerpo k generado por un conjunto finito de monomios $\mathcal{M}$ y Λ es su matriz asociada, entonces

$$\dim k[\mathcal{M}] = \mathrm{rk}\,(\Lambda),$$

donde $\dim k[\mathcal{M}]$ denota la dimensión de Krull de $k[\mathcal{M}]$ y $\mathrm{rk}(\Lambda)$ denota el rango de la matriz Λ.

1.5.1. Curvas monomiales

Sean k un cuerpo y $a_1, \ldots, a_n \in \mathbb{N}$ números tales que $\gcd(a_1, \ldots, a_n) = 1$. Consideramos $\mathcal{S} = \langle a_1, \ldots, a_n\rangle$, el subsemigrupo de $\mathbb{N}_0$ generado por $a_1, \ldots, a_n$, que es un semigrupo numérico.

Definición 1.5.8. Una *curva monomial afín* es un conjunto de la forma

$$\Gamma = \{(t^{a_1}, \ldots, t^{a_n}) : t \in k\} \subset \mathbb{A}_k^n,$$

donde $\mathbb{A}_k^n$ denota el espacio afín n-dimensional sobre k^n, que confundimos habitualmente con el propio k^n.

Consideramos los anillos de polinomios $R = k[x_1, \ldots, x_n]$ y $k[t]$, ambos graduados definiendo $\deg(x_i) = a_i$, para cada $i = 1, \ldots, n$ y $\deg(t) = 1$. Sea $\varphi : R \to k[t]$ el homomorfismo de k-álgebras definido por $\varphi(x_i) = t^{a_i}$. Entonces $\mathrm{im}(\varphi) = k[\mathcal{S}]$ es el anillo del semigrupo $\mathcal{S}$ y $\mathfrak{p} = \ker\varphi$ es el ideal tórico (o ideal de presentación) de $k[\mathcal{S}]$, siguiendo la terminología que habíamos usado ya para los anillos monomiales.

Proposición 1.5.9 ([30, Lemma 8.8.1])**.** El ideal $\mathfrak{p}$ es un ideal primo, binomial y homogéneo de R (para la graduación dada por $\deg(x_i) = a_i$). Además, se verifica $\Gamma = V(\mathfrak{p})$, $\dim(R/\mathfrak{p}) = 1$ y, si k es un cuerpo infinito, entonces $I(\Gamma) = \mathfrak{p}$.

Observación 1.5.10. En particular, como $\Gamma = V(\mathfrak{p})$ independientemente del cuerpo k, una curva monomial afín es siempre una subvariedad afín de k^n.

Consideramos la inmersión del espacio afín $\mathbb{A}_k^n$ en el espacio proyectivo $\mathbb{P}_k^n$ dada por

$$\begin{aligned} \mathbb{A}_k^n &\overset{i}{\hookrightarrow} \mathbb{P}_k^n, \\ (x_1, \ldots, x_n) &\mapsto (1 : x_1 : \cdots : x_n). \end{aligned}$$

Proposición 1.5.11 ([29, Prop. 10.1.17])**.** Sean $a_1 < \cdots < a_n$ números naturales tales que $\gcd(a_1, \ldots, a_n) = 1$ y consideramos la curva afín monomial $\Gamma = \{(t^{a_1}, \ldots, t^{a_n}) : t \in k\}$. Si el cuerpo k es algebraicamente cerrado de característica cero, entonces la clausura proyectiva de Γ es

$$\overline{\Gamma} = \overline{i(\Gamma)} = \{(u^{a_n} : u^{a_n - a_1}v^{a_1} : \cdots : u^{a_n - a_{n-1}}v^{a_{n-1}} : v^{a_n}) \in \mathbb{P}^n_k \mid (u : v) \in \mathbb{P}^1_k\},$$

donde la barra en $i(\Gamma)$ denota la clausura para la topología de Zariski en $\mathbb{P}^n_k$.

La proposición 1.5.11 nos indica cómo debemos definir el concepto de curva monomial proyectiva.

Definición 1.5.12. Una *curva monomial proyectiva* es un conjunto de la forma

$$\overline{\Gamma} = \{(u^{a_n} : u^{a_n - a_1}v^{a_1} : \cdots : u^{a_n - a_{n-1}}v^{a_{n-1}} : v^{a_n}) \in \mathbb{P}^n_k \mid (u : v) \in \mathbb{P}^1_k\}.$$

Cuando el cuerpo k es algebraicamente cerrado y de característica cero, sabemos que una curva monomial proyectiva es, en particular, un conjunto algebraico proyectivo. Por lo tanto, podemos aplicar toda la teoría de variedades proyectivas que conocemos (ver, por ejemplo, [19]).

1.5.2. Variedades de Veronese y sus proyecciones monomiales

En esta última subsección vamos a cambiar ligeramente la notación, ahora utilizaremos como parámetros las variables $\mathbf{x}$ y como coordenadas unas nuevas variables, que llamaremos $\mathbf{w}$. Este cambio afecta también al capítulo 5, cuando trabajemos con las variedades de Veronese.

Sea $S = k[x_0, x_1, \ldots, x_n]$ el anillo de polinomios en $n+1$ variables con coeficientes en el cuerpo k, que suponemos algebraicamente cerrado, y consideramos en S la graduación estándar. Fijamos dos números $n, d \in \mathbb{N}$ y denotamos $N_{n,d} := \binom{n+d}{n}$. Consideramos el conjunto $\mathcal{M}_{n,d} = \{m_0, \ldots, m_{N_{n,d}-1}\} \subset S$ formado por todos los monomios de grado exactamente d en el anillo S, ordenados según el orden lexicográfico (LEX) con $x_0 > x_1 > \cdots > x_n$.

Definición 1.5.13. La *aplicación de Veronese de grado d* es

$$\begin{aligned} \nu_{n,d} : \mathbb{P}^n &\to \mathbb{P}^{N_{n,d}-1} \\ p = (x_0 : \cdots : x_n) &\mapsto \nu_{n,d}(p) = \left(m_0(\mathbf{x}) : \cdots : m_{N_{n,d}-1}(\mathbf{x})\right), \end{aligned}$$

donde $\mathbf{x} = (x_0, x_1, \ldots, x_n)$.

Observación 1.5.14. (1) Cualquier aplicación que difiere de $\nu_{n,d}$ en un automorfismo de $\mathbb{P}^{N_{n,d}-1}$ también se llama aplicación de Veronese.

(2) Geométricamente, la aplicación de Veronese está caracterizada por la propiedad siguiente: "las hipersuperficies de grado d en $\mathbb{P}^n$ son exactamente las secciones hiperplanas de la imagen $\nu_{n,d}(\mathbb{P}^n) \subset \mathbb{P}^{N_{n,d}-1}$". Esto se deduce de la teoría de sistemas lineales.

Consideramos nuevas variables $w_0, \ldots, w_{N_{n,d}-1}$ y denotamos $S' = k[w_0, \ldots, w_{N_{n,d}-1}]$ el anillo de polinomios en estas nuevas variables, con la graduación estándar.

Proposición 1.5.15. La imagen de la aplicación de Veronese, $X_{n,d} := \nu_{n,d}(\mathbb{P}^n)$ es una variedad algebraica proyectiva, denominada *variedad de Veronese*. Además, el ideal de anulación de la variedad de Veronese $I(X_{n,d}) \subset S'$ es el ideal homogéneo y primo engendrado por todos los binomios de grado 2 de la forma

$$w_i w_j - w_l w_l \text{ tales que } m_i m_j = m_k m_l.$$

Demostración. Consideramos el morfismo de k-álgebras $\varphi : S' = k[w_0, \ldots, w_{N_{n,d}-1}] \to S = k[x_0, x_1, \ldots, x_n]$ definido por $\varphi(w_i) = m_i$ para cada $i = 0, \ldots, N_{n,d} - 1$. Entonces está claro que $\ker \varphi$ es primo (porque S es un dominio) y homogéneo ($\varphi(S'_i) \subset S_{i \cdot d}$). Por la proposición 1.5.5, $\ker \varphi = I(X_{n,d})$, y es sencillo comprobar $V(\ker \varphi) = X_{n,d}$, lo que implica que $X_{n,d}$ es una subvariedad proyectiva de $\mathbb{P}^{N_{n,d}-1}$. □

Ejemplo 1.5.16. Sean $n = 1$ y $d \geq 1$ un número natural. En este caso tenemos $N_{n,d} = \binom{1+d}{1} = d+1$. La *curva racional normal de grado d* es la variedad de Veronese $X_{1,d} \subset \mathbb{P}^n$, que es la imagen del morfismo

$$\nu_{1,d} : \mathbb{P}^1 \to \mathbb{P}^d, \ \nu_{1,d}(x_0 : x_1) = (x_0^d : x_0^{d-1} x_1 : \cdots : x_0 x_1^{d-1} : x_1^d).$$

El ideal homogéneo $I(X_{1,d})$ está generado por las $\binom{d}{2}$ cuádricas obtenidas a partir de los menores 2×2 de la matriz

$$\begin{pmatrix} w_0 & w_1 & \ldots & w_{d-1} \\ w_1 & w_2 & \ldots & w_d \end{pmatrix}.$$

Si consideramos el morfismo $\varphi : S' \to S$ como en la demostración de la proposición 1.5.15, entonces es sencillo comprobar que $\varphi(S'_i) = S_{i \cdot d}$, de donde deducimos que

$$(S'/I(X_{1,d}))_i \simeq S_{i \cdot d},$$

luego la función de Hilbert de $X_{1,d}$ está dada por

$$\mathrm{HF}_{X_{1,d}}(s) = \dim_k (S'/I(X_{1,d}))_s = sd + 1, \ s \in \mathbb{N}_0.$$

Como esta expresión es un polinomio para todo $s \geq 0$, tenemos

$$\mathrm{HF}_{X_{1,d}}(s) = \mathrm{HP}_{X_{1,d}}(s) = sd + 1 \text{ para todo } s \in \mathbb{N}_0.$$

Observación 1.5.17. De manera análoga, la función de Hilbert de la variedad de Veronese $X_{n,d}$ es

$$\mathrm{HF}_{X_{n,d}}(s) = \binom{sd+n}{n} = \mathrm{HP}_{X_{n,d}}(s), \ \forall s \geq 0.$$

En particular, de aquí se deduce que la dimensión de la variedad $X_{n,d}$ es n y su grado es d^n.

Veamos ahora cómo construir proyecciones monomiales de las variedades de Veronese. Dado un subconjunto $\Omega_{n,d} = \{m_{i_0}, \dots, m_{i_{\mu_{n,d}-1}}\} \subset \mathcal{M}_{n,d}$ de monomios de grado d, con cardinal $|\Omega_{n,d}| = \mu_{n,d}$, consideramos la aplicación racional

$$\varphi\Omega_{n,d} : \mathbb{P}^n \dashrightarrow \mathbb{P}^{\mu_{n,d}-1}$$

definida por $p = (x_0 : \cdots : x_n) \dashmapsto \Big(m_{i_0}(\mathbf{x}) : \cdots : m_{i_{\mu_{n,d}-1}}(\mathbf{x})\Big)$, donde $\mathbf{x} = (x_0, \dots, x_n)$. Notemos que esta aplicación es racional, pues no tiene por qué estar bien definida en todos los puntos de $\mathbb{P}^n$ (puede haber puntos en los que se anulen todos los monomios de $\Omega_{n,d}$).

Observación 1.5.18. En el lenguaje de sistemas lineales, lo que estamos haciendo es considerar un subsistema lineal del sistema lineal de las hipersuperficies de grado d en $\mathbb{P}^n$. Aunque el sistema completo no tiene puntos base, el subsistema puede tener algún punto base (por eso la aplicación $\varphi\Omega_{n,d}$ es racional).

Ejemplo 1.5.19. Consideramos la aplicación de Cremona, que es la aplicación $\mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ definida por $(x_0 : x_1 : x_2) \dashmapsto (x_0x_1 : x_0x_2 : x_1x_2)$. Está claro que esta aplicación no está definida en los puntos $(1 : 0 : 0)$, $(0 : 1 : 0)$ y $(0 : 0 : 1)$. Estos son los puntos base del subsistema lineal que estamos considerando.

Definición 1.5.20. La *proyección monomial de la variedad de Veronese $X_{n,d}$ parametrizada por $\Omega_{n,d}$* es la variedad algebraica proyectiva definida por $Y_{n,d} := \overline{\varphi\Omega_{n,d}(\mathbb{P}^n)} \subset \mathbb{P}^{\mu_{n,d}-1}$, donde la barra denota la clausura para la topología de Zariski.

Notemos que podemos factorizar $\varphi\Omega_{n,d}$ a través de la aplicación de Veronese $\nu_{n,d}$, como se muestra en el diagrama conmutativo siguiente

$$\begin{array}{ccc} \mathbb{P}^n & \xrightarrow{\nu_{n,d}} & X_{n,d} \\ & \searrow^{\varphi\Omega_{n,d}} & \downarrow \pi \\ & & Y_{n,d} \end{array}$$

donde $\pi : X_{n,d} \to Y_{n,d}$ es la proyección de la variedad de Veronese $X_{n,d}$ desde el subespacio lineal generado por los puntos $(0 : \cdots : 0 : 1 : 0 \cdots : 0) \in \mathbb{P}^{N_{n,d}-1}$ que tienen 1 en la posición i-ésima para los índices i tales que $m_i \notin \Omega_{n,d}$, sobre el subespacio lineal $V(w_{m_i} : m_i \notin \Omega_{n,d}) \simeq \mathbb{P}^{\mu_{n,d}-1} \subset \mathbb{P}^{N_{n,d}-1}$. En términos de coordenadas, esta proyección lo que hace es eliminar las coordenadas correspondientes a los monomios de $\mathcal{M}_{n,d} \setminus \Omega_{n,d}$. En particular, diremos que $Y_{n,d} \subset \mathbb{P}^{\mu_{n,d}-1}$ es una *proyección monomial simple* (resp. *doble*) si $\Omega_{n,d}$ se obtiene a partir de $\mathcal{M}_{n,d}$ eliminando un único monomio (resp. dos monomios).

Como estas variedades están definidas paramétricamente por monomios, algunas de sus propiedades se pueden abordar desde el punto de vista de la combinatoria. Aplicando la proposición 1.5.7 tenemos que la dimensión del anillo $k[\Omega_{n,d}]$ es igual al rango de la matriz $\Lambda_{n,d}$ cuyas columnas son los exponentes de los monomios en Ω. Por lo tanto, es claro que la dimensión de la variedad $Y_{n,d}$ es

$$\dim(Y_{n,d}) = \dim\left(k[\Omega_{n,d}]\right) - 1 = \mathrm{rk}(\Lambda_{n,d}) - 1. \tag{1.5.1}$$

Por otra parte, el grado de $Y_{n,d}$ está determinado por el resultado siguiente:

Proposición 1.5.21 ([26, Thm. 2.13 & Thm. 4.5])**.** Sean $n, d \in \mathbb{N}$ números naturales y $\Omega_{n,d} = \{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_m}\} \subset \mathcal{M}_{n,d}$ un conjunto de monomios de grado d en $n+1$ variables. Si r denota el rango de la matriz $\Lambda_{n,d}$, entonces el grado de la proyección monomial $Y_{n,d}$ de la variedad de Veronese $X_{n,d}$ se puede calcular como

$$\deg(Y_{n,d}) = \frac{r! \cdot \operatorname{vol}(\operatorname{conv}(\{\alpha_1, \ldots, \alpha_m, 0\}))}{\Delta_r},$$

donde $\operatorname{vol}(\operatorname{conv}(\{\alpha_1, \ldots, \alpha_m, 0\}))$ denota el volumen de la envolvente convexa del conjunto $\{\alpha_1, \ldots, \alpha_m, 0\} \subset \mathbb{R}^n$ y Δ_r denota el máximo común divisor de todos los menores $r \times r$ de la matriz $\Lambda_{n,d}$.
Además, si $B = \operatorname{diag}(\beta_1, \ldots, \beta_r, 0, \ldots, 0)$ es la forma normal de Smith de $\Lambda_{n,d}$, entonces $\Delta_r = \beta_1 \ldots \beta_r$.

Capítulo 2

Combinatoria Aditiva. Sumas iteradas

Dados un (semi)grupo[1] abeliano $(G,+)$ y subconjuntos finitos no vacíos $A, B \subset G$, el *conjunto suma* $A+B$ se define de la manera siguiente

$$A+B=\{a+b : a \in A, b \in B\}.$$

Como es lógico, esto se puede definir de igual manera para s subconjuntos $A_1, \ldots, A_s \subset G$,

$$A_1+\cdots+A_s=\{a_1+\cdots+a_s : a_i \in A_i, 1 \leq i \leq s\}.$$

El caso más interesante se tiene cuando $A_i = A$ para cada $i = 1, \ldots, s$. En este caso, denotamos el conjunto $A_1+\cdots+A_s$ por sA,

$$\begin{aligned} sA &:= \{a_1+\cdots+a_s : a_i \in A, 1 \leq i \leq s\},\ s \in \mathbb{N}; \\ 0A &:= \{0\}. \end{aligned}$$

Los conjuntos sA, se denominan *sumas iteradas* del conjunto A o simplemente *conjuntos suma* de A.

Un problema central de la combinatoria aditiva se centra en entender el comportamiento de $|sA|$ cuando s crece. Como veremos en este capítulo, un resultado de Khovanskii asegura que la función $\mathbb{N}_0 \to \mathbb{N}_0$ definida por $s \mapsto |sA|$ toma los valores de un polinomio para s suficientemente grande, mientras que para valores de s pequeños, el comportamiento de $|sA|$ depende de la estructura (o la falta de estructura) del conjunto A.

El estudio de estas propiedades en los grupos abelianos se enmarca dentro de la combinatoria aditiva. Cuando $G = \mathbb{Z}$, la teoría aditiva de números se ocupa del estudio de los conjuntos suma.

[1]Para todo lo que vamos a exponer en este trabajo no necesitamos la existencia de inversos, por lo que podemos trabajar en cualquier semigrupo abeliano.

Este capítulo se organiza de la manera siguiente. En la sección 2.1 presentamos algunos resultados básicos de teoría aditiva de números, y en la sección 2.2 enunciamos uno de los teoremas más importantes en la combinatoria aditiva, el teorema de Khovanskii, y algunas de sus consecuencias. Posponemos la demostración de este teorema al capítulo 3.

La referencia principal para este capítulo es [25], aunque también incluiremos algunos resultados como el teorema de Khovanskii [20] y un resultado de Lev [21].

2.1. Teoría aditiva de números

La teoría aditiva de números estudia las sumas iteradas de los conjuntos finitos de número enteros $A \subset \mathbb{Z}$. En teoría aditiva de números existen dos tipos de problemas distintos.

- Un *problema directo* es aquel en el que el conjunto $A \subset \mathbb{Z}$ es conocido y tratamos de determinar propiedades sobre los conjuntos suma de A, sA. Un ejemplo clásico de problema directo es el teorema de Lagrange en teoría de números, que afirma que todo entero no negativo se puede escribir como suma de cuatro cuadrados perfectos. Es decir, si $A = \{n^2 : n \in \mathbb{Z}\}$, entonces $4A = \mathbb{N}_0$.
- Un *problema inverso* es aquel en el que se trata de deducir propiedades del conjunto A a partir de sus conjuntos suma, sA.

2.1.1. Algunos problemas directos

Sea $A \subset \mathbb{Z}$ un conjunto de números enteros con $|A| = n$ y denotamos sus elementos $a_0 < a_1 < \cdots < a_{n-1}$. Para estudiar los conjuntos de sumas de A, vamos a construir un nuevo conjunto $A^{(N)}$ más sencillo tal que los conjuntos de sumas de $A^{(N)}$ determinan los de A. La construcción simplemente consiste en desplazar y reescalar el conjunto A.

Construcción de la forma normal de A . Dado un conjunto $A = \{a_0 < a_1 < \cdots < a_{n-1}\} \subset \mathbb{Z}$, definimos

$$d(A) = \gcd(a_1 - a_0, a_2 - a_0, \ldots, a_{n-1} - a_0).$$

Para cada $i = 0, 1, \ldots, n-1$, denotamos $a_i' = (a_i - a_0)/d(A)$ y definimos

$$A^{(N)} = \{a_0', a_1', \ldots, a_{n-1}'\}.$$

Entonces tenemos que $0 = a_0' < a_1' < \cdots < a_{n-1}'$, $d\left(A^{(N)}\right) = \gcd(a_1', \ldots, a_{n-1}') = 1$ y $A = a_0 + d(A) \cdot A^{(N)}$. Por lo tanto,

$$sA = \{sa_0\} + d(A) \cdot sA^{(N)},$$

de donde se sigue que

$$|sA| = |sA^{(N)}|, \text{ para cada } s \in \mathbb{N}_0.$$

El conjunto $A^{(N)}$ que acabamos de construir se denomina la *forma normal de* A.

Definición 2.1.1. Dado un subconjunto finito $A = \{a_0 < a_1 < \cdots < a_{n-1}\} \subset \mathbb{Z}$, diremos que A está en forma normal si $a_0 = 0$ y se verifica $\gcd(a_1, \ldots, a_{n-1})$.

Ejemplo 2.1.2. Sea $A = \{8, 29, 71, 92\}$. En este caso, $d(A) = \gcd(21, 63, 84) = 21$, luego $A^{(N)} = \{0, 1, 3, 4\}$ es la forma normal de A. Por ejemplo, notemos que para $s = 2$, $2A^{(N)} = [0, 8]$ y $2A = \{16 + 21m : m \in [0, 8]\}$.

Observación 2.1.3. Una de las ventajas de tener un conjunto A en su forma normal es que $0 \in A$, luego los conjuntos suma están encajados, es decir, $sA \subset (s+1)A$ para todo $s \in \mathbb{N}_0$.

Lema 2.1.4 ([25, Lemma 1.1])**.** Sean $m \geq 2$, $a_1, \ldots, a_{n-1} \in \mathbb{N}$ tales que

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

y $s \in \mathbb{N}$. Si

$$(a_{n-1} - 1)\sum_{i=1}^{n-2} a_i \leq m \leq sa_{n-1} - (n-2)(a_{n-1} - 1)a_{n-1},$$

entonces existen $u_1, \ldots, u_{n-1} \in \mathbb{N}_0$ tales que

$$\begin{aligned} m &= u_1a_1 + \cdots + u_{n-1}a_{n-1}, \\ u_1 &+ \cdots + u_{n-1} \leq s. \end{aligned}$$

Dicho de otra forma, si $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1}\}$, entonces

$$\left[(a_{n-1} - 1)\sum_{i=1}^{n-2} a_i, sa_{n-1} - (n-2)(a_{n-1} - 1)a_{n-1}\right] \subset sA.$$

Demostración. Como $\gcd(a_1, \ldots, a_{n-1}) = 1$, por la identidad de Bézout existen enteros $x_1, \ldots, x_{n-1}$ tales que

$$m = x_1a_1 + \cdots + x_{n-1}a_{n-1}.$$

Para cada $i = 1, \ldots, n-2$, sea $u_i \in \mathbb{N}_0$ el menor entero no negativo congruente con x_i módulo a_{n-1}. Entonces

$$\begin{aligned} m &\equiv x_1a_1 + \cdots + x_{n-2}a_{n-2} \quad \text{mód } a_{n-1} \\ &\equiv u_1a_1 + \cdots + u_{n-2}a_{n-2} \quad \text{mód } a_{n-1}. \end{aligned}$$

Por lo tanto, existe un número entero u_{n-1} tal que

$$m = u_1a_1 + \cdots + u_{n-2}a_{n-2} + u_{n-1}a_{n-1}.$$

Veamos que $u_{n-1} \geq 0$ y $u_1 + \cdots + u_{n-1} \leq s$, lo que termina la prueba. Como $0 \leq u_i \leq a_{n-1} - 1$ para $i = 1, \ldots, n-2$, entonces

$$u_{n-1}a_{n-1} = m - (u_1a_1 + \cdots + u_{n-2}a_{n-2}) \geq m - (a_{n-1} - 1)\sum_{i=1}^{n-2} a_i \geq 0,$$

luego $u_{n-1} \geq 0$. De manera análoga,

$$u_{n-1}a_{n-1} \leq m \leq sa_{n-1} - (n-2)(a_{n-1}-1)a_{n-1}$$

y

$$u_{n-1} \leq s - (n-2)(a_{n-1}-1).$$

De aquí deducimos que

$$u_1 + \cdots + u_{n-2} + u_{n-1} \leq (n-2)(a_{n-1}-1) + u_{n-1} \leq s.$$

□

Teorema 2.1.5 (Teorema de estructura, [25, Thm. 1.1])**.** Sean $n \geq 2$ y $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1}\} \subset \mathbb{Z}$ un conjunto en forma normal. Entonces existen dos números $c_1, c_2 \in \mathbb{N}_0$ y conjuntos $C_i \subset [0, c_i - 2]$, $i = 1, 2$, tales que

$$sA = C_1 \sqcup [c_1, sa_{n-1} - c_2] \sqcup (sa_{n-1} - C_2) \tag{2.1.1}$$

para todo $s \geq \max\{1, s_0\}$, siendo $s_0 := (n-2)(a_{n-1}-1)a_{n-1}$.

Demostración. Notemos primero que, si probamos la existencia de los números c_1, c_2 y los conjuntos C_1, C_2, entonces la unión en (2.1.1) debe ser disjunta, puesto que $C_1 \subset [0, c_1 - 2]$ y $sa_{n-1} - C_2 \subset [sa_{n-1} - c_2 + 2, sa_{n-1}]$, y los tres intervalos $[0, c_1 - 2]$, $[c_1, sa_{n-1} - c_2]$ y $[sa_{n-1} - c_2 + 2, sa_{n-1}]$ son disjuntos dos a dos. Por lo tanto, nos preocupamos únicamente de demostrar la existencia de c_1, c_2, C_1, C_2 cumpliendo las condiciones del enunciado.
Si $n = 2$, entonces $a_1 = 1$, $A = \{0, 1\}$ y $sA = \{0, s\}$, por lo que el teorema se verifica para todo $s \geq 1$ tomando $c_1 = c_2 = 0$.
Supongamos que $n \geq 3$, entonces $a_{n-1} \geq 2$ y definimos

$$s_0 := (n-2)(a_{n-1}-1)a_{n-1}.$$

El resultado se prueba por inducción sobre $s \geq s_0$, pero antes veamos dos desigualdades que nos servirán más adelante en la prueba.
Como $a_1 + \cdots + a_{n-2} \leq (n-2)a_{n-2} < (n-2)a_{n-1}$, es claro que

$$s_0 \geq (a_{n-1}-1)\left(1 + \sum_{i=1}^{n-2} a_i\right) \tag{2.1.2}$$

y, teniendo en cuenta esto,

$$s_0 a_{n-1} \geq 2s_0 \overset{(2.1.2)}{\geq} (n-2)(a_{n-1}-1)a_{n-1} + a_{n-1} - 1 + (a_{n-1}-1)\sum_{i=1}^{n-2} a_i. \tag{2.1.3}$$

Para probar el caso $s = s_0$ notemos que, por el lema 2.1.4, el intervalo

$$I := \left[(a_{n-1}-1)\sum_{i=1}^{n-2} a_i, s_0 a_{n-1} - (n-2)(a_{n-1}-1)a_{n-1}\right] \subset s_0 A.$$

Por lo tanto, podemos considerar los enteros c_1 y c_2 tales que el intervalo $[c_1, s_0a_{n-1} - c_2]$ es el más grande que verifica

$$I \subset [c_1, s_0a_{n-1} - c_2] \subset s_0A. \tag{2.1.4}$$

Por la elección de c_1 y c_2, tenemos que $c_1 - 1 \notin s_0A$ y $s_0a_{n-1} - (c_2 - 1) \notin s_0A$. Además, de la primera contención en (2.1.4) deducimos que

$$c_1 \leq (a_{n-1} - 1)\sum_{i=1}^{n-2} a_i \overset{(2.1.2)}{<} s_0 \leq s \tag{2.1.5}$$

y

$$c_2 \leq (n-2)(a_{n-1} - 1)a_{n-1}. \tag{2.1.6}$$

Y de aquí se sigue que

$$\begin{aligned} c_1 + c_2 &\overset{(2.1.3)}{\leq} (a_{n-1} - 1)\sum_{i=1}^{n-2} a_i + (n-2)(a_{n-1} - 1)a_{n-1} \\ &\leq s_0a_{n-1} - a_{n-1} + 1, \end{aligned}$$

luego

$$[c_1, c_1 + a_{n-1} - 1] \subset [c_1, s_0a_{n-1} - c_2]. \tag{2.1.7}$$

Consideramos los conjuntos $C_1, C_2 \subset \mathbb{Z}$ definidos del siguiente modo

$$C_1 = s_0A \cap [0, c_1 - 2]$$

y

$$s_0a_{n-1} - C_2 = s_0A \cap [s_0a_{n-1} - (c_2 - 2), s_0a_{n-1}].$$

Entonces es claro que $C_2 \subset [0, c_2 - 2]$, pues para cada $d' \in C_2$ tenemos que

$$s_0a_{n-1} - (c_2 - 2) \leq s_0a_{n-1} - d' \leq s_0a_{n-1}.$$

Falta comprobar que se verifica (2.1.1) para s_0, es decir,

$$s_0A = C_1 \cup [c_1, s_0a_{n-1} - c_2] \cup (s_0a_{n-1} - C_2)\,.$$

Ya hemos visto que el conjunto de la derecha está contenido en el conjunto de la izquierda. Para probar la otra contención, sea $m \in s_0A$ un número natural y supongamos que $m \notin C_1 \cup [c_1, s_0a_{n-1} - c_2]$. Por lo tanto, tenemos $s_0a_{n-1} - (c_2 - 2) \leq m \leq s_0a_{n-1}$, luego $m \in s_0a_{n-1} - C_2$.

Paso inductivo: Supongamos ahora que la igualdad (2.1.1) se verifica para un cierto $s \geq s_0$ y veámoslo para $s + 1$ Denotamos

$$B := C_1 \cup [c_1, (s+1)a_{n-1} - c_2] \cup ((s+1)a_{n-1} - C_2)\,,$$

el lado derecho de la igualdad (2.1.1), y veamos que este conjunto es igual a A. Teniendo en cuenta (2.1.7), es claro que

$$B = C_1 \cup [c_1, c_1 + a_{n-1} - 1] \cup [c_1 + a_{n-1}, (s+1)a_{n-1} - c_2] \cup ((s+1)a_{n-1} - C_2)$$

$B \subset (s+1)A$: Como $0 \in A$, tenemos $s_0A \subset sA \subset (s+1)A$ y, por tanto,

$$C_1 \cup [c_1, c_1 + a_{n-1} - 1] \overset{(2.1.7)}{\subset} C_1 \cup [c_1, s_0a_{n-1} - c_2] \subset s_0A \subset (s+1)A.$$

Por otra parte, como $a_{n-1} \in A$, entonces $a_{n-1} + sA \subset (s+1)A$, luego

$$[c_1 + a_{n-1}, (s+1)a_{n-1} - c_2] \subset a_{n-1} + [c_1, sa_{n-1} - c_2].$$

Notemos que

$$[c_1, sa_{n-1} - c_2] = [c_1, s_0a_{n-1} - c_2] \cup [s_0a_{n-1} - c_2, sa_{n-1} - c_2] \subset sA,$$

de donde deducimos que

$$[c_1 + a_{n-1}, (s+1)a_{n-1} - c_2] \subset a_{n-1} + sA \subset (s+1)A.$$

De manera análoga,

$$(s+1)a_{n-1} - C_2 = a_{n-1} + (sa_{n-1} - C_2) \subset (s+1)A.$$

Por lo tanto, queda probado $B \subset (s+1)A$.
$(s+1)A \subset B$: Sea $b \in (s+1)A$. Hay tres posibilidades distintas para b:

- Si $b < c_1$, entonces por (2.1.5) tenemos que b no se puede escribir como la suma de $s+1$ elementos no nulos de A, luego $b \in sA$ y, por tanto, $b \in C_1 \subset B$.
- Si $c_1 \leq b \leq c_1 + a_{n-1} - 1$, entonces $b \in [c_1, c_1 + a_{n-1} - 1] \subset B$.
- Si $b \geq c_1 + a_{n-1}$, razonamos por reducción al absurdo. Supongamos que $b - a_{n-1} \notin sA$, entonces b es la suma de $s+1$ elementos de A que son estrictamente menores que a_{n-1}, luego

  $$b \leq (s+1)(a_{n-1} - 1). \tag{2.1.8}$$

  Recordemos que, por hipótesis de inducción, $[c_1, sa_{n-1} - c_2] \subset sA$ y, como estamos suponiendo que $b - a_{n-1} \geq c_1$ y $b - a_{n-1} \notin sA$, entonces $b - a_{n-1} \notin [c_1, sa_{n-1} - c_2]$, de donde deducimos que

  $$b - a_{n-1} > sa_{n-1} - c_2 \overset{(2.1.6)}{\geq} sa_{n-1} - (n-2)(a_{n-1} - 1)a_{n-1}. \tag{2.1.9}$$

  Juntando las desigualdades (2.1.8) y (2.1.9) obtenemos

  $$(s+1)a_{n-1} - (n-2)(a_{n-1} - 1)a_{n-1} < b \leq (s+1)(a_{n-1} - 1),$$

  luego

  $$s + 1 < (n-2)(a_{n-1} - 1)a_{n-1} = s_0 \leq s,$$

  lo que es absurdo. Por lo tanto, se debe verificar $b - a_{n-1} \in sA$. Aplicando la hipótesis de inducción, o bien

  $$b \in a_{n-1} + [c_1, sa_{n-1} - c_2] = [c_1 + a_{n-1}, (s+1)a_{n-1} - c_2] \subset B,$$

  o bien

  $$b \in a_{n-1} + (sa_{n-1} - C_2) = ((s+1)a_{n-1} - C_2) \subset B,$$

  de donde deducimos que $(s+1)A \subset B$.

□

Notación. En las condiciones del teorema de estructura, denotamos $\sigma(A)$, o simplemente σ, al menor número s a partir del cual se verifica la descomposición (2.1.1).

Observación 2.1.6.

(1) Es sencillo comprobar que

$$c_1 = 0 \Leftrightarrow a_1 = 1,$$
$$c_2 = 0 \Leftrightarrow a_{n-1} - a_{n-2} = 1.$$

(2) La prueba del teorema que hemos presentado aquí es la original del artículo de Nathanson [24]. Posteriormente, se han dado otras pruebas para este resultado en las que se mejora el valor del mínimo número $s_0^N := s_0$ (la N hace referencia a Nathanson) para el cual se tiene la descomposición (2.1.1). Estas cotas son:

- [31, Thm. 2] (Wu, Chen, Chen) $\sigma \leq \left(\sum_{i=2}^{n-1} a_i\right) - n + 1 =: s_0^{WCC}$.
- [14, Thm. 1] (Granville, Shakan) $\sigma \leq 2\lfloor \frac{a_{n-1}}{2} \rfloor =: s_0^{GS}$.
- [16, Thm. 1] (Granville, Walker) $\sigma \leq a_{n-1} - (n-2) = a_{n-1} - n + 2 =: s_0^{GW}$.

En la subsección 4.2.1 daremos una interpretación de la cota de Granville y Walker, relacionándola con la conjetura de Eisenbud-Goto.

(3) Si el conjunto $A = \{0 = a_0 < a_1 < \cdots < a_{n-1}\}$ es simétrico, es decir, si $A = a_{n-1} - A$, entonces $c_1 = c_2$. Esto es cierto porque si $A = a_{n-1} - A$, entonces $sA = sa_{n-1} - sA = s\,(a_{n-1} - A)$ para cada $s \in \mathbb{N}_0$.

(4) Si $A \subset \mathbb{Z}$ no está en forma normal, podemos aplicar el teorema 2.1.5 a la forma normal de A, $A^{(N)}$ y recuperar la estructura de los conjuntos suma de A teniendo en cuenta que $sA = \{sa_0\} + d(A) \cdot sA^{(N)}$.

Veamos cómo es la descomposición del teorema 2.1.5 en dos ejemplos concretos:

Ejemplo 2.1.7.

(a) Sea $A = \{0, 1, 3, 4\} \subset \mathbb{Z}$. Es inmediato comprobar que $sA = [0, 4s]$ para todo $s \geq 2$, luego $c_1 = c_2 = 0$ y el mínimo número s para el que se verifica el teorema 2.1.5 es $\sigma = 2$. Si calculamos las cotas que conocemos para σ, tenemos

$$s_0^N = 24,\ s_0^{WCC} = 5,\ s_0^{GS} = 4,\ s_0^{GW} = 2.$$

Observamos aquí que la cota de Nathanson para σ no es la mejor. De hecho, está muy alejada de serlo. En este caso concreto, se alcanza la cota de Granville y Walker.

(b) Sea $A = \{0, 2, 3, 5\} \subset \mathbb{Z}$. Siguiendo la demostración del teorema 2.1.5, consideramos $s_0 = 40$. Si calculamos $s_0 A$, obtenemos

$$40A = \{0\} \sqcup [2, 198] \sqcup \{200\}.$$

Elegimos c_1, c_2 tales que el intervalo $[c_1, 200 - c_2]$ sea el más grande entre los que verifican

$$[20, 160] \subset [c_1, 200 - c_2] \subset 40A.$$

De aquí, deducimos $c_1 = c_2 = 2$. En este caso, las distintas cotas para σ son

$$s_0^N = 40,\ s_0^{WCC} = 7,\ s_0^{GS} = 8,\ s_0^{GW} = 3.$$

De hecho, se puede comprobar fácilmente que $\sigma = 2$, por lo que

$$sA = \{0\} \sqcup [2, 5s - 2] \sqcup \{5s\},\ \text{para todo } s \geq 2.$$

Un resultado interesante que no vamos a probar es el siguiente teorema de V.F. Lev, que relaciona los cardinales de dos conjuntos suma de A consecutivos.

Teorema 2.1.8 ([21, Thm. 1])**.** Sea $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1}\} \subset \mathbb{N}_0$ un conjunto de cardinal $|A| = n \geq 2$ escrito en su forma normal. Para cada número natural $s \geq 2$ se verifica

$$|sA| \geq |(s-1)A| + \min\left(a_{n-1}, s(n-2) + 1\right).$$

Observación 2.1.9. Notemos que $a_{n-1} \leq s(n-2)+1$ si, y solo si, $s \geq \frac{a_{n-1}-1}{n-2}$. Si denotamos $s_0 := \lceil \frac{a_{n-1}-1}{n-2} \rceil$, entonces tenemos

$$|sA| - |(s-1)A| \geq \begin{cases} s(n-2)+1 & \text{si} \quad 0 \leq s \leq s_0 - 1 \\ a_{n-1} & \text{si} \quad s \geq s_0. \end{cases}$$

2.1.2. Algunos problemas inversos

Las progresiones aritméticas (finitas) aparecen con gran frecuencia en los resultados de teoría aditiva de números.

Definición 2.1.10. Dados 3 números $n, q \in \mathbb{N}$ y $a_0 \in \mathbb{Z}$, la *progresión aritmética* de longitud n con diferencia q y término inicial a_0 es el conjunto

$$\{a_0, a_0 + q, a_0 + 2q, \ldots, a_0 + (n-1)q\} = a_0 + q \cdot [0, n-1].$$

Mediante el siguiente resultado, podemos identificar cuándo un conjunto A es una progresión aritmética conociendo únicamente el conjunto suma $2A$. Esta es la filosofía de los problemas inversos, deducir propiedades del conjunto A a partir de propiedades de los conjuntos suma sA.

Teorema 2.1.11 ([25, Thm. 1.2])**.** Sea $A \subset \mathbb{Z}$ un conjunto de cardinal $|A| = n \in \mathbb{N}$, entonces $|2A| \geq 2n - 1$. Además, la cota inferior se alcanza únicamente en el caso en que A es una progresión aritmética.

Demostración. Escribimos $A = \{a_0 < a_1 < \cdots < a_{n-1}\}$. Entonces el conjunto suma $2A$ contiene los n enteros $2a_i$ para $i = 0, 1, \ldots, n-1$, y los $n-1$ enteros $a_{i+1} + a_i$ para $i = 1, \ldots, n-1$. Como

$$2a_{i-1} < a_{i-1} + a_i < 2a_i, \text{ para cada } i = 1, \ldots, n-1,$$

entonces se tiene $|2A| \geq 2n-1$.
Si $|2A| = 2n-1$, entonces todo elemento de $2A$ es de la forma $2a_i$ ó $a_{i-1} + a_i$. Como

$$a_{i-1} + a_i < a_{i-1} + a_{i+1} < a_i + a_{i+1}$$

y

$$a_{i-1} + a_i < 2a_i < a_i + a_{i+1}$$

para $i = 1, \ldots, n-2$, entonces se debe verificar

$$2a_i = a_{i-1} + a_{i+1}$$

o, equivalentemente,

$$a_i - a_{i-1} = a_{i+1} - a_i$$

para $i = 1, \ldots, n-2$, es decir, A es una progresión aritmética. □

A continuación presentamos dos cotas sencillas (una inferior y otra superior) para el cardinal de las sumas iteradas sA:

Teorema 2.1.12 ([25, Thm. 1.3], [28, Lemma 2.1])**.** Sean $s \geq 2$ y $A \subset \mathbb{Z}$ un conjunto de enteros con $|A| = n$. Entonces se verifica

$$sn - (s-1) \leq |sA| \leq \binom{n+s-1}{s}.$$

Demostración. Sin pérdida de generalidad, podemos suponer que A está en forma normal, es decir, $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1}\}$ y se verifica $\gcd(a_1, \ldots, a_{n-1}) = 1$.
Notemos que los elementos $(s-1)a_{n-1} + a_1, \ldots, (s-1)a_{n-1} + a_{n-1} \in sA \setminus (s-1)A$. Por lo tanto, $|sA| - |(s-1)A| \geq n-1$ y aplicando esto recursivamente obtenemos $|sA| \geq 1 + s(n-1) = sn - (s-1)$, lo que prueba la desigualdad de la izquierda.
Para probar la otra desigualdad, razonamos por inducción sobre n. Si $n = 1$, los dos lados de la desigualdad son iguales a 1. Supongamos $n > 1$, entonces podemos escribir $A = B \cup \{a_{n-1}\}$, donde $B = \{a_0 \ldots, a_{n-2}\}$ verifica $|B| = n-1 \geq 1$. Entonces tenemos

$$sA = \bigcup_{j=0}^{s} \left(jB + (s-j) \cdot a_{n-1}\right).$$

Ahora, aplicando la hipótesis de inducción a B y utilizando la identidad de Pascal tenemos

$$|sA| \leq \sum_{j=0}^{s} |jB| \leq \sum_{j=0}^{s} \binom{n-1+j-1}{j} = \binom{n+s-1}{s},$$

lo que completa la prueba. □

A continuación, presentamos dos resultados de problemas inversos que caracterizan de varias formas distintas cuándo un conjunto A es una progresión aritmética. No vamos a demostrar ahora estos dos teoremas, puesto que son consecuencia inmediata de un resultado del capítulo 4.

Teorema 2.1.13 ([25, Thm. 1.6])**.** Sean $s \geq 2$ y $A \subset \mathbb{Z}$ un conjunto finito de cardinal $|A| = n$. Entonces $|sA| = sn - (s-1)$ si, y solo si, A es una progresión aritmética de n términos.

Teorema 2.1.14 ([25, Thm. 1.8])**.** Sean $A \subset \mathbb{Z}$ un subconjunto finito con $|A| = n$ y $s \in \mathbb{N}_0 \mapsto o(s) \in \mathbb{N}_0$ una función aritmética tal que $\lim_{s\to\infty} o(s) = 0$. Si

$$|sA| = sn - (s-1) + o(s)$$

para infinitos valores de s, entonces A es una progresión aritmética de n términos.

Un resultado clásico de combinatoria aditiva es la desigualdad de Plünecke, que relaciona los cardinales de los conjuntos suma de A entre sí. Este resultado es general para cualquier subconjunto finito A de un grupo abeliano G.

Teorema 2.1.15 (Desigualdad de Plünecke, [25, Thm. 7.5])**.** Sean G un semigrupo abeliano, $A \subset G$ un subconjunto finito y $s \in \mathbb{N}$ un número natural. Entonces

$$|sA| \leq |iA|^{s/i} \text{ para cada } i = 1, \ldots, s. \tag{2.1.10}$$

Observación 2.1.16. El teorema 2.1.15 es equivalente al caso $i = s-1$, es decir,

$$|(s-1)A| \geq |sA|^{(s-1)/s}. \tag{2.1.11}$$

Esto es fácil de probar por inducción sobre $s - i$:

$$|iA| \overset{(2.1.11)}{\geq} |(i+1)A|^{i/(i+1)} \overset{(HI)}{\geq} \left(|sA|^{(i+1)/s}\right)^{i/(i+1)} = |sA|^{i/s}.$$

Existen varias pruebas de la desigualdad de Plünecke en la literatura. La más conocida es seguramente la que aparece en el libro de Nathanson [25], que se obtiene del estudio de los denominados *grafos de Plünecke*. No vamos a presentar en este trabajo dicha prueba, puesto que es demasiado extensa y se aleja de los objetivos planteados. No obstante, en el capítulo 3 obtendremos una desigualdad más fina que la de Plünecke usando herramientas de álgebra conmutativa.

2.2. Teorema de Khovanskii

Hasta ahora hemos considerado únicamente conjuntos finitos de números enteros $A \subset \mathbb{Z}$, vamos a situarnos ahora en un contexto más general. Sean $G = (G, +)$ un semigrupo abeliano y $A \subset G$ un subconjunto finito, nos interesamos ahora por las sumas iteradas (o conjuntos suma) de A.

Lo más elemental es comenzar preguntándose por el comportamiento del cardinal de las sumas iteradas de A, es decir, por $|sA|$, para cada $s \in \mathbb{N}_0$. Cuando $G = \mathbb{Z}$, del teorema 2.1.5 se deduce que $|sA|$ coincide con los valores de un polinomio de grado 1 con coeficientes enteros para s suficientemente grande. Khovanskii se dio cuenta de que esto se podía generalizar del siguiente modo para cualquier semigrupo abeliano G:

Teorema 2.2.1 (Khovanskii, [20, Thm. 1])**.** Sean G un semigrupo abeliano y $A \subset G$ un subconjunto finito de cardinal n. Entonces existe un polinomio $p_A(z) \in \mathbb{Q}[z]$ de grado menor o igual que n tal que $|sA| = p_A(s)$ para todo s suficientemente grande.

Notación. En los siguientes capítulos, denotaremos $n_0(A)$, o simplemente n_0 si no hay confusión, al mínimo número s a partir del cual se verifica $|sA| = p_A(s)$.

Este resultado de 1992 se puede considerar como el punto de partida de la conexión entre la combinatoria aditiva y el álgebra conmutativa. La prueba original de Khovanskii consistía en asociar al conjunto A un módulo graduado M_A sobre un cierto anillo de polinomios, de modo que los valores de la función de Hilbert de M_A coinciden con los cardinales de los conjuntos suma de A. Entonces, utilizando el teorema de Hilbert que garantiza la existencia del polinomio de Hilbert (teorema 1.4.5) se deduce el resultado. Posteriormente, se han dado otras pruebas más combinatorias de este resultado. En este trabajo, vamos a deducir el resultado también del teorema 1.4.5, pero utilizando la construcción de Eliahou y Mazumdar [11] del capítulo 3.

Aunque el teorema de Khovanskii es válido para cualquier semigrupo abeliano G, se obtienen resultados más prometedores cuando $G = \mathbb{Z}$ (teoría aditiva de números) o cuando $G = \mathbb{Z}^d$, para algún $d \in \mathbb{N}$. En el propio artículo de Khovanskii aparecen resultados en esta línea.

Dados $d \in \mathbb{N}$ y un subconjunto finito $A \subset \mathbb{Z}^d$, denotamos $\mathbb{Z}(A - A)$ el subgrupo de $\mathbb{Z}^d$ que genera el conjunto $A - A$ y $\Delta_A = \operatorname{conv}(A)$ la envolvente convexa del conjunto A en $\mathbb{R}^d$. Entonces podemos describir el coeficiente líder de p_A en términos de estos dos elementos:

Teorema 2.2.2 ([20, Thm. 3 & Cor. 2])**.** Sean $A \subset \mathbb{Z}^d$ un subconjunto finito y supongamos que el subgrupo $\mathbb{Z}(A - A)$ tiene índice finito en $\mathbb{Z}^d$. Si $[\mathbb{Z}^d : \mathbb{Z}(A - A)]$ denota el índice de este subgrupo, entonces el coeficiente líder del polinomio p_A en el teorema de Khovanskii es

$$\frac{\operatorname{vol}(\Delta_A)}{[\mathbb{Z}^d : \mathbb{Z}(A - A)]},$$

donde $\operatorname{vol}(\Delta_A)$ denota el volumen de $\Delta_A = \operatorname{conv}(A)$ en $\mathbb{R}^d$.

También podemos encontrar en la bibliografía cotas para el número $n_0(A)$, como la que presentamos a continuación.

Definición 2.2.3. Dado un subconjunto finito $A \subset \mathbb{Z}^d$, la *anchura* de A es el número

$$w(A) := \max_{\mathbf{a}_1, \mathbf{a}_2 \in A} \|\mathbf{a}_1 - \mathbf{a}_2\|_\infty,$$

donde $\| \cdot \|_\infty$ denota la norma infinito de $\mathbb{R}^d$.

Teorema 2.2.4 ([15, Thm. 1.1])**.** Si $A \subset \mathbb{Z}^d$ es un subconjunto finito, entonces

$$|sA| = p_A(s), \text{ para todo } s \geq (2|A| \cdot w(A))^{(d+4)|A|}.$$

Es decir, $n_0(A) \leq (2|A| \cdot w(A))^{(d+4)|A|}$.

El teorema siguiente muestra el comportamiento de la función $s \mapsto |sA|$ cuando A tiene cardinal $d+2$. Este resultado lo obtendremos en el capítulo 5 de una manera sencilla.

Teorema 2.2.5 ([6, Thm. 1.2])**.** Sea $A \subset \mathbb{Z}^d$ un conjunto de cardinal $|A| = d+2$ tal que $\mathbb{Z}(A-A) = \mathbb{Z}^d$ y denotamos Δ_A la envolvente convexa de A en $\mathbb{R}^d$. Entonces

$$|sA| = \begin{cases} \binom{s+d+1}{d+1}, & \text{si} \quad 0 \leq s < \mathrm{vol}(\Delta_A) \cdot d! - d - 1 \\ \binom{s+d+1}{d+1} - \binom{s-\mathrm{vol}(\Delta_A)\cdot d! + d + 1}{d+1}, & \text{si} \quad s \geq \mathrm{vol}(\Delta_A) \cdot d! - d - 1. \end{cases}$$

Hemos tratado los casos $G = \mathbb{Z}$ y $G = \mathbb{Z}^d$ pero no nos hemos preocupado por el caso en que G es un grupo finito (aquí sí que exigimos que sea un grupo). En este caso todo es muy sencillo: si $A \subset G$ es un subconjunto de G, entonces para todo s suficientemente grande se tiene que

$$sA = sa + \langle A - A \rangle,$$

donde $a \in A$ es cualquier elemento de A y $\langle A - A \rangle$ denota el subgrupo de G generado por el conjunto $A - A = \{a_1 - a_2 : a_1, a_2 \in A\}$. Por lo tanto, la función $s \mapsto |sA|$ es eventualmente constante, es decir, el polinomio p_A en el teorema de Khovanskii es constante.

Parte II

Interacciones

Capítulo 3

Conjuntos suma y función de Hilbert

El teorema de Khovanskii (1992) supuso el inicio de la interacción entre la combinatoria aditiva y el álgebra conmutativa. No obstante, esta interacción no se volvió a explorar hasta 2018, cuando Eliahou utilizó el teorema de Macaulay en 2022, en el artículo [11] conjunto con Mazumdar.

En este capítulo, presentamos la construcción de Eliahou y Mazumdar [11], que consiste en asociar una k-álgebra graduada estándar a cada subconjunto $A \subset G$ finito de un semigrupo conmutativo G (sección 3.1). Posteriormente, en la sección 3.2 caracterizamos la k-álgebra $R(A)$, identificándola con el cociente de un anillo de polinomios por un ideal homogéneo. Por último, en la sección 3.3 aplicamos el teorema de Macaulay a esta k-álgebra, de donde obtendremos la desigualdad de Plünecke (de hecho, obtendremos una desigualdad más fina).

Las referencias empleadas en este capítulo son [10] y [11].

3.1. Construcción de la k-álgebra $R(A)$

Sean $(G, +)$ un semigrupo conmutativo y $A \subset G$ un subconjunto finito. Queremos asociar al conjunto A una k-álgebra graduada estándar, que denotaremos $R(A)$, cuya función de Hilbert tome los mismos valores que la sucesión $|sA|$ para $s \in \mathbb{N}_0$.

Consideramos la k-álgebra del semigrupo G, $k[G]$, que está generada como k-espacio vectorial por el conjunto $\{t^g : g \in G\}$, y está provista del producto

$$t^{g_1} \cdot t^{g_2} := t^{g_1+g_2}, \forall g_1, g_2 \in G.$$

Ahora consideramos $S = k[G][w]$, el álgebra de polinomios en la variable w con coeficientes en $k[G]$. Una base de S como k-espacio vectorial es

$$\mathcal{B} = \{t^g w^n : g \in G, n \in \mathbb{N}_0\},$$

y el producto de dos elementos de la base está dado por

$$t^{g_1} w^{n_1} \cdot t^{g_2} w^{n_2} = t^{g_1+g_2} w^{n_1+n_2}, \forall g_1, g_2 \in G, \forall n_1, n_2 \in \mathbb{N}_0.$$

Para cada elemento de la base $\mathcal{B}$, definimos su grado de la forma usual, $\deg(t^g w^n) = n$, de modo que

$$\deg\left(\sum_{j=1}^{m} t^{g_j} w^{n_j}\right) = \max\{n_j : 1 \leq j \leq m\}.$$

Esto nos permite dotar a S de una estructura de álgebra graduada, $S = \oplus_{i\in\mathbb{N}_0} S_i$, siendo S_i el k-espacio vectorial generado por $\{t^g w^i : g \in G\}$.

Definición 3.1.1. Sean G un semigrupo conmutativo y $A = \{a_0, \ldots, a_{n-1}\} \subset G$ un subconjunto no vacío. Definimos $R(A)$ como la k-subálgebra de S generada por el conjunto $\{t^{a_0}w, \ldots, t^{a_{n-1}}w\}$, es decir,

$$R(A) := k[t^{a_0}w, \ldots, t^{a_{n-1}}w] \subset S,$$

considerando las variables con grados $\deg(t) = 0$ y $\deg(w) = 1$.

Teorema 3.1.2. *$R(A)$ es una k-álgebra graduada estándar que verifica $\mathrm{HF}_{R(A)}(s) = |sA|$ para todo $s \geq 0$.*

Demostración. La k-álgebra $R(A)$ verifica $R(A) = \oplus_{s\geq 0} R(A)_s$, donde para cada $s \in \mathbb{N}_0$, $R(A)_s$ es el k-espacio vectorial generado por el conjunto $\{t^b w^s : b \in sA\}$, que es linealmente independiente sobre k. Por lo tanto,

$$\mathrm{HF}_{R(A)}(s) = \dim R(A)_s = |sA|, \ \forall s \geq 0.$$

Además, $R(A)$ está generada como k-álgebra por elementos de grado 1, luego es una k-álgebra graduada estándar. □

Como en el capítulo 4 nos vamos a centrar en el caso $G = \mathbb{Z}$, nos interesa ver qué aspecto adquiere la k-álgebra $R(A)$ en esta situación.

Observación 3.1.3. Supongamos que $A \subset \mathbb{N}_0$ es un conjunto en forma normal, es decir, $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1}\}$ con $\gcd(a_1, \ldots, a_{n-1}) = 1$. En este caso tenemos $k[G] = k[\mathbb{N}_0] = k[t]$, la k-álgebra de polinomios en la variable t. Por lo tanto, $R(A) = k[w, t^{a_1}w, \ldots, t^{a_{n-1}}w]$ es la k-subálgebra de $k[t, w]$ generada por el conjunto $\{w, t^{a_1}w, \ldots, t^{a_{n-1}}w\}$, donde estamos considerando las variables con grados $\deg(t) = 0$, $\deg(w) = 1$.

La construcción de Eliahou y Mazumdar nos permite dar una prueba elegante y sencilla del teorema de Khovanskii.

Demostración del teorema de Khovanskii (teorema 2.2.1). Sea $A \subset G$ un subconjunto finito de un semigrupo abeliano G. Consideramos la k-álgebra graduada estándar $R(A)$ asociada al conjunto A, que verifica $|sA| = \mathrm{HF}_{R(A)}(s)$ para cada $s \in \mathbb{N}_0$. Entonces el resultado se deduce del teorema 1.4.5 (Hilbert). □

3.2. Caracterización de la k-álgebra $R(A)$

Dados un semigrupo abeliano $(G,+)$ y un subconjunto finito $A \subset G$, hemos asociado al conjunto A una k-álgebra graduada estándar, $R(A)$. El objetivo de esta sección es identificar esta k-álgebra con un cociente del álgebra de polinomios $S = k[x_0, x_1, \ldots, x_{n-1}]$ por un ideal homogéneo I.

Sea $\varphi : k[x_0, \ldots, x_{n-1}] \to R(A)$ el morfismo de k-álgebras dado por $\varphi(x_i) = t^{a_i}w$, $i = 0, \ldots, n-1$, que es graduado (de grado 0) y sobreyectivo. Por lo tanto, existe un isomorfismo de k-álgebras graduadas $R(A) \simeq k[x_0, \ldots, x_{n-1}]/\ker\varphi$. Entonces lo que nos falta es encontrar un sistema de generadores del ideal $\ker\varphi$.

Sea $\mathcal{M} = \{\mathbf{x}^\alpha : \alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{N}_0^n\}$ el conjunto de todos los monomios de $k[x_0, \ldots, x_{n-1}]$. Definimos en $\mathcal{M}$ la relación de equivalencia siguiente

$$\mathbf{x}^\alpha \sim \mathbf{x}^\beta \Leftrightarrow \varphi(\mathbf{x}^\alpha) = \varphi(\mathbf{x}^\beta).$$

Equivalentemente, esto es lo mismo que decir

$$\mathbf{x}^\alpha \sim \mathbf{x}^\beta \Leftrightarrow \begin{cases} \sum_{i=0}^{n-1} \alpha_i = \sum_{i=0}^{n-1} \beta_i \\ \sum_{i=0}^{n-1} \alpha_i a_i = \sum_{i=0}^{n-1} \beta_i a_i. \end{cases} \tag{3.2.1}$$

En particular, dos monomios equivalentes tienen necesariamente el mismo grado.

Definición 3.2.1. Sea $f \in k[x_0, \ldots, x_{n-1}]$ un polinomio. Diremos que f es *simple* si $f \neq 0$ y para cada par de monomios $\mathbf{x}^\alpha, \mathbf{x}^\beta$ que aparecen en f, se tiene $\mathbf{x}^\alpha \sim \mathbf{x}^\beta$.

Observación 3.2.2. Todo polinomio simple es homogéneo. Además, cualquier polinomio no nulo $g \in k[x_0, \ldots, x_{n-1}]$ se puede escribir de forma única como suma de polinomios simples $g = f_1 + \cdots + f_r$ de modo que si $1 \leq i < j \leq r$, entonces los monomios que aparecen en f_i no son equivalentes a los que aparecen en f_j. Llamaremos a estos polinomios las *componentes simples* de f.

Lema 3.2.3 ([11, Lemma 6.3])**.** Sea $g \in k[x_0, \ldots, x_{n-1}]$ un polinomio no nulo tal que $g \in \ker\varphi$. Entonces toda componente simple de g pertenece al núcleo de φ.

Demostración. Sea f una componente simple de g, veamos que $\varphi(f) = 0$. Como f es simple, es un polinomio homogéneo, y denotamos $d = \deg(f)$ a su grado. Escribimos $f = \sum_{i=1}^m \lambda_i \mathbf{x}^{\alpha_i}$, donde $\lambda_i \in k^*$, $\alpha_i \in \mathbb{N}_0^n$ para todo $i = 1, \ldots, m$ y además los monomios $\mathbf{x}^{\alpha_i}$ son distintos dos a dos. Por hipótesis, $\mathbf{x}^{\alpha_i} \sim \mathbf{x}^{\alpha_j}$ para todo $i, j = 1, \ldots, m$, luego existen un cierto $s \in \mathbb{N}$ y $b \in sA$ (que no dependen de i) tales que $\varphi(\mathbf{x}^{\alpha_i}) = t^b w^s$ para todo $i = 1, \ldots, m$. Por lo tanto,

$$\varphi(f) = \sum_{i=1}^m \lambda_i t^b w^s = \left(\sum_{i=1}^m \lambda_i\right) t^b w^s.$$

Ahora, notemos que para cada monomio $\mathbf{x}^\beta \in \mathcal{M}$ que aparece en g pero no en f tenemos $\varphi(\mathbf{x}^\beta) \neq t^b w^s$, puesto que $\mathbf{x}^\beta \not\sim \mathbf{x}^{\alpha_i}$. Por lo tanto, del hecho $\varphi(g) = 0$ deducimos $\sum_{i=1}^m \lambda_i = 0$, es decir, $\varphi(f) = 0$. □

Proposición 3.2.4 ([11, Prop. 6.4])**.** Si $I \subset k[x_0, \ldots, x_{n-1}]$ es el ideal definido por $I = \langle \mathbf{x}^\alpha - \mathbf{x}^\beta : \mathbf{x}^\alpha, \mathbf{x}^\beta \in \mathcal{M}, \mathbf{x}^\alpha \sim \mathbf{x}^\beta \rangle$, entonces $\ker \varphi = I$.

Demostración. Está claro que $I \subset \ker \varphi$, por lo que basta probar la otra inclusión. Sea $f \in \ker \varphi$, $f \neq 0$ y veamos que $f \in I$. Por el lema 3.2.3, podemos suponer que f es simple. Por lo tanto, podemos escribir $f = \sum_{i=1}^m \lambda_i \mathbf{x}^{\alpha_i}$, donde $\lambda_i \in k^*$, $\alpha_i \in \mathbb{N}_0^n$ para cada $i = 1, \ldots, m$ y los monomios $\mathbf{x}^{\alpha_i}$ son distintos dos a dos. Como $\varphi(\mathbf{x}^{\alpha_i}) = \varphi(\mathbf{x}^{\alpha_j})$ para cada par de índices $i, j = 1, \ldots, m$, entonces

$$\varphi(f) = \left(\sum_{i=1}^m \lambda_i \right) \varphi(\mathbf{x}^{\alpha_1}),$$

luego $\sum_{i=1}^m \lambda_i = 0$. De aquí deducimos que $\lambda_m = -\sum_{i=1}^{m-1} \lambda_i$ y, por tanto,

$$f = \sum_{i=1}^{m-1} \lambda_i (\mathbf{x}^{\alpha_i} - \mathbf{x}^{\alpha_m}) \in I.$$

□

Corolario 3.2.5 ([11, Cor. 6.5])**.** Usando las notaciones de la proposición anterior, existe un isomorfismo de k-álgebras graduadas $R(A) \simeq k[x_0, \ldots, x_{n-1}]/I$.

De nuevo, nos preocupamos por el caso particular $G = \mathbb{Z}$ que trataremos en el capítulo 4.

Observación 3.2.6. Cuando $A = \{a_0 < a_1 < \cdots < a_{n-1}\} \subset \mathbb{Z}$, podemos dar una descripción sencilla del ideal I que define la k-álgebra $R(A)$. En este caso, la relación de equivalencia (3.2.1) se traduce en

$$\mathbf{x}^\alpha \sim \mathbf{x}^\beta \Leftrightarrow \begin{cases} |\alpha| = |\beta| \\ |\alpha|_A = |\beta|_A, \end{cases} \tag{3.2.2}$$

donde $|\alpha| = \sum_{i=0}^{n-1} \alpha_i$ denota el grado usual del monomio $\mathbf{x}^\alpha$ y $|\alpha|_A = \sum_{i=0}^{n-1} = \alpha_i a_i$ denota el grado del monomio $\mathbf{x}^\alpha$ pesado por el vector $(a_0, a_1, \ldots, a_{n-1})$.

3.3. Generalización de la desigualdad de Plünecke

En esta sección vamos a utilizar el teorema de Macaulay (teorema 1.4.13) para demostrar la desigualdad de Plünecke (teorema 2.1.15). De hecho, vamos a probar una desigualdad más fina que la de Plünecke.

Comenzamos dando una versión un poco distinta del teorema de Macaulay, que Eliahou denomina "versión condensada del teorema de Macaulay" en [10]. Dados $m \in \mathbb{N}$ y $x \in \mathbb{R}$, denotamos

$$\binom{x}{m} = \frac{x(x-1)\ldots(x-m+1)}{m!} = \prod_{i=0}^{m-1} \frac{x-i}{m-i}.$$

Además, denotamos $\binom{x}{0} = 1$ para todo $x \in \mathbb{R}$.

Lema 3.3.1 ([10, Lemma 5.6])**.** Sea $i \in \mathbb{N}$. Entonces la aplicación $y \mapsto \binom{y}{i}$ es una biyección continua y creciente (de hecho, es un homeomorfismo) del intervalo $[i-1, \infty)$ en $[0, \infty)$. En particular, para cada par de números reales $y_1, y_2 \geq i-1$, se verifica

$$y_1 \leq y_2 \Leftrightarrow \binom{y_1}{i} \leq \binom{y_2}{i}. \tag{3.3.1}$$

Demostración. Consideramos la función polinómica dada por $f(z) = z(z-1)\dots(z-i+1)$. Por el teorema de Rolle, para cada $j = 1, \dots, i-1$ existe un número λ_j tal que $j-1 < \lambda_j < j$ y de modo que $f'(z) = i(z-\lambda_1)\dots(z-\lambda_{i-1})$. Por lo tanto, es claro que f es estrictamente creciente en $[i-1, \infty)$, lo que nos permite concluir el resultado. □

Lema 3.3.2 ([11, Lemma 3.6])**.** Sean $s, d \geq 1$, entonces existe un único número real $x \geq s$ tal que $d = \binom{x}{s}$.

Demostración. Por el lema 3.3.1, existe un único número real $x \geq s-1$ tal que $d = \binom{x}{s}$. Como $d \geq 1$, entonces $\binom{x}{s} \geq \binom{s}{s}$, y aplicando la equivalencia (3.3.1) deducimos $x \geq s$. □

Lema 3.3.3 ([10, Lemma 5.7])**.** Sean $r \geq 2$ un número entero y $u \geq v \geq w$ números reales tales que $v \geq r-1$ y $w \geq r-2$. Si $\binom{u}{r} = \binom{v}{r} + \binom{w}{r-1}$, entonces $\binom{u}{r-1} \leq \binom{v}{r-1} + \binom{w}{r-2}$.

Proposición 3.3.4 ([10, Prop. 5.8])**.** Sean $r \in \mathbb{N}$ un número natural y $u \geq v \geq w$ números reales tales que $v \geq r$ y $w \geq r-1$. Si $\binom{u}{r} = \binom{v}{r} + \binom{w}{r-1}$, entonces $\binom{u+1}{r+1} \geq \binom{v+1}{r+1} + \binom{w+1}{r}$.

Demostración. Veamos primero que se verifica lo siguiente

$$\binom{u}{r+1} \geq \binom{v}{r+1} + \binom{w}{r}. \tag{3.3.2}$$

Supongamos que no se verifica la desigualdad (3.3.2), es decir, que el lado izquierdo es estrictamente menor que el lado derecho. Por el lema 3.3.1, existe un número $z > u$ tal que

$$\binom{u}{r+1} < \binom{z}{r+1} = \binom{v}{r+1} + \binom{w}{r}.$$

Entonces, aplicando el lema 3.3.3, se tiene

$$\binom{z}{r} \leq \binom{v}{r} + \binom{w}{r-1},$$

lo que es absurdo, puesto que el lado derecho de la fórmula es igual a $\binom{u}{r}$ por hipótesis y $z > u$. Ahora, sumando $\binom{u}{r}$ en (3.3.2) y aplicando la hipótesis del enunciado obtenemos lo siguiente:

$$\binom{u+1}{r+1} = \binom{u}{r+1} + \binom{u}{r} \geq \binom{v}{r+1} + \binom{w}{r} + \binom{v}{r} + \binom{w}{r-1} = \binom{v+1}{r+1} + \binom{w+1}{r}.$$

□

Proposición 3.3.5 ([10, Thm. 5.9])**.** Sean $d \in \mathbb{N}_0$, $s \in \mathbb{N}$, y sea $x \geq s$ el único número real tal que $d = \binom{x}{s}$. Entonces $d^{\langle s \rangle} \leq \binom{x+1}{s+1}$.

Demostración. Lo demostramos por inducción sobre s. Si $s = 1$, entonces tenemos $x = d$ y el resultado se deduce de la propia definición. Sea $s \geq 2$ y supongamos que el resultado es cierto para $s - 1$. Consideramos la s-ésima representación binomial de d:

$$d = \sum_{i=1}^{s} \binom{d_i}{i} = \binom{d_s}{s} + b, \text{ donde } b = \sum_{i=1}^{s-1} \binom{d_i}{i}.$$

Entonces tenemos

$$d^{\langle s \rangle} = \binom{d_s + 1}{s + 1} + b^{\langle s-1 \rangle}.$$

Sea $y \geq s - 1$ el único número real tal que $b = \binom{y}{s-1}$. Entonces

$$d = \binom{x}{s} = \binom{d_s}{s} + \binom{y}{s-1}. \tag{3.3.3}$$

Por hipótesis de inducción, tenemos que $b^{\langle s-1 \rangle} \leq \binom{y+1}{s}$, y de ahí deducimos que

$$d^{\langle s \rangle} \leq \binom{a_s + 1}{s + 1} + \binom{y + 1}{s}.$$

A partir de (3.3.3) y la proposición 3.3.4 se sigue que

$$\binom{x + 1}{s + 1} \geq \binom{a_s + 1}{s + 1} + \binom{y + 1}{s},$$

lo que concluye la prueba. □

Aplicando el teorema de Macaulay a la k-álgebra $R(A)$ obtenemos el siguiente resultado sobre los conjuntos suma de A.

Teorema 3.3.6 (Teorema de Macaulay, versión condensada, [10, Thm. 5.10])**.**
Sea $R = \oplus_{i \in \mathbb{N}_0} R_i$ una k-álgebra graduada estándar con función de Hilbert dada por $h_i = \mathrm{HF}_R(i)$ para cada $i \in \mathbb{N}_0$. Sea $s \in \mathbb{N}$, y consideramos $x \geq s$ el único número real tal que $h_s = \binom{x}{s}$. Entonces

$$h_{s-1} \geq \binom{x - 1}{s - 1} \text{ y } h_{s+1} \leq \binom{x + 1}{s + 1}.$$

Demostración. Sea $d = h_s$. Por el teorema de Macaulay (teorema 1.4.13) y la proposición 3.3.5, tenemos que $h_{s+1} \leq d^{\langle s \rangle} \leq \binom{x+1}{s+1}$. Para probar la otra desigualdad razonamos por reducción al absurdo. Supongamos que

$$h_{s-1} < \binom{x - 1}{s - 1}.$$

Sea $y \geq s-1$ el único número real tal que $h_{s-1} = \binom{y}{s-1}$. Entonces del lema 3.3.1 se deduce que $y < x-1$. Por lo tanto, aplicando la parte que ya hemos demostrado de este teorema tenemos

$$h_s \leq \binom{y+1}{s} < \binom{x}{s},$$

lo que es absurdo. □

Teorema 3.3.7 ([11, Thm. 4.3])**.** Sean A un subconjunto no vacío de un semigrupo abeliano G y $s \in \mathbb{N}$ un número natural. Entonces

$$|(s+1)A| \leq |sA|^{\langle s \rangle}.$$

Demostración. Sea $R(A)$ la k-álgebra graduada estándar asociada al conjunto A. Entonces tenemos $\mathrm{HF}_{R(A)}(i) = |iA|$ para cada $i \in \mathbb{N}_0$. Aplicando el teorema 1.4.13 (Macaulay) obtenemos la desigualdad del enunciado. □

Si ahora utilizamos la versión condensada del teorema de Macaulay (teorema 3.3.6), podemos obtener una desigualdad mejor que la de Plünecke (2.1.10).

Teorema 3.3.8 ([11, Thm. 4.4])**.** Sean G un semigrupo conmutativo y $A \subset G$ un subconjunto no vacío. Sea $s \geq 2$ un entero y $x \geq s$ el único número real tal que $|sA| = \binom{x}{s}$. Entonces se verifica

$$|(s-1)A| \geq \binom{x-1}{s-1} \text{ y } |(s+1)A| \leq \binom{x+1}{s+1}.$$

Demostración. Sea $R(A)$ la k-álgebra graduada estándar asociada al conjunto A. Entonces tenemos $\mathrm{HF}_{R(A)}(i) = |iA|$ para cada $i \in \mathbb{N}_0$. Aplicando la versión condensada del teorema de Macaulay (teorema 3.3.6) se deduce el resultado. □

Observación 3.3.9. Notemos que la cota superior del teorema 3.3.8 es más débil que la del teorema 3.3.7. Esto se obtiene directamente de la proposición 3.3.5.

Finalmente, estamos en condiciones de demostrar la desigualdad de Plünecke a partir del teorema de Macaulay, para eso utilizaremos la versión que hemos obtenido en el teorema 3.3.8.

Notación. Dados un número $s \in \mathbb{N}$ y un número real $x \geq s$, denotamos

$$\theta(x,s) = \frac{s}{x}\binom{x}{s}^{1/s}.$$

Teorema 3.3.10 ([11, Thm. 4.9])**.** Sean G un grupo abeliano, $A \subset G$ un subconjunto no vacío, y un número natural $s \geq 2$. Entonces

$$|(s-1)A| \geq \theta(x,s)|sA|^{(s-1)/s},$$

donde $x \in \mathbb{R}$ es el único número real que verifica $x \geq s$ y $|sA| = \binom{x}{s}$.

Demostración. Por el teorema 3.3.8 tenemos

$$|(s-1)A| \geq \binom{x-1}{s-1}. \tag{3.3.4}$$

Teniendo en cuenta que

$$\binom{x}{s} = \prod_{i=0}^{s-1} \frac{x-i}{s-i} = \frac{x}{s} \prod_{i=1}^{s-1} \frac{x-i}{s-i} = \frac{x}{s}\binom{x-1}{s-1}$$

obtenemos

$$\binom{x-1}{s-1} = \frac{s}{x}\binom{x}{s}. \tag{3.3.5}$$

Juntando las ecuaciones (3.3.4) y (3.3.5),

$$\begin{aligned} |(s-1)A|^s &\geq \binom{x-1}{s-1}^s = \left(\frac{s}{x}\right)^s \binom{x}{s}^s \\ &= \left(\frac{s}{x}\right)^s \binom{x}{s}\binom{x}{s}^{s-1} = \left(\frac{s}{x}\right)^s \binom{x}{s}|sA|^{s-1}, \end{aligned}$$

de donde se deduce el resultado de forma inmediata. □

Corolario 3.3.11 ([11, Cor. 4.10])**.** El teorema 3.3.8 implica la desigualdad de Plünecke (teorema 2.1.15).

Demostración. Utilizando el teorema 3.3.10, lo único que tenemos que demostrar es que $\theta(x,s) \geq 1$ o, lo que es lo mismo, $\theta(x,s)^s \geq 1$. Para ello, notemos que

$$\theta(x,s)^s = \left(\frac{s}{x}\right)^s \binom{x}{s} = \prod_{i=0}^{s-1} \frac{s(x-i)}{x(s-i)}, \tag{3.3.6}$$

y en cada uno de los términos del producto se verifica que el numerador es mayor o igual que el denominador, pues $s \leq x$. □

Observación 3.3.12. De hecho, si $s \geq 2$ y $|sA| \geq 2$, entonces $\theta(x,s) > 1$. Esto es porque como $|sA| = \binom{x}{s} \geq 2$, entonces $x > s$, luego $s(x-1) > x(s-1)$ y aplicando (3.3.6) deducimos que $\theta(x,s)^s > 1$.

Recapitulando, dado un semigrupo abeliano G y un subconjunto finito $A \subset G$, lo primero que hemos hecho ha sido asociar al conjunto A una k-álgebra graduada estándar que denotamos $R(A)$. Aplicando el teorema de Macaulay clásico y la versión condensada del teorema de Macaulay, hemos obtenido la cota

$$|(s-1)A| \geq \theta(x,s)|sA|^{(s-1)/s},$$

donde $\theta(x,s) \in \mathbb{R}$ es un número real mayor o igual que 1. Por lo tanto, esta desigualdad implica la de Plünecke y, de hecho, es más fina.

En [11, §5] se estudia el comportamiento de la función $\theta(x,s)$. Para terminar este capítulo, presentamos una acotación para $\theta(x,s)$ cuando $x > s \geq 2$.

Proposición 3.3.13 ([11, Prop. 5.1])**.** Sean $s \in \mathbb{N}$ y $x \in \mathbb{R}$ tales que $x > s \geq 2$. Entonces se verifica

$$1 < \theta(x, s) < e.$$

Demostración. La cota inferior se deduce de (3.3.6) y la observación 3.3.12. Para la cota superior, notemos que

$$\binom{x}{s} \leq \frac{x^s}{s!} = \frac{x^s}{s^s}\frac{s^s}{s!} < \frac{x^s}{s^s}e^s,$$

puesto que $\frac{s^s}{s!} < \sum_{j=0}^{\infty} \frac{s^j}{j!} = e^s$. De la desigualdad anterior se sigue que

$$\theta(x, s) = \frac{s}{x}\binom{x}{s}^{1/s} < \frac{s}{x}\frac{x}{s}e = e.$$

□

Por otra parte, utilizando la aproximación de Stirling se puede probar fácilmente que para $s \geq 2$ fijo,

$$\lim_{x\to\infty} \theta(x, s) = (2\pi s)^{-1/(2s)}e.$$

En particular, comprobamos cómo el álgebra conmutativa permite recuperar y mejorar algunos resultados clásicos de combinatoria aditiva.

Capítulo 4

Conjuntos suma y curvas proyectivas monomiales

Tanto en este capítulo como en el siguiente, la filosofía que seguimos consiste en asociar un objeto geométrico a cada subconjunto finito A de un grupo abeliano G, estableciendo así un puente entre la combinatoria aditiva y el álgebra conmutativa (y la geometría algebraica). En este capítulo nos centramos en el caso $G = \mathbb{Z}$.

Consideramos un conjunto $A \subset \mathbb{Z}$ finito, que supondremos en forma normal, es decir, $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\}$, con $\gcd(a_1, \ldots, a_{n-1}) = 1$. En la sección 4.1 asociamos al conjunto A una curva monomial proyectiva, que denotamos $\mathfrak{C}_A$, y relacionamos los conjuntos suma de A con propiedades de la curva $\mathfrak{C}_A$. En particular, el cardinal de los conjuntos suma de A coincide con los valores de la función de Hilbert de la curva. En la sección 4.2 relacionamos las propiedades de la curva $\mathfrak{C}_A$ con los conjuntos suma de A; en la subsección 4.2.1 incluimos resultados propios obtenidos durante la realización de este trabajo. En la sección 4.3 primero recuperamos algunos resultados de teoría aditiva de números y, finalmente, utilizamos un resultado de teoría aditiva de números para dar una cota sobre la regularidad de Castelnuovo-Mumford de la curva $\mathfrak{C}_A$.

A lo largo de todo este capítulo, supondremos que el cuerpo k es algebraicamente cerrado y de característica cero. Por fijar ideas, podemos pensar que estamos trabajando en $k = \mathbb{C}$.

En este capítulo, las referencias principales son [12] y el preprint [13], en fase de elaboración.

4.1. Asociación de la curva monomial $\mathfrak{C}_A$ al conjunto A

Sea $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{Z}$ un conjunto en forma normal. Recordemos que la construcción de Eliahou asocia al conjunto A una k-álgebra graduada

estándar, $R(A)$, de modo que $|sA| = \mathrm{HF}_{R(A)}(s)$ para todo $s \in \mathbb{N}_0$. Como vimos en la observación 3.1.3, $R(A) = k[w, t^{a_1}w, \ldots, t^{a_{n-1}}w]$ es la k-subálgebra de $k[t, w]$ generada por el conjunto $\{w, t^{a_1}w, \ldots, t^{a_{n-1}}w\}$, considerando las variables con grados $\deg(t) = 0$, $\deg(w) = 1$.

Si consideramos el morfismo de k-álgebras graduado $\varphi : k[x_0, \ldots, x_{n-1}] \to k[t, w]$ definido por $\varphi(x_i) = t^{a_i}w$ para $i = 0, \ldots, n-1$, entonces tenemos $\mathrm{im}(\varphi) = R(A)$ y, por tanto, $R(A) \simeq k[x_0, \ldots, x_{n-1}]/\ker\varphi$. Además, por la observación 3.2.6 tenemos que

$$\ker\varphi = \left\langle \mathbf{x}^\alpha - \mathbf{x}^\beta : \alpha, \beta \in \mathbb{N}_0^n, |\alpha| = |\beta| \text{ y } |\alpha|_A = |\beta|_A \right\rangle \subset k[x_0, \ldots, x_{n-1}],$$

donde recordemos que $|\alpha|$ y $|\alpha|_A$ denotan $|\alpha| = \sum_{i=0}^{n-1} \alpha_i$ y $|\alpha|_A = \sum_{i=0}^{n-1} \alpha_i a_i$, respectivamente.

Por otra parte, podemos considerar el morfismo de k-álgebras $\psi : k[x_0, \ldots, x_{n-1}] \to k[u, v]$ dado por $\psi(x_i) = u^{b-a_i}v^{a_i}$ para $i = 0, \ldots, n-1$. Teniendo en cuenta la teoría de curvas monomiales presentada en la subsección 1.5.1, el núcleo de ψ define una curva monomial proyectiva $\mathfrak{C}_A$ dada por la parametrización

$$\mathfrak{C}_A = \left\{ (u^b : u^{b-a_1}v^{a_1} : \cdots : u^{b-a_{n-2}}v^{a_{n-2}} : v^b) \mid (u : v) \in \mathbb{P}^1_k \right\}.$$

Notación. Para la curva monomial $\mathfrak{C}_A$, denotamos I_A su ideal de anulación, es decir, $I_A = \ker\psi$ y $k[\mathfrak{C}_A] = k[x_0, \ldots, x_{n-1}]/I_A$ el anillo de coordenadas de $\mathfrak{C}_A$. Además, HF_A y HP_A denotan la función y el polinomio de Hilbert del anillo $k[\mathfrak{C}_A]$, respectivamente.

Proposición 4.1.1 ([12, Prop. 2.6])**.** En las condiciones anteriores se verifica $\ker\varphi = I_A (= \ker\psi)$. Por lo tanto existe un isomorfismo de k-álgebras graduadas $R(A) \simeq k[\mathfrak{C}_A]$.

Demostración. Consideramos un binomio $\mathbf{x}^\alpha - \mathbf{x}^\beta \in \ker\varphi$, es decir, de modo que $\alpha, \beta \in \mathbb{N}_0^n$ verifican $|\alpha| = |\beta|$ y $|\alpha|_A = |\beta|_A$. Entonces

$$\psi\left(\mathbf{x}^\alpha - \mathbf{x}^\beta\right) = u^{a_{n-1}|\alpha| - |\alpha|_A}v^{|\alpha|_A} - u^{a_{n-1}|\beta| - |\beta|_A}v^{|\beta|_A} = 0,$$

luego $\ker\varphi \subset \ker\psi = I_A$.
Para probar la otra inclusión, como $I_A \subset k[x_0, \ldots, x_{n-1}]$ es un ideal homogéneo y binomial (proposición 1.5.9), basta considerar un binomio $\mathbf{x}^\alpha - \mathbf{x}^\beta \in I_A$ y comprobar que $\mathbf{x}^\alpha - \mathbf{x}^\beta \in \ker\varphi$. Como

$$0 = \psi(\mathbf{x}^\alpha - \mathbf{x}^\beta) = u^{a_{n-1}|\alpha| - |\alpha|_A}v^{|\alpha|_A} - u^{a_{n-1}|\beta| - |\beta|_A}v^{|\beta|_A},$$

entonces se debe verificar $|\alpha| = |\beta|$ y $|\alpha|_A = |\beta|_A$, luego $\mathbf{x}^\alpha - \mathbf{x}^\beta \in \ker\varphi$. □

Observación 4.1.2. Como consecuencia trivial de este resultado y el teorema 3.1.2, tenemos que los valores de la función de Hilbert de la curva monomial $\mathfrak{C}_A$ coinciden con los cardinales de los conjuntos suma de A, es decir,

$$|sA| = \mathrm{HF}_A(s), \text{ para todo } s \in \mathbb{N}_0. \tag{4.1.1}$$

Además de la curva monomial $\mathfrak{C}_A$, más adelante nos interesará la sección hiperplana de $\mathfrak{C}_A$ definida por $x_0 = 0$. Denotamos $\mathcal{B}_A = \frac{k[\mathfrak{C}_A]}{x_0 k[\mathfrak{C}_A]}$ al anillo de coordenadas de esta sección hiperplana.

Lema 4.1.3 ([12, Remark 2.7])**.** $\mathcal{B}_A = \frac{k[\mathfrak{C}_A]}{x_0 k[\mathfrak{C}_A]}$ es una k-álgebra graduada estándar de dimensión 1.

Demostración. Notemos que la clase de x_0 en $\mathcal{B}_A$ no es un divisor de cero de $\mathcal{B}_A$ pues, de serlo, existiría un polinomio $f \in k[x_0, \ldots, x_{n-1}]$ tal que $x_0 f \in I_A$, que es un ideal primo, luego $f \in I_A$. Por lo tanto, $\dim(\mathcal{B}_A) = 1$. Para probar que $\mathcal{B}_A$ es una k-álgebra graduada estándar, usamos la identificación $k[\mathfrak{C}_A] \simeq R(A)$ de la proposición 4.1.1:

$$k[\mathfrak{C}_A] \simeq R(A) = k[w, t^{a_1}w, \ldots, t^{a_{n-1}}w] \Rightarrow \mathcal{B}_A \simeq R(A)/\langle w\rangle = k[w, t^{a_1}w, \ldots, t^{a_{n-1}}w]/\langle w\rangle .$$

Recordemos que en $R(A)$, las variables tienen grado $\deg(t) = 0$ y $\deg(w) = 1$. Según la identificación anterior, la parte de grado 1 de $\mathcal{B}_A$ está generada como k-espacio vectorial por el conjunto $\{\overline{t^{a_1}w}, \ldots, \overline{t^{a_{n-1}}w}\}$ (las barras denotan clases en el cociente) luego

$$(\mathcal{B}_A)_1 = \{\sum_{i=1}^{n-1} \lambda_i \overline{t^{a_i}w} : \lambda_i \in k\},$$

y está claro que $\mathcal{B}_A$ está generada como k-álgebra por $(\mathcal{B}_A)_1$, es decir, $\mathcal{B}_A = k\left[(\mathcal{B}_A)_1\right]$. □

Veamos en un ejemplo concreto qué aspecto tiene el ideal I_A y cómo los valores la función de Hilbert de $\mathfrak{C}_A$ coinciden con los cardinales de los conjuntos suma de A.

Ejemplo 4.1.4. Consideramos el conjunto $A = \{0, 2, 4, 6, 9\} \subset \mathbb{N}_0$. La curva proyectiva monomial $\mathfrak{C}_A \subset \mathbb{P}^4_k$ asociada al conjunto A está definida por la parametrización

$$(u : v) \mapsto (u^9 : u^7v^2 : u^5v^4 : u^3v^6 : v^9).$$

Para calcular el ideal I_A de forma efectiva, utilizamos la proposición 1.5.5.

```
> ring r = 0, (x(0..4),u,v), dp;
> poly f0 = x(0)-u^9;
> poly f1 = x(1)-u^7*v^2;
> poly f2 = x(2)-u^5*v^4;
> poly f3 = x(3)-u^3*v^6;
> poly f4 = x(4)-v^9;
> ideal I = f0,f1,f2,f3,f4;
> ideal IA = eliminate(I,u*v);
```

De aquí obtenemos que

$$I_A = \left\langle x_2^2 - x_1x_3, x_1x_2 - x_0x_3, x_1^2 - x_0x_2, x_3^3 - x_0x_4^2\right\rangle .$$

Por otra parte, para calcular la función de Hilbert de $k[\mathfrak{C}_A]$ trabajamos en el anillo $k[x_0, x_1, x_2, x_3, x_4]$.

```
> ring s = 0, x(0..4), dp;
> ideal IA = imap(r,IA);
> hilb(std(IA), 1);
1,0,-3,1,0,3,-2,0
```

La serie de Hilbert de la curva $\mathfrak{C}_A$ es

$$\mathrm{HF}_A(t) = \frac{1 - 3t^2 + t^3 + 3t^5 - 2t^6}{(1-t)^5} = 1 + 5t + 12t^2 + 21t^3 + 30t^4 + 39t^5 + \dots.$$

Notemos que

$$\begin{aligned}
0A &= \{0\} \to |0A| = 1 = \mathrm{HF}_A(0),\\
A &= \{0,2,4,6,9\} \to |A| = 5 = \mathrm{HF}_A(1),\\
2A &= \{0,2,4,6,8,9,10,11,12,13,15,18\} \to |2A| = 12 = \mathrm{HF}_A(2),\\
3A &= \{0,2,4,6,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,24,27\} \to |3A| = 21 = \mathrm{HF}_A(3).
\end{aligned}$$

En general, hemos demostrado que $|sA| = \mathrm{HF}_A(s)$ para todo $s \in \mathbb{N}_0$, luego $|4A| = 30$, $|5A| = 39$, ... También podemos calcular el polinomio de Hilbert de $\mathfrak{C}_A$.

```
> LIB "poly.lib";
> hilbPoly(IA);
-6,9
```

El polinomio de Hilbert de $\mathfrak{C}_A$ es $\mathrm{HP}_A(s) = 9s - 6$, y observamos que $\mathrm{HF}_A(s) = \mathrm{HP}_A(s)$ para todo $s \geq 2$.

4.2. Álgebra conmutativa → teoría aditiva de números

En esta sección vamos a utilizar algunas propiedades de la curva $\mathfrak{C}_A$ para establecer resultados que nos ayuden a entender bien la función $s \mapsto |sA|$ y el teorema de estructura de la teoría aditiva de números. En la subsección 4.2.1, todos los resultados a partir de la proposición 4.2.5 son de elaboración propia y aparecerán publicados en [13], junto con más resultados sobre la regularidad de Castelnuovo-Mumford de las curvas monomiales proyectivas.

A continuación resumimos algunas propiedades de la curva $\mathfrak{C}_A$, todas ellas ampliamente conocidas.

Propiedades 4.2.1. Sean $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{N}_0$ un conjunto en forma normal y consideramos la curva proyectiva monomial asociada al conjunto A, $\mathfrak{C}_A$.

(a) $\mathfrak{C}_A \subset \mathbb{P}_k^{n-1}$ es una curva proyectiva de grado $b = a_{n-1}$.

(b) $\mathfrak{C}_A$ tiene dos posibles puntos singulares, que son $P_1 = (1 : 0 : \cdots : 0)$ y $P_2 = (0 : 0 : \cdots : 1)$.

- P_1 es no singular si, y solo si, $a_1 = 1$.
- P_2 es no singular si, y solo si $a_{n-1} - a_{n-2} = 1$.

(c) Si $\delta(\mathfrak{C}_A, P_i)$ denota el orden (también llamado invariante δ) de la singularidad de $\mathfrak{C}_A$ en P_i, $i = 1, 2$, entonces

$$\delta(\mathfrak{C}_A, P_1) = |\mathbb{N}_0 \setminus \langle A\rangle|,$$
$$\delta(\mathfrak{C}_A, P_2) = |\mathbb{N}_0 \setminus \langle b - A\rangle|,$$

donde $\langle A\rangle$ y $\langle b - A\rangle$ denotan el semigrupo generado por A y el semigrupo generado por $b - A$, respectivamente.

(d) La curva $\mathfrak{C}_A$ es racional, luego el género aritmético de $\mathfrak{C}_A$ es $p_a(\mathfrak{C}_A) = \delta(\mathfrak{C}_A, P_1) + \delta(\mathfrak{C}_A, P_2)$ y se tiene

$$\mathrm{HP}_A(0) = 1 - \delta(\mathfrak{C}_A, P_1) - \delta(\mathfrak{C}_A, P_2).$$

Notación. Denotamos $\mathrm{r}(k[\mathfrak{C}_A])$ la regularidad de la función de Hilbert y $\mathrm{reg}(k[\mathfrak{C}_A])$ la regularidad de Castelnuovo-Mumford del anillo $k[\mathfrak{C}_A]$.

El siguiente resultado muestra cómo calcular los cardinales de los conjuntos suma de A para s suficientemente grande en función de las propiedades de la curva $\mathfrak{C}_A$; en particular, aparecen el grado de $\mathfrak{C}_A$ y el orden de las singularidades en P_1 y P_2.

Proposición 4.2.2 ([12, Prop. 3.1])**.** Sea $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{N}_0$ un conjunto en forma normal, es decir, tal que $\gcd(a_1, \ldots, a_{n-1}) = 1$. Entonces

$$|sA| = \mathrm{HF}_A(s) = sb + 1 - \delta(\mathfrak{C}_A, P_1) - \delta(\mathfrak{C}_A, P_2)$$

para cada $s \geq \mathrm{r}(k[\mathfrak{C}_A])$.

Demostración. Por la observación 4.1.2, $|sA| = \mathrm{HF}_A(s)$ para todo $s \geq 0$. Por otra parte, aplicando las propiedades 4.2.1 tenemos que

$$\mathrm{HP}_A(s) = sb + \mathrm{HP}_A(0) = sb + 1 - \delta(\mathfrak{C}_A, P_1) - \delta(\mathfrak{C}_A, P_2),$$

y el resultado se deduce teniendo en cuenta que $\mathrm{HF}_A(s) = \mathrm{HP}_A(s)$ para todo $s \geq \mathrm{r}(k[\mathfrak{C}_A])$. □

Observación 4.2.3. Para cada $s \in \mathbb{N}$, la parte de grado s de la k-álgebra graduada estándar $\mathcal{B}_A$ es

$$(\mathcal{B}_A)_s = \frac{k[\mathfrak{C}_A]_s}{x_0 k[\mathfrak{C}_A]_{s-1}},$$

luego

$$\mathrm{HF}_{\mathcal{B}_A}(s) = \mathrm{HF}_A(s) - \mathrm{HF}_A(s-1), \text{ para todo } s \geq 1.$$

En particular, $\mathrm{HP}_{\mathcal{B}_A} = a_{n-1} = b$, de donde deducimos que la multiplicidad de la k-álgebra $\mathcal{B}_A$ es igual a b.

4.2.1. Entendiendo el teorema de estructura

Recordemos que, dado un subconjunto finito $A \subset \mathbb{Z}$ en forma normal, el teorema de estructura (teorema 2.1.5) afirma que existen números $\sigma, c_1, c_2 \in \mathbb{N}_0$ y conjuntos $C_i \subset [0, c_i - 2]$, $i = 1, 2$, tales que

$$sA = C_1 \sqcup [c_1, sb - c_2] \sqcup (sb - C_2)\,, \text{ para todo } s \geq \sigma.$$

Una de las principales aportaciones del artículo de J. Elias es la interpretación de los números c_i y los conjuntos C_i que aparecen en el teorema de estructura.

Notación. Dado un conjunto $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{N}_0$ en forma normal, denotamos $\Gamma_1 = \langle A \rangle$ el semigrupo numérico generado por A y $\Gamma_2 = \langle b - A \rangle$ el semigrupo numérico generado por $b - A$.

Teorema 4.2.4 ([12, Prop. 3.4])**.** Siguiendo las notaciones del teorema 2.1.5, para $i = 1, 2$ son ciertas las siguientes afirmaciones:

(1) c_i es el conductor del semigrupo Γ_i.

(2) $C_i = \Gamma_i \cap [0, c_i - 2]$.

(3) $\delta(\mathfrak{C}_A, P_i) = c_i - |C_i|$.

Demostración. Notemos que $\Gamma_1 = \langle a_1, \ldots, a_{n-1} \rangle = \cup_{s=1}^{\infty} sA$. Además, como $a_0 = 0$, se tiene $sA \subset (s+1)A$ para todo $s \in \mathbb{N}_0$, luego $(sA)_{s=0}^{\infty} \uparrow \Gamma_1$. Por el teorema 2.1.5, podemos escribir

$$sA = C_1 \sqcup [c_1, sa_{n-1} - c_2] \sqcup (sa_{n-1} - C_2)$$

para cada $s \geq \sigma$, donde $C_i \subset [0, c_i - 2]$ para $i = 1, 2$.

(1) Como $a_{n-1} > a_0 = 0$, $\lim_{s\to\infty} (sa_{n-1} - c_2) = \infty$ y se tiene $[c_1, sa_{n-1} - c_2] \uparrow [c_1, \infty)$. Por lo tanto, $\Gamma_1 = C_1 \sqcup [c_1, \infty)$. Entones es claro que c_1 es el conductor de Γ_1 (y, por tanto, $c_1 - 1$ es el número de Fröbenius).

(2) $C_1 = \Gamma_1 \cap [0, c_1 - 2]$, puesto que $\Gamma_1 = C_1 \sqcup [c_1, \infty)$.

(3) Teniendo en cuenta (2),

$$\delta(\mathfrak{C}_A, P_1) = |\mathbb{N}_0 \setminus \Gamma_1| = (c_1 - 1) - |C_1| + 1 = c_1 - |C_1|.$$

Para $i = 2$, basta aplicar el razonamiento anterior al conjunto $A^* = \{a_{n-1}\} - A$, para el que se tiene

$$sA^* = \{sa_{n-1}\} - sA = C_2 \sqcup [c_2, sa_{n-1} - c_1] \sqcup (\{sa_{n-1}\} - C_1)\,,$$

y tener en cuenta que $\Gamma_2 = \cup_{s=1}^{\infty} s\,(\{a_{n-1}\} - A)$.

□

Lo único que falta para terminar de entender el teorema de estructura es determinar de algún modo el número σ. El siguiente resultado va en esta línea:

Proposición 4.2.5. El mínimo número σ a partir del cual se verifica la descomposición del teorema 2.1.5 se puede escribir de la manera siguiente:

$$\sigma = \text{máx}\left\{\text{r}(k[C_A]), \left\lceil \frac{c_1+c_2}{a_{n-1}} \right\rceil \right\}. \tag{4.2.1}$$

Demostración. Sea $s \geq \sigma$, entonces podemos escribir sA en la forma (2.1.5), de donde deducimos que $\sigma \geq \lceil \frac{c_1+c_2}{a_{n-1}} \rceil$ y

$$\begin{aligned} \text{HF}_A(s) &= |sA| = sa_{n-1} + 1 - (c_1 - |C_1| + c_2 - |C_2|) \\ &= sa_{n-1} + 1 - \delta(\mathfrak{C}_A, P_1) - \delta(\mathfrak{C}_A, P_2) = \text{HP}_A(s), \end{aligned} \tag{4.2.2}$$

luego $s \geq \text{r}(k[C_A])$. Recíprocamente, si $s \geq \text{máx}\left\{\text{r}(k[C_A]), \lceil \frac{c_1+c_2}{a_{n-1}} \rceil \right\}$, se verifica la ecuación (4.2.2) por ser $s \geq \text{r}(k[C_A])$. Por otra parte, como $s \geq \lceil \frac{c_1+c_2}{a_{n-1}} \rceil$, se tiene $sa_{n-1} - c_2 \geq c_1$ y, por tanto,

$$\begin{aligned} sA &= (sA \cap C_1) \sqcup (sA \cap [c_1, sa_{n-1} - c_2]) \sqcup (sA \cap (sa_{n-1} - C_2)) \\ &\subset C_1 \sqcup [c_1, sa_{n-1} - c_2] \sqcup (sa_{n-1} - C_2)\,. \end{aligned}$$

Como los dos conjuntos sA y $C_1 \sqcup [c_1, sa_{n-1} - c_2] \sqcup (sa_{n-1} - C_2)$ son finitos y tienen el mismo número de elementos, entonces son iguales, es decir, se verifica $s \geq \sigma$. □

Ejemplo 4.2.6. Sea $A = \{0, 2, 4, 6, 9\} \subset \mathbb{N}_0$ el conjunto del ejemplo 4.1.4. Entonces se puede comprobar que

$$sA = \{0, 2, 4, 6\} \sqcup [8, 9s - 5] \sqcup \{9s - 3, 9s\}, \text{ para todo } s \geq 2.$$

Por lo tanto, tenemos $c_1 = 8$, $C_1 = \{0, 2, 4, 6\}$, $c_2 = 5$ y $C_2 = \{0, 3\}$. En este caso, los puntos $P_1 = (1 : 0 : 0 : 0 : 0)$ y $P_2 = (0 : 0 : 0 : 0 : 1)$ son singulares y el orden de las singularidades es

$$\begin{aligned} \delta(\mathfrak{C}_A, P_1) &= c_1 - |C_1| = 4, \\ \delta(\mathfrak{C}_A, P_2) &= c_2 - |C_2| = 2. \end{aligned}$$

Como $\text{HP}_A(s) = \text{HF}_A(s)$ para cada $s \geq 2$, la regularidad de la función de Hilbert de la curva es $\text{r}(k[\mathfrak{C}_A]) = 2$ y

$$\sigma = \text{máx}\left\{\text{r}(k[C_A]), \left\lceil \frac{c_1+c_2}{a_{n-1}} \right\rceil \right\} = \text{máx}\left\{2, \left\lceil \frac{13}{9} \right\rceil \right\} = 2.$$

En la figura 4.2.1 presentamos un diagrama que permite entender los conjuntos suma de forma muy clara. Explicamos el significado de este diagrama en la observación siguiente.

Observación 4.2.7. Asociado al conjunto $A \subset \mathbb{N}_0$ podemos considerar su "homogeneizado" en $\mathbb{N}_0^2$, que es el conjunto

$$\tilde{A} = \{(b - a, a) : a \in A\} = \{(b, 0), (b - a_1, a_1), \ldots, (b - a_{n-2}, a_{n-2}), (0, b)\},$$

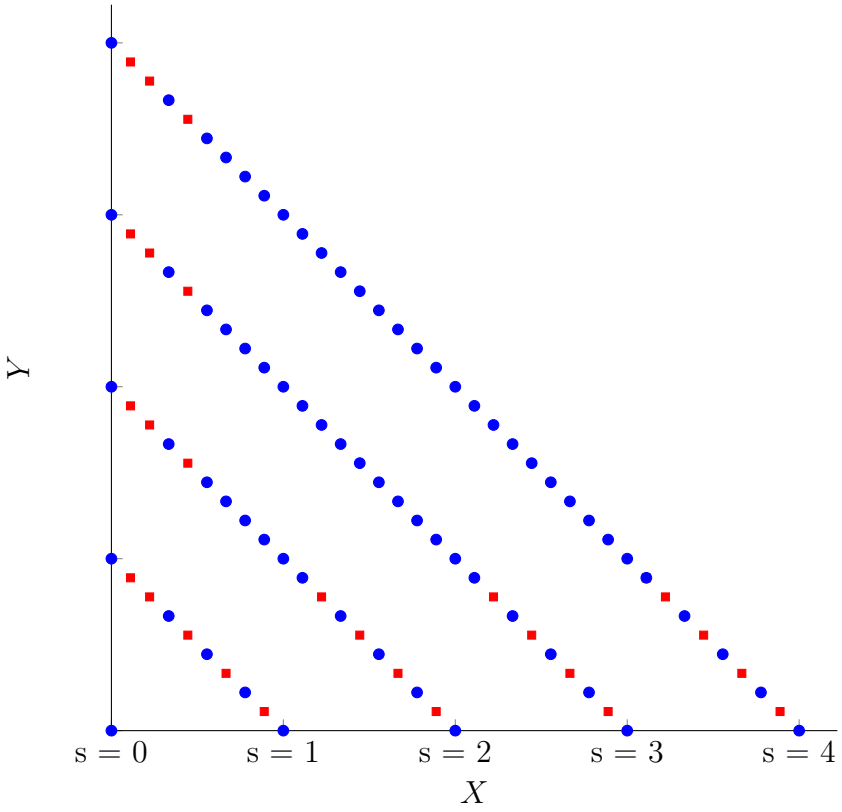


Figura 4.2.1: Subsemigrupo de $\mathbb{N}_0^2$ asociado a la curva $\mathfrak{C}_A$ del ejemplo 4.2.6.

cuyos elementos son los exponentes de los monomios que parametrizan $\mathfrak{C}_A$.
Es inmediato comprobar que los conjuntos suma de $\tilde{A}$ están completamente determinados por los de A, puesto que para cada $s \in \mathbb{N}_0$,

$$s\tilde{A} = \{(sb - \alpha, \alpha) : \alpha \in sA\}.$$

Es decir, el semigrupo generado por el conjunto $\tilde{A}$ en $\mathbb{N}_0^2$ está completamente determinado por el semigrupo generado por A en $\mathbb{N}_0$, en concreto, por los conjuntos suma $\{sA\}_{s\in\mathbb{N}_0}$.
Esto se puede visualizar de la manera siguiente: si dibujamos unos ejes cartesianos en el plano y representamos el conjunto sA en el eje de ordenadas (Y), entonces los elementos del semigrupo $\langle\tilde{A}\rangle$ que están sobre la recta $X+Y = sb$ se obtienen proyectando los puntos de sA de forma horizontal (es decir, considerando el punto de la recta $X+Y = sb$ con la misma ordenada).
En la figura 4.2.1, los círculos azules representan elementos del semigrupo $\langle\tilde{A}\rangle$, mientras que los cuadrados rojos representan elementos de $\mathbb{N}_0^2$ que no pertenecen al semigrupo $\langle\tilde{A}\rangle$.

Si volvemos al conjunto A del ejemplo 4.2.6, entonces proyectando la figura 4.2.1 sobre el eje de ordenadas podemos recuperar toda la información sobre los conjuntos suma de A: los números $c_1, c_2, \sigma \in \mathbb{N}_0$, los conjuntos $C_i \subset [0, c_i - 2]$, etc.

Tras este pequeño paréntesis, volvemos al tema que nos ocupa. La proposición 4.2.5 nos da la clave para entender la cota de Granville y Walker [16]. Para explicar un poco mejor esto, primero vamos a acotar superiormente el número $\lceil \frac{c_1+c_2}{a_{n-1}} \rceil$.

Lema 4.2.8. Sean $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{N}_0$ un conjunto en forma normal, $\Gamma_1 = \langle A \rangle$ el semigrupo generado por A y $\Gamma_2 = \langle b - A \rangle$ el semigrupo generado por $b - A$. Si c_i denota el conductor del semigrupo Γ_i, $i = 1, 2$, entonces se verifica

$$\left\lceil \frac{c_1 + c_2}{a_{n-1}} \right\rceil \leq a_{n-1} - n + 1.$$

Demostración. Por [27, Thm. 3.1.1], los conductores de los semigrupos se pueden acotar de la manera siguiente:

$$\begin{aligned} c_1 &\leq (a_1 - 1)(a_{n-1} - 1) = (a_1 - 1)(b - 1), \\ c_2 &\leq (b - a_{n-2} - 1)(b - a_1 - 1). \end{aligned}$$

Por lo tanto, podemos escribir

$$\begin{aligned} c_1 + c_2 &\leq b^2 - 3b - ba_{n-2} + a_1 a_{n-2} + a_{n-2} + 2 \\ &\leq b^2 - 3b - b(a_1 + n - 3) + (b - 1)a_1 + (b - 1) + 2 \\ &\leq b^2 - 3b - nb + 3b - a_1 + b + 1 \\ &\leq b^2 - nb + b = b(b - n + 1), \end{aligned}$$

donde hemos tenido en cuenta que $a_{n-2} \geq a_1 + n - 3$ y $a_{n-2} \leq b - 1$. Dividiendo por b obtenemos el resultado. □

Para acotar la regularidad de la función de Hilbert de la curva $\mathfrak{C}_A$, recordemos que $\mathrm{r}(k[\mathfrak{C}_A]) \leq \mathrm{reg}(k[\mathfrak{C}_A])$ por la proposición 1.4.8. Por otra parte, la conjetura de Eisenbud-Goto para la curva $\mathfrak{C}_A$ es cierta, como probaron Gruson, Lazarsfeld y Peskine [17], y afirma que

$$\mathrm{reg}(k[\mathfrak{C}_A]) \leq \deg(\mathfrak{C}_A) - \mathrm{codim}(I_A) = b - (n - 2) = b - n + 2.$$

Ahora podemos dar una buena cota para σ.

Proposición 4.2.9. Sean $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{N}_0$ un conjunto en forma normal y σ el mínimo número natural a partir del cual es cierta la descomposición del teorema de estructura. Entonces se verifica $\sigma \leq b - n + 2$.

Demostración. Por la proposición 4.2.5, tenemos que $\sigma = \max\{\mathrm{r}(k[\mathfrak{C}_A]), \lceil \frac{c_1+c_2}{b} \rceil\}$. Por otra parte, sabemos que $\mathrm{r}(k[\mathfrak{C}_A]) \leq b - n + 2$ y, por el lema 4.2.8, $\lceil \frac{c_1+c_2}{b} \rceil \leq b - n + 1$, luego el máximo de estas dos cantidades está acotado superiormente por $b - n + 2$. □

Si volvemos a pensar ahora en las cotas para el valor de σ que se conocían hasta la actualidad (observación 2.1.6), podemos imaginar por qué desde el artículo [16] de Granville y Walker no se ha obtenido ninguna cota mejor para σ. Es sorprendente observar cómo, sin tener conocimiento del artículo de Eliahou y Mazumdar [11], ni del de Elías [12], Granville y Walker llegaron a establecer esa cota que nos lleva a la conjetura de Eisenbud-Goto.

4.3. Polinomios de Hilbert rígidos y problemas inversos

Definición 4.3.1. Sea $H : \mathbb{N}_0 \to \mathbb{N}_0$ una *función numérica asintóticamente polinómica*, es decir, tal que existen un polinomio $p(T) \in \mathbb{Z}[T]$ y un número $s_0 \in \mathbb{N}_0$ de modo que $H(s) = p(s)$ para todo $s \geq s_0$. Sea $\mathcal{C}$ una clase de k-álgebras graduadas. Se dice que $p(T)$ es un *polinomio rígido* para la clase $\mathcal{C}$ si para toda k-álgebra $D \in \mathcal{C}$ se cumple la condición siguiente:

$$\text{si } \mathrm{HP}_D = p, \text{ entonces } \mathrm{HF}_D = H.$$

En el siguiente resultado vamos a demostrar que el polinomio $p(T) = (n-1)T + 1$ es rígido para la clase de k-álgebras

$$\mathcal{C} = \{k[\mathfrak{C}_A] : A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \text{ con } \gcd(a_1, \ldots, a_{n-1}) = 1\}$$

y la condición $|sA| = s(n-1) + 1$ para algún $s \geq 2$ es una propiedad rígida, es decir, determina la función de Hilbert por completo.

Teorema 4.3.2 ([12, Thm. 4.3])**.** Sea $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{N}_0$ un conjunto en forma normal. Las siguientes condiciones son equivalentes:

(1) $|sA| = s(n-1) + 1 + o(s)$ para infinitos valores de s, donde $o : \mathbb{N}_0 \to \mathbb{N}_0$ es una función aritmética que verifica $\lim_{s\to\infty} o(s) = 0$.

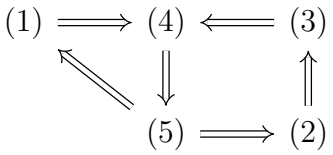
(2) $|sA| = s(n-1) + 1$ para todo $s \gg 0$.

(3) $|sA| = s(n-1) + 1$ para algún $s \geq 2$.

(4) $A = [0, n-1] = \{0, 1, \ldots, n-1\}$.

(5) $|sA| = s(n-1) + 1$ para todo $s \in \mathbb{N}_0$.

Demostración. El esquema que vamos a seguir para demostrar la equivalencia es



De estas implicaciones, vamos a demostrar únicamente (1) ⇒ (4), (4) ⇒ (5) y (3) ⇒ (4), pues el resto ((5) ⇒ (1), (5) ⇒ (2) y (2) ⇒ (3)) son inmediatas.
(1) ⇒ (4): Si suponemos que se verifica (1), entonces existe una sucesión $(s_m)_{m=0}^{\infty} \subset \mathbb{N}_0$ estrictamente creciente tal que

$$|s_m A| = s_m(n-1) + 1 + o(s_m), \text{ para todo } m \in \mathbb{N}_0.$$

Como $(s_m)_{m=0}^{\infty}$ es estrictamente creciente, existe $m_0 \in \mathbb{N}_0$ tal que $s_m \geq \mathrm{r}(k[\mathfrak{C}_A])$ para todo $m \geq m_0$ y, aplicando la proposición 4.2.2 tenemos que

$$|s_m A| = s_m b + 1 - \delta(\mathfrak{C}_A, P_1) - \delta(\mathfrak{C}_A, P_2), \text{ para todo } m \geq m_0.$$

Por lo tanto, para cada $m \geq m_0$ se verifica

$$s_m(n-1) + 1 + o(s_m) = s_m b + 1 - \delta(\mathfrak{C}_A, P_1) - \delta(\mathfrak{C}_A, P_2),$$

de donde deducimos que

$$s_m\,[b-(n-1)] - \delta(\mathfrak{C}_A, P_1) - \delta(\mathfrak{C}_A, P_2) = o(s_m) \xrightarrow[m\to\infty]{} 0. \tag{4.3.1}$$

Si $b-(n-1) \neq 0$, entonces el lado izquierdo de (4.3.1) tiende hacia ∞ cuando $m \to \infty$. Por lo tanto, debe ser $b = n-1$, es decir, $A = \{0, 1, \ldots, n-1\} = [0, n-1]$. De hecho, hemos probado que P_1 y P_2 son no singulares si se verifica (1).
(4) $\Rightarrow$ (5): Si $A = [0, n-1]$, entonces $sA = [0, s(n-1)]$ para todo $s \in \mathbb{N}_0$, luego $|sA| = s(n-1)+1$ para todo $s \geq 0$.
(3) $\Rightarrow$ (4): Sea $s \geq 2$ un entero tal que $|sA| = s(n-1)+1$. Vamos a probar que, en este caso, $b \leq n-1$, lo que implicará que $b = n-1$ y, por tanto, $A = [0, n-1]$.
Como $(s-1)A \subset [0, (s-1)b]$, tenemos que

$$(s-1)A \sqcup \{(s-1)b + a_1, \ldots, (s-1)b + b\} \subset sA.$$

Ahora bien, según el teorema 2.1.12, $|(s-1)A| \geq (s-1)(n-1)+1$. Por lo tanto,

$$(s-1)A \sqcup \{(s-1)b + a_1, \ldots, (s-1)b + b\} = sA. \tag{4.3.2}$$

Para el valor de $s \geq 2$ que tenemos fijado, consideramos el k-espacio vectorial $(\mathcal{B}_A)_s = \frac{k[\mathfrak{C}_A]_s}{x_1 k[\mathfrak{C}_A]_{s-1}}$. Por (4.3.2), un sistema de generadores del k-espacio vectorial $(\mathcal{B}_A)_s$ es

$$\{\overline{t^{(s-1)b+a_1}w^s}, \ldots, \overline{t^{(s-1)b+a_{n-1}}w^s}\},$$

donde estamos identificando la k-álgebra graduada $k[\mathfrak{C}_A]$ con $R(A)$ (proposición 4.1.1) y la barra denota la clase en el anillo cociente. Por otra parte, como $(\mathcal{B}_A)_1$ está generado como k-espacio vectorial por $\{\overline{t^{a_1}w}, \ldots, \overline{t^{a_{n-1}}w}\}$ y para cada $i = 1, \ldots, n-1$ se verifica

$$x_{n-1}^{s-1} \cdot (t^{a_i}w) \equiv t^{a_{n-1}(s-1)}w^{s-1}t^{a_i}w = t^{a_{n-1}(s-1)+a_i}w^s,$$

por la identificación $k[\mathfrak{C}_A] \simeq R(A)$. Entonces está claro que $x_{n-1}^{s-1}(\mathcal{B}_A)_1 = (\mathcal{B}_A)_s$. Ahora, como la k-álgebra $\mathcal{B}_A$ es estándar, multiplicando a los dos lados por $(\mathcal{B}_A)_{(r-1)(s-1)}$ deducimos lo siguiente:

$$\begin{aligned}
&(\mathcal{B}_A)_s \cdot (\mathcal{B}_A)_{(r-1)(s-1)} = (\mathcal{B}_A)_{s+(r-1)(s-1)} = (\mathcal{B}_A)_{r(s-1)+1}\,,\\
&(\mathcal{B}_A)_{(r-1)(s-1)} \cdot x_{n-1}^{s-1}(\mathcal{B}_A)_1 = x_{n-1}^{r(s-1)}(\mathcal{B}_A)_1\,,
\end{aligned}$$

luego $x_{n-1}^{r(s-1)}(\mathcal{B}_A)_1 = (\mathcal{B}_A)_{r(s-1)+1}$ para todo $r \geq 1$. Ahora bien, por la proposición 4.2.2 tenemos que para r suficientemente grande

$$\dim_k (\mathcal{B}_A)_{r(s-1)+1} = |\,(r(s-1)+1)\,A| - |\,(r(s-1))\,A| = a_{n-1},$$

y

$$\dim_k \left(x_{n-1}^{r(s-1)}(\mathcal{B}_A)_1\right) \leq n-1,$$

de donde concluimos que $a_{n-1} \leq n-1$. □

Observación 4.3.3. Teniendo en cuenta que dado un conjunto $A \subset \mathbb{Z}$, A es una sucesión aritmética si, y solo si, la forma normal de A es el intervalo $[0, n-1]$ y aplicando el teorema 4.3.2, se deducen de forma inmediata los siguientes resultados del capítulo 2:

- Teorema 2.1.13: equivalencia (3) $\Leftrightarrow$ (4).
- Teorema 2.1.14: equivalencia (1) $\Leftrightarrow$ (4).

Para concluir esta sección, vamos a aprovechar un resultado conocido de teoría aditiva de números, el teorema 2.1.8, para dar una cota sobre la regularidad de Castelnuovo-Mumford del anillo $k[\mathfrak{C}_A]$. Para ello, nos restringimos al caso en que el anillo $k[\mathfrak{C}_A]$ es Cohen-Macaulay y razonamos sobre la k-álgebra $\mathcal{B}_A$, cuya función de Hilbert viene dada por

$$\mathrm{HF}_{\mathcal{B}_A}(s) = |sA| - |(s-1)A| \geq \min\left(a_{n-1}, s(n-2)+1\right).$$

Teorema 4.3.4 ([12, Thm. 4.7])**.** Sea $A = \{a_0 = 0 < a_1 < \cdots < a_{n-1} = b\} \subset \mathbb{N}_0$ un conjunto en forma normal. Si el anillo 2-dimensional $k[\mathfrak{C}_A]$ es Cohen-Macaulay, entonces

$$\mathrm{reg}(k[\mathfrak{C}_A]) \leq \left\lceil \frac{b-1}{n-2} \right\rceil.$$

Demostración. Denotamos $s_0 := \lceil \frac{b-1}{n-2} \rceil$. Como $k[\mathfrak{C}_A]$ es Cohen-Macaulay, aplicando la proposición 1.4.9 tenemos que $\mathrm{r}(k[\mathfrak{C}_A]) + 1 = \mathrm{reg}(k[\mathfrak{C}_A])$. Por el lema 4.1.3, $\mathcal{B}_A$ es un anillo de dimensión 1. Además, por [22, Thm. 12.10] sabemos que $\mathcal{B}_A$ es Cohen-Macaulay y $\mathrm{HF}_{\mathcal{B}_A}(s) \leq a_{n-1}$ para todo $s \in \mathbb{N}_0$. Por lo tanto, del teorema 2.1.8 y la observación 2.1.9 se sigue que

$$s(n-2)+1 \leq \mathrm{HF}_{\mathcal{B}_A}(s) \leq \min\left\{a_{n-1}, \binom{s+n-2}{s}\right\} \text{ para } s = 1, \ldots, s_0 - 1,$$
$$\mathrm{HF}_{\mathcal{B}_A}(s) = a_{n-1} \text{ para } s \geq s_0,$$

puesto que $\mathrm{HP}_{\mathcal{B}_A}(s) = a_{n-1}$. De aquí deducimos que $\mathrm{r}(\mathcal{B}_A) \leq s_0$. Por otra parte, como $\mathrm{r}(k[\mathfrak{C}_A]) + 1 = \mathrm{r}(\mathcal{B}_A)$, entonces

$$\mathrm{reg}(k[\mathfrak{C}_A]) = \mathrm{r}(k[\mathfrak{C}_A]) + 1 = \mathrm{r}(\mathcal{B}_A) \leq s_0,$$

lo que completa la prueba. □

Ejemplo 4.3.5. Si consideramos la curva $\mathfrak{C}_A$ del ejemplo 4.1.4, entonces el anillo $k[\mathfrak{C}_A]$ es Cohen-Macaulay, puesto que $2 = \dim(k[\mathfrak{C}_A]) = \mathrm{depth}(k[\mathfrak{C}_A]) = 5 - 3$ (Auslander-Buchsbaum). En este caso se verifica $\mathrm{reg}(k[\mathfrak{C}_A]) = 3 = \lceil 8/3 \rceil$, es decir, la regularidad de Castelnuovo-Mumford de $k[\mathfrak{C}_A]$ alcanza la cota superior en el teorema 4.3.4.

```
> ring s = 0, x(0..4), dp;
> ideal I = x(2)^2-x(1)*x(3),x(1)*x(2)-x(0)*x(3),
            x(1)^2-x(0)*x(2),x(3)^3-x(0)*x(4)^2;
> list rI=mres(I,0);
> print(betti(rI),"betti");
```

	0	1	2	3
0:	1	-	-	-
1:	-	3	2	-
2:	-	1	-	-
3:	-	-	3	2
total:	1	4	5	2

Capítulo 5

Conjuntos suma y variedades de Veronese

En este capítulo nos centramos en el estudio de los conjuntos suma cuando $G = \mathbb{Z}^n$. Dado un conjunto $A \subset \mathbb{Z}^n$ finito, en la sección 5.1 asociamos al conjunto A una proyección monomial Y_{n,d_A} de la variedad de Veronese X_{n,d_A} ($d_A \in \mathbb{N}$ es un número que depende del conjunto A) de modo que los valores de la función de Hilbert de Y_{n,d_A} coinciden con los cardinales de los conjuntos suma de A. En la sección 5.2 hablamos sobre el grado y la dimensión de esta variedad. Finalmente, en las secciones 5.3 y 5.4 presentamos algunos resultados sobre los conjuntos suma obtenidos a partir de otros resultados de álgebra conmutativa o geometría algebraica.

En este capítulo utilizamos la notación de la subsección 1.5.2, es decir, consideramos el anillo de polinomios $S = k[x_0, x_1, \ldots, x_n]$ y si $d \in \mathbb{N}$, entonces $N_{n,d} := \binom{n+d}{n}$ y $\mathcal{M}_{n,d} = \{m_0, \ldots, m_{N_{n,d}-1}\}$ denota el conjunto formado por todos los monomios de grado d en S, ordenados con el orden lexicográfico. Recordamos que aquí las variables $\mathbf{x}$ denotan los parámetros y las variables $\mathbf{w}$ denotan las coordenadas de las variedades monomiales que vamos a considerar. Al igual que en el capítulo 4, suponemos que el cuerpo k es algebraicamente cerrado de característica cero.

La referencia principal seguida en este capítulo es [3].

5.1. Asociación de la proyección monomial Y_{n,d_A} al conjunto A

Sean $n \in \mathbb{N}$ y $A \subset \mathbb{Z}^n$ un subconjunto finito. El teorema de Khovanskii (teorema 2.2.1) afirma que la función definida por $s \mapsto |sA|$, $s \in \mathbb{N}_0$, es eventualmente polinómica. Es decir, existe un polinomio $p_A(z) \in \mathbb{Q}[z]$ tal que $|sA| = p_A(s)$ para todo $s \gg 0$. En particular, recordemos que denotamos $n_0(A)$ al mínimo número natural tal que $|sA| = p_A(s)$ para todo $s \geq n_0(A)$.

Comenzamos la sección con dos ejemplos en los que mostramos que una ligera modificación del conjunto A puede cambiar el polinomio p_A de una forma considerable.

Ejemplo 5.1.1. (I) Sea $A^1 = \{(0,0),(3,0),(2,2),(0,1)\} \subset \mathbb{Z}^2$. Es claro que

$$sA^1 = \{a(0,0) + b(3,0) + c(2,2) + d(0,1) : a,b,c,d \in \mathbb{N}_0, a+b+c+d = s\}.$$

Para contar el número de elementos de sA^1, distinguimos dos casos:

- Para $s \leq 7$ tenemos que $|sA^1| = \binom{s+3}{3} = 1/6(s^3 + 6s^2 + 11s + 6)$, que es el número de 4-uplas $(a,b,c,d) \in \mathbb{N}_0^4$ tales que $a+b+c+d = s$.
- Sin embargo, para $s \geq 8$ debemos tener en cuenta la relación $2(3,0)+6(0,1) = 3(2,2)$, lo que nos lleva a identificar las 4-uplas de la forma $(a, 2k+b, c, 6k+d)$ y $(a+5k, b, 3k+c, d)$ para todo $k \geq 1$. Teniendo en cuenta esto obtenemos que

$$|sA^1| = \binom{s+3}{3} - \binom{s-5}{3} = 4s^2 - 16s + 36, \ \forall s \geq 8.$$

En particular, las dos expresiones anteriores coinciden para $5 \leq s \leq 7$, por lo que $n_0(A) = 5$ y los cardinales de los conjuntos suma de A^1 vienen dados por

$$|A^1| = 4, \ |2A^1| = 10, \ |3A^1| = 20, \ |4A^1| = 35 \text{ y}$$
$$|sA^1| = 4(s^2 - 4s + 9), \text{ para todo } s \geq 5.$$

Notemos que el polinomio $p_{A^1}(z) = 4(z^2 - 4z + 9)$ tiene coeficientes enteros.

(II) Sea $A^2 = \{(0,0),(2,0),(2,2),(0,1)\} \subset \mathbb{Z}^2$. Notemos que únicamente hemos cambiado el elemento $(3,0)$ por $(2,0)$ en A^1. Siguiendo la idea del ejemplo previo, en este caso tenemos $(2,0) + 2(0,1) = (2,2)$. Para $s \leq 2$, $|sA^2| = \binom{s+3}{3}$, mientras que para $s \geq 3$ tenemos que tener en cuenta la relación anterior (identificando las 4-uplas $(a, b+k, c, d+2k)$ y $(a+2k, b, c+k, d)$ para todo $k \geq 1$) y obtenemos

$$|sA^2| = \binom{s+3}{3} - \binom{s}{3} = \frac{3}{2}(s^2 + s) + 1.$$

Notemos que ambas expresiones coinciden para $0 \leq s \leq 3$, luego $|sA^2| = \frac{3}{2}(s^2+s)+1$ para todo $s \in \mathbb{N}_0$ y tenemos que $n_0(A) = 0$. En este caso, el polinomio del teorema de Khovanskii es $p_{A^2}(z) = \frac{3}{2}(z^2 + z) + 1$ y tiene coeficientes racionales.

Ahora vamos a asociar al conjunto A una proyección monomial de una variedad de Veronese.

Definición 5.1.2. Sean $n \in \mathbb{N}$ y $A \subset \mathbb{N}_0^n$ un subconjunto finito. Denotamos d_A al número natural

$$d_A = \text{máx}\left\{ |\mathbf{a}| = \sum_{i=1}^{n} a_i : \mathbf{a} = (a_1, \ldots, a_n) \in A \right\}.$$

Para este número d_A, consideramos el conjunto de monomios

$$\Omega_{n,d_A} = \{x_0^{d_A - |\mathbf{a}|} x_1^{a_1} \ldots x_n^{a_n} : \mathbf{a} \in A\} \subset \mathcal{M}_{n,d_A}$$

y denotamos Y_{n,d_A} la proyección monomial de la variedad de Veronese X_{n,d_A} parametrizada por Ω_{n,d_A}.

Observación 5.1.3. Aunque escribimos Y_{n,d_A}, notemos que esta proyección monomial depende del conjunto A, no solo del número d_A.

Gracias al siguiente resultado, podemos reducir el estudio a subconjuntos $A \subset \mathbb{N}_0^n$ que verifican $\gcd(m \in \Omega_{n,d_A}) = 1$. La idea es "empujar" el conjunto A hacia los ejes coordenados lo máximo posible:

Proposición 5.1.4 ([3, Remark 3.2])**.** Dado un subconjunto finito $A \subset \mathbb{Z}^n$, existe una única traslación $\tau : \mathbb{Z}^n \to \mathbb{Z}^n$ tal que $\tau(A) \subset \mathbb{N}_0^n$ y $\gcd\left(m \in \Omega_{n,d_{\tau(A)}}\right) = 1$. Además, $|sA| = |s\tau(A)|$ para todo $s \in \mathbb{N}_0$.

Demostración. Sea $\mathbf{c} \in \mathbb{Z}^n$ el vector definido por $c_i = \min\{a_i : \mathbf{a} = (a_1, \ldots, a_n) \in A\}$ para cada $1 \leq i \leq n$, y consideramos la traslación τ definida por el vector $-\mathbf{c}$. Entonces $\tau(A) = \{\mathbf{a} - \mathbf{c} : \mathbf{a} \in A\} \subset \mathbb{N}_0^n$, $d_{\tau(A)} = \max\{|\mathbf{a} - \mathbf{c}| = |\mathbf{a}| - |\mathbf{c}| : \mathbf{a} \in A\}$ y

$$\Omega_{n,d_{\tau(A)}} = \{x_0^{d_{\tau(A)}-|\mathbf{a}-\mathbf{c}|} x_1^{a_1-c_1} \ldots x_n^{a_n-c_n} : \mathbf{a} \in A\},$$

y está claro que se cumplen todas las propiedades del enunciado. □

Dados $n \geq 1$ y un subconjunto finito $A \subset \mathbb{N}_0^n$, consideramos el conjunto de monomios $\Omega_{n,d_A} = \{m_1, \ldots, m_{|A|}\} \subset S$ determinado por A (definición 5.1.2), ordenados por el orden lexicográfico. Consideramos ahora unas nuevas variables $w_1, \ldots, w_{|A|}$ y el anillo de polinomios $S' = k[w_1, \ldots, w_{|A|}]$. El ideal de anulación de Y_{n,d_A} es el ideal homogéneo $I(Y_{n,d_A}) \subset S'$, núcleo del morfismo de anillos

$$\begin{aligned} \rho : S' &\to k[\Omega_{n,d_A}] \\ w_i &\mapsto \rho(w_i) = m_i,\ 1 \leq i \leq |A|. \end{aligned}$$

Observación 5.1.5. Si denotamos $A(Y_{n,d_A}) := S'/I(Y_{n,d_A})$ el anillo de coordenadas de Y_{n,d_A}, entonces ρ induce un isomorfismo de k-álgebras graduadas $A(Y_{n,d_A}) \simeq k[\Omega_{n,d_A}]$.

Notación. Denotamos $\mathrm{HF}_A = \mathrm{HF}_{Y_{n,d_A}}$ la función de Hilbert de la variedad Y_{n,d_A} y $\mathrm{HP}_A = \mathrm{HP}_{Y_{n,d_A}}$ el polinomio de Hilbert de Y_{n,d_A}.

Al igual que en el caso de las curvas monomiales proyectivas, es útil tener caracterizado el ideal $I(Y_{n,d_A})$:

Proposición 5.1.6. Con las notaciones anteriores, $I(Y_{n,d_A}) \subset S'$ es un ideal binomial y primo definido por

$$\begin{aligned} I(Y_{n,d_A}) &= \left\langle \prod_{i=1}^{|A|} w_i^{\alpha_i} - \prod_{i=1}^{|A|} w_i^{\beta_i} : \prod_{i=1}^{|A|} m_i^{\alpha_i} = \prod_{i=1}^{|A|} m_i^{\beta_i},\ \alpha_i, \beta_i \in \mathbb{N}_0 \right\rangle \\ &= \left\langle \mathbf{w}^\alpha - \mathbf{w}^\beta : \rho(\mathbf{w}^\alpha) = \rho(\mathbf{w}^\beta), \alpha, \beta \in \mathbb{N}_0^{|A|} \right\rangle. \end{aligned}$$

Para demostrar este resultado vamos a utilizar ideas similares a las de la sección 3.2. Primero definimos una relación de equivalencia en el conjunto de monomios de S':

$$\mathbf{w}^\alpha \sim \mathbf{w}^\beta \Leftrightarrow \rho(\mathbf{w}^\alpha) = \rho(\mathbf{w}^\beta).$$

Teniendo en cuenta la descripción de los monomios de Ω_{n,d_A}, tenemos que

$$\mathbf{w}^\alpha \sim \mathbf{w}^\beta \Leftrightarrow \begin{cases} |\alpha| = |\beta|, \\ |\alpha|_{\mathbf{a}} = |\beta|_{\mathbf{a}}, \ \forall \mathbf{a} \in A, \end{cases} \tag{5.1.1}$$

donde $|\alpha| = \sum_{i=1}^{|A|} \alpha_i$ y $|\alpha|_{\mathbf{a}} = \sum_{i=1}^{|A|} a_i \alpha_i$, si $\alpha = (\alpha_1, \ldots, \alpha_{|A|})$.

Esta relación de equivalencia nos permite escribir cada polinomio $f \in S'$ como suma de sus componentes simples para la relación de equivalencia inducida por ρ.

Lema 5.1.7. Sea $f \in S'$ un polinomio no nulo, y sea $f = f_1 + \cdots + f_c$ la expresión de f como suma de sus componentes simples. Si $f \in \ker \rho$, entonces $f_i \in \ker \rho$ para cada $i = 1, \ldots, c$.

Demostración. Sea $i \in \{1, \ldots, c\}$. De (5.1.1) se deduce que f_i es homogéneo, luego podemos escribirlo en la forma $f_i = \sum_{j=1}^{l} \lambda_j \mathbf{w}^{\alpha_j}$ para ciertos $\alpha_j \in \mathbb{N}_0^{|A|}$ con $\mathbf{w}^{\alpha_j} \neq \mathbf{w}^{\alpha_{j'}}$ si $j \neq j'$. Como $\mathbf{w}^{\alpha_j} \sim \mathbf{w}^{\alpha_{j'}}$ para todo $j, j' = 1, \ldots, l$, entonces

$$\rho(f_i) = \left(\sum_{j=1}^{l} \lambda_{\alpha_j} \right) \rho(\mathbf{w}^{\alpha_1}),$$

y denotamos $\rho_i = \rho(\mathbf{w}^{\alpha_1})$. Ahora, si $i \neq i'$, entonces $\rho_i \neq \rho_{i'}$, de donde deducimos que $\rho(f_i) = 0$. □

Demostración de la proposición 5.1.6. Sea $f \in \ker \rho$ un polinomio no nulo. Por el lema 5.1.7 podemos suponer que f es simple. Escribimos $f = \sum_{i=1}^{l} \lambda_i \mathbf{w}^{\alpha_i}$ para ciertos $\lambda_i \in k^*$ y monomios $\mathbf{w}^{\alpha_i}$ distintos dos a dos. Como $\rho(f) = 0$ y $\rho(\mathbf{w}^{\alpha_i}) = \rho(\mathbf{w}^{\alpha_{i'}})$ para todo $i, i' = 1, \ldots, l$, entonces $\sum_{i=1}^{l} \lambda_i = 0$. Por lo tanto, $\lambda_1 = -\sum_{i=2}^{l} \lambda_i$ y podemos escribir

$$f = \sum_{i=2}^{l} \lambda_i \left(\mathbf{w}^{\alpha_i} - \mathbf{w}^{\alpha_1} \right) \in \left\langle \mathbf{w}^\alpha - \mathbf{w}^\beta : \mathbf{w}^\alpha \sim \mathbf{w}^\beta, \alpha, \beta \in \mathbb{N}_0^{|A|} \right\rangle.$$

□

Proposición 5.1.8 ([3, Prop. 3.3])**.** Sean $n \in \mathbb{N}$ y $A \subset \mathbb{N}_0^n$ un subconjunto finito. Entonces:

(1) $\mathrm{HF}_A(s) = |sA|$ para todo $s \in \mathbb{N}_0$.

(2) Existe un polinomio $p_A(z) \in \mathbb{Q}[z]$ de grado $r = \dim(Y_{n,d_A}) \leq n$, el polinomio de Hilbert de Y_{n,d_A}, tal que $p_A(s) = |sA|$ para todo s suficientemente grande.

Demostración. (1) El isomorfismo inducido por ρ, $\bar{\rho} : A(Y_{n,d_A}) \xrightarrow{\sim} k[\Omega_{n,d_A}]$ verifica $\bar{\rho}\left(A(Y_{n,d_A})_s\right) = k[\Omega_{n,d_A}]_{sd_A}$ para cada $s \in \mathbb{N}_0$. Por lo tanto,

$$\mathrm{HF}_A(s) = \dim_k A(Y_{n,d_A})_s = \dim_k k[\Omega_{n,d_A}]_{sd_A}, \text{ para todo } s \geq 0.$$

Por otra parte, una base del k-espacio vectorial $k[\Omega_{n,d_A}]_{sd_A}$ es el conjunto de monomios

$$\left\{ \prod_{j=1}^{s} m_{i_j} : m_{i_j} \in \Omega_{n,d_A}, 1 \leq j \leq s \right\} = \left\{ x_0^{sd_A - |\alpha|} x_1^{\alpha_1} \dots x_n^{\alpha_n} : \alpha \in sA \right\}.$$

Por lo tanto, es claro que $|sA| = \mathrm{HF}_A(s)$ para todo $s \geq 0$.

(2) Basta aplicar el teorema 1.4.5 y la observación 1.4.7.

□

5.2. Dimensión y grado de la variedad Y_{n,d_A}

Hemos visto que para s suficientemente grande, $|sA|$ es un polinomio $p_A(z) \in \mathbb{Q}[z]$ de grado $r = \dim\left(Y_{n,d_A}\right)$ y su coeficiente líder es $\frac{\deg(Y_{n,d_A})}{r!}$, siendo $\deg(Y_{n,d_A})$ el grado de la variedad Y_{n,d_A}. Como Y_{n,d_A} es una proyección (monomial) de la variedad de Veronese X_{n,d_A}, que tiene dimensión n, entonces

$$\dim(Y_{n,d_A}) \leq n = \dim(X_{n,d_A}).$$

Por otra parte, podemos acotar también el grado de Y_{n,d_A},

$$\deg(Y_{n,d_A}) \leq d_A^n = \deg(X_{n,d_A}).$$

Veamos esto en algunos ejemplos:

Ejemplo 5.2.1. (1) Sean $n, d \in \mathbb{N}$ y consideramos el conjunto $A = \{\mathbf{a} \in \mathbb{N}_0^n : |\mathbf{a}| = a_1 + \dots + a_n \leq d\}$. En este caso tenemos $d_A = d$, $|A| = N_{n,d}$ y Ω_{n,d_A} es el conjunto constituido por todos los monomios de grado d en $S = k[x_0, x_1, \dots, x_n]$. Por lo tanto, Y_{n,d_A} es la variedad de Veronese $X_{n,d} \subset \mathbb{P}^{N_{n,d}-1}$, y en este caso no baja ni el grado ni la dimensión.

(2) Vamos a analizar lo que ocurre en los dos conjuntos del ejemplo 5.1.1.

- Para el conjunto $A^1 = \{(0,0), (3,0), (2,2), (0,1)\}$ tenemos $d_{A^1} = 4 = |A^1|$. La variedad monomial asociada al conjunto A^1, denotada $Y^1_{2,4} \subset \mathbb{P}^3$, es la proyección monomial de $X_{2,4} \subset \mathbb{P}^{14}$ parametrizada por $\Omega^1_{2,4} = \{x_0^4, x_0^3 x_2, x_0 x_1^3, x_1^2 x_2^2\}$. El ideal de anulación de $Y^1_{2,4}$ es

$$\begin{aligned} I(Y^2_{2,4}) &= \left\langle w_0 - x_0^4, w_1 - x_0^3 x_2, w_2 - x_0 x_1^3, w_3 - x_1^2 x_2^2 \right\rangle \cap k[w_0, w_1, w_2, w_3] \\ &= \left\langle w_0^5 w_3^3 - w_2^2 w_1^6 \right\rangle, \end{aligned}$$

de donde deducimos que $Y^1_{2,4}$ es una superficie de grado 8 en $\mathbb{P}^3$.

- Para el conjunto $A^2 = \{(0,0),(2,0),(0,2),(1,1)\}$ tenemos $d_{A^2} = 4 = |A^2|$ y la proyección monomial de $X_{2,4} \subset \mathbb{P}^{14}$ asociada a A^2, denotada $Y^2_{2,4} \subset \mathbb{P}^3$, está parametrizada por $\Omega^2_{2,4} = \{x_0^4, x_0^3x_2, x_0^2x_1^2, x_1^2x_2^2\}$. El ideal de anulación de $Y^2_{2,4}$ es

$$\begin{aligned} I(Y^2_{2,4}) &= \left\langle w_0 - x_0^4, w_1 - x_0^3x_2, w_2 - x_0^2x_1^2, w_3 - x_1^2x_2^2 \right\rangle \cap k[w_0,w_1,w_2,w_3] \\ &= \left\langle w_0^2w_3 - w_2w_1^2 \right\rangle, \end{aligned}$$

de donde deducimos que $Y^2_{2,4}$ es una superficie cúbica de $\mathbb{P}^3$.

En ambos casos no baja la dimensión pero sí el grado, puesto que $\deg(X_{2,4}) = 16$.

(3) Sean $n = 2$ y $A = \{(3,1),(2,2),(1,3),(0,4)\} \subset \mathbb{N}_0^2$. Notemos que este conjunto no verifica las hipótesis que estamos pidiendo al conjunto A, puesto que el conjunto de monomios que define es $\Omega_{2,4} = \{x_1^3x_2, x_1^2x_2^2, x_1x_2^3, x_2^4\}$ y $\gcd(m \in \Omega_{2,4}) = x_2$. Lo que tenemos que hacer es trasladar A por el vector $(0,-1)$, obteniendo $A' = \{(3,0),(2,1),(1,2),(0,3)\}$. De este modo, la proyección monomial $Y_{2,4} \subset \mathbb{P}^3$ de $X_{2,4} \subset \mathbb{P}^{14}$ asociada al conjunto A' es la curva racional normal de grado 3. Notemos que, en este caso, $\dim(Y_{2,4}) < \dim(X_{2,4})$.

De hecho, ya sabemos calcular la dimensión y el grado de estas variedades. Si denotamos $A = \{\mathbf{a}^1, \ldots, \mathbf{a}^{|A|}\}$, entonces por la proposición 1.5.7, la dimensión de $Y_{n,d}$ es

$$\dim(Y_{n,d_A}) = \dim\left(k[\Omega_{n,d_A}]\right) - 1 = \operatorname{rk}\left(\Lambda_{n,d_A}\right) - 1,$$

donde Λ_{n,d_A} es la matriz definida por los exponentes de los monomios en Ω_{n,d_A}, es decir,

$$\Lambda_{n,d_A} = \begin{pmatrix} d_A - |\mathbf{a}^1| & d_A - |\mathbf{a}^2| & \ldots & d_A - |\mathbf{a}^{|A|}| \\ a_1^1 & a_1^2 & \ldots & a_1^{|A|} \\ \vdots & \vdots & \ddots & \vdots \\ a_n^1 & a_n^2 & \ldots & a_n^{|A|} \end{pmatrix},$$

si $\mathbf{a}^i = (a_1^i, \ldots, a_n^i)$ para cada $i = 1, \ldots, |A|$.
Por otra parte, según la proposición 1.5.21, si r denota el rango de la matriz Λ_{n,d_A}, el grado de $Y_{n,d}$ se puede calcular de la forma siguiente:

$$\deg\left(Y_{n,d}\right) = \frac{r! \cdot \operatorname{vol}\left(\operatorname{conv}\left(\{\mathbf{a}^1, \ldots, \mathbf{a}^{|A|}, \mathbf{0}\}\right)\right)}{\Delta_r}, \tag{5.2.1}$$

siendo Δ_r el máximo común divisor de los menores $r \times r$ de la matriz Λ_{n,d_A} (que son todos no nulos).

5.3. Recuperando algunos resultados

Nos centramos ahora en estudiar los subconjuntos finitos $A \subset \mathbb{N}_0^n$ tales que la dimensión de Y_{n,d_A} sea máxima, es decir, $\dim\left(Y_{n,d_A}\right) = n$. Como

$$\dim(Y_{n,d_A}) = \operatorname{rk}(\Lambda_{n,d_A}) - 1 \leq \min\{n+1, |A|\} - 1 = \min\{n, |A| - 1\},$$

si $\dim(Y_{n,d_A}) = n$, en particular se verifica $|A| \geq n+1$. Veamos entonces cómo es la función $s \mapsto |sA|$ para valores pequeños de $|A|$, $|A| = n+1$ y $|A| = n+2$. Presentamos aquí demostraciones más sencillas para fórmulas ya conocidas.

Proposición 5.3.1 ([3, Prop. 3.7])**.** Sean $n \in \mathbb{N}$ y $A \subset \mathbb{N}_0^n$ un subconjunto finito. Denotamos por Y_{n,d_A} a la variedad asociada al conjunto A, sea $e = \deg(Y_{n,d_A})$ su grado y suponemos que $\dim(Y_{n,d_A}) = n$.

(a) Si $|A| = n+1$, entonces

$$|sA| = p_A(s) = \binom{n+s}{n}, \text{ para todo } s \geq 0.$$

(b) Si $|A| = n+2$, entonces $n_0(A) = e-n-1$ y

$$|sA| = \begin{cases} \binom{n+s+1}{n+1} & \text{si} \quad 0 \leq s \leq e-n-2, \\ \binom{n+s+1}{n+1} - \binom{n+1+s-e}{n+1} & \text{si} \quad s \geq e-n-1. \end{cases}$$

Demostración. (a) El conjunto A define una aplicación racional $\psi : \mathbb{P}^n \dashrightarrow \mathbb{P}^n$, de modo que $Y_{n,d_A} = \overline{\psi(\mathbb{P}^n)}$ es una variedad de dimensión n. Entonces tenemos $Y_{n,d_A} = \mathbb{P}^n$ y

$$|sA| = \mathrm{HF}_S(s) = \binom{n+s}{n}, \text{ para todo } s \geq 0.$$

Por lo tanto, $|sA| = p_A(s) = \binom{n+s}{n}$ para todo $s \geq 0$.

(b) En este caso, A define una aplicación racional $\psi : \mathbb{P}^n \dashrightarrow \mathbb{P}^{n+1}$ y se tiene que $Y_{n,d_A} = \overline{\psi(\mathbb{P}^n)} \subset \mathbb{P}^{n+1}$ es una hipersuperficie de $\mathbb{P}^{n+1}$ de grado e. Por lo tanto, existe un polinomio homogéneo $F \in S' = k[w_0, \ldots, w_{n+1}]$ de grado e tal que $I(Y_{n,d_A}) = \langle F \rangle$. Si ahora consideramos el morfismo de k-álgebras que consiste en la multiplicación por F, $\varphi_F : S \to S'$, tenemos que φ_F es graduado de grado e. Por lo tanto, $\varphi_F : S'(-e) \to S'$ nos permite escribir la siguiente sucesión exacta de k-álgebras graduadas

$$0 \to S'(-e) \xrightarrow{\varphi_F} S' \to S'/I(Y_{n,d_A}) \to 0.$$

En consecuencia, por el lema 1.4.3 obtenemos

$$\mathrm{HF}_A(s) = \mathrm{HF}_{S'}(s) - \mathrm{HF}_{S'(-e)}(s) = \binom{n+1+s}{n+1} - \binom{n+1+s-e}{n+1}$$

$$= \begin{cases} \binom{n+1+s}{n+1} & \text{si} \quad 0 \leq s \leq e-n-2, \\ \binom{n+1+s}{n+1} - \binom{n+1+s-e}{n+1} & \text{si} \quad s \geq e-n-1. \end{cases}$$

Entonces es claro que $n_0(A) = e-n-1$.

□

Observación 5.3.2. Como consecuencia inmediata del resultado anterior, obtenemos el teorema 2.2.5: si $|A| = n+2$ y $\mathbb{Z}(A-A) = \mathbb{Z}^n$, entonces por el teorema 2.2.2 tenemos que $e = \mathrm{vol}(\mathrm{conv}(A))$ y, por tanto,

$$|sA| = \begin{cases} \binom{s+n+1}{n+1}, & \text{si} \quad 0 \leq s \leq \mathrm{vol}(\mathrm{conv}(A)) \cdot n! - n - 2, \\ \binom{s+n+1}{n+1} - \binom{s-\mathrm{vol}(\mathrm{conv}(A))\cdot n!+n+1}{n+1}, & \text{si} \quad s \geq \mathrm{vol}(\mathrm{conv}(A)) \cdot n! - n - 1. \end{cases}$$

En particular, $n_0(A) = \mathrm{vol}(\mathrm{conv}(A)) \cdot n! - n - 1$.

Ejemplo 5.3.3. (I) Consideramos los dos conjuntos del ejemplo 5.1.1,

$$A^1 = \{(0,0),(3,0),(2,2),(0,1)\} \text{ y } A^2 = \{(0,0),(2,0),(2,2),(0,1)\}.$$

Para $i = 1, 2$ se tiene $\mathbb{Z}(A^i - A^i) = \mathbb{Z}^2$ y los grados de las variedades $Y^1_{2,1}$ e $Y^2_{2,1}$ son

$$\deg(Y^1_{2,1}) = 8, \ \deg(Y^2_{2,1}) = 4.$$

Aplicando la proposición 5.3.1 obtenemos

$$p_{A^1}(z) = \binom{z+3}{3} - \binom{z-5}{3} = 4(z^2 - 4z + 9),$$
$$p_{A^2}(z) = \binom{z+3}{3} - \binom{z}{3} = \frac{3}{2}(z^2 + z) + 1.$$

(II) Sea $A = \{(3,0),(2,1),(1,2),(0,3)\} \subset \mathbb{N}_0^2$. En este caso ya sabemos que $\dim(Y_{n,d_A}) < \dim(X_{n,d_A})$. Por lo tanto, no estamos en condiciones de aplicar la proposición 5.3.1. Lo que sí podemos hacer es aplicar la fórmula combinatoria (5.2.1) para calcular el grado de Y_{n,d_A}. Para ello, denotamos $\bar{A} = \{(0,3,0),(0,2,1),(0,1,2),(0,0,3)\}$, el conjunto formado por los exponentes de los monomios en $\Omega_{2,3}$, y consideramos la matriz cuyas columnas son las coordenadas de los elementos de $\bar{A}$,

$$\Lambda_{2,3} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \mathrm{diag}(1,3,0),$$

donde el símbolo $\sim$ denota que se han realizado operaciones por filas y por columnas sobre la matriz $\Lambda_{2,3}$, de modo que $\mathrm{diag}(1,3,0)$ es su forma normal de Smith. Entonces $r = \mathrm{rk}(\Lambda_{2,3}) = 2$, $\Delta_2 = 1 \cdot 3 = \gcd(3,6,9)$ y el grado de $Y_{2,3}$ es

$$\deg(Y_{2,3}) = \frac{r! \cdot \mathrm{vol}\left(\mathrm{conv}\left(\bar{A} \cup \{(0,0,0)\}\right)\right)}{\Delta_2} = \frac{2! \cdot 9/2}{3} = 3.$$

5.4. Algunos resultados más

5.4.1. Fórmula recursiva para calcular el grado de Y_{n,d_A}

Ahora vamos a dar un método para calcular el término líder del polinomio $p_A(z) \in \mathbb{Q}[z]$ utilizando técnicas de geometría algebraica.

Sean $A_1 \subsetneq A_2 \subset \mathbb{N}_0^n$ dos subconjuntos de cardinal finito con $|A_2| = |A_1| + 1$, con variedades proyectivas asociadas

$$A_1 \mapsto Y_{n,d_{A_1}} \subset \mathbb{P}^{|A_1|-1},$$
$$A_2 \mapsto Y_{n,d_{A_2}} \subset \mathbb{P}^{|A_2|-1} \simeq \mathbb{P}^{|A_1|}.$$

Notemos que $Y_{n,d_{A_1}}$ se obtiene a partir de $Y_{n,d_{A_2}}$ proyectando desde un punto $p_{2,1} \in \mathbb{P}^{|A_2|-1} \simeq \mathbb{P}^{|A_1|}$. En términos de coordenadas, esta proyección consiste simplemente en eliminar la coordenada correspondiente al elemento $\mathbf{a} \in A_2 \setminus A_1$.

Lema 5.4.1. Siguiendo las notaciones anteriores, sea $\pi_{2,1} : Y_{n,d_{A_2}} \to Y_{n,d_{A_1}}$ la proyección desde el punto $p_{2,1} \in \mathbb{P}^{|A_2|-1}$. Entonces $\pi_{2,1}$ es una aplicación racional finita de grado $\deg(\pi_{2,1}) = |\pi_{2,1}^{-1}(q)|$, donde $q \in Y_{n,d_{A_1}}$ es un punto genérico. Además, se verifica lo siguiente:

$$\deg(\pi_{2,1}) \cdot \deg(Y_{n,d_{A_1}}) = \begin{cases} \deg(Y_{n,d_{A_2}}) & \text{si } p_{2,1} \notin Y_{n,d_{A_1}}, \\ \deg(Y_{n,d_{A_2}}) - 1 & \text{si } p_{2,1} \in Y_{n,d_{A_1}} \text{ es liso}, \\ \deg(Y_{n,d_{A_2}}) - n_{2,1} & \text{s } p_{2,1} \in Y_{n,d_{A_1}} \text{ tiene multiplicidad } n_{2,1}. \end{cases} \tag{5.4.1}$$

Demostración. La aplicación $\pi_{2,1} : Y_{n,d_{A_2}} \to Y_{n,d_{A_1}}$ induce un morfismo inyectivo entre los anillos coordenados $k[\Omega_{n,d_1}] \hookrightarrow k[\Omega_{n,d_2}]$, de modo que $k[\Omega_{n,d_2}]$ es entero sobre $k[\Omega_{n,d_1}]$. Por lo tanto, la aplicación racional $\pi_{2,1}$ es finita. La otra parte del lema es una consecuencia sencilla de los teoremas de Bertini y Bézout, los detalles se pueden consultar en [18, Example 18.16]. □

La idea de la construcción es iterar este proceso y, de este modo, calcular el término líder del polinomio $p_A(z) \in \mathbb{Q}[z]$. Para ello, si denotamos $|A| = r$, consideramos una cadena

$$A = A_0 \subsetneq A_1 \subsetneq \cdots \subsetneq A_{N_{n,d}-r} = \mathcal{M}_{n,d} \subset \mathbb{N}_0^n,$$

donde $|A_i| = |A_{i-1}| + 1$ y $\mathcal{M}_{n,d}$ denota el subconjunto de $\mathbb{N}_0^n$ que corresponde a todos los monomios de grado d en S, es decir, $\mathcal{M}_{n,d} = \{\mathbf{a} \in \mathbb{N}_0^n : |\mathbf{a}| = d\}$. Entonces para cada $i = 1, \ldots, N_{n,d} - r$, la variedad proyectiva n-dimensional $Y_{n,d_A} \subset \mathbb{P}^{|A_{i-1}|-1}$ se obtiene proyectando $Y_{n,d_{A_i}} \subset \mathbb{P}^{|A_i|-1}$ desde un punto $p_{i,i-1}$. Denotamos por $\pi_{i,i-1}$ a esta proyección y definimos

$$d_{i,i-1} := \begin{cases} 0 & \text{si } p_{i,i-1} \notin Y_{n,d_{A_i}}, \\ 1 & \text{si } p_{i,i-1} \in Y_{n,d_{A_i}} \text{ es un punto liso }, \\ n_{i,i-1} & \text{si } p_{i,i-1} \in Y_{n,d_{A_i}} \text{ tiene multiplicidad } n_{i,i-1}. \end{cases}$$

Proposición 5.4.2 ([3, Prop. 3.10])**.** Sean $A \subset \mathbb{N}_0^n$ un subconjunto finito tal que $\dim(Y_{n,d_A}) = n$ y $p_A(z) \in \mathbb{Q}[z]$ el polinomio correspondiente al conjunto A. Entonces el coeficiente líder de p_A es

$$\frac{\deg(Y_{n,d_A})}{n!} = \frac{1}{n! \cdot \prod_{i=1}^{N_{n,d}-r} \deg \pi_{i,i-1}} \left[d^n - \sum_{i=1}^{N_{n,d}-r} \left(n_{i,i-1} \prod_{j=i+1}^{N_{n,d}-r} \deg \pi_{j,j-1} \right) \right].$$

Ejemplo 5.4.3. Consideramos el conjunto $A = \{(0,0),(3,0),(2,0),(2,2),(0,1)\} \subset \mathbb{N}_0^n$ y la superficie $Y_{2,4} \subset \mathbb{P}^4$ asociada, es decir, la superficie parametrizada por el conjunto de monomios $\Omega_{2,4} = \{x_0^4, x_0x_1^3, x_0^2x_1^2, x_1^2x_2^2, x_0^3x_2\}$. Si fijamos coordenadas homogéneas $(w_0 : w_1 : w_2 : w_3 : w_4)$ en $\mathbb{P}^4$, entonces $Y_{2,4}$ está definida paramétricamente por

$$Y_{2,4} = \overline{\{(x_0^4 : x_0^3x_2 : x_0^2x_1^2 : x_0x_1^3 : x_0^2x_1^2) : (x_0 : x_1 : x_2) \in \mathbb{P}^2\}},$$

y el ideal $I(Y_{2,4}) \subset S' = k[w_0, \ldots, w_4]$ viene dado por

$$\begin{aligned} I(Y_{2,4}) &= \left\langle w_0 - x_0^4, w_1 - x_0^3x_2, w_2 - x_0^2x_1^2, w_3 - x_0x_1^3, w_4 - x_1^2x_2^2 \right\rangle \cap k[w_0, \ldots, w_4] \\ &= \left\langle w_2^3 - w_0w_3^2, w_1^2w_2 - w_0^2w_4, w_1^2w_3^2 - w_0w_2^2w_4 \right\rangle. \end{aligned}$$

El polinomio de Hilbert de $Y_{2,4}$ es $\mathrm{HP}_{Y_{2,4}}(z) = 4z^2 - 2z + 3$, de donde deducimos que $Y_{2,4}$ es una superficie de grado 8 en $\mathbb{P}^4$.
Sean $A^1 = \{(0,0),(3,0),(2,2),(0,1)\}$ y $A^2 = \{(0,0),(2,0),(2,2),(0,1)\}$ los conjuntos del ejemplo 5.1.1. Si denotamos $p_0 = (1:0:0:0:0)$, $p_1 = (0:1:0:0:0)$, ..., $p_4 = (0:0:0:0:1)$ y $\pi_i : Y_{2,4} \to \mathbb{P}^3$ es la proyección de $Y_{2,4}$ desde el punto p_i, entonces

$$\pi_2(Y_{2,4}) = Y_{2,4}^1, \text{ y } \pi_3(Y_{2,4}) = Y_{2,4}^2.$$

Ahora podemos aplicar la fórmula (5.4.1) para calcular el grado de las variedades $Y_{2,4}^1$ e $Y_{2,4}^2$:

- Notemos que $p_2 \notin Y_{2,4}$ (basta sustituir las coordenadas del punto en las ecuaciones de $Y_{2,4}$). Además, la proyección π_2 está definida por

  $$(x_0^4 : x_0^3x_2 : x_0^2x_1^2 : x_0x_1^3 : x_1^2x_2^2) \mapsto (x_0^4 : x_0^3x_2 : x_0x_1^3 : x_1^2x_2^2),$$

  luego está claro que su grado es $\deg(\pi_2) = 1$. Entonces tenemos

  $$\deg(Y_{2,4}^1) = \deg(Y_{2,4}) = 8.$$

- Por otra parte, el punto $p_3 \in Y_{2,4}$, puesto que los generadores de $I_{2,4}$ se anulan en $(0,0,0,0,1)$. La multiplicidad de p_3 es $n_3 = 2$ ($[*]$) y la proyección π_3 viene dada por

  $$(x_0^4 : x_0^3x_2 : x_0^2x_1^2 : x_0x_1^3 : x_1^2x_2^2) \mapsto (x_0^4 : x_0^3x_2 : x_0^2x_1^2 : x_1^2x_2^2),$$

  luego está claro que su grado es $\deg(\pi_3) = 2$ (dos puntos con distinto signo en x_1 pertenecen a la misma fibra). Entonces tenemos

  $$2 \cdot \deg(Y_{2,4}^2) = \deg(Y_{2,4}) - 2 \Rightarrow \deg(Y_{2,4}^2) = 3.$$

Estos cálculos concuerdan con lo que ya sabíamos, puesto que

$$\begin{aligned} \mathrm{HP}_{Y_{2,1}^1}(z) &= 4z^2 - 16z + 36, \\ \mathrm{HP}_{Y_{2,1}^2}(z) &= 3/2(z^2 + z) + 1. \end{aligned}$$

[∗] Para calcular la multiplicidad de $p_3 \in Y_{2,4}$, trabajamos en la carta afín $w_3 \neq 0$, en la que el ideal de la variedad es

$$I = \left\langle w_2^3 - w_0, w_1^2 w_2 - w_0^2 w_4, w_1^2 - w_0 w_2^2 w_4 \right\rangle \subset k[w_0, w_1, w_2, w_4].$$

La multiplicidad del punto en la variedad es la multiplicidad del ideal homogéneo que define el cono tangente:

```
> LIB "sing.lib";
> LIB "poly.lib";
> ring r = 0, (w0,w1,w2,w4), ds;
> ideal I = w2^3-w0,w1^2*w2-w0^2*w4,w1^2-w0*w2^2*w4;
> tangentcone(I);
_[1]=w0
_[2]=w1^2
> degree(std(I));
// dimension (local)   = 2
// multiplicity = 2
```

5.4.2. Cotas para $n_0(A)$

Hemos presentado los aspectos más relevantes para el estudio de los conjuntos suma utilizando álgebra conmutativa y geometría algebraica. El estudio que sigue en esta dirección está centrado en obtener cotas para el número $n_0(A)$ imponiendo restricciones sobre el conjunto A. Para finalizar esta sección presentamos algunos resultados en esta línea.

Definición 5.4.4. Sea $A \subset \mathbb{N}_0^n$ un subconjunto finito. Se dice que la envolvente convexa de A en $\mathbb{R}^n$, $\mathrm{conv}(A)$, es un *n-símplice* si existe un subconjunto $B = \{\mathbf{u}_1, \ldots, \mathbf{u}_{n+1}\} \subset A$ de cardinal $|B| = n+1$ tal que el conjunto $B - B$ genera $\mathbb{R}^n$ y $\mathrm{conv}(A) = \mathrm{conv}(B)$.

Teorema 5.4.5 ([3, Thm. 4.2])**.** Sea $A \subset \mathbb{N}_0^n$ un subconjunto finito tal que $\mathrm{conv}(A)$ es un n-símplice. Entonces

$$n_0(A) \leq (n+1)\left(n! \frac{\mathrm{vol}\left(\mathrm{conv}\left(A\right)\right)}{[\mathbb{Z}^n : \mathbb{Z}(A-A)]} - |A| + n\right) + 1.$$

Si además $\mathbb{Z}(A-A) = \mathbb{Z}^n$, entonces

$$n_0(A) \leq (n+1)! \cdot \mathrm{vol}\left(\mathrm{conv}(A)\right) - \mathrm{máx}\left\{3n+1, (n+1)(|A|-n) - 1\right\}.$$

Dado un subconjunto finito $A \subset \mathbb{N}_0^n$, denotamos $\mathbf{v}_1 = (d_A, 0, \ldots, 0)$, $\ldots$, $\mathbf{v}_n = (0, \ldots, 0, d_A)$.

Teorema 5.4.6 ([3, Thm. 4.5])**.** Sea $A \subset \mathbb{N}_0^n$ un subconjunto finito tal que $\{\mathbf{0}, \mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset A$. Si se verifica cualquiera de las condiciones siguientes,

(1) $n = 1$,

(2) $k[\Omega_{n,d_A}]$ es un anillo Cohen-Macaulay,

(3) $\deg(Y_{n,d_A}) \leq |A| - n$,

(4) $|A| - n - 1 \leq \deg(Y_{n,d_A})/d_A$,

(5) $\deg(Y_{n,d_A}) = d_A^n$ y $d_A \leq n$,

entonces

$$n_0(A) \leq \deg(Y_{n,d_A}) - |A| + n + 2.$$

Si además Y_{n,d_A} es una variedad lisa, entonces se verifica

$$n_0(A) \leq \text{mín}\{n(d_A - 2) + 1, \deg(Y_{n,d_A}) - |A| + n + 2\}.$$

La clave para demostrar este resultado está en que bajo cualquiera de las hipótesis (1)-(5), la conjetura de Eisenbud-Goto es cierta.

Teorema 5.4.7 ([3, Thm. 4.6])**.** Sea $A \subset \mathbb{N}_0^n$ un subconjunto finito tal que $\{\mathbf{0}, \mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset A$. Entonces

$$n_0(A) \leq (d_A - 1)(|A| - n - 1) + 1.$$

Además, si $\deg(Y_{n,d_A}) \geq |A| - n + 1$, entonces

$$n_0(A) \leq \text{mín}\left\{(n+1)\left(\deg(Y_{n,d_A}) - |A| + n - 1\right) + 3, (d_A - 1)(|A| - n - 1) + 1\right\}.$$

Nuevas líneas de investigación

Los recientes trabajos [11], [12] y [3] han abierto una línea de investigación muy interesante. En estos 3 trabajos se establecen puentes entre la combinatoria aditiva y el álgebra conmutativa que permiten entender mejor algunos resultados ya existentes y encontrar resultados nuevos en ambas áreas.

El trabajo que sigue comienza por estudiar las curvas proyectivas monomiales para entender perfectamente cómo se comporta la regularidad de Castelnuovo-Mumford. En este sentido, la definición de la regularidad en términos homológicos es muy útil. Esta es la línea que estamos siguiendo en el trabajo [13], que esperamos esté disponible pronto en arXiv. En este trabajo, los conjuntos suma son una herramienta muy útil, e incluso un lenguaje para expresar de manera clara algunas ideas intuitivas sobre semigrupos que no son fáciles de escribir sin utilizar conjuntos suma.

Después de entender bien todo lo que sucede con las curvas monomiales, el siguiente paso es estudiar las superficies monomiales proyectivas. Para este fin, comenzaremos trabajando en el caso Cohen-Macaulay y después abordaremos el caso general. Si el trabajo es fructífero, intentaremos generalizar los resultados a variedades monomiales proyectivas de dimensión $3, 4, \ldots$

En conclusión, queda mucho trabajo por hacer en esta dirección y todo parece indicar que se van a descubrir resultados interesantes a partir de esta conexión entre la combinatoria aditiva y el álgebra conmutativa.

Bibliografía

[1] M. F. Atiyah and I. G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley series in mathematics; 361. Addison-Wesley, Reading, Massachusetts, 1969.

[2] W. Bruns and J. Herzog. *Cohen-Macaulay rings*. Cambridge studies in advanced mathematics; 39. Cambridge University Press, second edition, 1998.

[3] L. Colarte-Gómez, J. Elias, and R. M. Miró-Roig. Sumsets and Veronese varieties. *Collectanea Mathematica*, 2022.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer New York, 2nd edition, 1997.

[5] D. A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics, 185. Springer New York, New York, NY, 1st ed. 19 edition, 1998.

[6] M. J. Curran and L. Goldmakher. Khovanskii's theorem and effective results on sumset structure. *Discrete analysis journal*, 27, 2021.

[7] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 4-3-0 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de, 2020.

[8] D. Eisenbud. *The Geometry of Syzygies. A Second Course in Algebraic Geometry and Commutative Algebra*. Graduate Texts in Mathematics, 229. Springer New York, first edition, 2005.

[9] D. Eisenbud and S. Goto. Linear free resolutions and minimal multiplicity. *Journal of Algebra*, 88(1):89–133, 1984.

[10] S. Eliahou. Wilf's conjecture and Macaulay's theorem. *Journal of the European Mathematical Society*, 20(9):2105–2129, 2018.

[11] S. Eliahou and E. Mazumdar. Iterated sumsets and hilbert functions. *Journal of Algebra*, 593:274–294, 2022.

[12] J. Elias. Sumsets and projective curves. *Mediterranean Journal of Mathematics (to appear)*, 2022.

[13] P. Gimenez and M. González-Sánchez. Castelnuovo-mumford regularity of projective monomial curves via sumsets. En fase de redacción.

[14] A. Granville and G. Shakan. The Frobenius postage stamp problem, and beyond. *Acta Mathematica Hungarica*, 161(2):700–718, 2020.

[15] A. Granville, G. Shakan, and A. Walker. Effective results on the size and structure of sumsets. *arXiv*, 2021.

[16] A. Granville and A. Walker. A tight structure theorem for sumsets. *Proceedings of the American Mathematical Society*, 149(10), 2021.

[17] L. Gruson, R. Lazarsfeld, and C. Peskine. On a theorem of Castelnuovo, and the equations defining space curves. *Inventiones mathematicae*, 72(3):491–506, 1983.

[18] J. Harris. *Algebraic Geometry: A First Course*. Graduate Texts in Mathematics 133. Springer-Verlag New York, 1st edition, 1992.

[19] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, 52. Springer New York, 1977.

[20] A. G. Khovanskii. Newton polyhedron, Hilbert polynomial, and sums of finite sets. *Functional Analysis and Its Applications*, 26(4):276–281, 1992.

[21] V. F. Lev. Structure theorem for multiple addition and the Frobenius problem. *Journal of Number Theory*, 58(1):79–88, 1996.

[22] E. Matlis. *One-Dimensional Cohen-Macaulay Rings*. Lecture Notes in Mathematics. Springer-Verlag, 1 edition, 1973.

[23] J. McCullough and I. Peeva. Counterexamples to the Eisenbud-Goto regularity conjecture. *Journal of the American Mathematical Society*, 31:1, 2017.

[24] M. B. Nathanson. Sums of finite sets of integers. *The American Mathematical Monthly*, 79(9):1010–1012, 1972.

[25] M. B. Nathanson. *Additive number theory: inverse problems and the geometry of sumsets*. Graduate texts in Mathematics; 165. Springer, New York, 1996.

[26] L. O'Carroll, F. Planas-Vilanova, and R. H. Villarreal. Degree and algebraic properties of lattice and matrix ideals. *SIAM Journal on Discrete Mathematics*, 28(1):394–427, 2014.

[27] J. L. Ramírez Alfonsín. *The diophantine Frobenius problem*. Oxford lectures series in mathematics and its applications; 30. Oxford University Press, 2005.

[28] T. Tao and V. Vu. *Additive combinatorics*. Cambridge studies in advanced mathematics; 105. Cambridge University Press, 2006.

[29] R. H. Villarreal. *Monomial Algebras*. Chapman & Hall. Taylor & Francis Group, 1st edition, 2001.

[30] R. H. Villarreal. *Monomial algebras*. Monographs and research notes in mathematics. CRC Press, 2nd edition, 2015.

[31] J. D. Wu, F. J. Chen, and Y. G. Chen. On the structure of the sumsets. *Discrete Mathematics*, 311(6), 2011.

Índice Alfabético